

to Kolyvagin, Rubin and Thaine. Not only does this treatment have the advantage of using less machinery, but it also gives for example, a very simple proof of the existence of the p -adic analogue of the Riemann zeta function.

If one looks at the past evolution of algebraic number theory, there has been a tendency to discover that the ideas which initially seem special to cyclotomic fields do, in the end, turn out to have very general counterparts. To quote Iwasawa [Iw1]:

"The theory of cyclotomic fields is in a unique position in algebraic number theory. On the one hand, it has provided us with a typical example of algebraic number fields from which we have been able to develop the theory of algebraic number fields in general; and on the other hand, it has also revealed to us many beautiful properties of the cyclotomic fields which are proper to these fields and which give us deep insights into important arithmetic results in elementary number theory."

Already, it is known that the ideas discussed in this book work in some measure for elliptic curves over certain abelian p -adic Lie extensions, both for curves with complex multiplication ([CW2], [Ru], [Y]) and without complex multiplication ([Ka2], [SU]). It does not seem unreasonable to hope that this may turn out to be true in much greater generality, perhaps even in the direction of the non-abelian main conjecture made in [CFKSV].

Finally, we thank Karl Rubin for his very helpful comments on the manuscript.

Contents

Preface	V
Notation	IX
1 Cyclotomic Fields	1
1.1 Introduction	1
1.2 Herbrand-Ribet Theorem	3
1.3 The Cyclotomic Tower	4
1.4 The Main Conjecture	6
1.5 Iwasawa's Theorem	8
2 Local Units	13
2.1 Introduction	13
2.2 Norm and Trace Operators	15
2.3 Interpolating Power Series	17
2.4 The Logarithmic Derivative	20
2.5 An Exact Sequence	26
2.6 The Higher Logarithmic Derivative Maps	28
3 Iwasawa Algebras and p-adic Measures	33
3.1 Introduction	33
3.2 p -adic Measures	33
3.3 The Mahler Transform	36
3.4 Restriction of Measures	38
3.5 The Fundamental Exact Sequence	41
3.6 Image of δ_k	43
4 Cyclotomic Units and Iwasawa's Theorem	47
4.1 Introduction	47
4.2 p -adic Zeta Function	47

4.3	Cyclotomic Units	52
4.4	Iwasawa's Theorem	53
4.5	Relation to the Main Conjecture	54
4.6	Another Property of Cyclotomic Units	58
4.7	Global Units	62
4.8	Ideal Class Groups	68
5	Euler Systems	71
5.1	Introduction	71
5.2	Euler Systems	72
5.3	Values of Euler Systems	76
5.4	The Factorization Theorem	77
5.5	An Application of the Chebotarev Theorem	84
6	Main Conjecture	89
6.1	Introduction	89
6.2	The Inductive Argument	89
6.3	Proof of the Main Conjecture	98
7	Appendix	101
	References	111

Notation

General Notations

The symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ will denote the ring of integers, and the fields of rational numbers, real numbers and complex numbers, respectively. For a prime number p , we write $\mathbb{Q}_p$ for the completion of $\mathbb{Q}$ with respect to the p -adic valuation, normalized so that $|p|_p = p^{-1}$, and $\mathbb{C}_p$ for the completion of some fixed algebraic closure of $\mathbb{Q}_p$. As usual, $\mathbb{Z}_p$ will denote the ring of p -adic integers in $\mathbb{Q}_p$.

If L/F is a Galois extension of fields, we write $\text{Gal}(L/F)$ for the Galois group of L over F .

If m is an integer ≥ 1 , μ_m will denote the group of m -th roots of unity lying in some fixed algebraic closure of $\mathbb{Q}$ or $\mathbb{Q}_p$.

If R is a ring, $R^\times$ will denote the multiplicative group of units of R . If Δ is a group, and R is a commutative ring, we write $R[\Delta]$ for the group ring of Δ with coefficients in R .

Specific Notations

It may help the reader to bear in mind the following notational convention. In general, we shall use script capital Latin symbols (e.g. $\mathcal{F}$, $\mathcal{K}$, $\mathcal{U}$, ...) to denote objects associated with the field which is generated over $\mathbb{Q}$ by all p -power roots of unity, while plain capital Latin symbols (e.g. F , K , U , ...) will denote the analogous objects attached to the corresponding maximal real subfield.

We now list some of the most commonly used symbols in the text. Let n be either an integer ≥ 0 or ∞ .

$$\begin{aligned}\mathcal{F}_n &= \mathbb{Q}(\mu_{p^{n+1}}), & F_n &= \mathbb{Q}(\mu_{p^{n+1}})^+ \\ \mathcal{K}_n &= \mathbb{Q}_p(\mu_{p^{n+1}}), & K_n &= \mathbb{Q}_p(\mu_{p^{n+1}})^+ \\ \mathcal{G} &= \text{Gal}(\mathcal{F}_\infty/\mathbb{Q}), & G &= \text{Gal}(F_\infty/\mathbb{Q})\end{aligned}$$

$\mathcal{L}_n$ = maximal abelian p -extension of $\mathcal{F}_n$ unramified everywhere
 L_n = maximal abelian p -extension of F_n unramified everywhere
 $\mathcal{M}_n$ = maximal abelian p -extension of $\mathcal{F}_n$ unramified outside p
 M_n = maximal abelian p -extension of F_n unramified outside p

$$\mathcal{X}_\infty = \text{Gal}(\mathcal{M}_\infty/\mathcal{F}_\infty), \quad X_\infty = \text{Gal}(M_\infty/F_\infty) \\ \mathcal{Y}_\infty = \text{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty), \quad Y_\infty = \text{Gal}(L_\infty/F_\infty).$$

For integers n with $0 \leq n < \infty$, we define

$\mathcal{U}_n$ = group of units of $\mathcal{K}_n$
 U_n = group of units of K_n
 D_n = group of cyclotomic units of F_n
 V_n = group of units of F_n
 C_n = closure of D_n in U_n
 E_n = closure of V_n in U_n .

In the following definitions, the projective limits are taken with respect to the norm maps:-

$$\begin{aligned} \mathcal{U}_\infty &= \varprojlim \mathcal{U}_n \\ U_\infty &= \varprojlim U_n \\ C_\infty &= \varprojlim C_n \\ E_\infty &= \varprojlim E_n. \end{aligned}$$

Finally, a superscript 1 on any of these objects indicates that it has been formed with the subgroup consisting of those elements which are congruent to 1 modulo the unique prime ideal above p .

Cyclotomic Fields

1.1 Introduction

Let p be an odd prime number. We owe to Kummer the remarkable discovery that there is a connexion between the arithmetic of the field generated over $\mathbb{Q}$ by the p -th roots of unity and the values of the Riemann zeta function at the odd negative integers. This arose out of his work on Fermat's last theorem. Almost a hundred years later, Iwasawa made the equally major discovery that the p -adic analogue of the Riemann zeta function is deeply intertwined with the arithmetic of the field generated over $\mathbb{Q}$ by all p -power roots of unity. The main conjecture, which is now a theorem (first completely proved by Mazur and Wiles [MW]), is the natural final outcome of these ideas. This main conjecture is the deepest result we know about the arithmetic of cyclotomic fields. In this first chapter, we explain more fully this background, and also give the precise statement of the main conjecture towards the end of the chapter. However, all proofs will be postponed until the later chapters.

Let μ_p denote the group of p -th roots of unity, and put

$$\mathcal{F} = \mathbb{Q}(\mu_p), \quad \varpi = \text{Gal}(\mathcal{F}/\mathbb{Q}). \quad (1.1)$$

Now ϖ acts on μ_p , and thus gives an injective homomorphism

$$\theta : \varpi \hookrightarrow \text{Aut}(\mu_p) = (\mathbb{Z}/p\mathbb{Z})^\times \quad (1.2)$$

In fact, θ is an isomorphism by the irreducibility of the p -th cyclotomic polynomial. Thus the powers θ^n for $n = 1, \dots, p-1$ give all the characters of ϖ with values in $\mathbb{F}_p$. Let $\mathfrak{C}$ denote the ideal class group of $\mathcal{F}$. We stress that $\mathfrak{C}$ becomes impossible to compute numerically by naive methods once n is at all large. However, as is explained below,

we owe to Kummer the discovery of a miraculous connexion between the p -primary subgroup of $\mathfrak{C}$ and the values

$$\zeta(s) \text{ for } s = -1, -3, -5, \dots, \quad (1.3)$$

where $\zeta(s)$ is the classical complex Riemann zeta function. We recall that $\zeta(s)$ is defined by the Euler product

$$\zeta(s) = \prod_l (1 - l^{-s})^{-1} \quad (1.4)$$

for complex s with real part greater than 1, and has an analytic continuation over the whole complex plane, apart from a simple pole at $s = 1$. It has been known since Euler that the values (1.3) are rational numbers. In fact,

$$\zeta(-n) = -B_{n+1}/(n+1) \quad (n = 1, 3, 5, \dots) \quad (1.5)$$

where the Bernoulli numbers B_n are defined by the expansion

$$t/(e^t - 1) = \sum_{n=0}^{\infty} B_n t^n/n!. \quad (1.6)$$

One computes easily from these equations that

$$\zeta(-1) = -\frac{1}{12}, \quad \zeta(-3) = \frac{1}{120}, \quad \zeta(-5) = -\frac{1}{252}, \dots$$

Definition 1.1.1. We say that the prime number p is irregular if p divides the order of $\mathfrak{C}$.

The first few irregular primes are $p = 37, 59, 67, 101, 103, \dots$. It would be very difficult numerically to test whether a prime number p is irregular if we did not have the following remarkable criterion for irregularity due to Kummer.

Theorem 1.1.2. The prime p is irregular if and only if p divides the numerator of at least one of $\zeta(-1), \zeta(-3), \dots, \zeta(4-p)$.

For example, we have

$$\zeta(-11) = \frac{691}{32760}, \quad \zeta(-15) = \frac{3617}{8160},$$

and thus, thanks to Kummer's theorem, we conclude that both 691 and 3617 are irregular primes. The irregularity of 37 follows from the fact that

$$\zeta(-31) = \frac{37 \times 208360028141}{16320}.$$

We point out that the numerators and denominators of these zeta values tend to grow very rapidly. For example, the numerator of $\zeta(-179)$ has 199 digits. However, fortunately Kummer's theorem basically reduces the problem of deciding whether a prime p is irregular to a question of arithmetic modulo p , and is numerically very powerful. Indeed, using computational techniques derived from Kummer's theorem, all irregular primes up to 12,000,000 have been determined [BCEMS]. One finds that, up to this limit, the percentage of regular primes is approximately 60.61 percent, which fits remarkably well with the distribution which would occur if the numerators of the zeta values occurring in Theorem 1.1.2 were random modulo p (see the discussion after Theorem 5.17 in [Wa]).

This mysterious link given in Theorem 1.1.2 between two totally different mathematical objects, namely the ideal class group of $\mathcal{F}$ on the one hand, and the special values of the Riemann zeta function on the other, is unquestionably one of the great discoveries in number theory, whose generalization to other arithmetic situations is a major theme of modern arithmetic geometry.

We end this introduction by recalling the following remarkable congruences, which were first discovered by Kummer as part of his proof of Theorem 1.1.2, and which provide the first evidence for the existence of the p -adic analogue of $\zeta(s)$.

Theorem 1.1.3. Let n and m be odd positive integers such that $n \equiv m \not\equiv -1 \pmod{p-1}$. Then the rational numbers $\zeta(-n)$ and $\zeta(-m)$ are p -integral, and

$$\zeta(-n) \equiv \zeta(-m) \pmod{p}.$$

1.2 Herbrand-Ribet Theorem

The beginning of the deeper understanding of Kummer's criterion for irregularity comes from considering the action of the Galois group $\mathfrak{G}$ on $\mathfrak{C}$. After some work in this direction by both Kummer and Stickelberger, Herbrand considered the following specific refinement of Kummer's criterion. Let $\mathfrak{V} = \mathfrak{C}/\mathfrak{C}^p$, which is a finite dimensional vector space over the field $\mathbb{F}_p$, on which the Galois group $\mathfrak{G}$ acts in a natural fashion. This action is semi-simple, because the order of $\mathfrak{G}$ is prime to p . It is therefore natural to ask which of the characters θ^n , where $n = 1, \dots, p-1$, occur in $\mathfrak{V}$, and what is their multiplicity when they do occur? The theorem below, first established by Herbrand in one direction [He], and by Ribet [Ri] in the other, is today one of the important consequences of the main conjecture for the field $\mathcal{F}$.

Theorem 1.2.1. *Assume that n is an odd integer with $3 \leq n \leq p-2$. Then θ^n occurs in $\mathfrak{V} = \mathfrak{C}/\mathfrak{C}^p$ if and only if p divides the numerator of $\zeta(n+1-p)$.*

Note that Theorem 1.2.1 says nothing about the occurrence in $\mathfrak{V}$ of θ^n for even integers n . In fact, no prime number p has ever been found for which an even power of θ does occur in $\mathfrak{V}$, and Vandiver's conjecture asserts that no such p exists. As we shall explain later, the main conjecture itself would be an easy consequence of a theorem of Iwasawa if Vandiver's conjecture were true. However, as far as we know, the main conjecture itself implies nothing in the direction of Vandiver's conjecture. Thus it is perhaps fair to say that Vandiver's conjecture seems inaccessible in our present state of knowledge, although it has been verified for all p less than 12,000,000 in [BCEMS].

Here are some numerical examples of Theorem 1.2.1. For the irregular primes $p = 37, 59, 67, 101, 103, 131, 149$, $\mathfrak{V}$ has dimension 1 over $\mathbb{F}_p$. For the next irregular prime, namely $p = 157$, $\mathfrak{V}$ has dimension 2 over $\mathbb{F}_p$, with two distinct powers of θ occurring in it. A much more exotic example is given by $p = 12613$. In this example, $\mathfrak{V}$ has dimension 4 over $\mathbb{F}_p$, and 4 distinct powers of θ occur, namely

$$\theta^n, \text{ with } n \equiv 2077, 3213, 12111, 12305 \pmod{12612}. \quad (1.7)$$

In fact, the decomposition of $\mathfrak{V}$ into eigenspaces for the action of ϖ is completely determined for all p less than 12,000,000 in [BCEMS]. For such p , the characters which occur always have multiplicity 1, and the largest dimension of $\mathfrak{V}$ is 7.

1.3 The Cyclotomic Tower

Iwasawa's great insight was that one could go much further in explaining the above links by undertaking a seemingly more complicated study of the infinite tower of fields generated over $\mathbb{Q}$ by all p -power roots of unity. Although on the face of it, this will lead us to more elaborate and inaccessible arithmetic objects, the great benefit is that these objects are endowed with a natural action of the Galois group of the field generated over $\mathbb{Q}$ by all p -power roots of unity, which in the end can explain more easily and completely their relationship to the p -adic analogue of $\zeta(s)$.

Let n be a natural number, and write $\mu_{p^{n+1}}$ (respectively, μ_{p^∞}) for the group of all p^{n+1} -th (resp. all p -power) roots of unity in some fixed algebraic closure of $\mathbb{Q}$. We define

$$\mathcal{F}_n = \mathbb{Q}(\mu_{p^{n+1}}), \quad \mathcal{F}_\infty = \mathbb{Q}(\mu_{p^\infty}), \quad (1.8)$$

and let

$$F_n = \mathbb{Q}(\mu_{p^{n+1}})^+, \quad F_\infty = \mathbb{Q}(\mu_{p^\infty})^+ \quad (1.9)$$

be their respective maximal totally real subfields (i.e. the fixed fields of the element induced by complex conjugation in their respective Galois groups over $\mathbb{Q}$). We write

$$\mathcal{G} = \text{Gal}(\mathcal{F}_\infty/\mathbb{Q}), \quad G = \text{Gal}(F_\infty/\mathbb{Q}) \quad (1.10)$$

for the corresponding Galois groups over $\mathbb{Q}$. The action of $\mathcal{G}$ on μ_{p^∞} defines an injection

$$\chi: \mathcal{G} \longrightarrow \mathbb{Z}_p^\times = \text{Aut}(\mu_{p^\infty}) \quad (1.11)$$

which is an isomorphism by the irreducibility of the cyclotomic equation. In particular, both $\mathcal{G}$ and G are abelian. Let $\mathcal{L}_\infty$ (resp. L_∞) be the maximal abelian p -extension of $\mathcal{F}_\infty$ (resp. F_∞) which is unramified everywhere. Note that, since p is always assumed to be odd, there is never any ramification of the primes at infinity in a p -extension. Put

$$\mathcal{Y}_\infty = \text{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty), \quad Y_\infty = \text{Gal}(L_\infty/F_\infty). \quad (1.12)$$

Since $\mathcal{Y}_\infty$ (resp. Y_∞) is abelian, the Galois group $\mathcal{G}$ (resp. G) acts on it by inner automorphisms as follows. If σ is an element of $\mathcal{G}$ (resp. G), pick any lifting $\tilde{\sigma}$ to the Galois group of $\mathcal{L}_\infty$ (resp. L_∞) over $\mathbb{Q}$, and define $\sigma.y = \tilde{\sigma}y\tilde{\sigma}^{-1}$ for y in $\mathcal{Y}_\infty$ (resp. Y_∞). We remark that this is a very typical example of such a Galois action occurring in Iwasawa theory, and below we shall encounter another example of this kind.

The Iwasawa algebras of $\mathcal{G}$ and G (see Appendix) are defined by

$$\Lambda(\mathcal{G}) = \varprojlim \mathbb{Z}_p[\mathcal{G}/\mathcal{H}], \quad \Lambda(G) = \varprojlim \mathbb{Z}_p[G/H],$$

where $\mathcal{H}$ (resp. H) runs over the open subgroups of $\mathcal{G}$ (resp. G). Since $\mathcal{Y}_\infty$ (resp. Y_∞) is by construction a compact $\mathbb{Z}_p$ -module, the $\mathcal{G}$ -action (resp. G -action) on it extends by continuity and linearity to an action of the whole Iwasawa algebra $\Lambda(\mathcal{G})$ (resp. $\Lambda(G)$) (see Appendix). Standard arguments in Iwasawa theory show that $\mathcal{Y}_\infty$ (resp. Y_∞) is a finitely generated torsion module over $\Lambda(\mathcal{G})$ (resp. $\Lambda(G)$).

We digress briefly here to point out that the two Iwasawa modules $\mathcal{Y}_\infty$ and Y_∞ have a very different nature arithmetically. In fact, $Y_\infty = 0$ if Vandiver's conjecture is true for p (and hence, in particular, for all $p < 12,000,000$). However, $\mathcal{Y}_\infty$ has positive $\mathbb{Z}_p$ -rank precisely when

the prime p is irregular. In addition, an important theorem of Ferrero-Washington [Fe-W] shows that both $\mathcal{Y}_\infty$ and Y_∞ are always finitely generated $\mathbb{Z}_p$ -modules. Let $\mathcal{J} = \{1, \iota\}$ be the subgroup of $\mathcal{G}$ fixing F_∞ . Since p is odd, there is a decomposition

$$\mathcal{Y}_\infty = \mathcal{Y}_\infty^+ \oplus \mathcal{Y}_\infty^- \quad (1.13)$$

as $\Lambda(\mathcal{G})$ -modules, where the complex conjugation ι acts on the first direct summand by $+1$ and on the second by -1 . In fact, it is easily seen that the natural surjection from $\mathcal{Y}_\infty$ onto Y_∞ induces an isomorphism from $\mathcal{Y}_\infty^+$ onto Y_∞ . Even after taking this decomposition, the discrepancies between these two modules continue. For example, it is known that $\mathcal{Y}_\infty^-$ is a free finitely generated $\mathbb{Z}_p$ -module. On the other hand, it is an important unsolved problem about the tower of fields $\mathcal{F}_\infty$, whether or not Y_∞ has any non-zero finite submodule which is stable under the action of G . In fact, as we shall see in Chapters 4 and 6, the maximal finite G -submodule of Y_∞ plays an important role in the completion of the proof of the main conjecture using Euler systems. One of the beauties of the main conjecture is that it can be proven for all p , irrespective of knowing the answers to these finer questions.

1.4 The Main Conjecture

The main conjecture could in fact be stated in terms of the $\Lambda(\mathcal{G})$ -module $\mathcal{Y}_\infty^-$ of the previous section. However, because of the method of proof that we shall follow, it is more natural to work with an equivalent version in terms of a different Iwasawa module. For this reason, we consider larger abelian extensions of the fields $\mathcal{F}_\infty$ and F_∞ . Let $\mathcal{M}_\infty$ (resp. M_∞) be the maximal abelian p -extension of $\mathcal{F}_\infty$ (resp. F_∞) which is unramified outside the unique prime above p in $\mathcal{F}_\infty$ (resp. F_∞). We write

$$\mathcal{X}_\infty = \text{Gal}(\mathcal{M}_\infty/\mathcal{F}_\infty), \quad X_\infty = \text{Gal}(M_\infty/F_\infty). \quad (1.14)$$

In an entirely similar manner to that described earlier, $\mathcal{G}$ (resp. G) acts on $\mathcal{X}_\infty$ (resp. X_∞) via inner automorphisms, making it a module over $\Lambda(\mathcal{G})$ (resp. over $\Lambda(G)$). While both these modules are finitely generated over the respective Iwasawa algebras, the module $\mathcal{X}_\infty$ is not $\Lambda(\mathcal{G})$ -torsion whereas X_∞ is $\Lambda(G)$ -torsion by the following important theorem due to Iwasawa [Iw4].

Theorem 1.4.1. *The module X_∞ is a finitely generated torsion $\Lambda(G)$ -module.*

Before stating the Main Conjecture, whose formulation requires some results from the structure theory of $\Lambda(G)$ -modules, it is perhaps interesting to again digress and note (although neither fact is needed for the version given below), that the theorem of Ferrero-Washington [Fe-W] implies that X_∞ is a finitely generated $\mathbb{Z}_p$ -module, and that a theorem of Iwasawa [Iw4] implies that X_∞ has no non-zero $\mathbb{Z}_p$ -torsion (see Proposition 4.7.2). Thus X_∞ is a free finitely generated $\mathbb{Z}_p$ -module, on which the group G , which is topologically generated by one element, is acting continuously. One could then take the characteristic polynomial of some topological generator of G acting on X_∞ as a generator of the characteristic ideal of X_∞ . However, we shall work without assuming these stronger results, and simply recall that the structure theory of finitely generated torsion $\Lambda(G)$ -modules (see Appendix) implies that for each such module N , there is an exact sequence of $\Lambda(G)$ -modules

$$0 \longrightarrow \bigoplus_{i=1}^r \frac{\Lambda(G)}{\Lambda(G)f_i} \longrightarrow N \longrightarrow D \longrightarrow 0,$$

where f_i ($i = 1, \dots, r$) is a non-zero divisor, and D is finite. Then the characteristic ideal of N , which we denote by $\text{ch}_G(N)$, is defined to be the ideal of $\Lambda(G)$ generated by the product $f_1 \dots f_r$.

It is at first utterly surprising that, as we now explain, there is a generator of $\text{ch}_G(X_\infty)$ which is intimately related to the Riemann zeta function. We owe to Kubota-Leopoldt [KL] the first proof that a p -adic analogue of $\zeta(s)$ exists. Iwasawa then discovered [Iw3] that this p -adic analogue, which we denote by ζ_p , has a natural interpretation in terms of the Iwasawa algebra $\Lambda(G)$. As will be shown in Chapter 3, the elements of $\Lambda(G)$ can be viewed as $\mathbb{Z}_p$ -valued measures on the Galois group G . To take account of the fact that ζ_p has, like the Riemann zeta function, a simple pole, one defines a pseudo-measure on G to be any element μ of the ring of fractions of $\Lambda(G)$ such that $(g-1)\mu$ belongs to $\Lambda(G)$ for all g in G (see §3.2). The integral

$$\int_G \nu d\mu$$

of any non-trivial continuous homomorphism $\nu : G \rightarrow \mathbb{Z}_p^\times$ against a pseudo-measure μ is then well-defined.

Theorem 1.4.2. *There exists a unique pseudo-measure ζ_p on G such that*

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1-k)$$

for all even integers $k \geq 2$.

As hinted at above, ζ_p has a simple pole at the trivial character, with residue $1 - p^{-1}$, in the following sense. Write κ for the composition of the cyclotomic character χ with the natural projection from $\mathbb{Z}_p^\times$ to the multiplicative group $1 + p\mathbb{Z}_p$. It is clear that κ factors through G , and that it makes sense to raise it to any power in $\mathbb{Z}_p$. Then it can be shown that, if s is an element of $\mathbb{Z}_p$ distinct from 1, we have an expansion of the form

$$\int_G \kappa^{1-s} d\zeta_p = (1 - p^{-1})(s - 1)^{-1} + a_0 + a_1(s - 1) + \cdots,$$

where $a_0, a_1, \dots$ are elements of $\mathbb{Z}_p$. This is closely related to the classical von-Staudt-Clausen theorem on Bernoulli numbers.

Let $I(G)$ denote the kernel of the augmentation homomorphism from $\Lambda(G)$ to $\mathbb{Z}_p$. As ζ_p is a pseudo-measure, $I(G)\zeta_p$ is an ideal of $\Lambda(G)$.

Theorem 1.4.3. (Main Conjecture) *We have*

$$\text{ch}_G(X_\infty) = I(G)\zeta_p.$$

The first complete proof was given by Mazur-Wiles [MW] using the arithmetic of modular curves. A second proof, based on the generalization of Ribet's proof of Theorem 1.2.1, was given by Wiles [W]. The goal of this book is to give what is probably the simplest proof of this theorem, which proceeds along the following lines. We first establish Iwasawa's theorem (see the next section) for a $\Lambda(G)$ -module closely related to X_∞ , and then use arguments from Euler systems due to Kolyagin, Rubin and Thaine [Ko], [Ru3], [Th], to show that the discrepancy between these two modules does not alter their characteristic ideals. In fact, this discrepancy is zero for all known numerical examples, including all $p < 12,000,000$.

1.5 Iwasawa's Theorem

The genesis of the main conjecture is Iwasawa's paper [Iw2], and his important theorem below arises from combining the results of this paper with his construction of ζ_p in [Iw3]. For each $n \geq 0$, consider now the local field

$$K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+ \quad (1.15)$$

We write U_n^1 for the group of units of K_n , which are $\equiv 1 \pmod{p_n}$, where p_n is the maximal ideal of the ring of integers of K_n . Let D_n be the group of cyclotomic units of F_n . Thus D_n is generated by all Galois conjugates of

$$\pm \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}}$$

where ζ_n denotes a primitive p^{n+1} -th root of unity, and e is a primitive root modulo p such that $e^{p-1} \not\equiv 1 \pmod{p^2}$. We define D_n^1 to be the subgroup of all elements of D_n which are $\equiv 1 \pmod{p_n}$. Finally, let

$$C_n^1 = \overline{D}_n^1$$

be the closure of D_n^1 in U_n^1 with respect to the p_n -adic topology. Define

$$U_\infty^1 = \varprojlim U_n^1, \quad C_\infty^1 = \varprojlim C_n^1, \quad (1.16)$$

where the projective limits are taken with respect to the norm maps. Of course, the group G acts continuously on both these $\mathbb{Z}_p$ -modules, endowing them with an action of $\Lambda(G)$. Iwasawa's theorem is the following:-

Theorem 1.5.1. *The $\Lambda(G)$ -module U_∞^1/C_∞^1 is canonically isomorphic to $\Lambda(G)/I(G) \cdot \zeta_p$, where ζ_p is the p -adic zeta function, and $I(G)$ is the augmentation ideal.*

We shall give a very elementary proof of this theorem, different from Iwasawa's (see Theorem 4.4.1), which does not even use local class field theory. This proof was discovered by Wiles and one of us [CW2] when studying the analogous theorem for elliptic curves with complex multiplication. However, we follow Coleman's beautiful proof [Co] of the existence of the interpolating power series lying behind this approach, rather than using the ad hoc method of [CW2].

The comparison between the Galois group X_∞ and the module U_∞^1/C_∞^1 is provided by class field theory. Let V_n^1 be the group of units of the ring of integers of F_n which are $\equiv 1 \pmod{p_n}$, and define

$$E_n^1 = V_n^1, \quad E_\infty^1 = \varprojlim E_n^1 \quad (1.17)$$

where the closure in U_n^1 is again taken with respect to the p -adic topology and the projective limit is taken with respect to the norm maps. As we explain in more detail in § 4.5, the Artin map of global class field theory gives a canonical $\Lambda(G)$ -isomorphism

$$\text{Gal}(M_\infty/L_\infty) \simeq U_\infty^1/E_\infty^1.$$

Thus we have the four term exact sequence of $\Lambda(G)$ -modules

$$0 \longrightarrow E_\infty^1/C_\infty^1 \longrightarrow U_\infty^1/C_\infty^1 \longrightarrow X_\infty \longrightarrow Y_\infty \longrightarrow 0, \quad (1.18)$$

all of which are finitely generated torsion modules. But the characteristic ideal is multiplicative in exact sequences (see Appendix). Hence, granted Iwasawa's theorem, we have the following result.

Proposition 1.5.2. *The main conjecture is true if and only if $\text{ch}_G(Y_\infty) = \text{ch}_G(E_\infty^1/C_\infty^1)$.*

Of course, this last proposition does not involve the p -adic zeta function ζ_p , and is only of real interest when combined with Iwasawa's theorem via the exact sequence (1.18). The proof of Proposition 1.5.2 using Euler systems is given in Chapters 4 and 5, and broadly follows Rubin's generalization of the method discovered by Kolyvagin and Thaine. It is striking that this proof largely uses ideas already known to Kummer, combined with global class field theory.

We end this chapter by making some brief remarks about applications of the main conjecture. However, we omit detailed proofs in this book because these applications are dealt with rather fully in the literature, and also because some of them involve higher K -theory.

We first explain why Kummer's criterion for irregularity is a consequence of the main conjecture. Using an important result of Iwasawa (see Proposition 4.7.2), which asserts that X_∞ has no non-zero finite $\Lambda(G)$ -submodule, it follows easily from the main conjecture and the structure theory of finitely generated torsion $\Lambda(G)$ -modules (see Appendix), that

$$I(G)\zeta_p = \Lambda(G) \quad (1.19)$$

if and only if

$$X_\infty = 0. \quad (1.20)$$

However, we claim that (1.19) is equivalent to the assertion that all of the values

$$\zeta(-1), \zeta(-3), \dots, \zeta(4-p) \quad (1.21)$$

are p -adic units. Indeed, as is explained in the Appendix (see (A2)), for any finitely generated torsion $\Lambda(G)$ -module M , we have a decomposition

$$M = \bigoplus_{i \bmod \frac{p-1}{2}} M^{(i)},$$

where $M^{(i)}$ denotes the submodule of M on which $G(F_0/\mathbb{Q})$ acts via θ^{2i} . As was mentioned earlier (see the discussion after Theorem 1.4.2), ζ_p has a simple pole with residue $1 - p^{-1}$ at the trivial character, from which it follows easily that

$$(I(G)\zeta_p)^{(0)} = \Lambda(G)^{(0)}.$$

On the other hand, taking i to be any of $1, \dots, (p-3)/2$, and combining Theorem 1.4.2 with Lemma 3.6.2, we see that

$$(I(G)\zeta_p)^{(i)} = \Lambda(G)^{(i)}$$

if and only if p does not divide the numerator of $\zeta(1-2i)$. In particular, it follows that (1.19) is valid if and only if all the values in (1.21) are p -adic units.

Next, we must relate (1.20) to the ideal class group of the field $F_0 = \mathbb{Q}(\mu_p)$. For each $n \geq 0$, let $\mathcal{A}_n$ denote the p -primary part of the ideal class group of F_n and define

$$\mathcal{A}_\infty = \varinjlim \mathcal{A}_n,$$

where the inductive limit is taken with respect to the natural maps coming from the inclusion of fields. As always, we write $\mathcal{A}_\infty^-$ for the submodule of $\mathcal{A}_\infty$ on which complex conjugation acts by -1 . To relate X_∞ to $\mathcal{A}_\infty^-$, we invoke the following isomorphism coming from multiplicative Kummer theory (see, for example, [C1]). There is a canonical G -isomorphism

$$\mathcal{A}_\infty^- = \text{Hom}(X_\infty, \mu_{p^\infty}). \quad (1.22)$$

Moreover, it is known that the natural map from $\mathcal{A}_n^-$ to $\mathcal{A}_\infty^-$ is injective and induces an isomorphism

$$\mathcal{A}_n^- \simeq (\mathcal{A}_\infty^-)^{I_n}$$

for all $n \geq 0$, where $I_n = \text{Gal}(\mathcal{F}_\infty/\mathcal{F}_n)$ [Iw1]. But, for any discrete p -primary I_0 -module N , $N^{I_0} = 0$ if and only if $N = 0$. In view of these remarks, we see that

$$\mathcal{A}_0^- \neq 0 \text{ if and only if } X_\infty \neq 0. \quad (1.23)$$

To complete the proof of Kummer's criterion given in Theorem 1.2.1, one has to prove the stronger statement that $\mathcal{A}_0 \neq 0$ if and only if

$X_\infty \neq 0$. One direction is proved by (1.23). Conversely, assume that $\mathcal{A}_0^+ \neq 0$, or equivalently that p divides the class number of F_0 . Thus, writing L_0 for the p -Hilbert class field of F_0 , we have $L_0 \neq F_0$, and so $L_0 F_\infty \neq F_\infty$ because F_∞/F_0 is totally ramified at the unique prime above p . But clearly, $L_0 F_\infty$ is contained in M_∞ , and so $X_\infty \neq 0$ as required. A slight refinement of this argument, in which one considers eigenspaces for the action of the subgroup ϖ of $\mathcal{G}$ of order $p-1$ on these modules, enables one to prove the Herbrand-Ribet Theorem 1.2.1.

Finally, the applications to K -theory arise from the fact that the higher K -groups of the rings of integers of finite extensions of $\mathbb{Q}$ contained in F_∞ can be related to the module $\mathcal{A}_\infty^-$ twisted by positive powers of the cyclotomic character χ of $\mathcal{G}$.