1
Overview of Modular Forms

It is difficult to provide a brief summary of techniques used in modern number theory. Traditionally, mathematical research has been classified by the method mathematicians exploit to study their research areas, except possibly for number theory. For example, algebraists study mathematical questions related to abstract algebraic systems in a purely algebraic way (only allowing axioms defining their algebraic systems), differential geometers study manifolds via infinitesimal analysis, and algebraic geometers study geometry of algebraic varieties (and its siblings) via commutative algebras and category theory. There are no central techniques which distinguish number theory from other subjects, or rather, number theorists exploit any techniques available to hand to solve problems specific to number theory. In this sense, number theory is a discipline in mathematics which cannot be classified by methodology from the above traditional viewpoint but is just a web of rather specific problems (or conjectures) tightly and subtly knit to each other. We just study numbers, those simple ones, like integers, rational numbers, algebraic numbers, real and complex numbers and p-adic numbers, and that is it.

What has emerged from our rather long history is that we continue to study at least two aspects of these numbers: the numbers of the base field and the numbers of its extensions. For example, the *quadratic reciprocity law* describes in a simple way how rational primes decompose as a product of prime ideals in a quadratic extension only using data from rational integers. More generally, by class field theory, we know how rational primes decompose in an abelian extension out of the datum from rational numbers. Thus we have two sets of numbers, the first is the numbers of the base field and the other from an extension of the base field. Nowadays, class field theory is often described using transcendental numbers from all possible completions of the base fields,

involving complex, real and p-adic numbers. The *adele ring* $\mathbb{A}$ is just a subring of $(\prod_p \mathbb{Q}_p) \times \mathbb{R}$ generated by p-adic integers (for all primes p), real numbers and rational numbers (even additively):

$$\mathbb{A} = ((\widehat{\mathbb{Z}} \times \mathbb{R}) + \mathbb{Q}) \subset \left(\prod_p \mathbb{Q}_p\right) \times \mathbb{R} \quad \left(\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p\right),$$

where we regard $\mathbb{Q} \subset \mathbb{A}$ by the diagonal embedding $\xi \mapsto (\xi, \xi, \dots, \xi, \dots) \in \prod_p \mathbb{Q}_p \times \mathbb{R}$. Thus for a given *number field* F (that is, a finite extension of the rational numbers $\mathbb{Q}$), the adele ring $F_{\mathbb{A}} = F \otimes_{\mathbb{Q}} \mathbb{A}$ of F represents all data from the base field. For a given algebraic group G defined over F, which we may think of as just a coherent rule assigning a group $G(A)$ to any F-algebra A, $G(F_{\mathbb{A}})$ is an immediate source of information. For example, $A \mapsto GL_n(A)$, the group of invertible $n \times n$ matrices with coefficients in A, is an algebraic group. Global class field theory is typically described as a canonical exact sequence:

$$1 \to \overline{GL_1(F)C} \to GL_1(F_{\mathbb{A}}) \to \mathrm{Gal}(F^{ab}/F) \to 1$$

for the identity connected component C of $GL_1(F_{\mathbb{A}})$, where '$\overline{X}$' indicates the topological closure of X, and F^{ab}/F is the composite of all Galois extensions M/F (inside an algebraic closure $\overline{F}$ of F) with $\mathrm{Gal}(M/F)$ abelian (such an extension is called an *abelian extension* of F). Thus we have the second set of numbers F^{ab}: those numbers in a Galois extension specific to our choice of the algebraic group $G = GL_1$. In this first example, $G = GL_1$, which is the simplest (and most important) of all abelian algebraic groups. Thus we might call the study of extensions of a base field the *Galois side* of number theory.

The above example tells us that it is important to study the geometry of the homogeneous space $G(F)\backslash G(F_{\mathbb{A}})$. Most geometers, if they are given a topological space, start studying functions on the space, because they know by experience that functions are easier to manipulate and eventually determine the space. We call functions on $G(F)\backslash G(F_{\mathbb{A}})$ *modular forms*. The homogeneous space $G(F)\backslash G(F_{\mathbb{A}})$ often classifies geometric objects, like abelian varieties and motives (as is often the case for a quotient of a big group by a discrete subgroup, because the big group is somehow a (local) transformation group of a collection of geometric objects, and elements of the discrete subgroup give rise to (global) isomorphisms between the objects). For example, when $G = GL_2$, $X = G(\mathbb{Q})\backslash G(\mathbb{A})/G(\widehat{\mathbb{Z}})Z(\mathbb{R})SO_2(\mathbb{R})$ for the maximal connected compact subgroup $SO_2(\mathbb{R}) \subset GL_2(\mathbb{R})$ and the center $Z(\mathbb{R}) \subset G(\mathbb{R})$ classifies isomorphism classes of elliptic curves over

$\mathbb{C}$, and therefore, gives rise to the set of complex points of the (coarse) moduli scheme $\mathbf{P}^1(j)$ (defined over $\mathbb{Q}$) classifying elliptic curves over $\mathbb{Q}$. Because of the classification property of X, we have a canonical algebraic variety $\mathbf{P}^1(j)$ defined over $\mathbb{Q}$ (and actually defined over $\mathbb{Z}$) which gives rise to X. The scheme $\mathbf{P}^1(j)$ is called a *canonical model* of X. This phenomenon that the homogeneous space $G(F)\backslash G(F_{\mathbb{A}})$ classifies some algebro-geometric objects is prevalent in many other cases of different algebraic groups (like symplectic groups $G = Sp(2g)$ and unitary groups $U(m,n)$), and the resulting canonical models are called *Shimura varieties* of PEL-type. In any case, a general homogeneous space $X(U) = GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A})/U \cdot Z(\mathbb{R})SO_2(\mathbb{R})$ for an open subgroup $U \subset GL_2(\widehat{\mathbb{Z}})$ classifies elliptic curves with some additional structure (such as a given point of order N) over $\mathbb{Z}$ (see [AME] and [GMF]). Then the canonical model $X(U)$ is called a *modular curve*, because it is a finite covering of $\mathbf{P}^1(j)$ and hence is an algebraic curve. Thus finding an elliptic curve (with a given additional structure) defined over $\mathbb{Q}$ (or $\mathbb{Z}$) is equivalent to finding a rational (or integral) solution to the defining equations of a specific modular curve $X(U)$. In this way, our effort in understanding the homogeneous space $X(U)$ provides us with another number theoretic question: a *Diophantine problem* of the equations of modular curves. This is a typical example in Number theory of where a serious study of one good problem yields another interesting question, making the life of the theory virtually inexhaustible.

An elliptic curve E defined over a number field $\mathbb{Q}$ is a natural source of a Galois representation $\rho_{E,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p)$ ramifying at p and a finite set S of primes (independent of p). This comes from the fact that the group $E[p^r]$ of p^r-torsion points of an elliptic curve $E_{/\mathbb{Q}}$ is isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^2$ and that the Galois action on $E[p^r]$ therefore gives rise to a Galois representation $\rho_E \mod p^r : \mathrm{Gal}(\overline{F}/F) \to GL_2(\mathbb{Z}/p^r\mathbb{Z}) \cong Aut(E[p^r])$. This Galois representation has a remarkable property, found by Hasse, that $L_p(X) = \det(1 - \rho_{E,p}(Frob_\ell)X) = 1 - a(\ell)X + \ell X^2$ has rational integral coefficients $a(\ell)$ independent of p for primes $\ell \notin S \cup \{p\}$ (see, for example, [AME] or [GMF]). Here $Frob_\ell$ is the Frobenius element in the Galois group. Then it is traditional to make an Euler product:

$$L(s,E) = \prod_p L_p(p^{-s})^{-1}.$$

This *Hasse–Weil L-function* is absolutely convergent if $\mathrm{Re}(s) > \frac{3}{2}$, and Hasse and Weil conjectured that it should have an analytic continuation to the whole s-plane with a functional equation relating $L(s,E)$ to $L(2-$

s, E). This is a hard question, because $L(s, E)$ is defined in a purely algebraic way, while the conjecture predicts a purely analytic property (typical for Number theoretic questions, as number theory belongs neither to algebra nor to analysis).

Since a modular form f is a function on a topological group $GL_2(\mathbb{A})$, it is natural to make a convolution product with a compactly supported function ϕ on $GL_2(\mathbb{A})$. This operator $f \mapsto \phi * f$ is called a Hecke operator. Sometime in the 1930's, Hecke discovered that the space of holomorphic modular forms on $X(U)$ has a base made of common eigenforms of standard Hecke operators $T(n)$ indexed by positive integers n (see Section 1.2 for a description of $T(n)$). Pick a common eigenform f, and write the eigenvalues for $T(n)$ as $\lambda(T(n))$. Hecke made an L-function: $L(s, \lambda) = \sum_{n=1}^{\infty} \lambda(T(n))n^{-s}$. This is a (modular) Hecke L-function, which satisfies a functional equation relating $L(s, \lambda)$ to $L(k - s, \lambda)$ for a positive integer k called the *weight* of f. A remarkable fact is that the eigenvalues are algebraic integers in a number field $\mathbb{Q}(\lambda)$ (as implied by Theorem 3.13 in Chapter 3) independent of n. It is not very often but not rare either that $\lambda(T(n)) \in \mathbb{Z}$ for all n when the weight k is 2 (although $\mathbb{Q}$-rational eigenforms become sporadic as k grows); thus, $\mathbb{Q}(\lambda) = \mathbb{Q}$ in such cases. Another remarkable fact is that this L-function has an Euler product: $L(s, f) = \prod_p H_p(p^{-s})^{-1}$ with an Euler factor $H_p(X) = 1 - a(p)X + \psi(p)p^{k-1}X^2$ for the weight $k \geq 1$ and a Dirichlet character ψ, which is called the *'Neben'* character of f by Hecke. Thus when $k = 2$ and $\psi = 1$, the case Hecke called 'Haupt typus' (principal type), the L-function looks like a Hasse–Weil L-function. Since Hecke initiated the study of the modular side (in the non-abelian case), it would be appropriate to call the study of modular forms (or the numbers of the base field) the *Hecke side* of Number theory.

The *Shimura–Taniyama conjecture* states that the Hasse–Weil L-function of every elliptic curve rational over $\mathbb{Q}$ appears as a Hecke L-function of a rational Hecke eigen cusp form, or equivalently, (and more geometrically) that every $\mathbb{Q}$-rational elliptic curve appears as a factor of the jacobian of a modular curve (see [Lg] and [Sh3] for the history of the conjecture, and see also [Sh4] for an account of Shimura's work in the 50's and 60's). As was shown by Shimura ([IAT] Chapter 7), to each Hecke eigen cusp form of weight 2 defined on a modular curve $X(U)$, one can attach a canonical subabelian variety A (or a quotient) of the jacobian of $X(U)$ so that the L-function of A coincides with the Hecke L-function of the cusp form. This fact implies that a Hecke eigen cusp form with eigenvalue $\lambda(T(\ell))$ and with 'Neben' character ψ has a unique

two-dimensional p-adic Galois representation ρ_λ whose characteristic polynomial of the Frobenius element is given by $X^2-\lambda(T(\ell))X+\psi(\ell)\ell$ for almost all primes ℓ. Later, the association of such a Galois representation to a cusp form was generalized to all weights (≥ 1) by Deligne, Shimura and Deligne–Serre (see Theorem 3.26 in Chapter 3). If one varies p, these p-adic Galois representations indexed by p have a peculier property that the characteristic polynomials of the Frobenius elements at (unramified) primes ℓ different from p are independent of p. This type of system of Galois representations is called a compatible system. One might then ask, in the spirit of Shimura and Langlands, whether every such compatible system of two-dimensional Galois representations is associated to an elliptic cusp form. This is a typical example of inter-related problems, which in aggregate form a grand program, initiated by Shimura and later developped by Langlands, connecting intricately arithmetic of the Galois side and the Hecke side.

We assume that the p-adic member of a given compatible system is p-adically close to a p-adic Galois representation associated to a cusp form, to ease further the difficulty when we study the above question of modularity of the system. Then one could approach this problem directly from the theory of p-adic Galois representations. For a given p-adic Galois representation $\varphi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Z}_p)$, we take its reduction modulo p: $\overline{\rho} = (\varphi \mod p) : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_p)$. Then we consider all Galois representations $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(A)$ for p-adic local rings A with residue field $\mathbb{F}_p$ which give rise to $\overline{\rho}$ after reducing modulo the maximal ideal of A. A representation ρ with the above property is called a *deformation* of $\overline{\rho}$. As pointed out by Mazur, the totality of such ρ unramified outside $S \cup \{p\}$ for a fixed finite set S is indexed by an affine local ring R; in other words, any such ρ is induced by a universal representation $\varrho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(R)$ composed by a unique algebra homomorphism $R \to A$. If $\overline{\rho}$ is, for example, given by a modular form as $\overline{\rho} = \rho_\lambda \mod p$, one could ask if all deformations are associated to modular forms; in other words, if the algebra R is isomorphic to a factor of the algebra generated by Hecke operators $T(n)$ over $\mathbb{Z}_p$. Mazur made this type of conjecture which asserts the identity of the universal ring R with a Hecke algebra (see [MT] and [FM]). The conjecture is, of course, interesting on its own, but it gives at least some meaning to the rather random decomposition of the p-adic Hecke algebra into local pieces. A question of Taniyama (see [Sh3]) to find a way of decomposing the jacobian of a given modular curve into rational simple factors is, after the work of Shimura ([IAT] Chapter 7), obviously related to decomposing

the Hecke algebra over $\mathbb{Q}$ into simple factors. Computed examples of such a decomposition over $\mathbb{Q}$ look more random at this moment than p-adic decomposition (although Maeda conjectured that the Hecke algebra for $SL_2(\mathbb{Z})$ at each weight is simple; see, [HM]). Deciding theoretically the number fields (the Hecke fields) appearing as a simple piece of the Hecke algebra seems difficult at this moment (although it may not be out of reach).

Another development in knitting conjectures in Number theory was given by Frey. In 1986, Frey constructed a semi-stable elliptic curve: $y^2 = x(x+u^p)(x-v^p)$ out of a (hypothetical) rational solution of Fermat's equation: $u^p + v^p + w^p = 0$ with $uvw \neq 0$ and suggested that this curve could not be modular (that is, cannot be identified with a Hecke eigenform). A close study of the ramification of the p-adic Galois representation of the elliptic curve initiated by Serre and studied by Ribet tells us that the elliptic curve has to be associated to a weight 2 modular forms of 'Haupt' type of level 2. By computation, such a modular form does not exist; so, the Shimura–Taniyama conjecture implies Fermat's last theorem (see [Se1] and [R2]).

Wiles' strategy to prove the Shimura-Taniyama conjecture for semi-stable elliptic curves (and hence Fermat's last theorem) is separated into three steps: First, starting from a modular irreducible $\overline{\rho}$ with minimal ramification, prove that the universal ring with minimal ramification and fixed determinant is actually isomorphic to a Hecke algebra. Then, using congruences between minimal (primitive) cusp forms and non-minimal ones (studied principally by Ribet), extend the identification (of the universal Galois deformation ring with a Hecke algebra) to non-minimal Galois representations. Thus for a given semi-stable elliptic curve $E_{/\mathbb{Q}}$, if the Galois module $E[p]$ is modular irreducible, E is modular (basically, forgetting the conditions of ramification), because its p-adic representation is a deformation of $E[p]$. Second, look at $E[3]$. Since $GL_2(\mathbb{F}_3)$ is soluble, the representation on $E[3]$ is modular by a result of Langlands and Tunnell if it is absolutely irreducible. In the two-dimensional soluble cases, Langlands and Tunnell have proved Artin's conjecture identifying the Artin L-function with a modular Hecke L-function of weight 1 (see [Ro], for example). Since a Galois representation into $GL_2(\mathbb{C})$ has finite image (see Proposition 2.2 in Chapter 2), it has values in $GL_2(\mathbb{Z}[\mu_N])$ for the group μ_N of appropriate Nth roots of unity. After reducing modulo a prime ideal of $\mathbb{Z}[\mu_N]$, one may consider the representation as having values in a finite field; in particular, an irreducible Galois representation into $GL_2(\mathbb{F}_3)$ is modular. Third, even if

$E[3]$ is not irreducible, look at $E[5]$ and write its Galois representation as $\overline{\rho}$. By sheer luck, the modular curve $X(\overline{\rho})$ classifying elliptic curves $\mathscr{E}$ with specified Galois module structure $\mathscr{E}[5] \cong \overline{\rho}$ is of genus 0. Since $(E, E[5])$ is rational over $\mathbb{Q}$, $X(\overline{\rho})$ has infinitely many rational points (including the one corresponding to $(E, E[5])$). Out of elliptic curves sitting on the rational points of $X(\overline{\rho})$, Wiles found (basically by Hilbert's irreducibility theorem) a particular one E' with absolutely irreducible $E'[3]$. Thus E' is modular by the first step; hence, $\overline{\rho} \cong E'[5]$ is modular. Applying deformation theory in the 5-adic setting of $\overline{\rho}$, E itself is known to be modular. We refer readers to the details of this argument in the original paper of Wiles [W2] Chapter 5.

In this book, I shall give a detailed exposition of the deformation theory of Galois representation (Mazur's approach) and the identification of the universal deformation ring R with a Hecke algebra (a result due to Wiles and Taylor), restricting ourselves to the case where ramification is limited to a single prime $p > 3$ and ∞. At the end (Chapter 5), I shall briefly give an application of the theory to the special values of the adjoint L-functions of modular forms and their Selmer groups, recalling some of my old and new results ([H81a] and [H99b]).

In this chapter, I shall give an overview of the theory of modular forms, expanding a bit the above description, as an introduction to the subject of the book, starting from Hecke characters, which can be regarded as abelian modular forms. Since this is the introductory part, proofs of some results may not be given here, putting them off until later chapters (or to somewhere else as indicated). The reader can find an outline of the chapters of this book in Subsection 1.2.1.

1.1 Hecke Characters

Let F be a number field, that is, a finite extension of $\mathbb{Q}$. A continuous character $\varphi : F_{\mathbb{A}}^{\times}/F^{\times} \to \mathbb{C}^{\times}$ is called a Hecke character. A Hecke character is a function on the homogeneous space $GL_1(F)\backslash GL_1(F_{\mathbb{A}})$, and hence, the simplest among modular forms on algebraic groups. We study in this section Hecke characters in terms of class field theory.

1.1.1 Hecke characters of finite order

Let $\mathbb{A}$ be the adele ring of $\mathbb{Q}$, and put $F_{\mathbb{A}} = F \otimes_{\mathbb{Q}} \mathbb{A}$, which is the adele ring of F. We write $O = O_F$ for the integer ring of F. We write $\mathbb{A}^{(\infty)}$ for the finite part of the adele ring. Thus $\mathbb{A} = \mathbb{A}^{(\infty)} \times \mathbb{R}$, $F_{\mathbb{A}^{(\infty)}} = F \otimes_{\mathbb{Q}} \mathbb{A}^{(\infty)}$

and $F_{\mathbb{A}} = F_{\mathbb{A}^{(\infty)}} \times F_{\mathbb{R}}$ for $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R}$. We write $F_{\mathbb{R}+}^{\times}$ for the connected component of $F_{\mathbb{R}}^{\times}$ containing the identity (the identity component). Then for each prime ideal $\mathfrak{p}$ of O, we consider the $\mathfrak{p}$-adic integer ring $O_{\mathfrak{p}} = \varprojlim_n O/\mathfrak{p}^n$, which is a valuation ring free of finite rank over $\mathbb{Z}_p$. Here p is the prime generating $\mathbb{Z} \cap \mathfrak{p}$. By class field theory, we have an exact sequence

$$1 \to \overline{F^{\times} F_{\mathbb{R}+}^{\times}} \to F_{\mathbb{A}}^{\times} \xrightarrow{[\ ,F]} \mathrm{Gal}(F_{ab}/F) \to 1, \qquad \text{(CFT)}$$

where F_{ab} is the maximal abelian extension of F, $\overline{F^{\times} F_{\mathbb{R}+}^{\times}}$ is the topological closure of $F^{\times} F_{\mathbb{R}+}^{\times}$ in $F_{\mathbb{A}}^{\times}$ and $[\ ,F]$ is the Artin reciprocity law map (see [CFN], Chapter III). Let $\varphi : F_{\mathbb{A}}^{\times}/F^{\times} \to \mathbb{C}^{\times}$ be a Hecke character of finite order. We look at the restriction φ_{∞} of φ to $F_{\mathbb{R}}^{\times}$. Since the inclusion $F_{\mathbb{R}}^{\times} \hookrightarrow F_{\mathbb{A}}^{\times}$ is continuous, $\varphi_{\infty} : F_{\mathbb{R}}^{\times} \to \mathbb{C}^{\times}$ is a continuous character. If φ is of order N, φ_{∞} also has values in the discrete group $\mu_N(\mathbb{C})$ of Nth roots of unity. Thus φ_{∞} has to be trivial on the connected component $F_{\mathbb{R}+}^{\times}$, and φ factors through $\mathrm{Gal}(F_{ab}/F)$. This shows the following one-to-one onto correspondence:

$$\{\textit{Hecke characters of finite order}\} \leftrightarrow \{\textit{Galois characters of finite order}\}.$$

Let $\varphi : \mathrm{Gal}(F_{ab}/F) \to \mathbb{C}^{\times}$ be a continuous character, and suppose that $|\varphi(\sigma) - 1| < 1/2$. If $\varphi(\sigma) \neq 1$, we see that $|\varphi(\sigma)^N - 1| > 1/2$ for some integer N. Since $\mathrm{Gal}(F_{ab}/F)$ is a profinite group (see Chapter 2 2.1.2 for a brief description of profinite groups), its image under φ is a compact set in $\mathbb{C}$, and for a sufficiently small open normal subgroup U of $\mathrm{Gal}(F_{ab}/F)$, $\varphi(U)$ has values in an open disk of radius $\frac{1}{2}$ centered at 1. Thus the above argument for $\sigma \in U$ shows that $\varphi(U) = 1$. Therefore φ factors through the finite group $\mathrm{Gal}(F_{ab}/F)/U$, and φ is of finite order. This argument tells us that any continuous character from a profinite group into $\mathbb{C}^{\times}$ has a finite image.

Here are some examples. Let $F = \mathbb{Q}$. Then for $\widehat{\mathbb{Z}}^{\times} = \prod_{p:primes} \mathbb{Z}_p^{\times}$, we have

$$\mathbb{A}^{\times} = \mathbb{Q}^{\times} \widehat{\mathbb{Z}}^{\times} \mathbb{R}_{+}^{\times} \cong \mathbb{Q}^{\times} \times \widehat{\mathbb{Z}}^{\times} \times \mathbb{R}_{+}^{\times}$$

in the following way. For each $x = (x_v) \in \mathbb{A}^{\times}$, we consider the rational number $rat(x) = (x_{\infty}/|x_{\infty}|) \prod_p p^{v_p(x_p)}$ for the valuation v_p at p with $v_p(p) = 1$. Then $rat(x)^{-1} x^{(\infty)} \in \widehat{\mathbb{Z}}^{\times}$ and $rat(x)^{-1} x_{\infty} \in \mathbb{R}_{+}^{\times}$. Thus the above isomorphism is induced by

$$x \mapsto (rat(x), rat(x)^{-1} x^{(\infty)}, rat(x)^{-1} x_{\infty}).$$

Let N be a positive integer, and write $\mu_N(A)$ for the multiplicative group

of N-th roots of unity for any ring A. Let $\overline{\mathbb{Q}}$ be the totality of algebraic numbers in $\mathbb{C}$. We consider the cyclotomic field $\mathbb{Q}(\mu_N)$. We can define the cyclotomic character $\chi_N : \mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q}) \to (\mathbb{Z}/N\mathbb{Z})^\times$ by $\zeta^\sigma = \zeta^{\chi_N(\sigma)}$ for $\zeta \in \mu_N(\overline{\mathbb{Q}})$. By the compatibility of local and global class field theory, $[x, \mathbb{Q}] = \prod_v [x_v, \mathbb{Q}_v]$, where v runs over places of $\mathbb{Q}$ including ∞. If x_∞ is negative, $[x_\infty, \mathbb{R}]$ is the complex conjugation (unique in $\mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q})$), and $[x_\infty, \mathbb{R}] = 1$ if $x_\infty > 0$. For a prime ℓ outside N, ℓ is unramified in $\mathbb{Q}(\mu_N)$. Thus $[\ell, \mathbb{Q}_\ell]|_{\mathbb{Q}(\mu_N)}$ is the Frobenius $Frob_\ell$ at ℓ, and $\chi_N([\ell, \mathbb{Q}_\ell]) = \ell \mod N$ for $\ell \nmid N$. Writing ℓ_N for an idele such that its p-component for $p|N$ is equal to ℓ and it is equal to 1 outside N, we define $\ell^{(N)} \in \mathbb{A}^\times$ by $\ell_N \ell^{(N)} = \ell$. Note that $[\ell_p^{(N)}, \mathbb{Q}_p]|_{\mathbb{Q}(\mu_N)} = 1$ unless $p = \ell$ because p is unramified in $\mathbb{Q}(\mu_N)$ if $p \nmid N$ and $\ell_p^{(N)} \in \mathbb{Z}_p^\times$ if $\ell \neq p$. Then we see, for $\ell \nmid N$,

$$\chi_N([\ell^{(N)}, \mathbb{Q}]) = \chi_N(\prod_{p \nmid N} [\ell_p, \mathbb{Q}_p]) = \chi_N([\ell_\ell, \mathbb{Q}_\ell]) = \ell \mod N.$$

Since $[\ell, \mathbb{Q}] = 1$,

$$\chi_N([\ell_N, \mathbb{Q}]) = \chi_N([\ell^{(N)}, \mathbb{Q}])^{-1} = (\ell \mod N)^{-1}.$$

Let $\varphi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a Dirichlet character. We can regard φ as an idele character in two ways: Since we have a natural projection $\pi : \widehat{\mathbb{Z}}^\times \to (\mathbb{Z}/N\mathbb{Z})^\times$, we just define $\varphi_* : \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$ by $\varphi_*(x) = \varphi(\pi(rat(x)^{-1}x^{(\infty)}))$. The second way is to define $\varphi^* : \mathbb{A}^\times/\mathbb{Q}^\times$ by $\varphi^*(x) = \varphi(\chi_N([x, \mathbb{Q}]))$. By the above computation, for primes $\ell \nmid N$,

$$\varphi^*(\ell_\ell) = \varphi(\ell) \quad \text{and} \quad \varphi_*(\ell^{(\ell)}) = \varphi(\ell).$$

We have in either way an onto correspondence:

$$\{\textit{Dirichlet characters}\} \twoheadrightarrow \{\textit{finite order Hecke characters of } \mathbb{A}^\times/\mathbb{Q}^\times\}.$$

To make this one to one, we need to impose primitivity on Dirichlet characters:

$$\{\textit{primitive Dirichlet characters}\} \leftrightarrow \{\textit{finite order Hecke characters of } \mathbb{A}^\times/\mathbb{Q}^\times\}.$$

1.1.2 Arithmetic Hecke characters

Let p be a prime. We simply write χ_n for χ_{p^n}. By taking the projective limit, we get the p-adic *cyclotomic* character

$$\chi = \varprojlim_n \chi_n : \mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q}) \to \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

Since $\mathbb{Q}(\mu_{p^n})/\mathbb{Q}$ is unramified at any prime $\ell \neq p$, $[u_\ell, \mathbb{Q}_\ell]$ is trivial on $\mathbb{Q}(\mu_{p^n})$. Thus $\chi([p^{(p)}, \mathbb{Q}]) = 1$. Since $[p, \mathbb{Q}] = 1$, we get $\chi([p_p, \mathbb{Q}]) = 1$. For primes $\ell \neq p$, we see that

$$\chi([\ell_\ell, \mathbb{Q}]) = \chi([\ell, \mathbb{Q}_\ell]) = \chi(Frob_\ell) = \ell.$$

From $[\ell, \mathbb{Q}] = 1$, we get

$$\chi([\ell^{(\ell)}, \mathbb{Q}]) = \chi([\ell_\ell, \mathbb{Q}])^{-1} = \ell^{-1} \in \mathbb{Z}_p^\times.$$

This Galois character is actually associated to an infinite order Hecke character $\varphi(x) = |x|_{\mathbb{A}}^{-1} = (|x_\infty| \prod_p |x_p|_p)^{-1}$, because $\varphi(\ell_\ell) = |\ell|_\ell^{-1} = \ell = \chi(Frob_\ell)$. As a result, it would be legitimate to write $\chi = \varphi^*$. Let $\mathscr{A} = \mathscr{A}_{\mathbb{Q}}$ be the set of Hecke characters $\varphi : \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times$ such that $x \mapsto \varphi(x)|x|_{\mathbb{A}}^m$ is a finite order character for an integer m. We call an element of $\mathscr{A}$ an arithmetic Hecke character. Since every finite order character of $\mathbb{A}^\times/\mathbb{Q}^\times$ is associated with a Galois character, we get the following correspondence:

$$\mathscr{A}_{\mathbb{Q}} \leftrightarrow \left\{ \begin{array}{l} \textit{characters } \psi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \overline{\mathbb{Q}}_p^\times | \psi\chi^{-m} \\ \textit{is of finite order for an integer } m \end{array} \right\},$$

where $\overline{\mathbb{Q}}_p$ is an algebraic closure of $\mathbb{Q}_p$.

Is there an intrinsic characterization of characters in $\mathscr{A}$ without using specific characters like $|\ |_{\mathbb{A}}$? There is! If a Hecke character φ restricted to $\mathbb{R}_+^\times$ is just $x \mapsto x^m$, then $\varphi_0 = \varphi|\ |_{\mathbb{A}}^{-m}$ is trivial on $\mathbb{Q}^\times\mathbb{R}_+^\times$ and hence factors through $\mathrm{Gal}(\mathbb{Q}_{ab}/\mathbb{Q})$. As already seen, any complex valued Galois character is of finite order; hence, φ_0 is of finite order. This shows that $\varphi \in \mathscr{A}$. The Lie group $\mathbb{R}_+^\times$ has invariant differential operators. For the additive group, the differential operator $\frac{d}{dx}$ is invariant under the group operation, that is, $\frac{df}{dx}(x+y) = \frac{df(x+y)}{dx}$. Any other invariant differential operator is a polynomial of $\frac{d}{dx}$. For the multiplicative group, the invariant differential operator is given by $\Delta = exp_*(\frac{d}{dx}) = t\frac{d}{dt}$, writing the variable $t = exp(x)$ of $\mathbb{R}_+^\times$. We may regard each Hecke character φ as a function of $t \in \mathbb{R}^\times$ fixing the variable at the finite part. Then we apply Δ. Then

$$\mathscr{A} = \{\textit{characters } \varphi : \mathbb{A}^\times/\mathbb{Q}^\times \to \mathbb{C}^\times | \Delta\varphi = m\varphi \textit{ for } m \in \mathbb{Z}\}.$$

We now generalize this fact to an arbitrary number field F. Let $I = I_F$ be the set of all field embeddings of F into $\mathbb{C}$. If $\sigma(F) \subset \mathbb{R}$, we call $\sigma \in I$ real, and otherwise, we call σ complex or imaginary. The Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \langle c \rangle$ acts on I so that $x^{\sigma c} = (x^\sigma)^c$. Then we put $\mathbf{a} = I/\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, which is the set of archimedean places of F. We write F_σ for the σ-completion of F, that is, $\mathbb{R}$ or $\mathbb{C}$ according as σ is real or