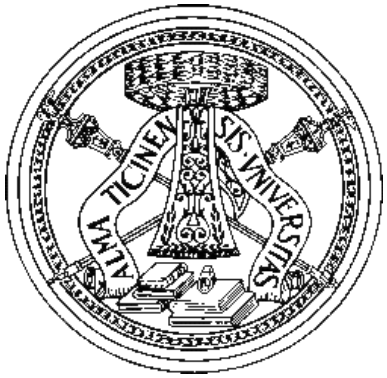
UNIVERSITÀ DEGLI STUDI DI PAVIA
FACOLTÀ DI SCIENZE MM.FF.NN.
Dipartimento di Matematica



Certifying exceptional primes for residual modular Galois representations

$\sim \cdot \sim$

Certificazione di numeri primi eccezionali per rappresentazioni di Galois residuali modulari

Relatore: Dott. Luis V. Dieulefait

Co-Relatore: Dott. Alberto Canonaco

TESI DI LAUREA SPECIALISTICA
di Samuele Anni
Mat. 360179/79

Anno Accademico 2009/2010

Certificazione di numeri primi eccezionali per rappresentazioni di Galois residuali modulari

Lo scopo della Tesi è quello di presentare alcuni risultati che permettono di stabilire una certificazione di eccezionalità per numeri primi rispetto a rappresentazioni di Galois residuali modulari, oggetto di studio in Geometria Aritmetica e Teoria Algebrica di Numeri.

Sia $\mathbb{Q}$ il campo dei numeri razionali e si indichi con $\overline{\mathbb{Q}}$ la chiusura algebrica di $\mathbb{Q}$. Il gruppo di Galois $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, detto gruppo di Galois assoluto di $\mathbb{Q}$, è il gruppo degli automorfismi del campo $\overline{\mathbb{Q}}$. Il gruppo $G_{\mathbb{Q}}$ è infinito e non commutativo. Al fine di studiarne la struttura, si introduce il concetto di rappresentazione galoisiana di dimensione d, definita come un omomorfismo di gruppi $\rho : G_{\mathbb{Q}} \to GL_d(\mathbf{K})$, dove $\mathbf{K}$ è un campo e $GL_d(\mathbf{K})$ è il gruppo delle matrici a coefficienti in $\mathbf{K}$ aventi determinante diverso da zero. Nei casi in cui la definizione ha senso, si richiede che l'omomorfismo ρ sia un'applicazione continua. Nel seguito considereremo soltanto rappresentazioni 2-dimensionali.

Si indichi con $\Gamma_0(N)$ il sottogruppo di $SL_2(\mathbb{Z})$ contenente le matrici che sono triangolari superiori modulo un intero positivo N. Si fissi un gruppo $\Gamma = \Gamma_0(N)$ per un certo N.

Definizione. *Una forma modulare di peso intero pari $k \geq 2$ rispetto a Γ è una funzione $f : \mathbb{H} \to \mathbb{C}$, dove $\mathbb{H}$ è il semipiano superiore, soddisfacente le condizioni seguenti:*

(i) *f è olomorfa su $\mathbb{H}$;*

(ii) *f soddisfa l'equazione funzionale $f(\gamma z) = (cz+d)^k f(z)$ per ogni scelta di $z \in \mathbb{H}$ e di $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, e dove γz indica l'elemento $\frac{az+b}{cz+d}$;*

(iii) *è possibile sviluppare $f(z)$ in serie di Fourier: $f(z) = \sum_n a_n q^n$ dove $q = e^{2\pi i z}$ e n è un razionale positivo con denominatore N. Questa espansione è detta q-espansione e N si dice livello della forma.*

In conclusione, si può affermare che una forma modulare è una funzione olomorfa sul semipiano superiore e all'infinito, simmetrica rispetto a Γ.

Si consideri ora lo spazio vettoriale complesso $S_k(\Gamma)$ delle forme modulari di peso k rispetto a Γ aventi il primo coefficiente di Fourier a_0 uguale a zero. Vi è una famiglia di operatori T_n, $\langle n \rangle$ per $n \geq 1$ intero, detti operatori di Hecke, che agiscono come endomorfismi su $S_k(\Gamma)$. Per esempio, se p è primo e non divide N, allora $T_p(f) = \sum_{p|n} a_n e^{2\pi \frac{n}{p} z} + p^{k-1} \sum_n a_n e^{2\pi (pn) z}$, dove

la prima somma è svolta sugli indici interi positivi n divisibili per p mentre la seconda su tutti gli indici interi positivi. Si supponga che $T_n f = a_n f$ per ogni $n \geq 1$, dove $a_1 = 1$ e a_n indica l'n-esimo coefficiente di Fourier di f. Una simile forma modulare, detta autofunzione o autoforma, riveste un particolare interesse aritmetico. Infatti, grazie al lavoro di Eichler-Shimura e Deligne-Serre, è possibile associare a una autofunzione f una rappresentazione galoisiana

$$\rho_f : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_f)$$

dove $\mathbb{Q}_f$ è il campo di numeri generato dai coefficienti a_n dello sviluppo di Fourier di f su $\mathbb{Q}$: $\mathbb{Q}_f = \mathbb{Q}(\{a_n\})$. Indicheremo con $\mathcal{O}_f$ l'anello degli interi di $\mathbb{Q}_f$. Utilizzando un abuso di notazione standard in Teoria dei numeri, se $\ell \in \mathbb{Z}$ primo e $\lambda \subset \mathcal{O}_f$ ideale primo, indicheremo con $\lambda \mid \ell$ se $\ell \in \lambda$ e con $\lambda \in \mathcal{O}_f$ la condizione $\lambda \subset \mathcal{O}_f$.

Fissato un primo $\ell \in \mathbb{Z}$, considero $\lambda \in \mathcal{O}_f$ ideale primo, tale che $\lambda \mid \ell$, è quindi possibile costruire una rappresentazione residuale $\overline{\rho_\lambda}$ indotta da ρ_f:

$$\overline{\rho_\lambda} : G_{\mathbb{Q}} \to GL_2(\mathbf{F}_\lambda)$$

dove $\mathbf{F}_\lambda = \mathcal{O}_f/\lambda$ è un campo finito di caratteristica ℓ. Oggetto di questo elaborato è lo studio delle rappresentazioni residuali indotte da ρ_f. Ricordiamo un risultato dovuto a Ribet, per una referenza [27] e [28]:

Teorema. *Per ogni λ eccetto un numero finito abbiamo:*

(a) la rappresentazione $\overline{\rho_\lambda}$ è una rappresentazione 2-dimensionale irriducibile su $\boldsymbol{F}_\lambda$;

(b) l'ordine del gruppo $\overline{\rho_\lambda}(G_{\mathbb{Q}})$ è divisibile per ℓ.

Utilizzando la caratterizzazione dell'immagine residuale dovuta al teorema precedente è possibile definire un insieme di primi per i quali l'immagine non è la massimale possibile, chiamiamo tali primi eccezionali. Inoltre, definiamo eccezionale un primo $\ell \in \mathbb{Z}$ se esiste $\lambda \in \mathcal{O}_f$ ideale primo, tale che $\lambda \mid \ell$ e λ è eccezionale. Ricordiamo il teorema di classificazione di Dickson:

Teorema di Dickson. *Sia $\boldsymbol{F}$ un campo e sia G un sottogruppo finito di $GL_2(\boldsymbol{F})$, di ordine primo rispetto alla caratteristica del campo. Sia H l'immagine di G in $PGL_2(\boldsymbol{F})$. Allora vale una delle seguenti condizioni:*

- *H è ciclico e G è contenuto in un sottogruppo di Cartan;*
- *H è diedrale, e G è contenuto nel normalizzatore di un sottogruppo di Cartan ma non nel sottogruppo di Cartan;*
- *H è isomorfo a A_4, S_4 o A_5.*

Utilizzando questo teorema, possiamo caratterizzare l'immagine della rappresentazione residuale nel caso di primi eccezionali.
Due forme modulari sono congruenti modulo λ se e solo se, considerati gli sviluppi di Fourier, i coefficienti ridotti modulo λ sono congruenti.
Per ogni possibile caratterizzazione dell'immagine di $\overline{\rho_\lambda}$ (escluso il caso di immagine A_4, S_4 o A_5) è possibile ottenere una corrispondenza con una congruenza $\mod \lambda$ di forme modulari: si ha in questo modo un criterio che permette di stabilire se un primo ℓ sia eccezionale o meno considerando solo la forma modulare assegnata e la sua congruenza modulo λ, $\lambda \in \mathcal{O}_f$ primo, $\lambda \mid \ell$, con un'altra forma modulare che si ottiene dalla forma data tramite twist o coniugazione galoisiana.
Possiamo riassumere la classificazione ottenuta, per autoforme di peso 2 rispetto $\Gamma_0(N)$, segnalando che ogni caso esclude il precedente:

Definizione. *ℓ è un primo* eccezionale di tipo $(*)$ *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ se ℓ ramifica in $\mathbb{Q}_f/\mathbb{Q}$.*

Teorema. *Sia f un'autoforma di peso $k \geq 2$ e livello N tale che il suo campo di numeri $\mathbb{Q}_f$ sia Galois chiuso. Se ℓ se è eccezionale di tipo $(*)$ allora esiste un primo λ di $\mathcal{O}_f$ con $\lambda \mid \ell$ ed un elemento non banale $\gamma \in I_\lambda \subset \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, dove $I_\lambda = \{\sigma \in G_\mathbb{Q} : \sigma(a) \equiv a \mod \lambda$ per ogni $a \in \mathcal{O}_f\}$ tale che :*

$$f^\gamma \equiv f \mod \lambda$$

Definizione. *ℓ è un primo* eccezionale di tipo (0) *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ se $\exists \lambda \in \mathcal{O}_f$ primo tale che $\lambda \mid \ell$, e $\overline{\rho_\lambda}(G_\mathbb{Q})$ è un sottogruppo riducibile di $GL_2(\boldsymbol{F}_\lambda)$ i.e. $\overline{\rho_\lambda}$ è una rappresentazione riducibile.*

Teorema. *Un primo $\ell \nmid N$ è un primo* eccezionale di tipo (0) *per la forma modulare $f = \sum a_n q^n$ se e solo se*

$$f \equiv \epsilon + \chi\, \epsilon^{-1} \mod \lambda \quad \textit{i.e.} \quad a_p = \epsilon(p) + p\, \epsilon^{-1}(p)\ \forall p \textit{ primo}$$

dove ϵ è un carattere di Dirichlet che può ramificare solo in N.

Definizione. *ℓ è un primo* eccezionale di tipo (1) *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ di livello N se $\exists \lambda \in \mathcal{O}_f$ primo tale che $\lambda \mid \ell$ e $\forall p$, $p \nmid N\,\ell$, $a_p \mod \lambda \in \boldsymbol{F} \subsetneq \boldsymbol{F}_\lambda$.*

Teorema. *Un primo $\ell \nmid N$ è un primo* eccezionale di tipo (1) *se e solo se*

$$f^\sigma \equiv f \mod \lambda$$

dove $\sigma \in \mathrm{Gal}(\boldsymbol{F}_\lambda/\boldsymbol{F})$ è il generatore del gruppo di Galois.

Definizione. *ℓ è un primo* eccezionale di tipo (2) *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ di livello N se $\exists \lambda \in \mathcal{O}_f$ primo tale che $\lambda | \ell$ e $\forall p$, $p \nmid N\,\ell$, $a_p^2 \mod \lambda \in \boldsymbol{F} \subsetneq \boldsymbol{F}_\lambda$.*

Teorema. *Un primo $\ell \nmid N$ è un primo* eccezionale di tipo (2) *se e solo se esiste un carattere di Dirichlet quadratico χ tale che*

$$f^\sigma \equiv \chi\, f \mod \lambda$$

dove σ è il generatore del gruppo di Galois dell'estensione $\boldsymbol{F}_\lambda / \boldsymbol{F}$.

Definizione. *ℓ è un primo* eccezionale di tipo (3) *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ se $\exists \lambda \in \mathcal{O}_f$ primo tale che $\lambda \mid \ell$, e $\overline{\rho_\lambda}(G_\mathbb{Q})$ è un sottogruppo diedrale di $GL_2(\boldsymbol{F}_\lambda)$.*

Teorema. *Un primo $\ell \nmid N$ è un primo* eccezionale di tipo (3) *se e solo se*

$$f \equiv \alpha\, f \mod \lambda$$

dove α è un carattere di Dirichlet quadratico che può ramificare solo nei primi il cui quadrato è un divisore del livello.

Definizione. *ℓ è un primo* eccezionale di tipo (4) *per la rappresentazione associata alla forma modulare $f = \sum a_n q^n$ se $\exists \lambda \in \mathcal{O}_f$ primo tale che $\lambda \mid \ell$, $\ell \nmid N$, e $\overline{\rho_\lambda}(G_\mathbb{Q})$ è isomorfo ad un gruppo speciale A_4, S_4 o A_5.*

La determinazione dei vari tipi di eccezionalità è nota nella letteratura a riguardo, per esempio Serre [32], ad eccezione del tipo (1) e (2) che vengono introdotti qui per la prima volta.

La classificazione data è stata implementata in SAGE, in modo da ottenere un algoritmo capace di classificare i primi eccezionali per la rappresentazione residuale una volta fissato il livello dell'autoforma. In primo luogo viene definito un insieme finito di primi, possibili primi eccezionali, basandosi sulla caratterizzazione dell'immagine dovuta al tipo di eccezionalità e sulle proprietà della rappresentazione e dei coefficienti della q-espansione della forma. Per ogni primo dell'insieme ottenuto si controlla la congruenza associata al tipo di eccezionalità e si può, quindi, certificare o meno tale eccezionalità. Il risultato fondamentale su cui si basa l'algoritmo è il Teorema di Sturm che permette di limitare il controllo della congruenza di forme modulari ad un controllo su un insieme finito di coefficienti:

Teorema di Sturm. *Sia $\mathfrak{m}$ un ideale massimale nell'anello di interi $\mathcal{O}$ di un campo di numeri $\boldsymbol{K}$ e sia f una forma modulare di peso k rispetto a $\Gamma_0(N)$ con coefficienti in $\mathcal{O}$. Se $ord_\mathfrak{m}(f) > \frac{k\,[SL_2(\mathbb{Z}):\Gamma_0(N)]}{12}$ allora $f \equiv 0 \mod \mathfrak{m}$.*

Contents

Introduction

Number theory is one of the oldest branches of mathematics and it is concerned with the properties of numbers in general. In the past few decades, research in number theory has progressed at a rapid rate on many fronts. Recently, important new results have arisen from analytic, geometric, and p-adic methods. These advances have been used to bring about breakthroughs, solve longstanding problems, and raise new inspiring questions.

One of the basic problems in mathematics is the description of the absolute Galois group G of the field $\mathbb{Q}$ of rational numbers, i.e. the group of automorphis of $\overline{\mathbb{Q}}/\mathbb{Q}$, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. This group is so large and complicated that conjecturally all finite groups can be realized as its quotients. Arguments in Galois cohomology reduce many of the fundamental questions of arithmetic geometry to the study of G.

A fruitful approach to understanding this group is through its representations; the study of 1-dimensional representations constitutes global class field theory. Some forty years ago, a vast program aimed at understanding all representations of G was advanced. More recently, some very precise conjectures about the 2-dimensional representations of G were put forward. Major success has been achieved in the past decades in proving these conjectures through the combined efforts of several mathematicians: Weil, Serre, Deligne, Eichler, Shimura, Diamond, Dieulefait, Edixhoven...

Definition. *Let A be an Hausdorff Abelian topological group. Then an A-valued* Galois representation *for $\boldsymbol{K}$ is a continuous homomorphism*

$$\rho : G_{\boldsymbol{K}} \to \mathrm{Aut}(A)$$

where we endow $G_{\boldsymbol{K}} = \mathrm{Gal}(\overline{\boldsymbol{K}}/\boldsymbol{K})$ with the Krull topology, and where $\mathrm{Aut}(A)$ is the group of continuous automorphisms of A, endowed with the compact-open topology. A is called the representation space *for ρ.*

The group $SL_2(\mathbb{R})$ acts on $\mathbb{H}$, the upper half plane, through fractional linear transformations. That is, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z \in \mathbb{H}$, then we let $\gamma z = \frac{az+b}{cz+d}$. For any natural number N, define the congruence subgroup $\Gamma_0(N)$ of level N to be the subgroup of $SL_2(\mathbb{Z})$ which elements are upper triangular matrices modulo N.

Definition. *A* holomorphic modular form *of level N and weight $k \in \mathbb{N}$ is a holomorphic function f on $\mathbb{H}$ such that:*

- *$f(\gamma z) = (cz+d)^k f(z)$ for all $\gamma \in \Gamma_0(N)$,*
- *f is holomorphic at the cusps i.e. for all $\sigma \in SL_2(\mathbb{Z})$, the function $f(\sigma z)$ has a power series expansion in $e^{\frac{2i\pi z}{M}}$ for some integer $M \geq 1$, with exponents ≥ 0.*

The aim of this short exposition is to explain results about Galois 2-dimensional representations in the particular case of residual modular representations, where modular means that the representation space is $GL_2(\mathbb{Q}_f)$, where $\mathbb{Q}_f$ is the field associated to a weight 2 modular form f, and residual means that we are interested in the representation reduced modulo λ, where λ is a prime in $\mathbb{Q}_f$. Following Dickson classification for maximal subgroup of $GL_2(\mathbf{F})$, where $\mathbf{F}$ is a finite field, we will complete the known characterization for "exceptional primes" for the representation, where exceptional means that the associated Galois representation is not "as large as possible" (following Ribet and Serre's definition).

For each possible characterization of the residual image we have information about the behavior of the coefficients of the expansion of the modular form. In this way we can use this information to state congruence relations between the modular forms considered and other modular forms, obtained from the given one by twist or Galois conjugation.
Hence we can give a correspondence between "exceptionality" conditions for residual representation at given primes and congruences between modular forms modulo a prime corresponding to the one considered in $\mathbb{Z}$.

Since we know, by Ribet results, that the set of exceptional primes is finite and since for each exceptionality type we have enough conditions on the coefficients of the modular form to have a list of possible exceptional primes, we can use the correspondence obtained to translate the problem of certifying exceptionality for a prime for the residual representation into checking a particular congruence between modular forms.
In this direction, Sturm Theorem allows us to certificate a congruence considering only a finite number of coefficients of the modular forms, hence we

can certify exceptionality of a given type for a possible exceptional prime, checking the related congruence up to the bound given by the Theorem.

We have implemented the results obtained, writing an explicit algorithm in SAGE, to give a certificate of exceptionality for primes.

In the first Chapter, we recall preliminary results from Number Theory and Algebra. After recalling basic properties about number fields and ring of integers, we list statements from finite field theory, and then describe elements of Galois Theory in order to present Galois representations. In the end we explain Dickson Classification Theorem and Čebotarev Density Theorem.

In the second Chapter we present modular form theory, in particular modular curves, modular forms, Hecke algebra and its properties. In this Chapter we state and prove results about congruences between modular forms, we explain Sturm theorem in order to present Sturm Bound, which is an important tool for the computational point of view: in fact it reduces the check of relations for infinite primes to the check for a finitie number of primes.

In the third Chapter we recall results about Galois Representations attached to Modular Forms, we give a sketch of the Deligne-Serre Theorem or the existence of such representations and explain shortly Eichler-Shimura geometric contruction for weight 2 case. We also present results of Ribet.

In the fourth Chapter we construct the correspondence between exeptional primes and congruences between modular forms. We list all the possible cases, introducing two new cases with rispect to the known literature about this subject. In particular we introduce the definition of *"inner twist* mod ℓ*"*.

In the last Chapter we explain the structure of the Algorithm implemented in SAGE, and we describe examples of the classification.

Chapter 1

Preliminary Concepts

1.1 Number Fields

Definition 1.1.1. *An extension $\boldsymbol{K}$ of $\mathbb{Q}$ of finite degree is called an* algebraic number field*, $[\boldsymbol{K} : \mathbb{Q}]$ is called the* degree *of $\boldsymbol{K}$.*

Every quadratic extension $\mathbf{K}$ of $\mathbb{Q}$ can be written as $Q(\sqrt{e})$ for a square-free integer e. Indeed, if $\{1, \alpha\}$ is a basis of $\mathbf{K}$ over $\mathbb{Q}$, then $\alpha^2 = a_1 + a_2\,\alpha$ with rational a_i, so α is a root of the polynomial $X^2 - a_2\,X - a_1$ whose roots are of the form $\frac{a_2 \pm \sqrt{d}}{2}$ where $d \in \mathbb{Q}$ is the discriminant. Write $d = \frac{f}{g}$ with integer f, g and notice that $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{d\,g^2}) = \mathbb{Q}(\sqrt{fg})$. Obviously, we can get rid of all square divisors of fg without changing the extension $\mathbb{Q}(\sqrt{fg})$.
Another example of number field is given by cyclotomic extensions of $\mathbb{Q}$: $\mathbb{Q}(\zeta_m)$ where ζ_m is a primitive m-th root of unity. If p is prime then the monic irreducible polynomial of ζ_p over $\mathbb{Q}$ is $X^{p-1}+\ldots+1 = (X^p-1)/(X-1)$ of degree $p-1$.

In a number field there is a particular subring: the ring of integers, which has a lot of relevant properties. In order to give a complete description of its structure we need to introduce the concepts of algebraic element over a number field, norm and trace.

1.1.1 Algebraic integers and algebraic elements

Definition 1.1.2. *Let us consider a ring R and $A \subseteq R$ a subring. An element $x \in R$ such that there exist $a_0, \ldots, a_{n-1} \in A$ satisfying:*

$$P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

i.e. such that x is a root of a monic polynomial $P \in A[x]$, is called an algebraic integer *over A and the relation $P(x) = 0$ is called an* integral dependence relation *for x over A.*

Theorem 1.1.3. *Let us consider a ring R, $A \subseteq R$ a subring and an element $x \in R$. The following conditions are equivalent:*

1. *x is an algebraic integer over A;*
2. *$A[x]$ is a finitely generated A-module, i.e. x is integral;*
3. *There exists a subring $B \subseteq R$ such that $A \subseteq B$, $x \in B$ and which is a finitely generated A-module.*

Proof. For a proof, look at Samuel [30]. □

Hence, each of the previous condition could be used to characterize algebraic integers.

Proposition 1.1.4. *Given a ring R, $A \subseteq R$ a subring, and $\{x_i\}_{1 \leq i \leq n}$ a finite family of element of R; if for all i the element x_i is an algebraic integer over $A[x_1, \ldots, x_{i-1}]$ then $A[x_1, \ldots, x_n]$ is finitely generated as A-module.*

Proof. For a proof, look at Samuel [30]. □

Corollary 1.1.5. *Given a ring R, $A \subseteq R$ a subring, α and β algebraic integers over A, then $\alpha + \beta$ and $\alpha\beta$ are algebraic integers over A. The set of algebraic integers over A form a subring of R.*

Proof. Suppose α, β are algebraic integers over A, and let m, n be the degrees of the minimal polynomials of α, β, respectively. Then $1, \alpha, \ldots, \alpha^{m-1}$ span $A[\alpha]$ and $1, \beta, \ldots, \beta^{n-1}$ span $A[\beta]$ as A-module.
Thus, applying Proposition 1.1.4, the elements $\alpha^i \beta^j$ for $i \leq m, j \leq n$ span $A[\alpha, \beta]$. By Theorem 1.1.3 part (3) with $B = A[\alpha, \beta]$, it follows that $\alpha + \beta$ and $\alpha\beta$ are algebraic integers. □

Definition 1.1.6. *Let $\boldsymbol{K}$ be a field. An extension field $\overline{\boldsymbol{K}}$ of $\boldsymbol{K}$ is called an* algebraic closure *of $\boldsymbol{K}$ if $\overline{\boldsymbol{K}}$ is algebraically closed and the extension $\overline{\boldsymbol{K}}/\boldsymbol{K}$ is algebraic, i.e. any $\alpha \in \overline{\boldsymbol{K}}$ is algebraic over $\boldsymbol{K}$, which means that each $\alpha \in \overline{\boldsymbol{K}}$ is a root of a polynomial $P \in \boldsymbol{K}[x]$.*

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Since all algebraic closure of a given field are isomorphic, for example, let $\overline{\mathbb{Q}}$ be the subfield of the complex numbers $\mathbb{C}$ given by all roots in $\mathbb{C}$ of all polynomials with coefficients in $\mathbb{Q}$.

For examples, the numbers $\sqrt{2}, \sqrt{3}, i, e^{\frac{2\pi i}{5}}$ are algebraic integers over $\mathbb{Q}$: in fact they satisfy, for instance, $x^2 - 2 = 0$, $x^2 - 3 = 0$, $x^2 + 1 = 0$, $x^5 - 1 = 0$ respectively.

Definition 1.1.7. *The* Minimal Polynomial *of $\alpha \in \overline{\mathbb{Q}}$ is the monic polynomial $f \in \mathbb{Q}[x]$ of least positive degree such that $f(\alpha) = 0$.*

Lemma 1.1.8. *If α is an algebraic integer then the minimal polynomial of α has coefficients in $\mathbb{Z}$.*

Proof. Suppose $f \in \mathbb{Q}[x]$ is the minimal polynomial of α and $g \in \mathbb{Z}[x]$ is a monic integral polynomial such that $g(\alpha) = 0$. Clearly $g = fh$, for some $h \in \mathbb{Q}[x]$ by definition of minimal polynomial.
If $f \notin \mathbb{Z}[x]$, then some prime p divides the denominator of some coefficient of f. Let p^i be the largest power of p that divides some denominator of some coefficient of f, and likewise let p^j be the largest power of p that divides some denominator of a coefficient of h.
Then $p^{i+j}g = (p^i\, f)(p^j\, h)$, and if we reduce both sides modulo p, then the left hand side is 0 but the right hand side is a product of two nonzero polynomials in $\mathbb{F}_p[x]$, hence nonzero, a contradiction. □

From Theorem 1.1.3 follows that:

Proposition 1.1.9. *An element $\alpha \in \overline{\mathbb{Q}}$ is an algebraic integer if and only if $\mathbb{Z}[\alpha]$ is finitely generated as a $\mathbb{Z}$-module.*

For example, the rational number $\alpha = 1/2$ is not an algebraic integer: indeed $\mathbb{Z}[1/2]$ is not finitely generated as $\mathbb{Z}$-module, since $\mathbb{Z}[1/2]$ is infinite and $\mathbb{Z}[1/2]/2\mathbb{Z}[1/2] = 0$.
Applying Corollary 1.1.5 we have that:

Proposition 1.1.10. *The set $\overline{\mathbb{Z}}$ of all algebraic integers is a ring.*

1.1.2 Norm and Trace

If $\mathbf{K}$ is a number field and $a \in \overline{\mathbb{Q}}$, let $\mathbf{K}(a)$ be the number field generated by a, which is the smallest number field that contains a and $\mathbf{K}$. Suppose $\mathbf{K} \subseteq \mathbf{L}$ is an inclusion of number fields and let $a \in \mathbf{L}$. Then left multiplication by a defines a $\mathbf{K}$-linear transformation $\ell_a : \mathbf{L} \to \mathbf{L}$ ($\mathbf{K}$-linear because $\mathbf{L}$ is commutative).

Definition 1.1.11. *The* Norm *and the* Trace *of a from $\boldsymbol{L}$ to $\boldsymbol{K}$ are*

$$\mathrm{Norm}_{\boldsymbol{L}/\boldsymbol{K}}(a) = \det(\ell_a) \quad \textit{and} \quad \mathrm{Tr}_{\boldsymbol{L}/\boldsymbol{K}}(a) = \mathrm{Tr}(\ell_a)$$

It is a standard concept from linear algebra that determinants are multiplicative and traces are additive, so for $a, b \in \mathbf{L}$ we have

$$\mathrm{Norm}_{\mathbf{L}/\mathbf{K}}(ab) = \mathrm{Norm}_{\mathbf{L}/\mathbf{K}}(a) \cdot \mathrm{Norm}_{\mathbf{L}/\mathbf{K}}(b)$$

and

$$\mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(a+b) = \mathrm{Tr}_{\mathbf{L}/\mathbf{K}}(a) + \mathrm{Tr}_{L/\mathbf{K}}(b)$$

Note that if $f \in \mathbf{K}[X]$ is the characteristic polynomial of ℓ_a, then the constant term of f is $(-1)^{\deg(f)} \det(\ell_a)$, and the coefficient of $x^{\deg(f)-1}$ is $-\mathrm{Tr}(\ell_a)$.

Definition 1.1.12. *A polynomial $f \in \boldsymbol{K}[X]$ is said to be* separable *over $\boldsymbol{K}$ if none of its irreducible factors has a multiple root in a splitting field. An algebraic extension $\boldsymbol{F}/\boldsymbol{K}$ is said to be a* separable extension *if the minimal polynomial of every element of $\boldsymbol{F}$ is separable; otherwise, it is inseparable.*

In this setting we have the following results, for a reference Knapp [14]:

Primitive Element Theorem. *Let $\boldsymbol{F}/\boldsymbol{K}$ be a finite degree separable extension. Then $\boldsymbol{F}$ is a simple extension of $\boldsymbol{K}$, i.e., $\boldsymbol{F} = \boldsymbol{K}[\gamma]$ for some $\gamma \in \boldsymbol{F}$.*

Proposition 1.1.13. *If $\boldsymbol{F}$ is a splitting field of a monic separable polynomial $f \in \boldsymbol{K}[X]$, then $\mathrm{Aut}(\boldsymbol{F}/\boldsymbol{K})$ has order $[\boldsymbol{F} : \boldsymbol{K}]$.*

Proposition 1.1.14. *Let $a \in \boldsymbol{L}$ and let $\sigma_1, \ldots, \sigma_d$, where $d = [\boldsymbol{L} : \boldsymbol{K}]$, be the distinct field embeddings $\boldsymbol{L} \hookrightarrow \overline{\mathbb{Q}}$ that fix every element of $\boldsymbol{K}$. Then*

$$\mathrm{Norm}_{\boldsymbol{L}/\boldsymbol{K}}(a) = \prod_{i=1}^{d} \sigma_i(a) \quad \text{and} \quad \mathrm{Tr}_{\boldsymbol{L}/\boldsymbol{K}}(a) = \sum_{i=1}^{d} \sigma_i(a).$$

Proof. We prove the proposition by computing the characteristic polynomial F of a. Let $f \in \mathbf{K}[x]$ be the minimal polynomial of a over $\mathbf{K}$, and note that f has distinct roots because the extension is separable. Since f is irreducible, $[\mathbf{K}(a) : \mathbf{K}] = \deg(f)$, and a satisfies a polynomial if and only if ℓ_a does, the characteristic polynomial of ℓ_a acting on $\mathbf{K}(a)$ is f. Let $b_1, \ldots, b_n$ be a basis for $\mathbf{L}$ over $\mathbf{K}(a)$ and note that $1, \ldots, a^m$ is a basis for $\mathbf{K}(a)/\mathbf{K}$, where $m = \deg(f) - 1$. Then $a^i b_j$ is a basis for $\mathbf{L}$ over $\mathbf{K}$, and left multiplication by a acts the same way on the span of $b_j, ab_j, \ldots, a^m b_j$ as on the span of $b_k, ab_k, \ldots, a^m b_k$, for any pair $j, k \leq n$. Thus the matrix of ℓ_a on $\mathbf{L}$ is a block direct sum of copies of the matrix of ℓ_a acting on $\mathbf{K}(a)$, so the characteristic polynomial of ℓ_a on $\mathbf{L}$ is $f^{[\mathbf{L}:\mathbf{K}(a)]}$. The proposition follows because the roots of $f^{[\mathbf{L}:\mathbf{K}(a)]}$ are exactly the images $\sigma_i(a)$, with multiplicity $[\mathbf{L} : \mathbf{K}(a)]$ (since each embedding of $\mathbf{K}(a)$ into $\overline{\mathbb{Q}}$ extends in exactly $[\mathbf{L} : \mathbf{K}(a)]$ ways to $\mathbf{L}$). □

Corollary 1.1.15. *Suppose $\boldsymbol{K} \subseteq \boldsymbol{L} \subseteq \boldsymbol{M}$ is a tower of number fields, and let $a \in \boldsymbol{M}$. Then*

$$\mathrm{Norm}_{\boldsymbol{M}/\boldsymbol{K}}(a) = \mathrm{Norm}_{\boldsymbol{L}/\boldsymbol{K}}(\mathrm{Norm}_{\boldsymbol{M}/\boldsymbol{L}}(a))$$

$$\mathrm{Tr}_{\boldsymbol{M}/\boldsymbol{K}}(a) = \mathrm{Tr}_{\boldsymbol{L}/\boldsymbol{K}}(\mathrm{Tr}_{\boldsymbol{M}/\boldsymbol{L}}(a))$$

Proof. For the first equation, both sides are the product of $\sigma_i(a)$, where σ_i runs through the embeddings of $\mathbf{M}$ into $\mathbf{K}$. To see this, suppose $\sigma : \mathbf{L} \to \overline{\mathbb{Q}}$ fixes $\mathbf{K}$. If σ' is an extension of σ to $\mathbf{M}$, and $\tau_1, \ldots, \tau_d$ are the embeddings of $\mathbf{M}$ into $\overline{\mathbb{Q}}$ that fix $\mathbf{L}$, then $\tau_1\sigma', \ldots, \tau_d\sigma'$ are exactly the extensions of σ to $\mathbf{M}$. For the second statement, both sides are the sum of the $\sigma_i(a)$. □

The norm and trace of an algebraic integer a are element of $\mathbb{Z}$, because the minimal polynomial of a has integer coefficients, and the characteristic polynomial of a is a power of the minimal polynomial, as we have seen.

1.1.3 The Ring of Integers

Definition 1.1.16. *The* Ring of Integers *of a number field $\boldsymbol{K}$ is the ring*

$$\mathcal{O}_{\boldsymbol{K}} = \boldsymbol{K} \cap \overline{\mathbb{Z}} = \{x \in \boldsymbol{K} \,:\, x \text{ is an algebraic integer } \}$$

The field $\mathbb{Q}$ of rational numbers is a number field of degree 1, and the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$. The field $\mathbf{K} = \mathbb{Q}(i)$ of Gaussian integers has degree 2 and $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[i]$. For quadratic extension it can be proved that:

Theorem 1.1.17. *If $\boldsymbol{K}$ is a quadratic extension of $\mathbb{Q}$ then $\boldsymbol{K} = \mathbb{Q}(\sqrt{D})$ for some squarefree integer D. Then $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[w] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot w$, with integral basis $\{1, w\}$, where*

$$w = \begin{cases} \sqrt{D} & \text{if } D \equiv 2,3 \mod 4 \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \mod 4 \end{cases}$$

The field $\mathbf{K} = \mathbb{Q}(\sqrt{5})$ has ring of integers $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[(1+\sqrt{5})/2]$, note that the "Golden ratio" $(1+\sqrt{5})/2$ satisfies $x^2 - x - 1$. According to the previous definition, it is possible to show that the ring of integers of $\mathbf{K} = \mathbb{Q}(\sqrt[3]{9})$ is $\mathbb{Z}[\sqrt[3]{3}]$, where $\sqrt[3]{3} = \frac{1}{3}(\sqrt[3]{9})^2$.

Definition 1.1.18. *An* order *in $\mathcal{O}_{\boldsymbol{K}}$ is any subring R of $\mathcal{O}_{\boldsymbol{K}}$ such that the quotient $\mathcal{O}_{\boldsymbol{K}}/R$ as abelian groups is finite.*

Note that R must contain 1 because it is a ring, and we are assuming that every ring has a 1. As noted above, $\mathbb{Z}[i]$ is the ring of integers of $\mathbb{Q}(i)$. For every nonzero integer n, the subring $\mathbb{Z} + ni\mathbb{Z}$ of $\mathbb{Z}[i]$ is an order. The subring $\mathbb{Z}$ of $\mathbb{Z}[i]$ is not an order, because $\mathbb{Z}$ does not have finite index in $\mathbb{Z}[i]$. Also the subgroup $2\mathbb{Z} + i\mathbb{Z}$ of $\mathbb{Z}[i]$ is not an order because it is not a ring. If $\mathbf{K} = \mathbb{Q}(\alpha)$ and α is an algebraic integer, then $\mathbb{Z}[\alpha]$ is an order in $\mathcal{O}_{\mathbf{K}}$, but frequently $\mathbb{Z}[\alpha] \neq \mathcal{O}_{\mathbf{K}}$.

Lemma 1.1.19. *Let $\mathcal{O}_{\boldsymbol{K}}$ be the ring of integers of a number field. Then $\mathcal{O}_{\boldsymbol{K}} \cap \mathbb{Q} = \mathbb{Z}$ and $\mathbb{Q}\mathcal{O}_{\boldsymbol{K}} = \boldsymbol{K}$.*

Proof. Suppose $\alpha \in \mathcal{O}_{\mathbf{K}} \cap \mathbb{Q}$ with $\alpha = a/b$ in lowest terms and $b > 0$. The minimal polynomial of α is $x - \frac{a}{b} \in \mathbb{Q}[x]$, so if $b \neq 1$ then Lemma 1.1.8 implies that α is not an algebraic integer, a contradiction. To prove that $\mathbb{Q}\mathcal{O}_{\mathbf{K}} = \mathbf{K}$, suppose $\alpha \in \mathbf{K}$, and let $f(x) \in \mathbb{Q}[x]$ be the minimal monic polynomial of α. For any positive integer d, the minimal monic polynomial of $d\alpha$ is $d^{\deg(f)} f(x/d)$, i.e., the polynomial obtained from $f(x)$ by multiplying the coefficient of $x^{\deg(f)}$ by 1, multiplying the coefficient of $x^{\deg(f)-1}$ by d,

multiplying the coefficient of $x^{\deg(f)-2}$ by d^2, etc.
If d is the least common multiple of the denominators of the coefficients of f, then the minimal monic polynomial of $d\alpha$ has integer coefficients, so $d\alpha$ is integral and $d\alpha \in \mathcal{O}_{\mathbf{K}}$. This proves that $\mathbb{Q}\mathcal{O}_{\mathbf{K}} = \mathbf{K}$. □

Proposition 1.1.20. *Let $\boldsymbol{K}$ be a number field. The ring of integers $\mathcal{O}_{\boldsymbol{K}}$ is a lattice in $\boldsymbol{K}$, i.e., $\mathbb{Q}\mathcal{O}_{\boldsymbol{K}} = \boldsymbol{K}$ and $\mathcal{O}_{\boldsymbol{K}}$ is a free abelian group of rank $[\boldsymbol{K} : \mathbb{Q}]$.*

Proof. We have seen that $\mathbb{Q}\mathcal{O}_{\mathbf{K}} = \mathbf{K}$ so there exists a basis $a_1, \ldots, a_n$ for $\mathbf{K}$, where each a_i is in $\mathcal{O}_{\mathbf{K}}$. Suppose that as $x = \sum c_i a_i \in \mathcal{O}_{\mathbf{K}}$ varies over all elements of $\mathcal{O}_{\mathbf{K}}$ the denominators of the coefficients c_i are arbitrarily large. Then subtracting off integer multiples of the a_i, we see that as $x = \sum c_i a_i \in \mathcal{O}_{\mathbf{K}}$ varies over elements of $\mathcal{O}_{\mathbf{K}}$ with c_i between 0 and 1, the denominators of the c_i are also arbitrarily large. This implies that there are infinitely many elements of $\mathcal{O}_{\mathbf{K}}$ in the bounded subset

$$S = \{c_1 a_1 + \cdots + c_n a_n : c_i \in \mathbb{Q},\ \ 0 \leq c_i \leq 1\} \subseteq \mathbf{K}$$

Thus for any $\varepsilon > 0$, there are elements $a, b \in \mathcal{O}_{\mathbf{K}}$ such that the coefficients of $a - b$ are all less than ε (otherwise the elements of $\mathcal{O}_{\mathbf{K}}$ would all be a "distance" of least ε from each other, so only finitely many of them would fit in S).

As mentioned above, the norms of elements of $\mathcal{O}_{\mathbf{K}}$ are integers. Since the norm of an element is the determinant of left multiplication by that element, the norm is a homogenous polynomial of degree n in the indeterminate coefficients c_i. If the c_i get arbitrarily small for elements of $\mathcal{O}_{\mathbf{K}}$, then the values of the norm polynomial get arbitrarily small, which would imply that there are elements of $\mathcal{O}_{\mathbf{K}}$ with positive norm too small to be in $\mathbb{Z}$, a contradiction. So the set S contains only finitely many elements of $\mathcal{O}_{\mathbf{K}}$.
Thus the denominators of the c_i are bounded, so for some d, we have that $\mathcal{O}_{\mathbf{K}}$ has finite index in $A = \frac{1}{d}\mathbb{Z}a_1 + \cdots + \frac{1}{d}\mathbb{Z}a_n$.
Since A is isomorphic to $\mathbb{Z}^n$, it follows from the structure theorem for finitely generated abelian groups that $\mathcal{O}_{\mathbf{K}}$ is isomorphic as a $\mathbb{Z}$-module to $\mathbb{Z}^n$, as claimed. □

Corollary 1.1.21. *The ring of integers $\mathcal{O}_{\boldsymbol{K}}$ of a number field is Noetherian.*

Proof. The ring $\mathcal{O}_{\mathbf{K}}$ is a finitely generated $\mathbb{Z}$-module, so it is certainly finitely generated as a ring over $\mathbb{Z}$. By the Hilbert Basis Theorem, $\mathcal{O}_{\mathbf{K}}$ is Noetherian. □

If R is an integral domain, the fraction field or quotient field of R is the field of all elements a/b, where $a, b \in R$. The field of fractions of R is the smallest field that contains R. For example, the field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$ and of $\mathbb{Z}[(1+\sqrt{5})/2]$ is $\mathbb{Q}(\sqrt{5})$.

Definition 1.1.22. *An* Integrally Closed *domain R is an integral domain where if α is in the field of fractions of R and α satisfies a monic polynomial $f \in R[x]$, then $\alpha \in R$.*

Proposition 1.1.23. *If $\boldsymbol{K}$ is any number field, then $\mathcal{O}_{\boldsymbol{K}}$ is integrally closed. Also, the ring $\overline{\mathbb{Z}}$ of all algebraic integers is integrally closed.*

Proof. We first prove that $\overline{\mathbb{Z}}$ is integrally closed. Suppose $c \in \overline{\mathbb{Q}}$ is integral over $\overline{\mathbb{Z}}$, so there is a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $a_i \in \overline{\mathbb{Z}}$ and $f(c) = 0$. The a_i all lie in the ring of integers $\mathcal{O}_{\mathbf{K}}$ of the number field $\mathbf{K} = \mathbb{Q}(a_0, a_1, \ldots a_{n-1})$, and $\mathcal{O}_{\mathbf{K}}$ is finitely generated as a $\mathbb{Z}$-module, so $\mathbb{Z}[a_0, \ldots, a_{n-1}]$ is finitely generated as a $\mathbb{Z}$-module. Since $f(c) = 0$, we can write c^n as a $\mathbb{Z}[a_0, \ldots, a_{n-1}]$-linear combination of c^i for $i < n$, so the ring $\mathbb{Z}[a_0, \ldots, a_{n-1}, c]$ is also finitely generated as a $\mathbb{Z}$-module. Thus $\mathbb{Z}[c]$ is finitely generated as $\mathbb{Z}$-module because it is a submodule of a finitely generated $\mathbb{Z}$-module, which implies that c is integral over $\mathbb{Z}$.

Suppose $c \in \mathbf{K}$ is integral over $\mathcal{O}_{\mathbf{K}}$. Then since $\overline{\mathbb{Z}}$ is integrally closed, c is an element of $\overline{\mathbb{Z}}$, so $c \in \mathbf{K} \cap \overline{\mathbb{Z}} = \mathcal{O}_{\mathbf{K}}$, as required. □

Definition 1.1.24. *An integral domain R is a* Dedekind Domain *if it is Noetherian, integrally closed, and every nonzero prime ideal of R is maximal.*

The ring $\mathbb{Z}[\sqrt{5}]$ is not a Dedekind domain because it is not integrally closed in its field of fractions, as $(1 + \sqrt{5})/2$ is integral over $\mathbb{Z}$ and lies in $\mathbb{Q}(\sqrt{5})$, but not in $\mathbb{Z}[\sqrt{5}]$. The ring $\mathbb{Z}$ is a Dedekind domain, as is any ring of integers $\mathcal{O}_{\mathbf{K}}$ of a number field, as we will see below. Also, every field K is a Dedekind domain, since it is a domain, it is trivially integrally closed in itself, and there are no nonzero prime ideals.

Proposition 1.1.25. *The ring of integers $\mathcal{O}_{\boldsymbol{K}}$ of a number field is a Dedekind domain.*

Proof. The ring $\mathcal{O}_{\mathbf{K}}$ is integrally closed, and it is Noetherian (both facts have been proved before). Suppose that $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_{\mathbf{K}}$. Let $\alpha \in \mathfrak{p}$ be a nonzero element, and let $f(x) \in \mathbb{Z}[x]$ be the minimal polynomial of α. Then

$$f(\alpha) = \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0,$$

so $a_0 = -(\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha) \in \mathfrak{p}$. Since f is irreducible, a_0 is a nonzero element of $\mathbb{Z}$ that lies in $\mathfrak{p}$. Every element of the finitely generated abelian group $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ is killed by a_0, so $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ is a finite set. Since $\mathfrak{p}$ is prime, $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ is an integral domain. Every finite integral domain is a field, so $\mathfrak{p}$ is maximal, which completes the proof. □

Definition 1.1.26. *A* Fractional Ideal *is an $\mathcal{O}_{\boldsymbol{K}}$-submodule, $I \subseteq K$, that is finitely generated as an $\mathcal{O}_{\boldsymbol{K}}$-module.*

Since fractional ideals are finitely generated, we can clear denominators of a generating set to see that every fractional ideal is of the form

$$a\,I = \{ab : b \in I\}$$

for some $a \in \mathbf{K}$ and ideal $I \subseteq \mathcal{O}_{\mathbf{K}}$. For example, the set $\frac{1}{2}\mathbb{Z}$ of rational numbers with denominator 1 or 2 is a fractional ideal of $\mathbb{Z}$.

Theorem 1.1.27. *The set of nonzero fractional ideals of a Dedekind domain R is an abelian group under ideal multiplication.*

Before proving this theorem we prove a lemma. For the rest of this section $\mathcal{O}_{\mathbf{K}}$ is the ring of integers of a number field $\mathbf{K}$.

Lemma 1.1.28. *Suppose I is an ideal of $\mathcal{O}_{\boldsymbol{K}}$. Then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_n \subseteq I$. In other words, I divides a product of prime ideals. By convention the empty product is the unit ideal. Also, if $I = 0$, then we take $\mathfrak{p}_1 = (0)$, which is a prime ideal.*

Proof. The key idea is to use that $\mathcal{O}_{\mathbf{K}}$ is Noetherian to deduce that the set S of ideals that do not satisfy the lemma is empty. If S is nonempty, then because $\mathcal{O}_{\mathbf{K}}$ is Noetherian, there is an ideal $I \in S$ that is maximal as an element of S. If I were prime, then I would trivially contain a product of primes, so I is not prime. By definition of prime ideal, there exists $a, b \in \mathcal{O}_{\mathbf{K}}$ such that $ab \in I$ but $a \notin I$ or $b \notin I$. Let $J_1 = I + (a)$ and $J_2 = I + (b)$. Then neither J_1 nor J_2 is in S, since I is maximal, so both J_1 and J_2 contain a product of prime ideals. Thus so does I, since

$$J_1 J_2 = I^2 + I(b) + (a)I + (ab) \subseteq I$$

which is a contradiction. Thus S is empty, which completes the proof. □

Now we can give a proof of the theorem.

Proof of Theorem 1.1.27. The product of two fractional ideals is again finitely generated, so it is a fractional ideal, and $I\mathcal{O}_{\mathbf{K}} = \mathcal{O}_{\mathbf{K}}$ for any nonzero ideal I, so to prove that the set of fractional ideals under multiplication is a group it suffices to show the existence of inverses.
We will first prove that if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ has an inverse, then we will prove that nonzero integral ideals have inverses, and finally observe that every fractional ideal has an inverse. Suppose $\mathfrak{p}$ is a nonzero prime ideal of $\mathcal{O}_{\mathbf{K}}$. We will show that the $\mathcal{O}_{\mathbf{K}}$-module

$$I = \{a \in \mathbf{K} \,:\, a\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{K}}\}$$

is a fractional ideal of $\mathcal{O}_{\mathbf{K}}$ such that $I\mathfrak{p} = \mathcal{O}_{\mathbf{K}}$, so that I is an inverse of $\mathfrak{p}$.

For the rest of the proof, fix a nonzero element $b \in \mathfrak{p}$. Since I is an $\mathcal{O}_{\mathbf{K}}$-module, $bI \subseteq \mathcal{O}_{\mathbf{K}}$ is an $\mathcal{O}_{\mathbf{K}}$ ideal, hence I is a fractional ideal. Since

$\mathcal{O}_{\mathbf{K}} \subseteq I$ we have $\mathfrak{p} \subseteq I\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{K}}$, hence either $\mathfrak{p} = I\mathfrak{p}$ or $I\mathfrak{p} = \mathcal{O}_{\mathbf{K}}$. If $I\mathfrak{p} = \mathcal{O}_{\mathbf{K}}$, we are done since then I is an inverse of $\mathfrak{p}$. Thus suppose that $I\mathfrak{p} = \mathfrak{p}$. Our strategy is to show that there is some $d \in I$ not in $\mathcal{O}_{\mathbf{K}}$; such a d would leave $\mathfrak{p}$ invariant (i.e., $d\mathfrak{p} \subseteq \mathfrak{p}$), so since $\mathfrak{p}$ is an $\mathcal{O}_{\mathbf{K}}$-module it will follow that $d \in \mathcal{O}_{\mathbf{K}}$, a contradiction.

By the previous lemma, we can choose a product $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$, with m minimal, such that

$$\mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_m \subseteq (b) \subseteq \mathfrak{p}$$

If no $\mathfrak{p}_i$ is contained in $\mathfrak{p}$, then we can choose for each i an $a_i \in \mathfrak{p}_i$ with $a_i \notin \mathfrak{p}$; but then $\prod a_i \in \mathfrak{p}$, which contradicts that $\mathfrak{p}$ is a prime ideal. Thus some $\mathfrak{p}_i$, say $\mathfrak{p}_1$, is contained in $\mathfrak{p}$, which implies that $\mathfrak{p}_1 = \mathfrak{p}$ since every nonzero prime ideal is maximal. Because m is minimal, $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ is not a subset of (b), so there exists $c \in \mathfrak{p}_2 \cdots \mathfrak{p}_m$ that does not lie in (b). Then $\mathfrak{p}(c) \subseteq (b)$, so by definition of I we have $d = c/b \in I$. However, $d \notin \mathcal{O}_{\mathbf{K}}$, since if it were then c would be in (b). We have thus found our element $d \in I$ that does not lie in $\mathcal{O}_{\mathbf{K}}$. To finish the proof that $\mathfrak{p}$ has an inverse, we observe that d preserves the $\mathcal{O}_{\mathbf{K}}$-module $\mathfrak{p}$, and is hence in $\mathcal{O}_{\mathbf{K}}$, a contradiction. More precisely, if $b_1, \ldots, b_n$ is a basis for $\mathfrak{p}$ as a $\mathbb{Z}$-module, then the action of d on $\mathfrak{p}$ is given by a matrix with entries in $\mathbb{Z}$, so the minimal polynomial of d has coefficients in $\mathbb{Z}$. This implies that d is integral over $\mathbb{Z}$, so $d \in \mathcal{O}_{\mathbf{K}}$, since $\mathcal{O}_{\mathbf{K}}$ is integrally closed. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{\mathbf{K}}$, then $\mathfrak{p}^{-1} = \{a \in \mathbf{K} : a\mathfrak{p} \subseteq \mathcal{O}_{\mathbf{K}}\}$ is the inverse of $\mathfrak{p}$ in the monoid of nonzero fractional ideals of $\mathcal{O}_{\mathbf{K}}$; and every nonzero fractional ideal is of the form aI for $a \in \mathbf{K}$ and I an integral ideal, so since (a) has inverse $(1/a)$, it suffices to show that every integral ideal I has an inverse. If not, then there is a nonzero integral ideal I that is maximal among all nonzero integral ideals that do not have an inverse. Every ideal is contained in a maximal ideal, so there is a nonzero prime ideal $\mathfrak{p}$ such that $I \subseteq \mathfrak{p}$. Multiplying both sides of this inclusion by $\mathfrak{p}^{-1}$ and using that $\mathcal{O}_{\mathbf{K}} \subseteq \mathfrak{p}^{-1}$, we see that $I \subseteq \mathfrak{p}^{-1}I \subseteq \mathcal{O}_{\mathbf{K}}$. If $I = \mathfrak{p}^{-1}I$, then arguing as in the proof that $\mathfrak{p}^{-1}$ is the inverse of $\mathfrak{p}$, we see that each element of $\mathfrak{p}^{-1}$ preserves the finitely generated $\mathbb{Z}$-module I and is hence integral. But then $\mathfrak{p}^{-1} \subseteq \mathcal{O}_{\mathbf{K}}$, which implies that $\mathcal{O}_{\mathbf{K}} = \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathfrak{p}$, a contradiction. Thus $I \neq \mathfrak{p}^{-1}I$. Because I is maximal among ideals that do not have an inverse, the ideal $\mathfrak{p}^{-1}I$ does have an inverse, call it J. Then $\mathfrak{p}J$ is the inverse of I. □

Theorem 1.1.29. *Suppose I is an integral ideal of $\mathcal{O}_{\boldsymbol{K}}$, non trivial, then I can be written as a product*

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$$

of prime ideals of $\mathcal{O}_{\boldsymbol{K}}$, and this representation is unique up to order. If $I = 0$, then the representation is not unique.

Proof. Suppose I is an ideal that is maximal among the set of all ideals in $\mathcal{O}_{\mathbf{K}}$ that can not be written as a product of primes. Every ideal is contained in a maximal ideal, so I is contained in a nonzero prime ideal $\mathfrak{p}$. If $I\mathfrak{p}^{-1} = I$, then by the previous theorem we can cancel I from both sides of this equation to see that $\mathfrak{p}^{-1} = \mathcal{O}_{\mathbf{K}}$, a contradiction. Thus I is strictly contained in $I\mathfrak{p}^{-1}$, so by our maximality assumption on I there are maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $I\mathfrak{p}^{-1} = \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Then $I = \mathfrak{p} \cdot \mathfrak{p}_1 \cdots \mathfrak{p}_n$, a contradiction. Thus every ideal can be written as a product of primes.

Suppose $\mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m$. If no $\mathfrak{q}_i$ is contained in $\mathfrak{p}_1$, then for each i there is an $a_i \in \mathfrak{q}_i$ such that $a_i \notin \mathfrak{p}_1$. But the product of the a_i is in the $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, which is a subset of $\mathfrak{p}_1$, which contradicts the fact that $\mathfrak{p}_1$ is a prime ideal. Thus $\mathfrak{q}_i = \mathfrak{p}_1$ for some i. We can thus cancel $\mathfrak{q}_i$ and $\mathfrak{p}_1$ from both sides of the equation. Repeating this argument finishes the proof of uniqueness. □

Corollary 1.1.30. *If I is a fractional ideal of $\mathcal{O}_{\boldsymbol{K}}$ then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$, unique up to order, such that*

$$I = (\mathfrak{p}_1 \cdots \mathfrak{p}_n)(\mathfrak{q}_1 \cdots \mathfrak{q}_m)^{-1}$$

Proof. We have $I = (a/b)J$ for some $a, b \in \mathcal{O}_{\mathbf{K}}$ and integral ideal J. Applying Theorem 1.1.29 to (a), (b), and J gives an expression as claimed. For uniqueness, if one has two such product expressions, multiply through by the denominators and use the uniqueness part of Theorem 1.1.29. □

Let us give an example: the ring of integers of $\mathbf{K} = \mathbb{Q}(\sqrt{-6})$ is $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\sqrt{-6}]$. In $\mathcal{O}_{\mathbf{K}}$, we have

$$6 = -\sqrt{-6}\sqrt{-6} = 2 \cdot 3$$

so it is not UFD. If $ab = \sqrt{-6}$, with $a, b \in \mathcal{O}_{\mathbf{K}}$ and neither a unit, then $\mathrm{Norm}(a)\,\mathrm{Norm}(b) = 6$, so without loss $\mathrm{Norm}(a) = 2$ and $\mathrm{Norm}(b) = 3$. If $a = c + d\sqrt{-6}$, then $\mathrm{Norm}(a) = c^2 + 6d^2$; since the equation $c^2 + 6d^2 = 2$ has no solution with $c, d \in \mathbb{Z}$, there is no element in $\mathcal{O}_{\mathbf{K}}$ with norm 2, so $\sqrt{-6}$ is irreducible. Also, $\sqrt{-6}$ is not a unit times 2 or times 3, since again the norms would not match up. Thus 6 can not be written uniquely as a product of irreducibles in $\mathcal{O}_{\mathbf{K}}$. Theorem 1.1.29, however, implies that the principal ideal (6) can, however, be written uniquely as a product of prime ideals, in this case we have:

$$(6) = (2, \sqrt{-6})^2 \cdot (3, \sqrt{-6})^2,$$

where each of the ideals $(2, \sqrt{-6})$ and $(3, \sqrt{-6})$ is prime.

1.1.4 Discriminant of a number field

The discriminant of an algebraic number field is a numerical invariant that, loosely speaking, measures the size of the ring of integers of the algebraic number field. More specifically, it is related to the volume of the fundamental domain of the ring of integers, and it regulates which primes are ramified.

Definition 1.1.31. *Let $\boldsymbol{K}$ be an algebraic number field, and let $\mathcal{O}_{\boldsymbol{K}}$ be its ring of integers. Let $b_1, \ldots, b_n$ be an integral basis of $\mathcal{O}_{\boldsymbol{K}}$ id est a basis as a $\mathbb{Z}$-module, and let $\{\sigma_1, \ldots, \sigma_n\}$ be the set of embeddings of $\boldsymbol{K}$ into the complex numbers (i.e. ring homomorphisms $\boldsymbol{K} \to \mathbb{C}$). The* discriminant *of $\boldsymbol{K}$ is the square of the determinant of the n by n matrix B whose (i,j)-entry is $\sigma_i(b_j)$. Symbolically,*

$$\Delta_{\boldsymbol{K}} = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \cdots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \cdots & \cdots & \sigma_n(b_n) \end{pmatrix}^2$$

Equivalently, the trace from $\mathbf{K}$ to $\mathbb{Q}$ can be used: defining the trace form to be the matrix whose (i,j)-entry is $\mathrm{Tr}_{\mathbf{K}/\mathbb{Q}}(b_i b_j)$, we may identify this as $B^T B$. Then the discriminant of $\mathbf{K}$ is the determinant of this matrix:

$$\Delta_{\mathbf{K}} = \det(\mathrm{Tr}_{\mathbf{K}/\mathbb{Q}}(b_i b_j))$$

it is also denoted as $\mathrm{disc}_{\mathbb{Q}}(\mathbf{K})$.
In a quadratic number fields, let d be a square-free integer, then it can be showed that the discriminant of $\mathbf{K} = \mathbb{Q}(\sqrt{d})$ is

$$\Delta_{\mathbf{K}} = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2, 3 \bmod 4 \end{cases}$$

Ramification and Discriminant

A prime number p is said to be ramified in a number field $\mathbf{K}$ if the prime ideal factorisation

$$(p) = p\,\mathcal{O}_{\mathbf{K}} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$$

has some e_i greater than 1. If every e_i equals 1, we say p is unramified in $\mathbf{K}$. For example in $\mathbb{Z}[i]$, the only prime which ramifies is 2: $(2) = (1+i)^2$.

Ramified primes can be well thought in terms of the ring structure of $\mathcal{O}_{\mathbf{K}}/(p)$: by the Chinese Remainder Theorem it follows that

$$\mathcal{O}_{\mathbf{K}}/(p) \cong \mathcal{O}_{\mathbf{K}}/(\mathfrak{p}_1^{e_1}) \times \cdots \mathcal{O}_{\mathbf{K}}/(\mathfrak{p}_g^{e_g}) \tag{1.1}$$

If some e_i is greater than 1, then the quotient ring $\mathcal{O}_{\mathbf{K}}/(\mathfrak{p}_i^{e_i})$ has a nonzero nilpotent element, so the product ring has a nonzero nilpotent element. If each e_i equals 1, then $\mathcal{O}_{\mathbf{K}}/(p)$ is a product of finite fields, and a product of fields has no nonzero nilpotent elements. Thus, p ramifies in $\mathbf{K}$ if and only if $\mathcal{O}_{\mathbf{K}}/(p)$ has a nonzero nilpotent element.

It is possible define the ramification primes in terms of the discriminant of the ring of integers of the number field considered, but before to state the result some preliminaries are needed.

Definition 1.1.32. *Let A be a commutative ring and B be a ring extension of A which is a finite free A-module:*

$$B = A\,e_1 \oplus \cdots \oplus A\,e_n$$

Then we define the discriminant of B with respect to A as:

$$\mathrm{disc}_A(B) = \mathrm{disc}_A(e_1, \ldots, e_n) = \det(\mathrm{Tr}_{B/A}(e_i\,e_j)) \in A$$

Given a number field $\mathbf{K}$, ramification of the prime p in $\mathbf{K}$ is linked to the structure of the ring $\mathcal{O}_{\mathbf{K}}/(p)$, so we can consider its discriminant over $\mathbb{Z}/p\mathbb{Z}$. Letting $\mathbf{K}$ have degree n over $\mathbb{Q}$, the ring $\mathcal{O}_{\mathbf{K}}$ is a free rank-n $\mathbb{Z}$-module, say

$$\mathcal{O}_{\mathbf{K}} = \bigoplus_{i=1}^{n} \mathbb{Z}\,\omega_i$$

Reducing both sides modulo p,

$$\mathcal{O}_{\mathbf{K}}/(p) = \bigoplus_{i=1}^{n} (\mathbb{Z}/p\mathbb{Z})\bar{\omega}_i$$

so $\mathcal{O}_{\mathbf{K}}/(p)$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$ of dimension n. The discriminant of $\mathcal{O}_{\mathbf{K}}$ is $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}})$. The next lemma says that reduction modulo p is compatible with discriminant construction.

Lemma 1.1.33. *Choosing bases for $\mathcal{O}_{\boldsymbol{K}}$ and $\mathcal{O}_{\boldsymbol{K}}/(p)$,*

$$\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\boldsymbol{K}}) \mod p = \mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\boldsymbol{K}}/(p)).$$

Proof. Pick a $\mathbb{Z}$-basis $\omega_1, \ldots, \omega_n$ of $\mathcal{O}_{\mathbf{K}}$. The reductions $\overline{\omega}_1, \ldots, \overline{\omega}_n$ in $\mathcal{O}_{\mathbf{K}}/(p)$ are a $\mathbb{Z}/p\mathbb{Z}$-basis, so the representative matrix m_x of any $x \in \mathcal{O}_{\mathbf{K}}$, with respect to the basis $\{\omega_i\}$, reduces modulo p to the matrix $m_{\overline{x}}$ for $\overline{x}$ on $\mathcal{O}_{\mathbf{K}}/(p)$ with respect to the basis $\{\overline{\omega}_i\}$. Therefore

$$\mathrm{Tr}_{(\mathcal{O}_{\mathbf{K}}/(p))/(\mathbb{Z}/p\mathbb{Z})}(\overline{x}) = \mathrm{Tr}(m_{\overline{x}}) = \mathrm{Tr}(m_x) \mod p = \mathrm{Tr}_{\mathcal{O}_{\mathbf{K}}/\mathbb{Z}}(x) \mod p$$

Thus, the mod p reduction of the matrix $(\mathrm{Tr}_{\mathcal{O}_\mathbf{K}/\mathbb{Z}}(\omega_i\,\omega_j))$ is:

$$(\mathrm{Tr}_{(\mathcal{O}_\mathbf{K}/(p))/(\mathbb{Z}/p\mathbb{Z})}(\overline{\omega}_i\,\overline{\omega}_j)).$$

Now taking determinants we complete the proof. □

Lemma 1.1.34. *Let A be a commutative ring and B_1 and B_2 be commutative ring extensions of A which are each finite free A-modules. Then, choosing A-module bases,*

$$\mathrm{disc}_A(B_1 \times B_2) = \mathrm{disc}_A(B_1) \cdot \mathrm{disc}_A(B_2)$$

Proof. Pick A-module bases for B_1 and B_2:

$$B_1 = \bigoplus_{i=1}^{m} Ae_i \qquad B_2 = \bigoplus_{j=1}^{n} Af_j$$

As an A-module basis for $B_1 \times B_2$ we will use $e_1, \ldots, e_m, f_1, \ldots, f_n$. Since $e_i\,f_j = 0$ in $B_1 \times B_2$, the matrix whose determinant is $\mathrm{disc}_A(B_1 \times B_2)$ is a block diagonal matrix

$$\begin{pmatrix} (\mathrm{Tr}_{(B_1\times B_2)/A}(e_i\,e_k)) & 0 \\ 0 & (\mathrm{Tr}_{(B_1\times B_2)/A}(f_j\,f_l)) \end{pmatrix}$$

In particular for any $x \in B_i$:

$$\mathrm{Tr}_{(B_1\times B_2)/A}(x) = \mathrm{Tr}_{B_i/A}(x) \quad x \in B_i \;\; i = 1, 2$$

Thus

$$\begin{pmatrix} (\mathrm{Tr}_{(B_1\times B_2)/A}(e_i\,e_k)) & 0 \\ 0 & (\mathrm{Tr}_{(B_1\times B_2)/A}(f_j\,f_l)) \end{pmatrix}$$

is equal to

$$\begin{pmatrix} (\mathrm{Tr}_{B_1/A}(e_i\,e_k)) & 0 \\ 0 & (\mathrm{Tr}_{B_2/A}(f_j\,f_l)) \end{pmatrix}$$

and taking determinants gives

$$\mathrm{disc}_A(B_1 \times B_2) = \mathrm{disc}_A(B_1) \cdot \mathrm{disc}_A(B_2).$$

□

The discriminants is compatible with base change: indeed pick a second basis $e'_1, \ldots, e'_n$ of B as an A-module. Then $e'_i = \sum_{j=1}^n a_{ij}e_j$ where $a_{ij} \in A$ and the change of basis matrix (a_{ij}) has determinant in A. Then

$$\mathrm{Tr}_{B/A}(e'_i\,e'_j) = \mathrm{Tr}_{B/A}(\sum_{k=1}^{n} a_{ik}e_k \sum_{l=1}^{n} a_{jl}e_l) = \sum_{k=1}^{n}\sum_{l=1}^{n} a_{ik}\,\mathrm{Tr}_{B/A}(e_k\,e_l)a_{jl}$$

Therefore

$$\mathrm{disc}_A(e'_1,\ldots,e'_n) = (\det(a_{ij}))^2\,\mathrm{disc}_A(e_1,\ldots,e_n)$$

So discriminant is well-defined up to a unit squared. In particular, the condition $\mathrm{disc}_A(B) = 0$ is independent of the choice of basis.

Now we have all elements to state the theorem:

Theorem 1.1.35. *For a number field $\boldsymbol{K}$, the primes which ramify are those dividing the integer* $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\boldsymbol{K}})$.

Proof. Since $\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}) \neq 0$, by the fact that it always exists an integral basis of $\mathcal{O}_{\mathbf{K}}$ over $\mathbb{Z}$ (for a reference Milne [20]), only finitely many primes ramify in $\mathbf{K}$.
Let us observe that

$$p \mid \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}) \Leftrightarrow \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}) \equiv 0 \mod p$$

By Lemma 1.1.33

$$\mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}) \mod p = \mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/(p))$$

so $p \mid \mathrm{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}})$ if and only if $\mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/(p)) = \bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$. In (1.1), each factor $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}_i^{e_i}$ is a $\mathbb{Z}/p\mathbb{Z}$-vector space since $p \in \mathfrak{p}_i^{e_i}$. Using (1.1) and Lemma 1.1.34,

$$\mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/(p)) = \prod_{i=1}^{g} \mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}_i^{e_i})$$

Therefore we need to show for any prime number p and prime-power ideal $\mathfrak{p}^e$, such that $\mathfrak{p}^e \mid (p)$, that $\mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e)$ is $\bar{0}$ in $\mathbb{Z}/p\mathbb{Z}$ if and only if $e > 1$. Firstly let recall that the vanishing of a discriminant is independent of the choice of basis.
Suppose $e > 1$. Then any $x \in \mathfrak{p} - \mathfrak{p}^e$ is a nonzero nilpotent element in $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e$. By linear algebra over fields, such an x can be used as part of a $\mathbb{Z}/p\mathbb{Z}$-basis of $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e$, say $\{x_1,\ldots,x_n\}$ with $x = x_1$. The first column of the matrix

$$(\mathrm{Tr}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e)/(\mathbb{Z}/p\mathbb{Z})(x_i\,x_j))_{ij}$$

contains the numbers $\mathrm{Tr}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e)/(\mathbb{Z}/p\mathbb{Z})(x_i\,x)$. These traces are all 0: $x_i\,x$ is nilpotent, so the linear transformation $m_{x_i\,x}$ on $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e$ is nilpotent and thus its eigenvalues all equal zero. Since one column of the trace-pairing matrix is all 0, $\mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e) = 0$.
Now suppose $e = 1$. Then $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}^e = \mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ is a finite field of characteristic p. We want to prove $\mathrm{disc}_{\mathbb{Z}/p\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}/\mathfrak{p}) \neq \bar{0}$. If this discriminant is $\bar{0}$, then the trace function $\mathrm{Tr} : \mathcal{O}_{\mathbf{K}}/\mathfrak{p} \to \mathbb{Z}/p\mathbb{Z}$ is identically zero because of the

definition of discriminant and the fact that $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ is a finite field of characteristic p. However, the trace function can be written as a polynomial function:

$$\mathrm{Tr}(t) = t + t^p + t^{p^2} + \cdots + t^{p^{r-1}}$$

since it is defined as sum of the Galois conjugates of $t \in \mathcal{O}_{\mathbf{K}}/\mathfrak{p}$ and $|\mathcal{O}_{\mathbf{K}}/\mathfrak{p}| = p^r$, so it takes the given form (later in this Chapter we will provide elements to understand this statement). Since the degree of this polynomial is less than the size of $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$, this function is not identically zero on $\mathcal{O}_{\mathbf{K}}/\mathfrak{p}$. Therefore the discriminant of a finite extension of $\mathbb{Z}/p\mathbb{Z}$ does not equal zero. □

1.2 Finite Fields

Definition 1.2.1. *A* finite field *is a field that has finitely many elements. The number of elements in a finite field is called the* order *of the field.*

In this section we will recall elements of Finite fields theory, for a reference look at Knapp [14].

Proposition 1.2.2. *A finite field $\boldsymbol{F}$ has positive characteristic $p > 0$ for some prime p. The cardinality of $\boldsymbol{F}$ is p^n where $n = [\boldsymbol{F} : \mathbb{F}_p]$ and $\mathbb{F}_p$ denotes the prime subfield [1] of $\boldsymbol{F}$.*

Lemma 1.2.3. *A field of prime power order p^n is a splitting field over $\mathbb{F}_p$ of $x^{p^n} - x$.*

Theorem 1.2.4. *Any two finite fields of the same order are isomorphic.*

Proof. The order of a finite field must be a prime power, say p^n. By Lemma 1.2.3, any field of order p^n is a splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$. By field theory, any two splitting fields of a fixed polynomial over $\mathbb{F}_p$ are isomorphic, so any two fields of order p^n are isomorphic. □

Theorem 1.2.5. *For any prime power p^n, a field of order p^n exists.*

Theorem 1.2.6. *The subfields of $\mathbb{F}_{p^n}$ have order p^d where $d \mid n$, and there is one such field for each d.*

[1] The prime subfield of a field $\mathbf{F}$ is the intersection of all subfields of $\mathbf{F}$. If $\mathbf{F}$ has characteristic p prime, then the prime subfield of $\mathbf{F}$ is isomorphic to the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of integers mod p. When $\mathbf{F}$ has characteristic zero, the prime subfield of $\mathbf{F}$ is isomorphic to the field of rational numbers.

1.2.1 Factorising polynomials

Theorem 1.2.7. *(Dedekind). Let $\boldsymbol{K}$ be a number field and $\alpha \in \mathcal{O}_{\boldsymbol{K}}$ such that $\boldsymbol{K} = \mathbb{Q}(\alpha)$. Let $f(T)$ be the minimal polynomial of α in $\mathbb{Z}[T]$. For any prime p not dividing $[\mathcal{O}_{\boldsymbol{K}} : \mathbb{Z}[\alpha]]$,write*

$$f(T) \equiv \pi_1(T)^{e_1} \dots \pi_g(T)^{e_g} \mod p$$

where $\pi_i(T)$ are distinct monic irreducibles in $\mathbb{F}_p[T]$. Then $(p) = p\mathcal{O}_{\boldsymbol{K}}$ factors into prime ideals as

$$(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

where there is a bijection between the $\mathfrak{p}_i$ and $\pi_i(T)$ such that $f_i = \deg \pi_i$. In particular, this applies for all p if $\mathcal{O}_{\boldsymbol{K}} = \mathbb{Z}[\alpha]$.

Proof. The main idea is that when p does not divide $[\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]]$ we will show the rings $\mathcal{O}_{\mathbf{K}}/(p)$ and $\mathbb{F}_p[T]/(\overline{f}(T))$ are isomorphic.
Let $m = [\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]]$, so

$$m\,\mathcal{O}_{\mathbf{K}} \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbf{K}}$$

For any prime p, there is a natural ring homomorphism $\mathbb{Z}[\alpha]/(p) \to \mathcal{O}_{\mathbf{K}}/(p)$. When p does not divide m, the first inclusion implies that the application $\mathbb{Z}[\alpha]/(p) \to \mathcal{O}_{\mathbf{K}}/(p)$ is onto: let $m\,m' \equiv 1 \mod p\mathbb{Z}$, so for any $x \in \mathcal{O}_{\mathbf{K}}$ we have $x \equiv m'mx \mod p\mathcal{O}_{\mathbf{K}}$ and $mx \in \mathbb{Z}[\alpha]$, so $m'mx \in \mathbb{Z}[\alpha]$ too. $\mathbb{Z}[\alpha]$ and $\mathcal{O}_{\mathbf{K}}$ are free rank n $\mathbb{Z}$-modules, so $\mathbb{Z}[\alpha]/(p)$ and $\mathcal{O}_{\mathbf{K}}/(p)$ both have size p^n, hence the surjective ring homomorphism between them is an isomorphism:

$$\mathbb{Z}[\alpha]/(p) \cong \mathcal{O}_{\mathbf{K}}/(p)$$

Since $\mathbb{Z}[T]/(f(T)) \cong \mathbb{Z}[\alpha]$ as rings by $h(T) \mod f(T) \mapsto h(\alpha)$,

$$\mathbb{Z}[\alpha]/(p) \cong \mathbb{Z}[T]/(f(T), p) \cong (\mathbb{Z}/p\mathbb{Z})[T]/(\overline{f}(T)) = \mathbb{F}_p[T]/(\overline{f}(T))$$

Therefore $\mathbb{F}_p[T]/(\overline{f}(T))$ and $\mathcal{O}_{\mathbf{K}}/(p)$ are isomorphic rings, as both are isomorphic to $\mathbb{Z}[\alpha]/(p)$. Let $\overline{f}(T) = \pi_1(T)^{e_1} \dots \pi_g(T)^{e_g}$ in $\mathbb{F}_p[T]$ where the $\pi_i(T)$ are distinct monic irreducibles and $e_i \geq 1$.
The number g is the number of maximal ideals in $\mathbb{F}_p[T]/(\overline{f}(T))$. Indeed, the maximal ideals of $\mathbb{F}_p[T]/(\overline{f}(T))$ are the ideals of the form $M/(\overline{f}(T))$ where M is a maximal ideal of $\mathbb{F}_p[T]$ containing $(\overline{f}(T))$. Any maximal ideal in $\mathbb{F}_p[T]/(\overline{f}(T))$ has the form (π) for one monic irreducible π in $\mathbb{F}_p[T]$, and (π) contains $(\overline{f}(T))$ precisely when $\pi \mid \overline{f}(T)$ in $\mathbb{F}_p[T]$.
For each maximal ideal M of $\mathbb{F}_p[T]/(\overline{f}(T))$, writing it as $(\pi_i)/(\overline{f}(T))$, we have

$$(\mathbb{F}_p[T]/(\overline{f}(T)))/M \cong \mathbb{F}_p[T]/(\pi_i(T))$$

whose size is $p^{\deg(\pi_i)}$. So counting the size of the residue ring modulo M tells us the degree of the irreducible polynomial associated to M. Finally, we show the multiplicity e_i of $\pi_i(T)$ in the factorisation of $\overline{f}(T)$ is the number of different positive integral powers of M.
Under the reduction map $\mathbb{F}_p[T] \to \mathbb{F}_p[T]/(\overline{f}(T))$, the ideal (π_i) maps onto the ideal $M = (\pi_i)/(\overline{f}(T))$, so we can compute powers of M by computing powers of (π_i) in $\mathbb{F}_p[T]$ first and then reducing. For $k \geq 1$, the k-th power of (π_i) in $\mathbb{F}_p[T]$ is $(\pi_i)^k = (\pi_i^k)$, whose image in $\mathbb{F}_p[T]/(\overline{f}(T))$ is $((\pi_i^k) + (\overline{f}(T)))/(\overline{f}(T))$. This image is also M^k. Since

$$(\pi_i^k) + (\overline{f}(T)) = (gcd(\pi_i^k, \overline{f}(T))) = \begin{cases} (\pi_i^k) & \text{if } 1 \leq k < e_i \\ (\pi_i^{e_i}) & \text{if } k \geq e_i \end{cases}$$

we have

$$M^k = \begin{cases} (\pi_i^k)/(\overline{f}(T)) & \text{if } 1 \leq k < e_i \\ (\pi_i^{e_i})/(\overline{f}(T)) & \text{if } k \geq e_i \end{cases}$$

Thus the positive integral powers of M in $\mathbb{F}_p[T]/(\overline{f}(T))$ are the ideals $(\pi_i^k)/(\overline{f}(T))$ for $1 \leq k \leq e_i$. The ring modulo such an ideal is isomorphic to $\mathbb{F}_p[T]/(\pi_i^k)$, which has different size for different k, so these powers of M are different from each other. To summarize, the monic irreducible factors of $\overline{f}(T)$ in $\mathbb{F}_p[T]$ are in bijection with the maximal ideals of the ring $\mathbb{F}_p[T]/(\overline{f}(T))$. For each monic irreducible factor, its degree as a polynomial and its multiplicity in the factorisation of $\overline{f}(T)$ can be read off from counting the size of the residue ring modulo the corresponding maximal ideal in $\mathbb{F}_p[T]$ and the number of different positive powers of this maximal ideal.
Now we turn to $\mathcal{O}_{\mathbf{K}}/(p)$. Factor $(p) = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$ with distinct primes $\mathfrak{p}_i$ and powers $e_i \geq 1$. Every maximal ideal of $\mathcal{O}_{\mathbf{K}}/(p)$ has the form $\mathfrak{p}/(p)$ where $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_{\mathbf{K}}$ containing (p), so $\mathfrak{p}$ is one of $\mathfrak{p}_1, \dots, \mathfrak{p}_g$. This shows that the maximal ideals of $\mathcal{O}_{\mathbf{K}}/(p)$ are in bijection with the prime factors of (p).
For each maximal ideal $\mathfrak{p}_i/(p)$ in $\mathcal{O}_{\mathbf{K}}/(p)$, its residue ring $(\mathcal{O}_{\mathbf{K}}/(p))/(\mathfrak{p}_i/(p)) \cong \mathcal{O}_{\mathbf{K}}/\mathfrak{p}_i$ has size p^{f_i} by definition of inertia degree. What are the powers of $\mathfrak{p}_i/(p)$ in $\mathcal{O}_{\mathbf{K}}/(p)$? They are images of powers of $\mathfrak{p}_i$ in $\mathcal{O}_{\mathbf{K}}$ under the reduction map $\mathcal{O}_{\mathbf{K}} \to \mathcal{O}_{\mathbf{K}}/(p)$. The image of $\mathfrak{p}_i^k$ under this reduction is $(\mathfrak{p}_i^k + (p))/(p)$ and

$$\mathfrak{p}_i^k + (p) = (gcd(\mathfrak{p}_i^k, (p))) = \begin{cases} (\mathfrak{p}_i^k) & \text{if } 1 \leq k < e_i \\ (\mathfrak{p}_i^{e_i}) & \text{if } k \geq e_i \end{cases}$$

so the positive integral powers of $\mathfrak{p}_i/(p)$ are the ideals $\mathfrak{p}_i^k/(p)$ for $1 \leq k \leq e_i$. Such ideals are different for different k (for instance, the quotients of $\mathcal{O}_{\mathbf{K}}/(p)$ by these ideals are rings of different size), so e_i is the number of different positive integral powers of $\mathfrak{p}_i/(p)$ in $\mathcal{O}_{\mathbf{K}}/(p)$. We have read off the shape of the factorisation of (p) from the ring structure of $\mathcal{O}_{\mathbf{K}}/(p)$ in the same way

that we did for the shape of the factorisation of $\overline{f}(T)$ from the structure of $\mathbb{F}_p[T]/(\overline{f}(T))$: for each maximal ideal in $\mathcal{O}_{\mathbf{K}}/(p)$, count the size of its residue ring as a power of p and also count the number of different positive powers of the maximal ideal. Such counting over all maximal ideals returns the same answers for isomorphic finite rings, so the isomorphism between $\mathbb{F}_p[T]/(\overline{f}(T))$ and $\mathcal{O}_{\mathbf{K}}/(p)$ shows the factorisations of $\overline{f}(T)$ and (p) have the same shape. □

For example, let $\mathbf{K} = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer. Then $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\omega]$ where $\omega = \sqrt{d}$ if $d \equiv 2, 3 \mod 4$ and $\omega = \frac{1+\sqrt{d}}{2}$ if $d \equiv 1 \mod 4$. In the first case, ω is a root of $T^2 - d$, so the way a prime p factors in $\mathcal{O}_{\mathbf{K}}$ is reflected by how $T^2 - d$ factors in $\mathbb{F}_p[T]$. In the second case, ω is a root of $T^2 - T + (1-d)/4$, so the way this polynomial factors modulo p tells us how p factors in $\mathcal{O}_{\mathbf{K}}$.

Proposition 1.2.8. *Suppose $\mathcal{O}$is an order in $\mathcal{O}_{\boldsymbol{K}}$. Then*

$$\operatorname{disc}_{\mathbb{Z}}(\mathcal{O}) = \operatorname{disc}_{\mathbb{Z}}(\mathcal{O}_{\boldsymbol{K}}) \cdot [\mathcal{O}_{\boldsymbol{K}} : \mathcal{O}]^2$$

Proof. Let $\sigma : K \to \mathbb{C}^n$ be the embedding $\sigma(a) = (\sigma_1(a), \ldots, \sigma_n(a))$, where σ_i are the distinct embeddings of $\mathbf{K}$ into $\mathbb{C}$, and n is the degree of $\mathbf{K}$ over $\mathbb{Q}$. Let A be a matrix whose rows are the images via σ of a basis for $\mathcal{O}_{\mathbf{K}}$, and let B be a matrix whose rows are the images via σ of a basis for $\mathcal{O}$. Since $\mathcal{O} \subseteq \mathcal{O}_{\mathbf{K}}$ has finite index, it is possible to show that there is an integer matrix C such that $CA = B$, and $|\det(C)| = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]$. Then

$$\operatorname{disc}_{\mathbb{Z}}(\mathcal{O}) = \det(B)^2 = \det(CA)^2 = [\mathcal{O}_{\mathbf{K}} : \mathcal{O}]^2 \cdot \operatorname{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}}).$$

□

Corollary 1.2.9. *Let $\boldsymbol{K} = Q(\alpha)$ and $\alpha \in \mathcal{O}_{\boldsymbol{K}}$ have minimal polynomial $f(T)$ in $\mathbb{Z}[T]$. For any prime p not dividing* $\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\alpha])$*, the shape of the factorisations of (p) in $\mathcal{O}_{\boldsymbol{K}}$ and $\overline{f}(T)$ in $\mathbb{F}_p[T]$ agree.*

Proof. Since $\operatorname{disc}_{\mathbb{Z}}(\mathbb{Z}[\alpha]) = [\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]]^2 \operatorname{disc}_{\mathbb{Z}}(\mathcal{O}_{\mathbf{K}})$, if p does not divide $\operatorname{disc}(\mathbb{Z}[\alpha])$ then p does not divide $[\mathcal{O}_{\mathbf{K}} : \mathbb{Z}[\alpha]]$, so Theorem 1.2.7 applies to p. □

1.3 Elements of Galois Theory

1.3.1 The Galois correspondence

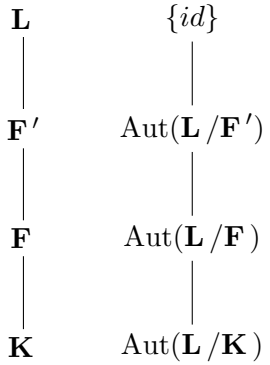
Let $\mathbf{L}/\mathbf{K}$ be a field extension, a $\mathbf{K}$-automorphism of L is a field automorphism $\sigma : \mathbf{L} \to \mathbf{L}$ which fixes the elements of $\mathbf{K}$: $\sigma(c) = c$ for all $c \in \mathbf{K}$. The set of $\mathbf{K}$-automorphisms of $\mathbf{L}$ is a group under composition and is denoted $\mathrm{Aut}(\mathbf{L}/\mathbf{K})$. Its identity element is the identity function on $\mathbf{L}$.
From any intermediate field $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$ we get a subgroup in $\mathrm{Aut}(\mathbf{L}/\mathbf{K})$:

$$\mathrm{Aut}(\mathbf{L}/\mathbf{F}) = \{\sigma \in \mathrm{Aut}(\mathbf{L}/\mathbf{K}) : \sigma(\alpha) = \alpha \text{ for all } \alpha \in \mathbf{F}\}$$

In the other direction, from any subgroup H of $\mathrm{Aut}(\mathbf{L}/\mathbf{K})$ we get a field which lies between $\mathbf{K}$ and $\mathbf{L}$:

$$\mathbf{L}^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}$$

The correspondences $\mathbf{F} \to \mathrm{Aut}(\mathbf{L}/\mathbf{F})$ and $H \to \mathbf{L}^H$ between intermediate fields in the extension $\mathbf{L}/\mathbf{K}$ and subgroups of $\mathrm{Aut}(\mathbf{L}/\mathbf{K})$ is inclusion-reversing: if $\mathbf{F} \subset \mathbf{F}'$ then $\mathrm{Aut}(\mathbf{L}/\mathbf{F}') \subset \mathrm{Aut}(\mathbf{L}/\mathbf{F})$, while if $H \subset H'$ then $L^{H'} \subset L^H$.



Definition 1.3.1. *An extension $\boldsymbol{L}/\boldsymbol{K}$ is said* normal *if every irreducible polynomial in $\boldsymbol{K}[X]$ with a root in $\boldsymbol{L}$ splits in $\boldsymbol{L}[X]$.*

Theorem 1.3.2. *If $\boldsymbol{L}/\boldsymbol{K}$ is a finite extension the following are equivalent:*

- $|\mathrm{Aut}(\boldsymbol{L}/\boldsymbol{K})| = [\boldsymbol{L} : \boldsymbol{K}]$,
- $\boldsymbol{L}^{\mathrm{Aut}(\boldsymbol{L}/\boldsymbol{K})} = \boldsymbol{K}$,
- $\boldsymbol{L}/\boldsymbol{K}$ *is separable and normal,*
- $\boldsymbol{L}$ *is the splitting field over $\boldsymbol{K}$ of a separable polynomial with coefficients in $\boldsymbol{K}$.*

For a proof look at [14] and [13].

Definition 1.3.3. *A finite extension* $\boldsymbol{L}/\boldsymbol{K}$ *is called a* finite Galois extension *when it satisfies the equivalent properties of Theorem 1.3.2. When* $\boldsymbol{L}/\boldsymbol{K}$ *is a finite Galois extension, the group* $\mathrm{Aut}(\boldsymbol{L}/\boldsymbol{K})$ *is denoted* $\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K})$ *and is called the* Galois group *of the extension.*

Theorem 1.3.4. *If* $\boldsymbol{L}/\boldsymbol{K}$ *is a finite Galois extension and* $\boldsymbol{K} \subset \boldsymbol{F} \subset \boldsymbol{L}$ *then* $\boldsymbol{L}/\boldsymbol{F}$ *is a finite Galois extension.*

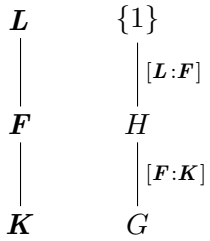
Proof. When $\mathbf{K} \subset \mathbf{F} \subset \mathbf{L}$, separability and normality are both preserved in the passage from $\mathbf{L}/\mathbf{K}$ to $\mathbf{L}/\mathbf{F}$ because the minimal polynomial over $\mathbf{F}$ of any element of $\mathbf{L}$ divides its minimal polynomial over $\mathbf{K}$. □

Now we can state a famous Theorem due to Artin, for a reference Knapp [14]:

Theorem 1.3.5. *Let* E *be a field and* H *be a finite group of automorphisms of* E *then* $\left[E : E^H\right]$ *is finite and* E/E^H *is a Galois extension and* $\mathrm{Gal}(E/E^H) = H$.

Fundamental Theorem of Galois theory. *Let* $\boldsymbol{L}/\boldsymbol{K}$ *be a finite Galois extension with* $G = \mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K})$. *Then the inclusion-reversing mappings* $\boldsymbol{F} \to \mathrm{Gal}(\boldsymbol{L}/\boldsymbol{F})$ *and* $H \to \boldsymbol{L}^H$ *between the intermediate fields between* $\boldsymbol{K}$ *and* $\boldsymbol{L}$ *and the subgroups of* G *are inverse of each other and satisfy the following properties when* $\boldsymbol{F}$ *and* H *correspond* $(\boldsymbol{F} = \boldsymbol{L}^H ; H = \mathrm{Gal}(\boldsymbol{L}/\boldsymbol{F}))$*:*

1. $|H| = [\boldsymbol{L} : \boldsymbol{F}]$ *and* $[\boldsymbol{F} : \boldsymbol{K}] = [G : H]$,
2. *two intermediate fields* $\boldsymbol{F}$ *and* $\boldsymbol{F}'$*, with corresponding subgroups* H *and* H'*, are isomorphic over* $\boldsymbol{K}$ *if and only if* H *and* H' *are conjugate subgroups of* G*; in particular,* $\mathrm{Gal}(\boldsymbol{L}/\sigma(\boldsymbol{F})) = \sigma\,\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{F})\sigma^{-1}$ *for* $\sigma \in G$,
3. $\boldsymbol{F}/\boldsymbol{K}$ *is Galois if and only if* $H \triangleleft G$*, in which case the restriction map* $G \to \mathrm{Gal}(\boldsymbol{F}/\boldsymbol{K})$*, where* $\sigma \mapsto \sigma|_{\boldsymbol{F}}$*, is surjective with kernel* H*, so* $G/H \cong \mathrm{Gal}(\boldsymbol{F}/\boldsymbol{K})$.



The bijection in Theorem 1.3.1 is called the *Galois correspondence* and it holds only for finite Galois extensions.

1.3.2 Galois Theory and Number fields

Definition 1.3.6. *Suppose* $\boldsymbol{K} \subset \mathbb{C}$ *is a number field,* $\boldsymbol{K}$ *is* Galois *if* $\boldsymbol{K}/\mathbb{Q}$ *is a finite Galois extension.*

For example, trivially $\mathbb{Q}$ is Galois over itself. Any quadratic extension $\mathbf{K}/\mathbf{L}$ is Galois, since it is of the form $\mathbf{L}(\sqrt{a})$, for some $a \in \mathbf{L}$, and the non trivial embedding is induced by $\sqrt{a} \mapsto -\sqrt{a}$, this means that there is always one nontrivial automorphism. If $f \in \mathbf{L}[x]$ is an irreducible cubic polynomial, and a is a root of f, then $\mathbf{L}(a)$ is Galois over $\mathbf{L}$ if and only if the discriminant of f is a perfect square in $\mathbf{L}$.

If $\mathbf{K}/\mathbb{Q}$ is a number field, then the Galois closure $\mathbf{K}^{gc}$ of $\mathbf{K}$ is the field generated by all images of $\mathbf{K}$ under all embeddings in $\mathbb{C}$, more generally, if $\mathbf{K}/\mathbf{L}$ is an extension, the Galois closure of $\mathbf{K}$ over $\mathbf{L}$ is the field generated by images of embeddings $\mathbf{K} \to \mathbb{C}$ that are the identity map on $\mathbf{L}$. If $\mathbf{K} = \mathbb{Q}(a)$, then $\mathbf{K}^{gc}$ is generated by each of the conjugates of a, and is hence Galois over $\mathbb{Q}$, since the image under an embedding of any polynomial in the conjugates of a is again a polynomial in conjugates of a. Hence there is a natural embedding of $\mathrm{Gal}(K^{gc}/\mathbb{Q})$ into the group of permutations of the conjugates of a. If there are n conjugates of a, then this is an embedding $\mathrm{Gal}(\mathbf{K}^{gc}/\mathbb{Q}) \hookrightarrow S_n$, where S_n is the symmetric group on n elements, thus the degree of the $\mathbf{K}^{gc}$ over $\mathbb{Q}$ is a divisor of $n!$.

Let n be a positive integer. Consider the field $\mathbf{K} = \mathbb{Q}(\zeta_n)$, where $\zeta_n = e^{2\pi i/n}$ is a primitive nth root of unity. If $\sigma : \mathbf{K} \to \mathbb{C}$ is an embedding, then $\sigma(\zeta_n)$ is also an nth root of unity, and the group of nth roots of unity is cyclic, so $\sigma(\zeta_n) = \zeta_n^m$ for some m which is invertible modulo n. Thus $\mathbf{K}$ is Galois and $\mathrm{Gal}(\mathbf{K}/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$. However, it can be proved that $[\mathbf{K} : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler function, so this map is an isomorphism.

Let $\mathbf{F}/\mathbf{K}$ be an extension of number fields and let $\mathcal{O}_\mathbf{F}$ and $\mathcal{O}_\mathbf{K}$ be their respective rings of integers. The ring of integers of a number field is a Dedekind domain, and every ideal factors uniquely as a finite product of prime ideals as we have seen. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_\mathbf{K}$, $\mathfrak{p} \neq 0$. Then $\mathfrak{p}\,\mathcal{O}_\mathbf{F}$ is an ideal of $\mathcal{O}_\mathbf{F}$. Let us assume that the prime ideal factorisation of $\mathfrak{p}\,\mathcal{O}_\mathbf{F}$ into primes of $\mathcal{O}_\mathbf{F}$ is as follows:

$$\mathfrak{p}\,\mathcal{O}_\mathbf{F} = \prod_{i=1}^{g} P_i^{e_i} \tag{1.2}$$

We say that the primes P_i lie above $\mathfrak{p}$ and $P_i \mid \mathfrak{p}$ (divides). The exponent e_i is the ramification index of P_i over $\mathfrak{p}$. Notice that for each prime ideal P_i, the quotient ring $\mathcal{O}_\mathbf{F}/P_i$ is a finite field extension of the finite field $\mathcal{O}_\mathbf{K}/\mathfrak{p}$.

The degree of this extension is called the inertial degree of P_i over $\mathfrak{p}$ and it is usually denoted by:

$$f_i = [\mathcal{O}_{\mathbf{F}}/P_i : \mathcal{O}_{\mathbf{K}}/\mathfrak{p}]$$

As before the ramification index and the inertial degree are related by the formula:

$$\sum_{i=1}^{g} e_i f_i = [\mathbf{F} : \mathbf{K}]$$

where g is the number of prime ideals lying above $\mathfrak{p}$. This follows taking Norm on both size of (1.2), for a reference Takashi [35], 2.12.

Definition 1.3.7. *Let $\boldsymbol{F}, \boldsymbol{K}$ and $P_i, \mathfrak{p}$ be as above.*

1. *If $e_i > 1$ for some i, then we say that P_i is* ramified *over $\mathfrak{p}$ and $\mathfrak{p}$ ramifies in $\boldsymbol{F}/\boldsymbol{K}$. If $e_i = 1$ for all i then we say that $\mathfrak{p}$ is* unramified *in $\boldsymbol{F}/\boldsymbol{K}$.*

2. *If there is a unique prime ideal P lying above $\mathfrak{p}$ (so $r = 1$) and $f = 1$ then we say that $\mathfrak{p}$ is* totally ramified *in $\boldsymbol{F}/\boldsymbol{K}$. In this case $e = [\boldsymbol{F} : \boldsymbol{K}]$.*

3. *On the other hand, if $e_i = f_i = 1$ for all i, we say that $\mathfrak{p}$ is* totally split *in $\boldsymbol{F}/\boldsymbol{K}$. Notice that there are exactly $r = [\boldsymbol{F} : \boldsymbol{K}]$ prime ideals of $\mathcal{O}_{\boldsymbol{F}}$ lying above $\mathfrak{p}$.*

4. *Let p be the characteristic of the residue field $\mathcal{O}_{\boldsymbol{K}}/\mathfrak{p}$. If e_i and p are relatively prime, then we say that P_i is* tamely ramified. *If $p \mid e_i$ then we say that P_i is* wildly ramified.

When the extension $\mathbf{F}/\mathbf{K}$ is a Galois extension then we are in a more simple case:

Lemma 1.3.8. *Let $P_1, \ldots, P_g$ be ideals of $\mathcal{O}_{\boldsymbol{F}}$ such that $(P_i, P_j) = 1$, $i \neq j$. Then, for any $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ in $\mathcal{O}_{\boldsymbol{K}}$, the system:*

$$\begin{cases} x \equiv \mathfrak{p}_1 \mod P_1 \\ \cdots \\ x \equiv \mathfrak{p}_g \mod P_g \end{cases}$$

has a solution in $\mathcal{O}_{\boldsymbol{K}}$ uniquely determined $\mod P_1 \cdots P_g$.

Proof. For a proof Knapp [13]. □

Proposition 1.3.9. *For each prime $\mathfrak{p} \in \mathcal{O}_{\boldsymbol{K}}$, the Galois group acts transitively on $P_1, \ldots, P_g$ if $\mathfrak{p}\,\mathcal{O}_{\boldsymbol{F}} = \prod_{i=1}^{g} P_i^{e_i}$.*

Proof. We must show that there is a $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$ such that $P_i^{\sigma} = P_j$ $i \neq j$. Let us proceed by contradiction and suppose that $P_0^{\sigma} \neq P_1$ for any $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$. By Lemma 1.3.8, there exists an $\alpha \in \mathcal{O}_{\mathbf{K}}$ such that $\alpha \equiv 0 \mod P_1$ and $\alpha \equiv 1 \mod P_0^{\sigma}$, $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$. Therefore, we have $\alpha \in P_1$ but $\alpha \notin P_0^{\sigma}$ for all $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$. However, since

$$\mathrm{Norm}_{\mathbf{F}/\mathbf{K}}\, \alpha = \prod_{\sigma} \alpha^{\sigma} \in P_1 \cap \mathcal{O}_{\mathbf{K}} = \mathfrak{p} \subset P_0$$

we have $P_0 \mid \prod_{\sigma} \alpha^{\sigma}$ and so, for some $\sigma_0, P_0 \mid \alpha^{\sigma_0}$, i.e. $\alpha \in P_0^{\sigma_0^{-1}}$, a contradiction. □

Theorem 1.3.10. *Assume that $\boldsymbol{F}/\boldsymbol{K}$ is a Galois extension of number fields. Then all the ramification indices e_i are equal to the same number $e := e(\boldsymbol{F}/\boldsymbol{K})$, all the inertial degrees f_i are equal to the same number $f := f(\boldsymbol{F}/\boldsymbol{K})$ and the ideal $\mathfrak{p}\,\mathcal{O}_{\boldsymbol{F}}$ factors as:*

$$\mathfrak{p}\,\mathcal{O}_{\boldsymbol{F}} = \prod_{i=1}^{g} P_i^{e} = (P_1 \cdot P_2 \cdot \ldots \cdot P_g)^{e}$$

Moreover, $g := g(\boldsymbol{F}/\boldsymbol{K})$:

$$e \cdot f \cdot g = [\boldsymbol{F} : \boldsymbol{K}]$$

Proof. Let $\mathfrak{p}\,\mathcal{O}_{\mathbf{F}} = \prod_{i=1}^{g} P_i^{e_i}$, where $P_1, \ldots, P_g$ are distinct prime ideals of $\mathcal{O}_{\mathbf{F}}$, and let $f_i = [\mathcal{O}_{\mathbf{F}}/P_i : \mathcal{O}_{\mathbf{K}}/\mathfrak{p}]$ for $i = 1, \ldots, g$.
For any $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$, we clearly have $\sigma(\mathfrak{p}) = \mathfrak{p}$ and $\sigma(\mathcal{O}_{\mathbf{F}}) = \mathcal{O}_{\mathbf{F}}$, hence $\sigma(\mathfrak{p}\,\mathcal{O}_{\mathbf{F}}) = \mathfrak{p}\,\mathcal{O}_{\mathbf{F}}$. The action of the Galois group is transitive for Proposition 1.3.9, so for any i with $1 \leq i \leq r$, there exists $\sigma \in \mathrm{Gal}(\mathbf{F}/\mathbf{K})$ such that $\sigma(P_i) = P_1$, and consequently, $\mathcal{O}_{\mathbf{F}}/P_i \cong \sigma(\mathcal{O}_{\mathbf{F}})/\sigma(P_i) = \mathcal{O}_{\mathbf{F}}/P_1$. Thus $e_i = e_1$ and similarly it is possible to show that $f_i = f_1$. Since $\sum_{i=1}^{g} e_i f_i = n$, the last statement of the theorem follows. □

Let us give an example in a simple setting: let consider a quadratic extensions. Suppose $\mathbf{K}/\mathbb{Q}$ is a quadratic field. Then $\mathbf{K}$ is Galois, so for each prime $p \in \mathbb{Z}$ we have $2 = e\,f\,g$. There are exactly three possibilties:

- *Ramified*: $e = 2$, $f = g = 1$
  The prime p ramifies in $\mathcal{O}_{\mathbf{K}}$, so $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}^2$. There are only finitely many such primes, since if $f(x)$ is the minimal polynomial of a generator for $\mathcal{O}_{\mathbf{K}}$, then p ramifies if and only if $f(x)$ has a multiple root modulo p. However, $f(x)$ has a multiple root modulo p if and only if p divides the discriminant of $f(x)$, which is nonzero because $f(x)$

is irreducible over $\mathbb{Z}$. This argument shows there are only finitely many ramified primes in any number field, in particular by Theorem 1.1.35 it follows that these primes are exactly the ones that divide the discriminant.

- *Inert*: $e = 1$, $f = 2$, $g = 1$
  The prime p is inert in $\mathcal{O}_{\mathbf{K}}$, so $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}$ is prime.

- *Split*: $e = f = 1$, $g = 2$
  The prime p splits in $\mathcal{O}_{\mathbf{K}}$: $p\mathcal{O}_{\mathbf{K}} = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$.

Let us give an example. Suppose that $\mathbf{K} = \mathbb{Q}(\sqrt{5})$, so $\mathcal{O}_{\mathbf{K}} = \mathbb{Z}[\gamma]$, where $\gamma = (1+\sqrt{5})/2$. Then $p = 5$ is ramified, since $p\mathcal{O}_{\mathbf{K}} = (\sqrt{5})^2$. More generally, the order $\mathbb{Z}[\sqrt{5}]$ has index 2 in $\mathcal{O}_{\mathbf{K}}$, so for any prime $p \neq 2$ we can determine the factorisation of p in $\mathcal{O}_{\mathbf{K}}$ by finding the factorisation of the polynomial $x^2 - 5 \in \mathbb{F}_p[x]$, using Corollary 1.2.9.
The polynomial $x^2 - 5$ splits as a product of two distinct factors in $\mathbb{F}_p[x]$ if and only if $e = f = 1$ and $g = 2$. For $p \neq 2, 5$ this is the case if and only if 5 is a square in $\mathbb{F}_p$, i.e., if $\left(\frac{5}{p}\right) = 1$, where $\left(\frac{5}{p}\right)$ is $+1$ if 5 is a square mod p and -1 if 5 is not. By quadratic reciprocity[2],

$$\left(\frac{5}{p}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases} +1 & \text{if } p \equiv \pm 1 \mod 5 \\ -1 & \text{if } p \equiv \pm 2 \mod 5 \end{cases}$$

Thus whether p splits or is inert in $\mathcal{O}_{\mathbf{K}}$ is determined by the residue class of p modulo 5.

1.3.3 The Decomposition and the Inertia

Suppose $\mathbf{K}$ is a Galois number field over $\mathbb{Q}$ and Galois group $G = \mathrm{Gal}(\mathbf{K}/\mathbb{Q})$. Fix a prime $\mathfrak{p} \subset \mathcal{O}_{\mathbf{K}}$ lying over $p \in \mathbb{Z}$.

Definition 1.3.11. *The* decomposition group *of* $\mathfrak{p}$ *is the subgroup*

$$D_{\mathfrak{p}} = \{\sigma \in G : \sigma(\mathfrak{p}) = \mathfrak{p}\} \leq G$$

Recall that G acts on the set of primes $\mathfrak{p}$ lying over p. Thus the decomposition group is the stabilizer in G of $\mathfrak{p}$, in particular we have $[G : D_{\mathfrak{p}}] = g$.

Lemma 1.3.12. *The decomposition subgroups* $D_{\mathfrak{p}}$ *corresponding to primes* $\mathfrak{p}$ *lying over a given* p *are all conjugate in* G.

Proof. We have $\tau(\sigma(\tau^{-1}(\mathfrak{p}))) = \mathfrak{p}$ if and only if $\sigma(\tau^{-1}(\mathfrak{p})) = \tau^{-1}\mathfrak{p}$. Thus $\tau\sigma\tau^{-1} \in D_{\mathfrak{p}}$ if and only if $\sigma \in D_{\tau^{-1}\mathfrak{p}}$, so $\tau^{-1}D_{\mathfrak{p}}\tau = D_{\tau^{-1}\mathfrak{p}}$. The lemma follows because G acts transitively on the set of $\mathfrak{p}$ lying over p, by Proposition 1.3.9. □

[2]For a reference, Milne [21], Chapter V.

The decomposition group is extremely useful because it allows us to see the extension $\mathbf{K}/\mathbb{Q}$ as a tower of extensions, such that at each step in the tower we understand the splitting behavior of the primes lying over p.

Proposition 1.3.13. *The fixed field $\boldsymbol{K}^D$ of $D_{\mathfrak{p}}$*

$$\boldsymbol{K}^D = \{a \in \boldsymbol{K} : \sigma(a) = a \text{ for all } \sigma \in D_{\mathfrak{p}}\}$$

is the smallest subfield $\boldsymbol{L} \subset \boldsymbol{K}$ such that $\mathfrak{p} \cap \boldsymbol{L}$ does not split in $\boldsymbol{K}$, i.e., $g(\boldsymbol{K}/\boldsymbol{L}) = 1$.

Proof. First suppose $\mathbf{L} = \mathbf{K}^D$, and note that by Galois theory $\mathrm{Gal}(\mathbf{K}/\mathbf{L}) \cong D$, and the group $D_{\mathfrak{p}}$ acts transitively on the primes of $\mathbf{K}$ lying over $\mathfrak{p} \cap \mathbf{L}$. One of these primes is $\mathfrak{p}$, and $D_{\mathfrak{p}}$ fixes $\mathfrak{p}$ by definition, so there is only one prime of $\mathbf{K}$ lying over $\mathfrak{p} \cap \mathbf{L}$, i.e., $\mathfrak{p} \cap \mathbf{L}$ does not split in $\mathbf{K}$. Conversely, if $\mathbf{L} \subset \mathbf{K}$ is such that $\mathfrak{p} \cap \mathbf{L}$ does not split in $\mathbf{K}$, then $\mathrm{Gal}(\mathbf{K}/\mathbf{L})$ fixes $\mathfrak{p}$, because it is the only prime over $\mathfrak{p} \cap \mathbf{L}$, so $\mathrm{Gal}(\mathbf{K}/\mathbf{L}) \subset D_{\mathfrak{p}}$, hence $\mathbf{K}^D \subset \mathbf{L}$. □

It can be proved, for a reference Knapp [13] that:

Proposition 1.3.14. *Let $\boldsymbol{L} = \boldsymbol{K}^D$ for our fixed prime p and Galois extension $\boldsymbol{K}/\mathbb{Q}$. Then p does not ramify and splits completely in $\boldsymbol{L}$. Also $f(\boldsymbol{K}/\mathbb{Q}) = f(\boldsymbol{K}/\boldsymbol{L})$ and $e(\boldsymbol{K}/\mathbb{Q}) = e(\boldsymbol{K}/\boldsymbol{L})$.*

Each $\sigma \in D = D_{\mathfrak{p}}$ acts on the finite field $\mathbf{F}_{\mathfrak{p}} = \mathcal{O}_{\mathbf{K}}/\mathfrak{p}$: we have a homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$$

Let $f = [\mathbf{F}_{\mathfrak{p}} : \mathbb{F}_p]$. The group $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ contains the element $\mathrm{Frob}_{\mathfrak{p}}$ defined by

$$\mathrm{Frob}_{\mathfrak{p}}(x) = x^p,$$

because $(xy)^p = x^p y^p$ and

$$(x+y)^p = x^p + px^{p-1}y + \cdots + y^p \equiv x^p + y^p \mod p$$

The group $\mathbf{F}_{\mathfrak{p}}^*$ is cyclic, so there is an element $a \in \mathbf{F}_{\mathfrak{p}}^*$ of order $p^f - 1$, and $\mathbf{F}_{\mathfrak{p}} = \mathbb{F}_p(a)$.
Then $\mathrm{Frob}_{\mathfrak{p}}^n(a) = a^{p^n} = a$ if and only if $(p^f - 1) \mid p^n - 1$ which is the case precisely when $f \mid n$, so the order of $\mathrm{Frob}_{\mathfrak{p}}$ is f. Since the order of the automorphism group of a field extension is at most the degree of the extension, we conclude that $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is generated by $\mathrm{Frob}_{\mathfrak{p}}$.
Also, since $\mathrm{Aut}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ has order equal to the degree, we conclude that $\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p$ is Galois, with group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ cyclic of order f generated by $\mathrm{Frob}_{\mathfrak{p}}$.

Theorem 1.3.15. *The homomorphism* $\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\boldsymbol{F}_{\mathfrak{p}}/\mathbb{F}_p)$ *is surjective.*

Proof. Let $\tilde{a} \in \mathbf{F}_{\mathfrak{p}}$ be an element such that $\mathbf{F}_{\mathfrak{p}} = \mathbb{F}_p(\tilde{a})$. Lift $\tilde{a}$ to an algebraic integer $a \in \mathcal{O}_{\mathbf{K}}$, and let $f = \prod_{\sigma \in D_{\mathfrak{p}}}(x - \sigma(a)) \in \mathbf{K}^D[x]$ be the characteristic polynomial of a over $\mathbf{K}^D$.
Using Proposition 1.3.14 we see that f reduces to the minimal polynomial $\tilde{f} = \prod(x - \sigma(\tilde{a})) \in \mathbb{F}_p[x]$ of $\tilde{a}$: by the Proposition the coefficients of $\tilde{f}$ are in $\mathbb{F}_p$; $\tilde{a}$ satisfies $\tilde{f}$, and the degree of $\tilde{f}$ equals the degree of the minimal polynomial of $\tilde{a}$.
The roots of $\tilde{f}$ are of the form $\sigma(\tilde{a})$, and the element $\mathrm{Frob}_{\mathfrak{p}}(a)$ is also a root of $\tilde{f}$, so it is of the form $\sigma(\tilde{a})$. We conclude that the generator $\mathrm{Frob}_{\mathfrak{p}}$ of $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is in the image of φ, which proves the theorem. □

Definition 1.3.16. *The* inertia group $I_{\mathfrak{p}}$ *is the kernel of the application* $\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\boldsymbol{F}_{\mathfrak{p}}/\mathbb{F}_p)$.

So combining everything, we find an exact sequence of groups

$$1 \to I_{\mathfrak{p}} \to D_{\mathfrak{p}} \to \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p) \to 1 \tag{1.3}$$

The inertia group is a measure of how p ramifies in $\mathbf{K}$.

Corollary 1.3.17. *We have* $\#I_{\mathfrak{p}} = e(\mathfrak{p}/p)$, *where* $\mathfrak{p}$ *is a prime of* $\boldsymbol{K}$ *over* p.

Proof. The sequence (1.3) implies that $\#I_{\mathfrak{p}} = \#D_{\mathfrak{p}}/f(\mathbf{K}/\mathbb{Q})$. Applying Propositions 1.3.13 and 1.3.14, we have

$$\#D_{\mathfrak{p}} = [\mathbf{K} : \mathbf{L}] = \frac{[\mathbf{K} : \mathbb{Q}]}{g} = \frac{efg}{g} = ef$$

Dividing both sides by $f = f(\mathbf{K}/\mathbb{Q})$ proves the corollary. □

We have the following characterization of $I_{\mathfrak{p}}$.

Proposition 1.3.18. *Let* $\boldsymbol{K}/\mathbb{Q}$ *be a Galois extension with group* G, *let* $\mathfrak{p}$ *be a prime lying over a prime* p. *Then*

$$I_{\mathfrak{p}} = \{\sigma \in G : \sigma(a) \equiv a \mod \mathfrak{p} \text{ for all } a \in \mathcal{O}_{\boldsymbol{K}}\}.$$

Proof. By definition $I_{\mathfrak{p}} = \{\sigma \in D_{\mathfrak{p}} : \sigma(a) = a \pmod{\mathfrak{p}} \text{ for all } a \in \mathcal{O}_{\mathbf{K}}\}$, so it suffices to show that if $\sigma \notin D_{\mathfrak{p}}$, then there exists $a \in \mathcal{O}_{\mathbf{K}}$ such that $\sigma(a) \not\equiv a \pmod{\mathfrak{p}}$. If $\sigma \notin D_{\mathfrak{p}}$, we have $\sigma^{-1}(\mathfrak{p}) \neq \mathfrak{p}$, so since both are maximal ideals, there exists $a \in \mathfrak{p}$ with $a \notin \sigma^{-1}(\mathfrak{p})$, i.e., $\sigma(a) \notin \mathfrak{p}$. Thus $\sigma(a) \not\equiv a \mod \mathfrak{p}$. □

1.3.4 Frobenius Elements

Suppose that $\mathbf{K}/\mathbb{Q}$ is a finite Galois extension with group G and p is a prime such that $e = 1$, an unramified prime. Then $I = I_{\mathfrak{p}} = 1$ for any $\mathfrak{p} \mid p$, so the map φ of 1.3 is a canonical isomorphism $D_{\mathfrak{p}} \cong \mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$. By the previous section, the group $\mathrm{Gal}(\mathbf{F}_{\mathfrak{p}}/\mathbb{F}_p)$ is cyclic with canonical generator Frob_p. The *Frobenius element* corresponding to $\mathfrak{p}$ is $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. It is the unique element of G such that for all $a \in \mathcal{O}_{\mathbf{K}}$ we have

$$\mathrm{Frob}_{\mathfrak{p}}(a) \equiv a^p \mod \mathfrak{p}.$$

Just as the primes $\mathfrak{p}$ and decomposition groups D are all conjugate, the Frobenius elements over a given prime are conjugate.

Proposition 1.3.19. *For each $\sigma \in G$, we have*

$$\mathrm{Frob}_{\sigma\mathfrak{p}} = \sigma \,\mathrm{Frob}_{\mathfrak{p}}\, \sigma^{-1}.$$

In particular, the Frobenius elements lying over a given prime are all conjugate.

Proof. Fix $\sigma \in G$. For any $a \in \mathcal{O}_{\mathbf{K}}$ we have $\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - \sigma^{-1}(a) \in \mathfrak{p}$. Multiply by σ we see that $\sigma\,\mathrm{Frob}_{\mathfrak{p}}(\sigma^{-1}(a)) - a \in \sigma\mathfrak{p}$, which proves the proposition. □

Thus the conjugacy class of $\mathrm{Frob}_{\mathfrak{p}}$ in G is a well defined function of p. For example, if G is abelian, then $\mathrm{Frob}_{\mathfrak{p}}$ does not depend on the choice of $\mathfrak{p}$ lying over p and we obtain a well defined symbol $\left(\frac{\mathbf{K}/\mathbb{Q}}{p}\right) = \mathrm{Frob}_{\mathfrak{p}} \in G$ called the *Artin symbol*. It extends to a map from the free abelian group on unramified primes to the group G.

1.3.5 The absolute Galois group

Definition 1.3.20. *A group G with a topology is a* topological group *if the maps*

$$(g,h) \mapsto gh : G \times G \to G, \qquad g \mapsto g^{-1} : G \to G$$

are continuous with rispect to the topology of the group.

Let $\mathbf{K}$ be a Galois extension of $\mathbf{F}$, finite or not, in which case we extend the definition given in the obvious way:

Definition 1.3.21. *A field $\boldsymbol{K} \supseteq \boldsymbol{F}$, not necessarily of finite degree, is said to be* Galois *over $\boldsymbol{F}$ if*

(a) it is algebraic and separable over $\boldsymbol{F}$, i.e., every element of $\boldsymbol{K}$ is a simple root of a polynomial with coefficients in $\boldsymbol{F}$;

(b) it is normal over $\boldsymbol{F}$, i.e., every irreducible polynomial with coefficients in $\boldsymbol{F}$ having a root in $\boldsymbol{K}$ splits in $\boldsymbol{K}[X]$.

Definition 1.3.22. *Let $\boldsymbol{K}$ be any field, $\overline{\boldsymbol{K}}$ a separable algebraic closure of $\boldsymbol{K}$. The* absolute Galois group $\mathrm{Gal}(\overline{\boldsymbol{K}}/\boldsymbol{K})$ *of $\boldsymbol{K}$ is the group of all field automorphisms $\sigma : \overline{\boldsymbol{K}} \to \overline{\boldsymbol{K}}$ that restrict to the identity map on $\boldsymbol{K}$ under the group operation of composition.*

We will use the following notation for the rest of this section:

$$G = \mathrm{Gal}(\mathbf{K}/\mathbf{F})$$
$$\mathcal{I} = \{\mathbf{E} \ : \ \mathbf{F} \subseteq \mathbf{E} \subseteq \mathbf{K} \ , \ [\mathbf{E} : \mathbf{F}] < \infty \ \text{ and } \ \mathbf{E}/\mathbf{F} \ \text{ is Galois}\}$$
$$\mathcal{N} = \{N \subseteq G \ : \ N = \mathrm{Gal}(\mathbf{K}/\mathbf{E}) \ \text{ for some } \ \mathbf{E} \in \mathcal{I}\}$$

Lemma 1.3.23. *If $\alpha_1, \ldots, \alpha_n \in \boldsymbol{K}$, then there is an $\boldsymbol{E} \in \mathcal{I}$ with $\alpha_i \in \boldsymbol{E}$ $\forall i$.*

Proof. Let $\mathbf{E} \subseteq \mathbf{K}$ be the splitting field of the minimal polynomial of the α_i over $\mathbf{F}$. Then, as each α_i is separable over $\mathbf{F}$, the field $\mathbf{E}$ is normal and separable over $\mathbf{F}$; hence $\mathbf{E}$ is Galois over $\mathbf{F}$. Since there are finitely many $\alpha : i$, we have $[\mathbf{E} : \mathbf{F}] < \infty$, so $\mathbf{E} \in \mathcal{I}$. □

Lemma 1.3.24. *Let $N \in \mathcal{N}$, and set $N = \mathrm{Gal}(\boldsymbol{K}/\boldsymbol{E})$ with $\boldsymbol{E} \in \mathcal{I}$. Then N is normal in G. Moreover $G/N \cong \mathrm{Gal}(\boldsymbol{E}/\boldsymbol{F})$. Thus, $|G/N| = |\mathrm{Gal}(\boldsymbol{E}/\boldsymbol{F})| = [\boldsymbol{E} : \boldsymbol{F}] < \infty$.*

Proof. Since $\mathbf{K}$ is normal and separable over $\mathbf{F}$, the field $\mathbf{K}$ is also normal and separable over $\mathbf{E}$, so $\mathbf{K}$ is Galois over $\mathbf{E}$. The map $\theta : G \to \mathrm{Gal}(\mathbf{E}/\mathbf{F})$ given by $\sigma \mapsto \sigma|_{\mathbf{E}}$ is a group homomorphism with kernel $\mathrm{Gal}(\mathbf{K}/\mathbf{E}) = N$. It can be showed that θ is surjective using the Fundamental Theorem of Galois theory and so the statement follows. □

Lemma 1.3.25. *We have $\bigcap_{N \in \mathcal{N}} N = \{id\}$. Furthermore, $\bigcap_{N \in \mathcal{N}} \sigma N = \{\sigma\}$ for all $\sigma \in G$.*

Proof. Let $\tau \in \bigcap_{N \in \mathcal{N}} N$ and let $a \in \mathbf{K}$. By Lemma 1.3.23, there is an $\mathbf{E} \in \mathcal{I}$ with $a \in \mathbf{E}$. Set $N = \mathrm{Gal}(\mathbf{K}/\mathbf{E}) \in \mathcal{N}$. The automorphism τ fixes $\mathbf{E}$ since $\tau \in N$, so $\tau(a) = a$. Thus, $\tau = id$, so $\bigcap_{N \in \mathcal{N}} N = \{id\}$. For the second statement, if $\tau \in \sigma N$ for all N, then $\sigma^{-1}\tau \in N$ for all N; thus $\sigma^{-1}\tau = id$ by the first part. This yelds $\tau = \sigma$, so $\bigcap_{N \in \mathcal{N}} \sigma N = \{\sigma\}$. □

Lemma 1.3.26. *Let $N_1, N_2 \in \mathcal{N}$, then $N_1 \cap N_2 \in \mathcal{N}$.*

Proof. Let $N_i = \mathrm{Gal}(\mathbf{K}/\mathbf{E}_i)$ with $\mathbf{E}_i \in \mathcal{I}$. Each $\mathbf{E}_i$ is finite Galois over $\mathbf{F}$, hence $\mathbf{E}_1\mathbf{E}_2$ is also finite Galois over $\mathbf{F}$, so $\mathbf{E}_1\mathbf{E}_2 \in \mathcal{I}$. However, it can be proved that $\mathrm{Gal}(\mathbf{K}/\mathbf{E}_1\mathbf{E}_2) = N_1 \cap N_2$, so it belongs to $\mathcal{N}$. □

We can now define a topology on the Galois group G.

Definition 1.3.27. *The* Krull topology *on G is defined as follows: a subset X of G is open if $x = \emptyset$ or if $X = \bigcup_i \sigma_i N_i$ for some $\sigma_i \in G$ and $N_i \in \mathcal{N}$.*

From the definition, it is clear that G and $\emptyset$ are open sets and that the union of open sets is open. To show that we do indeed have a topology on G, it remains to see that the intersection of two open sets is again open. It is sufficient to show that $\tau_1 N_1 \cap \tau_2 N_2$ is open for any $N_1, N_2 \in \mathcal{N}$. To see this, if $\sigma \in \tau_1 N_1 \cap \tau_2 N_2$, then

$$\tau_1 N_1 \cap \tau_2 N_2 = \sigma N_1 \cap \sigma N_2 = \sigma(N_1 \cap N_2)$$

and $\sigma(N_1 \cap N_2)$ is open, since $N_1 \cap N_2 \in \mathcal{N}$ by Lemma 1.3.26.

We point out some properties of the Krull topology. Since each nonempty open set of G is a union of cosets of subgroups of $\mathcal{N}$, the set

$$\{\sigma N : \sigma \in G\ ,\ N \in \mathcal{N}\}$$

is a basis for the Krull topology. If $N \in \mathcal{N}$, then $|G : N| < \infty$, so $G - \sigma N$ is a union of finitely many cosets of N. Therefore, σN is both open and closed. A set that is both open and closed is called *clopen*, the Krull topology thus has a basis of clopen sets. Moreover, if we set on G the Krull topology, then G becomes a topological group. One last remark is that Krull topology for finite extension coincide with discrete topology.

Theorem 1.3.28. *As a topological space G is Hausdorff, compact and totally disconnected.*

Proof. If X is a subset of G and $\sigma, \tau \in X$, let σN be an open neighborhood of σ not containing τ. The existence of N follows by Lemma 1.3.25. Then

$$X = (\sigma N \cap X) \cup ((G - \sigma N) \cap X)$$

an union of two disjoint, nonempty open sets in X, so X is not connected. Therefore, G is totally disconnected.

To show that G is Hausdorff, let $\sigma \in G$. Lemma 1.3.25 shows that $\{\sigma\} = \bigcap_N \sigma N$. If $\tau \neq \sigma$, then there is an $N \in \mathcal{N}$ with $\tau \notin \sigma N$. Each σN is an open neighborhood of σ but it is also closed, as noted above. Thus, σN and $G - \sigma N$ are disjoint open sets with $\sigma \in \sigma N$ and $\tau \in G - \sigma N$, so G is Hausdorff.

In proving that G is compact, we will show how G can be constructed from finite Galois groups. Let P be the direct product $\prod_{N \in \mathcal{N}} G/N$ of the finite groups G/N. We make P into a topological space by giving P the product topology. Note that each G/N is both Hausdorff and compact, and so P. There is a natural group homomorphism $f : G \to P$ defined by

$f(\sigma) = \{\sigma N\}$. We will show f is a homeomorphism from G to the image of f and that this image is a closed subset of P. So compactness will follow by compactness of $Im(f)$.

The kernel of f consists of those $\sigma \in G$ with $\{\sigma N\} = \{N\}$. Therefore, if $\sigma \in ker(f)$, then $\sigma \in \bigcap_{N \in \mathcal{N}} N = \{id\}$ by Lemma 1.3.25. Thus, f is injective. Let $\pi_N : P \to G/N$ be the projection onto the N-component. Then $\pi_N(f(\sigma)) = \sigma N$ for any $\sigma \in G$. The sigleton sets τN form a basis for the discrete topology on G/N, so by definition of the product topology, every open set in P is a union of a finite intersection of sets of the form $\pi_N^{-1}(\tau N)$ for various $\tau \in G$ and $N \in \mathcal{N}$. To show that f is continuous, it is enough to show that $f^{-1}(\pi_N^{-1}(\{\tau N\}))$ is open in G for any τN. But this preimage is just τN, which is open, so f is continuous. Futhermore, $f(\tau N) = \pi_N^{-1}(\{\tau N\}) \cap Im(f)$ is open in $Im(f)$, so f^{-1} is also continuous. Therefore, f is an homeomorphism from G to $Im(f)$. For Lemma 1.3.24, we can identify G/N with $\mathrm{Gal}(\mathbf{E}/\mathbf{F})$. This amounts to identifying the coset τN with $\tau|_{\mathbf{E}}$. With this identification, for $\rho \in P$ the element $\pi_N(\rho)$ is an automorphism of $\mathbf{E}$. Note that for $\tau \in G$, $\pi_N(f(\tau)) = \tau|_{\mathbf{E}}$. Let

$$C = \{\rho \in P : \text{ for each } N, M \in \mathcal{N}, \pi_N(\rho)|_{\mathbf{E}_N \cap \mathbf{E}_M} = \pi_M(\rho)|_{\mathbf{E}_N \cap \mathbf{E}_M}\}$$

We claim that $C = Im(f)$. Now, $Im(f) \subseteq C$ since $\pi_N(f(\tau))|_{\mathbf{E}_N} = \tau|_{\mathbf{E}_N}$ for any $\tau \in G$. For the reverse inclusion,let $\rho \in C$. We define $\tau : \mathbf{K} \to \mathbf{K}$ as follows. For $a \in \mathbf{K}$, pick any $\mathbf{E}_N \in \mathcal{I}$ with $a \in \mathbf{E}_N$, possible by Lemma 1.3.23, and define $\tau(a) = \pi_N(\rho)(a)$. This map is well-defined since $\rho \in C$. It is possible to prove that τ is a ring homomorphism and that $\tau \in G$ since τ fix $\mathbf{F}$. Now, as $\tau|_{\mathbf{E}} = \pi_N(\rho)$, we see that $f(\tau) = \rho$. Thus $C = Im(f)$. To show that C is closed in P, take any $\rho \in P$ with $\rho \notin C$. Then there are $N, M \in \mathcal{N}$ with $\pi_N(\rho)|_{\mathbf{E}_N \cap \mathbf{E}_M} \neq \pi_M(\rho)|_{\mathbf{E}_N \cap \mathbf{E}_M}$. Thus, $\pi_N^{-1}(\pi_N(\rho)) \cap \pi_M^{-1}(\pi_M(\rho))$ is an open subset of P containing ρ and disjoint from C. Therefore, $P - C$ is open, so $C = Im(f)$ is closed. □

The set $\mathcal{N}$, ordered by reverse inclusion, is a direct set: if $N_1, N_2 \in \mathcal{N}$, then there is an $N_3 \in \mathcal{N}$ with with $N_3 \subseteq N_1 \cap N_2$, namely $N_3 = N_1 \cap N_2 \in \mathcal{N}$. The set $\{G/N : N \in \mathcal{N}\}$ togheter with the natural projection maps $G/N_1 \to G/N_2$ for $N_1 \subseteq N_2$ form a direct system of groups. As seen in the previous proof, G can be viewed as an inverse limit of finite groups. G is then a profinite group.

Now we can state the Fundamental Theorem for Infinite Galois Theory, for a reference Knapp [13]:

Fundamental Theorem of Infinite Galois theory. *Let $\boldsymbol{K}/\boldsymbol{F}$ be an infinite Galois extension with $G = \mathrm{Gal}(\boldsymbol{K}/\boldsymbol{F})$. With the Krull topology on G, the maps $\boldsymbol{L} \mapsto \mathrm{Gal}(\boldsymbol{K}/\boldsymbol{L})$ and $H \to \boldsymbol{L}^H$ give an inclusion reversing correspondence between the fields $\boldsymbol{L}$ with $\boldsymbol{F} \subseteq \boldsymbol{L} \subseteq \boldsymbol{K}$ and the closed subgroups*

H of G. Futhermore, if $\boldsymbol{L}$ corresponds to H, then $|G : H| < \infty$ if and only if $[\boldsymbol{L} : \boldsymbol{F}] < \infty$, if and only if H is open. When this occurs, $|G : H| = [\boldsymbol{L} : \boldsymbol{F}]$. Also, H is normal in G if and only if $\boldsymbol{L}$ is Galois over $\boldsymbol{F}$, and when this occurs, there is a group isomorphism $\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{F}) \cong G/N$. If G/N is given the quotient topology, this isomorphism is also a homeomorphism.

For an infinite Galois group, we can define the decomposition group and the inertia as limit of decomposition and inertia of finite Galois groups.
Let us consider the Galois group $\mathrm{Gal}(\mathbf{K}/\mathbf{F})$, for an infinite Galois extension $\mathbf{K}/\mathbf{F}$, fix a prime $p \in \mathbf{F}$ and $\mathfrak{p} \in \mathbf{K}$ such that $\mathfrak{p} \mid p$. Locally at $\mathfrak{p} \in \mathbf{K}$ we want to define the decomposition group $D_{\mathfrak{p}}$. Let $\mathbf{L}$ be a finite Galois extension of $\mathbf{F}$ and let w be a prime of $\mathbf{L}$ lying over p. Then the decomposition group at w is defined to be $D_w = \{\sigma \in \mathrm{Gal}(\mathbf{L}/\mathbf{F}) : \sigma w = w\}$. Let

$$D_{\mathfrak{p}} = \varprojlim_{w|p} D_w$$

For each $w \mid p$ let the inertia group I_w be the kernel of the map from D_w into $\mathrm{Gal}(\mathcal{O}_{\mathbf{L}}/w, \mathcal{O}_{\mathbf{F}}/p)$. Let

$$I_p = \varprojlim_{w|p} I_w$$

In the same way as before we can define the Frobenius element at $\mathfrak{p}$: it is the unique element $\sigma \in \mathrm{Gal}(\mathbf{K}/\mathbf{F})$ satisfying the following two conditions:

(a) $\sigma \in D_{\mathfrak{p}}$, i.e. $\sigma(\mathfrak{p}) = \mathfrak{p}$;

(b) for all $\alpha \in \mathcal{O}_{\mathbf{K}}$, $\sigma\alpha \equiv \alpha^q \mod \mathfrak{p}$, where q is the number of elements the residue field $\mathcal{O}_{\mathbf{F}}/\mathfrak{p}$, $\mathfrak{p} \mid p$.

This really does depend on the choice of $\mathfrak{p}$: given another choice $\mathfrak{p}'|p$, there is an element $\tau \in \mathrm{Gal}(\mathbf{K}/\mathbf{F})$ such that $\tau(\mathfrak{p}) = \mathfrak{p}'$, and we then see that $\mathrm{Frob}_{\mathfrak{p}'} = \tau\,\mathrm{Frob}_{\mathfrak{p}}\,\tau^{-1}$. In this case, we must treat not just the elements themselves but the entire conjugacy class.
We define the *Frobenius symbol* of $p \in \mathbf{F}$ in $\mathbf{K}/\mathbf{F}$ to be the conjugacy class

$$\{\mathrm{Frob}_{\mathfrak{p}} : \mathfrak{p}\,|p\}$$

Note that in the case of an abelian group, this set contains only a single element. We will often abuse notation and denote by $\mathrm{Frob}_{\mathfrak{p}}$ any element of the conjugacy class and then treat it as something well-defined only up to conjugacy. The Frobenius element has several good properties: for example, it is compatible with subfields restriction, and it has a good behavior with extensions.

1.4 Galois representations

Definition 1.4.1. *Let X and Y be topological spaces, and let* $\mathrm{Hom}(X,Y)$ *be the set of continuous maps from X to Y. Given a compact subspace K of X and an open set U in Y, let*

$$U_{K,U} := \{f \in \mathrm{Hom}(X,Y) : \ f(x) \in U \ \text{ whenever } x \in K\}$$

Define the compact-open topology *on* $\mathrm{Hom}(X,Y)$ *to be the topology generated by the sub-basis*

$$\{U_{K,U}\} : \ K \subset X \text{ compact}, \quad U \subset Y \text{ open}$$

Definition 1.4.2. *Let A be an Hausdorff Abelian topological group. Then an* A-valued Galois representation *for $\boldsymbol{K}$ is a continuous homomorphism*

$$\rho : G_{\boldsymbol{K}} \to \mathrm{Aut}(A)$$

where we endow $G_{\boldsymbol{K}} = \mathrm{Gal}(\overline{\boldsymbol{K}}/\boldsymbol{K})$ with the Krull topology, and where $\mathrm{Aut}(A)$ *is the group of continuous automorphisms of A, endowed with the compact-open topology. A is called the* representation space *for ρ.*

If $A \cong \mathbb{C}^n$ is a complex vector space, if $A \cong \mathbb{Q}_\ell^{\,d}$ is an ℓ-adic vector space, or if $A \cong \mathbb{F}_\ell^d$ is a vector space over a finite field, we call ρ a complex, ℓ-adic, or residual Galois representation, respectively.

The simplest case is where $A = \mathbb{C}^n$, the group of $n \times 1$ column vectors with complex entries. Then $\mathrm{Aut}(\mathbb{C}^n) = GL_n(\mathbb{C})$, and we have what is called a complex representation of degree n. In the same manner, letting $A = \mathbf{F}^n$, with $\mathbf{F}$ any field (such as $\mathbb{R}$ or a finite field $\mathbb{F}_p$) we obtain a degree n representation over $\mathbf{F}$.

In the general case we can define $\mathbb{Z}[G_{\mathbf{K}}]$ for the group ring of $G_{\mathbf{K}}$ with coefficients in $\mathbb{Z}$. Then a Galois representation for $\mathbf{K}$ is simply a continuous $\mathbb{Z}[G_{\mathbf{K}}]$ -module A (i.e. the action of $G_{\mathbf{K}}$ on A is given by a continuous homomorphism ρ). In other words, all the information in a representation ρ is preserved in considering the representation space A as a continuous $\mathbb{Z}[G_{\mathbf{K}}]$ -module.
Fix a field $\mathbf{K}$, and consider the set of formal sums

$$\mathbf{K}\,[G_{\mathbb{Q}}] = \left\{ \sum_\tau a_\tau \tau \,|\, a_\tau \in \mathbf{K} \ \text{ and } \ a_\tau = 0 \ \text{ for almost all } \ \tau \in G_{\mathbb{Q}} \right\}$$

This is the group ring of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbf{K}$, it is a non-commutative ring with zero divisors, but if we regard each $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as a vector, then

$\mathbf{K}\ \left[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right]$is an infinite dimensional vector space over $\mathbf{K}$. We can construct a map $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to End(\mathbf{K}\ \left[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\right])$ sending $\sigma \mapsto \rho(\sigma)$ where

$$\rho(\sigma) \circ (\sum_{\tau} a_\tau \tau) = \sum_{\tau} a_\tau \sigma\tau$$

In other words, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has an action on the group ring via left multiplication.

Suppose G is a group, $\rho : G \to \mathrm{Aut}(A)$ is a representation and $H \subseteq G$ a subgroup. Then we let

$$A^H = \{a \in A \mid \rho(h)a = a, \text{ for all } h \in H\}$$

the subgroup of A fixed pointwise by H. Given a Galois representation ρ, let $G_0 = ker\rho$. By the fundamental theorem of Galois theory, since G_0 is a closed normal subgroup of $G_{\mathbf{K}}$, it corresponds to a certain normal subfield of $\overline{\mathbf{K}}$. Naturally, this is the fixed field of G_0, and we denote it by $\mathbf{K}(\rho)$. Notice that since ρ is trivial on $G_0 = \mathrm{Gal}(\overline{\mathbf{K}}/\mathbf{K}(\rho))$, it factors through a representation

$$\tilde{\rho} : \mathrm{Gal}(\mathbf{K}(\rho)/\mathbf{K}) \to \mathrm{Aut}(A),$$

which is faithful. This property characterizes $\mathbf{K}(\rho)$.

For a first application of definition, we say that ρ is discrete if for all $a \in A$, the stabilizer of a in $G_{\mathbf{K}}$ is open in $G_{\mathbf{K}}$. This is the case when A is given the discrete topology. When A is finite and Hausdorff, the stabilizer of any $a \in A$ fixes a finite extension of $\mathbf{K}$, which we denote by $\mathbf{K}(a)$. One has that $\mathbf{K}(\rho)$ is the field generated by the union of all the $\mathbf{K}(a)$.

As a second application, suppose that the image $\rho(G_{\mathbf{K}})$ is Abelian. Then the quotient $G_{\mathbf{K}}/G_0$ is Abelian, so G_0 contains the commutator subgroup of $G_{\mathbf{K}}$, which means that $\mathbf{K}(\rho)$ is contained in $\mathbf{K}^{ab}$, the maximal Abelian extension of $\mathbf{K}$. This is the case when ρ is a character, i.e. a 1-dimensional representation over some commutative ring with unit,

$$\rho : G_{\mathbf{K}} \to GL_1(A) = A^*.$$

Associated to any field $\mathbf{K}$ are two basic Galois representations, namely those with representation spaces $A = \mathbf{L}$ and $A = \mathbf{L}^*$, for any normal intermediate field $\mathbf{K} \subseteq \mathbf{L} \subseteq \overline{\mathbf{K}}$, with the usual action of the Galois group on them and where on A is consideredthe discrete topology or an appropriate one. Both of these representations are discrete.
The additive representation is rather simple if $\mathbf{L}/\mathbf{K}$ is finite: by the normal basis theorem, it is merely a permutation representation on the normal basis. Also, if $\mathbf{L} = \overline{\mathbf{K}}$ and $x \in \overline{\mathbf{K}}$, then $\mathbf{K}(x)$, the field obtained by

adjoining x to $\mathbf{K}$, agrees with the fixed field of the stabilizer of x in $G_{\mathbf{K}}$. This motivates the notation $\mathbf{K}(a)$ introduced above.
By contrast, in general, $\mathbf{L}^*$ can become a rather complicated object. To look at just a piece of the representation $\mathbf{L}^*$, assume that $\mathbf{L}$ contains the group μ_m of m-th roots of unity, where m is prime to the characteristic of $\mathbf{K}$. Then we let $A = \mu_m$.

It is possible to choose an isomorphism of Abelian groups $\mu_m \cong \mathbb{Z}/m\mathbb{Z}$, and it follows that our representation is

$$\rho : G_{\mathbf{K}} \to (\mathbb{Z}/m\mathbb{Z})^*.$$

Now assume that m has the form p^n, where p is a prime not equal to the characteristic, and set $A_n = \mu_{p^n}$.
This gives a sequence of representations $\rho_n : G_{\mathbf{K}} \to (\mathbb{Z}/p^n)^*$, which are compatible with the natural maps $(\mathbb{Z}/p^{n+1}\mathbb{Z})^* \to (\mathbb{Z}/p^n\mathbb{Z})^*$. This compatibility allows us to glue them together into a representation called the p-adic cyclotomic representation of $\mathbf{K}$.

1.4.1 Complex Representations

Regular Representations

Consider a complex representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_d(\mathbb{C})$ with finite image. Let $\mathbf{F} = \overline{\mathbb{Q}}^{ker\rho}$, then we can write a faithful map $\rho : \mathrm{Gal}(\mathbf{F}/\mathbb{Q}) \to GL_d(\mathbb{C})$ where $\mathbf{F}/\mathbb{Q}$ is a finite Galois extension.
Fix an irreducible polynomial $q(x) \in \mathbb{Q}[x]$ of degree d having roots $\{x_k\}$, $k = 1, \ldots, d$, and set $\mathbf{L} = \mathbb{Q}(x_1, x_2, \ldots, x_d)$ as its splitting field. The group of permutations of the roots $\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ has a canonical representation as $d \times d$-matrices: write the d roots as d-dimensional unit vectors, such as

$$x_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad x_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} \quad \cdots \quad x_d = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$$

Any permutation $\tau \in \mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ on these roots may be represented as a $d \times d$-matrix $\rho(\sigma)$ with entries 0 or 1. It can be easily checked that ρ is a multiplicative map $\rho(\sigma_1 \sigma_2) = \rho(\sigma_1)\rho(\sigma_2)$.
This map is known as the regular representation of $\mathrm{Gal}(\mathbf{L}/\mathbb{Q})$ and the matrices $\rho(\sigma)$ are usually called permutation matrices.

As an explicit example, consider $q(x) = a\,x^2 + b\,x + c$. Then $\mathbf{L} = \mathbb{Q}\,(\sqrt{b^2 - 4\,a\,c})$, and the only permutation of interest is

$$\sigma : \frac{-b + \sqrt{b^2 - 4\,a\,c}}{2a} \mapsto \frac{-b - \sqrt{b^2 - 4\,a\,c}}{2a}$$

so

$$\rho(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Using group rings we can consider $V = \mathbb{C}\,[\mathrm{Gal}(\mathbf{L}\,/\mathbb{Q}\,)] = \mathbb{C} \oplus \mathbb{C}\,\sigma$ as a complex vector space of dimension 2. If we consider the idempotent elements

$$e_1 = \frac{1 + \sigma}{2} \quad e_2 = \frac{1 - \sigma}{2}$$

we can define subspaces $V_i = \mathbb{C}\,[\mathrm{Gal}(\mathbf{L}\,/\mathbb{Q}\,)]\,e_i$ for $i = 1, 2$, these subspaces are 1-dimensional:

$$\mathbb{C}\,[\mathrm{Gal}(\mathbf{L}\,/\mathbb{Q}\,)]\,e_i = \{(a + b\sigma)\frac{1 \pm \sigma}{2} | a, b \in \mathbb{C}\,\} = \{(a \pm b)\frac{1 \pm \sigma}{2} | a, b \in \mathbb{C}\,\} \cong \mathbb{C}$$

Clearly $V = V_1 \oplus V_2$, and we have $\sigma\,e_1 = e_1$ and $\sigma\,e_2 = -e_2$. Hence V_1 corresponds to the trivial representation while V_2 corresponds to the alternating representation.

As another example, consider an irreducible cubic polynomial $q(x)$ with roots x_1, x_2 and x_3, of Galois type S_3. The Galois group of the field $\mathbf{L} = \mathbb{Q}\,(x_1, x_2, x_3)$ is generated by two automorphisms:

$$\sigma_2 = (12), \sigma_3 = (123)$$

$$\rho(\sigma_2) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \rho(\sigma_3) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

The vector space $V = \mathbb{C}\,[\mathrm{Gal}(\mathbf{L}\,/\mathbb{Q}\,)]$ has dimension 6, so consider the following idempotents:

$$e_1 = \frac{[1] + [\sigma_2] + [\sigma_3]}{6}, \quad e_2 = \frac{[1] - [\sigma_2] + [\sigma_3]}{6}, \quad e_3 = \frac{2[1] - [\sigma_3]}{3}$$

where $[1] = 1$, $[\sigma_2] = \sigma_2 + \sigma_2\sigma_3 + \sigma_3\sigma_2$ and $[\sigma_3] = \sigma_3 + \sigma_3^{-1}$.
One checks that $e_1 + e_2 + e_3 = 1$, $e_i^2 = e_i$ while $e_i\,e_j = 0$ for $i \neq j$. Consider the subspaces $V_i = \mathbb{C}\,[\mathrm{Gal}(\mathbf{L}\,/\mathbb{Q}\,)]\,e_i$ for $i = 1, 2, 3$, since

$$\sigma_2\,e_1 = \sigma_3\,e_1 = e_1, \quad \sigma_2\,e_2 = -e_2, \quad \sigma_3\,e_2 = e_2$$

we have that V_1 and V_2 are 1-dimensional subspaces of V, it can be shown that V_1 corresponds to the trivial representation, V_2 corresponds to the alternating representation. V_3 corresponds to the irreducible 2-dimensional representation of the symmetric group of three elements. It is possible to prove that $V = V_1 \oplus V_2 \oplus V_3^2$.

Dirichlet Characters

We want to define a 1-dimensional complex Galois representation using a Dirichlet character. Fix a positive integer N, and consider a group homomorphism

$$\chi : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$$

this is a Dirichler character modulo N. On the other hand we have the Artin map that is an isomorphism:

$$\begin{aligned} \phi_{\mathbb{Q}(\zeta_N)/\mathbb{Q}} : (\mathbb{Z}/N\mathbb{Z})^* &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \\ a &\mapsto \{\sigma_a : \zeta_N \mapsto \zeta_N^a\} \end{aligned}$$

Hence the composition gives a Galois representation:

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \overset{\phi^{-1}_{\mathbb{Q}(\zeta_N)/\mathbb{Q}}}{\longrightarrow} (\mathbb{Z}/N\mathbb{Z})^* \xrightarrow{\chi} \mathbb{C}^*$$

One can create also a d-dimensional representation by placing d Dirichlet characters along the diagonal. One checks that when $p \nmid N$ is a prime then $\rho(\mathrm{Frob}_{\mathfrak{p}}) = \chi(p)$. In this case $\mathbf{L}$, the field fixed by $\ker(\rho)$ is such that $\mathbf{L} \subseteq \mathbb{Q}(\zeta_N)$, in particular, if χ is a quadratic character then $\mathbf{L}$ is a quadratic field. Note that $\mathbf{L}/\mathbb{Q}$ is always finite.

1.4.2 ℓ-adic Representations

Cyclotomic Characters

Fix a prime ℓ, and say $N = \ell^n$ is a prime power. We have a series of isomorphisms

$$(\mathbb{Z}/\ell^n\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^n})/\mathbb{Q})$$

coming from the Artin map so this gives an isomorphism

$$\phi_{\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}} : \mathbb{Z}_\ell^* \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/\ell^n\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q})$$

where $\mathbb{Q}(\zeta_{\ell^\infty}) = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_{\ell^n})$. The inverse of this map is known as the ℓ-adic cyclotomic character:

$$\epsilon_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}) \overset{\phi^{-1}_{\mathbb{Q}(\zeta_{\ell^\infty})/\mathbb{Q}}}{\longrightarrow} \mathbb{Z}_\ell^* \to \mathbb{Q}_\ell^*$$

As before, one can create a d-dimensional representation by placing d cyclotomic characters, or their powers, along the diagonal. One checks that when $p \neq \ell$ is a prime then the Frobenius automorphism maps to p:

$$\epsilon(\mathrm{Frob}_{\mathfrak{p}}) = p$$

In this case the field cut out by ρ is $\mathbf{L} = \mathbb{Q}(\zeta_{\ell^\infty})$; note that $\mathbf{L}/\mathbb{Q}$ is not finite.

1.5 Čebotarev Density Theorem

Before giving the proof of the Čebotarev Density Theorem, some preliminaries from Class Field Theory are necessary.

Definition 1.5.1. *A* valuation *on* $\boldsymbol{K}$ *is a map* $|\cdot| : \boldsymbol{K} \to \mathbb{R}$ *such that for all* $a, b \in \boldsymbol{K}$*, we have:*

- $|a| \geq 0$ *and* $|a| = 0$ *if and only if* $a = 0$*;*
- $|a| \cdot |b| = |ab|$*;*
- $|a + b| \leq |a| + |b|$*;*

If the stronger condition $|a + b| \leq max\{|a|, |b|\}$ *holds, then* $|\cdot|$ *is called a* non-archimedean valuation*.*

Let us give some examples. On any field $\mathbf{K}$, the trivial valuation is the one given by

$$|a| = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \end{cases}$$

Suppose $\sigma : \mathbf{K} \hookrightarrow \mathbb{C}$ and let $|a| = |\sigma(a)|$ where $|\sigma(a)|$ is the usual absolute value on $\mathbb{C}$. Let p be a prime number, the the p-adic valuation $|\cdot|_p$ is defined to be

$$|a|_p = p^{-ord_p(a)} \quad \text{where} \quad ord_{p_j}(a) = n_j \text{ if } a = \prod_{p_i \text{ primes}} p_i^{n_i}$$

Definition 1.5.2. *In a number field* $\boldsymbol{K}$*, we define a* prime *of* $\boldsymbol{K}$ *to be an equivalence class of nontrivial valuations of* $\boldsymbol{K}$*. There are two types of primes: the* finite primes*, which can be identified with the prime ideals of* $\mathcal{O}_{\boldsymbol{K}}$*, and the infinite primes. A* real infinite prime *can be identified with an embedding of* $\boldsymbol{K}$ *into* $\mathbb{R}$*, and a* complex infinite prime *can be identified with a conjugate pair of embeddings of* $\boldsymbol{K}$ *into* $\mathbb{C}$*.*

Definition 1.5.3. *Let* $\boldsymbol{K}$ *be a number field with ring of integers* $\mathcal{O}_{\boldsymbol{K}}$*, and* $\mathfrak{p}$ *a nonzero ideal of* $\mathcal{O}_{\boldsymbol{K}}$*. Then the norm of* $\mathfrak{p}$ *is defined to be*

$$\text{Norm}(\mathfrak{p}) = [\mathcal{O}_{\boldsymbol{K}} : \mathfrak{p}] = |O_{\boldsymbol{K}}/\mathfrak{p}|$$

By convention, the norm of the zero ideal is taken to be zero.

Finally, we can introduce the notion of Dirichlet density.

Definition 1.5.4. *Let* $\mathcal{P}_{\boldsymbol{K}}$ *the set of all finite primes of* $\boldsymbol{K}$*. Given a subset* $S \subset \mathcal{P}_{\boldsymbol{K}}$*, the Dirichlet density of* S *is the limit*

$$\delta(S) = lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} \frac{1}{\text{Norm}(\mathfrak{p})^s}}{\log \frac{1}{s-1}}$$

Čebotarev Density Theorem. *Let $\boldsymbol{L}/\boldsymbol{K}$ be a finite Galois extension of number fields, and denote* $\mathrm{Gal}(\boldsymbol{L}/\boldsymbol{K})$ *by G. For each subset $C \subset G$ that is stable under conjugation, let S denote the set of places v of $\boldsymbol{K}$ that are unramified in $\boldsymbol{L}$, such that, for $w \mid v$, the Frobenius symbol* Frob_w *is C. Then S has Dirichlet density equal to*

$$\delta(S) = \frac{|C|}{|G|}$$

Proof. For a proof of this result, look at Milne [21], Chapter V and Chapter VII. □

Corollary 1.5.5. *Let $\boldsymbol{L}$ be a Galois number field. Then every element of* $\mathrm{Gal}(\boldsymbol{L}/\mathbb{Q})$ *takes the form $Frob_{\mathfrak{p}}$ for infinitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_{\boldsymbol{L}}$.*

Proof. For a proof of this result, Milne [21], Chapter VII. □

1.6 Dickson Classification Theorem

Definition 1.6.1. *A module over a ring with unity is said to be* semi-simple *if it is a direct sum of simple submodules, where simple means that each submodules does not admit non-zero proper submodules.*

Definition 1.6.2. *Let $\boldsymbol{F}$ be a field, $\overline{\boldsymbol{F}}$ its algebraic closure and V a 2-dimensional vector space on $\boldsymbol{F}$. Let H be a subgroup of $GL_2(\boldsymbol{F})$, then H is said to be a* semi-simple subgroup *if each $\alpha \in H$ is such that $\overline{V} = V \otimes_{\boldsymbol{F}} \overline{\boldsymbol{F}} = \overline{\boldsymbol{F}}^2$ is semi-simple over $\overline{F}[\alpha]$.*

Let $\mathbf{F}$ be a field and consider a 2-dimensional vector space V on $\mathbf{F}$. Let us consider D_1 and D_2 subspaces of V such that $V = D_1 \oplus D_2$, then we can define a split Cartan subgroup for V with respect to the decomposition chosen:

Definition 1.6.3. *$C \subset GL(V)$ is said to be a* split Cartan subgroup for *$GL(V)$ with respect to the decomposition $\{D_1, D_2\}$ if:*

$$C = \{s \in GL(V) \mid sD_i = D_i \text{ for } i = 1, 2\}$$

If we fix a normalized basis for V, $\mathcal{B}_V = \{d_1, d_2;\ d_i \in D_i \text{ for } i = 1, 2\}$ then every element of C can be represented as a matrix of the form $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$. C is clearly a commutative subgroup of $GL(V)$. C admits two proper subgroups, the ones given by the elements which act only on one subspace:

Definition 1.6.4. *$C_i \subset C$, $C \subset GL(V)$ which is a split Cartan subgroup for $GL(V)$ with respect to $\{D_1, D_2\}$, is said to be a* split semi-Cartan subgroup for *V with respect to $\{D_1, D_2\}$ if:*

$$C_i = \{t \in C \mid tD_i = D_i\} \text{ for } i = 1, 2$$

Again, fixed a basis on V with respect to $\{D_1, D_2\}$, as done before, the elements of the subgroups C_1 and C_2 can be represented by $\begin{pmatrix} 1 & 0 \\ 0 & * \end{pmatrix}, \begin{pmatrix} * & 0 \\ 0 & 1 \end{pmatrix}$ rispectively.
A split Cartan subgroup can be seen as the extension of a split semi-Cartan subgroup with homotheties:

$$C \cong C_i \cdot \mathbf{F}^*$$

so the image of a split Cartan subgroup in $PGL(V) = GL(V)/\mathbf{F}^*$ is the same as the image of a split semi-Cartan subgroup. If $\mathbf{F}$ is a finite field of characteristic p, $p \neq 2$, it is a cyclic group of order $p^n - 1$ and it is called the *split Cartan subgroup of* $PGL(V)$.

Proposition 1.6.5. *For a field $\boldsymbol{F}$, every maximal commutative semi-simple subgroup of $GL_2(\boldsymbol{F})$ is a split Cartan subgroup and conversely.*

Proof. The fact that C is commutative and semi-simple follows directly by definition. It is maximal semi-simple commutative because if $\alpha \in GL_2(\mathbf{F})$ commutes with all elements of C then by computation α lies in C.
Suppose that H is a maximal commutative semi-simple subgroup of $GL_2(\mathbf{F})$. If H is diagonalizable over $\mathbf{F}$, then H is contained in a split Cartan.
On the other hand, suppose H is not diagonalizable over $\mathbf{F}$. It is diagonalizable over the sepable closure of $\mathbf{F}$, $\mathbf{F}^{sep}$, and the two eighenspaces of dimension one give rise to two characters

$$\psi,\ \psi' : H \to \mathbf{F}^{sep}$$

of H in the multiplicative group of the separable closure. For each element $\alpha \in H$ the values $\psi(\alpha), \psi'(\alpha)$ are the eigenvalues of α, and for some element $\alpha \in H$ these eigenvalues are distinct, otherwise H is diagonalizable over $\mathbf{F}$. Hence the pair of elements $\psi(\alpha), \psi'(\alpha)$ are conjugate over $\mathbf{F}$ because H is semi-simple so α as to be too by definition. The image $\psi(H)$ is cyclic and if $\psi(\alpha)$ generates this image then we see that $\psi(\alpha)$ generate a quadratic extension $\mathbf{K}$ of $\mathbf{F}$. The map $\alpha \mapsto \psi(\alpha)$, $\alpha \in H$, extends to a $\mathbf{F}$-linear mapping also denoted by ψ, of the algebra $\mathbf{F}[H]$ into $\mathbf{K}$. Since $\mathbf{F}[H]$ is semi-simple, it follows that

$$\psi : \mathbf{F}[H] \xrightarrow{\cong} \mathbf{K}$$

is an isomorphism. Hence ψ maps H into $\mathbf{K}^*$, and in fact maps H onto $\mathbf{K}^*$ because H was taken to be maximal. □

In the previous proof, the two characters $\psi,\ \psi'$ are called the *characters of the Cartan subgroup*. In the split case, if α has diagonal elements a, d then we get two characters $\psi,\ \psi'$ such that:

$$\psi(\alpha) = a, \quad \psi'(\alpha) = d$$

so the values of the characters are in $\mathbf{F}$.

It is possible define also the non-split Cartan subgroup of $GL(V)$:

Definition 1.6.6. *A subgroup of $GL(V)$ (rispectively $PGL(V)$) is called* non-split Cartan subgroup *if exists k a proper subalgebra of $End(V)$ such that it is a field with p^2 elements, k^* is a subgroup of $GL(V)$ of p^2-1 elements and its image in $PGL(V)$ it is cyclic of order $p+1$.*

In this case it is possible to prove that the characters of the Cartan subgroup are conjugate quadratic over $\mathbf{F}$.
It is possible give a characterisation of being element of a Cartan subgroup for $s \in GL(V)$, if $p \neq 2$:

Proposition 1.6.7. *Let $\boldsymbol{F}$ be a finite field of characteristic p and V a 2-dimensional vector space over $\boldsymbol{F}$. If $p \neq 2$, and if $s \in GL(V)$ is such that $\mathrm{Tr}(s)^2 - 4\det(s) \neq 0$ then s belongs to a unique Cartan subgroup of $GL(V)$, and if $\mathrm{Tr}(s)^2 - 4\det(s) \neq 0$ is a square in $\boldsymbol{F}$ the s belongs to a split Cartan.*

Proof. Look at [32], pg 279 or [17] or simply by direct computation applying $s \in GL(V)$ to a generic element of V and imposing that it belongs to a Cartan subgroup. □

Theorem 1.6.8. *Let C be a Cartan subgroup of $GL_2(\boldsymbol{F})$ and N its normalizer, then C is of index 2 in N.*

Proof. An element of the normalizer of a Cartan subgroup must either fix or interchange the subspaces $\{D_1, D_2\}$. If it fixes them, then it lies in C by the maximality of C. If it interchanges them, then it does not lie in C and generates a unique coset of N/C, so that C is of index 2 in N. □

Now let us consider the image N^1 and C^1 of N and C in $PGL(V)$, by the canonical projection $\pi : GL(V) \to PGL(V)$, we have that N^1 is the normalizer of C^1 in $PGL(V)$ in particular by the previous description it has to be a dihedral group given by the semi-direct product of a group $\{1, \sigma\}$ of order 2 and the cyclic group C^1, such that $\sigma\, x\, \sigma = x^{-1}$ for all $x \in C^1$ and each element of $N^1 \setminus C^1$ is of order 2:

$$\pi(N) = N^1 = \{1, \sigma\} \ltimes C^1 = \{1, \sigma\} \ltimes \pi(C)$$

As before let $\mathbf{F}$ be a field and V a 2-dimensional vector space over $\mathbf{F}$. Let D be a 1-dimensional subspace of V, then we can define the Borel subgroup of $GL(V)$:

Definition 1.6.9. *$B \subset GL(V)$ is said to be a* Borel subgroup of $GL(V)$ *with stable subspace $D \subset V$ if:*

$$B = \{s \in GL(V) \,|\, sD = D\}$$

The elements of a Borel subgroup can be represented by a matrix of type $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. If a Cartan subgroup or a split semi-Cartan subgroup is contained in a Borel subgroup, then it is split.

Proposition 1.6.10. *If $\boldsymbol{F}$ is a filed of characteristic p, then an element of finite order in $GL_2(\boldsymbol{F})$ is semi-simple if and only if its order is prime to p.*

Proof. Let $\alpha \in GL_2(\mathbf{F})$, so it has to have finite order. Its Jordan normal form over the algebraic closure is of type

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$$

where a, d lie in the finite field $\mathbf{F}$, and $a, d \neq 0$. Being semi-simple for α means being diagonalizable over the algebraic closure, and so $(ord(a), p) = 1$. Hence the first case is excluded since the element has order p but it is not semisimple while in the second case the element is semisimple and of oder prime to p since $(ord(a), p) = 1$, $(ord(d), p) = 1$. □

Theorem 1.6.11. *Let G be a subgroup of $GL_2(\boldsymbol{F})$ and $p = char(\boldsymbol{F})$. If the order of G is divisible by p, then either G is contained in a Borel subgroup of $GL_2(\boldsymbol{F})$, or G contains $SL_2(\boldsymbol{F})$.*

Proof. Let α be an element of order p, then the Jordan normal form of α is $\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$. Consequently α has a one-dimensional eigensubspace W of V. If every element of G has W as eigenspace, then G is contained in the associated Borel subgroup. If not, let $\sigma \in G$ map W into another 1-dimensional subspace W', so that $V = W \oplus W'$. Using basis elements of W, W' as a basis for V, we see that α and $\sigma\alpha\sigma^{-1}$ can be represented by the matrices

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix}$$

These generate $SL_2(\mathbf{F})$ and so the theorem follows. □

Lemma 1.6.12. *Let G be a subgroup of $GL_2(\boldsymbol{F})$, where $\boldsymbol{F}$ is a field of characteristic p. Suppose that the order of G is prime to p. If two elements of G have one eigenvector in common, then they have both eigenvectors in common.*

Proof. The two elements can be simultaneously triangularized. Their commutator is then an element with 1 on the diagonal, and must therefore be the identity, otherwise it would have period p. □

Proposition 1.6.13. *Let G be a finite subgroup of $GL_2(\boldsymbol{F})$, of order prime to p. If G is contained in a Cartan subgroup, then $\pi(G)$ is cyclic.*

Proof. Let ψ, ψ' be the two character of the Cartan subgroup, split or non-slpit, so we have that $\alpha \mapsto (\psi(\alpha),\ \psi'(\alpha))$ is an injection of G in $\mathbf{K}^* \times \mathbf{K}^*$, where $\mathbf{K} = \mathbf{F}$ or $\mathbf{K}$ is quadratic over $\mathbf{F}$. Let D be the diagonal in $\mathbf{K}^* \times \mathbf{K}^*$, consider the composite homomorphism

$$G \to \mathbf{K}^* \times \mathbf{K}^* \to (\mathbf{K}^* \times \mathbf{K}^*)/D \sim \mathbf{K}^*$$

Its kernel is precisely the group of scalar matrices in G, so $\pi(G)$ is embedded in $\mathbf{K}^*$, and every finite subgroup of $\mathbf{K}^*$ is cyclic. □

Proposition 1.6.14. *Let G be a finite subgroup of $GL_2(\boldsymbol{F})$, of order prime to p. If G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup, then $\pi(G)$ is dihedral.*

Proof. See [17] chapter IX. □

Dickson Theorem. *Let $\boldsymbol{F}$ be a field and let G be a finite subgroup of $GL_2(\boldsymbol{F})$, of order prime to the characteristic of the field. Let H be the image of G in $PGL_2(\boldsymbol{F})$. Then we have the following cases:*

- *H is cyclic and G is contained in a Cartan subgroup;*
- *H is dihedral, and G is contained in the normalizer of a Cartan subgroup but not in the Cartan subgroup itself;*
- *H is isomorphic to A_4, S_4 or A_5.*

Proof. The set of eigenspaces of non-trivial elements of H is finite and stable under H. Let $E_1, \ldots, E_r$ be representatives of the orbits under H. Let h be the order of H, and let h_i be the order of the isotropy subgroup of E_i in H. Then the orbit of E_i has h/h_i elements. Counting the number of pairs (α, E) consisting of an element $\alpha \in H$, $\alpha \neq 1$ and an eigenspace E for α, we find the relation:

$$2h - 2 = \frac{h}{h_1}(h_1 - 1) + \cdots + \frac{h}{h_r}(h_r - 1)$$

We shall determine all solutions of this equation with positive integers h, h_i dividing h. The relation can be re-written in the following way:

$$2(1 - \frac{1}{h}) = 1 - \frac{1}{h_1} + \cdots + 1 - \frac{1}{h_r}$$

Lemma 1.6.15. *The only solutions to the above equation are:*

1. $r = 2;\ h_1 = h_2 = h$;
2. $r = 3; h$ *even* $\ h_1 = h_2 = 2\ h_3 = \frac{h}{2}$
3. $r = 3; h = 12\ \ h_1 = 2\, h_2 = 3\, h_3 = 3$

4. $r = 3; h = 24 \;\; h_1 = 2\, h_2 = 3\, h_3 = 4$

5. $r = 3; h = 60 \;\; h_1 = 2\, h_2 = 3\, h_3 = 5$

Proof. Suppose some of the $h_i = h$, then it's immediate that we are in the first case. We suppose from now on that $h_i < h$ for all i. We must have $r > 2$ because

$$1 - \frac{1}{h} > 1 - \frac{1}{h_i}$$

We cannot have $r \geq 4$ because otherwise on the righ-side there would be at least four terms, each of which is at least $\frac{1}{2}$, while the left side is < 2. Therefore $r = 3$ from now on.
Not all $h_i \geq 3$, otherwise the right-side is greater than 2, that is impossibile. Hence some $h_i = 2$ and in particular h is even. Let's suppose $h_1 \leq h_2 \leq h_3$. If $h_3 = \frac{h}{2}$ we obtain the second case, from now on $h_3 < \frac{h}{2}$. We have $h_1 = 2$, we cannot have $h_2 = 2$ because in that case $h_3 = \frac{h}{2}$ and we are supposing $h_3 < \frac{h}{2}$. On the other hand, we cannot have $h_2 \geq 4$, otherwise the sum is > 2. So we can assume $h_2 = 3$. If $h_3 \geq 6$ we have again that the right-side is > 2 that is impossible, therefore we must have $h_3 = 3, 4$ or 5. □

We shall now prove that the cases of the lemma correspond to the ones of theorem.

(1)All elements of H have the same eigenspaces, because in this case there are only two of them. Hence G is contained in the associated Cartan subgroup. Since H is obtained by projectivizing, it follows that H is cyclic.

(2)In this case, the orbit HE_3 has 2 elements, and the isotropy group H_3 of E_3 in H has index 2 in H, and is normal in H. Let G_3 be the inverse image of H_3 in G. Then G_3 admits E_3 as eigenspace, and by Theorem 1.6.8, we conclude that G_3 is contained in the corresponding Cartan subgroup. It follows that H_3 is cyclic, so H is dihedral. Since $G/G_3 \sim H/H_3$ we see that G permutes the two eigenspaces, and hence cannot be contained in the Cartan subgroup, but it is contained in the normalizer.

(3)$H \sim A_4$. The orbit of E_3 under H has 4 elements and the isotropy group H_3 has 3 elements. The representation of H as a permutation group of 4 elements is faithful, otherwise an element of the kernel admits 4 distinct eigenspaces, which is impossible. Hence H is isomorphic to a subgroup of the permutation group on the eigenspaces $E_1, \ldots, E_4$ and must be isomorphic to A_4 since H has order 12.

(4)$H \sim S_4$. The orbit of E_2 under H has 8 elements, and the isotropy group H_2 has 3 elements. If E is an eigenspace of H whose isotropy group has order 3 then E is necessarly in the orbit of E_2. Hence we consider the

orbit HE_2 as consisting of four pairs of eigenspace, and we obtain a representation of H as a permutation group of these pairs. The representation is faithful, and hence $H \sim S_4$, the order of H is 24. Otherwise an element $\alpha \in H$ leaves every pair invariant, $\alpha \neq 1$, then α has order 2 and interchanges the elements of each pair. This determines α uniquely, and hence α lies in the center of H. This would imply that H as an element of order 6, which is impossible.

(5)$H \sim A_5$. H has order 60 and the unique simple group of order 60 is A_5, so if we show that H is simple we have proved the statement. Every element of H lies in one of the isotropy group of some eigenspace, and the orders of these isotropy groups are 2,3 or 5, in particular are prime. Any two eigenspaces belonging to elements of the same order are in the same orbit of H. Hence any two cyclic subgroup of the same order of H are conjugate. So any normal subgroup of H contains all or none of the elements of any given order. Counting pairs of eigenspaces belonging to any given element, we see that H has 15 elements of order 2, 20 of order 3 and 24 of order 5. Hence H can have no non-trivial normal subgroup, so it is simple. □

Corollary 1.6.16. *If $char(\boldsymbol{F}) = 2, 3$ then every finite subgroup of $PGL_2(\boldsymbol{F})$ of order prime to $2, 3$ is cyclic or dihedral.*

Proposition 1.6.17. *Let $\boldsymbol{F}$ be a field, we have that:*

- *$PGL_2(\boldsymbol{F})$ contains a subgroup isomorphic to A_4 if $char(\boldsymbol{F}) \neq 2$ and there exist $x, y \in \boldsymbol{F}$ such that $x^2 + y^2 = -1$ or if $char(\boldsymbol{F}) = 2$ and there exists $x \in \boldsymbol{F}$ such that $x^2 + x = 1$;*
- *$PGL_2(\boldsymbol{F})$ contains a subgroup isomorphic to S_4 if and only if $char(\boldsymbol{F}) \neq 2$ and there exist $x, y \in \boldsymbol{F}$ such that $x^2 + y^2 = -1$;*
- *$PGL_2(\boldsymbol{F})$ contains a subgroup isomorphic to A_5 if and only if there exist $x, y, z \in \boldsymbol{F}$ such that $y^2 + z^2 = -1$ and $x^2 + x = 1$.*

For a reference [32] pg. 281.

Chapter 2

Modular form theory

2.1 Continuous group actions

Let G be a topological group and let X be a topological space. An *action* of G on X on the left,

$$(g, x) \mapsto gx : G \times X \to X$$

is continuous if this map is continuous. Then, for each $g \in G$, $x \mapsto gx : X \to X$ is a homeomorphism (with inverse $x \mapsto g^{-1}x$). An *orbit* under the action is the set Gx of translates of an $x \in X$. The *stabilizer* of $x \in X$, called also *isotropy group* at x, is

$$Stab(x) = \{g \in G | gx = x\}$$

If X is Hausdorff, then $Stab(x)$ is closed because it is the inverse image of x under of $g \mapsto gx : G \to X$. There is a bijection

$$G/Stab(x) \to Gx \quad g \cdot Stab(x) \mapsto gx$$

in particular, when G acts transitively on X, i.e. it possesses only a single group orbit, which means that for every pair of elements x and y, there is a group element g such that $gx = y$, then there is a bijection

$$G/Stab(x) \to X$$

Let $G\backslash X$ be the set of orbits for the action of G on X: it has a natural quotient topology, if π denotes the map $G \to G\backslash X$ sending $x \mapsto Gx$, then $U \subset G\backslash X$ is open if and only if $\pi^{-1}(U)$ is open in G. Note that $\pi : X \to G\backslash X$ is continuous and open: continuity by definition of the topology, open because if U is an open subset of X then $\pi^{-1}(\pi(U)) = \bigcup_{g \in G} gU$, which is open.
Let H be a subgroup of G. Then H acts on G on the left and on the right, and $H\backslash G$ and G/H are the spaces of right and left cosets. In particular it is possible to show that:

Lemma 2.1.1. *The space G/H is Hausdorff if and only if H is closed in G.*

Proof. For example [34], Chapter 1. □

When G acts transitively on X, there is a bijection $G/Stab(x) \to X$ for any $x \in X$. Under some mild hypotheses, this will be a homeomorphism:

Proposition 2.1.2. *Suppose G acts continuously and transitively on X. If G and X are locally compact and Hausdorff, and there is a countable basis for the topology of G, then the map*

$$[g] \mapsto gx : G/Stab(x) \to X$$

where $[g]$ is the equivalence class of g in $G/Stab(x)$, is a homeomorphism.

Proof. For example [34], Chapter 1. □

Let Γ be a group acting on a topological space X. If $\Gamma\backslash X$ is Hausdorff, then the orbits are closed, but this condition is not sufficient to ensure that the quotient space is Hausdorff.

Definition 2.1.3. *Let Γ be a group acting on a topological space X. The action is said to be* discontinuous *if for every $x \in X$ and infinite sequence (γ_i) of distinct elements of Γ, the set $\{\gamma_i\, x\}$ has no cluster point; it is said to be* properly discontinuous *if, for any pair of points x and y of X, there exist neighbourhoods U_x and U_y of x and y such that the set $\{\gamma \in \Gamma | \gamma U_x \cap U_y \neq \emptyset\}$ is finite.*

Proposition 2.1.4. *Let G be a locally compact group acting on a topological space X such that for one point, hence every, $x_0 \in X$, the stabilizer K of x_0 in G is compact and $gK \mapsto gx_0 : G/K \to X$ is a homeomorphism. The following conditions on a subgroup Γ of G are equivalent:*

- *Γ acts discontinuously on X;*
- *Γ acts properly discontinuously on X;*
- *for any compact subsets A and B of X,$\{\gamma \in \Gamma | \gamma A \cap B \neq \emptyset\}$ is finite;*
- *Γ is a discrete subgroup of G.*

Proof. For example [34] □

Proposition 2.1.5. *Let G, K, X be as in the previous Proposition, and let Γ be a discrete subgroup of G. Then:*

1. *For any $x \in X$, $\{g \in \Gamma | gx = x\}$ is finite.*

2. *For any $x \in X$, there is a neighbourhood U of x with the following property: if $\gamma \in \Gamma$ and $U \cap \gamma U \neq \emptyset$, then $\gamma x = x$.*

3. *For any points x and $y \in X$ that are not in the same Γ-orbit, there exist neighbourhoods U of x and V of y such that $\gamma U \cap V = \emptyset$ for all $\gamma \in \Gamma$.*

Proof. For example [34] □

Corollary 2.1.6. *Under the hypotheses of Proposition 2.1.5, the space $\Gamma\backslash X$ is Hausdorff.*

Proof. Let x and y be points of X not in the same Γ-orbit, and choose neighbourhoods U and V as in Proposition 2.1.5. Then the images of U and V in $\Gamma\backslash X$ are disjoint neighbourhoods of Γx and Γy. □

Definition 2.1.7. *A group Γ is said to* act freely *on a set X if $Stab(x) = e$ for all $x \in X$, where e is the identity element of the group.*

2.2 Modular curves

2.2.1 Congruence subgroups

Let us consider the complex upper half plane:

$$\mathbb{H} = \{z \in \mathbb{C} \,|\, Im(z) > 0\}$$

It is possible to define an action of $SL_2(\mathbb{R})$ on $\mathbb{H}$ as follows:

$$SL_2(\mathbb{R}) \times \mathbb{H} \to \mathbb{H}, \quad (\alpha, z) \mapsto \alpha(z) = \frac{az+b}{cz+d}, \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

The action is well-defined since $Im(\alpha z) = Im(z)/|cz+d|^2$ and $Im(z) > 0$ so $Im(\alpha z) > 0$. When we set on $SL_2(\mathbb{R})$ and $\mathbb{H}$ their natural topologies, this action is continuous.
The special orthogonal group $SO_2(\mathbb{R})$ is a closed subgroup of $SL_2(\mathbb{R})$, and so $SL_2(\mathbb{R})/SO_2(\mathbb{R})$ is an Hausdorff topological space by Lemma 2.1.1.

Proposition 2.2.1. *The following statements hold:*

1. *The group $SL_2(\mathbb{R})$ acts transitively on $\mathbb{H}$, i.e., for any elements $z, w \in \mathbb{H}$, there exists an $\alpha \in SL_2(\mathbb{R})$ such that $\alpha z = w$.*

2. *The action of $SL_2(\mathbb{R})$ on $\mathbb{H}$ induces an isomorphism*

$$SL_2(\mathbb{R})/\{\pm I\} \xrightarrow{\cong} \mathrm{Aut}_{bh}(\mathbb{H})$$

where $\mathrm{Aut}_{bh}(\mathbb{H})$ is the set of biholomorphic automorphisms on $\mathbb{H}$.

3. *The stabilizer of i is $SO_2(\mathbb{R})$.*

4. *The map*

$$SL_2(\mathbb{R})/SO_2(\mathbb{R}) \to \mathbb{H}, \quad \alpha \cdot SO_2(\mathbb{R}) \mapsto \alpha(i)$$

is a homeomorphism.

Proof. (1) Let $z \in \mathbb{H}$; it suffices to show that there exists an $\alpha \in SL_2(\mathbb{R})$ such that $\alpha(i) = z$: in fact if w is a second point, then $\alpha'(i) = w$ for some $\alpha' \in SL_2(\mathbb{R})$, and $\alpha'\alpha^{-1}(z) = w$. Write $z = x + iy$; then choose $\alpha = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix} \in SL_2(\mathbb{R})$, and $\alpha(i) = z$.
(2) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = z$ then $cz^2 + (d-a)z - b = 0$. If this is true for all $z \in \mathbb{H}$, then the polynomial must have zero coefficients, and so $c = 0$, $d = a$, and $b = 0$. Thus $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ and this has determinant 1 if and only if $a = \pm 1$. Thus only $\pm I$ act trivially on $\mathbb{H}$. Let γ be an automorphism $\mathbb{H}$. We know from (1) that there is an $\alpha \in SL_2(\mathbb{R})$ such that $\alpha(i) = \gamma(i)$. After replacing γ with $\alpha^{-1} \circ \gamma$, we can assume that $\gamma(i) = i$. The map

$$\rho : \mathbb{H} \to D, z \mapsto \frac{z-i}{z+i}$$

is an isomorphism from $\mathbb{H}$ onto the open unit disk, and it maps i to 0. Use ρ to transfer γ into an automorphism γ' of D fixing 0. The automorphisms of D fixing 0 are the maps of the form $z \mapsto \lambda z$, with $|\lambda| = 1$, by Schwarz Lemma for holomorphic functions on the disk. It follows directly that there is a $\theta \in \mathbb{R}$ such that

$$\rho \circ \gamma \circ \rho^{-1}(z) = e^{2\theta i} \cdot z \ \ \forall z$$

and by simple computations $\gamma(z) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \cdot z$. Thus $\gamma \in SO_2(\mathbb{R}) \subset SL_2(\mathbb{R})$.
(3) We have $\frac{ai+b}{ci+d} = i$ so $ai + b = -c + di$, hence $a = d, b = -c$. Therefore the matrix is of the form $\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ with $a^2 + b^2 = 1$, and so is in $SO_2(\mathbb{R})$.
(4) This is a consequence of Proposition 2.1.2. □

Proposition 2.2.2. *Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$ such that Γ (or $\Gamma/\{\pm I\}$ if $-I \in \Gamma$) acts freely on $\mathbb{H}$. Then there is a unique complex structure on $\Gamma\backslash\mathbb{H}$ with the following property: a function f on an open subset U of $\Gamma\backslash\mathbb{H}$ is holomorphic if and only if $f \circ \pi$ is holomorphic, where π is the projection to quotient.*

Proof. The uniqueness follows from the fact that the sheaf of holomorphic functions on a Riemann surface determines the complex structure.
Let $z \in \Gamma\backslash\mathbb{H}$ and choose an $x \in \pi^{-1}(z)$. From (2) of Proposition 2.1.5, there is a neighbourhood U of x such that γU is disjoint from U for all $\gamma \in \Gamma$, $\gamma \neq Id$. The map $\pi|_U : U \to \pi(U)$ is a homeomorphism, and we take all pairs of the form $(\pi(U), (\pi|_U)^{-1})$ to be coordinate neighbourhoods. It is easy to check that they are all compatible, and that the holomorphic functions are as described. □

To check that a subgroup Γ of $SL_2(\mathbb{R})$ is discrete, it suffices to check that Id is isolated in Γ. A discrete subgroup of $SL_2(\mathbb{R})$ is called a *Fuchsian group.*

Definition 2.2.3. *For any positive integer N, we define*

$$\begin{aligned}
\Gamma_0(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\} \\
\Gamma_1(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \mod N \right\} \\
\Gamma(N) &:= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \right\}
\end{aligned}$$

and call $\Gamma(N)$ the principal congruence subgroup of level N*, clearly:*

$$\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$$

In general a congruence subgroup of $SL_2(\mathbb{Z})$ is a subgroup containing $\Gamma(N)$ for some N.

For $N \geq 1$, $\Gamma_1(N) \subset SL_2(\mathbb{Z})$ is the finite index subgroup whose elements are upper unipotent modulo N. It can be proved that it is torsion-free when $N \geq 4$ and moreover acts freely on $\mathbb{H}$ in this case. The group $\Gamma_1(N)$ is normalized by the slightly bigger subgroup $\Gamma_0(N) \subset SL_2(\mathbb{Z})$. The application $\gamma \mapsto d \mod N$ induces a group isomorphism

$$\Gamma_0(N)/\Gamma_1(N) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times$$

We shall view in this way any Dirichlet character $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ as a character of $\Gamma_0(N)$.

$SL_2(\mathbb{Z})$, which is usually referred as $\Gamma(1)$, is discrete and, a fortiori, $\Gamma(N)$ is discrete. The sequence

$$1 \to \Gamma(N) \to SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$$

is exact. In fact, the map $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective: to prove this, we have to show that if $A \in M_2(\mathbb{Z})$ and $\det(A) \equiv 1 \mod N$, then

there is a $B \in M_2(\mathbb{Z})$ such that $B \equiv A \mod N$ and $\det(B) = 1$. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$; the condition on A is that $ad - bc - N\,m = 1$ for some $m \in \mathbb{Z}$. Hence $(c, d, N) = 1$, and we can find an integer n such that $(c, d + nN) = 1$ by the Chinese Remainder Theorem. We can replace d with $d + nN$, and so assume that $(c, d) = 1$.

Consider the matrix $B = \begin{pmatrix} a + eN & b + fN \\ c & d \end{pmatrix}$ for some integers e, f. Its determinant is $ad - bc + N(ed - fc) = 1 + (m + ed - fc)N$. Since $(c, d) = 1$, there exist integers e, f such that $m = fc - ed$, and with this choice, B is the required matrix.

2.2.2 Fundamental Domains

The group $SL_2(\mathbb{C})$ acts on $\mathbb{C}^2$, and hence on the set $\mathbb{P}^1(\mathbb{C})$ of lines through the origin in $\mathbb{C}^2$. When we identify a line with its slope, $\mathbb{P}^1(\mathbb{C})$ becomes identified with $\mathbb{C} \cup \{\infty\}$, and we get an action of $GL_2(\mathbb{C})$ on $\mathbb{C} \cup \{\infty\}$:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}$$

These mappings are called the linear fractional transformations of $\mathbb{P}^1(\mathbb{C})$. They map circles and lines in $\mathbb{C}$ into circles or lines in $\mathbb{C}$. The scalar matrices $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ act as the identity transformation. By the theory of Jordan canonical forms, any nonscalar matrix α is conjugate to a matrix of the following type:

$$(i) \quad \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix} \quad (ii) \quad \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \; \lambda \neq \mu$$

according as it has repeated eigenvalues or distinct eigenvalues. In the first case, α is conjugate to a transformation $z \mapsto z + \lambda^{-1}$, and in the second to $z \mapsto c\,z$, $c \neq 1$. In case (i), α is called *parabolic*, and case (ii), it is called *elliptic* if $|c| = 1$, *hyperbolic* if c is real and positive, and *loxodromic* otherwise.

When $\alpha \in SL_2(\mathbb{C})$, the four cases can be distinguished by the trace of α :

- α is parabolic if and only if $\mathrm{Tr}(\alpha) = \pm 2$;
- α is elliptic if and only if $\mathrm{Tr}(\alpha)$ is real and $|\,\mathrm{Tr}(\alpha)| < 2$;
- α is hyperbolic if and only if $\mathrm{Tr}(\alpha)$ is real and $|\,\mathrm{Tr}(\alpha)| > 2$;
- α is loxodromic if and only if $\mathrm{Tr}(\alpha)$ is not real.

We now investigate the elements of these types in $SL_2(\mathbb{R})$.
Suppose $\alpha \in SL_2(\mathbb{R})$, $\alpha \neq \pm I$, is parabolic. Then it has exactly one eigenvector, and that eigenvector is real. Suppose the eigenvector is $\binom{e}{f}$; if $f \neq 0$, then α has a fixed point in $\mathbb{R}$; if $f = 0$, then ∞ is a fixed point (the transformation is then of the form $z \mapsto z + c$). Thus α has exactly one fixed point in $\mathbb{R} \cup \{\infty\}$.
Suppose $\alpha \in SL_2(\mathbb{R})$, $\alpha \neq \pm I$, is elliptic. Its characteristic polynomial is $X^2 + b\,X + 1$ with $|b| < 2$; hence $\Delta = b^2 - 4 < 0$, and so α has two complex conjugate eigenvectors. Thus α has exactly one fixed point z in $\mathbb{H}$ and a second fixed point, namely, $\overline{z}$, in the lower half plane.
Suppose $\alpha \in SL_2(\mathbb{R})$ and α is hyperbolic. Its characteristic polynomial is $X^2 + b\,X + 1$ with $|b| > 2$; hence $\Delta = b^2 - 4 > 0$, and so α has two distinct real eigenvectors. Thus α has two distinct fixed points in $\mathbb{R} \cup \{\infty\}$.

Definition 2.2.4. *Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$. A point $z \in \mathbb{H}$ is called an* elliptic point *if it is the fixed point of an elliptic element $\gamma \in \Gamma$; a point $s \in \mathbb{R} \cup \{\infty\}$ is called a* cusp *if there exists a parabolic element $\gamma \in \Gamma$ with s as its fixed point.*

Proposition 2.2.5. *If z is an elliptic point of Γ, then $\{\gamma \in \Gamma | \gamma\, z = z\}$ is a finite cyclic group.*

Proof. There exists an $\alpha \in SL_2(\mathbb{R})$ such that $\alpha(i) = z$, and $\gamma \mapsto \alpha^{-1}\,\gamma\,\alpha$ defines an isomorphism

$$\{\gamma \in \Gamma | \gamma\, z = z\} \approx SO_2(\mathbb{R}) \cap (\alpha^{-1}\Gamma\,\alpha)$$

and this last group is finite. The correspondences

$$\theta \;\leftrightarrow\; e^{2\pi\, i\theta} \;\leftrightarrow\; \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

are isomorphisms

$$\mathbb{R}/\mathbb{Z} \;\leftrightarrow\; \{z \in \mathbb{C}\,|\,|z| = 1\} \;\leftrightarrow\; SO_2(\mathbb{R})$$

Therefore $SO_2(\mathbb{R})_{torsion} \approx \mathbb{Q}/\mathbb{Z}$, and every finite subgroup of $\mathbb{Q}/\mathbb{Z}$ is cyclic (each is of the form $n^{-1}\mathbb{Z}/\mathbb{Z}$ where n is the least common denominator of the elements of the group). □

Definition 2.2.6. *Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$, a* fundamental domain *for Γ is a connected open subset D of $\mathbb{H}$ such that no two points of D are equivalent under Γ and $\mathbb{H} = \bigcup \gamma\,\overline{D}$, where $\overline{D}$ is the closure of D, $\gamma \in \Gamma$.*

The definition is equivalent to state that the map $D \to \Gamma\backslash\mathbb{H}$ is injective and the map $\overline{D} \to \Gamma\backslash\mathbb{H}$ is surjective.
Let us consider $\Gamma(1)$, in particular its elements:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

For $z \in \mathbb{H}$ we have that:

$$S\,z = -\frac{1}{z} \qquad T\,z = z + 1$$
$$S^2 \equiv 1 \mod \pm I \qquad (S\,T)^3 \equiv 1 \mod \pm I$$

Applying S to a $z \in \mathbb{H}$, with $|z| = 1$, means first reflect with respect to the x-axis, and then reflect through the origin since $S(e^{i\,\theta}) = -(e^{-i\,\theta})$. Meanwhile applying T means do a translation.

Theorem 2.2.7. *Let $D = \left\{z \in \mathbb{H} \;|\, |z| > 1,\ |Re(z)| < \frac{1}{2}\right\}$, then:*

- *D is a fundamental domain for $\Gamma(1) = SL_2(\mathbb{Z})$; moreover, two elements z and z' of $\overline{D}$ are equivalent under $\Gamma(1)$ if and only if*
  - *$Re(z) = \pm\frac{1}{2}$ and $z' = z \pm 1$,*
  - *$|z| = 1$ and $z' = -\frac{1}{z}$.*
- *Let $z \in \overline{D}$; if the stabilizer of $z \neq \{\pm I\}$, then*
  - *$z = i$, and $Stab(i) = \langle S\rangle$, which has order 2 in $\Gamma(1)/\{\pm I\}$, or*
  - *$z = \rho = e^{\frac{2\,\pi\,i}{6}}$, and $Stab(\rho) = \langle T\,S\rangle$, which has order 3 in $\Gamma(1)/\{\pm I\}$, or*
  - *$z = \rho^2$, and $Stab(\rho) = \langle S\,T\rangle$, which has order 3 in $\Gamma(1)/\{\pm I\}$.*
- *The group $\Gamma(1)/\{\pm I\}$ is generated by S and T.*

Proof. For a reference look at Shimura [34] or Milne [22]. □

Proposition 2.2.8. *Let Γ be a discrete subgroup of $SL_2(\mathbb{R})$, and let D be a fundamental domain for Γ. Let Γ' be a subgroup of Γ of finite index, and write Γ as a disjoint union of right cosets of Γ':*

$$\Gamma = \Gamma'\gamma_1 \cup \cdots \cup \Gamma'\gamma_m$$

Then $D' = \bigcup \gamma_i\,D$ is a fundamental domain for Γ'.

Proof. Let $z \in \mathbb{H}$. Then $z = \gamma\,z'$ for some $z' \in \overline{D}$, $\gamma \in \Gamma$ and $\gamma = \gamma'\,\gamma_i$ for some $\gamma' \in \Gamma'$. Thus $z = \gamma'\gamma_i\,z \in \Gamma' \cdot (\gamma_i\,\overline{D})$.
If $\gamma D' \cap D' \neq \emptyset$, then it would contain a transform of D. But then $\gamma\gamma_i D = \gamma_j D$ for some $i \neq j$, which would imply that $\gamma\gamma_i = \gamma_j$, and this is a contradiction. □

Corollary 2.2.9. *It is possible to choose the γ_i in Proposition 2.2.8 so that the closure of D' is connected; the interior of the closure of D' is then a connected fundamental domain for Γ.*

2.2.3 Modular curves

Now we want to define the complex structure on $\Gamma(1)\backslash\mathbb{H}$. As usual, denote with π the quotient map $\mathbb{H} \to \Gamma(1)\backslash\mathbb{H}$. Let P be a point of $\Gamma(1)\backslash\mathbb{H}$, and let Q be a point of $\mathbb{H}$ mapping to it. If Q is not an elliptic point, we can choose a neighbourhood U of Q such that π is a homeomorphism $U \to \pi(U)$. We define $(\pi(U), \pi^{-1})$ to be a coordinate neighbourhood of P.
If Q is equivalent to i, we may as well take it equal to i. The map $z \mapsto \frac{z-i}{z+i}$ defines an isomorphism of an open disk D with centre i onto an open disk D' with centre 0, and the action of $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ on D is transformed into the automorphism $\sigma : z \mapsto -z$ of D' because it fixes i and has order 2. Thus $\langle S\rangle \backslash D$ is homeomorphic to $\langle\sigma\rangle \backslash D'$, and we give $\langle S\rangle \backslash D$ the complex structure making this a bi-holomorphic isomorphism: in fact S maps the previous map to:

$$\frac{-z^{-1} - i}{-z^{-1} + i} = \frac{-1 - iz}{-1 + iz} = -\frac{z - i}{z + i}$$

Thus $z \mapsto (\frac{z-i}{z+i})^2$ is a holomorphic function defined in a neighbourhood of i which is invariant under the action of S; it therefore defines a holomorphic function in a neighbourhood of $\pi(i)$, and we take this to the coordinate function near $\pi(i)$. The point $Q = \rho^2$ can be treated similarly. Apply a linear fractional transformation that maps Q to zero, and then take the cube of the map. Explicitly, ρ^2 is fixed by ST, which has order 3 (as a transformation). The function $z \mapsto \frac{z-\rho^2}{z-\bar{\rho}^2}$ defines an isomorphism from a disk with centre ρ^2 onto a disk with centre 0, and $(\frac{z-\rho^2}{z-\bar{\rho}^2})^3$ is invariant under ST. It therefore defines a function on a neighbourhood of $\pi(\rho^2)$, and we take this to be the coordinate function near $\pi(\rho^2)$.

Giving such a complex structure we obtain a Riemann surface $\Gamma(1)\backslash\mathbb{H}$ which is not compact. To compactify it we add a point ∞ to $\mathbb{H}$, and use the function $q(z) = exp(2\,\pi\,i\,z)$ to map some neighbourhood $U = \{z \in \mathbb{H}\,|Im(z) > N\}$ of ∞ onto an open disk V with centre 0. The function q is invariant under the action of the stabilizer of $\langle T\rangle$ of ∞, and so defines a holomorphic function $q : \langle T\rangle \backslash U \to V$, which we take to be the coordinate function near $\pi(\infty)$. So now we are considering $\mathbb{H}^* = \mathbb{H} \cup \{cusps\}$.

Proposition 2.2.10. *The Riemann surface $\Gamma(1)\backslash\mathbb{H}^*$ is compact and of genus zero; it is therefore isomorphic to the Riemann sphere.*

Proof. It is compact because $\bar{D} \cup \{\infty\}$ is compact. We sketch the proof that it has genus 0. First, by examining carefully how the points of $\bar{D}$ are identified, one can see that it must be homeomorphic to a sphere. Second, show that it is simply connected (loops can be contracted), and the Riemann sphere is the only simply connected compact Riemann surface. Third, triangulate it by taking ρ, i, and ∞ as the vertices of the obvious triangle, add a fourth vertex not on any side of the triangle, and join it to the first three vertices; then $2 - 2g = 4 - 6 + 4 = 2$. □

Let $\Gamma \subset \Gamma(1)$ of finite index. We can define a compact Riemann surface $\Gamma\backslash\mathbb{H}^*$ in much the same way as for $\Gamma(1)$. The complement of $\Gamma\backslash\mathbb{H}$ in $\Gamma\backslash\mathbb{H}^*$ is the set of equivalence classes of cusps for Γ.
First $\Gamma\backslash\mathbb{H}$ is given a complex structure in exactly the same way as in the case $\Gamma = \Gamma(1)$. The point ∞ will always be a cusp (Γ must contain T^h for some h, and T^h is a parabolic element fixing ∞). If h is the smallest power of T in Γ, then the function $q = exp(2\,\pi\,i\,z/h)$ is a coordinate function near ∞. Any other cusp for Γ is of the form $\sigma\infty$ for $\sigma \in \Gamma(1)$, and $z \mapsto q(\sigma^{-1}(z))$ is a coordinate function near $\sigma\infty$.

Definition 2.2.11. *Using the complex structure described before we define:* $Y(\Gamma) := \Gamma\backslash\mathbb{H}$ *and* $X(\Gamma) := \Gamma\backslash\mathbb{H}^*$, *similarly* $Y(\Gamma(N)) := Y(N)$, $X(\Gamma(N)) := X(N)$, $Y(\Gamma_0(N)) := Y_0(N)$, $X(\Gamma_0(N)) := X_0(N)$. $X(N)$ *is called a* modular curve of level N.

Genus computation

We want now compute the genus of $X(\Gamma)$ by considering it as a covering of $X(\Gamma(1))$. According to Riemann-Hurwitz Formula:

$$2g - 2 = -2m + \sum(e_P - 1)$$

or

$$g = 1 - m + \sum(e_P - 1)/2$$

where m is the degree of the covering $X(\Gamma) \to X(\Gamma(1))$ and e_P is the ramification index at the point P. The ramification points are the images of elliptic points on $\mathbb{H}^*$ and the cusps.

Theorem 2.2.12. *Let* Γ *be a subgroup of* $\Gamma(1)$ *of finite index, and let* ν_2 *the number of inequivalent elliptic points of order* 2*;* ν_3 *the number of inequivalent elliptic points of order 3;* ν_∞ *the number of inequivalent cusps. Then the genus of* $X(\Gamma)$ *is*

$$g = 1 + \frac{m}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

Proof. Let π be the quotient map $\mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$, and let ϕ be the map $\Gamma\backslash\mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$. If Q is a point of $\mathbb{H}^*$ and P and P' are its images in $\Gamma\backslash\mathbb{H}^*$ and $\Gamma(1)\backslash\mathbb{H}^*$ then the ramification indices multiply:

$$e(Q/P) = e(Q/P') \cdot e(P'/P)$$

If Q is a cusp, then this formula is not useful, as $e(Q/P) = \infty = e(Q/P')$. For $Q \in \mathbb{H}$ and not an elliptic point it tells us P' is not ramified.
Suppose that $P = \pi(i)$, so that Q is $\Gamma(1)$-equivalent to i. Then either $e(Q/P') = 2$ or $e(P'/P) = 2$. In the first case, Q is an elliptic point for Γ and P' is unramified over P; in the second, Q is not an elliptic point for Γ, and the ramification index of P' over P is 2. There are ν_2 points P' of the first type, and $(m - \nu_2)/2$ points of the second. Hence:

$$\sum_{P' \text{ over } \phi(i)} e'_P - 1 = \frac{(m - \nu_2)}{2}$$

Suppose that $P = \pi(\rho)$, so that Q is $\Gamma(1)$-equivalent to ρ. Then either $e(Q/P') = 3$ or $e(P'/P) = 3$. In the first case, Q is an elliptic point for Γ and P' is unramified over P; in the second, Q is not an elliptic point for Γ, and the ramification index of P' over P is 3. There are ν_3 points P' of the first type, and $(m - \nu_3)/3$ points of the second. Hence:

$$\sum_{P' \text{ over } \phi(\rho)} e'_P - 1 = 2\frac{(m - \nu_3)}{3}$$

Suppose that $P = \pi(\infty)$, so that Q is a cusp for Γ. There are ν_∞ points P' and $\sum e_i = m$; hence

$$\sum_{P' \text{ over } \phi(\infty)} e'_P - 1 = (m - \nu_\infty)$$

Therefore:

$$g = 1 - m + \sum(e_P - 1)/2 = 1 + \frac{m}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

□

2.3 Modular forms

The natural projective action of $GL_2(\mathbb{C})$ on $\mathbb{P}^1(\mathbb{C})$ induces an action of $SL_2(\mathbb{R})$ on $\mathbb{H}$, and even of $GL_2(\mathbb{R})^+ = \{g \in GL_2(\mathbb{R}), \det(g) > 0\}$, given, as explained before, by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\,\tau + b}{c\,\tau + d} \quad \tau \in \mathbb{H}$$

Definition 2.3.1. *A function $f : \mathbb{H} \to \mathbb{C}$ is said to be a* modular function *for a congruence subgroup Γ if it satisfies:*

1. *f is meromorphic in $\mathbb{H}$,*
2. *$f(\gamma z) = f(z)$ for every matrix $\gamma \in \Gamma$,*
3. *the Laurent series of f has the form $f(z) = \sum_{n=-m}^{\infty} a_n e^{\frac{2\pi i n z}{M}}$ for some integer $M \geq 1$.*

Let us conside $k \in \mathbb{Z}$, $f : \mathbb{H} \to \mathbb{C}$ a holomorphic function, if we define

$$(f|_k\,\gamma)(\tau) = (c\tau + d)^{-k}\, f(\gamma\,\tau)\det(\gamma)^{\frac{k}{2}} \qquad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R})^+$$

we have a right action of $GL_2(\mathbb{R})^+$ on the space $\mathcal{O}(\mathbb{H})$ of holomorphic functions on $\mathbb{H}$, hence an action of its discrete subgroup $SL_2(\mathbb{Z})$ as well by restriction.

Definition 2.3.2. *A* holomorphic modular form *of level N, weight k, and character or nebentypus ϵ, is a holomorphic function f on $\mathbb{H}$ such that:*

MF1 *$f|_k\,\gamma = \epsilon(\gamma)\, f$ for all $\gamma \in \Gamma_0(N)$,*

MF2 *f is holomorphic at the cusps i.e. for all $\sigma \in SL_2(\mathbb{Z})$, the function $f|_k\,\sigma$ has a power series expansion in $e^{\frac{2i\pi\, z}{M}}$ for some integer $M \geq 1$, with exponents ≥ 0.*

An holomorphic modular form *for a congruence subgroup Γ of weight k, and character or nebentypus ϵ, is a holomorphic function f on $\mathbb{H}$ wich satisfies to $f|_k\,\gamma = \epsilon(\gamma)\, f$ for all $\gamma \in \Gamma$, and to (MF2).*

As a first remark from the definition, note that does not exist modular forms with odd weight and trivial nebentypus: the element $\gamma = -Id \in \Gamma$ so by (MF1) it follows that $f(z) = (-1)^k f(z)$, so the weight has to be even. As $-Id \in \Gamma$, note that $M_k(N, \epsilon) = 0$ if $\epsilon(-Id) \neq (-1)^k$. Moreover, we will see later that $M_k(N, \epsilon) = 0$ if $k < 0$, so we assume from now on $k > 0$.

Lemma 2.3.3. *(MF2) is equivalent to the similar property where $\sigma \in SL_2(\mathbb{Z})$ is replaced by $\sigma \in GL_2(\mathbb{Q})^+$.*

Proof. Firstly we can recall that: $GL_2(\mathbb{Q})^+ = SL_2(\mathbb{Z}) \cdot B$ where B is the subgroup of upper triangular matrices in $GL_2(\mathbb{Q})^+$ and that any element in $\mathbb{P}^1(\mathbb{Q})$ may be written as $\gamma(\infty)$ for $\gamma \in SL_2(\mathbb{Z})$: given $x = \frac{a}{b} \in \mathbb{Q}$ with $(a, b) = 1$ using a Bezout relation it is possible to define γ such that $\gamma(\infty) = x$ (γ will have the form $\begin{pmatrix} a & m \\ b & n \end{pmatrix} \in SL_2(\mathbb{Z})$). B is stable at ∞ while

$SL_2(\mathbb{Z})$ acts transitively, so if f has an expansion as a power series in $e^{\frac{2i\pi\,\tau}{M}}$ for some integer $M \geq 1$, with only exponents ≥ 0, then so does $f(a\tau + b)$ for $a \in \mathbb{Q}^\times$ and $b \in \mathbb{Q}$ (increasing M if necessary). □

Note that if (MF1) is satisfied, then (MF2) only has to be checked for σ in a system of representative of the finite set of orbits

$$\Gamma_1(N)\backslash GL_2(\mathbb{Q})^+/B = \Gamma_1(N)\backslash\mathbb{P}^1(\mathbb{Q})$$

called the *cusps* of $\Gamma_1(N)$.

Definition 2.3.4. *Modular forms of level N, weight k, character ϵ form a complex sub-vectorspace of $\mathcal{O}(\mathbb{H})$ denoted by $M_k(N,\epsilon)$. We say f is a* cusp-form *if its expansion in (MF2) has only strictly positive exponents. Cusp-forms form a sub-vector space $S_k(N,\epsilon) \subset M_k(N,\epsilon)$. If we need to stress that the coefficients of the Fourier expansion belong to a ring $\mathcal{O}$we will use the notation $M_k(N,\epsilon,\mathcal{O})$, $S_k(N,\epsilon,\mathcal{O})$. If we are in the trivial nebentypus case we will omit it in the notation.*

Definition 2.3.5. $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \in \Gamma_1(N)$, *hence* $f(\tau+1) = f(\tau)$ *for* $f \in M_k(N,\epsilon)$, *so*

$$f(\tau) = \sum_{n\geq 0} a_n\, q^n$$

where $q := e^{2i\pi\,\tau}$. This specific expansion is called the q-expansion *of f.*

The first nonzero cuspform is the Ramanujan Δ function, which is a generator of $S_{12}(1,1)$, and whose q-expansion is

$$\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n$$

The coefficients $\tau(n)$ define the *Ramanujan τ-function*. It can be proved, using the theory of Hecke operators, that τ is multiplicative and satisfies $\forall\nu$:

$$\tau(p^{\nu+1}) = \tau(p)\tau(p^\nu) - p^{11}\tau(p^{\nu-1})$$

As another example, $S_2(11,\epsilon) = 0$ if $\epsilon \neq 1$ and $S_2(11,1) = \mathbb{C}\,f$ where $f = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2$.

2.3.1 Eisenstein series

Write for any lattice $\Lambda \subseteq \mathbb{C}$:

$$G_k(\Lambda) = \sum_{\omega\in\Lambda,\,\omega\neq 0}\omega^{-2k}$$

and define $G_k(z) = G_k(z\mathbb{Z}+\mathbb{Z}), \forall z \in \mathbb{H}$.

Proposition 2.3.6. *The generalised Eisenstein series $G_k(z)$, $k > 1$, converges to a holomorphic function on $\mathbb{H}$; it takes the value $2\zeta(2k)$ at infinity, where $\zeta(s) = \sum n^{-s}$ is the Riemann zeta function.*

Proof. $G_k(z)$ is a holomorphic function on $\mathbb{H}$, for example look at Diamond [5]. It remains to consider $G_k(z)$ as $z \to i\infty$, remaining in D, the fundamental domain for $\Gamma(1)$.
Because the series for $G_k(z)$ converges uniformly absolutely on D,

$$\lim_{z\to i\infty} G_k(z) = \sum \lim_{z\to i\infty} 1/(mz+n)^{2k}.$$

But $\lim_{z\to i\infty} 1/(mz+n)^{2k} = 0$ unless $m = 0$, and so

$$lim_{z\to i\infty} G_k(z) = \sum_{n\in\mathbb{Z},\, n\neq 0} 1/n^{2k} = 2\zeta(2k).$$

□

The generalised Eisenstein series is a modular form. Indeed, the key property is its $SL_2(\mathbb{Z})$-invariance: for $a, b, c, d \in \mathbb{Z}$, $ad - bc = 1$

$$G_{2k}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{2k} G_{2k}(\tau)$$

and G_{2k} is therefore a modular form of weight $2k$. Note that it is important to assume that $k \geq 2$, otherwise it would be illegitimate to change the order of summation, and the $SL_2(\mathbb{Z})$-invariance would not hold. In fact, there are no nontrivial modular forms of weight 2 as we will see.
The Fourier series of the generalised Eisenstein series is

$$G_{2k}(\tau) = 2\zeta(2k)\left(1 + c_{2k}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n\right)$$

where the Fourier coefficients c_{2k} are given by

$$c_{2k} = \frac{(2\pi i)^{2k}}{(2k-1)!\zeta(2k)} = \frac{-4k}{B_{2k}} = \frac{2}{\zeta(1-2k)}$$

Here, B_n are the Bernoulli numbers, $\zeta(z)$ is Riemann zeta function and $\sigma_p(n)$ is the divisor sum function, the sum of the p-th powers of the divisors of n. In particular, for example one has

$$G_4(\tau) = \frac{\pi^4}{45}\left[1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right]$$

When working with the q-expansion of the generalised Eisenstein series, we can define the normalized Eisenstein serie to which we will refer again later:

$$E_{2k}(\tau) = \frac{G_{2k}(\tau)}{2\zeta(2k)} = 1 + \frac{2}{\zeta(1-2k)}\sum_{n=1}^{\infty}\frac{n^{2k-1}q^n}{1-q^n}$$

2.4 Hecke algebra

The vector space $M_k(N,\epsilon)$ is equipped with a natural collection of endomorphisms called Hecke operators.

Let Γ_1, Γ_2 be two congruence subgroups of $SL_2(\mathbb{Z})$. If $\alpha \in GL_2^+(\mathbb{Q})$ we can consider the *double coset*

$$\Gamma_1 \alpha \Gamma_2 := \{g_1 \alpha g_2 \mid g_i \in \Gamma_i,\ i = 1,2\}$$

If we have $\Gamma_1 \alpha g = \Gamma_1 \alpha g'$ for $g, g' \in \Gamma_2$, then $\alpha g' g^{-1} \alpha^{-1} \in \Gamma_1$ i.e. $g'g^{-1} \in \alpha^{-1}\Gamma_1 \alpha$ i.e. $g'g^{-1} \in (\alpha^{-1}\Gamma_1\alpha) \cap \Gamma_2$. But $(\alpha^{-1}\Gamma_1\alpha)\cap\Gamma_2$ is a congruence subgroup and so has finite index in Γ_2. Hence we have obtained that we can write $\Gamma_1\alpha\Gamma_2 = \cup_j \Gamma_1 \beta_j$, the decomposition into right cosets, where, for the previous discussion, the number of β_j is finite.

Now we will define a linear application induced by the coset $\Gamma_1\alpha\Gamma_2$ as follows:

$$\begin{aligned} M_k(\Gamma_1) &\to M_k(\Gamma_2) \\ f &\mapsto f|_k[\Gamma_1\alpha\Gamma_2] := \sum_j f|_k \beta_j \end{aligned}$$

This application is well-defined: in fact, another set of representatives $\left\{\beta_j'\right\}$ necessarily has form $\beta_j' = \gamma_j\beta_j$ with $\gamma_j \in \Gamma_1$, so for each $f \in M_k(\Gamma_1)$ we have that:

$$f|_k \beta_j' = f|_k \beta_j$$

Clearly $f|_k[\Gamma_1\alpha\Gamma_2]$ is holomorphic on $\mathbb{H}$, so each $f|_k\beta_j$ is holomorphic at all cusps and vanishes at all cusps if f does. Finally, if $\gamma \in \Gamma_2$ then $\Gamma_1\alpha\Gamma_2 = \Gamma_1\alpha\Gamma_2\gamma$ so γ only permutes the cosets $\{\Gamma_1\beta_j\}$; so it follows that $\{\beta_j\gamma\}$ is also a system of coset representatives. Hence:

$$\begin{aligned} f|_k[\Gamma_1\alpha\Gamma_2]|_k\gamma &= \sum_j f|_k\beta_j|_k\gamma = \sum_j f|_k\beta_j\gamma = \\ &= \sum_\iota f|_k\beta_\iota = f|_k[\Gamma_1\alpha\Gamma_2] \end{aligned}$$

so $f|_k[\Gamma_1\alpha\Gamma_2]$ is in $M_k(\Gamma_2)$ and if f was taken in $S_k(\Gamma_1)$ it will map to $S_k(\Gamma_2)$.

Definition 2.4.1. *Fix $N \in \mathbb{N}$, $d \in (\mathbb{Z}/N\mathbb{Z})^*$ and choose δ such that $\delta \equiv d$* mod N. *Choose $a,b,c \in \mathbb{Z}$ such that $\alpha = \begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$. The* diamond operator $\langle d\rangle$ *on $M_k(\Gamma_1(N))$ by:*

$$\langle d\rangle f := f|_k[\Gamma_1(N)\alpha\Gamma_1(N)]$$

Recall that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and that $\alpha \mod \Gamma_1(N)$ is completely determined by $d \equiv \delta \mod N$. It follows that $\langle d \rangle$ is a well-defined operator on $M_k(\Gamma_1(N))$, and also that:

$$\langle d \rangle f = \chi(d) f$$

if $f \in M_k(\Gamma_0(N), \chi)$.

For each prime ℓ, we have an operator T_ℓ defined as follows. Let

$$\Delta(N,\ell) = \left\{ \gamma \in M_2(\mathbb{Z}) |\ \det(\gamma) = \ell \text{ and } \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & \ell \end{pmatrix} \mod N \right\}$$

then we have that:

Lemma 2.4.2. *For ℓ prime with $(\ell, N) = 1$:*

$$\Delta(N,\ell) = \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_1(N) = \coprod_{i=0}^{\ell} \Gamma_1(N) x_i$$

where $x_i = \begin{pmatrix} 1 & i \\ 0 & \ell \end{pmatrix}$ if $i < \ell$ and $x_\ell = \delta \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$ where $\delta \in \Gamma_0(N)$ is any element mapping to $\ell \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Definition 2.4.3. *Fix $k \in \mathbb{Z}$. If $f \in M_k(\Gamma_1(N))$, we define the ℓ* Hecke operator *as*

$$T_\ell(f) := \ell^{\frac{k}{2}-1} (\sum_{i=0}^{\ell} f|_k x_i)$$

so as the action of the double coset $[\Delta(N,\ell)] = \left[\Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \Gamma_1(N) \right]$.

Lemma 2.4.4. *T_ℓ preserves $M_k(N,\epsilon)$ and $S_k(N,\epsilon)$. On q-expansions:*

$$T_\ell(\sum_{n \geq 0} a_n q^n) = \sum_{n \geq 0} a_{\ell n} q^n + \epsilon(\ell) \ell^{k-1} \sum_{n \geq 0} a_n q^{\ell n}$$

Moreover, T_ℓ and $T_{\ell'}$ commute each other.

Proof. $\Delta(N,\ell)$ is stable by left and right translations by $\Gamma_1(N)$, and by conjugation by $\Gamma_0(N)$. Any coset $\Gamma_1(N) x_i$ is then set to another one by any right translation of an element of $\Gamma_1(N)$, or conjugation by an element of $\Gamma_0(N)$. It follows that if f satisfies (MF1) then so does $T_\ell(f)$. It follows from lemma 2.3.3 that if f satisfies (MF2) (respectly is a cuspform), then so does $T_\ell(f)$, hence the first part of the statement.
By definition,

$$\begin{aligned} (f|_k x_i)(\tau) &= \ell^{-\frac{k}{2}} f(\tfrac{\tau+i}{\ell}) && \text{if } i < \ell \\ (f|_k x_\ell)(\tau) &= \ell^{\frac{k}{2}} \epsilon(\ell) f(\ell\,\tau) && \text{if } i = \ell \end{aligned}$$

The expression for T_ℓ follows then from the relation $\sum_{i=0}^{\ell-1} e^{2\pi\, i\, n \frac{(\tau+i)}{\ell}} = 0$ for $(n,\ell) = 1, \ell\, q^{\frac{n}{\ell}}$ otherwise. One checks on the q-expansion that T_ℓ and $T_{\ell'}$ commute. □

We can now define the Hecke operator T_n for a generic $n \in \mathbb{N}$ as follows: if $n = 1$ assign $T_1 = Id$, the identity operator, if $m = \ell^r$, where ℓ is a prime, define T_m recursively:

$$T_{p^r} = T_{p^{r-1}}\, T_p - \, p^{k-1}\, \langle p \rangle \cdot T_{p^{r-2}}, \;\; r \geq 2$$

If $m = p_1^{a_1} \dots p_t^{a_t}$ with distinct primes $p_1 < \dots < p_t$, define $T_m := T_{p_1^{a_1}} \dots T_{p_t^{a_t}}$. In particular it is possible to prove the following Theorem which describes the shape of the generic q-expansion for T_m, for a reference look at Diamond [5]:

Theorem 2.4.5. *Let $f \in M_k(\Gamma_0(N), \chi)$ with q-expansion $f = \sum_{n=0}^{\infty} a_n q^n$. Let $m \in \mathbb{N}$. Then the q-expansion of $T_m f$ is:*

$$T_m f = \sum_{n=0}^{\infty} b_n q^n$$

where:

$$b_n := \sum_{d|(m,n)} \chi(d)\, d^{k-1}\, a_{\frac{mn}{d^2}}$$

where $\chi(d) := 0$ if $(d, N) > 1$.

It is possible to prove that the operators T_m, $m \in \mathbb{N}$, commute with the diamond operator $\langle d \rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^*$ using double coset action description in terms of representatives. Note that for a prime p:

$$T_p f = \sum_{n=0}^{\infty} a_{pn} + \chi(p)\, p^{k-1}\, a_{\frac{n}{p}}$$

where $\chi(p) = 0$ if $p \mid N$, and $a_{\frac{n}{p}} = 0$ if $p \nmid N$.

Definition 2.4.6. *The Hecke algebra $\mathbb{T}_k(\Gamma_1(N))$ is the $\mathbb{Z}$-algebra generated by the operators T_n, $\langle n \rangle$, acting on $S_k(\Gamma_1(N))$, for $n \in \mathbb{N}$.*

As a last remark we can stress the fact that the action of T_p on $S_k(\Gamma_1(N))$, for $p \in \mathbb{N}$, depends not only on p but also on N. In literature, the operators T_p for p prime dividing N are usually referred as U_p.

2.5 Petterson scalar product

Definition 2.5.1. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let $k \in \mathbb{N}$. Let F be a fundamental domain for Γ. Suppose $f, g \in M_k(\Gamma)$ and at least one between f and g is a cuspform, we define the* Petterson scalar product *of f and g to be:*

$$\langle f, g \rangle := \frac{1}{\left[PSL_2(\mathbb{Z}) : \overline{\Gamma}\right]} \int_F f(z)\,\overline{g(z)}\,y^k\,\frac{dx\,dy}{y^2}$$

where $\overline{\Gamma}$ is the image of Γ in $PSL_2(\mathbb{Z})$, $x := Re(z)$ and $y := Im(z)$.

Directly from the definition it is possible to deduce that $\langle \cdot, \cdot \rangle$ has the following proprieties:

1. it is linear in the first variable;
2. it is antilinear in the second variable: $\langle f, c \cdot g \rangle = \bar{c}\,\langle f, g \rangle \ \forall c \in \mathbb{C}$;
3. $\langle f, f \rangle > 0$ if $f \neq 0$;
4. $\langle f, g \rangle = \overline{\langle g, f \rangle}$.

In short, $\langle \cdot, \cdot \rangle$ is an Hermitian inner product. Now we will show that it is independent on the choice of F, in this direction we will need the following Theorem, for a reference look at Koblitz [15], Chapter III:

Theorem 2.5.2. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$, let $k \in \mathbb{N}$ and suppose $f \in M_k(\Gamma)$ with q-expansion $f = \sum_{n \geq 0} a_n\, q^{\frac{n}{N}}$. Then*

$$|a_n| = O(n^c)$$

for some positive constant c, i.e. the a_n have at most polynomial growth.

Proposition 2.5.3. *Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$, let $k \in \mathbb{N}$ and let $f, g \in M_k(\Gamma)$ and at least one is a cuspform. Then:*

1. *The integral $\int_F \frac{dx\,dy}{y^2}$ converges and it is independent on the choice of F;*
2. *The integral $\int_F f(z)\,\overline{g(z)}\,y^{k-2}\,dx\,dy$ converges and it is independent on the choice of F.*

Proof. Suppose that $PSL_2(\mathbb{Z}) = \cup_i \alpha_i \overline{\Gamma}$, $\alpha_i \in SL_2(\mathbb{Z})$, is a decomposition of $PSL_2(\mathbb{Z})$ into left cosets with respect to $\overline{\Gamma}$. Let F_0 be the standard fundamental domain for $SL_2(\mathbb{Z})$. We then know that $F_1 := \cup_i \alpha_i^{-1} F_0$ is a fundamental domain for Γ by Proposition 2.2.8.

Now we first claim that the measure $\frac{dx\,dy}{y^2}$ is invariant under the action of $SL_2(\mathbb{Z})$: let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. We have:

$$\frac{d\,gz}{dz} = (cz+d)^{-2} \;\; Im(gz) = |cz+d|^{-2} \cdot Im(z)$$

and recall that: $dz = dx + i\,dy$, $d\bar{z} = dx - i\,dy$ so that $dx \wedge dy = \frac{i}{2}\,dz \wedge d\bar{z}$. It follows that:

$$d\,g\bar{z} = \overline{(cz+d)}^{-2} d\bar{z} \;\; d\,gz = (cz+d)^{-2} dz$$

and so

$$\frac{d\,gz \,\wedge\, d\,g\bar{z}}{(Im(gz))^2} = \frac{|cz+d|^{-4}\,dz \wedge d\bar{z}}{|cz+d|^{-4}(Im(z))^2} = \frac{dz \wedge d\bar{z}}{(Im(z))^2}$$

Since both F and F_1 are fundamental domains for Γ, we know that for each of the pieces $\alpha_i^{-1}F_0$ of F there is $\gamma_i \in \Gamma$ such that $\gamma_i\alpha_i^{-1}F_0 \subseteq F$ and so $F = \cup_i\, \gamma_i\alpha_i^{-1}F_0$. Integrating over the piece $\gamma_i\alpha_i^{-1}F_0$ means integrating over $\alpha_i^{-1}F_0$ under a change $z \mapsto \gamma_i\, z$ of variables. It is now clear that if the first integral converge then it is independent of the choice of F.
Let us look at the second integrand $f(z)\,\overline{g(z)}\,y^{k-2}\,dx\,dy$. We already know that $\frac{dx\,dy}{y^2}$ is invariant under $SL_2(\mathbb{Z})$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, then since $f, g \in M_k(\Gamma)$:

$$\begin{aligned} f(\gamma z)\,\overline{g(\gamma z)}\,(Im(\gamma z))^k &= f(z)(cz+d)^k\,\overline{g(z)(cz+d)}^k\,\frac{(Im(z))^k}{|cz+d|^{2k}} = \\ &= f(z)\,\overline{g(z)}\,(Im(\gamma z))^k \end{aligned}$$

so also the second integrand is independent of the choice of F if it converges. Now

$$\begin{aligned} \int_{F_0} \frac{dx\,dy}{y^2} &\leq \int_{-\frac{1}{2}}^{\frac{1}{2}} (\int_{\frac{1}{2}\sqrt{3}}^{\infty} \frac{dy}{y^2})dx = \\ &= \int_{-\frac{1}{2}}^{\frac{1}{2}} \frac{2}{\sqrt{3}} dx = \frac{2}{\sqrt{3}} < \infty \end{aligned}$$

and so in fact

$$\int_{F_0} \frac{dx\,dy}{y^2} = \int_{F_1} \frac{dx\,dy}{y^2} = [SL_2(\mathbb{Z}) : \Gamma] \cdot \frac{2}{\sqrt{3}} < \infty$$

Let us see that the second integral coverges. It is enough to see that each integral $\int_{\alpha_i^{-1}F_0} f(z)\,\overline{g(z)}\,y^{k-2}\,dx\,dy$ converges absolutely. Making the change of variables $z \mapsto \alpha_i^{-1}\,z$ we have to consider:

$$\int_{F_0} f(\alpha_i^{-1}z)\,\overline{g(\alpha_i^{-1}z)}\,(Im(\alpha_i^{-1}z))^k\,\frac{dx\,dy}{y^2}$$

since $\frac{dx\,dy}{y^2}$ is invariant. Now we show that the function

$$f(\alpha_i^{-1}z)\,\overline{g(\alpha_i^{-1}z)}\,(Im(\alpha_i^{-1}z))^k$$

is bounded on F_0 which will prove the claim. Now with $\alpha_i^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ we have

$$f(\alpha_i^{-1}z) = (f|_k\,\alpha_i^{-1})(z)\,(cz+d)^k \quad \overline{g(\alpha_i^{-1}z)} = \overline{(g|_k\,\alpha_i^{-1})}(z)\,\overline{(cz+d)}^k$$

but since $(Im(\alpha_i^{-1}z))^k = \frac{(Im(z))^k}{|cz+d|^{2k}}$ our claim is that

$$(f|_k\,\alpha_i^{-1})(z)\,\overline{(g|_k\,\alpha_i^{-1})}(z)\,(Im(z))^k$$

is bounded on F_0. Since $f, g \in M_k(\Gamma)$ we know that $f|_k\,\alpha_i^{-1}$ and $g|_k\,\alpha_i^{-1}$ have q-expansion of shape:

$$(f|_k\,\alpha_i^{-1})(z) = \sum_{n\geq 0} a_n\,q^{\frac{n}{N}} \quad (g|_k\,\alpha_i^{-1})(z) = \sum_{n\geq 0} b_n\,q^{\frac{n}{N}}$$

and since either f or g is a cuspform, we have either $a_0 = 0$ or $b_0 = 0$, so it follows that $(f|_k\,\alpha_i^{-1})(z)\,\overline{(g|_k\,\alpha_i^{-1})}(z)$ has shape $\sum_{n=1}^{\infty} c_n\,\tau_n$ with c_n constants and $\tau_n = O(e^{-\frac{2\pi\,yn}{N}})$. The constant c_n for the previous Theorem have at most polynomial growth, τ_n goes to 0 exponentially with respect to y and $(Im(z))^k = y^k$ goes polynomially to ∞ so the claim follows. □

In the same assumptions of the previous Proposition, it is possible to show that the Petterson scalar product is compatible with congruence subgroup. More precisely if $\Gamma_1 \subseteq \Gamma$ is a congruence subgroup, hence we have that if $f, g \in M_k(\Gamma)$ then $f, g \in M_k(\Gamma_1)$. Then if we calculate $\langle f, g\rangle$ considering f and g as forms on Γ_1 we get the same if we compute $\langle f, g\rangle$ as before, for a reference Koblitz [15].

Proposition 2.5.4. *Consider $\Gamma_1(N)$ and let $f, g \in M_k(\Gamma_1(N))$ with at least one cusp form. Let $\alpha \in GL_2^+(\mathbb{Q})$. Considering $f|_k\,\alpha$ and $g|_k\,\alpha$ as forms on the congruence subgroup $\Gamma_1 = \Gamma_1(N) \cap \alpha^{-1}\Gamma_1(N)\alpha$ we have:*

$$\langle f|_k\,\alpha, g|_k\,\alpha\rangle = (\det\alpha)^{k-2}\,\langle f, g\rangle$$

consequently

$$\langle f|_k\,\alpha, g\rangle = \left\langle f, g|_k\,(\det\alpha)\alpha^{-1}\right\rangle$$

The value $\langle f|_k\,\alpha, g\rangle$ depends only on the double coset $\Gamma_1(N)\alpha\Gamma_1(N)$.

Proof. We will prove only the first statement since the others follow by easy computations and from the fact that the scalar $\det\alpha$ acts in weight k as multiplication by $(\det\alpha)^{k-2}$. So let F_1 be a fundamental domain for Γ_1, we have:

$$\langle f|_k\,\alpha, g|_k\,\alpha\rangle = \frac{1}{\left[PSL_2(\mathbb{Z}):\overline{\Gamma_1}\right]}\int_F (f|_k\,\alpha)(z)\,\overline{(g|_k\,\alpha)(z)}\,(Im(z))^k\,\frac{dx\,dy}{y^2}$$

Firstly it is possible to show that the measure $\frac{dx\,dy}{y^2} = \frac{i}{2}\frac{dz\wedge d\bar{z}}{(Im(z))^2}$ is invariant under the action of α. Then using the formulas:

$$Im(\alpha z) = \frac{Im(z)}{|cz+d|^2}\cdot\det\alpha \quad \frac{d\,\alpha z}{dz} = \frac{\det\alpha}{(cz+d)^2}$$

for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, so we get:
$f(\alpha z)(cz+d)^{-k}\,\overline{g(\alpha z)}(c\bar{z}+d)^{-k}\,(\det\alpha)^{2k-2}\,(Im(\alpha z))^k\,|cz+d|^{2k}\,(\det\alpha)^{k-2}\frac{dx\,dy}{y^2} =$
$= f(\alpha z)\,\overline{g(\alpha z)}\,(Im(\alpha z))^k\,(\det\alpha)^{k-2}\frac{dx\,dy}{y^2}$

and changing variables we have:

$$\langle f|_k\,\alpha, g|_k\,\alpha\rangle = \frac{(\det\alpha)^{k-2}}{\left[PSL_2(\mathbb{Z}):\overline{\Gamma_1}\right]}\int_{\alpha F_1} f(z)\,\overline{g(z)}\,(Im(z))^k\,\frac{dx\,dy}{y^2}$$

Now it is easy to see that αF_1 is a fundamental domain for the group $\Gamma_2 := \alpha\Gamma_1\alpha^{-1} = \alpha^{-1}\Gamma_1(N)\alpha\cap\Gamma_1(N)$ which means that $\left[PSL_2(\mathbb{Z}):\overline{\Gamma_2}\right] = \left[PSL_2(\mathbb{Z}):\overline{\Gamma_1}\right]$ since Γ_2 is conjugate to Γ_1. Now since $\Gamma_2\subseteq\Gamma_1(N)$, both f and g are on Γ_2 and so:

$$\langle f, g\rangle = \frac{1}{\left[PSL_2(\mathbb{Z}):\overline{\Gamma_2}\right]}\int_{\alpha F_1} f(z)\,\overline{g(z)}\,y^k\,\frac{dx\,dy}{y^2}$$

so the claim follows. □

Lemma 2.5.5. *Let Γ be a congruence subgroup and let $\alpha\in GL_2^+(\mathbb{Q})$. Then there are elements β_j, finite in number, such that:*

$$\Gamma\alpha\Gamma = \cup_j\Gamma\beta_j = \cup_j\beta_j\Gamma$$

as disjoint unions.

Proof. For a proof check Koblitz [15] or Diamond [5]. □

In the setting of the Lemma, notice that we have

$$\Gamma(\det\alpha)\alpha^{-1}\Gamma = \cup_j\Gamma(\det\beta_j)\,\beta_j^{-1}$$

as disjoint unions.

Theorem 2.5.6. *Suppose that $N \in \mathbb{N}$, $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ is a Dirichlet character modulo N and that $k \in \mathbb{N}$. Let $n \in \mathbb{N}$ with $(n, N) = 1$. Then if $f, g \in M_k(\Gamma_0(N), \chi)$ with at least one a cuspform, we have*

$$\langle T_n f,\, g\rangle = \chi(n)\,\langle f, T_n\, g\rangle$$

Proof. Let us first prove the statement in the case $n = p$ a prime number. Applying the previous Lemma:

$$\Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N) = \cup_j \Gamma_1(N)\beta_j = \cup_j \beta_j \Gamma_1(N)$$

Notice that $\det \beta_j = \det \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix} = \beta$. We now find:

$$\begin{aligned}
\langle T_n f,\, g\rangle &= \left\langle f|_k\, \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N),\, g\right\rangle = \\
&= \left\langle \sum_j f|_k\, \beta_j,\, g\right\rangle = \sum_j \langle f|_k\, \beta_j,\, g\rangle = \\
&= \sum_j \left\langle f,\, g|_k\, (\det \beta_j)\, \beta_j^{-1}\right\rangle = \left\langle f,\, \sum_j g|_k\, (\det \beta_j)\, \beta_j^{-1}\right\rangle = \\
&= \left\langle f,\, \sum_j g|_k\, \Gamma_1(N)\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\Gamma_1(N)\right\rangle
\end{aligned}$$

since $(\det \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}) \cdot \begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}^{-1} = \begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}$.
Now choose $b, d \in \mathbb{Z}$ such that $dp - bN = 1$, this is possible because $p \nmid N$ by assumption. Then

$$\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix} = \begin{pmatrix}1 & b\\ N & dp\end{pmatrix}^{-1}\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\begin{pmatrix}p & b\\ N & d\end{pmatrix}$$

Since $\begin{pmatrix}1 & b\\ N & dp\end{pmatrix} \in \Gamma_1(N)$, $\begin{pmatrix}p & b\\ N & d\end{pmatrix} \in \Gamma_0(N)$, and since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, we can then conclude that:

$$\begin{aligned}
\Gamma_1(N)\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix}\Gamma_1(N) &= \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\begin{pmatrix}p & b\\ N & d\end{pmatrix}\Gamma_1(N) = \\
&= \Gamma_1(N)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N)\begin{pmatrix}p & b\\ N & d\end{pmatrix} = \\
&= \cup_j \Gamma_1(N)\,\beta_j\begin{pmatrix}p & b\\ N & d\end{pmatrix}
\end{aligned}$$

Now observe again that $\begin{pmatrix} p & b \\ N & d \end{pmatrix} \in \Gamma_0(N)$ so this matrix acts as $\langle d \rangle$ on forms in $M_k(\Gamma_0(N), \chi)$. Since $pd \equiv 1 \mod N$ we have that $\chi(d) = \chi(p)^{-1} = \overline{\chi(p)}$, hence $\langle d \rangle$ acts as multiplication by $\overline{\chi(p)}$ on elements of $M_k(\Gamma_0(N), \chi)$. Hence we have:

$$\begin{aligned}
\langle T_n f,\, g \rangle &= \left\langle f,\, \sum_j g|_k \, \Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \right\rangle = \\
&= \left\langle f,\, \sum_j g|_k \, \beta_j \begin{pmatrix} p & b \\ N & d \end{pmatrix} \right\rangle = \left\langle f,\, (\sum_j g|_k \beta_j)|_k \begin{pmatrix} p & b \\ N & d \end{pmatrix} \right\rangle = \\
&= \left\langle f,\, (T_p g)|_k \begin{pmatrix} p & b \\ N & d \end{pmatrix} \right\rangle = \left\langle f,\, \overline{\chi(p)} T_p g \right\rangle = \\
&= \chi(p)\, \langle f,\, T_p g \rangle
\end{aligned}$$

Now let us consider the case $n = p^r$ with p a prime not dividing N, and let us show:

$$\langle T_{p^r} f,\, g \rangle = \chi(p^r)\, \langle f,\, T_{p^r} g \rangle$$

by induction on r, having just seen the case $r = 1$. Let us consider the inductive step, so assume that the statement holds for r and let us prove it holds for $r + 1$. Use the relation:

$$T_{p^{r+1}} = T_{p^r} T_p - \langle p \rangle\, p^{k-1} T_{p^{r-1}}$$

and the induction hypothesis to see that:

$$\begin{aligned}
\langle T_{p^r} f,\, g \rangle &= \langle T_{p^r} T_p\, f, g \rangle - \left\langle \langle p \rangle\, p^{k-1} T_{p^{r-1}} f, g \right\rangle = \\
&= \chi(p^r)\chi(p)\, \langle f,\, T_{p^r} T_p g \rangle - \left\langle \chi(p) p^{k-1} T_{p^{r-1}} f, g \right\rangle = \\
&= \chi(p^{r+1})\, \langle f,\, T_{p^r} T_p g \rangle - \chi(p) \left\langle p^{k-1} T_{p^{r-1}} f, g \right\rangle = \\
&= \chi(p^{r+1})\, \langle f,\, T_{p^r} T_p g \rangle - \chi(p)\chi(p^{r-1}) \left\langle f, p^{k-1} T_{p^{r-1}} g \right\rangle = \\
&= \chi(p^{r+1})\, \langle f,\, T_{p^r} T_p g \rangle - \chi(p^r)\chi(p)\overline{\chi(p)} \left\langle f, p^{k-1} T_{p^{r-1}} g \right\rangle = \\
&= \chi(p^{r+1})\, (\langle f,\, T_{p^r} T_p g \rangle - \left\langle f, \chi(p)\, p^{k-1} T_{p^{r-1}} g \right\rangle) = \\
&= \chi(p^{r+1})\, (\left\langle f,\, (T_{p^r} T_p - \langle p \rangle\, p^{k-1} T_{p^{r-1}}) g \right\rangle) = \\
&= \chi(p^{r+1})\, \left\langle f,\, T_{p^{r+1}} g \right\rangle
\end{aligned}$$

Finally, observe that if $m, n \in \mathbb{N}$ with $(m, n) = 1$, and if

$$\begin{aligned}
\langle T_m f,\, g \rangle &= \chi(m)\, \langle f,\, T_m g \rangle \\
\langle T_n f,\, g \rangle &= \chi(n)\, \langle f,\, T_n g \rangle
\end{aligned}$$

for any $f, g \in M_k(\Gamma_0(N), \chi)$, at least one is a cuspform, we can deduce:

$$\begin{aligned} \langle T_{mn} f,\, g\rangle &= \chi(m)\chi(n)\, \langle f,\, T_n\, T_m g\rangle \\ &= \chi(mn)\, \langle f, T_{mn}\, g\rangle \end{aligned}$$

From this observation the general case of the Theorem follows. □

2.6 Oldforms and Newforms

Let $N, k \in \mathbb{N}$ and let $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character modulo N. We have introduced linear operators $\langle d\rangle$, $d \in (\mathbb{Z}/N\mathbb{Z})^*$, and T_n on the finite dimensional complex vector space $S_k(\Gamma_0(N), \chi)$, as we will prove later. On this space we have also the Petterson scalar product $\langle \cdot, \cdot \rangle$, which is an Hermitian positive definite inner product. In particular, $\langle \cdot, \cdot \rangle$ is non-degenerate on $S_k(\Gamma_0(N), \chi)$, meaning that if $\langle f, g\rangle = 0$ for all $g \in S_k(\Gamma_0(N), \chi)$, then $f = 0$.
In this setting we are interested in the adjoints of the above operators.
Suppose that $d \in (\mathbb{Z}/N\mathbb{Z})^*$, if $\delta \in \mathbb{Z}$ is such that $d \equiv \delta \mod N$ then $\langle d\rangle\, f = \chi(\delta) f$ for all $f \in S_k(\Gamma_0(N), \chi)$. For $f, g \in S_k(\Gamma_0(N), \chi)$:

$$\begin{aligned} \langle \langle d\rangle\, f,\, g\rangle &= \langle \chi(\delta)\, f, g\rangle = \\ &= \chi(\delta)\, \langle f,\, g\rangle = \left\langle f, \overline{\chi(\delta)}\, g \right\rangle = \\ &= \left\langle f, \chi(\delta)^{-1}\, g \right\rangle = \left\langle f,\, \left\langle d^{-1}\right\rangle g\right\rangle = \\ &= \left\langle f,\, \langle d\rangle^{-1} g\right\rangle \end{aligned}$$

So we have that

$$\langle d\rangle^* = \langle d\rangle^{-1}$$

Suppose then that $n \in \mathbb{N}$ with $(n, N) = 1$. We have showed that for $f, g \in S_k(\Gamma_0(N), \chi)$:

$$\langle T_n f,\, g\rangle = \chi(n)\, \langle f,\, T_n g\rangle$$

which can be rewritten as:

$$\langle T_n f,\, g\rangle = \left\langle f,\ \langle n\rangle^{-1}\, T_n g\right\rangle$$

so we can define the adjoint operator as:

$$T_n^* = \langle n\rangle^{-1}\, T_n \quad \text{for} \quad n \in \mathbb{N}\ (n, N) = 1$$

By previous results we can now see that not only do the operators $\langle d\rangle$ and T_n, $d \in (\mathbb{Z}/N\mathbb{Z})^*$, $n \in \mathbb{N}$, $(n, N) = 1$, commute, but they even commute with all of their adjoints.

Definition 2.6.1. *A linear operator that commutes with its own adjoint on a complex vector space equipped with a non-degenerate Hermitian inner product is called a* normal operator*.*

Hence $\langle d \rangle$ and T_n are normal operator. For this kind of linear operators a result, known as Spectral Theorem for normal operators, holds:

Spectral Theorem for normal operators. *Let V be a finite dimensional complex vector space equipped with a non-degenerate Hermitian inner product. Let $\{L_\alpha\}_{\alpha \in I}$ be a family of commuting, normal linear operators of V. Then V has a basis consisting of simultaneous eigenvectors for the L_α i.e. there is a basis $v_1, \ldots, v_n$ of V such that each v_i is an eigenvector for every L_α.*

*Proof. (Sketch)*Each individual operator L_α can be diagonalized in V as it is a normal operator. Given L_α and $\lambda \in \mathbb{C}$ we can look at the eigenspace

$$V_{\lambda, L_\alpha} := \{v \in V \mid L_\alpha v = \lambda v\}$$

For each L_α there is a finite number of distinct number $\lambda_1, \ldots, \lambda_{m_\alpha}$ such that $V_{\lambda_j, L_\alpha} \neq \emptyset$ and

$$V = V_{\lambda_1, L_\alpha} \oplus \ldots V_{\lambda_{m_\alpha}, L_\alpha}$$

We can claim that for each L_α we have either $V_{\lambda, L_\alpha} = \emptyset$ or $V_{\lambda, L_\alpha} = V$ for every $\lambda \in \mathbb{C}$. In the particular case in which $dim(V) = 1$ we have that for each α there is a number $\lambda_\alpha \in \mathbb{C}$ such that $V_{\lambda_\alpha, L_\alpha} = V$, so the conclusion of the Theorem is reached picking any basis of V. Suppose the claim is not true, this means that there is an α_0 such that in the previous decomposition all $V_{\lambda_j, L_{\alpha_0}}$ have dimension strictly less than $dimV$. If we can now show that each $V_{\lambda_j, L_{\alpha_0}}$ is mapped into itself by every L_α, then the Theorem follows by induction on $dimV$. If $v \in V_{\lambda_j, L_{\alpha_0}}$ then, since L_{α_0} commutes with the other operators by hypothesis, for every α:

$$L_{\alpha_0}(L_\alpha(v)) = L_\alpha(L_{\alpha_0}(v)) = L_\alpha(\lambda_j v) = \lambda_j(L_\alpha(v))$$

so that $L_\alpha(v) \in V_{\lambda_j, L_{\alpha_0}}$. □

As an immediate corollary to the above Theorem we have:

Theorem 2.6.2. *Suppose that $N \in \mathbb{N}$, $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ is a Dirichlet character modulo N and that $k \in \mathbb{N}$. Then the space $S_k(\Gamma_0(N), \chi)$ has a basis consisting of forms such that each one is an eigenvector for T_n, for every $n \in \mathbb{N}$ with $(n, N) = 1$. We refer to such forms as* eigenforms*.*

Let $N, k \in \mathbb{N}$ and consider a divisor d of N. We can embed the space $S_k(\Gamma_1(\frac{N}{d}))$ into $S_k(\Gamma_1(N))$ in two different ways:

$$\begin{aligned} f(z) \to f(z) \qquad & \sum_n a_n q^n \mapsto \sum_n a_n q^n \\ f(z) \to f(dz) \qquad & \sum_n a_n q^n \mapsto \sum_n a_n q^{dn} \end{aligned}$$

In particular we can consider the linear map

$$\begin{aligned} i_d : S_k(\Gamma_1(\frac{N}{d})) \times S_k(\Gamma_1(\frac{N}{d})) &\to S_k(\Gamma_1(N)) \\ (f, g) &\mapsto f(z) + g(dz) \end{aligned}$$

Definition 2.6.3. *$S_k^{old}(N)$ is the subspace of $S_k(\Gamma_1(N))$ spanned by the images of all linear maps i_d, for all divisor $d > 1$ of N. The elements of $S_k^{old}(N)$ are called* oldforms.

Definition 2.6.4. *$S_k^{new}(N) := (S_k^{old}(N))^{\perp} \subseteq S_k(\Gamma_1(N))$, orthogonal complement with respect to the Petterson scalar product. We refer to elements of S_k^{new} as* newforms.

For example, since $d = 1$ is the only divisor of $N = 1$, we have that $S_k^{old}(1) = 0$, and so $S_k^{new}(1) = S_k(SL_2(\mathbb{Z}))$.

Proposition 2.6.5. *The space $S_k^{old}(N)$ is spanned by the images of the maps i_p where p runs through the prime divisors of N.*

Proof. Let S denote the subspace of $S_k(\Gamma_1(N))$ spanned by all $i_p(S_k(\Gamma_1(\frac{N}{p})))$ for all prime divisors p of N. Then clearly $S \subseteq S_k^{old}(N)$.
On the other hand, let $d > 1$ be an arbitrary divisor of N. The image of i_d is the sum of the subspaces $\mathcal{U}, \mathcal{U}' \subseteq S_k(\Gamma_1(N))$ given as images of the maps:

$$\begin{aligned} f(z) \to f(z) \qquad & \sum_n a_n q^n \mapsto \sum_n a_n q^n \\ f(z) \to f(dz) \qquad & \sum_n a_n q^n \mapsto \sum_n a_n q^{dn} \end{aligned}$$

of $S_k(\Gamma_1(\frac{N}{d}))$, rispectivly. Since $d > 1$, there is a prime divisor p of d. It is clear that $\mathcal{U}$ is contained in $Im(i_p)$: if $f \in S_k(\Gamma_1(\frac{N}{d}))$ then $f \in S_k(\Gamma_1(p\frac{N}{d})) = S_k(\Gamma_1(\frac{N}{\frac{d}{p}}))$ so that $f \in Im(i_p)$. Also $f(\frac{d}{p}z) \in S_k(\Gamma_1(\frac{N}{d}\frac{d}{p})) = S_k(\Gamma_1(\frac{N}{p}))$ and $f(dz) = f(p\frac{d}{p}z) = i_p(f(\frac{d}{p}z))$, so $\mathcal{U}' \subseteq Im(i_p)$. So $Im(i_d) \subseteq S$ for any divisor $d > 1$ of N. Hence $S = S_k^{old}(N)$. □

Proposition 2.6.6. *The subspaces $S_k^{old}(N)$ and $S_k^{new}(N)$ of $S_k(\Gamma_1(N))$ are stable under the action of all operators T_n and $\langle n \rangle$ for all $n \in \mathbb{N}$, where if $(n, N) > 1$ define $\langle n \rangle$ as the zero-operator.*

Proof. For a proof see Diamond [5] or just use the fact that both subspaces are given by eigenforms and the relative definition of the subspaces. □

Theorem 2.6.7. *Suppose that $f \in S_k(N)$ with q-expansion $f = \sum_{n=1}^{\infty} a_n q^n$. Suppose further that f is an eigenform for all Hecke operators T_n for all n with $(n, N) = 1$. Then, if $a_1 = 0$ we have $a_n = 0$ for all n whenever $(n, N) = 1$ and so f is an oldform.*

Proof. Let $m \in \mathbb{N}$ with $(m, N) = 1$. We have $T_m f = \lambda_m f$ for some $\lambda_m \in \mathbb{C}$. Recalling the formula for the n-th Fourier coefficient of $T_m f$, we see that:

$$\sum_{d|(m,n)} \chi(d) d^{k-1} a_{\frac{mn}{d^2}} = \lambda_m a_n \quad \forall n \in \mathbb{N} \quad \text{where} \quad \chi(d) = 0 \ \text{ if } \ (d, N) > 1$$

Now considering the previous expression for $n = 1$ we obtain:

$$a_m = \chi(1)\, 1^{k-1} a_m = \lambda_m a_1 = 0.$$

□

Corollary 2.6.8. *If $0 \neq f = \sum_{n=1}^{\infty} a_n q^n \in S_k^{new}(N, \chi)$ is an eigenform for T_m for all $m \in \mathbb{N}$ with $(m, N) = 1$ then $a_1 \neq 0$.*

Multiplicity One Theorem. *Suppose that $f, g \in S_k(N, \chi)$ are eigenforms for all T_n for all $n \in \mathbb{N}$ with $(n, N) = 1$, and with the same eigenvalues. Suppose futher that f is a nonzero newform. Then g is also a newform and $g = \lambda f$ for some $\lambda \in \mathbb{C}$.*

Proof. Suppose that $g \neq 0$ is an oldform. Hence for Theorem 2.6.2 $S_k^{old}(N)$ has a basis consisting of simultaneous eigenforms for all T_n, $(n, N) = 1$, so we can write g as

$$g = \sum_i c_i g_i$$

with $c_i \in \mathbb{C}$ and g_i such linearly independent eigenforms. Let $\lambda_{n,i}$ be the eigenvalue for T_n on g_i and λ_n be the eigenvalue for T_n on g, then:

$$\begin{aligned} \lambda_n g &= T_n g = \sum_i c_i T_n g_i = \sum_i c_i \lambda_{n,i} g_i \\ \lambda_n g &= \sum_i c_i \lambda_n g_i \end{aligned}$$

then $\sum_i c_i(\lambda_{n,i} - \lambda_n) g_i = 0$ so, since g_i are linearly independent and at least one $c_i \neq 0$ because $g \neq 0$, we have that $\lambda_{n,i} = \lambda_n$. Now look at any g_i: it has form $g_i(z) = h(dz)$ where h is a newform of some level M dividing N, and let $d \mid \frac{N}{M}$. Then h is also an eigenform for all T_n, $(n, N) = 1$, with the same eigenvalues as g_i, i.e. as f. Consider the q-expansion of f and h:

$$f = \sum_{n=1}^{\infty} a_n q^n \quad h = \sum_{n=1}^{\infty} b_n q^n$$

by the Corollary 2.6.8 we have that a_1 and b_1 are not 0. Then $f - \frac{a_1}{b_1}h$ is an eigenform for all T_n, $(n, N) = 1$, and $a_1 = 0$ for this eigenform. Hence applying Theorem 2.6.7 we have that $f - \frac{a_1}{b_1}h$ is an oldform. Since h is an oldform when viewed as an element of $S_k(N, \chi)$, we conclude that $f \in S_k^{old}(N, \chi)$. But since also $f \in S_k^{new}(N, \chi)$, we must have $f = 0$, a contradiction. Hence g is a newform.
Since the coefficient a_1 of the Fourier expansion of f is not zero, then there is a $\lambda \in \mathbb{C}$ such that the coefficient of q for the form $g - \lambda f$ is 0. So, as above, we can conclude that $g - \lambda f$ is both new and old and hence $g - \lambda f = 0$. □

It is important to remark that the Multiplicity One Theorem usually does not hold in the space of oldforms. Suppose for istance that f is a newform of some level N and let $d > 1$. Then both $f(z)$ and $f(dz)$ are oldforms of level Nd. If f is an eigenform for all T_n, $(n, Nd) = 1$, then so are both $f(z)$ and $f(dz)$, and with the same eigenvalues. But this two forms will be linearly independent if $f \neq 0$.

Theorem 2.6.9. *The space $S_k^{new}(N, \chi)$ has a basis consisting of forms that are eigenforms for all Hecke operators T_n for all $n \in \mathbb{N}$.*

Proof. We already know that $S_k^{new}(N, \chi)$ has a basis $f_1, \ldots, f_t$ consisting of forms that are eigenforms for all Hecke operators T_n, $(n, N) = 1$. Denote by $\lambda_{n,i}$, $i = 1, \ldots, t$ the corresponding eigenvalues. By the above Theorem we know that for $i = 1, \ldots, t$:

$$V_i := \{g \in S_k^{new}(N, \chi) \,|\, T_n\, g = \lambda_{n,i}\, g,\ \forall n \ \text{ such that } \ (n, N) = 1\} \cong \mathbb{C} \cdot f_i$$

Now consider the Hecke operator T_m, $m \in \mathbb{N}$. As T_m commutes with all T_n, $(n, N) = 1$, we see that T_m maps each V_i into itself. But this means that each f_i is in fact an eigenform for all Hecke operators T_m for all $m \in \mathbb{N}$. □

If $f \in S_k^{new}(N, \chi)$ is an eigenform for all T_n, $n \in \mathbb{N}$, then $a_1(f) \neq 0$ so we can normalize f by dividing for a_1.

Definition 2.6.10. *An eigenform for all Hecke operators T_m for all $m \in \mathbb{N}$ with $a_1 = 1$ is called a* normalized newform.

Now suppose $N = 1$ thus $\Gamma_1(N) = SL_2(\mathbb{Z})$. Because of the Petersson product all the T_n are diagonalizable, so $S_k = S_k(\Gamma_1(1))$ has a basis

$$f_1, \ldots, f_d$$

of normalized eigenforms where $d = \dim S_k$. Let $\mathbb{T}_{\mathbb{C}} = \mathbb{T} \otimes_{\mathbb{Z}} \mathbb{C}$, then there is a *canonical* map

$$\mathbb{T}_{\mathbb{C}} \hookrightarrow \mathbb{C}^{\,d}: \quad T \mapsto (\lambda_1, \ldots, \lambda_d)$$

where $f_i|T = \lambda_i f_i$. This map is clearly injective and since $\dim \mathbb{T}_{\mathbb{C}} = d$ then the map is an isomorphism of $\mathbb{C}$-vector spaces. The form

$$v = f_1 + \cdots + f_n$$

generates S_k as a $\mathbb{T}_{\mathbb{C}}$-module. Since v corresponds to the vector $(1, \ldots, 1)$ and $\mathbb{T}_{\mathbb{C}} \cong \mathbb{C}^d$ acts on $S_k \cong \mathbb{C}^d$ componentwise this is just the statement that $\mathbb{C}^d$ is generated by $(1, \ldots, 1)$ as a $\mathbb{C}^d$-module. Thus we have simultaneously that S_k is free of rank 1 over $\mathbb{T}_{\mathbb{C}}$, and that $S_k = \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$ as $\mathbb{T}_{\mathbb{C}}$-modules, hence

$$\mathbb{T}_{\mathbb{C}} \cong \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$$

The isomorphism sends an element of $T \in \mathbb{T}_{\mathbb{C}}$ to $Tv \in S_k$. Since the identification $S_k = \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$ was constructed using the Petersson product it is canonical and since the choice of a normalized eigenbasis $f_1, \ldots, f_d$ is canonical we see that the isomorphism $\mathbb{T}_{\mathbb{C}} \cong \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C})$ is canonical.

Proposition 2.6.11. *$v \in S_k(\mathbb{Q})$, where $S_k(\mathbb{Q})$ is the $\mathbb{Q}$ part of S_k.*

Proof. Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then if f_i is a normalized eigenform so is $\sigma(f_i)$ (it can be seen from the explicit formula). Thus $\sigma(f_1 + \cdots + f_n) = f_1 + \cdots + f_n$ for all σ as desired. □

Let $\mathbb{T}_{\mathbb{Q}} = \mathbb{Q}[\cdots, T_n, \cdots]$ and as usual $\Gamma = \Gamma(1)$. Let $f_1, \ldots, f_d$ be a basis of S_k consisting of normalized eigenforms.

Proposition 2.6.12. *The coefficients of the f_i are totally real algebraic integers.*

Proof. $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ acts on f_i by acting on the coefficients of its q-expansion. From the explicit formula, one can see that the set $\{f_1, \ldots, f_d\}$ is stable under the action of $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$. For any i, $a_n(f_i)$ is an eigenvalue of T_n since $f_i|T_n = a_n(f_i)f_i$, and T_n is self-adjoint so $a_n(f_i)$ must be real. Thus all conjugates of $a_n(f_i)$ are real and there are only finitely many since a conjugate of $a_n(f_i)$ must be $a_n(f_j)$ for some j, $1 \leq j \leq d$. □

Proposition 2.6.13. *The operators $\langle d \rangle$ on $S_k(\Gamma_1(N))$ lie in $\mathbb{Z}[\ldots, T_n, \ldots]$.*

Proof. It is enough to show $\langle p \rangle \in \mathbb{Z}[\ldots, T_n, \ldots]$ because there is a formula relating $\langle p \rangle$ and T_p,

$$p^{k-1}\langle p \rangle = {T_p}^2 - T_{p^2}$$

By Dirichlet's theorem on prime's in arithmetic progression, see VIII.4 of Lang [16], there is another prime q congruent to $p \mod N$. Since p^{k-1} and q^{k-1} are relatively prime there exist integers a and b so that $ap^{k-1} + bq^{k-1} = 1$. Then

$$\langle p \rangle = \langle p \rangle (ap^{k-1} + bq^{k-1}) = a({T_p}^2 - T_{p^2}) + b({T_q}^2 - T_{q^2}).$$

□

Let f be some cuspidal modular form of level N, weight k and Dirichlet character χ with q-expansion $\sum_{n\geq 1} a_n(f)q^n$. The coefficient field of f is defined as $\mathbb{Q}_f = \mathbb{Q}(a_n(f) : (n,N) = 1)$. It has the natural subfield $\mathbf{F}_f = \mathbb{Q}(\frac{a_n(f)^2}{\chi(n)} : (n,N) = 1)$, which we call the twist invariant coefficient field of f, since it is invariant under replacing the modular form f by any of its twists. The behaviour of the Hecke operators under the Petersson scalar product yields the formula

$$\overline{a_p(f)} = \chi(p)^{-1}\, a_p(f)$$

whence $\frac{a_p(f)^2}{\chi(p)} = |a_p(f)|^2$. Thus, $\mathbf{F}_f$ is totally real. It is well known that $\mathbb{Q}_f$ is either a field with complex multiplication, i.e. a totally imaginary quadratic extension of a totally real field, or a totally real field. In particular, if f has trivial nebentypus the latter case occurs by the previous equation. The modular form f is said to have *complex multiplication*, CM, if there exists a Dirichlet character ϵ such that, defining $a_p(f \otimes \epsilon) = a_p(f)\epsilon(p)$, holds

$$a_p(f \otimes \epsilon) = a_p(f)$$

for almost all primes p, i.e. all but finitely many.
A twist of f by a Dirichlet character ϵ is said to be *inner* if there exists a field automorphism $\sigma_\epsilon : \mathbb{Q}_f \to \mathbb{Q}_f$ such that

$$a_p(f \otimes \epsilon) = \sigma_\epsilon(a_p(f))$$

for almost all primes p. For a discussion about inner twists and CM we refer to Ribet [29] and [27].

2.7 Congruences

Let Γ be an arbitrary congruence subgroup of $SL_2(\mathbb{Z})$, and suppose $f \in M_k(\Gamma)$ is a modular form of integer weight k for Γ. Since $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$ for some integer N, the form f has a Fourier expansion in nonnegative powers of $q^{\frac{1}{N}}$. For a rational number n, let $a_n(f)$ be the coefficient of q^n in the Fourier expansion of f. Put

$$ord_q(f) = \min\{\, n \in \mathbb{Q} : a_n \neq 0\}$$

where by convention we take $\min \emptyset = +\infty$, so $ord_q(0) = +\infty$.

Let

$$j = \frac{1}{q} + 744 + 196884\, q + \ldots$$

be the j-function, which is a weight 0 modular function that is holomorphic except for a simple pole at ∞ and has integer Fourier coefficients.

Lemma 2.7.1. *Suppose g is a weight 0 level 1 modular function that is holomorphic except possibly with a pole of order n at ∞. Then g is a polynomial in j of degree at most n. Moreover, the coefficients of this polynomial lie in the ideal I of the ring of integer $\mathcal{O}_g$ of $\mathbb{Q}_g$, $I \subseteq \mathcal{O}_g$, generated by the coefficients $a_m(g)$ with $m \leq 0$.*

Proof. If $n = 0$, then $g \in M_0(SL_2(\mathbb{Z})) = \mathbb{C}$, so g is constant with constant term in I, so the statement is true.
Next suppose $n > 0$ and the lemma has been proved for all functions with smaller order poles. Let $\alpha = a_n(g)$, and note that

$$ord_q(g - \alpha j^n) = ord_q\big(g - \alpha \cdot (\frac{1}{q} + 744 + 196884\, q + \dots)^n\big) > -n$$

Thus by induction $h = g - \alpha j^n$ is a polynomial in j of degree less than n with coefficients in the ideal generated by the coefficients $a_m(g)$ with $m \leq 0$. It follows that $g = \alpha \cdot j^n - h$ satisfies the conclusion of the lemma. □

2.7.1 Congruences for Modular Forms

If $\mathcal{O}$is the ring of integers of a number field, $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}$, and $f = \sum a_n q^n \in \mathcal{O}\left[\left[q^{1/N}\right]\right]$ for some integer N, let

$$ord_{\mathfrak{m}}(f) = ord_q(f \mod \mathfrak{m}) = \min\{n \in \mathbb{Q} : a_n \notin \mathfrak{m}\}$$

Note that $ord_{\mathfrak{m}}(fg) = ord_{\mathfrak{m}}(f) + ord_{\mathfrak{m}}(g)$.
For simplicity, in this section we will use the following notation: for $\gamma \in GL_2(\mathbb{Q})$ we define

$$(f|[\gamma]_k)(z) = det(\gamma)^{k-1}(cz + d)^k f(\gamma z)$$

Sturm Theorem. *Let $\mathfrak{m}$ be a maximal ideal in the ring of integers $\mathcal{O}$of a number field $\boldsymbol{K}$, and let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ of index m and level N. Suppose $f \in M_k(\Gamma, \mathcal{O})$ is a modular form and*

$$ord_{\mathfrak{m}}(f) > \frac{k\,m}{12}$$

or $f \in S_k(\Gamma, \mathcal{O})$ is a cusp form and

$$ord_{\mathfrak{m}}(f) > \frac{k\,m}{12} - \frac{m-1}{N}$$

Then $f \equiv 0(\mod \mathfrak{m})$.

Proof. Let's proceede analyzing first the case $\Gamma = SL_2(\mathbb{Z})$ and then the general case with Γ arbitrary.

- Case 1: First we assume $\Gamma = SL_2(\mathbb{Z})$.

Let

$$\Delta = q + 24\,q^2 + \cdots \in S_{12}(SL_2(\mathbb{Z}), \mathbb{Z})$$

be the Δ function. Since $ord_{\mathfrak{m}}(f) > k/12$, we have $ord_{\mathfrak{m}}(f^{12}) > k$. We have

$$ord_q(f^{12} \cdot \Delta^{-k}) = 12 \cdot ord_q(f) - k \cdot ord_q(\Delta) \geq -k$$

since f is holomorphic at infinity and Δ has a zero of order 1. Also

$$ord_{\mathfrak{m}}(f^{12} \cdot \Delta^{-k}) = ord_{\mathfrak{m}}(f^{12}) - k \cdot ord_{\mathfrak{m}}(\Delta) > k - k = 0$$

Combining the previous results we have that

$$f^{12} \cdot \Delta^{-k} = \sum_{n \geq -k} b_n q^n$$

with $b_n \in \mathcal{O}$ and $b_n \in \mathfrak{m}$ if $n \leq 0$. By Lemma 2.7.1,

$$f^{12} \cdot \Delta^{-k} \in \mathfrak{m}[j]$$

is a polynomial in j of degree at most k with coefficients in $\mathfrak{m}$. Thus

$$f^{12} \in \mathfrak{m}[j] \cdot \Delta^k$$

so since the coefficients of Δ are integers, every coefficient of f^{12} is in $\mathfrak{m}$. Thus $ord_{\mathfrak{m}}(f^{12}) = +\infty$, hence $ord_{\mathfrak{m}}(f) = +\infty$, so $f \equiv 0 \mod \mathfrak{m}$, as claimed.

- Case 2: Γ Arbitrary.

Let N be such that $\Gamma(N) \subset \Gamma$, so also $f \in M_k(\Gamma(N))$. If $g \in M_k(\Gamma(N))$ is arbitrary, then because $\Gamma(N)$ is a normal subgroup of $SL_2(\mathbb{Z})$, we have that for any $\gamma \in \Gamma(N)$ and $\delta \in SL_2(\mathbb{Z})$:

$$(g|[\delta]_k)|[\gamma]_k = g|[\delta\gamma]_k = g|\left[\gamma'\delta\right]_k = g|\left[\gamma'\right]_k|[\delta]_k = g|[\delta]_k$$

where $\gamma' \in \Gamma(N)$. Thus for any $\delta \in SL_2(\mathbb{Z})$, we have that $g|[\delta]_k \in M_k(\Gamma(N))$, so $SL_2(\mathbb{Z})$ acts on $M_k(\Gamma(N))$. It is a standard fact about modular forms that $M_k(\Gamma(N))$ has a basis with Fourier expansions in $\mathbb{Z}[\zeta_N]\left[\left[q^{1/N}\right]\right]$, (where ζ_N is an N-th rooth of unity) and that the action of $SL_2(\mathbb{Z})$ on $M_k(\Gamma(N))$ preserves

$$M_k(\Gamma(N), \mathbb{Q}(\zeta_N)) = M_k(\Gamma(N)) \cap (\mathbb{Q}(\zeta_N)\left[\left[q^{1/N}\right]\right])$$

and the cuspidal subspace $S_k(\Gamma(N), \mathbb{Q}(\zeta_N))$. In particular, for any $\gamma \in SL_2(\mathbb{Z})$,

$$f|[\gamma]_k \in M_k(\Gamma(N), \mathbf{K}(\zeta_N))$$

Moreover, the denominators of $f|[\gamma]_k$ are bounded, since f is an $\mathcal{O}[\zeta_N]$-linear combination of a basis for $M_k(\Gamma(N), \mathbb{Z}[\zeta_N])$, and the denominators of $f|[\gamma]_k$ divide the product of the denominators of the images of each of these basis vectors under $[\gamma]_k$.
Let $\mathbf{L} = \mathbf{K}(\zeta_N)$. Let $\mathfrak{M}$ be a prime of $\mathcal{O}_\mathbf{L}$ that divides $\mathfrak{m} \otimes_\mathbb{Z} \mathcal{O}_\mathbf{L}$. We will now show that for each $\gamma \in SL_2(\mathbb{Z})$, the Chinese remainder theorem implies that there is an element $A_\gamma \in \mathbf{L}^*$ such that

$$A_\gamma \cdot f|[\gamma]_k \in M_k(\Gamma(N), \mathcal{O}_\mathbf{L}) \qquad \text{and} \qquad ord_\mathfrak{M}(A_\gamma \cdot f|[\gamma]_k) < \infty$$

How to do this: first find $A \in \mathbf{L}^*$ such that $A \cdot f|[\gamma]_k$ has coefficients in $\mathcal{O}_\mathbf{L}$. Choose $\alpha \in \mathfrak{M}$ with $\alpha \notin \mathfrak{M}^2$, and find a negative power α^t such that $\alpha^t \cdot A \cdot f|[\gamma]_k$ has $\mathfrak{M}$-integral coefficients and finite valuation. This is possible because we assumed that f is nonzero. Use the Chinese remainder theorem to find $\beta \in \mathcal{O}_\mathbf{L}$ such that $\beta \equiv 1 (\mod \mathfrak{M})$ and $\beta \equiv 0 (\mod \mathfrak{P})$ for each prime $\mathfrak{P} \neq \mathfrak{M}$ that divides (α). Then for some s we have

$$\beta^s \cdot \alpha^t \cdot A \cdot f|[\gamma]_k = A_\gamma \cdot f|[\gamma]_k \in M_k(\Gamma(N), \mathcal{O}_\mathbf{L})$$

and $ord_\mathfrak{M}(A_\gamma \cdot f|[\gamma]_k) < \infty$. We have.

$$SL_2(\mathbb{Z}) = \bigcup_{i=1}^{m} \Gamma \gamma_i$$

with $\gamma_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and let

$$F = f \cdot \prod_{i=2}^{m} A_{\gamma_i} \cdot f|[\gamma_i]_k$$

Then $F \in M_{km}(SL_2(\mathbb{Z}))$ by construction and since $\mathfrak{M} \cap \mathcal{O}_\mathbf{K} = \mathfrak{m}$, we have $ord_\mathfrak{M}(f) = ord_\mathfrak{m}(f)$, so

$$ord_\mathfrak{M}(F) \geq ord_\mathfrak{M}(f) = ord_\mathfrak{m}(f) > \frac{k\,m}{12}$$

Thus we can apply case 1 to conclude that

$$ord_\mathfrak{M}(F) = +\infty$$

Thus

$$\infty = ord_\mathfrak{M}(F) = ord_\mathfrak{m}(f) + \sum_{i=2}^{m} ord_\mathfrak{M}(A_{\gamma_i} \cdot f|[\gamma_i]_k)$$

so $ord_{\mathfrak{m}}(f) = +\infty$, because $ord_{\mathfrak{M}}(A_\gamma \cdot f|\,[\gamma]_k) < \infty$ and so for each γ_i. When f is a cusp form, since $\bullet|\,[\gamma]_k$ preserves cusp forms,

$$ord_{\mathfrak{M}}(A_{\gamma_i} \cdot f|\,[\gamma]_i) \geq \frac{1}{N} \qquad \forall i$$

Thus:

$$ord_{\mathfrak{M}}(F) \geq ord_{\mathfrak{M}}(f) + \frac{m-1}{N} = ord_{\mathfrak{m}}(f) + \frac{m-1}{N} > \frac{k\,m}{12} \tag{2.1}$$

since now we are merely assuming that

$$ord_{\mathfrak{m}}(f) > \frac{k\,m}{12} - \frac{m-1}{N}$$

Thus we again apply case 1 to conclude that $ord_{\mathfrak{M}}(F) = +\infty$, and using (2.1) conclude that $ord_{\mathfrak{m}}(f) = +\infty$. □

Corollary 2.7.2. *Let $\mathfrak{m}$ be a maximal ideal in the ring of integers $\mathcal{O}$ of a number field. Suppose $f, g \in M_k(\Gamma, \mathcal{O})$ are modular forms of level N, such that called $m = [SL_2(\mathbb{Z}) : \Gamma]$, we have $a_n(f) \equiv a_n(g)$ (mod $\mathfrak{m}$) for all*

$$n \leq \begin{cases} \frac{k\,m}{12} - \frac{m-1}{N} & \text{if } f - g \in S_k(\Gamma, \mathcal{O}) \\ \\ \frac{k\,m}{12} & \text{otherwise} \end{cases}$$

then $f \equiv g$ (mod $\mathfrak{m}$).

The proof follows directly from the theorem.

Corollary (Buzzard). *Let $\mathfrak{m}$ be a maximal ideal in the ring of integers $\mathcal{O}$ of a number field. Suppose $f, g \in M_k(\Gamma_1(N), \epsilon, \mathcal{O})$ are modular forms with Dirichlet character $\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$ and assume that*

$$a_n(f) \equiv a_n(g) \mod \mathfrak{m} \qquad \text{for all} \quad n \leq \frac{k\,m}{12}$$

where

$$m = [SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \cdot \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

Then $f \equiv g$(mod $\mathfrak{m}$).

Proof. Let $h = f - g$ and let $r = \frac{k\,m}{12}$, so $ord_{\mathfrak{m}}(h) > r$ and let s be the order of the Dirichlet character. Then $h^s \in M_{ks}(\Gamma_0(N), \mathcal{O})$ and

$$ord_{\mathfrak{m}}(h^s) > sr = \frac{k\,m\,s}{12}$$

By Theorem 2.7.1, we have $ord_{\mathfrak{m}}(h^s) = \infty$, so $ord_{\mathfrak{m}}(h) = \infty$. It follows that $f \equiv g$(mod $\mathfrak{m}$). □

2.7.2 Congruences for Newforms

Sturm Theorem for newforms. *Let N be a square-free positive integer, and suppose f and g are two newforms in $S_k(\Gamma_1(N), \epsilon, \mathcal{O})$, where $\mathcal{O}$is the ring of integers of a number field, and suppose that $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}$. Let I be an arbitrary subset of the prime divisors of N. If $a_p(f) = a_p(g)$ for all $p \in I$,and*

$$a_p(f) \equiv a_p(g) \mod \mathfrak{m}$$

for all primes

$$p \leq \frac{k \cdot [SL_2(\mathbb{Z}) : \Gamma_0(N)]}{12 \cdot 2^{\#I}}$$

then $f \equiv g(\mod \mathfrak{m})$.

Buzzard and Stein have proved a different result which does not require the level be square free.

Theorem 2.7.3. *Let $N > 4$ be any integer, and suppose f and g are two normalized eigenforms in $S_k(\Gamma_1(N), \epsilon, \mathcal{O})$, where $\mathcal{O}$is the ring of integers of a number field, and suppose that $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}$. Let I be the set of prime divisors of N that do not divide $\frac{N}{cond(\epsilon)}$. If*

$$a_p(f) \equiv a_p(g) (\mod \mathfrak{m})$$

for all primes $p \in I$ and for all primes

$$p \leq \frac{k \cdot [SL_2(\mathbb{Z}) : \Gamma_0(N)]}{12 \cdot 2^{\#I}}$$

then $f \equiv g(\mod \mathfrak{m})$.

For the proof, see Lemma 1.4 and Corollary 1.7 in [2] by Buzzard and Stein.

2.7.3 Dimension fomula

Theorem 2.7.4. *Let Γ be a congruence subgroup, and let $k \in \mathbb{Z}$. If $k < 0$ then $M_k(\Gamma) = 0$, if $k = 0$ then $M_k(\Gamma) = \mathbb{C}$, for $k \in \mathbb{N}$ the space $M_k(\Gamma)$ is a finite-dimensional complex vector space.*

Proof. If $f \in M_K(\Gamma)$, where $k < 0$, then as in the proof of Sturm Theorem, we can construct an element

$$F = \prod_{i=1}^{n} (f|_k \gamma_i) \in M_{kn}(SL_2(\mathbb{Z}))$$

since $kn < 0$ we then know that $F = 0$, hence at least one $f|_k\gamma_i$ is 0, hence f is 0.

Suppose that $f \in M_0(\Gamma)$ with q-expansion $f = \sum_n a_n q^n$. Then $f - a_0 \in M_0(\Gamma)$ and since $ord_q(f - a_0) > 0$ we have by Sturm Theorem $f - a_0 = 0$ so the statement follows.
Let now $k \in \mathbb{N}$. If $\Gamma \supseteq \Gamma(N)$ then $M_k(\Gamma) \subseteq M_k(\Gamma(N))$ so it will be enough to prove that any space $M_k(\Gamma(N))$ is finite-dimensional. Define a linear map:

$$\begin{aligned} M_k(\Gamma(N)) &\to \mathbb{C}^{d+1} \\ f = \sum_n a_n q^n &\mapsto (a_0, \ldots, a_d) \end{aligned}$$

where d is the integer part of $N \cdot \frac{k[SL_2(\mathbb{Z}):\Gamma(N)]}{12}$. This is clearly a linear map. By Sturm Theorem and its Corollaries we have that the kernel of this map is 0, i.e., it is an injection. So, not only can we deduce $\dim M_k(\Gamma(N)) < \infty$, but we have in fact an upper bound on the dimension:

$$\dim M_k(\Gamma(N)) \leq d + 1.$$

□

Using Riemmann-Roch Theorem, one can give an explicit formula for computing dimensions, for a proof look at Diamond [5] or Shimura [34].

Proposition 2.7.5. *Let $k \in \mathbb{Z}$ and E_k the Eisenstein serie of weight k, then:*

- $M_k(SL_2(\mathbb{Z})) = \mathbb{C} \cdot E_k$ *for* $k \in \{4, 6, 8, 10, 14\}$;
- *If* $k < 12$ *or* $k = 14$ *then* $S_k(SL_2(\mathbb{Z})) = 0$, *we have that* $S_1 2(SL_2(\mathbb{Z})) = \mathbb{C} \cdot \Delta$ *and* $S_k(SL_2(\mathbb{Z})) = \Delta \cdot M_{k-12}(SL_2(\mathbb{Z}))$ *for* $k \geq 16$;
- *for* $k \geq 4$:
$$M_k(SL_2(\mathbb{Z})) = S_k(SL_2(\mathbb{Z})) \oplus \mathbb{C} \cdot E_k.$$

Note that $M_0(\Gamma)$ consists of modular functions that are holomorphic on $\mathbb{H}$ and at the cusps, and therefore define holomorphic functions on $\Gamma\backslash\mathbb{H}^*$. Because $\Gamma\backslash\mathbb{H}^*$ is compact, such a function is constant, and so $M_0(\Gamma) = \mathbb{C}$. The product of a modular form of weight k with a modular form of weight ℓ is a modular form of weight $k + \ell$. Therefore,

$$M(\Gamma) = \bigoplus_k M_k(\Gamma)$$

is a graded ring.

Theorem 2.7.6. *The dimension of $M_k(\Gamma)$ is given by:*

$$dim_{\mathbb{C}}(M_k(\Gamma)) = \begin{cases} 0 & \text{if } k \leq 1 \\ 1 & \text{if } k = 0 \\ (2k-1)(g-1) + \nu_\infty k + \sum_P \left\lfloor k(1 - \frac{1}{e_P}) \right\rfloor & \text{if } k \geq 1 \end{cases}$$

where g is the genus of $X(\Gamma)$; ν_∞ is the number of inequivalent cusps; the last sum is over a set of representatives for the the elliptic points P of Γ; e_P is the order of the stabilizer of P in the image $\bar{\Gamma}$ of Γ in $\Gamma(1)/\{\pm I\}$; and $\left\lfloor k(1 - \frac{1}{e_P}) \right\rfloor$ is the integer part of $k(1 - \frac{1}{e_P})$.

Chapter 3

Galois Representations and Modular Forms

3.1 Galois Representations

For this chapter let $\ell \in \mathbb{Z}$ denote a prime number.

Definition 3.1.1. *An* ℓ-adic integer *is a sequence*

$$\alpha = (a_1, a_2, a_3, \dots)$$

with $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ *and* $a_{n+1} \equiv a_n \mod \ell^n\mathbb{Z}$ *for each* $n \in \mathbb{Z}^+$. *The ring of* ℓ*-adic integers, where the operations are componentwise addition and multiplication, is denoted* $\mathbb{Z}_\ell$.

Thus each entry a_n in an ℓ-adic integer determines the preceding entries a_{n-1} down to a_1, while the entry a_{n+1} to its right is one of its ℓ lifts from $\mathbb{Z}/\ell^n\mathbb{Z}$ to $\mathbb{Z}/\ell^{n+1}\mathbb{Z}$. This makes the ℓ-adic integers a case of inverse limit construction: the inverse limit of the rings $\mathbb{Z}/\ell^n\mathbb{Z}$ for $n \in \mathbb{Z}^+$,

$$\mathbb{Z}_\ell = \varprojlim_n \{\mathbb{Z}/\ell^n\mathbb{Z}\}$$

It is possible to prove that the ring $\mathbb{Z}_\ell$ is an integral domain. The natural map

$$\mathbb{Z} \to \mathbb{Z}_\ell \qquad a \mapsto (a + \ell\mathbb{Z}, a + \ell^2\mathbb{Z}, a + \ell^3\mathbb{Z}, \dots)$$

is a ring injection, so we view $\mathbb{Z}$as a subring of $\mathbb{Z}_\ell$. The map induces a natural isomorphism

$$\mathbb{Z}/\ell\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_\ell/\ell\mathbb{Z}_\ell \qquad a + \ell\mathbb{Z} \mapsto a + \ell\mathbb{Z}_\ell$$

so we identify $\mathbb{Z}/\ell\mathbb{Z}$ and $\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell$. As the inverse limit of a system of finite rings, $\mathbb{Z}_\ell$ is profinite. The multiplicative group of units in $\mathbb{Z}_\ell$ is

$$\mathbb{Z}_\ell^* = \{(a_1, a_2, a_3, \dots) \in \mathbb{Z}_\ell : a_n \in (\mathbb{Z}/\ell^n\mathbb{Z})^* \ \ \forall n\}.$$

Every ℓ-adic integer α with $a_1 \neq 0$ in $\mathbb{Z}/\ell\mathbb{Z}$ is invertible.
The ideal $\ell\mathbb{Z}_\ell$ is the unique maximal ideal of $\mathbb{Z}_\ell$, and $\mathbb{Z}_\ell^* = \mathbb{Z}_\ell - \ell\mathbb{Z}_\ell$. The ideal structure of $\mathbb{Z}_\ell$ is $\mathbb{Z}_\ell \supset \ell\mathbb{Z}_\ell \supset \ell^2\mathbb{Z}_\ell \supset \dots$.

Definition 3.1.2. *The field $\mathbb{Q}_\ell$ of ℓ-adic numbers is the field of quotients of $\mathbb{Z}_\ell$.*

Let $\mathbf{K}$ be any number field, not necessarily Galois over $\mathbb{Q}$, and let $\mathcal{O}_\mathbf{K}$ be its ring of integers. The factorization of $\ell\mathcal{O}_\mathbf{K}$ into maximal ideals, as we have seen in Chapter 1, is:

$$\ell\mathcal{O}_\mathbf{K} = \prod_{\lambda|\ell} \lambda^{e_\lambda}$$

where the notation $\lambda \mid \ell$ means that λ lies over the rational prime ℓ. Similarly to $\mathbb{Z}_\ell$ and $\mathbb{Q}_\ell$, for each λ the ring of λ-adic integers is the inverse limit

$$\mathcal{O}_{\mathbf{K},\lambda} = \varprojlim_n \{\mathcal{O}_\mathbf{K}/\lambda^n\}$$

and then the field of λ-adic numbers is the field of quotients $\mathbf{K}_\lambda$ of $\mathcal{O}_{\mathbf{K},\lambda}$. We may view $\mathbb{Z}_\ell$ as a subring of $\mathcal{O}_{\mathbf{K},\lambda}$ and $\mathbb{Q}_\ell$ as a subfield of $\mathbf{K}_\lambda$. Define the residue degree f_λ to be $[\mathbf{k}_\lambda : \mathbf{F}_\ell]$ where $\mathbf{k}_\lambda = \mathcal{O}_\mathbf{K}/\lambda$ and $\mathbf{F}_\ell = \mathbb{Z}/\ell\mathbb{Z}$. Then it is possible to prove that the containments $\mathbb{Z}_\ell \subset \mathcal{O}_{\mathbf{K},\lambda}$ and $\mathbb{Q}_\ell \subset \mathbf{K}_\lambda$ are equalities when $e_\lambda f_\lambda = 1$, and in fact $[\mathbf{K}_\lambda : \mathbb{Q}_\ell] = e_\lambda f_\lambda$.
It is possible to show that there is a ring isomorphism

$$\mathbf{K} \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} \mathbf{K}_\lambda.$$

In fact, we have:

$$\mathcal{O}_\mathbf{K} \otimes \mathbb{Z}_\ell \cong \varprojlim_n \{\mathcal{O}_\mathbf{K} \otimes \mathbb{Z}/\ell^n\mathbb{Z}\} \cong \varprojlim_n \{\mathcal{O}_\mathbf{K}/\ell^n\mathcal{O}_\mathbf{K}\}.$$

But $\mathcal{O}_\mathbf{K}/\ell^n\mathcal{O}_\mathbf{K} = \mathcal{O}_\mathbf{K}/\prod_\lambda \lambda^{ne_\lambda} \cong \prod_\lambda \mathcal{O}_\mathbf{K}/\lambda^{ne_\lambda}$. Thus

$$\mathcal{O}_\mathbf{K} \otimes \mathbb{Z}_\ell \cong \varprojlim_n \left\{ \prod_\lambda \mathcal{O}_\mathbf{K}/\lambda^{ne_\lambda} \right\} \cong \prod_\lambda \varprojlim_n \{\mathcal{O}_\mathbf{K}/\lambda^{ne_\lambda}\} \cong \prod_\lambda \mathcal{O}_{\mathbf{K},\lambda}$$

and this gives

$$\mathbf{K} \otimes_\mathbb{Q} \mathbb{Q}_\ell \cong \mathcal{O}_\mathbf{K} \otimes \mathbb{Q}_\ell \cong \mathcal{O}_\mathbf{K} \otimes \mathbb{Z}_\ell \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \prod_\lambda (\mathcal{O}_{\mathbf{K},\lambda} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \prod_\lambda \mathbf{K}_\lambda.$$

Each $\mathbf{K}_\lambda$ acquires a topology as a finite-dimensional vector space over $\mathbb{Q}_\ell$.

Definition 3.1.3. *Let d be a positive integer. A d-dimensional ℓ-adic Galois representation is a continuous homomorphism*

$$\rho : G_{\mathbb{Q}} \to GL_d(\boldsymbol{L})$$

where $\boldsymbol{L}$ is a finite extension field of $\mathbb{Q}_\ell$. If $\rho' : G_{\mathbb{Q}} \to GL_d(\boldsymbol{L})$ is another such representation and there is a matrix $A \in GL_d(\boldsymbol{L})$ such that $\rho'(\sigma) = A^{-1}\rho(\sigma)A$ for all $\sigma \in G_{\mathbb{Q}}$ then ρ and ρ' are said equivalent. *Equivalence is denoted by $\rho \sim \rho'$.*

We state without proof that every finite extension field $\mathbf{L}$ of $\mathbb{Q}_\ell$ takes the form $\mathbf{K}_\lambda$ for some number field $\mathbf{K}$ and maximal ideal $\lambda \mid \ell$ of $\mathcal{O}_{\mathbf{K}}$, and that for such $\mathbf{L}$ the ring $\mathcal{O}_{\mathbf{L}} = O_{\mathbf{K},\lambda}$ is well defined independently of $\mathbf{K}$ and λ. The ring $\mathcal{O}_{\mathbf{L}}$ is a lattice in $\mathbf{L}$, i.e., there is $\mathbb{Z}_\ell$-basis of $\mathcal{O}_{\mathbf{L}}$ that is also a $\mathbb{Q}_\ell$-basis of $\mathbf{L}$.

Given a Galois representation ρ we naturally want to know values $\rho(\sigma)$ for $\sigma \in G_{\mathbb{Q}}$. In particular we want to evaluate ρ at Frobenius elements. But each $\mathrm{Frob}_{\mathfrak{p}}$ is defined only up to the absolute inertia group $I_{\mathfrak{p}}$, recall the sequence 1.3, so the notion of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is well defined if and only if $I_{\mathfrak{p}} \subseteq \ker(\rho)$. Furthermore, if $\mathfrak{p}$ and $\mathfrak{p}'$ lie over the same rational prime ℓ then the inertia groups $I_{\mathfrak{p}}$ and $I'_{\mathfrak{p}}$ are conjugate in $G_{\mathbb{Q}}$, so the condition $I_{\mathfrak{p}} \subseteq \ker(\rho)$ depends only on the underlying prime p since $ker(\rho)$ is normal in $G_{\mathbb{Q}}$. Although $\rho(\mathrm{Frob}_{\mathfrak{p}})$ does depend on the choice of $\mathfrak{p}$ over ℓ when it is defined, its characteristic polynomial depends only on the conjugacy class of $\rho(\mathrm{Frob}_{\mathfrak{p}})$ and therefore only on p.

Definition 3.1.4. *Let ρ be a Galois representation and let ℓ be prime. Then ρ is* unramified *at ℓ if $I_{\mathfrak{p}} \subseteq \ker(\rho)$ for any maximal ideal $\mathfrak{p}$ lying over ℓ.*

Now let us go back to modular representations i.e. representation ρ such that $\exists f$ modular form such that $\rho = \rho_f$ an ℓ-adic Galois representation where $\mathbf{L} = \mathbb{Q}_{f,\lambda}$ where $\mathbb{Q}_f$ is the number field associated to f. Let us consider modular representations in details.

Let $f \in S_2(\Gamma_0(N))$ be a newform of weight 2 on $\Gamma_0(N)$, that is a normalized eigenform for the whole Hecke algebra which is new of level N. We assume that f does not have complex multiplication or inner twists. The newform has a Fourier developement: $f = \sum a_n q^n$, where $q = e^{2\pi i}$, let $\mathbb{Q}_f$ be the number field generated by the Fourier coefficients $\{a_n\}$, $\mathbb{Q}_f = \mathbb{Q}(\{a_n\})$ and $\mathcal{O}_f$ its ring of integer as usual.
For every prime ℓ put $\mathcal{O}_\ell = \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathbb{Q}_{f,\ell} = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
Serre-Deligne and Eichler-Shimura found a way to associate to f a family of ℓ-adic representations as we will see shortly in this Chapter. Let ℓ be a

prime number, one can associate to f a representation

$$\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_{f,\ell})$$

unramified at all primes $p \nmid \ell N$.

Lemma 3.1.5. *ρ_ℓ is equivalent to a representation which takes values in $GL_2(\mathcal{O}_\ell)$, where $\mathcal{O}_\ell$ is the ring of integers of $\mathbb{Q}_{f,\ell}$.*

Proof. View $GL_2(\mathbb{Q}_{f,l})$ as the group of automorphisms of a 2 dimensional $\mathbb{Q}_{f,l}$-vector space V. A lattice is a free $\mathcal{O}_\ell$-module of rank 2 such that $L \otimes Q_{f,l} \cong V$. It suffices to find an $\mathcal{O}_\ell$-lattice L in V which is invariant under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. For then the matrices of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ with respect to a basis of V consisting of vectors from L will have coefficients in $\mathcal{O}_\ell$.
Choose any lattice $L_0 \subset V$. Since L_0 is discrete and $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is compact, it is possible to see that the set of lattices gL_0 with $g \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ is finite. Let $L = \sum gL_0$ be the sum of the finitely many conjugates of L_0, then L is Galois invariant. □

Let us suppose we are considering a representation ρ from a group G to the endomorphisms of some vector space W, or a free module M if we are working over a ring instead of a field. A subspace W' of W is said to be *invariant* under ρ if ρ takes W' into itself. If W' is invariant, then ρ induces representations on both W' and W/W'.

Definition 3.1.6. *An* irreducible representation *ρ is a representation where the only invariant subspaces are 0 and W. A* semi-simple *representation ρ is a representation where for every invariant subspace W' there is a complementary invariant subspace W'', such that it is possible to write ρ as the direct sum of $\rho|_{W'}$ and $\rho|_{W''}$.*

Another way to say this is that if W' is an invariant subspace then we get a short exact sequence

$$0 \to \rho|_{W'} \to \rho \to \rho|_{W/W'} \to 0$$

Furthermore ρ is semi-simple if and only if every such sequence splits. Note that irreducible representations are semi-simple. One other fact is that semi-simple Galois representations are uniquely determined (up to isomorphism class) by their trace and determinant by Brauer-Nesbitt Theorem, for a reference Knapp [13].

Now, since in the case we are doing, $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is compact, it follows that the image of any Galois representation ρ into $GL_2(\mathbb{Q}_{f,\ell})$ is compact. Thus we can conjugate it into $GL_2(\mathcal{O}_\ell)$.

Now that we have a representation into $GL_2(\mathcal{O}_\ell)$, we can reduce to get a representation $\overline{\rho_\lambda}$ to $GL_2(\mathbf{F}_\lambda)$ where $\mathbf{F}_\lambda$ is the residue field for λ prime in $\mathbb{Q}_f$. In fact from the decomposition $\mathbb{Q}_{f,\ell} \cong \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$ and $\mathcal{O}_\ell \cong \prod_{\lambda|\ell} \mathcal{O}_\lambda$ we obtain a decomposition of ρ_ℓ as a direct sum of representations for

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_\lambda) \subseteq GL_2(\mathbb{Q}_{f,\lambda})$$

Now λ is a prime in $\mathbb{Q}_f$, so we can consider the reduction $\overline{\rho_\lambda}$ of ρ_λ, obatined composing ρ_λ with the reduction map $GL_2(\mathcal{O}_\lambda) \to GL_2(\mathbf{F}_\lambda)$, where $\mathbf{F}_\lambda$ is the residue field for λ. This reduced representation is not uniquely determined by ρ, since we had a choice of conjugators. However, the trace and determinant are invariant under conjugation, so the trace and determinant of the reduced representation are uniquely determined by ρ.

If ρ is not semi-simple, then one can define from ρ a semi-simple representation, unique up to isomorphism.
Indeed, let $\{W_i\}$ be a finite Jordan-Hölder composition series of W: $\{0\} = W_0 \subset W_1 \subset \cdots \subset W_n = W$ where all inclusions are strict, and W_i is a maximal G-submodule of W_{i+1}. Consider $Gr(W) = \oplus_{i \geq 0} W_{i+1}/W_i$, which carries a G-action, induced from the one on W: this representation is semi-simple by construction, and has the same character and characteristic polynomials as ρ. It is called the semi-simplification of ρ.

Now we will explain the fundamental results of Deligne-Serre and Eichler-Shimura that allow us to consider Galois representations: in the first case we have the proof of existence of

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$$

while in the second case we have the construction for weight 2 modular forms of

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_\lambda) \subseteq GL_2(\mathbb{Q}_{f,\lambda})$$

3.2 Deligne-Serre Theorem

Theorem 3.2.1. *Let $N \geq 1$ be an integer, ϵ a Dirichlet character $\mod N$ such that $\epsilon(-1) = -1$, and f a modular form in $M_1(\Gamma_0(N), \epsilon)$, not identically zero. Suppose that f is an eigenfunction of T_p, $p \nmid N$, with eigenvalues a_p. Then there exists a linear representation*

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{C})$$

which is unramified outside N, i.e. it may ramify in p prime if $p \mid N$, such that

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\mathfrak{p})) = a_p \quad \textit{and} \quad \det(\rho(\mathrm{Frob}_\mathfrak{p})) = \epsilon(p) \; \forall p \nmid N$$

This representation is irreducible if f is cuspidal.

The reader should refer to the original paper of Serre-Deligne [4]. We will recall only the main steps. The starting point is the following theorem due to Deligne:

Theorem 3.2.2. *Let f be a weight $k \geq 2$ cuspidal modular form, with nebentypus χ, level q, Hecke eigenvector with eigenvalues a_p for $(p,q) = 1$. Let $\boldsymbol{K}$ be a number field containing $\mathbb{Q}_f$, and let λ be a finite prime of $\boldsymbol{K}$ of residue characteristic ℓ. Then there exists an irreducible λ-adic Galois representation, unique up to isomorphism, $\rho : G_{\mathbb{Q}} \to GL_2(\boldsymbol{K}_\lambda)$, unramified away from $q\,\ell$, such that at any prime p not dividing $q\,\ell$:*

$$\mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) = a_p \quad \textit{and} \quad \det(\rho(\mathrm{Frob}_{\mathfrak{p}})) = p^{k-1}\chi(p)$$

Once Deligne-Serre is proven, the above is true for weight one as well, by choosing an algebraic embedding $\iota : \mathbf{K}_\lambda \to \mathbb{C}$. The uniqueness statement follows from *Čebotarev* density Theorem.

Step 1: Reduction modulo a prime. Let us consider the following preliminary result:

Theorem 3.2.3. *Let f be a weight $k \geq 1$ cuspidal modular form, with nebentypus χ, level q, Hecke eigenvector with eigenvalues a_p for $p \nmid q$. Let $\boldsymbol{K}$ be a number field containing $\mathbb{Q}_f$, and let λ be a finite prime of $\boldsymbol{K}$ of residue characteristic ℓ and let $k_f = \mathbb{F}_\ell(a_p, \chi(p); p \nmid q)$. Then there exists a semi-simple Galois representation, unique up to isomorphism, $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(k_f)$, unramified away from $q\,\ell$, such that at any prime p not dividing $q\,\ell$:*

$$\mathrm{Tr}(\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}})) \equiv a_p \mod \lambda \qquad \det(\bar{\rho}(\mathrm{Frob}_{\mathfrak{p}}) \equiv p^{k-1}\chi(p) \mod \lambda$$

It is possible to strengthen the theorem, as it is actually only necessary that f be a Hecke eigenform modulo λ: see Deligne-Serre.

(1) If f is a weight one form, multiplication of f by a weight Eisentein series in $M_m(SL_2(\mathbb{Z}))$ produces a weight $m+1$ modular form. By considering the normalized Eisenstein series:

$$E_m(z) = 1 - \frac{b_m}{2m}\sum_{n=1}^{\infty}\sigma_{m-1}(n)\,e(nz)$$

the Bernouilli numbers b_m satisfy congruence relations (Clausenvon Staudt theorem): $\ell\, b_m \equiv 1 \mod (\ell)$ if $(\ell - 1) \mid m$ (cf. Borevich-Shafarevitch, chap. 5), so $f\,E_m \equiv f \mod \lambda$ for such a m.

(2) Re-establish good Hecke behaviour: there exists a weight $m+1$ modular form f', eigenform at good primes, defined over some extension $\mathbf{K}'/\mathbf{K}$, such that $a'_p \equiv a_p \mod \lambda'$ for some $\lambda' \mid \lambda$, and $p \nmid \ell\, q$.

(3) One can apply Theorem 3.2.2 to this f', getting a representation ρ' with values in $GL_2(\mathbf{K}'_{\lambda'})$.

(4) $\rho'(G_{\mathbb{Q}})$ is a compact subgroup of $GL_2(\mathbf{K}'_{\lambda'})$, which one can suppose to be contained in $GL_2(\mathcal{O}'_{\lambda'})$, after possible conjugation. So one can reduce ρ' modulo λ', and get $\bar{\rho'}$ with values in $GL_2(\mathcal{O}'_{\lambda'}/\lambda')$. Note that so far we preserved the congruences between the initial f and the Galois representations,

(5) but $\bar{\rho'}$ may not be semi-simple: taking its semi-simplification, one gets a semi-simple representation satisfying the congruences required in the theorem.

(6) One can reduce the field of definition from $\mathcal{O}'_{\lambda'}/\lambda'$ to k_f , because the characteristic polynomials of all the $\bar{\rho'}(g)$ have their coefficients in k_f by definition of k_f, using Čebotarev theorem, more precisely, $\bar{\rho'}$ is isomorphic to a representation $\bar{\rho_f} : G_{\mathbb{Q}} \to GL_2(k_f) \subset GL_2(\mathcal{O}'_{\lambda'}/\lambda')$, Deligne-Serre [4] for the details..

Step 2: Bounding the images of the reductions. In step one, one reduced Galois representations modulo a prime. To get a complex Galois representation, one needs to lift them back.

Proposition 3.2.4. *Let G be a finite group, ℓ be a prime not dividing $|G|$ and $\bar{\rho}_\ell : G \to GL_n(\boldsymbol{F}_\ell)$ a representation. Suppose there exists a number field $\boldsymbol{K}$ containing the roots of unity of order $|G|$, and a prime ideal λ for which $\mathcal{O}_{\boldsymbol{K}}/\lambda = \boldsymbol{F}_\lambda$. Then there exists a representation $\rho : G \to GL_n(\mathcal{O}_{\boldsymbol{K}})$ whose reduction modulo λ is isomorphic to $\bar{\rho}_\ell$.*

So, if $\mathbf{K} \supset \mathbb{Q}_f$ is sufficiently large, one decomposes $\bar{\rho_f}$ of Theorem 3.2.3 into $G_{\mathbb{Q}} \to \bar{\rho_f}(G_{\mathbb{Q}})$ followed by $\bar{\rho_f}(G_{\mathbb{Q}}) \hookrightarrow GL_2(k_f)$, and would like to lift the second to $GL_2(\mathbf{K})$. The previous proposition tells us this is possible, if we can assume that the characteristic of k_f is coprime to $|\bar{\rho_f}(G_{\mathbb{Q}})|$, at least for sufficiently many primes λ of $\mathbf{K}$. This is indeed the case, and one proceeds as follows.
Let $\mathbf{K} \supset \mathbb{Q}_f$ be a finite Galois extension of $\mathbb{Q}$; let $\mathcal{S}$ be the set of primes of $\mathbb{Q}$, totally split in $\mathbf{K}$. It is known that the Dirichlet density $\delta(\mathcal{S}) = 1/[\mathbf{K} : \mathbb{Q}]$, so $\mathcal{S}$ is infinite, and we have some flexibility in the choice of $\mathbf{K}$. For $\ell \in \mathcal{S}$, Theorem 3.2.3 gives a semi-simple representation $\bar{\rho}_\ell : (G_{\mathbb{Q}}) \to GL_2(\mathbf{F}_\ell)$. As a consequence, $G_\ell := \bar{\rho}_\ell(G_{\mathbb{Q}})$ is a semi-simple subgroup of $GL_2(\mathbf{F}_\ell)$. The key result is the following:

Proposition 3.2.5. *With this notation, one has:*

$$sup_{\ell \in \mathcal{S}} |G_\ell| < \infty$$

Deligne-Serre [4], proposition 7.2, for the details.

Step 3: Lift to $GL_2(\mathbb{C})$

Let $M = sup_{\ell \in \mathcal{S}} |G_\ell|$: by adjoining them if necessary, one can suppose that $\mathbf{K}$ contains the M-th roots of unity; and let

$$\mathcal{S}' = \{p \text{ prime } : p \text{ totally split in } \mathbf{K}, \ p > M\}$$

Proposition 3.2.4 produces, for each $\ell \in \mathcal{S}'$, a representation $\rho_\ell : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{\mathbf{K}})$ whose reduction modulo a prime λ dividing ℓ is $\bar{\rho}_\ell$ (ℓ being totally split in $\mathbf{K}$, any prime ideal λ dividing ℓ satisfies $\mathcal{O}_{\mathbf{K}}/\lambda \cong \mathbf{F}_\ell$).

The last point to be careful with is the effect of this lifting on the congruences as stated in Theorem 3.2.4. One can argue as follows. Consider the finite set of polynomials:

$$\mathcal{P}_M = \{P(X) = (1 - \alpha X)(1 - \beta X) \ : \ \alpha, \beta \ M - \text{ th roots of unity}\}$$

(1) For each prime p, and $\ell \in S'$, $\ell \neq p$ and $\lambda \mid \ell$, Theorem 3.2.4 implies that:

$$\exists R_\ell \in \mathcal{P}_M \quad \text{such that } \ 1 - a_p(f)X + \chi(p)X^2 \equiv R_\ell(X) \mod (\lambda)$$

As $\mathcal{P}_M$ is finite, the same polynomial works for infinitely many ℓ, so $1 - a_p(f)X + X^2$ itself is in $\mathcal{P}_M$.

(2) As the set $\mathcal{P}_M$ is finite, one can suppose that $\forall P, Q \in \mathcal{P}_M$, $P \neq Q$, then $P \not\equiv Q \mod (\lambda)$, after removing a finite set of unsatisfying primes ℓ.

(3) Fix a prime ℓ not dividing the level q of the form f, and let $p \neq \ell$ as above. The lift ρ_ℓ to $GL_2(\mathcal{O}_{\mathbf{K}})$ is unramified outside $q\,\ell$, and the characteristic polynomial of $\rho_\ell(\mathbb{F}_p)$ is in $\mathcal{P}_M$: this is because by construction $|\rho_\ell(G_{\mathbb{Q}})| = |G_\ell|$, so $\rho_\ell(\mathbb{F}_p)$ has order less than M. On the other hand, the polynomial $1 - a_p(f)X + \chi(p)X^2$ is in $\mathcal{P}_M$ as well, and as ρ_ℓ lifts $\overline{\rho_\ell}$, the two polynomials are congruent modulo λ: by the choice of ℓ, they are hence equal, so one has:

$$\forall p \nmid q\,\ell \quad \det(Id - X\rho_\ell(\mathbb{F}_p)) = 1 - a_p(f)X + \chi(p)X^2$$

(4) One has the same conclusion for another choice ℓ', by replacing ℓ by ℓ'.

(5) This means that the two representations $\rho_\ell, \rho_{\ell'} : G_{\mathbb{Q}} \to GL_2(\mathbb{C})$ are isomorphic as $\mathbb{C}$-representations, and all the ρ_ℓ are unramified outside q, and that the relation:

$$\forall p \nmid q\,\ell \quad \det(Id - X\rho_\ell(\mathbb{F}_p)) = 1 - a_p(f)X + \chi(p)X^2$$

holds. After this choice, one renames ρ_ℓ into ρ_f, and the construction is finished.

One should note that the finiteness of $\rho_f(G_{\mathbb{Q}})$ is a consequence of the construction; and that one gets the continuity of ρ_f from the finiteness of the image.

Step 4: Irreducibility. Reductio ad absurdum: if ρ_f were not irreducible, by semi-simplicity (automatic over $\mathbb{C}$), one could find two onedimensional stable subspaces of $\mathbb{C}^2$, on which $G_{\mathbb{Q}}$ would act by characters χ_1, χ_2, which are Dirichlet characters:

$$\rho_F \cong \chi_1 \oplus \chi_2$$

So $a_p(f) = \chi_1(p) + \chi_2(p)$, and $\chi_(p) = \det(\rho_f(\mathbb{F}_p)) = \chi_1(p)\chi_2(p)$, which proves by the way that $\chi_1 \neq \chi_2$ (else $\chi_1(-1) = \chi_2(-1) = 1$ and $f = 0$). One gets

$$\sum_{p\nmid q} \frac{|a_p(f)|^2}{p^s} = 2\sum_{p\nmid q} p^{-s} + \sum_{p\nmid q} \frac{\chi_1(p)\overline{\chi_2(p)}}{p^s} + \sum_{p\nmid q} \frac{\overline{\chi_1(p)}\chi_2(p)}{p^s}$$

It is well known that for any non-trivial Dirichlet character ψ, then $\sum_n \psi(n)n^{-s}$ is holomorphic at $s = 1$, so the two last terms are bounded. This would imply that

$$\sum_{p\nmid q} \frac{|a_p(f)|^2}{p^s} = 2\sum_{p\nmid q} p^{-s} = -2\log(s-1) + O_{s\to 1}(1)$$

This contradicts the result of Rankin-Selberg for any real number M:

$$\sum_{p\nmid q} \frac{|a_p(f)|^2}{p^s} \geq \sum_{p\nmid q} \frac{M^2}{p^s}$$

and proves the irreducibility of ρ_f.

3.3 Eichler-Shimura contruction for weight 2

This section associates Galois representations to modular curves and then decomposes them into 2-dimensional representations associated to modular forms.

Let N be a positive integer and let ℓ be prime. The modular curve $X_1(N)$ is a projective nonsingular algebraic curve over $\mathbb{Q}$. Let g denote its genus. The curve $X_1(N)_{\mathbb{C}}$ over $\mathbb{C}$ defined by the same equations can also be viewed as a compact Riemann surface. The Jacobian of the modular curve is a g-dimensional complex torus obtained from integration modulo homology,

$$J_1(N) = Jac(X_1(N)_{\mathbb{C}}) \cong \mathbb{C}^g/\Lambda_g$$

The Picard group of the modular curve is the Abelian group of divisor classes on the points of $X_1(N)$,

$$Pic^0(X_1(N)) = Div^0(X_1(N))/PDiv(X_1(N))$$

$Pic^0(X_1(N))$ can be identified with a subgroup of $Pic^0(X_1(N)_{\mathbb{C}})$, and the complex Picard group is naturally isomorphic to the Jacobian by Abel's Theorem. Thus there is an inclusion of ℓ^n-torsion,

$$i_n : Pic^0(X_1(N))\,[\ell^n] \to Pic^0(X_1(N)_{\mathbb{C}})\,[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$$

Recall that Igusa's Theorem states that $X_1(N)$ has good reduction at primes $p \nmid N$, so also there is a natural surjective reduction map $Pic^0(X_1(N)) \to Pic^0(\tilde{X}_1(N))$, where $\tilde{X}_1(N)$ is the reduction of $X_1(N)$ at p, for a reference Diamond [5] Chapter 8, restricting to

$$\pi_n : Pic^0(X_1(N))\,[\ell^n] \to Pic^0(\tilde{X}_1(N)_{\mathbb{C}})\,[\ell^n]$$

We state without proof two generalizations:

- The inclusion i_n is in fact an isomorphism.
- The surjection π_n is an isomorphism for $p \nmid N$.

The ℓ-adic Tate module of $X_1(N)$ is

$$Ta_\ell(Pic^0(X_1(N))) = \varprojlim \left\{Pic^0(X_1(N))[\ell^n]\right\}$$

Choosing bases of $Pic^0(X_1(N))\,[\ell^n]$ compatibly for all n shows that

$$Ta_\ell(Pic^0(X_1(N))) \cong \mathbb{Z}_\ell^{2g}$$

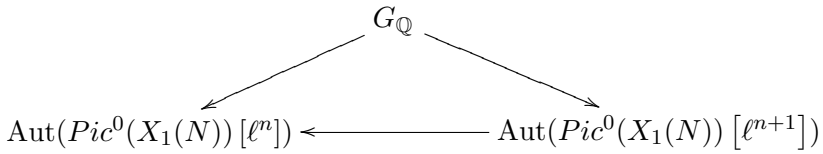
Any automorphism $\sigma \in G_{\mathbb{Q}}$ defines an automorphism of $Div^0(X_1(N))$,

$$(\sum n_P(P))^\sigma = \sum n_P(P^\sigma)$$

Since $div(f)^\sigma = div(f^\sigma)$ for any $f \in \overline{\mathbb{Q}}\,(X_1(N))$, the automorphism descends to $Pic^0(X_1(N))$,

$$Pic^0(X_1(N)) \times G_{\mathbb{Q}} \to Pic^0(X_1(N))$$

The field extension $\mathbb{Q}\,(Pic^0(X_1(N))\,[\ell^n])/\mathbb{Q}$, for an explanation on the costruction Diamond [5] Chapter 6 and Chapter 9, is Galois for each $n \in \mathbb{Z}^+$, so the action restricts to $Pic^0(X_1(N))\,[\ell^n]$. For each n there is a commutative diagram



This leads to a continuous homomorphism

$$\rho_{X_1(N),\ell} : G_{\mathbb{Q}} \to GL_{2g}(\mathbb{Z}_\ell) \subset GL_{2g}(\mathbb{Q}_\ell)$$

This is the $2g$-dimensional Galois representation associated to $X_1(N)$. Recall that the Hecke algebra over $\mathbb{Z}$ is the algebra of endomorphisms of $S_2(\Gamma_1(N))$ generated over $\mathbb{Z}$ by the Hecke operators,

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}\left[\left\{T_n, \langle n\rangle : n \in \mathbb{Z}^+\right\}\right]$$

The Hecke algebra acts on $Pic^0(X_1(N))$, for an explanation on the costruction Diamond [5] Chapter 7(this contruction follows from an iterepretation as Moduli Space and it is far beyond the aim of this exposition), so we have:

$$\mathbb{T}_{\mathbb{Z}} \times Pic^0(X_1(N)) \to Pic^0(X_1(N))$$

Since the action is linear it restricts to ℓ-power torsion, and so it extends to $Ta_\ell(Pic^0(X_1(N)))$. The Hecke action is defined over $\mathbb{Q}$. So it is possible to prove that the Galois action and the Hecke action on $Pic^0(X_1(N))$ commute, Diamond [5] Chapter 9, and therefore so do the two actions on $Ta_\ell(Pic^0(X_1(N)))$.

Theorem 3.3.1. *Let ℓ be prime and let N be a positive integer. The Galois representation $\rho_{X_1(N),\ell}$ is unramified at every prime $p \nmid \ell N$. For any such p let $\mathfrak{p} \in \bar{\mathbb{Z}}$ be any maximal ideal over p. Then $\rho_{X_1(N),\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation*

$$x^2 - T_p\, x + \langle p\rangle\ p = 0$$

Proof. Let $p \nmid \ell N$ and let $\mathfrak{p}$ lie over p. There is a commutative diagram

$$\begin{array}{ccc} D_{\mathfrak{p}} & \longrightarrow & \mathrm{Aut}(Pic^0(X_1(N))\,[\ell^n]) \\ \downarrow & & \downarrow \\ G_{\mathbb{F}_p} & \longrightarrow & \mathrm{Aut}(Pic^0(\tilde{X}_1(N))\,[\ell^n]) \end{array}$$

The vertical map on the right side is an isomorphism, and $I_{\mathfrak{p}} \subset \ker \rho_{X_1(N),\ell}$. The Eichler-Shimura Relation, for a reference Diamond [5], Chapter 9, restricts to ℓ^n-torsion,

$$\begin{array}{ccc} Pic^0(X_1(N))\,[\ell^n] & \xrightarrow{T_p} & Pic^0(X_1(N))\,[\ell^n] \\ \downarrow & & \downarrow \\ Pic^0(\tilde{X}_1(N))\,[\ell^n]\, G_{\mathbb{F}_p} & \xrightarrow{\sigma_{p,*}+\langle\tilde{p}\rangle_*\sigma_p^*} & Pic^0(\tilde{X}_1(N))\,[\ell^n] \end{array}$$

The same diagram but with $\mathrm{Frob}_{\mathfrak{p}} + \langle p\rangle\ p\ \mathrm{Frob}_{\mathfrak{p}}^{-1}$ across the top row instead also commutes. Since the vertical arrows are isomorphisms,

$$T_p = \mathrm{Frob}_{\mathfrak{p}} + \langle p\rangle\ p\ \mathrm{Frob}_{\mathfrak{p}}^{-1}$$

on $Pic^0(X_1(N))\,[\ell^n]$. This holds for all n, so the equality can be extended to $Ta_\ell(Pic^0(\tilde{X}_1(N)))$. The result follows. □

To proceed from Picard groups to modular forms, consider a normalized eigenform

$$f \in S_2(N, \chi)$$

The Hecke algebra contains an ideal associated to f, the kernel of the eigenvalue map,

$$I_f = \{T \in \mathbb{T}_{\mathbb{Z}} : T\, f = 0\}$$

and the Abelian variety of f is defined as

$$A_f = J_1(N)/I_f\, J_1(N)$$

There is an isomorphism

$$\mathbb{T}_{\mathbb{Z}}/I_f \to \mathcal{O}_f \quad \text{where } \mathcal{O}_f = \mathbb{Z}\left[\{a_n(f) : n \in \mathbb{Z}^+\}\right]$$

Under this isomorphism each Fourier coefficient $a_p(f)$ acts on A_f as $T_p + I_f$. Also, $\mathcal{O}_f$ contains the values $\chi(n)$ for $n \in \mathbb{Z}^+$ and $\chi(p)$ acts on A_f as $\langle p \rangle + I_f$. The ring $\mathcal{O}_f$ generates the number field of f, denoted $\mathbb{Q}_f$. The extension degree $d = \left[\mathbb{Q}_f : \mathbb{Q}\right]$ is also the dimension of A_f as a complex torus. The Abelian variety has an ℓ-adic Tate module,

$$Ta_\ell(A_f) = \lim_{\leftarrow} \{A_f[\ell^n]\} \cong \mathbb{Z}_\ell^{2d}$$

The action of O_f on A_f is defined on ℓ-power torsion and thus extends to an action on $Ta_\ell(A_f)$. The following lemma shows that $G_{\mathbb{Q}}$ acts on $Ta_\ell(A_f)$ as well.

Lemma 3.3.2. *The map $Pic^0(X_1(N))[\ell^n] \to A_f[\ell^n]$ is a surjection. Its kernel is stable under $G_{\mathbb{Q}}$.*

Proof. Multiplication by ℓ^n is surjective on the complex torus $J_1(N)$. This makes it surjective on $I_f\, J_1(N)$ as well: any $y \in I_f\, J_1(N)$ takes the form $y = \sum_i T_i\, y_i$ with $T_i \in I_f$ and $y_i \in J_1(N) = \ell^n\, J_1(N)$ for each i, so $y = \sum_i T_i\, (\ell^n\, x_i) = \ell^n \sum_i T_i\, x_i \in \ell^n\, I_f\, J_1(N)$ as desired. To show the first statement, take any $y \in A_f[\ell^n]$. Then $y = x + I_f\, J_1(N)$ for some $x \in J_1(N)$ such that $\ell^n\, x \in I_f\, J_1(N)$. Thus $\ell^n\, x = \ell^n\, x'$ for some $x' \in I_f\, J_1(N)$ by the previous paragraph. The difference $x - x'$ lies in $J_1(N)[\ell^n] = Pic^0(X_1(N))[\ell^n]$ and maps to y as desired.
The kernel is $Pic^0(X_1(N))[\ell^n] \cap I_f\, J_1(N) = (I_f\, J_1(N))[\ell^n]$. We claim that the inclusion $(I_f\, Pic^0(X_1(N)))[\ell^n] \subset (I_f\, J_1(N))[\ell^n]$ is in fact an equality. To see this, let $S_2 = S_2(\Gamma_1(N))$ and $H_1 = H_1(X_1(N)_{\mathbb{C}}, \mathbb{Z}) \in S_2^\wedge$, where $S_2^\wedge$ is the dual spave of S_2. Thus $J_1(N) = S_2^\wedge/H_1$ and

$$I_f\, J_1(N) = (I_f\, S_2^\wedge + H_1)/H_1 \cong I_f\, S_2^\wedge/(H_1 \cap I_f\, S_2^\wedge)$$

$I_f\, H_1$ is a subgroup of $H_1 \cap I_f\, S_2^\wedge$ with some finite index M. This shows that $M(\cap I_f\, S_2^\wedge) \subset I_f\, H_1$.

Now suppose that $y \in (I_f\, J_1(N))\,[\ell^n]$. Then $y = x + H_1 \cap I_f\, S_2^\wedge$ with $x \in I_f\, S_2^\wedge$, and since $\ell^n\, y = 0$ this implies $\ell^n\, x \in H_1 \cap I_f\, S_2^\wedge$. Therefore $M\,\ell^n\, x \in M(H_1 \cap I_f\, S_2^\wedge) \in I_f\, H_1$, and so $x \in I_f(M^{-1}\,\ell^{-n}\, H_1)$. It follows that $y \in I_f(J_1(N)\,[M\,\ell^n]) \subset I_f\, Pic^0(X_1(N))$, and since $\ell^n\, y = 0$ the equality is proved. Thus the kernel is $(I_f(Pic^0(X_1(N)))\,[\ell^n])$. This is stable under $G_{\mathbb{Q}}$ as desired since the Galois and Hecke actions on $Pic^0(X_1(N))$ commute. $\square$

So $G_{\mathbb{Q}}$ acts on $A_f\,[\ell^n]$ and therefore on $Ta_\ell(A_f)$. The action commutes with the action of $\mathcal{O}_f$ since the $G_{\mathbb{Q}}$-action and the $\mathbb{T}_{\mathbb{Z}}$-action commute on $Ta_\ell(Pic^0(X_1(N)))$. Choosing coordinates appropriately gives a Galois representation

$$\rho_{A_f,\ell} : G_{\mathbb{Q}} \to GL_{2d}(\mathbb{Q}_\ell)$$

This is continuous because $\rho_{X_1(N),\ell}$ is continuous and

$$\rho^{-1}_{X_1(N),\ell}(U(n,g)) \subset \rho^{-1}_{A_f,\ell}(U(n,d))$$

where $U(n,g) = \ker(GL_{2g}(\mathbb{Z}_\ell) \to GL_{2g}(\mathbb{Z}/\ell^n\mathbb{Z}))$ and similarly for $U(n,d)$. The representation is unramified at all primes $p \nmid N$ since its kernel contains $\ker \rho_{X_1(N),\ell}$. For any such p let $\mathfrak{p} \in \bar{\mathbb{Z}}$ be any maximal ideal over p. At the level of Abelian varieties, since T_p acts as $a_p(f)$ and $\langle p \rangle$ acts as $\chi(p)$, $\rho_{A_f,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)\, x + \chi(p)p = 0$$

The Tate module $Ta_\ell(A_f)$ has rank $2d$ over $\mathbb{Z}_\ell$. Since it is an $\mathcal{O}_f$-module the tensor product $V_\ell(A_f) = Ta_\ell(A_f) \otimes \mathbb{Q}$ is a module over $\mathcal{O}_f \otimes \mathbb{Q}_\ell = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

Lemma 3.3.3. *$V_\ell(A_f)$ is a free module of rank 2 over $\mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.*

Proof. Again let $S_2 = S_2(\Gamma_1(N))$ and $H_1 = H_1(X_1(N)_{\mathbb{C}}, \mathbb{Z}) \in S_2^\wedge$. Consider the quotients $\bar{S}_2^\wedge = S_2^\wedge / I_f S_2^\wedge$ and $\bar{H}_1 = (H_1 + I_f S_2^\wedge)/I_f S_2^\wedge$. Then $A_f = S_2^\wedge/(H_1 + I_f S_2^\wedge) = \bar{S}_2^\wedge/\bar{H}_1$. Thus $\bar{H}_1$ is an $\mathcal{O}_f$-module whose $\mathbb{Z}$-rank is $2d$. Since $\mathbb{Q}_f$ is a field, $\bar{H}_1 \otimes \mathbb{Q}$ is a free $\mathbb{Q}_f$-module of rank 2, and therefore $\bar{H}_1 \otimes \mathbb{Q}_\ell = \bar{H}_1 \otimes \mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is free of rank 2 over the ring $\mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. The $\mathcal{O}_f$ -linear isomorphisms $\ell^{-n}\bar{H}_1/\bar{H}_1 \to \bar{H}_1/\ell^n\bar{H}_1$ induced by multiplication by ℓ^n on $\ell^{-n}\bar{H}_1$ assemble to give an isomorphism of $\mathcal{O}_f \otimes \mathbb{Z}_\ell$-modules,

$$Ta_\ell(A_f) = \varprojlim \{A_f[\ell^n]\} = \varprojlim \left\{\ell^{-n}\bar{H}_1/\bar{H}_1\right\} = \varprojlim \left\{\bar{H}_1/\ell^n\bar{H}_1\right\} = \bar{H}_1 \otimes \mathbb{Z}_\ell$$

where the transition maps in the last inverse limit are the natural projection maps. And now $V_\ell(A_f) = Ta_\ell(A_f) \otimes \mathbb{Q} = \bar{H}_1 \otimes \mathbb{Z}_\ell \otimes \mathbb{Q} = \bar{H}_1 \otimes \mathbb{Q}_\ell$ is an isomorphism of modules over $\mathcal{O}_f \otimes \mathbb{Z}_\ell \otimes \mathbb{Q} = \mathbb{Q}_f \otimes \mathbb{Q}_\ell$, showing that $V_\ell(A_f)$ is free. □

The absolute Galois group $G_{\mathbb{Q}}$ acts $(\mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$-linearly on $V_\ell(A_f)$, and $V_\ell(A_f) \cong (\mathbb{Q}_f \otimes \mathbb{Q}_\ell)^2$ by the lemma. Choose a basis B of $V_\ell(A_f)$ to get a homomorphism $G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell)$. Also, for each $\lambda \mid \ell$ we can specialize to get $\mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$ and so we can compose the homomorphism with a projection to get

$$\rho_\lambda : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_{f,\lambda})$$

This is continuous, making it a Galois representation and $ker(\rho_{A_f,\ell}) \subset ker(\rho_{f,\lambda})$. We have proved:

Theorem 3.3.4. *Let $f \in S_2(\Gamma_1(N), \chi)$ be a normalized eigenform with number field $\mathbb{Q}_f$. Let ℓ be prime. For each maximal ideal λ of $\mathcal{O}_{\mathbb{Q}_f}$ lying over ℓ there is a 2-dimensional Galois representation*

$$\rho_\lambda : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_{f,\lambda})$$

This representation is unramified at every prime $p \nmid \ell N$. For any such p let $\mathfrak{p} \subset \bar{Z}$ be any maximal ideal lying over p. Then $\rho_\lambda(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$x^2 - a_p(f)\, x + \chi(p)\, p = 0$$

In particular, if $f \in S_2(\Gamma_0(N))$ then the relation is

$$x^2 - a_p(f)\, x + p = 0$$

3.4 Ribet results

In this section we will explain results due to Ribet, for a reference [27] and [28]. Let $f \in S_2(\Gamma_0(N))$ be a newform of weight 2 on $\Gamma_0(N)$, that is a normalized eigenform for the whole Hecke algebra which is new of level N. We assume that f does not have complex multiplication or inner twists. Let $\mathbb{Q}_f$ be the number field associated to f and $\mathcal{O}_f$ its ring of integer as usual. For every prime ℓ put $\mathcal{O}_\ell = \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $\mathbb{Q}_{f,\ell} = \mathbb{Q}_f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
Let ℓ be a prime number, we can consider a representation

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_\ell)$$

unramified at all primes $p \nmid \ell N$. We can reduce this representation to get a representation $\overline{\rho_\lambda}$ to $GL_2(\mathbf{F}_\lambda)$ where $\mathbf{F}_\lambda$ is the residue field for λ prime in $\mathbb{Q}_f$: in fact, as explained before, from the decomposition $\mathbb{Q}_{f,\ell} \cong \prod_{\lambda|\ell} \mathbb{Q}_{f,\lambda}$ and $\mathcal{O}_\ell \cong \prod_{\lambda|\ell} \mathcal{O}_\lambda$ we obtain a decomposition of ρ_ℓ:

$$\rho_\ell = \oplus_{\lambda|\ell}\rho_\lambda \qquad \rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{O}_\lambda)$$

where $\mathcal{O}_\lambda$ is the inverse limit over $n \in \mathbb{Z}^+$ of $\{\mathcal{O}_f/\lambda^n\}$. We can consider the reduction $\overline{\rho_\lambda}$ of ρ_λ, obatined composing ρ_λ with the reduction map $GL_2(\mathcal{O}_\lambda) \to GL_2(\mathbf{F}_\lambda)$, where $\mathbf{F}_\lambda$ is the residue field for λ.

Theorem 3.4.1. *For all but finitely many λ we have:*

(a) the representation $\overline{\rho_\lambda}$ is an irreducible 2-dimensional representation over $\boldsymbol{F}_\lambda$;

(b) the order of the group $\overline{\rho_\lambda}(G_\mathbb{Q})$ id divisible by ℓ.

Theorem 3.4.2. *Let $A_\ell = \{x \in GL_2(\mathcal{O}_\ell) \mid \det(x) \in \mathbb{Z}_l^*\}$, the equality $G_\ell = A_\ell$ holds for almost every prime. In fact the equality holds when the following conditions are all satisfied:*

(1) ℓ does not ramify in $\mathbb{Q}_f/\mathbb{Q}$;

(2) the determinant map $G_\mathbb{Q} \to \mathbb{Z}_l^*$ is surjective;

(3) $\ell \geq 5$;

(4) there exists $x_\ell \in G_\ell$ such that $(\mathrm{Tr}(x_\ell))^2$ generates $\mathcal{O}_\ell$ as $\mathbb{Z}_\ell$-algebra;

(5) for all λ such that $\lambda \mid \ell$ the group $\overline{\rho_\lambda}(G_\mathbb{Q})$ is an irreducible subgroup of $GL_2(\boldsymbol{F}_\lambda)$ whose order is divisible by ℓ.

For all but finitely many λ means that there is a finite set of primes ℓ such that no λ in $\mathcal{O}_f$ over it satisfy the Theorem.

We will not give a complete proof of these results, since it would required more preliminaries and reference to completely different theorical elements, in which we are not interested. We will give an exposition of some statement collected in the previous Theorems, in particular the method used in the proofs belove is the key element.

Suppose ℓ is odd. If the mod ℓ representation ρ is irreducible and modular, i.e. $\exists f$ modular form such that $\rho = \rho_f$, then is is possible to show that ρ arises from a newform f of some specific weight $k(\rho)$ and level $N(\rho)$. Here $N(\rho)$ is called the *Artin conductor* of the modular form, it is a product $\prod_{p \neq \ell} p^{e(p)}$ where $e(p)$ is a sum

$$\sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} \dim(W/W^{G_i})$$

here W is the representation space of ρ,

$$G_i := \{\sigma \in G \,|\, |x - \sigma(x)|_p > i \,\forall x \in \mathcal{O}_f\}\,.$$

The factor $\frac{1}{(G_0:G_i)}$ depends only on $G_0 = \rho|I_{\mathfrak{p}}$, where $I_{\mathfrak{p}}$ is the inertia subgroup defined in Chapter 1. There is, in particular, a term corresponding to $i = 0$ which is $\dim(V/V^{I_p})$.

Let $\mathbf{F}$ be a finite field, and let p be the characteristic of $\mathbf{F}$. We will assume that p is odd; most of the results will require that p be at least 5. Suppose that

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbf{F})$$

is an irreducible representation whose determinant is the mod p cyclotomic character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_p^*$. Let $k(\rho)$ and $N(\rho)$ be the weight and conductor of ρ.

Definition 3.4.3. *ρ is* semistable *if the conductor $N(\rho)$ of ρ is square free and Serre's weight $k(\rho)$ is either 2 or $p+1$.*

The semisimplification of $\rho|_I$, where I is the inertia subgroup, is described by a pair of characters $\phi, \phi' : I \to \overline{F}^*$. Since $\det\rho$ is the cyclotomic character χ, we have in particular $\phi\,, \phi' = \chi$. If $k(\rho)$ is one of $2, p+1$, then $\{\phi\,, \phi'\}$ is either $\{1\,, \chi\}$ or else the set of fundamental characters $\psi\,, \psi' : I \to \overline{F}^*$ of level 2, they may be thought as in the case of Dickson Theorem for the characters of the Cartan subgroup. It follows that the order of ϕ, ϕ' is either $p-1$ or $p+1$.

Proposition 3.4.4. *If ρ is semistable, then the image of ρ has order divisible by p.*

Proof. Let $G = \rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$, and assume that the order of G is prime to p. Since the semistability hypothesis implies that ramification subgroups of G for primes $\ell \neq p$ are unipotent, these ramification groups are forced to be trivial. In other words, we have $N(\rho) = 1$ and the representation ρ is unramified outside p. As Serre remarks in a note, it is possible to show that there are no irreducible representations ρ with this property when $p = 3$. Now assume that $p \geq 5$ and write $\bar{G}$ for the image of G in $PGL_2(\mathbf{F})$. Dickson Theorem shows that $\bar{G}$ is either cyclic or dihedral, or else one of the three exceptional groups S_4, A_4, A_5.
In fact, $\bar{G}$ cannot be cyclic, since the cyclicity of $\bar{G}$ would imply that G is abelian, and hence that ρ is not absolutely irreducible.
To rule out the other cases, one considers an inertia subgroup $\bar{I}$ of $\bar{G}$ for the prime p. We know that $\bar{I}$ is a cyclic group of order either $p+1$ or $p-1$. Indeed, $\bar{I}$ may be viewed as the image of $I \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ under the character ϕ/ϕ' which we introduced above. This character has order either $p-1$ or $p+1$; its image is cyclic because it is a finite subgroup of $\overline{F}^*$.
Assume now that $\bar{G}$ is dihedral, and let Z be the center of $\bar{G}$. It is evident that $\bar{I}$ is contained in Z, since $\bar{I}$ is a cyclic subgroup of a dihedral group and the order of $\bar{I}$ is greater than 2. Accordingly, the quadratic extension of $\mathbb{Q}$ corresponding to Z is everywhere unramified. This contradiction excludes the dihedral case and shows that $\bar{G}$ must be one of the three exceptional groups.
However, the fact that $\bar{I}$ has an element of order $p-1$ rules out the groups S_4, A_4, A_5 in case $p \geq 7$.
Thus we are left only with the possibility that $p = 5$, in which case $\bar{G}$ is either S_4 or A_4, since its order is prime to 5 by assumption. The group $\bar{I}$ is then cyclic of order 4, since S_4 has no element of order 6. Also, we have $\bar{G} \cong S_4$, since A_4 has no element of order 4. Consider the quotient S_3 of S_4. This quotient allows us to produce an S_3-extension of $\mathbb{Q}$ which is ramified only at 5 and such that the inertia groups for 5 in the extension have order 2. However, there certainly is no such extension, since the class number of $\mathbb{Q}(\sqrt{5})$ is 1. □

Corollary 3.4.5. *Let ρ satisfy to the same hypothesis of the previous Proposition; and suppose that $p > 2$. Then the image of ρ contains a subgroup isomorphic to $SL_2(\mathbb{F}_p)$. In particular, if $\boldsymbol{F} = \mathbb{F}_p$, then ρ is surjective.*

Proof. The second statement is a consequence of the first, since the cyclotomic character is surjective. To prove the first statement, let $g \in G$ be an element of order p, and let v be a non-zero vector in $\mathbf{F} \oplus \mathbf{F}$ which is fixed by g. Since ρ is irreducible, G cannot fix the line generated by v; therefore, there is an $r \in G$ such that v and rv form a basis of $\mathbf{F} \oplus \mathbf{F}$. With respect

to this basis, g has the form $\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$, while rgr^{-1} has the form $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$. Scaling one of the vectors v, rv, we may assume that $a = 1$.
Hence, in an appropriate basis, G contains the elements $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$.
By Theorem 1.6.11, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$ generate the group $SL_2(\mathbf{F}')$, where $\mathbf{F}' = \mathbb{F}_p(b)$. □

Lemma 3.4.6. *Suppose that ρ semistable and that $p \geq 5$. Then $\bar{G}$ lies in $PGL_2(\boldsymbol{K})$ if and only if G lies in $GL_2(\boldsymbol{K})$, where $\boldsymbol{K}$ is an arbitrary subfield of the algebraic closure of $\boldsymbol{F}$.*

Proof. If G lies in $GL_2(\mathbf{K})$, then it is evident that $\bar{G}$ is contained in $PGL_2(\mathbf{K})$. Conversely, suppose $\bar{G} \subseteq PGL_2(\mathbf{K})$. Then certainly $G \subseteq \bar{\mathbf{F}}^* \dot{G}L_2(\mathbf{K})$. Let $\alpha : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \bar{\mathbf{F}}^*/\mathbf{K}^*$ be the composite homomorphism

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\rho} G \hookrightarrow \bar{\mathbf{F}}^* \dot{G}L_2(\mathbf{K}) \to (\bar{\mathbf{F}}^* \dot{G}L_2(\mathbf{K}))/GL_2(\mathbf{K}) = \bar{\mathbf{F}}^*/\mathbf{K}^*$$

For $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have $\alpha(\sigma) = 1$ whenever the trace of $\rho(\sigma)$ is a nonzero element of $\mathbf{K}$. Indeed, write $\rho(\sigma) = t \cdot M$, with $M \in GL_2(\mathbf{K})$ and $t \in \bar{\mathbf{F}}^*$. Then $\mathrm{Tr}(\rho(\sigma)) = t \cdot \mathrm{Tr}(M)$ and we have $\mathrm{Tr}(M) \in \mathbf{K}$.
If $\mathrm{Tr}(\rho(\sigma))$ belongs to $\mathbf{K}^*$, then t lies in $\mathbf{K}$, so that $\rho(\sigma)$ is an element of $GL_2(\mathbf{K})$. In particular, $\alpha(\sigma) = 1$ whenever the trace of $\rho(\sigma)$ is a non-zero element of $\mathbb{F}_p$. Let M now be the finite abelian extension of $\mathbb{Q}$ which is cut out by α. We seek to show that α is identically 1, i.e., that $M = \mathbb{Q}$. We first prove that α is unramified outside p by using the remark about traces. If σ belongs to an inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for a prime $\ell \neq p$, then $\rho(\sigma)$ is unipotent, so that its trace is 2. Since p is odd, 2 is a non-zero element of $\mathbb{F}_p$, and we may conclude that $\alpha(\sigma) = 1$.
Thus M is a finite abelian extension of $\mathbb{Q}$ which is unramified outside p. Moreover, $[M : \mathbb{Q}]$ is prime to p, since $\bar{F}^*$ has no elements of order p. Hence one has $M \subseteq \mathbb{Q}(\mu_p)$; equivalently, α factors through the mod p cyclotomic character χ.
Now let I be an inertia group for p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. It suffices to show that there is an element σ of I for which $\alpha(\sigma) = 1$ and for which $\chi(\sigma)$ is a generator of the cyclic group $\bar{\mathbb{F}}_p^*$.
The semisimplification of $\rho|_I$ is described by a pair of characters $\phi, \phi' : I \to \bar{F}^*$. As we mentioned above, one has either $\{\phi, \phi'\} = \{1, \chi\}$ or $\{\phi, \phi'\} = \{\psi, \psi^p\}$, where ψ and ψ^p are the fundamental characters of level 2. Suppose first that we are in the former case, and let $\sigma \in I$ be such that $t = \chi(\sigma)$ is a generator of $\bar{\mathbb{F}}_p^*$. Then $\mathrm{Tr}(\rho(\sigma)) = 1 + t$ is non-zero since $p \neq 3$. Thus $\alpha(\sigma) = 1$, as required.
In the latter case, choose $\sigma \in I$ so that $t = \psi(\sigma)$ generates $\psi(I)$. Then $\chi(\sigma) = t^{p+1}$ is a generator of $\mathbb{F}_p^*$; note that $\chi = \psi\psi' = \psi^{p+1}$. On the other

hand, $\mathrm{Tr}(\rho(\sigma)) = t + t^p$. The number t^{p-1} cannot be -1, since it has order $p+1$. Since $\mathrm{Tr}(\rho(\sigma))$ is non-zero, we may conclude $\alpha(\sigma) = 1$. □

Theorem 3.4.7. *Assume that ρ is semistable, that $p \geq 5$ and that $\boldsymbol{F}$ is generated over $\mathbb{F}_p$ by the set $\{\mathrm{Tr}(\rho(\sigma)) \mid \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$. Then*

$$\rho(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) = \{M \in GL_2(\boldsymbol{F}) \mid \det(M) \in \mathbb{F}_p^*\}$$

Proof. For a proof see Ribet [25]. □

Chapter 4

Exceptional primes and Congruences

Let $f \in S_2(\Gamma_0(N))$ be a newform of weight 2 on $\Gamma_0(N)$, i.e., a normalized eigenform for the whole Hecke algebra which is new of level N. We assume that f does not have CM or inner twists. Let us also suppose that f has trivial nebentypus. As explained in Chapter 2, the newform has a Fourier developement of the form: $f = \sum a_n q^n$, where, as usual, $q = e^{2\pi i}$; let $\mathbb{Q}_f$ be the number field generated by the Fourier coefficients $\{a_n\}$, $\mathbb{Q}_f = \mathbb{Q}(\{a_n\})$ and $\mathcal{O}_f$ its ring of integer.

Let us consider a non maximal order $\mathcal{O} \subset \mathcal{O}_f$ such that its conductor is the observed conductor for the modular form, let us call it c. We say that this is the observed conductor because, given a modular form, we can compute c only using a finite number of Fourier coefficients, for example cheking until the Sturm Bound, what we obtain is a multiple of the conductor. This choice will be optimal for reasons that will be clear later. $\mathcal{O}$is the order generated by coefficients of the modular form observed until the Sturm Bound.
We will use a standard abuse of notation for Number Theory: if λ is a prime ideal in $\mathcal{O}$, we will denote $\lambda \in \mathcal{O}$, instead of $\lambda \subseteq \mathcal{O}$, $\mathcal{O}/\lambda\mathcal{O}$ for its residue field, and if $\ell \in \mathbb{Z}$, $\lambda \mid \ell$ instead of $\ell \in \lambda$.

Now let us take a prime ℓ such that $\ell \mid c$ and $\lambda \in \mathcal{O}$ such that it doesn't fully decompose ℓ in the quotient of the order $\mathcal{O}$and $\lambda\mathcal{O}$:

$$\begin{array}{c} \lambda_1, \lambda_2, \cdots \in \mathcal{O} \subseteq \mathcal{O}_f \\ \Big| \\ \ell \in \mathbb{Z} \end{array}$$

where λ_i can be equal to λ_j, after reduction modulo λ:

$$\mathcal{O}/\lambda\mathcal{O} \subseteq \mathcal{O}_f/\lambda\mathcal{O}_f$$

where $\mathcal{O}/\lambda\mathcal{O} \cong \mathbb{F}_{\ell^s}$ and $\mathcal{O}_f/\lambda\mathcal{O}_f \cong \mathbb{F}_{\ell^r}$, where $r \geq 1$ and $s \leq r$. Let us consider the set of λ with an inertia, i.e. such that $r > 1$, because if $r = 1$ we would have $\mathcal{O}_f/\lambda\mathcal{O}_f \cong \mathbb{F}_\ell$ and so λ doesn't give any information.
We want to consider the Galois representation associated to the modular form $f = \sum a_n q^n$, in particular, the residual Galois representation $\overline{\rho_\lambda}$, i.e. the Galois representation attached to the modular form reduced modulo λ. We have an explicit determination of the image of the reduced representation thanks to two results of Ribet [27], that we have presented in Chapter 3, :

Theorem 4.0.8. *For all but finitely many λ we have:*

(a) the representation $\overline{\rho_\lambda}$ is an irreducible 2-dimensional representation over $\boldsymbol{F}_{\ell^r}$;

(b) the order of the group $\overline{G_\lambda} = \overline{\rho_\lambda}(G_\mathbb{Q})$ is divisible by ℓ.

Theorem 4.0.9. *Let $A_\ell = \{x \in GL_2(\mathcal{O}_\ell) \,|\, \det(x) \in \mathbb{Z}_\ell^*\}$, the equality $G_\ell = A_\ell$ holds for almost every prime. In fact the equality holds when the following conditions are all satisfied:*

(1) ℓ does not ramify in $\mathbb{Q}_f/\mathbb{Q}$;

(2) the determinant map $G_\mathbb{Q} \to \mathbb{Z}_\ell^*$ is surjective;

(3) $\ell \geq 5$;

(4) there exists $x_\ell \in G_\ell$ such that $(\mathrm{Tr}(x_\ell))^2$ generates $\mathcal{O}_\ell$ as $\mathbb{Z}_\ell$-algebra;

(5) for all λ such that $\lambda \mid \ell$ the group $\overline{G_\lambda}$ is an irreducible subgroup of $GL_2(\boldsymbol{F}_\lambda)$ whose order is divisible by ℓ

Using Theorem 4.0.8 and 4.0.9, we say that the image of a representation is "as large as possible", following Ribet, if $G_\ell = \rho_\ell(G_\mathbb{Q})$ is isomorphic to A_ℓ.

4.0.1 Exceptional prime of type $(*)$

Definition 4.0.10. *ℓ is an* exceptional prime of type $(*)$ *for the Galois representation associated to the modular form $f = \sum a_n q^n$ if ℓ ramifies in $\mathbb{Q}_f/\mathbb{Q}$.*

If ℓ is exceptional of type $(*)$ then the Newform space has some Galois invariance in it: if the newform satisfies additional condition then a Theorem of Ghate, [10] Lemma 5, holds:

Theorem (Ghate). *Let f be a newform of weight $k \geq 2$ and level N such that its number field $\mathbb{Q}_f$ coincides with its Galois closure, let $\mathcal{O}_f$ denote its ring of integers. Then if $p \mid \mathrm{disc}(\mathcal{O}_f)$ there exists a prime λ of $\mathbb{Q}_f$ with $\lambda \mid p$ and a non-trivial element $\gamma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$, $\gamma \in I_\lambda$ such that:*

$$f^\gamma \equiv f \mod \lambda \quad \textit{and} \ \ \gamma \in I_\lambda$$

Proof. Suppose $p \mid \mathrm{disc}(\mathcal{O}_f)$ and fix a prime λ of $\mathbb{Q}_f$ with $\lambda \mid p$, so λ lies over p. Let I_λ denote the inertia subgroup of $\mathbb{Q}_f/\mathbb{Q}$ at λ. Since p ramifies in $\mathbb{Q}_f$ there exists a non-trivial element $\gamma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$. Since by definition:

$$\gamma(x) \equiv x \mod \lambda \ \ \forall x \in \mathcal{O}_f$$

the congruence holds in particular for all $x = a_n(f) \in \mathcal{O}_f$ and so directly $f^\gamma \equiv f \mod \lambda$.
Conversely, if $\lambda \subset \mathcal{O}_f$ and $1 \neq \gamma \in \mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ satisfy $f^\gamma \equiv f \mod \lambda$ then $\gamma(x) \equiv x \mod \lambda$ for all $x \in \mathcal{O}_f$. This implies that γ fixes λ and that $\gamma \in I_\lambda$. Thus p ramifies and $p \mid \mathrm{disc}(\mathcal{O}_f)$. □

Therefore, if the number field corresponding to the newform is Galois closed then the condition for a prime of being exceptional of type $(*)$ correspods to the presence of a congruence between the form and a conjugate given by the action of an element of the Galois group of the field exension $\mathbb{Q}_f/\mathbb{Q}$.

4.0.2 Exceptional prime of type (0)

Let us suppose that the prime ℓ is not exceptional of type $(*)$.

Definition 4.0.11. *ℓ is an* exceptional prime of type (0) *for the Galois representation associated to the modular form $f = \sum a_n q^n$ if $\exists \lambda \in \mathcal{O}$ such that $\lambda \mid \ell$, and $\overline{G_\lambda} = \overline{\rho_\lambda}(G_\mathbb{Q})$ is a reducible subgroup of $GL_2(\boldsymbol{F}_\lambda)$.*

Following Dieulefait-Vila [7] if $\overline{G_\lambda}$ is a reducible subgroup of $GL_2(\mathbf{F}_\lambda)$ then, as shown by Serre [33], Proposition 4, exists an equivalent representation such that

$$\overline{\rho_\lambda} \cong \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}$$

$\phi_i = \epsilon_i \, \overline{\chi}_\ell^{m_i}$ $i = 1, 2$ where ϵ_i are Dirichlet characters unramified outside N with image in $\mathbf{F}_\lambda$ and $\overline{\chi}_\ell^{m_i}$ is the cyclotomic character modulo ℓ.

$$\epsilon_i : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbf{F}_\lambda^*$$

If we apply Deligne-Serre result about Galois representations attached to modular forms we get that $\forall p \nmid \ell N$:

$$a_p = \mathrm{Tr}(\rho_\lambda(\mathrm{Frob}_\mathfrak{p})) \overset{\mathrm{mod}\ \lambda}{\equiv} \phi_1(\mathrm{Frob}_\mathfrak{p}) + \phi_2(\mathrm{Frob}_\mathfrak{p}) = \epsilon_1(p)\, p^{m_1} + \epsilon_2(p)\, p^{m_2}$$

$$p = \det(\rho_\lambda(\mathrm{Frob}_\mathfrak{p})) \overset{\mathrm{mod}\ \lambda}{\equiv} \phi_1(\mathrm{Frob}_\mathfrak{p})\, \phi_2(\mathrm{Frob}_\mathfrak{p}) = \epsilon_1(p)\, \epsilon_2(p)\, p^{m_1+m_2}$$

For $\ell \nmid N$, let us consider $p \nmid N$ a primitive root modulo ℓ such that $\epsilon_1(p) = \epsilon_2(p) = 1$. From the last formula follows that $p = p^{m_1+m_2}$ so $m_1 + m_2 \equiv 1(\mod \ell - 1)$ so it is possible to choose m_1 and m_2 such that $0 \leq m_1 < m_2 < \ell - 1$.
We can recall an important result from Faltings and Jordan [8] for a newform $f \in S_k(N)$ without nebetypus:

Theorem 4.0.12. *Suppose that $\overline{\rho_\lambda}$ is reducible, if $\ell > k$ and $\ell \nmid N$ then*

$$\overline{\rho_\lambda} = \epsilon_1 \oplus \epsilon_2 \, \overline{\chi}_\ell$$

with ϵ_i Dirichlet character unramified outside N and $\overline{\chi}_\ell$ is the cyclotomic character modulo ℓ.

Using the previous Theorem and the results of Carayol and Livnè on conductor of modular forms (1989), we can state the following corollary

Corollary 4.0.13. *Suppose $f \in S_2(N)$, and $\lambda \in \mathcal{O}$ $\lambda \mid \ell$ is a prime such that $\overline{\rho_\lambda}$ is reducible. If $\ell > 2$, $\ell \nmid N$, then $\forall p \nmid \ell N$ we have*

$$a_p \equiv \epsilon(p) + p\, \epsilon^{-1}(p) \mod \lambda$$

where ϵ is a Dirichlet character unramified outside N, whose conductor c verifies $c^2 \mid N$.

Follows directly from what we have shown that ℓ being an exceptional prime of type (0) is equivalent to the congruence $\mod \lambda$ of $f \in S_2(N)$ and the Eisenstein serie $\epsilon + \chi\, \epsilon^{-1}$ which, as every congruence, can be checked until Sturm bound.

Proposition 4.0.14. *Given a prime $\ell \nmid N$, ℓ is an exceptional prime of type* 0 *if and only if*

$$f \equiv \epsilon + \chi\,\epsilon^{-1} \mod \lambda$$

where ϵ is a Dirichlet characters unramified outside N and χ is the cyclotomic character.

Proof. The first implication follows directly by definition of exceptional of type (0): from the fact that the reduced Galois representation is reducible and so we get from Corollary 4.0.13 the congruences of the modular forms. On the other hand, we have trivially that the Galois representation is reducible cause it is written as direct sum of characters. □

In the particular case of N prime holds a criterion due to Mazur [19]:

Corollary 4.0.15. *Suppose $f \in S_2(N)$, with N prime. Let $\lambda \in \mathcal{O}$ $\lambda \mid \ell$, $\ell \geq 5$, is a prime such that $\overline{\rho_\lambda}$ is reducible. Then $\ell \mid N-1$.*

For the primes $q \mid N$, if they are not excetional of type $(*)$, in the case of weight 2, they could be exceptional of type (0). In this case we have to distinguish between primes such that $q||N$ and primes such that $q^2 \mid N$. In the first case it can be seen, looking at the abelian variety associated to the Newform, that q is a semistable prime, for a reference [3], so if the image is a reducible subgroup, then the character considered cannot ramify at q. Meanwhile if $q^2 \mid N$ then the character which determine the image may ramify at q. Hence, adding the cas+e of prime 2 which is not considered in the previous statement, if is is not excetional of type $(*)$, we can say that:

Proposition 4.0.16. *Given a prime $\ell \mid N$, if $\ell^2 \mid N$, ℓ is an exceptional prime of type* 0 *if and only if*

$$f \equiv \epsilon + \chi\,\epsilon^{-1} \mod \lambda$$

where ϵ is a Dirichlet characters which can ramifies at N and χ is the cyclotomic character.
Given a prime $\ell \,||\, N$, ℓ is an exceptional prime of type 0 *if and only if*

$$f \equiv \epsilon + \chi\,\epsilon^{-1} \mod \lambda$$

where ϵ is a Dirichlet characters unramified outside $\frac{N}{\ell}$ and χ is the cyclotomic character.
2 *is an exceptional prime of type* 0 *if and only if*

$$f \equiv \epsilon + \chi\,\epsilon^{-1} \mod \lambda$$

where ϵ is a Dirichlet characters which can ramifies at $2 \cdot N$ and χ is the cyclotomic character.

4.0.3 Exceptional prime of type (1)

Let us suppose that the prime ℓ is not exceptional of the previous types: so from now on we are supposing the representation to be irreducible.

Definition 4.0.17. *ℓ is an* exceptional prime of type (1) *for the Galois representation associated to the modular form $f = \sum a_n q^n$ if $\exists \lambda$ such that $\lambda \mid \ell$ and*

$$a_p \mod \lambda \in \mathcal{O}/\lambda\mathcal{O} \cong \boldsymbol{F} \subsetneq \mathbb{F}_{\ell^r} \qquad \forall p \ p \nmid N\,\ell$$

where N is the level of the form.

If the Fourier coefficients of the newform, reduced modulo λ, belong to the same subfield that is contained strictly into $\mathbb{F}_{\ell^r}$, we would have that $\overline{\rho_\lambda}$, i.e. the Galois representation attached to the modular form restricted at level λ, is such that

$$Im(\overline{\rho_\lambda}) \cong G \subset GL_2(\mathbf{F})$$

This is because: if $\overline{\rho}$ is irreducible and if we have that each $a_i \in \mathbb{F}$, that means that the trace of the representation is in $\mathbb{F}$, and since we are working only with finite fields, so the Brauer group is trivial [1], then we can consider a representation in this field $\overline{\rho'_\lambda}$:

$$\begin{array}{ccc} \overline{\rho'_\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & GL_2(\mathbf{F}) \\ & & \subseteq \downarrow \\ \overline{\rho_\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & GL_2(\mathbb{F}_{\ell^r}) \end{array}$$

such that $\overline{\rho'_\lambda}$ extended by scalar in $\mathbb{F}_{\ell^r}$:

$$\begin{array}{ccc} \overline{\rho'_\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \longrightarrow & GL_2(\mathbf{F}) \\ & \searrow & \downarrow \\ & & GL_2(\mathbf{F}) \otimes \mathbb{F}_{\ell^r} \end{array}$$

is equivalent to the representation $\overline{\rho_\lambda}$.
This implies that we can have a model of the representation, a similar representation, that is not "as large as possible" but it is in a strictly contained subspace, so λ is exceptional and so ℓ.

[1] Let $\mathbf{K}$ be a field, A be a central simple $\mathbf{K}$-algebra, that is, A is a finite $\mathbf{K}$-vector space such that its centre is $\mathbf{K}$ and it has no nontrivial two sided ideals. The Wedderburn-Artin theorem says the following: every central simple $\mathbf{K}$-algebra A is of the form $A \cong M_n(D)$ where D is some central division $\mathbf{K}$-algebra. We say that $A \cong M_n(D)$ and $A' \cong M_n(D')$ are equivalent if $D \cong D'$, and let $Br(\mathbf{K})$ denote the set of equivalence classes of central simple $\mathbf{K}$-algebras. Using the tensor product $\otimes_{\mathbf{K}}$ it is possible to put a group structure on $Br(\mathbf{K})$, which is called the Brauer group of $\mathbf{K}$. Wedderburn proved that $Br(\mathbb{F}_p) = 0$. For a reference [21] Chapter IV.

Theorem 4.0.18. *Let $f \in S_2(\Gamma_0(N))$ be a newform with q-expansion $f = \sum a_n q^n$, let c be the conductor of the order $\mathcal{O}$ and let give ℓ be a prime, then*

$$\ell \mid c$$

if and only if

$$a_p \mod \lambda \in \boldsymbol{F} \subsetneq \mathbb{F}_{\ell^r} \quad \forall p \quad p \nmid N\,\ell$$

where $\lambda \mid l$, if and only if

$$f^\sigma \equiv f \mod \lambda$$

with $\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^r}/\boldsymbol{F})$ is the generator of the Galois group.

Proof. We would like to rewrite the problem in terms of congruence between modular forms. Let us recall that two newforms of the same level, $f = \sum a_n q^n$ and $g = \sum b_m q^m$, are congruent modulo λ if and only if their Fourier coefficients are congruent:

$$f \equiv g \mod \lambda \quad \Leftrightarrow \quad a_p(f) \equiv b_p(g) \mod \lambda \quad \forall p \;\; p \nmid N\,\ell$$

In our case we have a tower of fields:

$$\begin{array}{c} \mathbb{F}_{\ell^r} \\ \neq \Big| \ni\sigma \\ \mathbf{F} \\ \Big| \\ \mathbb{F}_\ell \end{array}$$

so clearly $\mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbf{F}) \subseteq \mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbb{F}_\ell)$ and we can take $\sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbf{F})$ the generator of the Galois group.
Let us fix $\widehat{a_p} := a_p \mod \lambda \in \mathbf{F}$. We have that $a_p \in \mathbb{Q}_f$ so $a_p^{\tilde{\sigma}} \in \mathbb{Q}_f^{\tilde{\sigma}}$ where $\tilde{\sigma} \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is such that $\tilde{\sigma}|_{D_\ell} \equiv \sigma \mod I_l$:

$$\begin{array}{ccc} a_p & \xrightarrow{\tilde{\sigma}} & a_p^{\tilde{\sigma}} \\ {\scriptstyle \mod \lambda}\downarrow & & \downarrow{\scriptstyle \mod \lambda} \\ \widehat{a_p} & \xrightarrow{\sigma} & \widehat{a_p^\sigma} \end{array}$$

generally it can be that $\widehat{a_p} \in \mathbb{F}_{\ell^r}$ and $\widehat{a_p^\sigma} \in \mathbb{F}_{\ell^{r'}}$ with $r \neq r'$.
We can say that $\tilde{\sigma}$ is a lift of σ, in fact:

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \supset D_\ell \;\; \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbf{F}) \;\; \hookrightarrow \;\; \frac{D_\ell}{I_\ell}$$

Now we can claim that our problem is equivalent to check the congruence between f and $f^{\tilde{\sigma}} \mod \lambda$. First of all, if $f \equiv f^{\tilde{\sigma}} \mod \lambda$ then $f \equiv f^{\sigma} \mod \lambda$ since $\sigma \equiv \tilde{\sigma} \mod \lambda$. The congruence $f \equiv f^{\tilde{\sigma}} \mod \lambda$ is equivalent to $a_p(f) \equiv a_p(f^{\tilde{\sigma}}) \mod \lambda \ \forall p \ p \nmid N\ell$ that is the same that $\widehat{a_p} = \widehat{a_p^{\sigma}} \ \forall p \ p \nmid N\ell$.
Now, from Galois Theory follows directly that the equality between $\widehat{a_p}$ and its conjugate $\widehat{a_p}^{\sigma}$ traslate into the fact that $\widehat{a_p}$ belongs to the base field $\mathbf{F} \subsetneq \mathbb{F}_{\ell^r}$ and this clearly holds if and only if $\ell \mid c$, the conductor of the order $\mathcal{O}$. □

To check a congruence of type $f \equiv f^{\sigma}$ is equivalent to look for Galois invariance of the newform that is the reason why its Fourier coefficients give rise to a smaller field if reduced.

Corollary 4.0.19. *ℓ is exceptional of type* (1) *if and only if $\widehat{a_p} = \widehat{a_p^{\sigma}}$ for $p \leq$ Sturm Bound, $p \nmid N \cdot \ell$.*

Proof. Applying Theorem 4.0.18 we know that if ℓ is exceptional of type (1) then $\forall p$ we have $\widehat{a_p} = \widehat{a_p^{\sigma}}$, that correspond to the congruence $f \equiv f^{\tilde{\sigma}} \mod \lambda$. Hence for Sturm Theorem we have that the condition $\widehat{a_p} = \widehat{a_p^{\sigma}} \ \forall p \ p \nmid N\ell$, which is equivalent to the congruence $f \equiv f^{\sigma} \mod \lambda$, can be checked until the Sturm bound, so $\widehat{a_p} = \widehat{a_p^{\sigma}}$ for $p \leq S.B.$, $p \nmid N\ell$, because the congruence itself can be checked until the Sturm Bound. □

Theorem 4.0.18 and Corollary 4.0.19 can be extended for newforms of weight greater than 2 and for newforms with non trivial character, the proof holds as it has been stated, the only change required reguards the Sturm Boud: for example in the case of newforms with character it is needed the bound referred to $\Gamma_1(N)$.

4.0.4 Exceptional prime of type (2)

Let us suppose that the prime ℓ is not exceptional of the previous types, so in the sense of Definition 4.0.17, we have that $\widehat{a_p} = a_p \mod \lambda$, $\lambda|\ell$, generate $\mathbb{F}_{\lambda} = \mathbb{F}_{\ell^r}$ and not any intermediate field. In this setting we focus on $\left\{\widehat{a_p^2}\right\}$: it can happen that $\{\widehat{a_p}\}$ generate $\mathbb{F}_{\ell^r}$ but $\left\{\widehat{a_p^2}\right\}$ belong to $\mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_{\lambda}$; this means that the form, once reduced, has an *"inner twist* $\mod \ell$*"*.

If $\{\widehat{a_p}\}$ generate $\mathbb{F}_{\lambda}$ but if $\left\{\widehat{a_p}^2\right\}$ belong to $\mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_{\lambda} \, \forall p$ then we will prove in the Proposition 4.0.21 that

$$Im(\mathbb{P}(\overline{\rho_{f,\lambda}})) \subseteq \mathbb{P}GL_2(\mathbb{F}_{\lambda'})$$

so the image is not "as large as possible", following Ribet, and ℓ is exceptional.

Definition 4.0.20. *ℓ is an exceptional prime of type (2) for the Galois representation associated to the newform $f = \sum a_n\, q^n$ if it is not exceptional of type (1), 0, $(*)$ and if $\exists \lambda$ such that $\lambda | \ell$ and*

$$\widehat{a_p^2} = a_p^2 \mod \lambda \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \quad \forall p \;\; p \nmid N\,\ell$$

where N is the level of the form.

Proposition 4.0.21. *Let f be a newform, $f = \sum a_n\, q^n$ such that*

$$\mathbb{F}(\{\widehat{a_p}\}_p) \subseteq \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda''} \;\; \forall \mathbb{F}_{\lambda''} \subsetneq \mathbb{F}_\lambda \;\; \textit{and} \;\; \mathbb{F}(\{\widehat{a_p}^2\}_p) \subseteq \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \;\; p \nmid N\,\ell$$

then we have that the image of the Galois representation is such that:

$$Im(\overline{\rho_{f,\lambda}}) \subseteq \left\langle GL_2(\mathbb{F}_{\lambda'}), \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \right\rangle |_{\det \in \mathbb{F}_\ell^*}$$

where $\alpha \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$ and $\alpha^2 \in \mathbb{F}_{\lambda'}$. So we have that

$$Im(\mathbb{P}(\overline{\rho_{f,\lambda}})) \subseteq \mathbb{P}GL_2(\mathbb{F}_{\lambda'})$$

Proof. If $\{\widehat{a_p}\} \in \mathbb{F}_\lambda = \mathbb{F}_{\ell^r}\, \forall p$ and $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda\, \forall p$ we have that

$$\begin{array}{c} \mathbb{F}_\lambda \\ \neq \Big| \exists \sigma \\ \mathbb{F}_{\lambda'} \\ \Big| \\ \mathbb{F}_\ell \end{array}$$

and so we can choose σ as a generator of $\mathrm{Gal}(\mathbb{F}_\lambda / \mathbb{F}_{\lambda'})$. The extension $\mathbb{F}_\lambda : \mathbb{F}_{\lambda'}$ has to be quadratic because by construction we are working on finite fields and so its degree has to be smaller or equal to 2, but $\widehat{a_p} \in \mathbb{F}_\lambda\, \forall p$ because ℓ is not exceptional of type (1) and $\widehat{a_p} \notin \mathbb{F}_{\lambda'}$, so the degree of the extension has to be 2. So we have that

$$\begin{array}{c} \mathbb{F}_{\ell^{2s}} = \mathbb{F}_{\ell^r} = \mathbb{F}_\lambda \\ \neq \Big| \exists \sigma \\ \mathbb{F}_{\ell^s} = \mathbb{F}_{\lambda'} \\ \Big| \\ \mathbb{F}_\ell \end{array}$$

Now we consider the application $\kappa : \mathcal{O} \to \mathcal{O}$, where $\mathcal{O} \subseteq \mathcal{O}_f$ is an order in the ring of integer of $\mathbb{Q}_f$, such that sends the trace of each matrix in the image of the Galois representation to the trace of the squared image:

$$\begin{array}{ccccc} & & Im(\rho_f) \subseteq GL_2(\mathcal{O}) & & \\ & & \in & & \\ p \longrightarrow \mathrm{Frob}_{\mathfrak{p}} & \xrightarrow{\rho} & \rho(\mathrm{Frob}_{\mathfrak{p}}) & \xrightarrow{\bullet^2} & (\rho(\mathrm{Frob}_{\mathfrak{p}}))^2 \\ & & \Big\downarrow \mathrm{Tr} & & \Big\downarrow \mathrm{Tr} \\ & & \mathrm{Tr}(\mathrm{Frob}_{\mathfrak{p}}) & \xrightarrow{\kappa} & \mathrm{Tr}((\mathrm{Frob}_{\mathfrak{p}})^2) \end{array}$$

Hence taken a matrix in the image of the representation, computing trace and determinant, using Deligne theorem and then applying κ:

$$\rho(\mathrm{Frob}_{\mathfrak{p}}) = \begin{pmatrix} a & * \\ 0 & b \end{pmatrix} \quad \mathrm{Tr}(\rho(\mathrm{Frob}_{\mathfrak{p}})) = a + b = a_p \quad \det(\rho(\mathrm{Frob}_{\mathfrak{p}})) = ab = p$$

$$(\rho(\mathrm{Frob}_{\mathfrak{p}}))^2 = \begin{pmatrix} a^2 & * \\ 0 & b^2 \end{pmatrix} \quad \mathrm{Tr}((\rho(\mathrm{Frob}_{\mathfrak{p}})))^2) = a^2 + b^2 = a_p^2 - 2ab = a_p^2 - 2p$$

where $\lambda \mid p$.
Then we have that tha map κ corresponds to a map betweens the coefficient of the q-expansion of the newform:

$$a_p \xrightarrow{\kappa} a_p^2 - 2p$$

Reducing modulo λ we have

$$\begin{array}{ccc} a_p & \xrightarrow{\kappa} & a_p^2 - 2p \\ \mathrm{mod}\ \lambda \Big\downarrow & & \Big\downarrow \mathrm{mod}\ \lambda \\ \widehat{a_p} & \xrightarrow{\tilde{\kappa}} & \widehat{a_p^2 - 2p} \in \mathbb{F}_{\lambda'} \end{array}$$

this holds for each p prime, $p \in \mathbb{Z}$, so in particular the element $\widehat{a_p^2 - 2p}$ belongs to $\mathbb{F}_{\lambda'}$ because $\widehat{a_p^2} \in \mathbb{F}_{\lambda'}$ and $-2p \in \mathbb{Z}$. For simplicity we will use this notation: $\widehat{b_p} := \widehat{a_p^2 - 2p}$.
Now we can consider the action of $\sigma \in \mathrm{Gal}(\mathbb{F}_\lambda / \mathbb{F}_{\lambda'})$ hence we obtain:

$$\begin{array}{ccc} \widehat{a_p} & \xrightarrow{\tilde{\kappa}} & \widehat{b_p} \\ \sigma \Big\downarrow & & \Big\downarrow \sigma \\ \widehat{a_p}^{\sigma} & \xrightarrow{\tilde{\kappa}} & (\widehat{b_p})^{\sigma} = \widehat{b_p} \in \mathbb{F}_{\lambda'} \end{array}$$

because σ acts trivially on $\mathbb{F}_{\lambda'}$ and $\widehat{b_p} \in \mathbb{F}_{\lambda'}$.

Lemma 4.0.22. *The image of the Galois representation in the hypothesis of Proposition 4.0.21 contains a subgroup of index* 2 *contained in* $GL_2(\mathbb{F}_{\lambda'})$.

Proof. Let us consider the map $\tilde{\kappa} : \mathbb{F}_\lambda \to \mathbb{F}_{\lambda'}$ that sends $\widehat{a_p} \in \mathbb{F}_\lambda$ to the element $\widehat{b_p} \in \mathbb{F}_{\lambda'}$, so it is the reduction of κ modulo λ. So let $G = Im(\overline{\rho})$, we can define a subgroup $G^2 = \left\langle M^2 \, \forall M \in G \right\rangle$ and look at the previous map as

$$\begin{array}{ccc} G & \xrightarrow{\bullet^2} & G^2 \\ \downarrow{\scriptstyle \tilde{\kappa}} & & \downarrow{\scriptstyle \tilde{\kappa}} \\ \widehat{a_p} & \xrightarrow{\tilde{\kappa}} & \widehat{b_p} \\ \downarrow{\scriptstyle \in} & & \downarrow{\scriptstyle \in} \\ \mathbb{F}_\lambda & & \mathbb{F}_{\lambda'} \end{array}$$

We know that $G \subseteq GL_2(\mathbb{F}_\lambda) \setminus GL_2(\mathbb{F}_{\lambda''}) \; \forall \mathbb{F}_{\lambda''} \subsetneq \mathbb{F}_{\lambda'}$ because by hypothesis the set of $\{\widehat{a_p}\}$ cannot be inculded in an intermediate field; while we have that $G^2 \subseteq GL_2(\mathbb{F}_{\lambda'})$ because, again by hypothesis, we have that $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'}$.
Now we will show that G^2 is a subgroup of index 2 in the image.
Let choose $\alpha \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$, such that $\alpha^2 \in \mathbb{F}_{\lambda'}$. For each choice of a matrix M such that $\mathrm{Tr}(M) \notin \mathbb{F}_{\lambda'}$ we have that $M \in G \setminus GL_2(\mathbb{F}_{\lambda'})$ and we can re-write it as $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} N = M$ and $N^2, M^2 \in G^2$. Now, since we are working on finite fields, and since $\alpha \,\mathrm{Tr}(N) = \mathrm{Tr}(M)$, it follows that $\mathrm{Tr}(N) \in \mathbb{F}_{\lambda'}$.
Now we can observe that $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \alpha^2 \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix}$ where $\begin{pmatrix} 1 & 0 \\ 0 & \alpha^2 \end{pmatrix} \in GL_2(\mathbb{F}_{\lambda'})$ and $\begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \in G \setminus GL_2(\mathbb{F}_{\lambda'})$, then $M = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} N = \begin{pmatrix} 1 & 0 \\ 0 & \alpha^2 \end{pmatrix} \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot N$ so $M = A \cdot M'$ where $A \in GL_2(\mathbb{F}_{\lambda'})$ and $M' = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot M''$.
Hence, if we have an element in G then either it is in G^2, that means in particular that is in $GL_2(\mathbb{F}_{\lambda'})$, or it is an element in $G \setminus GL_2(\mathbb{F}_{\lambda'})$ and so applying the previous observation and using the fact that we are working over finite fields, we obtain that this element has to be of the form $A \cdot Mat$ where $A \in GL_2(\mathbb{F}_{\lambda'})$ and $Mat = \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot Mat'$ where $Mat' \in GL_2(\mathbb{F}_{\lambda'})$.
So, if we consider again the hypothesis given, we obtain that G^2 has to have index two in G because the only coset we can consider are G^2 and $\begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot G^2$. From this we can say also that G^2 is a normal subgroup of G. □

For lemma 4.0.22 we have that in the image of the modular Galois representation there is an index two subgroup contained in $GL_2(\mathbb{F}_{\lambda'})$ and in particular from this follows that the image has to have the form

$$Im(\overline{\rho_{f,\lambda}}) \subseteq \left\langle GL_2(\mathbb{F}_{\lambda'}), \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \right\rangle |_{\det \in \mathbb{F}_\ell^*}$$

where $\alpha \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$ and $\alpha^2 \in \mathbb{F}_{\lambda'}$. For each possible choice of other matrix in $G \setminus GL_2(\mathbb{F}_{\lambda'})$ it is clear that we obtain the same set from what we have observed during the proof of lemma 4.0.22.
The Galois representation associated to f is irreducible by hypotesis, and through the map $\tilde{\kappa}$ and lemma 4.0.22 we have shown that its image cannot be maximal, because from $\widehat{a_p} \in \mathbb{F}_\lambda \, \forall p$ and $\widehat{a_p^2} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \, \forall p$ we have the existence of a normal subgroup, while if it would have been maximal then the image of the square power, used to define $\tilde{\kappa}$, had been defined in $GL_2(\mathbb{F}_\lambda)$ and not only in $GL_2(\mathbb{F}_{\lambda'})$.
Hence, applying Dickson Theorem in the projective case, the only case than can occur is

$$Im(\mathbb{P}(\overline{\rho_{f,\lambda}})) \subseteq \mathbb{P}GL_2(\mathbb{F}_{\lambda'})$$

In particular, as we have shown

$$Im(\overline{\rho_{f,\lambda}}) \subseteq \left\langle GL_2(\mathbb{F}_{\lambda'}), \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \right\rangle |_{\det \in \mathbb{F}_\ell^*} = G$$

where $\alpha \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$ and $\alpha^2 \in \mathbb{F}_{\lambda'}$ and from this choice follows that the matrices $\begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \in GL_2(\mathbb{F}_\lambda) \setminus GL_2(\mathbb{F}_{\lambda'})$ and $\begin{pmatrix} \alpha^2 & 0 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{F}_{\lambda'})$ are projectivly equivalent, then

$$\mathbb{P}(G) = \mathbb{P}(GL_2(\mathbb{F}_{\lambda'})) = \mathbb{P}GL_2(\mathbb{F}_{\lambda'})$$

□

Theorem 4.0.23. *Let $f \in S_2(\Gamma_0(N))$ be a newform, $f = \sum a_n \, q^n$ such that $\{\widehat{a_p}\}_p \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda''} \;\; \forall \mathbb{F}_{\lambda''} \subsetneq \mathbb{F}_\lambda$ then*

$$\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \, \forall p$$

if and only if there exist a quadratic Dirichlet character

$$\chi : (\mathbb{Z}/M\mathbb{Z})^* \to \{\pm 1\}$$

such that

$$f^\sigma \equiv \chi \, f \mod \lambda$$

where σ is the generator of the Galois group of the extension $\mathbb{F}_\lambda / \mathbb{F}_{\lambda'}$.

Proof. First suppose that $\{\widehat{a_p}\}_p \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda''} \ \ \forall \mathbb{F}_{\lambda''} \subsetneq \mathbb{F}_\lambda$ and $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \, \forall p$. We can apply the result of Proposition 4.0.21 so we have that

$$Im(\overline{\rho_{f,\lambda}}) \subseteq \left\langle GL_2(\mathbb{F}_{\lambda'}), \begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \right\rangle |_{\det \in \mathbb{F}_\ell^*}$$

where $\alpha \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$ and $\alpha^2 \in \mathbb{F}_{\lambda'}$.
We know that in the image is contained a normal subgroup of index two, let us call it H (previously it has been denoted as G^2), so for Galois theory follows that this corresponds to a quadratic extension $\mathbf{K}$ of $\mathbb{Q}$ such that $\mathrm{Gal}(\mathbf{K}/\mathbb{Q}) \cong G/H$, where as usual $G = Im(\overline{\rho})$ and $H \subseteq GL_2(\mathbb{F}_{\lambda'})$:

$$\begin{array}{c} \overline{\mathbb{Q}} \\ | \\ \mathbf{K} \\ | \\ \mathbb{Q} \end{array}$$

We can associate to this quadratic extension a quadratic Dirichlet character χ such that $\chi(p) = 1 \ \forall p$ such that p splits in $\mathbf{K}$ and $\chi(p) = -1 \ \forall p$ that don't split in $\mathbf{K}$. In particular if p splits in $\mathbf{K}/\mathbb{Q}$ we have that $\overline{\rho}(\mathrm{Frob}_\mathfrak{p}) \in H$ while if p is stable in $\mathbf{K}/\mathbb{Q}$ we have that $\overline{\rho}(\mathrm{Frob}_\mathfrak{p}) \in G \setminus H$.

$$\begin{array}{rrrrl} p & \text{splits in} & \mathbf{K}/\mathbb{Q} & \Leftrightarrow & \chi(p) = 1 \quad \Leftrightarrow \overline{\rho}(\mathrm{Frob}_\mathfrak{p}) \in H \\ p & \text{not split in} & \mathbf{K}/\mathbb{Q} & \Leftrightarrow & \chi(p) = -1 \quad \Leftrightarrow \overline{\rho}(\mathrm{Frob}_\mathfrak{p}) \in G \setminus H \end{array}$$

$$\begin{array}{ccc} \overline{\mathbb{Q}} & & \{id\} \\ {\scriptstyle q\in}\big| & & \big| {\scriptstyle \ni \overline{\rho}(\mathrm{Frob}_q)} \\ \mathbf{K} & \overset{\overline{\rho}}{- - -} & H \\ {\scriptstyle r\in}\big| & & \big| {\scriptstyle \ni \overline{\rho}(\mathrm{Frob}_r)} \\ \mathbb{Q} & & G \end{array}$$

q, r primes

Now to prove that $f^\sigma \equiv \chi \, f \mod \lambda$ we have to show that $\widehat{a_p}^\sigma = \chi(p) \, \widehat{a_p} \ \forall p$ for the character χ that corresponds to $\mathbf{K}$.

If we consider a generic element of the image, it will have either the form $\begin{pmatrix} \alpha & 0 \\ 0 & \frac{1}{\alpha} \end{pmatrix} \cdot M$ either simply M, where $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{F}_{\lambda'})$.

In the first case it will be of type $\begin{pmatrix} \alpha a & \alpha b \\ \frac{c}{\alpha} & \frac{d}{\alpha} \end{pmatrix}$ so its trace is $\alpha \, a + \frac{1}{\alpha} \, d \in \mathbb{F}_\lambda$,

going on with computation we have that $\frac{\alpha^2 a+d}{\alpha} \in \mathbb{F}_\lambda$.
Let us choose a prime p such that $\overline{\rho}(\mathrm{Frob}_\mathfrak{p}) \in G \setminus H$, for this prime we have that $\chi(p) = -1$, in particular $\overline{\rho}(\mathrm{Frob}_\mathfrak{p}) = M_p \notin GL_2(\mathbb{F}_{\lambda'})$ and we have that $M_p^2 \in GL_2(\mathbb{F}_{\lambda'})$, that corresponds to image of form described in the first case. Hence looking at the trace of M_p we have that or it is 0, if $\alpha^2 a + d = 0$, that corresponds to $\widehat{a_p} = 0$, either if $\widehat{a_p} \neq 0$, $\widehat{a_p} \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$ and $\widehat{a_p}^2 \in \mathbb{F}_{\lambda'}$. In this last possibility $\widehat{a_p}^2 \in \mathbb{F}_{\lambda'}$ implies $(\widehat{a_p}^2)^\sigma = \widehat{a_p}^2 \in \mathbb{F}_{\lambda'}$. Now we can remember that the action of σ correspond to take the ℓ^r power, so the previous expression can be state as: $(\widehat{a_p}^2)^{\ell^r} = \widehat{a_p}^2$, that can be traslated in

$$\widehat{a_p}^{\ell^r - 1} = -1$$

because $\widehat{a_p} \in \mathbb{F}_\lambda \setminus \mathbb{F}_{\lambda'}$.
So we can write $\widehat{a_p}^\sigma = -\widehat{a_p} = \chi(p)\,\widehat{a_p}$ for p that not split in $\mathbf{K}$.

In the second case, we have that $M \in GL_2(\mathbb{F}_{\lambda'})$ so its trace is in $\mathbb{F}_{\lambda'}$.
Let us choose a prime q such that $\overline{\rho}(\mathrm{Frob}_q) \in H \subseteq GL_2(\mathbb{F}_{\lambda'})$, for this prime we have that $\chi(q) = 1$. Then $\overline{\rho}(\mathrm{Frob}_q) = M_q \in GL_2(\mathbb{F}_{\lambda'})$ then $\widehat{a_q} \in \mathbb{F}_{\lambda'}$ so $\widehat{a_q}^\sigma = \widehat{a_q} \in \mathbb{F}_{\lambda'}$ and so we can write that $\widehat{a_q}^\sigma = \chi(q)\,\widehat{a_q}$ for q that splits in $\mathbf{K}$. Again we have the equality $(\widehat{a_p}^2)^{\ell^r} = \widehat{a_p}^2$, that can be traslated in

$$\widehat{a_p}^{\ell^r - 1} = 1$$

because $\widehat{a_p} \in \mathbb{F}_{\lambda'}$.
Hence, applying Čebotarev density theorem, it is possible define the character $\chi : (\mathbb{Z}/N\mathbb{Z})^* \to \{\pm 1\}$ that satisfies the previous condition, and so we have shown that $\widehat{a_p}^\sigma = \chi(p)\,\widehat{a_p}\ \forall p$ then $f^\sigma \equiv \chi\, f \mod \lambda$.

On the other hand let's suppose $\widehat{a_p}^\sigma = \chi(p)\,\widehat{a_p}\ \forall p$, we have to show that $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda$. Because $\chi(p)$ is a Dirichlet character related to a quadratic extension, its values can be only ± 1 or 0, so we have that:

$$\widehat{a_p}^\sigma = \pm\,\widehat{a_p} \quad (\widehat{a_p}^\sigma)^2 = (\widehat{a_p})^2$$

The action of σ commutes with the power, so

$$(\widehat{a_p^2})^\sigma = (\widehat{a_p^2})$$

with $\sigma \in \mathrm{Gal}(\mathbb{F}_\lambda/\mathbb{F}_{\lambda'})$. This means that $\widehat{a_p^2}$ is fixed under the action of the Galois group, and so $\widehat{a_p^2} \in \mathbb{F}_{\lambda'}$. □

Lemma 4.0.24. *Given a modular form $f \in S_2(\Gamma_0(N))$, for $p \neq \ell$ if $p^i \,||\, N$, then we have that $p^j \,||\, M$ $j \leq i$ where M is the Artin conductor of $\overline{\rho_{f,\lambda}}$.*

Proof. A proof of this statement can be found in [18]. □

Proposition 4.0.25. *Let us suppose $f^\sigma \equiv \chi f \mod \lambda$ where $f \in S_2(\Gamma_0(N))$ is a newform, $\sigma \in \mathrm{Gal}(\boldsymbol{K}/\boldsymbol{K}')$, with $\boldsymbol{K}$ and $\boldsymbol{K}'$ are finite fields, and χ is a quadratic Dirichlet character. If $\lambda \mid \ell$, $\ell > 2$, $\ell^2 \nmid N$ then χ cannot ramify in ℓ.*

Proof. If we have that $f^\sigma \equiv \chi f \mod \lambda$ we can consider the associated modular representations that will satisfy:

$$\overline{\rho}_{f^\sigma,\lambda} = \overline{\rho}_{f,\lambda} \otimes \tilde{\chi}$$

where $\tilde{\chi}$ is the quadratic Dirichlet character that lifts χ, and it's defined from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$. Let us choose ℓ such that $\lambda \mid \ell$, and consider the Artin conductor N of the associated Galois representation. From $f^\sigma \equiv \chi f \mod \lambda$ se have a similar picture for Galois representation:

$$\overline{\rho}_{f^\sigma,\lambda}|_{I_\ell} = (\overline{\rho}_{f,\lambda} \otimes \tilde{\chi})|_{I_\ell}$$

that is

$$\overline{\rho}_{f^\sigma,\lambda}|_{I_\ell} = (\overline{\rho}_{f,\lambda})|_{I_\ell} \otimes \tilde{\chi}$$

If $\ell \nmid N$, we have that $\overline{\rho_{f^\sigma,\lambda}}|_{I_\ell}$ is equivalent to $\begin{pmatrix} \eta & * \\ 0 & 1 \end{pmatrix}$ where η is the cyclotomic character $\mod \ell$ or to $\begin{pmatrix} \psi & * \\ 0 & \psi^\ell \end{pmatrix}$ where ψ is a fondamental character $\mod \ell$. While if $\ell \mid\mid N$, it will occour that $\overline{\rho_{f^\sigma,\lambda}}|_{I_\ell}$ is equivalent to $\begin{pmatrix} \eta & * \\ 0 & 1 \end{pmatrix}$ where, again, η is the cyclotomic character $\mod \ell$.
In both case we will procede by contradiction, so let us suppose that $\tilde{\chi}$ ramifies in ℓ. It is clear that $(\tilde{\chi})|_{I_\ell}$ is of the form $\eta^{\frac{\ell-1}{2}}$ because it is a quadratic character $\mod \ell$ that ramifies in ℓ. So, proceding with direct computation from $\overline{\rho}_{f^\sigma,\lambda}|_{I_\ell} = (\overline{\rho}_{f,\lambda} \otimes \tilde{\chi})|_{I_\ell}$, where we have that $\overline{\rho}_{f^\sigma,\lambda}$ and $\overline{\rho}_{f,\lambda}$ has to have the same form restricted to I_ℓ, we obtain a contradiction in the case $\begin{pmatrix} \eta & * \\ 0 & 1 \end{pmatrix}$ and in the other case $\begin{pmatrix} \psi & * \\ 0 & \psi^\ell \end{pmatrix}$ we have that $\psi\, \chi^{\frac{\ell-1}{2}} = \psi^\ell$, and, once observed that $\psi^{\ell+1} = \chi$, $\psi^{\frac{(\ell-1)^2}{2}} = 1$, that gives a contradiction if $\frac{(\ell-1)^2}{2} \neq \ell^2 - 1$ and so for all $\ell \geq 3$.
Hence χ cannot ramify in ℓ, $\ell > 2$, $\lambda \mid \ell$. □

Proposition 4.0.26. *Let N and r be positive integers and M the least common multiple of N and r^2. Let χ be a primitive character of $(\mathbb{Z}/r\mathbb{Z})^*$ and let $f(z) = \sum_{n=1}^\infty a_n q^n$ be a cuspidal form in $S_k(\Gamma_0(N))$. Then $h = \chi f$, $h(z) = \sum_{n=1}^\infty \chi(n) a_n q^n$ belongs to $S_k(\Gamma_0(M), \chi^2)$. In particular if χ is a quadratic character, follows that $h \in S_k(\Gamma_0(M))$.*

Proof. Put $\xi = e^{2\pi i \frac{1}{r}}$ and $\alpha_u = \begin{pmatrix} 1 & \frac{u}{r} \\ 0 & 1 \end{pmatrix}$ for $u \in \mathbb{Z}$. Then

$$f|\,[\alpha_u]_k = \sum_{n=1}^{\infty} a_n\, e^{2\pi i n (z+\frac{u}{r})} = \sum_{n=1}^{\infty} a_n\, \xi^{nu} e^{2\pi i n z}$$

so we have that, defyning the Gauss sum associated to χ as

$$W(\chi) = \sum_{c=0}^{r-1} \chi(c)\xi^c$$

then

$$\sum_c \chi(c)\xi^{bc} = \sum_a \chi(b^{-1}a)\xi^a = \chi(b^{-1}) \sum_a \chi(a)\xi^a = \overline{\chi}(b)W(\chi)$$

and from this and the form of f follow that

$$W(\overline{\chi})h(z) = \sum_{u=1}^{r} \overline{\chi}(u) f|\,[\alpha_u]_k$$

This means that $h \in S_k(\Gamma(r^2N))$ because, for a modular form, the application $h \to h|\,[\alpha]_k$ is an injection and in this case it's surjective for the choise of α_u done. Hence to prove our statement, it is sufficient to check the behaviour of h under an element $\gamma = \begin{pmatrix} a & b \\ cM & d \end{pmatrix} \in \Gamma_0(M)$. We have that $f|\,[\alpha_u\,\gamma]_k = d^2\, f|\,[\alpha_u]_k$, so with the previous expression we obtain:

$$h|\,[\gamma]_k = W(\chi)^{-1}\chi(d^2) \sum_v \overline{\chi}(v) f|\,[\alpha_v]_k = \chi(d^2)h(z)$$

so $S_k(\Gamma_0(M), \chi^2)$. If χ is a quadratic character the assertion follows trivially. □

Corollary 4.0.27. *Let us suppose $q \neq \ell$, $q > k$ and $q \mid N$ where N is the Artin conductor of the modular representation $\overline{\rho_{f,\lambda}}$, then if χ ramifies in q then $q^2 \mid N$.*

Proof. This follows from Proposition 4.0.26 and lemma 4.0.24. □

Corollary 4.0.28. *If ℓ is exceptional of type (2), $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda\, \forall p$ then the condition about coefficient is equivalent to check the congruence between f^σ and $\chi(p)f$ until the Sturm Bound computed for the minimum common multiple between the level of f and the conductor of the character squared.*

Proof. For the previous theorem we have that $\left\{\widehat{a_p^2}\right\} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \, \forall p$ corresponds to

$$\widehat{a_p}^\sigma = \chi(p)\, \widehat{a_p} \, \forall p \longleftrightarrow f^\sigma \equiv \chi(p)\, f \mod \lambda \, \forall p$$

So this congruence can be computed using the Sturm Bound, so in particular can be checked until the Sturm Bound computed the minimum common multiple between the level of f and the conductor of the character squared following Proposition 4.0.26. □

For $\ell = 2, 3$, ℓ is an exceptional prime of type (2) if and only if ℓ is not exceptional for the previous cases and satisfies the same condition:

$$f^\sigma \equiv \chi\, f \mod \lambda$$

where χ is a Dirichlet character as before but that can ramify at $\ell = 2, 3$.

Theorem 4.0.23 does not hold in dimension greater than 2 as it is stated, because in this case the form taken by the determinant by Deligne-Serre Theorem does not allow the same result. Meanwhile, introducing a nebentypus, the result still holds.

4.0.5 Exceptional prime of type (3)

Assume ℓ is not exceptional for the previous cases.

Definition 4.0.29. *ℓ is an* exceptional prime of type (3) *for the Galois representation associated to the modular form $f = \sum a_n q^n$ if $\exists \lambda \in \mathcal{O}$, $\lambda \mid \ell$, $\ell \nmid N$, such that $\overline{G_\lambda} = \overline{\rho_\lambda}(G_\mathbb{Q})$ is a dihedral subgroup of $GL_2(\boldsymbol{F}_\lambda)$.*

In this case we have that there exists a Cartan subgroup $C_\lambda \subseteq GL_2(\mathbf{F}_\lambda)$ such that $\overline{G_\lambda}$ is contained in the normalizer N_λ of C_λ, but not in C_λ. Let conside $\phi_\lambda : G_\mathbb{Q} \to \{\pm 1\}$ as the composition:

$$G_\mathbb{Q} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{G_\lambda} \subseteq N_\lambda \to \frac{N_\lambda}{C_\lambda} \cong \{\pm 1\}$$

The kernel of ϕ_λ is an open subgroup of $G_\mathbb{Q}$ of index 2, so its fixed field K_λ is quadratic and unramified outside $N\ell$. In particular following Serre [33] we have that K_λ is not ramified at ℓ if $\ell > 3$.
With similar arguments as in Theorem 4.0.23 we have the following Lemma:

Lemma 4.0.30. *Suppose that $\ell > 3$ we have $a_p \equiv \alpha(p) a_p \mod \lambda \, \forall p \nmid N\ell$ where α is a quadratic charater. In particular if N is squarefree no λ verifies this Lemma.*

Again using Livnè we can say that the quadratic character α is unramified otside $\prod_{r|N \; r^2|N}^{r\, prime} r$. Hence, also this case can be seen as a congruence between modular forms and so computed using Sturm bound:

Corollary 4.0.31. *ℓ is an exceptional prime of type* (3) *if and only if*

$$f \equiv \alpha\, f \mod \lambda$$

where α is a quadratic character which is unramified outside

$$\prod_{\substack{r\, prime \\ r|N\ r^2|N}} r$$

.

Again for $\ell = 2, 3$, in the case of modular forms of weight 2, ℓ is an exceptional prime of type (3) if and only if ℓ is not exceptional for the previous cases and satisfies the same condition:

$$f^{\sigma} \equiv \alpha\, f \mod \lambda$$

where this time α can ramify at $\ell = 2, 3$.

4.0.6 Exceptional prime of type (4)

Suppose ℓ not exceptional for the previous cases.

Definition 4.0.32. *ℓ is an* exceptional prime of type (4) *for the Galois representation associated to the modular form $f = \sum a_n q^n$ if $\exists \lambda \in \mathcal{O}$, $\lambda \mid \ell$, $\ell \nmid N$, such that $\overline{G_\lambda} = \overline{\rho_\lambda}(G_{\mathbb{Q}})$ is isomorphic to a special group A_4, S_4 or A_5.*

From Serre [32] we are allowed to say that ℓ is an exceptional prime of type (4) if the coefficients of the modular form sataisfy certain conditions:

Proposition 4.0.33. *ℓ is an exceptional prime of type (4) for the Galois representation associated to the $f \in S_2(N)$ if $\exists \lambda \in \mathcal{O}$, $\lambda \mid \ell$, $\ell \nmid N$, such that $\forall p \nmid \ell N$:*

$$a_p^2 \equiv 0,\, p,\, 2p,\, 4p \mod \lambda \qquad or \qquad a_p^4 - 3p\, a_p^2 + p \equiv 0 \mod \lambda$$

Following the argument in Ribet [25] it is possible to prove that this case cannot occour if $\ell \geq 7$ for irreducible residual representations, weight 2 case. This because the image of the restriction of $\overline{\rho}_\lambda$ to an inertia subgroup for ℓ contains an element of order $\ell \pm 1$, so when $\ell \geq 7$ the image cannot be of type (4). In the case of N square-free, Ribet [25] proved that this case is ruled out even for $\ell = 5$.
Actually, it is not possible state the equivalence of a congruence between modular forms and exceptionality of type (4), it seems this is not the case. In this case other methods can be applied like those of Kiming in [12] to check exceptionality of this type.

Chapter 5

Algorithm

5.1 Description of the algorithm

At this point we can give a description of the algorithm for checking if a prime is exceptional for the residual modular Galois representation. The algorithm soon will be published on SAGE webpage:

http://www.sagenb.org/pub/

Let us suppose we have a newform $f \in S_2(N)$ and we want to certify if a prime ℓ is an exeptional prime for its Galois residual representation:

$$\overline{\rho_\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_{\ell^r})$$

for $\lambda \in \mathcal{O}_f$, $\lambda \mid \ell$, where r is the degree of inertia at λ.

Step (0)

Using Theorem 1.1.35 we compute the set of exceptional primes of type $(*)$: firstly we compute the maximal order for $\mathbb{Q}_f$, that in the weight 2 case is the ring of integer $\mathcal{O}_f$, and then its discriminant ant its factorisation. The primes that occours in the factorisation are exceptional primes of type $(*)$ according to Definition 4.0.10.

Step (1)

Find the maximal c such that $c^2 \mid N$ and a coefficient a_p with $p \equiv 1 \mod c$ such that:

$$p \nmid \ell N \quad \text{and} \quad a_p - (1+p) \equiv 0 \mod \lambda$$

for any $\lambda \mid \ell$. Checking the congruence is the same that observe that holds $\ell \mid \mathrm{Norm}(a_p - (1+p))$. Similarly, we could take a prime $p \equiv -1 \mod c$ such that:

$$p \nmid \ell N \quad \text{and} \quad a_p \equiv \pm(1+p) \mod \lambda$$

and again check that $\ell \mid \mathrm{Norm}(a_p \pm (1+p))$. Then it can be that the prime ℓ is a reducible prime for the Galois representation.
Note that in the squarefree case, this control can be translated into finding all primes ℓ such that

$$\forall p \nmid \ell N \text{ and } a_p - (1+p) \equiv 0 \mod \lambda$$

so such that $\ell \mid \mathrm{Norm}(a_p - (1+p))$.
In this way, after taking out all primes of type $(*)$ and adding all the primes of the level and the prime 2, if they are not exceptional of type $(*)$, we get a set of possible reducible primes for the modular residual Galois representation. Now we have to certify if the prime in the set determined it is really exceptional or not.

Step $(*)$

For each prime ℓ in the set obtained we consider the reduction $\mod \ell$ of the minimal polynomial of α, where α is an algebraic integer, given by SAGE, in terms of which it is possible to express all the coefficients of the Fourier expansion associated to the newform considered.
Once obtained the reduced polynomial we factor it and, from the factorisation, we read off all the data about ramification and inertia needed thanks to Theorem 1.2.7 and Corollary 1.2.9 when α has optimal behaviour in the sense of Theorem 1.2.7, while if this does not happen we change α with an optimal integer and apply the result. Then we use the roots of each factor to compute $\alpha \mod \lambda$ and use this datum to get form $a_p = P(\alpha)$, $\widehat{a_p} = a_p \mod \lambda$.
Hence from this Step we have all the data to check any needed conguence, since we have all finite fields where the congruences should be stated and all the values $\mod \lambda$.

Step (1) continuation

After going trought Step $(*)$ we can easily compute the congurence corresponding to the reducible case:

$$f \equiv \epsilon + \chi\, \epsilon^{-1} \mod \lambda$$

Firstly we can apply Proposition 4.0.14 and 4.0.16 to get a set of possible characters ϵ, and for each of them check if the conguence of Corollary 4.0.13 holds:

$$a_p \equiv \epsilon(p) + p\, \epsilon^{-1}(p) \mod \lambda$$

if the condition is true for a character up to the Sturm bound of level N, the level of the newform considered, then the prime is exceptional of type (0) since for the Sturm Theorem we get a congruence of the newform with a sum of characters and so its reduced image has to be a reducible subgroup of $GL_2(\mathbf{F}_\lambda)$.

Now in order to proceed in the analysis we have first to check that the modular form is not of CM type and it does not have inner twist:

Step (2)

It is known (Ribet [29]) that a newform $f \in S_2(N)$ does not have CM neither inner twists if the level is squarefree. If $\exists\, q \,||\, N$ then the modular form does not have CM, this comes out from a Neron model of the abelian variety A_f associated to f at q, for a reference [3]. In the general case, for a modular form have CM it is equivalent to

$$f = f \otimes \psi$$

where ψ is a Dirichlet character which can ramify at primes $q \mid N$ such that $q^2 \mid N$, so for each character we have to verify that the form is not CM.
To check that the form has not inner twist, it is sufficient to show that $\exists\, a_p$ such that

$$\mathbb{Q}\left(\left\{a_p^2\right\}\right) = \mathbb{Q}\left(\{a_p\}\right) = \mathbb{Q}_f$$

because in this way it is shown the absence of a twist.

Now we will poceed checking each case, giving a set o possible exceptional primes and then certifying exceptionality using the corresponding congruence between modular forms.

Step (3)

Let us suppose given the set Σ of relevant primes for the previous steps and let consider $\ell \notin \Sigma$, taken $\lambda \mid \ell$, I would like to check if ℓ is exceptional or not in the direction of Definition 4.0.17. Let us suppose $\overline{\rho_{f,\lambda}}$ irreducible. We want to check the structure of the image, in particular if it is surjective

$$Im(\overline{\rho_{f,\lambda}}) = GL_2(\mathbb{F}_\lambda)|_{\det \in \mathbb{F}_\ell^*}$$

or not. For Theorem 4.0.18 if we take $\ell \mid c$ where c is the observed conductor of the order, and we have that $\widehat{a_p} \in \mathbb{F}_{\lambda'} \subsetneq \mathbb{F}_\lambda \ \ \forall p$ then λ is exceptional, and so ℓ, because

$$Im(\overline{\rho_{f,\lambda}}) \subseteq GL_2(\mathbb{F}_{\lambda'})|_{\det \in \mathbb{F}_\ell^*}$$

In fact to compute a set of primes that can be of type (1), we compute the factorisation of the discriminant of the minimal polynomial of each a_p and

check if there are primes that come out in each factorisation. These primes, if are not in Σ, are suspected to be primes of type (1). For each of them we apply Step $(*)$.
Now, having all the data from Step $(*)$, we can apply Theorem 4.0.18 and checking the congruence:

$$f \equiv f^{\sigma} \mod \lambda \quad a_p \equiv a_p^{\sigma} \mod \lambda \ \ \sigma \in \mathrm{Gal}(\mathbb{F}_{\ell^r}/\mathbb{F}_{\ell^s})$$

up to the Sturm bound of level N, according to Corollary 4.0.19 to check if the prime it is of type (1) or not.
We will consider only one step of this process that, as it is clear, can be iterated.

Step (4)

Let us suppose given the set Σ' of relevant primes for the previous steps and let consider $\ell \notin \Sigma'$, taken $\lambda \mid \ell$, I would like to check if ℓ is exceptional or not in the direction of Definition 4.0.20.
In fact it can happen that we have a patological situation in which $\{\widehat{a_p}\}$ generate $\mathbb{F}_\lambda$ but $\left\{\widehat{a_p^2}\right\}$ generate a smaller field $\mathbb{F}_{\lambda'} \subset \mathbb{F}_\lambda$, so we have an "inner twist mod p" and the projective image is strictly contained in $PGL_2(\mathbb{F}'_\lambda)$, $\det \in \mathbb{F}_\ell^*$. In order to compute a set of primes that can be of type (2), we compute the factorisation of the discriminant of the minimal polynomial of each a_p^2 and check if there are primes that come out in each factorisation. These primes, if are not in Σ', are suspected to be primes of type (2). Adding all the primes of the level and the primes 2,3, if they are not in Σ', we get a set of possible primes of type (2) for the modular residual Galois representation.
For each of them we apply Step $(*)$. So we can check the congruence of Corollary 4.0.28 up to the correct Sturm Bound specified in the Corollary 4.0.28: $lcm(N, cond(\psi)^2)$, once determined the set of quadratic characters given by Proposition 4.0.25 and Corollary 4.0.27. If we have that

$$f^{\sigma} \equiv \psi \cdot f \quad a_p^{\sigma} \equiv \psi(p) a_p \mod \lambda$$

then we have that $\left\{\widehat{a_p^2}\right\}$ generate a smaller field $\mathbb{F}_{\lambda'}$ and so ℓ is exceptiona for Definition 4.0.20.

Step (5)

Let us suppose given the set Σ'' of relevant primes for the previous steps and let consider $\ell \notin \Sigma''$, taken $\lambda \mid \ell$, I would like to check if ℓ is exceptional or not for Definition 4.0.29.
To compute a set of primes that can be of type (3), we compute firstly the

set of quadratic characters using Corollary 4.0.31, and then for each character α we compute the list of primes p such that $\alpha(p) = -1$. For each prime we consider the corresponding a_p and then we check if in there are primes that come out in the factorisation of the norms for each a_p considered. In this way we obtain a set of possible prime of type (3). Adding all the primes of the level and the primes 2,3, if they are not in Σ'', we get a set of possible primes of type (3).
Now for each prime in the set obtained we can apply Step $(*)$ and check the congruence stated in Corollary 4.0.31

$$f \equiv \alpha \cdot f \quad a_p \equiv \alpha(p)a_p \mod \lambda$$

for the corresponding quadratic character, recalling that in this case the Sturm bound needed is the one for $lcm(N, cond(\alpha)^2)$. Hence we can certify if a prime is of type (3) or not.

Step (6)

In this case according to the fact that the level is squarefree or not, we can determine the set of possible primes of type (4) cheching the conditions given by Proposition 4.0.33.
For a prime that could be of type (4), the method given by Kiming-Verrill in [12] can certify if the prime is exceptional of type (4) or not.

The algorithm described above has been implemented in SAGE, a symbolic programmation language based on Phyton.

5.2 Examples and comments

In this section we will give examples about the classification explained in Chapter 4 about exceptional primes for modular residual Galois representations. To refer to a particular newform in a given newform space we will follow SAGE index structure: in the first column of each table we have the index for SAGE numeration of the base of the newform space.

Exceptional prime of type $(*)$

Let us consider any newform $f \in S_2(429)$, we have that:

429	$p,\ a_p$	$\mathbb{Q}_f$	exceptional primes of type $(*)$
[0]	$5, 0;\ 7, 0$	$\mathbb{Q}$	none
[1]	$5, -2;\ 7, 0$	$\mathbb{Q}$	none
[2]	$5, \alpha-1;\ 7, -2\,\alpha-4$	$\mathbb{Q}\,(x^2+2\,x-1)$	[2]
[3]	$5, -\alpha-1;\ 7, -2$	$\mathbb{Q}\,(x^2-3)$	[2, 3]
[4]	$5, \alpha^2+\alpha-4;$ $7, \alpha^2-3$	$\mathbb{Q}\,(x^3+x^2-5\,x-3)$	[2, 3, 47]
[5]	$5, -\alpha^2+\alpha+2;$ $7, -\alpha^2+2\,\alpha+1$	$\mathbb{Q}\,(x^3-x^2-3\,x+1)$	[2, 37]
[6]	$5, -\alpha^2+\alpha+4;$ $7, -\alpha^2+3$	$\mathbb{Q}\,(x^3-3\,x^2-x+5)$	[2, 37]
[7]	$5, \alpha^3-6\,\alpha-1;$ $7, \alpha^3-5\,\alpha$	$\mathbb{Q}\,(x^4+2\,x^3-6\,x^2-12\,x-1)$	[2, 29, 73]

where we have determined the exceptional primes of type $(*)$ computing firtsly the maximal order in $\mathbb{Q}_f$, which for weight 2 newforms it is the ring of integers $\mathcal{O}_f$, and then applying Theorem 1.1.35. We can deepen the analysis, for example in the particular case of the newform [2], in fact in this case it is possible to apply Theorem 4.0.1 since $\mathbb{Q}_f = \mathbb{Q}_f^{gc}$. In particular using SAGE, it is possible to show that the automorphism $\sigma : \alpha \mapsto -\alpha - 2$ is such that

$$f \equiv f^\sigma \pmod 2$$

and using Sturm bound we have certified such a congruence.

f	$q + \alpha\,q^2 + q^3 + (-2\,\alpha-1)\,q^4 + (\alpha-1)\,q^5 + O(q^6)$
f^σ	$q + (-\alpha-2)\,q^2 + q^3 + (2\,\alpha+3)\,q^4 + (-\alpha-3)\,q^5 + O(q^6)$

Exceptional prime of type (0)

Applying the algorithm we get that in the space of newforms of level 226, there exists a newfom $f \in S_2(226)$ with $\mathbb{Q}_f = \mathbb{Q}\,(x^4 - 8x^3 - 6x^2 + 128x - 179)$, for which it is possible to certify using Sturm bound, for example, that 19 is an exceptional prime of type (0) but not of type $(*)$. In particular checking the whole newform space for this level we get

226	$p,\ a_p$	possible reducible primes	exceptional primes of type (0)
[0]	$3, -2\ ;\ 5, -4;$	$[2, 3]$	$[2]$
[1]	$3, \alpha + 1\ ;\ 5, -\alpha - 3;$	$[3]$	none
[2]	$3, -1/2\,\alpha - 1/2\ ;\ 5, 2;$	none	none
[3]	$3, \alpha - 1\ ;\ 5, 1/2\,\alpha^3 - 5/2\,\alpha^2 - 1/2\,\alpha + 17/2;$	$[3, 19]$	$[19]$

The result obtained agree with a conjecture by Ribet-Jimenez-Dieulefait, for a reference [6], for which when the level is product of two primes, $N = p \cdot q$, then the exceptional primes of type (0), satisfy:

$$\ell \mid p + 1 \quad \text{or} \quad \ell \mid p - 1 \ \text{ and } \ q \equiv 1 \mod \ell \ \text{ or } \ q \equiv x^{\ell} \mod p$$

or simmetrically with respect to q:

$$\ell \mid q + 1 \quad \text{or} \quad \ell \mid q - 1 \ \text{ and } \ p \equiv 1 \mod \ell \ \text{ or } \ p \equiv x^{\ell} \mod q$$

In this particular case $226 = 2 \cdot 113$ and $19 \mid (113 + 1)$.
Similarly in the space of newforms of level 113, for the newfom $f \in S_2(113)$, number [3], is possible to certify that 7 is an exceptional prime of type (0). Again this result can be obtained using Theorem of Mazur, Corollary 4.0.15, for a reference [9], which say that in case of prime level all the primes $\ell > 3$ such that $\ell \mid N - 1$ are exceptional primes of type (0).

113	$p,\ a_p$	possible reducible primes	exceptional primes of type (0)
[0]	$3, 2\ ;\ 5, 2\ ;\ 7, 0;$	$[2, 3]$	$[2]$
[1]	$3, 1/2\,\alpha - 1/2\ ;\ 5, -\alpha + 3\ ;\ 7, 4;$	none	none
[2]	$3, -\alpha^2 - 2\,\alpha - 1\ ;\ 5, 2\,\alpha^2 + 2\,\alpha - 3\ ;\ 7, -\alpha^2 - \alpha - 2;$	$[2, 3]$	none
[3]	$3, \alpha^2 - 5\ ;\ 5, -1\ ;\ 7, -\alpha^2 - \alpha + 6;$	$[2, 7]$	$[7]$

Other examples obtained are collected in the following table:

	$p,\ a_p$	possible reducible primes	exceptional primes of type (0)
57			
[0]	$3,-1\ ;\ 5,-3\ ;\ 7,-5;$	$[2,3]$	none
[1]	$3,1\ ;\ 5,1\ ;\ 7,3;$	$[2,3,5]$	$[5]$
[2]	$3,1\ ;\ 5,-2\ ;\ 7,0;$	$[2,3]$	$[2]$
207			
[0]	$3,0\ ;\ 5,0\ ;\ 7,-2;$	$[2,3]$	$[2]$
[1]	$3,0\ ;\ 5,-\alpha-3\ ;\ 7,\alpha-1;$	$[3,7]$	none
[2]	$3,0\ ;\ 5,-\alpha+1\ ;\ 7,\alpha+1;$	$[2,3]$	$[2]$
[3]	$3,0\ ;\ 5,2\,\alpha\ ;\ 7,-2\,\alpha+2;$	$[2,3,11]$	none
[4]	$3,0\ ;\ 5,-\alpha+3\ ;\ 7,-\alpha-1;$	$[3,7]$	none
336			
[0]	$3,-1\ ;\ 5,-2\ ;\ 7,1;$	$[2,3]$	$[2]$
[1]	$3,-1\ ;\ 5,0\ ;\ 7,-1;$	$[2,3]$	$[2]$
[2]	$3,-1\ ;\ 5,2\ ;\ 7,1;$	$[2,3]$	$[2]$
[3]	$3,1\ ;\ 5,-2\ ;\ 7,1;$	$[2,3]$	$[2]$
[4]	$3,1\ ;\ 5,2\ ;\ 7,-1;$	$[2,3]$	$[2]$
[5]	$3,1\ ;\ 5,4\ ;\ 7,1;$	$[2,3]$	$[2]$

Exceptional prime of type (1)

Let us consider a Newform $f \in S_4(13,\chi_{13})$, of weight 4, level 13 and quadratic Dirichlet character χ_{13} of conductor 13. In this case we can prove that 3 is an exceptional prime of type (1): all the $\widehat{a_p}$ up to Sturm bound belong to $\mathbb{F}_3$, meanwhile, computing inertia, they have to belong to $\mathbb{F}_{3^2}$.

$13,\chi_{13}$ weight 4	$\mathbb{Q}_f$	q-expansion	exceptional primes of type (1)
	x^2+9	$q+\alpha\,q^2-q^3-q^4-3\,\alpha\,q^5-\alpha\,q^6-5\,\alpha\,q^7+7\,\alpha\,q^8-26\,q^9+27\,q^{10}+O(q^{11})$	$[3]$

In the same way, we can consider the space of newforms of level 207. In this case we can prove that exists a newform for which [2] is a reducible prime. If we want to deepen the study of the Galois residual representation we can show that [2] is also a prime of type (1) since all a_p once reduced have a priori to belong to $\mathbb{F}_4$ while they belong to $\mathbb{F}_2$. In this case we want compute the image directly.
We know that $Im(\overline{\rho_2}) \subseteq GL_2(\mathbb{F}_2)$ and so using Deligne-Serre Theorem we have that the ramification for the Galois representation is allowed only in 2 and in $207 = 3^2\,23$. Recalling the isomorphism $GL_2(\mathbb{F}_2) \cong S_3$, we get that we have to consider only number field that may ramify at 2,3,23, with Galois group isomorphic to S_3 or C_3, so given by irreducible polynomial of degree at most 3. For each extension of degree 3 of the previous type, we have that exist a Frobenius which has order 3 corresponding to a prime ≤ 19. In particular such an element in $GL_2(\mathbb{F}_2)$ corresponds to a matrix M with $\mathrm{Tr}(M) = 1$.
Meanwhile in the image of the residual representation at 2 we have that all element have trace 0, since each $\widehat{a_p}$ is zero, and determinant 1 since $\forall p$ prime $p \equiv 1 \mod 2$:

$$\left\langle \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq GL_2(\mathbb{F}_2) \cong S_3$$

In particular all elements in the image have at most degree 2, so the image cannot be S_3 and so it can be either a C_2 or the trivial subgroup. Considering the semi-semplification of the representation we get that the image is trivial:

$$\overline{\rho_2}^{ss} \cong Id$$

Exceptional prime of type (2)

Let us consider the space of newforms of weight 73, we can certify that there exists a form for which [3] is an exceptional prime of type (2) and of no other type. By Mazur study about modular form we know that [3] is a reducible prime, but this means that there exists a form for which it is exceptional of type (0), in particular the form [1] it is of type (2) and of no other type. In this case, indeed, we have that the inner twist modulo 3 is given by the quadratic Dirichlet character of conductor 3.

73	
[0]	[2, 3] possible reducible primes [2] reducible
[1]	[5] exceptional primes of type $(*)$ [2, 3] possible reducible primes no reducible prime no possible prime exceptional of type (1) [3] possible prime exceptional of type (2) [3] exceptional prime of type (2)
[2]	[13] exceptional primes of type $(*)$ [2, 3] possible reducible primes [3] reducible prime no possible prime exceptional of type (1) no possible prime exceptional of type (2)

So the image of the residual representation at 3 is characterized using Proposition 4.0.21 by:

$$Im(\overline{\rho_{f,3}}) \subseteq \left\langle GL_2(\mathbb{F}_3), \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \right\rangle |_{\det \in \mathbb{F}_3^*}$$

where $i \in \mathbb{F}_9 \setminus \mathbb{F}_3$ and $i^2 \in \mathbb{F}_3$, so

$$Im(\mathbb{P}(\overline{\rho_{f,3}})) \subseteq \mathbb{P}GL_2(\mathbb{F}_3)$$

A family of examples can be constructed using the procedure of level raising by Ribet [26], in fact considering a form with an inner twist it may be possible to construct a newform with a residual inner twist.

Exceptional prime of type (3)

In the space of newforms of level 608 and weight 2 it is possible to show that there exist a form such that [5] is an exceptional prime of type (3), where the twist is given by the quadratic character of conductor 4.

608	$2^5 \cdot 19$
[3]	[2, 3] possible reducible primes no reducible no possible prime exceptional of type (1) no possible prime exceptional of type (2) [2, 5] possible primes of type (3) [5] exceptional prime of type (3)

We can give also an example in weight 4, but firstly we have to remark that in this case, since the weight is greater than 2 we have that the character that gives the congruence corresponding to the case considered may ramify at more primes with respect to the weight 2 case. In particular, considering the space of newforms of weight 4 and level 25, with trivial character, we get that [7] is a dihedral prime with respect to the action of a quadratic character of conductor 7.

Exceptional prime of type (4)

In this case we can check that [3] is an exceptional prime of type (4) for a newform in the space of level 23, in fact the a_p, according to Proposition 4.0.33, satisfy the required conditions. Indeed, Kiming in [12] certified that in this case the image of the residual representation is exactly A_5.

Level examination

Using the algorithm we can analize, for a given level, the whole newform space and in particular for each newform in the space we can classify exceptional primes. The classification specify the type of exceptionality according to the previous classification. For example:

62	$2 \cdot 31$
[0]	[2, 3] possible reducible primes [2] reducible no possible dihedral primes no possible primes of type (4)
[1]	[2, 3] exceptional primes of type (∗) no possible reducible primes no possible primes exceptional of type (1) no possible primes exceptional of type (2) no possible dihedral primes no possible primes of type (4)

146	$2 \cdot 73$
[0]	[2, 101] exceptional primes of type (∗) [3] possible reducible prime no reducible prime no possible primes exceptional of type (1) no possible primes exceptional of type (2) no possible dihedral primes no possible primes of type (4)
[1]	[2, 389] exceptional primes of type (∗) [3, 37] possible reducible prime [37] reducible prime no possible primes exceptional of type (1) no possible primes exceptional of type (2) no possible dihedral primes no possible primes of type (4)

Bibliography

[1] Z. I. Borevich,I.R. Shafarevich, *Number Theory.* Academic Press, 1966;

[2] Buzzard K., Stein W.A., *A mod* 5 *approach to modularity of icosahedral Galois representations*, Pacific J. Math. 203, 2002;

[3] G. Cornell, Joseph H. Silverman, G. Stevens, *Modular forms and Fermat's last theorem*, Springer-Verlag, New York, 1998;

[4] P. Deligne, J. P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ecole Norm. Sup. (4), pp 507-530, 1974;

[5] Diamond F., Shurman J., *A First Course in Modular Forms*, Springer, 2005;

[6] L. V. Dieulefait, J. Jimenez, K. A. Ribet, *Modular forms with large coefficient fields via congruences*, in preparation;

[7] L. V. Dieulefait, N. Vila, *Projective linear groups as Galois groups over* $\mathbb{Q}$ *via modular representations.*, Journal Symbolic Comput. 30, p 799-810, 2000;

[8] Faltings G., Jordan B., *Crystalline cohomology and* $GL(2, \mathbb{Q})$, Israel Journal of Mathematics, 90, pp. 1–66, 1995;

[9] J. M. Fontaine, B. Mazur *Geometric Galois representations*, in *Elliptic curves, modular forms, and Fermat last theorem* , International Press, Cambridge, 1995;

[10] E. Ghate, *An introduction to congruences between modular forms*, Current trends in number theory, Hindustan Book Agency, 39-58, 2002;

[11] G. Janusz, *Algebraic number fields*, Academic Press, 1973;

[12] I. Kiming, H. Verrill, *On modular mod* ℓ *representations with exceptional images*, Journal Number Theory 110, pp. 236–266, 2005;

[13] Anthony W. Knapp, *Advanced Algebra*, Cornerstones, Birkhäuser,2000;

[14] Anthony W. Knapp, *Basic Algebra*, Cornerstones, Birkhäuser,2000;

[15] N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM 97, Springer, 1984;

[16] S. Lang, *Algebraic Number Theory*, GTM 110, Springer-Verlag, 2nd edition, 1994

[17] S. Lang, *Introduction to Modular Forms*, Grundlehren 222, Springer-Verlag, 1976;

[18] Livnè, *On the conductor of mod ℓ Galois Representations coming from modular forms*, Journal of Number Theory 31, 1989;

[19] Mazur B., *Modular curves and the Eisenstein ideal*, Publ. Math. IHES, 47,pp. 33–186, 1977;

[20] J. S. Milne, *Algebraic Number Theory* , lecture notes, http://www.jmilne.org/math/CourseNotes/ant.html;

[21] J. S. Milne, *Class Field Theory* , lecture notes, http://www.jmilne.org/math/CourseNotes/cft.html;

[22] J. S. Milne, *Modular Forms* , lecture notes, http://www.jmilne.org/math/CourseNotes/mf.html;

[23] Kenneth A.Ribet, *Endomorphism algebras of abelian varieties attached to newforms of weight 2.* Seminar on Number Theory, Paris 1979–80, pp. 263–276, Progr. Math., 12, Birkhäuser Boston, Mass., 1981;

[24] Kenneth A.Ribet, *Galois representations attached to eigenforms with Nebentypus.* Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), pp. 17–51. Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977. ;

[25] Kenneth A. Ribet, *Images of semistable Galois representations*, Pac. J. Math., 181. , 1997;

[26] Kenneth A. Ribet, *On ℓ-adic representations attached to modular forms.* Invent. Math. 28, 245–275, 1975;

[27] Kenneth A. Ribet, *On l-adic representations attached to modular forms II.* Glasgow Math. J. 27, 185–194, 1985;

[28] Kenneth A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. 100, no. 2, 431–476, 1990;

[29] Kenneth A. Ribet, *Twists of modular forms and endomorphisms of abelian varieties.* Math. Ann. 253, no. 1, 43–62, 1980;

[30] P. Samuel, *Theorie algebrique des nombres.* Hermann, 1971;

[31] J. P. Serre, *Local Fields*, GTM 67, Springer-Verlag, 1979;

[32] J. P. Serre, *Propriétés galoisennes de points d'ordre fini des courbes elliptiques*, Invent. Math. 15, (1972), 259–331;

[33] J. P. Serre, *Sur les représentations modulaires de degré* 2 *de* $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Mathematical Journal, Vol. 54, No. 1, 1987;

[34] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press, 1994;

[35] O. Takashi, *An introduction to algebraic number theory* , Plenum Press, 1987;

Ringraziamenti

Quando non ho avuto più niente da perdere, ho ottenuto tutto.
Quando ho cessato di essere chi ero, ho ritrovato me stesso.
Quando ho conosciuto l'umiliazione ma ho continuato a camminare,
ho capito che ero libero di scegliere il mio destino.
Paolo Coelho

È difficile scrivere dei ringraziamenti per molti motivi. Il primo, perchè tantissime persone hanno contribuito a formare la persona che sono oggi ed è impossibile elencarle tutte in una paginetta o poco più, il secondo perchè anche con l'enorme gioia di tagliare un traguardo importante come la laurea, si ha sempre paura di perdere qualcosa, ad esempio gli amici di questi cinque anni ... Un sincero ringraziamento va a tutti coloro che, in momenti diversi e in vari modi, mi hanno prestato il loro aiuto e la loro assistenza nella realizzazione di questo lavoro.

En primer lugar quiero agradecer a mi director, el profesor Dieulefait, quiero darle las gracias por toda la ayuda que me da dado, por su gran competencia con la que me guió en la preparación de la tesis y por darme la oportunidad de trabajar con él.
Voglio ringraziare il mio co-relatore il professor Canonaco a cui sono grato sia per la grande disponibilità, sia per l'immensa pazienza, sia per avermi fornito innumerevoli spunti per migliorare il lavoro svolto.

Voglio ringraziare anche la professoressa Pulvirenti per tutto l'aiuto che mi ha dato con gli Erasmus, la professoressa Frediani, per i suoi buoni consigli. Agradezco enormemente al profesores Pacetti, Vila y Arenas por l'ayuda y la disponibilidad .

Ora il mio pensiero si rivolge alla mia famiglia. Questo risultato non sarebbe stato possibile senza il sostegno dei miei cari. Grazie a te papà! Con il tuo esempio ho capito che lavorando sodo si possono raggiungere risultati sorprendenti e nonostante nella vita accada di tutto si può sempre andare avanti. Grazie anche a te mamma! La tua presenza mi ha rassicurato durante i momenti di sconforto e con il tuo affetto e la tua voglia di lottare per quello in cui credi mi hai dato la conferma che con la grinta nulla è

impossibile! E grazie anche a te sorellina! So che mi sei sempre stata vicino e che in silenzio hai sempre tifato per me, grazie!

Mi ritengo una persona molto fortunata, perché le mie esperienze sono state condivise con persone che stimo tantissimo e che hanno sempre le parole giuste al momento giusto. Con voi mi sento me stesso, mi fate sentire importante e forse sarà proprio questa vostra considerazione che mi ha dato la carica di portare a termine i miei progetti. Grazie a tutti i miei amici, a coloro che mi sono sempre stati vicini e con cui ho vissuto molti dei miei momenti più belli. Un uomo in fondo ha bisogno non tanto dell'amicizia, quanto della certezza di trovare sempre amici pronti ad aiutarlo, a sorreggerlo quando sta per cadere, a tendergli la mano per tirarsi su. Grazie di cuore!

Grazie a tutti i collegiali dell'Almo Borromeo, la mia seconda famiglia, grazie ai miei compagni d'anno per tutto quello che mi hanno insegnato e per tutto quello che abbiamo condiviso, Ghido, Sando, Jorjon, Ravio, Turco, Ross, Rox, Giulio, Paolo, Mangia, Diego grazie di tutto! Grazie a tutte le mie amiche papere, Chiara, Ilaria, Laura e Betta fra tutte. Vi ringrazio di cuore, trovare persone come voi è praticamente impossibile, ma ci sono riuscito e non vi lascio scappare. E grazie anche alle nuovine, Fra, Betta, Repi, Sere, Stefy, Lia, Mary e Patty grazie di tutto!

Un ringraziamento va ai miei compagni corso, Fra, Laura, Giulia, Marta, Marco, Erika ... Un "grazie" speciale a Gloria, spero che riusciremo sempre a mantenerci in contatto.

Gracias a todos los amigos que esperan el regreso del jefe de cocina a Barcelona, gracias por todas las agradables noches y por las largas discusiones de cine, música, mates... Maite, Nuno, Klara, Miquel, Maria, Juan, Celia, Thibault, Luz, Piermarco, Gemma.... es pasado poco pero ya me faltáis.... Grazie a Luna, il chaos e la libertà: un'amica come è davvero speciale.

Un grazie particolare ai miei due fratelli maggiori aquisiti, Nat e Bernat, che hanno saputo sostenermi e sopportarmi...

Grazie anche alle persone che non vedo da molto tempo ma non per questo dimenticate in un momento così importante: sono convinto che nella vita ci si possa anche allontanare, ma sono sicuro che se si tratta di vera amicizia, beh, allora ci rincontreremo.

Pavia, 13 luglio 2010