Main Conjecture of Iwasawa Theory

C. S. Rajan

Abstract. 1) Weil conjectures 2) Iwasawa's theorem on growth of class groups 3) Iwasawa's construction of p-adic L-functions via Stickelberger elements 4) Main conjecture.

1. Weil Conjectures

1.1. Zeta and L-functions. We recall the Riemann zeta function

$$\zeta(s) = \sum_{n\geq 1} n^{-s} \qquad (\mathrm{Re}(s) > 1).$$

The above series converges absolutely for $\mathrm{Re}(s) > 1$ and defines an analytic function there. $\zeta(s)$ admits an analytic continuation to the entire complex plane except for a pole at $s = 1$. The zeta function and its generalisations enjoy remarkable analytic properties, which have significant consequences to arithmetic. One of the outstanding problems concerned with the zeta function is the Riemann Hypothesis:

Riemann Hypothesis(RH): If ρ is any zero of $\zeta(s)$ with $\mathrm{Re}(\rho) \geq 0$ (such zeros are called the non-trivial zeros of $\zeta(s)$), then

$$\mathrm{Re}(\rho) = 1/2.$$

i.e., all the zeros to the right of the line $\mathrm{Re}(s) = 0$ lie on the line $\mathrm{Re}(s) = 1/2$.

How does one tackle this conjecture? One idea going back to Hilbert stems from the fact that the eigenvalues of a hermitian (skew-hermitian) matrix are real (purely imaginary). In other words the eigenvalues of a hermitian matrix all lie on a straight line. This leads to the following question:

Question 1.1.1. Is it possible to find a skew-hermitian operator acting on some space, such that the zeros of $\zeta(s+1/2)$ with non-negative real part, occur as eigenvalues of this operator?

Very little is known about this question. Recently some exciting numerical computations show that the known zeros of the $\zeta(s)$ behave like the eigenvalues of a random hermitian matrix. See works of Montogomery, Odlyzko, Katz, Sarnak and others.

The solution to many arithmetical problems lie in the analytic properties of the zeta function. It seems profitable then to look at analogous situations, also with a view to throw some light on the Riemann Hypothesis. One generalisation is to number fields. The Dedekind zeta function of a number field K is,

$$Z_K(s) = \sum_{\mathfrak{a} \neq 0} (N\mathfrak{a})^{-s},$$

where $\mathfrak{a}$ runs over the non-zero ideals of the ring of integers $\mathcal{O}_K$ of K, and $N\mathfrak{a} = |\mathcal{O}_K/\mathfrak{a}|$ is the number of elements in the ring $\mathcal{O}_K/\mathfrak{a}$. $Z_K(s)$ is defined as above for $\mathrm{Re}(s) > 1$, and has properties similar to the Riemann zeta function. The key fact that enables us to define the zeta function is that for a non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{a}$ is a finite ring. It can be shown that $Z_K(s)$ converges absolutely, and hence defines an analytic function in the half plane, $\mathrm{Re}(s) > 1$.

In order to generalise the definition of the zeta function to a more general context, it is easier to work with the Euler product expansion of the zeta function. Recall that for $\mathrm{Re}(s) > 1$, the zeta function can be expressed as a product,

$$Z_K(s) = \prod_{\mathfrak{m}} (1 - (N\mathfrak{m})^{-s})^{-1},$$

where $\mathfrak{m}$ runs over the maximal ideals of $\mathcal{O}_K$. Here we remark, although it is not essential for what follows, the fact that the above expression defines the zeta function is another way of expressing the unique factorisation of an ideal into a product of prime ideals, generalising the unique factorisation property of integers.

More generally let $f_1(x_1, \cdots, x_n), \cdots, f_r(x_1, \cdots, x_n)$ be polynomials with integral coefficients in the ring $\mathbb{Z}[x_1, \cdots, x_n]$. Let I be the ideal in $\mathbb{Z}[x_1, \cdots, x_n]$ generated by $f_1, \cdots, f_n$ and let A be the ring,

$$A = \mathbb{Z}[x_1, \cdots, x_n]/I.$$

The ring A can be thought of as the ring of polynomial functions restricted to the variety X defined by the common zeros of the polynomials $f_1, \cdots, f_n$, or equivalently of the common zeros of polynomials in the ideal I:

$$X = \{(a_1, \cdots, a_n) \in \mathbb{C}^n \mid f((a_1, \cdots, a_n)) = 0, \ \forall f \in I\}.$$

It follows from the finite generation of A as an algebra over $\mathbb{Z}$, that the following are equivalent:

i) $\mathfrak{m}$ is a maximal ideal of A.

ii) $A/\mathfrak{m}$ is a finite field.

Let X' denote the collection of maximal ideals of A. One can define the zeta function,

$$Z(X, s) = \prod_{\mathfrak{m} \in X'} (1 - (N\mathfrak{m})^{-s})^{-1}.$$

Here we assume that I is not the unit ideal. It can be shown that $Z(X,s)$ converges absolutely in some half plane, and thus defines an analytic function there.

EXAMPLE 1. Let L/K be a finite Galois extension of number (global) fields with Galois group G. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ unramified in L, and let $\mathcal{P}$ be a prime ideal of $\mathcal{O}_L$ dividing $\mathfrak{p}$. Then the Frobenius element $\sigma_{\mathcal{P}}$ is given by,

$$\sigma_{\mathcal{P}}(x) \equiv x^{N\mathfrak{p}}(\mathrm{m}od\ \mathcal{P}),$$

where $x \in \mathcal{O}_L$. For a fixed $\mathfrak{p}$, the Frobenius elements $\sigma_{\mathcal{P}}$ for $\mathcal{P}|\ \mathfrak{p}$ form a conjugacy class inside G. Let ρ be a finite dimensional representation of G into $GL(n,\mathbb{C})$. The incomplete Artin L-function associated to ρ is defined by,

$$L'(s,\rho) = \prod_{\mathfrak{p}} \det(1-\rho(\sigma_{\mathfrak{p}})N\mathfrak{p}^{-s})^{-1}, \mathrm{Re}(s) > 1.$$

Here the product is over the unramified primes of K with respect to L. It is possible to define the factors at the ramified primes, in order that the completed L-function has an analytic continuation to the entire plane and satisfies a suitable functional equation.

In particular, take $K = \mathbb{Q}$, and $L = \mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. Then $G \simeq (\mathbb{Z}/n\mathbb{Z})^*$. Let χ be a character of $(\mathbb{Z}/n\mathbb{Z})^*$, a Dirichlet character. Let

$$L(s,\chi) = \prod_{(p,n)=1} (1-\chi(p)p^{-s})^{-1}, \mathrm{Re(s)}> 1.$$

These are the L-functions considered by Dirichlet.

1.2. Arithemetical applications. a) *Dirichlet's theorem and Prime number theorem.* The non-vanishing of $L(s,\chi)$-functions at $s = 1$ when χ is a Dirichlet character, imply Dirichlet's theorem on infinitely many primes of the form $an+b,\ (a,b) = 1,\ n \in \mathbb{N}$. More generally, the non-vanishing of $L(s,\chi)$ on the line $\mathrm{Re}(s) = 1$ for all characters $\chi : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, imply for any $a,\ b,\ (a,b) = 1$ that,

$$\#\{p \le x \mid p = am+b, \text{ for some } m\} \sim \frac{1}{\phi(a)}\frac{x}{\log x}, \text{ as } x \to \infty,$$

where ϕ is Euler ϕ-function. In particular, when we take χ to be the trivial character, we obtain the prime number theorem, viz., that the number of primes of size at most x, grows asymptotically like $x/\log x$ as $x \to \infty$.

b) *Class number formulas.* It can be seen that the Dedekind zeta function $Z_K(s)$ has a meromorphic continuation to the entire plane, which is holomorphic except at $s = 1$. Let h denote the class number of K, R the regulator of K, D the absolute value of the discriminant of K, r_1 the number of real embeddings of K, $2r_2$ the number of complex embeddings, and w the number of roots of unity in K. Then the class number formula is,

$$\mathrm{res}_{s=1}Z_K(s)=\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{D}}.$$

Remark. The main theme in defining these zeta functions, is the local-global principle. The various Euler factors encode the arithmetical information at the various primes, and global arithmetical consequences arise from the analytical aspects of the global L-functions. The fact that these L-functions have suitable analytical properties, can be considered as a vast generalisation of the classical quadratic and higher reciprocity laws. However even the analytic properties similar to that enjoyed by $\zeta(s)$ are not known for these L-functions. Again these analytic properties have remarkable arithmetical applications. For example, take I to be generated by the polynomial $f(x,y)=y^2-x^3+ax+b,\ a,\ b\in\mathbb{Z}$, in the ring $\mathbb{Z}[x,y]$. X defines an elliptic curve minus the point at infinity. The analytic continuation of $Z(X,s)$ and related objects have been established by Wiles, and by Ribet's theorem imply Fermat's conjecture. Thus these generalisations seem to be even more difficult to handle than $\zeta(s)$!

1.3. Finite fields. However if we assume that the ideal I contains a prime number, the problem becomes tractable. In this case we are essentially replacing the base ring $\mathbb{Z}$ by a finite field $\mathbb{F}_q$ consisting of q elements. Again take I to be an ideal in the polynomial ring $\mathbb{F}_q[x_1,\cdots,x_n]$, and let $A=\mathbb{F}_q[x_1,\cdots,x_n]/I$ be the ring of polynomial functions on the variety $X=V(I)$ defined by I. As above, we can define the zeta function,

$$Z_X(s)=\prod_{\mathfrak{m}\in X'}(1-(N\mathfrak{m})^{-s})^{-1}.$$

Again this can be shown to make sense.

We will now translate the above definition for the zeta function, into a form which counts number of common solutions of polynomials in I, over finite extensions of the base field $\mathbb{F}_q$. To do this, suppose that $(a_1,\cdots,a_n)$ is a common solution of the polynomials $f_1,\cdots,f_r$ in some field k containing $\mathbb{F}_q$. Define a ring homomorphism $A\to k$, by sending the generators x_i to the element a_i. This prescription allows us to define a bijection between the set of solutions of $f_1,\cdots,f_r$ (equivalently the set of common solutions of the polynomials in the ideal generated by $f_1,\cdots,f_r$) in k, and the collection of ring homomorphisms from $A\to k$.

Let X_m be the set of solutions with values in $\mathbb{F}_{q^m}$. Identifying as above with ring homomorphisms, we see that this is the same as giving a maximal ideal $\mathfrak{m}\in X'$, and an embedding f of the finite field $f:A/\mathfrak{m}\to\mathbb{F}_{q^m}$, which is identity on the base field $\mathbb{F}_q$.

Being a subset of $\mathbb{F}_{q^m}^n$, X_m is finite. Define

$$\nu_m = |X_m|.$$

Let μ_l be the number of maximal ideals $\mathfrak{m}$ in X' such that the cardinality of the residue field $N\mathfrak{m} = q^l$.

Exercise 1.3.1. Show that $\nu_m = \sum_{l|m} l\mu_l$.

An alternate expression for the zeta function in terms of the number of solutions of varieties over finite fields is the following:

$$\log Z(X,s) = \sum_{m\geq 1} \frac{\nu_m q^{-ms}}{m}.$$

Proof. Exercise. *Hint:* The number of embeddings of $\mathbb{F}_{q^l}$ over $\mathbb{F}_q$ into $\mathbb{F}_{q^m}$ is $l = [\mathbb{F}_{q^l} : \mathbb{F}_q]$, where we assume that $l|m$. □

We can reformulate by substituting $t = q^{-s}$, to obtain a formal power series

$$\log Z(X,t) = \sum_{m\geq 1} \frac{\nu_m t^m}{m}.$$

We now look at some examples.

Exercise 1.3.2. 1) X a point. Then $\nu_n = 1$ for all n, and

$$Z(X,t) = \exp\left(\sum_{n\geq 1} \frac{t^n}{n}\right) = \frac{1}{1-t}.$$

2) Take X to be defined by the zero ideal in the polynomial ring $k[x_1, \cdots, x_m]$. Then $\nu_n = q^{mn}$ and

$$Z(X,t) = \exp\left(\sum_{n\geq 1} \frac{q^{mn}t^n}{n}\right) = \frac{1}{1-q^m t}.$$

Thus the above product converges absolutely to the right of $\mathrm{Re}(s) > n$.

3) Consider the variety defined by the zero ideal in $\mathbb{Z}[x_1, \cdots, x_n]$. Show that

$$X' = \cup_p X'_p,$$

where p is a rational prime and X'_p denotes the set of maximal ideals in X'_p with residue field a finite extension of $\mathbb{F}_p$. Hence conclude,

$$Z(X,s) = \prod_p (1-q^{n-s})^{-1} = \zeta(s-n).$$

In particular this shows that the above product defining the zeta function converges absolutely to the right of $\mathrm{Re}(s) > n+1$.

1.4. Affine varieties. Let I be an ideal in the ring $k[x_1, \cdots, x_n]$. To the ideal I, we can associate the set of solutions $X(R)$ over any k-algebra R,

$$\begin{aligned} X(R) &= \{s \in R \mid f(s) = 0, \ \forall f \in I\} \\ &= \{\phi : k[x_1, \cdots, x_n]/I \to R, \phi \text{ a ring homomorhism}\}. \end{aligned}$$

We will refer to the functor which assigns to any k-algebra R, the set of solutions $X(R)$ as the (affine) algebraic variety associated to the ideal I. For example, one can take I to be the zero ideal in $k[x_1, \cdots, x_n]$. Then the set of solutions associated to any k-algebra R is R^n. The algebraic variety associated to the zero ideal in $k[x_1, \cdots, x_n]$ will be referred to as the affine n-space $\mathbf{A}_k^n$ over the field k.

Note that if J is an ideal containing I, then there is a natural inclusion for any k-algebra R, of the set of common solutions of the polynomials in J, to the corresponding set for I. We will refer to this as the algebraic subsets of the variety X defined by I. A topology can be defined on the variety X, by taking algebraic subsets as closed subsets.

Remark. In particular one can take $R = \bar{k}$, an algebraic closure of the field k. Sometimes we will also refer to $X(\bar{k})$ as the algebraic variety associated to I. However the set $X(\bar{k})$ determines the radical

$$\begin{aligned} R(I) &= \{f \in k[x_1, \cdots, x_n] \mid f^n \in I, \text{ for some } n\} \\ &= \{f \in k[x_1, \cdots, x_n] \mid f(a) = 0, \ \forall a = (a_1, \cdots, a_n) \in X(\bar{k})\}, \end{aligned}$$

of the ideal I, and not necessarily the ideal I.

Remark. The Noether normalization theorem asserts that given a ring A as above, there is a finite morphism from a suitable polynomial ring on d generators onto A. d is then the dimension of the corresponding variety. Using this, it can be shown that the zeta function corresponding to the variety defined by the solutions of the ideal corresponding to A, converges absolutely in a suitable half plane.

1.5. Projective varieties. Before going onto further examples, we will now discuss a bit about projective varieties defined by homogeneous polynomials

$$f_1(x_0, \cdots, x_m), \cdots, f_r(x_0, \cdots, x_m).$$

Since the polynomials are homogeneous, if $a = (a_0, \cdots, a_m)$ is a common solution of f_i in some k-algebra R, then any multiple $\lambda a = (\lambda a_0, \cdots, \lambda a_m)$ for $\lambda \in R$ is also a solution. By the solutions in a k-algebra R of the projective variety defined by $f_1, \cdots, f_r$, we mean the equivalence classes of *non-zero* solutions, where two solutions are equivalent if they are scalar multiples of each other.

Remark. Let $\mathbf{P}_k^m$ denote the m-dimensional projective space defined by the zero ideal in $k[x_0, \cdots, x_m]$. As a set $\mathbf{P}_k^m$ can be identified with the set of lines passing through the origin. The set of solutions $a = (a_0, \cdots, a_m) \neq 0$ with $a_i \neq 0$ for some i, can be identified with $\mathbf{A}_k^m$ (as sets to start with), by sending $(a_0, \cdots, a_m) \mapsto (a_0/a_i, \cdots, a_m/a_i)$, with the i^{th} co-ordinate omitted. Given homogeneous polynomials $f_1, \cdots, f_r$ as above with degrees respectively $d_1, \cdots d_r$, then the set of common solutions of $f_1, \cdots f_r$ in $\mathbf{P}_k^m$ with $a_i \neq 0$, corresponds via the above correspondence to the set of common solutions of the 'dehomogenized' polynomials $x_i^{-d_j} f_j(x_0, \cdots, x_m)$ in the new variables $y_0 = x_0/x_i, \cdots, y_m = x_m/x_i$. This dehomogenization process is suitable for studying the local behaviour of a projective variety. Conversely given a polynomial, for example $f(x,y) = y^2 - x^3 - ax - b$, the solutions of the corresponding 'homogeneous' polynomial $f(x,y,z) = y^2z - x^3 - axz^2 - bz^3$ in $\mathbf{P}^2$, can be taken as the 'completion' or the projective analogue of the set of 'affine' solutions of the polynomial $f(x,y)$.

To distinguish from the affine case, we will denote the projective variety of solutions by $\bar{X}$, and by $\bar{\nu}_n$ the number of 'projective' solutions in $\mathbb{F}_{q^{n+1}}$. The zeta function $Z(\bar{X}, t)$ is defined by the formal power series,

$$\log Z(X,t) = \sum_{m \geq 1} \frac{\bar{\nu}_m t^m}{m}.$$

Example 2. Let $\mathbf{P}^m$ denote the m-dimensional projective space defined by the zero ideal in $\mathbb{F}_q[x_0, \cdots, x_m]$. Then

$$\bar{\nu}_n = \frac{q^{(m+1)n} - 1}{q^n - 1} = 1 + q^n + \cdots + q^{mn}, \text{ and so}$$

$$Z(\mathbf{P}^m, t) = \exp\left((1 + q^n + \cdots + q^{mn})t^n/n\right) = 1/(1-t)(1-qt)\cdots(1-q^m t).$$

Exercise 1.5.1. Let $\mathbf{P}_k^m$ denote the m-dimensional projective space defined by the zero ideal in $k[x_0, \cdots, x_m]$. Show the following:

i) The set of projective solutions of the zero ideal can be identified with $(k^{n+1} \backslash \{0\})/k^*$.

ii) $\mathbf{P}_{\mathbb{R}}^1 \simeq S^1$ as a topological space, (or as a manifold) where S^1 denotes the circle in the complex plane.

iii) Show that $\mathbf{P}_{\mathbb{R}}^m \simeq S^m/\pm 1$, obtained by identifying pairs of antipodal points on the m-sphere. Hence these spaces are all compact.

iv) Show that $\mathbf{P}_{\mathbb{C}}^1$ can be identified with the Riemann sphere, the one point compactification of the complex plane. Show that in general $\mathbf{P}_{\mathbb{C}}^m$ are compact topological spaces.

v) Let $\mathbf{A}_k^m$ denote the affine m-space defined by the zero ideal in $k[x_1, \cdots, x_m]$. Show that the projective m-space admits a decomposition (for example, as sets of solutions-disjoint),

$$\mathbf{P}_k^m = \mathbf{A}_k^m \cup \mathbf{A}_k^{m-1} \cdots \cup \mathbf{A}_k^0.$$

1.6. Smoothness. Heuristically a variety X of dimension d defined over the complex numbers, is smooth at a point $p \in X(\mathbb{C})$, if locally near the point p, the set of solutions looks like a ball in $\mathbb{C}^d$. Based on the implicit function theorem, an affine variety X of dimension d, defined by an ideal $I = (f_1, \cdots, f_m) \subset \mathbb{C}[x_1, \cdots, x_n]$ is said to be smooth at a point $a = (a_1, \cdots, a_n) \in X(\mathbb{C})$ if the matrix of partial derivatives,

$$\left((\frac{\partial f_i}{\partial x_j})(a_1, \cdots, a_n) \right),$$

has rank $n - d$.

Note that this definition is algebraic in character, and can be carried over to arbitrary fields, and not necessarily the complex numbers. We now take this as the definition of smoothness for an algebraic variety over k, in a neighbourhood of a point $a \in X(\bar{k})$.

Example 3. Let X be a variety defined by a single equation $f \in k[x_1, \cdots, x_n]$. Then X is smooth at a point $a = (a_1, \cdots, a_n) \in k^n$, if on Taylor expansion at the point a,

$$f(x_1, \cdots, x_n) = f(a) + \sum_i \frac{\partial f}{\partial x_i}(a)(x_i - a_i) + \text{ higher degree terms},$$

at least one $\partial f / \partial x_i(a)$ is non-zero.

For projective varieties, the condition of smoothness at a point, can be defined by dehomoginizing (see Remark above), and working with the corresponding affine space of solutions. Suppose now that we are considering the projective variety defined by a single homogeneous polynomial$f$. It can be checked that the projective variety $\bar{X}_f$ defined by f is smooth at a point $(a_0, \cdots, a_n)$, if $(a_0, \cdots, a_n)$ is not a solution of the system of equations,

$$\frac{\partial f}{\partial x_1}(x_1, \cdots, x_n) = 0, \cdots, \frac{\partial f}{\partial x_m}(x_1, \cdots, x_n) = 0.$$

Example 4. Let $f(x_0, \cdots, x_n) = a_0 x_o^m + \cdots + a_n x_n^m$, $(m, p) = 1$ and $a_0 \cdots a_n \neq 0$, where p is the characteristic of the base field. Then it can be checked that the projective variety defined by f is smooth.

1.7. Weil conjectures. Let X be a smooth, projective variety over a finite field k of dimension d.

a) $Z(X, t)$ is a rational function in t, i.e., of the form $P(t)/Q(t)$, where $P(t)$, $Q(t)$ are polynomial functions of t with rational integral coefficients. It also satisfies a suitable functional equation of the form,

$$Z(X, 1/q^d t) = \pm t^\alpha q^\beta Z(X, t),$$

where α and β are determined by the geometry of X.

b) (Riemann Hypothesis) There is a factorisation of $P(t)$ and $Q(t)$ in the ring $\mathbb{Z}[t]$ as,

$$P(t) = P_1(t)\cdots P_{2d-1}(t),$$
$$Q(t) = P_0(t)\cdots P_{2d}(t),$$

where $P_0(t) = (1-t)$ and $P_{2d}(t) = (1-q^d t)$. There is a factorisation of $P_i(t)$ over $\mathbb{C}$ of the form,

$$P_i(t) = \prod_{j=1}^{b_i}(1-\alpha_{ij}t).$$

α_{ij} are algebraic integers, and for any embedding $\iota : \bar{\mathbb{Q}} \to \mathbb{C}$, of an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, we have for all $i,\ j$ the analogue of the Riemann Hypothesis,

$$|\iota(\alpha_{ij})| = q^{i/2}.$$

c) (Topological interpretation for b_i) Suppose now that X is a smooth, projective variety over the integers (or after inverting a few primes), say defined by homogenous polynomials f_i. This amounts to saying that the set of solutions $X(\mathbb{C})$ of X over $\mathbb{C}$, admits a structure of a smooth, complex analytic manifold. In particular, the Betti numbers B_i are defined, where B_j is the $\mathbb{Z}$-rank of the cohomology group $H^j(X(\mathbb{C}),\mathbb{Z})$. For a prime p, it makes sense to consider the variety modulo p, i.e., the space of solutions defined by considering the polynomials f_i taken modulo modulo p. Then for any sufficiently large prime p, the conjecture is,

$$b_j = B_j.$$

In other words, the shape or the topology of the variety over $\mathbb{C}$, controls the growth of the number of solutions of the equations defining the variety over various finite fields.

Example 5. Suppose X is a smooth, projective curve defined over a finite field (analogous to that of number fields). For example, X can be the space of homogenous solutions in $\mathbf{P}^2$ of a homogeneous polynomial $f(x,y,z)$ in three variable of degree d, satisfying the smoothness condition:

there are no common solutions of the system of equations

$$\frac{\partial f}{\partial x} = 0,\ \frac{\partial f}{\partial y} = 0,\ \frac{\partial f}{\partial z} = 0.$$

In this case it can be seen that $B_0 = B_2 = 1$ and $B_1 = (d-1)(d-2)$. Further $P_1(X,s) = \prod(1-\alpha_{1j}q^{-s})$. Hence to say that the absolute values of α_{1j} be $\sqrt{q}$ is equivalent to saying that the zeros of P_1 lie on the line $\mathrm{Re}(s) = 1/2$. This is analogous to the usual Riemann Hypothesis for the Dedekind zeta function.

1.8. Frobenius and Weil cohomology. Let $F_q : \mathbb{A}^n \to \mathbb{A}^n$ be the Frobenius map sending,

$$(a_1, \cdots, a_n) \mapsto (a_1^q, \cdots, a_n^q).$$

Then X_m is the set of fixed points of F_q^m in $\overline{\mathbb{F}}_q^n$ which lie in the variety X. Now recall the Lefschetz fixed point theorem in topology: suppose $f : X \to X$ is a continuous self map of a topological manifold of dimension d, with isolated fixed points. Then the number of fixed points $\nu(f)$ is given by the expression,

$$\nu(f) = \sum_{i=0}^{d} (-1)^i \mathrm{Tr}(f \mid H^i(X, \mathbb{Z})).$$

In view of c) of the Weil conjectures stated above, Weil was inspired to conjecture the existence of a suitable cohomology theory for varieties defined over abstract fields and finite fields in particular having the following properties:

- The analogue of the Lefschetz fixed point theorem for the Frobenius morphism should be true. Since we are counting the number of fixed points, this forces the cohomology groups to have values in a characteristic zero ring, which we can assume to be a characteristic zero field L. Then we should have,

  $$\nu_n(X) = \sum_{i=0}^{2d} (-1)^i \mathrm{Tr}(F^n \mid H^i(\overline{X}, L),$$

  where F^n denotes the corresponding action of the Frobenius acting on $H^i(\overline{X}, L)$. From this it follows (exercise)

  $$Z(X, t) = \prod_{i=0}^{2d} \mathrm{d}et(1 - tF \mid H^i(X, L))^{-1}.$$

- The cohomology groups should have the correct Betti numbers. This means the following: Suppose $X(\mathbb{C})$ is the set of projective solutions of a system of homogeneous polynomial equations with integral coefficients. Assume that the corresponding space $X(\mathbb{C})$ is smooth as a topological manifold. Note that it will be a compact manifold, being a closed, subspace of the (compact) projective space. Since the equations have integral coefficients, it makes sense to consider the equations modulo a prime p, and to consider the corresponding projective variety of solutions X_p. Then for large enough p, the dimension of the $H^i(X_p, L)$, should be the i^{th} Betti number of the manifold $X(\mathbb{C})$.
- The duality for the zeta function should correspond to Poincare duality for the cohomology theory.

After initial efforts of Serre, such a cohomology theory was developed by Grothendieck and Artin. Grothendieck proved the Weil conjectures except for the Riemann Hypothesis, as a corollary of the cohomological machinery he had developed. Notice that this answers one of the initial hopes we had about the Riemann Zeta function- that of expressing the zeros of the zeta function as the eigenvalues of the Frobenius operator acting on the cohomology groups! The Riemann Hypothesis was proved by Deligne.

1.9. Modular forms. Consider the Ramanujan τ function defined formally by,

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

The corresponding Dirichlet series,

$$\sum_{n=1}^{\infty} \tau(n) n^{-s} = \prod_{p} (1-\tau(p)p^{-s}+p^{11-2s})^{-1},$$

defined for $\mathrm{Re}(s)$ large enough, admits analytic properties similar to the zeta function above- analytic continuation to the entire plane, is entire, and satisfies a functional equation. Ramanujan conjectured,

$$|\tau(p)| \leq 2p^{11/2}.$$

This conjecture was shown to be true by Deligne, as a consequence of the Weil conjectures. We have thus profited by searching for analogies of the Riemann Hypothesis!

Standard estimates for modular forms give the inequality, $\tau(n) = O(n^6)$. This was later refined by Rankin and Selberg, who provided the estimate $\tau(n) = O(n^{6-\epsilon})$.

Rankin's idea was to consider the Dirichlet series $\sum_n |\tau(n)|^2 n^{-s}$, the 'convolution' of the above series for $\tau(n)$ with itself, and to show that this Dirichlet series has suitable analytic properties. The germ of the idea to prove the Riemann Hypothesis, lies in adapting the Rankin-Selberg method to varieties defined over finite fields, and utilise the cohomological machinery developed by Grothendieck-roughly this amounts to relating Artin type L-functions on a n-fold product of the curve X^n for a curve X, to similar L-functions on curves. The starting point for the induction is the analogue of the prime number theorem, equivalent to providing a non-vanishing region for the L-functions.

1.10. Curves, Picard varieties and class groups. We now try to examine some algebraic ways of defining cohomology groups in the context of curves. It is this example which has served as a prime motivation for much of Iwasawa theory.

Let E be an elliptic curve defined over $\mathbb{C}$, i.e., a smooth, projective curve of genus 1 with a distinguished base point serving as the origin of a group law on the curve. E can also be explicitly given by a Weirstrass equation of the form

$$y^2z = 4x^3 + axz^2 + bz^3, \ a, b \in \mathbb{C},$$

in $\mathbf{P}^2_{\mathbb{C}}$, where the polynomial $4x^3 + ax + b$ has distinct roots in $\mathbb{C}$. Here the origin is given by the point at infinity $(0, 1, 0) \in \mathbf{P}^2_{\mathbb{C}}$. Complex analytically E is isomorphic to the complex analytic manifold $\mathbb{C}/L$, where L is a lattice in $\mathbb{C}$, i.e., a closed, discrete subgroup of $\mathbb{C}$ of rank 2 over $\mathbb{Z}$. Let $\mathcal{P}_L(z)$ be the Weierstrass $\mathcal{P}$-function associated to the lattice L,

$$\mathcal{P}_L(z) = \frac{1}{z^2} + \sum_{\omega \in L\backslash 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The corresponding Weierstrass equation as given above is the projective equivalent of the well-known identity

$$\mathcal{P}'_L(z)^2 = 4\mathcal{P}_L(z)^3 - g_4(L)\mathcal{P}_L(z) - g_6(L),$$

where $\mathcal{P}'_L(z) = \sum_{\omega \in L} -2/(z-\omega)^3$, and $g_4(L) = 60 \sum_{\omega \in L\backslash 0} 1/\omega^4$, $g_6 = 140 \sum_{\omega \in L\backslash 0} 1/\omega^6$.

The fundamental group $\pi_1(E, 0)$ can be identified with the lattice L. Since L is commutative, the first homology group of $H_1(E, \mathbb{Z})$ can again be identified with L. Given a finite covering $\mathbb{C}/L' \to \mathbb{C}/L$, where $L' \supset L$ is a lattice in $\mathbb{C}$, there exists an integer n such that $nL \subset L' \subset L$ ($\mathbb{C}/L'$ is an algebraic object and is in fact again an elliptic curve). Thus the collection of covers given by the multiplication by n map, $n_L : \mathbb{C}/L \to \mathbb{C}/L$ is cofinal in the collection of (algebraic) coverings of the curve E. The profinite completion $\hat{\pi}_1(E)$ of the fundamental group (analogous to the definition of the Galois group for an infinite Galois extension), can thus be identified with the profinite limit of

$$\pi_1(E) \simeq \varprojlim L/nL \simeq \varprojlim (\mathbb{Z}/n\mathbb{Z})^2,$$

where L/nL can be identified with the Galois group of the covering map $n : \mathbb{C}/L \to \mathbb{C}/L$. Since $(\mathbb{C}/L)/\text{Ker } n_L \simeq \mathbb{C}/L$, we have a natural identification,

$$\hat{\pi}_1(E) \simeq \varprojlim \text{Ker } n_L.$$

The key point to be observed in the above isomorphism, is that the left hand side is defined topologically as the profinite completion of the fundamental group, whereas the right hand side can be interpreted algebraically as the inverse limit over n of the n-division points $E_{[n]}$ on E. We can thus take the right hand side as a substitute for the first homology of an elliptic curve, defined over an arbitrary field k. To make a suitable theory, and in order to have values in a characteristic zero field, one should fix a prime l coprime to the characteristic of k, and consider $\lim_{\leftarrow} E_{[l^m]}$ as a substitute for the first homology.

For curves C of higher genus, we have the Jacobian variety $J(C)$, which complex analytically can be identified with $H^1(X,\mathbb{R})/H^1(X,\mathbb{Z})$, with $H^1(X,\mathbb{R})$ equipped with an almost complex structure coming from the complex structure on X. We can again imitate the same construction, provided there is an algebraic interpretation of the Jacobian of a curve. Such a construction is obtained by constructing the Picard group of a curve. We will now tabulate some of the well known analogies between number fields and algebraic curves:

NUMBER FIELDS	CURVES
number	meromorphic function
non-zero prime ideal $\mathfrak{p}$	Point P
valuation corresponding to $\mathfrak{p}$	order of zero at P
ideal $\mathfrak{a} = \prod_i \mathfrak{p}_i^{a_i}$	divisor $D = \sum_i a_i P_i$
principal ideal $(a) = \prod_i \mathfrak{p}_i^{a_i}$	divisor of a meromorphic function $(f) = \sum_i \mathrm{ord}_{P_i}(f) P_i$
ideal class group	Picard group=divisors of degree zero modulo principal divisors

In analogy with the Picard group of a curve, one is led to considering the ideal class group of a number field. If X is a curve defined over $\mathbb{F}_q$, then the group of divisors made up of points on the curve over $\mathbb{F}_q$ modulo principal rational divisors is finite. The relevant Picard group is obtained by considering these rational Picard groups over all the finite extensions $\mathbb{F}_{q^n}$, or equivalently that of the Picard group of the curve over $\bar{\mathbb{F}}_q$.

2. Diagonal Fermat hypersurfaces

We will now verify part of the Weil conjectures for the zeta function of a diagonal Fermat hypersurface of the form

$$f(x_0, \cdots, x_m) = x_0^k + \cdots x_m^k.$$

This example was worked out by Weil. The idea behind the proof is to count the number of solutions using character sums. The rationality of the zeta function then amounts the Davenport-Hasse theorem relating Gauss sums over extension fields. The Riemann Hypothesis comes from the fact that the absolute values of a Gauss sum $G(\chi)$ is $\sqrt{q}$, for a non-trivial character χ of $\mathbb{F}_q^*$.

Fix q a power of a prime p and let $k_s = \mathbb{F}_{q^s}$. Assume that $n|(q-1)$. Consider the projective variety defined by the homogeneous equation

$$f(x_o, \cdots, x_r) = x_0^n + \cdots + x_r^n = 0$$

in projective r-space $\mathbf{P}^r$. Let

$$\overline{N}_s = \#\{(a_0, \cdots, a_r) \in (k_s^{r+1} \backslash 0)/k_s^* \mid a_0^n + \cdots + a_r^n = 0\}$$

be the set of projective solutions of f in $\mathbf{P}^r_{k_s}$. We first concentrate on a single field, say $k = k_0$, and count the number of solutions over k. Let

$$N = \#\{(a_0, \cdots, a_r) \in k_s^{r+1} \mid a_0^n + \cdots + a_r^n = 0\}$$

be the number of affine solutions. Then

$$\overline{N} = \frac{N-1}{q-1}.$$

For each $u \in k$, let

$$N(u) = \#\{x \in k \mid x^n = u\}.$$

We will indicate the steps involved in calculation N.

Step 1: Expressing N as a character sum.

i) For each $u \in k$, let

$$N(u) = \#\{x \in k \mid x^n = u\} = \begin{cases} 1 & \text{if } u = 0, \\ d & \text{if } u \text{ is a n}th \text{ power}, \\ 0 & \text{otherwise}. \end{cases} \tag{2.0.1}$$

$$\text{Then } N = \sum_{u | L(u) = 0} N(u_0) \cdots N(u_r),$$

where $L(u) = u_0 + \cdots + u_r$.

ii) Choose a generator ω of k^* (a primitive root), and for

$$\alpha \in S = \left\{0, \frac{1}{n}, \cdots, \frac{n-1}{n}\right\},$$

$$\text{define } \chi_\alpha(\omega) = e^{2\pi i \alpha}.$$

Extend to 0, by defining

$$\chi_\alpha(0) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 0 & \alpha \neq 0. \end{cases} \tag{2.0.2}$$

$$\text{Then } N(u) = \sum_{\alpha \in S} \chi_\alpha(u), \tag{2.0.3}$$

$$\text{and so } N = \sum_{\{u|\ L(u)=0\}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r). \tag{2.0.4}$$

Step 2: Relating N to Jacobi sums.

The contribution from the term corresponding to $\alpha_0 = \cdots = \alpha_r = 0$ is q^r as $L(u) = 0$.

iii) If there exists $0 < s \le r$ such that $\alpha_0, \cdots, \alpha_{s-1}$ are non-zero, and $\alpha_s = \cdots = \alpha_r = 0$, then the contribution of the corresponding term is zero. Hence

$$N = q^r + \sum_{L(u)=0,\ \alpha_i \neq 0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r). \tag{2.0.5}$$

iv) If $u_0 = 0$, then contribution is zero. Assume now $u_0 \neq 0$. Write for $i \ge 1$, $u_i = u_o v_i$. Then v_i satisfy the equation

$$\sum v_i = -1.$$

Now $\#\{u \mid L(u) = 0, u_0 \neq 0\} = (q-1)\#\{v = (v_1, \cdots, v_r) \mid \sum v_i = -1\}$. Let $T = \{\alpha = (\alpha_1, \cdots, \alpha_r) \in S^r \mid \alpha_i \neq 0,\ \sum_{i=0}^r \alpha_i = 0\}$. For $\alpha \in T$, define $\alpha_0 = -(\sum_{i=1}^r \alpha_i \neq 0$. Define the Jacobi sum for $\alpha \in T$, as

$$J_k(\alpha) = \sum_{\sum v_i = -1} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r). \tag{2.0.6}$$

$$\text{Then } N = q^r + (q-1) \sum_{\alpha \in T} J_k(\alpha). \tag{2.0.7}$$

Step 3: Jacobi and Gauss sums.

v) Having related the number of solutions to Jacobi sums, we now relate this to Gauss sums. This would enable us to use the Davenport-Hasse theorem, relating Gauss sums over extension fields, in order to compute the zeta function.

Let $\psi : (k, +) \to S^1$ be a fixed additive character of the field k. Define the Gauss sum,

$$G_k(\chi, \psi) = \sum_{x \in \mathbb{F}_q} \chi(x)\psi(x).$$

The Gauss sum is the Fourier transform of the multiplicative character χ with respect to the additive character ψ, and can be thought of as the analogue of the Gamma function. For $\alpha \in T$ show that,

$$J_k(\alpha) = \frac{1}{q} G_k(\chi_{\alpha_0}, \psi) \cdots G_k(\chi_{\alpha_r}, \psi),$$

where $\alpha_0 = -(\sum_{i=1}^r \chi_{\alpha_i})$.

Hint: Can assume that $x_0 \neq 0$. Write $x_i = x_0 y_i$.

vi) Now substitute for $k = k_s$, with the obvious notation. Then,

$$\overline{N}_s = (N_s - 1)/(q^s - 1) = 1 + q^s + \cdots q^{s(r-1)} + \sum_{\alpha \in T_s} J_s(\alpha).$$

Step 4: Properties of Gauss sums.

vii) In order to compute the zeta function, we need to know the behaviour of Gauss sums by field extensions. The main result that is needed to show the rationality of the zeta function is the theorem of Davenport-Hasse,

$$G_s(\chi \circ N_s, \psi \circ T_s) = (-1)^{s-1} G(\chi, \psi)^s,$$

where $N_s : k_s^* \to k_0 = k$ denotes the norm map and $T_s : k_s \to k$ is the trace map. Our assumption that $n|(q-1)$ implies as χ runs over the characters of order n of k_0^*, then $\chi \circ N_s$ runs over the characters of order n of k_s^*. Hence we get,

$$J_s(\alpha \circ N_s) = (-1)^{(r-1)(s-1)} J(\alpha)^s,$$

with the evident notation.

Step 5. Rationality and the Riemann Hypothesis.

viii) The logarithmic derivative of $Z(X, t)$ becomes

$$\sum_{s=1}^{\infty} \overline{N}_s t^{s-1} = -\sum_{h=0}^{r-1} \frac{d}{dt}(1 - q^h t) + (-1)^r \sum_{\alpha \in T} \frac{d}{dt} \log(1 - (-1)^{r-1} J(\alpha) t).$$

Hence $Z(X, t) = \dfrac{1}{(1-t)\cdots(1-q^{r-1}t)} \left(\prod_{\alpha \in T} (1 - (-1)^{r-1} J(\alpha) t) \right)^{(-1)^{r-1}}$.

ix) Riemann Hypothesis follows from the fact,

$$|G_{\mathbb{F}_q}(\chi, \psi)| = \sqrt{q}.$$

Step 6. Betti numbers

x) We will leave it to the reader to check that the Betti numbers of the corresponding complex points of the projective variety are the same as that indicated by the Weil conjectures.

3. Growth of class groups along cyclotomic towers

Let us look at some of the aspects of zeta functions of varieties defined over finite fields, with a view to carry them over to number fields.

1) The first aspect that comes to our mind, is that the Galois group $G(\bar{\mathbb{F}}_q/\mathbb{F})$ of an algebraic closure $\bar{\mathbb{F}}_q$ over $\mathbb{F}_q$ is isomorphic to the profinite completion $\hat{\mathbb{Z}} = \lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z}$. A topological generator is given by the Frobenius automorphism $\phi(x) = x^q$ of $\bar{\mathbb{F}}_q$. This gives a distinguished generator, with respect to which it is possible to talk about characteristic polynomials. Thus one type of extensions in number fields we would like to look at are extensions which are topologically generated by a single element.

2) A second aspect is that $\bar{\mathbb{F}}_q$ is generated by roots of unity over the base field. This property is satisfied by the above example.

3) In analogy with curves over finite fields, the ideal class groups of number fields can be considered as a substitute for the Picard group. The analogue of working over the algebraic closure, lies in considering the collection of the ideal class groups along a tower of compatible cyclic extensions.

Example 6. Let p be a prime, and let $q = 4$ if $p = 2$, and $q = p$ if p is odd. Let d be a positive integer coprime to p. Denote by K_n be field $\mathbb{Q}(\zeta_{dqp^n})$. Then $\mathrm{Gal}(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}$.

The important observation of Iwasawa, is that instead of considering the full ideal class group, if we consider the p-primary component X_n of the ideal class group of K_n, these patch together to give a module over the group ring $\mathbb{Z}_p[\Gamma]$, where Γ is the Galois group of $(\cup_n K_n)/K_0$. The structure theory of modules over this ring can be worked out, and applying class field theory provides us with information about the growth of these groups X_n.

3.1. Inverse limits. We recall the notion of inverse limits. The reader who is familiar with inverse limits, can skip this section. We work in a general category $\mathcal{C}$- for example the category of sets, topological spaces, groups,...Let $(I, \leq)$ be a partially ordered set, and an inverse system consists of the following: a) for each $i \in I$ an object X_i in $\mathcal{C}$, b) for $i \leq j$, a map $\phi_{ij} : X_j \to X_i$. This satisfies the compatibility condition that for $i \leq j \leq k$, then $\phi_{jk}\phi_{ij} = \phi_{ik}$. Let X be an object equipped with a collection of maps $\pi_i : X \to X_i$ satisfying the compatibility condition $\phi_{ij}\pi_j = \pi_i$ for pairs $i, j \in I$, $i \leq j$. We say that X is a inverse limit of the of the inverse system (X_i, ϕ_{ij}, I) if it satisfies the following universal property:
given a family of maps $\psi_i : Z \to X_i$ from an object Z in $\mathcal{C}$, satisfying the compatibility condition $\phi_{ij}\psi_j = \psi_i$, for $i \leq j$, $i, j \in I$, then there exists a unique map $\Psi : Z \to X$, such that $\pi_i\Psi = \psi_i$ for all $i \in I$. The inverse limit if it exists, is unique upto a unique isomorphism.

If $\mathcal{C}$ is a full subcategory of the category of sets, then in terms of elements X can be described as,

$$X = \{(x_i) \in \prod_i X_i \mid \phi_{ij}(x_j) = x_i, \text{ for } i \leq j\}.$$

Example 7. Let A be a ring with an ideal J. Let the indexing set be the natural numbers $\mathbb{N}$ with the usual order. For $m \leq n$, we have natural ring homomorphisms $A/J^n \to A/J^m$. The inverse limit $\hat{A}_J$ taken in the category of rings, is called the J-adic completion of A. For example, take A to be the integers $\mathbb{Z}$, and $J = (p)$ the ideal generated by a prime number p. Then the p-adic completion of $\mathbb{Z}$ along (p) gives the ring of p-adic integers $\mathbb{Z}_p$.

Another similar example can be obtained by taking $A = \mathbb{Z}[T]$ (or even $\mathbb{Z}_p[T]$), and J to be the ideal (p, T) generated by p and T. Then the completion gives the ring of formal power series $\mathbb{Z}_p[[T]]$, with coefficients in $\mathbb{Z}_p$. In this case, it is possible to consider the completion in the category of topological rings, by equipping the finite ring quotients $\mathbb{Z}[T]/(p, T)^n$ with the discrete topology. The profinite completion $\mathbb{Z}_p[[T]]$ has the structure of a compact ring.

Example 8. Let L/K be an algebraic extension of fields. Since each element in L is algebraic over K, L can be written as the union of finite extension fields M of K. Assume not that L can be written as a union of finite Galois extensions over K. We will then say that L is Galois over K. Moreover the Galois group $G(L/K)$ is the projective(inverse) limit of the finite Galois groups $G(M/K)$, where M is a finite Galois extension of K. The inverse limit is taken over the indexing set of all finite Galois extensions M of K, ordered by inclusion. $G(L/K)$ has thus the structure of a profinite group, and is compact in particular.

Suppose K is a number field, and v a place of K. v is ramified (unramified) if v is ramified in some finite extension (unramified in any finite extension) $M \subset L$ of K. A valuation belonging to the place v can be extended to any finite extension, and thus extended to L. If w is a valuation on L extending v, then we say that $w|v$. Define the decomposition group D_w and inertia group I_w at w as,

$$D_w = \varprojlim_{M} D_{w|M} \text{ and } I_w = \varprojlim_{M} I_{w|M}$$

3.2. Our aim now is to prove the following theorem of Iwasawa concerning of growth of ideal class groups along a $\mathbb{Z}_p$ tower. Let K_0 be a finite extension of $\mathbb{Q}$, and let K_∞/K_0 be a $\mathbb{Z}_p$ extension, i.e., $\Gamma := \mathrm{Gal}(K_\infty/K_0) \simeq \mathbb{Z}_p$.

Write

$$K_\infty = \cup_{n\geq 0} K_n$$
$$\text{with } \Gamma_n := \mathrm{Gal}(K_n/K_0) \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Denote by $\gamma = (\gamma_n)$ a topological generator for Γ. γ_n is a compatible collection of generators for the groups Γ_n.

Example 9. Let p, q and d be as in the example above, and let $K_n = \mathbb{Q}(\zeta_{dqp^n})$. Write $K_\infty = \cup_n K_n$. Then $G(K_\infty/K_0) \simeq \mathbb{Z}_p$. These extensions will be referred to as cyclotomic $\mathbb{Z}_p$-extensions, and will constitute our primary examples.

Let X_n be the p-Sylow subgroup of the ideal class group of K_n. Write

$$|X_n| = p^{e_n}.$$

The theorem of Iwasawa is the following:

Theorem 3.2.1. *Let K_∞/K_0 be a $\mathbb{Z}_p$ extension. There exists integers $\lambda \geq 0, \mu \geq 0, \nu$ and a positive n_0, such that for $n \geq n_0$,*

$$e_n = \lambda p^n + \mu n + \nu.$$

For the proof, let

$$X = \lim_{\leftarrow} X_n,$$

where the inverse limit is taken with respect to the norm maps $N : K_m \to K_n$, $m \geq n$. We have a compatible action of $\mathrm{Gal}(K_n/K_0) = \Gamma_n$ on X_n,

$$N(\gamma_m x_m) = r(\gamma_m) N(x_m),$$

where $\gamma_m \in \Gamma_m$, and r denotes the natural restriction map $\Gamma_m \to \Gamma_n$. Hence we get a continuous action of Γ on X.

Further since each X_n is a p-primary abelian group of order p^{e_n}, there is an action of $\mathbb{Z}_p$ on $X(n)$, via the projection $\mathbb{Z}_p \to Z_p/p^{e_n}\mathbb{Z}_p \to \mathbb{Z}/p^{e_n}\mathbb{Z}$. This action is compatible with the norm maps. Thus we get an action of $\mathbb{Z}/p^{e_n}\mathbb{Z}[\Gamma_n]$, the group ring of Γ_n with coefficients in $\mathbb{Z}/p^{e_n}\mathbb{Z}$ on X_n. Let

$$\Lambda := \mathbb{Z}_p[\Gamma] = \lim_{\underset{n}{\leftarrow}} \mathbb{Z}/p^{e_n}\mathbb{Z}[\Gamma_n].$$

This is a profinite ring. Note that both $\mathbb{Z}_p[\Gamma]$ are profinite spaces, and thus carry a topology with respect to which they are compact. It can be checked that we obtain a continuous action of Λ on X.

The proof of Iwasawa's theorem follows from:

1) Structure theory of $\mathbb{Z}_p[\Gamma]$-modules.

2) Using class field theory to obtain information about the finite layers X_n from X.

3.3. Application of Class Field Theory. We will begin with 2) first. First some preliminaries:

Lemma 3.3.1. *a) Let K_∞/K_0 be a $\mathbb{Z}_p$-extension. l a prime of K_∞ not dividing p. Then K_∞ is unramified at l. In particular there are only finitely many primes of K_0 which ramify in K_∞.*

b) At least one prime ramifies.

c) There is a finite extension K_n such that every prime of K_n which ramifies is totally ramified.

We will not present a proof of the lemma, which follows quite easily from class field theory, but instead will be content upon remarking that for the cyclotomic $\mathbb{Z}_p$-extension the properties stated in the lemma are seen to be satisfied.

Henceforth we will assume the following, and it can be seen that the cyclotomic $\mathbb{Z}_p$-extension satisfy the following:

1) K_0 is such that all primes of K_0 which ramify in K_∞ are totally ramified.

2) There is only one prime of K_0 which is totally ramified.

These assumptions imply that there is a unique place of K_∞, lying over the ramified prime of K_0, and we have an identification of the inertia group I at this prime with Γ.

3.3.1. *Hilbert class fields.* The main aim is to recover X_n from X. For this we use class field theory. Recall that the Hilbert class field H_K of K, is the maximal abelian unramified extension of K. By class field theory, we know that H_K/K is a finite, abelian extension and there is canonical identification,

$$F: \ C(K) \to G(H_K/K),$$

where $C(K)$ denotes the class group of K. The identification is obtained by sending a prime ideal $\mathfrak{p}$ of K, to the corresponding Frobenius element, and extending it multiplicatively to the class group. Recall that the Frobenius element for an abelian extension of number fields L/K, corresponding to an unramified prime ideal $\mathcal{P}$ of L lying over a prime ideal $\mathfrak{p}$ of K, is the unique element $F(\mathfrak{p})$ in $G(L/K)$ satisfying,

$$F(\mathfrak{p})(x) \equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}}, \tag{3.3.1}$$

where x is an integral element in L. Since L/K is abelian, $F(\mathfrak{p})$ is independent of the choice of $\mathcal{P}$ dividing $\mathfrak{p}$.

Suppose K is a Galois extension of E, with Galois group Γ. Let G denote the Galois group of H_K/E. We have the exact sequence,

$$1 \to C(K) \simeq G(H_K/K) \to G \to \Gamma \to 1. \tag{3.3.2}$$

We have now two naturally defined actions of Γ on $C(K)$. The first action, is via the interpretation of Γ as automorphisms of K, and $C(K)$ in terms of fractional ideals in K. Namely, an element $\gamma \in \Gamma$, acts on an ideal I of K, by $(\gamma, I) \to \gamma(I)$. This descends down to an action of Γ on $C(K)$. The second action is via the exact sequence 3.3.2 above, and the interpretation of $C(K)$ as $G(H_K/K)$. For $\gamma \in \Gamma$, choose a lift to G, denoted again by γ. γ acts by sending an element $x \in C(K)$ to $x^\gamma := \gamma^{-1}x\gamma$. Via the identification $F : C(K) \to G(H_K/K)$, these two actions are the same:

Lemma 3.3.2. *Let $\mathfrak{p}$ be an unramified prime ideal of K over E. Then for $\gamma \in \Gamma$,*

$$\gamma^{-1}F(\mathfrak{p})\gamma = F(\gamma^{-1}\mathfrak{p}).$$

Proof. Let x be an algebraic integer in E, and $\mathcal{P}$ be a prime ideal in the ring of integers of E lying over $\mathfrak{p}$. We have,

$$F(\mathfrak{p})(\gamma x) \equiv (\gamma x)^{N\mathfrak{p}} \pmod{\mathcal{P}}.$$

We apply γ^{-1} to both sides. Then $\gamma^{-1}\mathcal{P}|\gamma^{-1}\mathfrak{p}$, and $N(\gamma^{-1}\mathfrak{p}) = N(\mathfrak{p})$. Hence,

$$\begin{aligned} \gamma^{-1}F(\mathfrak{p})\gamma(x) &\equiv \gamma^{-1}((\gamma x)^{N\mathfrak{p}}) \pmod{\mathcal{P}} \\ &\equiv x^{N\gamma^{-1}\mathfrak{p}} \pmod{\gamma^{-1}\mathcal{P}}. \end{aligned}$$

□

Let M_n be the maximal unramified abelian p-extension of K_n. From the identification of the Galois group with the Hilbert class field as in the above paragraph, we have the following identification, still denoted by F:

$$F: \; X_n \to G(M_n/K_n). \tag{3.3.3}$$

Let G_n denote the Galois group of M_n over K_0. Since K_{n+1} is a ramified extension of K_n and M_n an unramified extension of K_n, the fields M_n and K_{n+1} are linearly disjoint. The extension M_nK_{n+1} is unramified over K_{n+1}, and the Galois group $G(M_nK_{n+1}/K_{n+1})$ can be identified with $G(M_n/K_n)$. There is a natural restriction map $r : G(M_nK_{n+1}/K_{n+1}) \to G(M_n/K_n)$. We have,

Lemma 3.3.3. *a) The following diagram is commutative:*

$$\begin{tikzcd} X_{n+1} \arrow[r, "F"] \arrow[d, "N"] & G(M_{n+1}/K_{n+1}) \arrow[d, "r"] \\ X_n \arrow[r, "F"] & G(M_n/K_n) \end{tikzcd}$$

Proof. Choose a prime ideal $\mathcal{P}$ of $\mathcal{O}_{M_{n+1}}$ lying over a prime $\mathfrak{p}$ of $\mathcal{O}_{K_{n+1}}$. Assume that $\mathfrak{p}$ is unramified over K_n and divides the prime p of $\mathcal{O}_{K_n}$. Then the norm from K_{n+1} to K_n of the ideal $\mathfrak{p}$ is p^f, where f is the degree of the residue field extensions, satisfying $N\mathfrak{p} = Np^f$. Let x be an integral element in M_n. The restriction $rF(\mathfrak{p})(x)$ satisfies,

$$\begin{aligned} rF(\mathfrak{p})(x) &\equiv x^{N\mathfrak{p}} \pmod{\mathcal{P}} \\ i.e.,\ F(\mathfrak{p})(x) &\equiv x^{Np^f} \pmod{\mathcal{P}} \\ &\equiv F(p)(x)^f \pmod{\mathcal{P}} \\ &\equiv F(p)^f(x) \pmod{\mathcal{P}} \\ &\equiv F(N\mathfrak{p}) \pmod{\mathcal{P}} \end{aligned}$$

□

3.3.2. Let M_∞ be the compositum of the fields M_n. M_∞/K_∞ is Galois with Galois group isomorphic to X. It can be shown that M_∞ is the maximal unramified p-abelian extension of K_∞. Denote by G the Galois group of M_∞ over K_∞. We have the exact sequence,

$$1 \to X \to G \to \Gamma \to 1. \tag{3.3.4}$$

As before, let γ denote a topological generator of Γ. Note that the element $\gamma - 1$ in the Iwasawa algebra acts by sending $(\gamma-1) : x \mapsto x^{\gamma-1} = \gamma x \gamma^{-1} x^{-1}$.

Proposition 3.3.1. *X_0 is the group of coinvariants for the Γ action on X, i.e., we have*

$$X/X^{\gamma-1} \simeq X_0 \simeq G(M_0/K_0).$$

More generally for $n \geq 0$,

$$X/X^{\gamma^{p^n}-1} \simeq X_n \simeq G(M_n/K_n).$$

Before we prove this proposition, we recall a bit about semi-direct products. Given an exact sequence of groups,

$$1 \to X \to G \xrightarrow{\pi} \Gamma \to 1,$$

we say that the exact sequence splits, or that G is a semi-direct product of Γ by X, written $G = X \times \Gamma$, if there exists a (continuous) section $s : \Gamma \to G$, such that $\pi \circ s = \mathrm{id}_\Gamma$. This amounts to giving a subgroup $H \subset G$, such that $H \cap X = \{1\}$, and H maps onto Γ. The splitting provides an action of Γ on X. It can be checked that the following are equivalent for a semi-direct product G: i) $s(\Gamma)$ is a normal subgroup of G. ii) the induced action of Γ by a splitting section s on X is trivial. iii) G is isomorphic to the direct product of the groups $X \times s(\Gamma)$.

Lemma 3.3.4. *The exact sequence 3.3.4 splits.*

Proof. Let I denote the inertia group of a prime of M_∞ lying over the unique prime of K_0 ramifying inside K_∞. Since K_∞ is totally ramified over K_0, I restricted to K_∞ is surjective. Further M_∞ is an unramified extension of K_∞. Hence $I \cap X = 1$. This implies that G is the semi-direct product of I and X. □

Lemma 3.3.5. *The closure of the commutator group* $\overline{[G,G]}$ *is isomorphic to* $X^{\gamma-1}$.

Proof. Take $x \in X$. Then

$$x^{\gamma-1} = \tilde{\gamma}x\tilde{\gamma}^{-1}x^{-1} \in [G,G].$$

This implies $X^{\gamma-1} \subset [G,G]$.

Conversely look at the exact sequence,

$$1 \to X/X^{\gamma-1} \to G/X^{\gamma-1} \to \Gamma \to 1.$$

Note that $X^{\gamma-1}$ is a closed normal subgroup of G (why?- because I normalises, and it is closed since it is the image of the compact group X by the map $\gamma - 1$).

By definition, the Γ which is topologically generated by γ, acts trivially on the extension. Hence the semi-direct product becomes a product. Hence $G/X^{\gamma-1}$ is a commutative group. This implies that $X^{\gamma-1} \supset \overline{[G,G]}$.

□

Proof of Proposition 3.3.1 M_0 is the maximal p-primary abelian unramified extension of K_0. Since M_0 is an abelian extension of K_0, we have $G(M_\infty/M_0) \subset [G,G]$. Since M_0/K_0 is unramified implies that $G(M_\infty/M_0) \subset I$.

3.4. Structure theory of modules over the Iwasawa algebra. In this section, we follow Serre in understanding the structure theory of modules over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[\Gamma]$. The key point is to identify Λ with the power series ring $\mathbb{Z}_p[[T]]$.

Proposition 3.4.1.

$$\Lambda \simeq \mathbb{Z}_p[[T]].$$

Note that if we work at the finite level, then we have an obvious isomorphism of the group ring

$$\mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[U]/(U^{p^n} - 1),$$

by sending a generator γ_n of Γ_n to the element U. The problem with this isomorphism is that the isomorphism is not compatible with the inverse system formed by $\mathbb{Z}_p[\Gamma_n]$. In order to build a compatible system, we need to work with a different generator for the ring $\mathbb{Z}_p[U]/(U^{p^n} - 1)$. Substitute $U = T + 1$. We then have

$$\mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[U]/(U^{p^n} - 1) \simeq \mathbb{Z}_p[T]/((1+T)^{p^n} - 1).$$

The polynomial $h_n(T) = (1+T)^{p^n} - 1$ is an example of a *distinguished polynomial*:

Definition 1. A polynomial of the form $T^n + a_1T^{n-1} + \cdots + a_n$ is distinguished if all the coefficients a_i are divisible by p.

Lemma 3.4.1.

$$\lim_{\overleftarrow{n}} \mathbb{Z}_p[[T]]/(h_n) \simeq \mathbb{Z}_p[[T]].$$

Proof.

$$\begin{aligned} h_{n+1} = (1+T)^{p^{n+1}} - 1 &= ((1+T)^{p^n} - 1 + 1)^p - 1 \\ = (h_n + 1)^p - 1 &= h_n^p + ph_n^{p-1} + \cdots + ph_n. \end{aligned}$$

Thus by induction we see that h_{n+1} is in the ideal $(p,T)^{n+1}$. □

Lemma 3.4.2.

$$\mathbb{Z}_p[[T]]/(h_n) \simeq \mathbb{Z}_p[T]/(h_n) \simeq \mathbb{Z}_p[\Gamma_n].$$

Proof. The proof of this rests on the Euclidean algorithm for the power series ring: if f is a distinguished polynomial of degree n, and $g \in \mathbb{Z}_p[[T]]$, then there exists unique elements $q \in \mathbb{Z}_p[[T]]$ and a polynomial $r \in \mathbb{Z}_p[T]$ of degree less than n. □

From the above lemmas, we have a proof of the proposition. (Make a remark that the h_n are compatible with taking the inverse limit).

Remark. Note that if we are working over $\mathbb{Q}_p$ instead of $\mathbb{Z}_p$, then we will not have the above lemma, and the inverse limits of the group rings with coefficients in $\mathbb{Q}_p$ will not have the nice description in terms of formal power series as given above.

In terms of the identification of Λ with $\mathbb{Z}_p[[T]]$, we have by Proposition 3.3.1 (iii),

$$X_n = X/h_n(T)X.$$

In order to use the structure theorem, we need to know that X is finitely generated as a module over Λ, and this is provided by the following topological version of Nakayama's lemma. We begin with a topological version of Nakayama's lemma, which asserts the finite generation of X as a Λ-module.

Lemma 3.4.3. *Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{m}$. Let V be a compact topological module over $\mathcal{O}$ with respect to the $\mathfrak{m}$-adic topology.*

i) if $\mathfrak{m}V = V$, then $V = 0$.

ii) if $\mathcal{O}$ is compact, and $V/\mathfrak{m}V$ is finitely generated, then V is finitely generated.

Proof. Exercise. □

Going back to the proof of Iwasawa's theorem on the growth of class groups along $\mathbb{Z}_p$-extensions, we see that it follows from Nakayama's lemma, and the identification of $X/h_0X \simeq X_0$, that X is a finitely generated Λ-module.

Corollary 3.4.1. *X is finitely generated as a Λ-module.*

Remark. Note that this lemma is different from the usual Nakayama lemma, which assumes a priori that V is finitely generated. Here by imposing a topological notion, we are able to conclude the finite generation of V, from the finite generation of the covariants of V with respect to $\mathfrak{m}$.

We state without proof the following structure theorem for finitely generated modules over $\mathbb{Z}_p[[T]]$. For a proof, we refer to Washington's or Lang's book.

Theorem 3.4.2. *Let V be a finitely generated module over $\mathbb{Z}_p[[T]]$. Then there is morphism*

$$V \to \Lambda^r \oplus \prod_i \Lambda/(p^{n_i}) \oplus \prod_j \Lambda/(f_j^{m_j})$$

with finite kernel and cokernel, and where f_j are distinguished and irreducible polynomials.

As a corollary we obtain the following theorem:

Theorem 3.4.3. *There is an injective morphism from X to a Λ-module of the form $\prod_i \Lambda/(p^{n_i}) \oplus \prod_j \Lambda/(f_j^{m_j})$ with finite cokernel, and where f_j are distinguished polynomials.*

This follows from the fact that if X contains a copy of Λ, then X_0 will be infinite, contradicting the finiteness of the class number. In order to establish the growth of class numbers along a $\mathbb{Z}_p$-extension, we have to examine the growth of these modules. Note that

$$X_n = X/X^{\gamma^{p^n}-1},$$

a) $V = \Lambda/(p^m)$. Then,

$$V_n \simeq (\mathbb{Z}/p^m\mathbb{Z})[[T]]/(h_n) \simeq (\mathbb{Z}/p^m\mathbb{Z})[T]/(T^{p^n} - 1).$$

Thus V_n is a free module of rank p^n over $\mathbb{Z}/p^m\mathbb{Z}$, and is of cardinality p^{mn}.

b) $V = \Lambda/(f)$, f a distinguished polynomial of degree d. We assume that V_n is finite for all n, an assumption satisfied for the module X in our situation. Note that since f is distinguished,

$$f \cong T^d \pmod{p}.$$

Hence there exists n_0, such that for $n > n_0$,

$$T^{p^{n-1}} \cong 0 \pmod{(f,p)}.$$

For an element $P \in \Lambda$, denote by $L(P)$ the left multiplication by P on V. Then for $n > n_0$,

$$L(T)^{p^{n-1}} \cong 0 \ (\mathrm{mod}\ p).$$

It follows that,

$$L((1+X)^{p^{n-1}}) \cong 1 \ (\mathrm{mod}\ p).$$

$$L((1+X)^{p^n}) \cong (L((1+X)^{p^{n-1}})^p \cong 1 \ (\mathrm{mod}\ p^2).$$

We have,

$$(1+T)^{p^{n+1}} - 1$$

$$= \{(1+T)^{p^n} + (1+T)^{2p^n} + \cdots + (1+T)^{(p-1)p^n}\}\{(1+T)^{p^n} - 1\}.$$

From this it can be seen by induction that for some unit element u,

$$(\gamma_n - 1)V = p^{n-n_0}u(\gamma_{n_0} - 1)V, \ n > n_0 \gg 0.$$

Since $(\gamma_{n_0} - 1)V$ is of finite index in $\mathbb{Z}_p^d$, it is isomorphic to $\mathbb{Z}_p^d$, and so upto a constant error term the growth as n varies, is given by dn, where d is the degree of the distinguished polynomial f. Thus μ is the sum of the degrees of the polynomials $(f_j^{m_j})$ occurring in the decomposition of the module V.

4. Construction of p-adic L-function via Stickelberger

Let χ be a Dirichlet character, and fix a prime p. Our objective in this section is to outline a construction of the p-adic L-function $L_p(s,\chi)$ associated to the character χ, following a method of Iwasawa using Stickelberger elements. In the last section we saw that the profinite limit X of the p-primary part of the class group along a $\mathbb{Z}_p$-extension, is upto a finite cokernel isomorphic to,

$$X \to \prod_i \Lambda/(p^{n_i}) \oplus \prod_j \Lambda/(f_j^{m_j}).$$

Essentially this amounts to saying that $\prod_i p^{n_i} \prod_j f_j^{m_j}$ annihilates X. Recall that the Stickelberger element for the field K_n annihilates the class group. The question naturally arises about the relationship of the Stickelberger elements along a $\mathbb{Z}_p$-tower of fields, and the annihilator obtained above. The limit of the Stickelberger elements taken along a $\mathbb{Z}_p$-extension can be seen to belong to the Iwasawa algebra, and the analytic function associated to this formal power series turns out to be the p-adic L-function constructed by Kubota and Leopoldt. Roughly, the Main conjecture of Iwasawa theory says that these two methods give raise to same element in the Iwasawa algebra upto a unit, thus expressing the characteristic function of X as a p-adic L-function, in analogy with the Weil conjectures for curves.

4.1. Preliminaries. Let $\bar{\mathbb{Q}}_p$ be an algebraic closure of the field $\mathbb{Q}_p$. The natural valuation $|\ |$ on $\mathbb{Q}_p$ extends to a valuation on $\bar{\mathbb{Q}}_p$, which is no longer discrete. We normalise the valuation by fixing $|p| = 1/p$. The field $\bar{\mathbb{Q}}_p$ is no longer complete with respect to this valuation. Denote by $\mathbb{C}_p$ the completion of $\bar{\mathbb{Q}}_p$ with respect to this valuation. The absolute value extends to $\mathbb{C}_p$, and $\mathbb{C}_p$ is complete, algebraically closed. This is the analogue of the complex numbers. In fact, it can be seen that as abstract fields $\mathbb{C}_p$ and $\mathbb{C}$ are isomorphic. Fix an embedding of $\bar{Q}$ into $\mathbb{C}_p$, where $\mathbb{C}_p$ is an algebraic closure of the field $\mathbb{Q}_p$. With this we can think of Dirichlet characters as having values in $\mathbb{C}_p$. We remark however that the use of $\mathbb{C}_p$ is more for convenience, and we could have as well worked with the locally compact field $\mathbb{Q}_p(\chi)$, obtained by adjoining the values of χ.

We recall the definition of the Teichmuller character ω defined on $\mathbb{Z}_p^*$. Let $q = p$ if p is odd, and $q = 4$ if $p = 2$. ω is the unique character ω on $\mathbb{Z}_p^*$ with values in the $(p-1)$th roots of unity if p is odd, and values in $\{\pm 1\}$ if $p = 2$, satisfying the following congruence:

$$\omega(a) \equiv a \pmod{p}.$$

It can be seen that $\omega(a)$ is also equal to $\lim_{n\to\infty} a^{p^n}$. Define

$$< a >= \omega(a)^{-1}a.$$

Let N be the conductor of χ. The generalised Bernoulli numbers are defined by the series,

$$\sum_{a=1}^{N} \frac{\chi(a)te^{at}}{e^{Nt}-1} = \sum_{n=0}^{\infty} B_{n,\chi}\frac{t^n}{n}.$$

The Dirichlet L-functions associated $L(s,\chi)$ admit an analytic continuation to the entire complex plane, and the values at the negative integers are given by the Bernoulli numbers,

$$L(1-n,\chi) = -\frac{B_{n,\chi}}{n}, \quad n \geq 1.$$

For any integer $k,\ n \geq 0$, define

$$S_{n,\chi}(k) = \sum_{a=1}^{k} \chi(a)a^n. \tag{4.1.1}$$

An important property of the Bernoulli numbers we will need is the following:

Lemma 4.1.1. *In $\mathbb{C}_p$,*

$$B_{n,\chi} = \lim_{k\to\infty}\frac{1}{p^kN}S_{n,\chi}(p^kN) = \lim_{k\to\infty}\frac{1}{p^kN}\sum_{a=1}^{p^kN}\chi(a)a^n.$$

For a proof of this lemma, we refer to Iwasawa's book. Let $q = p$ if p is odd, and $q = 4$ if $p = 2$. We recall the following theorem:

THEOREM 4.1.1. *There exists a p-adic meromorphic function $L_p(s, \chi)$ defined in the domain $D = \{s \in \mathbb{C}_p \mid |s| < qp^{-1/(p-1)}\}$ satisfying the following:*

a) $L_p(s, \chi)$ is given by

$$L_p(s, \chi) = \frac{a_{-1}}{s-1} + \sum_{n=0}^{\infty} a_n (s-1)^n, \quad a_n \in \mathbb{Q}_p(\chi),$$

where $a_{-1} = 1 - 1/p$ if χ is the trivial character, and 0 otherwise.

$$\begin{aligned}(b)\ L_p(1-n, \chi) &= -(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n} \\ &= (1 - \chi\omega^{-n}(p)p^{n-1})L(1-n, \chi\omega^{-n}), \quad n \geq 1.\end{aligned}$$

Further as a p-adic meromorphic function on the domain D, $L_p(s, \chi)$ is uniquely characterised by the above properties.

In particular, let χ be an odd Dirichlet character, i.e., $\chi(-1) = -1$. It can be seen from properties of Bernoulli numbers, that for $n \equiv \pmod{\phi(q)}$, $B_{n,\chi} = 0$. Hence it follows that $L_p(s, \chi)$ is identically 0 if χ is an odd Dirichlet character.

4.2. Write the conductor of χ as dp^j, $(d, p) = 1$, for some $j \geq 0$. Let $q_n = dqp^n$, $n \geq 0$. Let

$$K_n = \mathbb{Q}(\zeta_{q_n}), \quad n \geq 0.$$

By the Kronecker-Weber theorem, we see that χ can be considered as a character of the Galois group $G(K_n/\mathbb{Q})$ of the field K_n over $\mathbb{Q}$. We have the exact sequence,

$$1 \to G(K_n/K_0) \to G(K_n/\mathbb{Q}) \to G(K_0/\mathbb{Q}) \to 1.$$

This exact sequence splits giving an idenitification

$$G(K_n/\mathbb{Q}) \simeq \Delta \times \Gamma_n,$$

where $\Delta \simeq G(K_0/\mathbb{Q})$ and $\Gamma_n \simeq G(K_n/K_0)$. Accordingly for $a \in G(K_n/\mathbb{Q})$, let $\delta(a) \in \Delta$ and $\gamma_n(a) \in \Gamma_n$ denote respectively the components with respect to the above decomposition. Note that $G(K_n/\mathbb{Q})$ can be identified with $(\mathbb{Z}/q_n\mathbb{Z})^* \simeq (\mathbb{Z}/q_0\mathbb{Z})^* \times \mathbb{Z}/p^n\mathbb{Z}$, where $q_n = m_0qp^n$, $(m_0, p) = 1$, $q = p$ if p is odd and $q = 4$ if $p = 2$. Then $\Delta \simeq (\mathbb{Z}/q_0\mathbb{Z})^*$ and $\Gamma_n \simeq \mathbb{Z}/p^n\mathbb{Z}$.

Write $\chi = \theta\psi$ accordingly, where θ is a character of Δ and ψ is a character of Γ_n. θ and ψ is called a character of the first kind, and ψ a character of the second kind. Note that θ is an unramified character, and that ψ is a even character of p-power order. Let $\mathcal{O}_\theta$ be the ring of integers in the field $\mathbb{Q}_p(\theta)$. The main theorem is the following:

THEOREM 4.2.1. *Let χ be an even character. There exists formal power series $f(T,\theta)$(if $\theta \neq 1$), $g(T,\theta)$, $h(T,\theta) \in \mathcal{O}_\theta[[T]]$, with*

$$h(T,\theta) = 1 - (1+q_0)/(1+T), \text{ and}$$

$$f(T,\theta) = \frac{g(T,\theta)}{h(T,\theta)}, \quad \theta \neq 1.$$

If $\theta = 1$, we take the above as the definition of $f(T,\theta)$ formally in the quotient field of $\mathcal{O}_\theta[[T]]$. Moreover in the domain D defined above,

$$L_p(s,\chi) = f(\psi(1+q_0)^{-1}(1+q_0)^s - 1, \theta).$$

There are a number of remarks to be made to clarify the above theorem.

REMARK. For $x \in \mathbb{C}_p$, define the exponential function,

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

It can be shown that this series converges absolutely in the region $|x| < p^{-1/(p-1)}$. Similarly define the logarithm function in the domain $\{x \in \mathbb{C}_p \mid |1-x| < 1\}$ by the series,

$$\log_p(1-x) = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

It can be shown that the above definition of $\log_p(x)$ can be extended uniquely to a continuous function on $\mathbb{C}_p^*$ such that $\log_p(p) = 0$. With this define,

$$(1+q_0)^s = \exp(s\log_p(1+q_0)).$$

REMARK. We have $|\log_p(1+q_0)| = |q_0|$. Thus for $s \in D$,

$$|(1+q_0)^s - 1| = |\exp(s\log_p(1+q_0)| < 1.$$

Since ψ of order a power of p, $\psi(1+q_0)$ is of p-power order, and so $|\psi(1+q_0)^{-1}(1+q_0)^s - 1| < 1$. Hence on substituting for $T = \psi(1+q_0)^{-1}(1+q_0)^s - 1$, in a power series with coefficients in $\mathcal{O}_\theta$, the series converges and defines an analytic function on D. Moreover the only possible zero for $h(T,\theta)$ is when $T = q_0$, equivalently when $s = 1$ and $\psi(1+q_0) = 1$. As $(1+q_0)$ is a generator for Γ, this implies ψ is trivial, and χ is an even character of the first kind. $L_p(s,\chi)$ is analytic except at $s = 1$, where it has a simple pole.

4.3. We will give an outline of the construction of the formal power series occurring in the theorem. In virtue of Theorem 4.1.1, and the above remark, it suffices to check that the values at the points $s = 1 - n$, n a rational integer satisfy (b) of Theorem 4.1.1.

Let χ be an even character, and let $\chi = \theta\psi$ be the decomposition as characters of the first and second kind respectively. Let $\theta^* = \theta\omega^{-1}$. Since ψ is an even character, θ will be even, and θ^* an odd character. Let

$$S_n = \{a \mid 0 < a < q_n, (a, q_0) = 1\}.$$

Define $\xi_n(\theta),\ \eta_n(\theta) \in K_\theta[\Gamma_n]$, elements in the group ring of Γ_n as,

$$\xi_n(\theta) = -\frac{1}{q_n}\sum_{a \in S_n} a\theta^*(a)\gamma_n(a)^{-1}$$

$$\text{and } \eta_n(\theta) = (1 - (1 + q_0)\gamma_n(1 + q_0)^{-1})\xi_n(\theta).$$

Remark. Recall that upto a sign, the Stickelberger element ψ_n of K_n is,

$$\psi_n = -\frac{1}{q_n}\sum_{a \in S_n} a\delta(a)^{-1}\gamma_n(a)^{-1}.$$

$\xi_n(\theta)$ is then the projection of the Stickelberger element to the group ring $K_\theta[\Gamma_n]$ of Γ_n, with respect to the idempotent $\frac{1}{|\Delta|}\sum_{\delta\in\Delta}\theta^*(\delta)^{-1}\delta^{-1}$.

Proposition 4.3.1. *a) If $m \geq n \geq 0$, then $\xi_m(\theta) \mapsto \xi_n(\theta)$ and $\eta_m(\theta) \mapsto \eta_n(\theta)$, with respect to the map $K_\theta[\Gamma_m] \to K_\theta[\Gamma_n]$, induced by the projection map from Γ_m to Γ_n.*

b) $\frac{1}{2}\eta_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$.

c) If $\theta \neq 1$, then $\frac{1}{2}\xi_n(\theta) \in \mathcal{O}_\theta[\Gamma_n]$.

Proof. We outline a proof when p is assumed to be a odd prime.

a) Write $a \in S_{n+1}$ as $a = b + iq_n,\ b \in S_n,\ 0 < i < p$. Denote by ξ_n' the image of ξ_{n+1} in $K_\theta[\Gamma_n]$, with respect to the projection map $\Gamma_{n+1} \to \Gamma_n$. Then $\gamma_{n+1}(a) \mapsto \gamma_n(b)$ and $\theta^*(a) = \theta^*(b)$. We have,

$$\begin{aligned} \xi_n(\theta)' &= \xi_n(\theta) - \frac{1}{q_{n+1}}\sum_{0<i<p}\sum_{b\in S_n} iq_n\theta^*(b)\gamma_n(b)^{-1} \\ &= \xi_n(\theta) - \frac{p-1}{2}\sum_{b\in S_n}\theta^*(b)\gamma_n(b)^{-1}. \end{aligned} \tag{4.3.1}$$

Let $S_n' = \{a \mid a \in S_n,\ a < q_n/2\}$. Since θ^* is odd and γ_n is even, we get

$$\begin{aligned} \sum_{b\in S_n}\theta^*(b)\gamma_n(b)^{-1} &= \sum_{b\in S_n'}\theta^*(b)\gamma_n(b)^{-1} + \sum_{b\in S_n'}\theta^*(q_n - b)\gamma_n(q_n - b)^{-1} \\ &= 0. \end{aligned} \tag{4.3.2}$$

b)

$$\eta_n(\theta) = \xi_n(\theta) + \frac{1}{q_n} \sum_{a \in S_n} (1+q_0)a\theta^*(a)\gamma_n((1+q_0)a)^{-1}.$$

Write $(1+q_0)a = a' + a''q_n,\ 0 \le a' \le q_n$. Then $\omega((1+q_0)a) = \omega(a'),\ \theta((1+q_0)a) = \theta(a')$ and $\gamma_n((1+q_0)a) = \gamma_n(a')$. Further as a ranges over elements of S_n, so does a'. Hence it follows,

$$\eta_n(\theta) = \sum_{a \in S_n} a''\theta^*(a')\gamma_n(a')^{-1}. \tag{4.3.3}$$

c)

$$\xi_n(\theta) = -\frac{1}{q_n} \sum_{a \in S'_n} a\theta^*(a)\gamma_n(a)^{-1} + -\frac{1}{q_n} \sum_{a \in S'_n} (q_n - a)\theta^*(q_n - a)\gamma_n(q_n - a)^{-1}.$$

Since $\theta^*(q_n - a) = -\theta^*(a)$ and $\gamma_n(q_n - a) = \gamma_n(a)$, we have,

$$\xi_n(\theta) = -\frac{2}{q_n} \sum_{a \in S'_n} a\theta^*(a)\gamma_n(a)^{-1} + \sum_{a \in S'_n} \theta^*(a)\gamma_n(a)^{-1}.$$

Fix a_0 coprime to q_0. It can be from the definition of ω and of γ_n, that $\gamma_n(a) = \gamma_n(b)$ if and only if $\omega(a)^{-1}a \equiv \omega(b)^{-1}b \mod q_n$. Hence $\mod q_n$ we have,

(4.3.4)
$$\sum_{\substack{a \in S'_n \\ \gamma_n(a) = \gamma_n(a_0)}} a\omega(a)^{-1}\theta(a)\gamma_n(a)^{-1} = a_0\omega(a_0)^{-1}\gamma_n(a_0) \sum_{\substack{a \in S'_n \\ \gamma_n(a) = \gamma_n(a_0)}} \theta(a).$$

Now as a ranges over the indexing set in the above equation, it can be seen that the projection of a to Δ ranges over all the elements of Δ. Since θ is a non-principal character, this sum vanishes. □

Proof of the theorem. A slight extension of the isomorphism of the last section provides an identification of the group ring $\mathcal{O}_\theta[\Gamma] \simeq T\mathcal{O}_\theta[[T]]$. Let u be a generator of Γ. We recall that this identification is obtained by sending the generator u to $1+T$. Note that in the particular example we had, we could have taken $\gamma(1+q_0)$ as an explicit generator for Γ.

Via this identification, the proposition implies the existence of formal power series $f(T,\theta)$ (if $\theta \neq 1$), $g(T,\theta) \in \mathcal{O}_\theta[[T]]$ as,

$$f(T,\theta) = lim_{\overleftarrow{n}}\, \xi_n(\theta), \text{if } \theta \neq 1, \tag{4.3.5}$$

$$\text{and } g(T,\theta) = lim_{\leftarrow n}\xi_n(\theta), \text{if } \theta \neq 1. \tag{4.3.6}$$

In view of the theorem 4.1.1, we need to understand at the level of group rings, the effect on substituting $T = \zeta_\psi(1+q_0)^{1-m} - 1$, where m is a natural number. Define for n sufficiently large depending on the conductor of ψ and for a fixed integer t,

$$\phi^{\psi}_{m,n} : \mathcal{O}_\theta[\Gamma_n] \to \mathcal{O}_\theta/q_n\mathcal{O}_\theta$$

such that

$$\gamma_n(a) \mapsto \psi(a)^{-1} < a >^{-t}, \ a \in \mathbb{Z}, \ (a, q_0) = 1.$$

For n varying the various maps patch together to give a morphism of $\mathcal{O}_\theta$-algebras $\phi_t : \mathcal{O}_\theta[\Gamma] \to \mathcal{O}_\theta$.

LEMMA 4.3.1. *Let $\xi \in \mathcal{O}_\theta[\Gamma]$ correspond to $f(T) \in \mathcal{O}_\theta[[T]]$ via the above isomorphism. Then*

$$\phi^{\psi}_t(\xi) = f(\psi(1+q_0)^{-1}(1+q_0)^{-t} - 1).$$

PROOF. Assume first that $f(T) = 1 + T$. Then $\xi = \gamma(1+q_0)$ and hence,

$$\phi_t(\gamma(1+q_0)) = \psi(1+q_0)^{-1}(1+q_0)^{-t} = f(\psi(1+q_0)^{-1}(1+q_0)^{-t} - 1).$$

The lemma now follows for all polynomials and hence for any f. □

In view of the above remarks, it suffices in order to prove the theorem to show that for any integer $m \geq 1$

$$g(\zeta_\psi(1+q_0)^{1-m} - 1, \theta)$$
$$= -h(\zeta_\psi(1+q_0)^{1-m} - 1, \theta)(1 - \chi\omega^{-m}(p)p^{m-1})B_{m,\chi\omega^{-m}}.$$

Applying $\phi_{t,n}$ to both sides of 4.3.3,

$$\phi_{t,n}(\eta_n) = \sum a''\chi_{t+1}(a')(a')^t \pmod{q}_n\mathcal{O}_\theta,$$

where $\chi_{t+1} = \chi\omega^{-t-1}$. From this it follows that,

$$(t+1)\phi_{t,n}(\eta_n) = -(1-\chi(1+q_0)(1+q_0)^{t+1})\frac{1}{q_n}\sum_a \chi_{t+1}(a)a^{t+1} \pmod{q}_n\mathcal{O}_\theta.$$

Hence,

$$(t+1)\phi_t(\eta_n) = -(1-\chi(1+q_0)(1+q_0)^{t+1})\lim\frac{1}{q_n}\sum_a \chi_{t+1}(a)a^{t+1}.$$

It follows from the identification of $g(T,\theta)$ with $\lim\phi_t(\eta_n)$ that,

$$f(\chi(1+q_0)(1+q_0)^{-t} - 1, \theta) = -\frac{1}{t+1}\lim\frac{1}{q_n}\sum_a \chi_{t+1}(a)a^{t+1}.$$

We break the above sum into two parts, one indexed by a coprime to p, and the other by $p|a$, to obtain

$$\sum_a \chi_{t+1}(a)a^{t+1} = S_{t+1,\chi_{t+1}}(q_n) - \chi_{t+1}(p)p^{t+1}S_{t+1,\chi_{t+1}}(q_{n-1}),$$

with $S_{n,\chi}$ defined as in 4.1.1. It follows from Lemma 4.1.1 upon substituting $m = t + 1 \geq 1$,

$$f(\chi(1+q_0)(1+q_0)^{1-m} - 1, \theta) = -(1 - \chi_m(p)p^{m-1}\frac{B_{m,\chi\omega^{-m}}}{m}.$$

This gives an outline of the proof of the theorem, and for more details we refer the reader to the books by Iwasawa and Washington.

5. Main conjecture

In analogy with the Weil conjectures, it is natural to ask whether the characteristic function of the pro p-part of the class group X of a $\mathbb{Z}_p$ extension, considered in Section 2, is of zeta type. Note that this characteristic function is well defined upto a unit in the Iwasawa algebra. We have also seen, that the Stickelberger elements patch together along a cyclotomic $\mathbb{Z}_p$-extension, and gives rise to a power series, which interpolates the special values of Dirichlet L-series. The Main conjecture is indeed the expectation that these two power series should be equal upto a unit in the Iwasawa algebra.

Let $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$, and θ be an odd character of $\Delta \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Let X_n denote the Galois group of the maximal abelian p-extension Ω_n of K_n, unramified outside of the prime above p, and X be the profinite limit $X = \lim_{\leftarrow[n]} X_n$. The Iwasawa algebra,

$$\Lambda = \mathbb{Z}_p[\Gamma] = \lim_{\leftarrow} \mathbb{Z}_p[\Gamma_n] \simeq \mathbb{Z}_p[[T]].$$

For any character χ of Δ, denote by ϵ_χ the projector in the group ring $\mathbb{Z}_p[\Delta]$,

$$\epsilon_\chi = \frac{1}{(p-1)} \sum_{\delta \in \Delta} \chi^{-1}(\delta)\delta.$$

As seen in section 2, there is a map of Λ-modules,

$$\epsilon_\chi X \to \oplus_i \left(\Lambda/(p^{n_i(\chi)})\right) \oplus \left(\oplus_j \Lambda/(g_j(T,\chi)^{m_j})\right),$$

with finite cokernel. We denote by,

$$\mathrm{char}(X(\chi)) = \prod_i p^{n_i} \oplus \prod_j g_j(T,\chi)^{m_j},$$

the characteristic function of X as a Λ-module. $g(T,\chi)$ is well defined only upto a unit in Λ.

In the last section we had constructed $f(T,\chi) \in \Lambda$ satisfying for any natural number $m \geq 1$,

$$f(\psi(1+q_0)^{-1}(1+q_0)^{1-m} - 1, \chi) = L(1-m, \chi) =$$
$$-(1 - \chi\omega^{-n}(p)p^{n-1})\frac{B_{n,\chi\omega^{-n}}}{n}.$$

We can now state a form of Iwasawa's main conjecture, which has been proved by Mazur and Wiles.

THEOREM 5.0.2 (Main conjecture of Iwasawa theory). *For all nontrivial even characters χ of Δ,*

$$\operatorname{char}(X(\chi)) = f(T, \chi)\Lambda.$$

REFERENCES

(1) Ireland, K. and Rosen, M., A classical introduction to modern number theory, Graduate Texts in Math., Springer-Verlag.

(2) Iwasawa, K., Lectures on p-adic L-functions, Annals of Math. Studies **74**, Princeton University Press, Princeton.

(3) Lang, S., Cyclotomic fields, Graduate Texts in Math., Springer-Verlag.

(4) Washington, L.C., Introduction to Cyclotomic Fields, Graduate Texts in Math., **83**, Springer-Verlag.

(5) Weil, A., Number of solutions of equations in finite fields, Collected Papers I, 399-410.

C. S. Rajan
School of Mathematics
Tata Institute of Fundamental Research
Homi Bhabha Road, Mumbai 400 005, India.
e-mail: rajan@math.tifr.res.in