BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 6, Number 3, May 1982

UNITS AND CLASS GROUPS IN NUMBER THEORY AND ALGEBRAIC GEOMETRY

BY SERGE LANG[1]

CONTENTS

§1. Introductory remarks

Determining unramified coverings over various base spaces is a classical activity, which can take place in many contexts: topological, complex analytic, algebraic, and arithmetic. The abelian coverings are simpler to handle than the non-abelian ones, and in these lectures, we shall concentrate on abelian cases. Furthermore, the base space will have mostly dimension 1.

It turns out that the study of the arithmetic case is inextricably intertwined with that of the other cases, in many ways. Thus even though I (for example) start being motivated by the arithmetic case, I come eventually to a consideration of the other cases.

Presented as the Colloquium Lectures at the eighty-fifth summer meeting of the American Mathematical Society, in Pittsburgh, August 17–20, 1981; received by the editors July 8, 1981.

1980 *Mathematics Subject Classification.* Primary 12A35, 12A90; Secondary 14G25, 10D12.

[1] Supported by NSF Grant.

"Motivation", by the way, is a very relative term. What is motivation for one is an irrelevancy for another. I hope that somewhere in the combination of different problems which I shall list, most people will find some motivation for themselves.

One source of motivation for many is that the problems which are considered have their roots in 19th century mathematics. I personally don't make a fetish of this particular item, but it is indeed the case for the arithmetic problems which we shall encounter here. The solutions (as far as they have gone today) however, lie in contemporary mathematics, including the vast panoply of algebraic geometry-commutative algebra developed by Grothendieck and his school, ranging over several thousand pages.

For the topologist, unramified coverings of a space are classified by the fundamental group, and the abelian ones are classified by the first homology group. Although I restrict these lectures to number theory and algebraic geometry, I cannot refrain from mentioning an application of cyclotomic theory to free actions of finite groups on spheres in §2.

Before passing to the arithmetic, which by definition will be our prime source of interest, I would like to mention briefly the general setting for the considerations of algebraic geometry and complex analytic geometry of curves which will play an important role. This may provide motivation for some analysts or geometers.

Let X be a (compact, oriented) Riemann surface, and let $D = D(X)$ be the free abelian group generated by the points on X. This is called the group of **divisors**. A divisor

$$\mathfrak{a} = \sum_P n_P(P)$$

is called **linearly equivalent** to 0 if it is the divisor of a (meromorphic) function on X. This means that there exists a function f on X such that $n_P = \operatorname{ord}_P f$ is the order of the zero (pole) of f at P. Since the number of zeros of a function is equal to the number of poles, the divisor of a function is contained in the group of divisors of **degree** 0, that is divisors such that $\sum n_P = 0$. The factor group

$$D_0/D_l = \operatorname{Pic}(X)$$

of divisors of degree 0 by divisors linearly equivalent to 0 is called the **Picard group** of X, or also the group of **divisor classes** of degree 0. If f is a function, we let (f) denote its associated divisor.

Over the complex numbers, it is known (theorem of Abel-Jacobi) that $\operatorname{Pic}(X)$ is isomorphic to a complex torus of dimension g, where g is the genus of X, that is

$$\operatorname{Pic}(X) \approx \mathbf{C}^g/\Lambda,$$

where Λ is a lattice in $\mathbf{C}^g$. In particular, the structure of its torsion subgroup is clear. For each positive integer N, let $\operatorname{Pic}_N(X)$ denote the subgroup of elements of order N. Then

$$\operatorname{Pic}_N(X) \approx (\mathbf{Z}/N\mathbf{Z})^{2g}.$$

This group is directly related to unramified coverings as follows. Let $\mathfrak{a}$ be a representative divisor for an element of Pic_N, so there exists a function f such that

$$N\mathfrak{a} = (f).$$

Let $K = \mathbf{C}(X)$ be the function field of X, i.e. the field of all meromorphic functions on X. Then

$$K(f^{1/N})$$

is the function field of an unramified covering. Taking roots in this manner for all elements of Pic_N yields a maximal unramified abelian covering of exponent N (meaning that if T is an element of the group of covering transformations, then $T^N = \mathrm{id}$). Furthermore, if Y/X is this maximal covering, and G is its Galois group (group of covering transformations), then it can easily be shown that as finite abelian groups, G and Pic_N are canonically dual to each other (Kummer theory), and in particular are isomorphic (non-canonically), so have the same order. Thus the abelian coverings of X are determined in terms of divisor classes, and conversely, divisor classes are interpreted in terms of abelian coverings. The description of the Kummer theory is so simple that I give it.

Let $c \in \mathrm{Pic}_N$ and let T be a covering transformation. Let $\mathfrak{a}$ be a divisor representing c with $N\mathfrak{a} = (f)$ as above. Let φ be a meromorphic function on the covering such that $\varphi^N = f$ (so loosely speaking, $\varphi = f^{1/N}$, but two N-th roots of f differ by an N-th root of unity). Let $\boldsymbol{\mu}_N$ denote the group of all N-th roots of unity. Then the association

$$(T, c) \mapsto T\varphi/\varphi \in \boldsymbol{\mu}_N$$

defines a pairing between the group G and Pic_N, which is easily shown to give the above mentioned duality.

The Riemann surface X may be associated with an algebraic curve defined over the rational numbers. In that case, we would reserve the letter X to denote the curve, and the complex analytic manifold of its complex points would then be denoted by $X_{\mathbf{C}}$ or $X(\mathbf{C})$. The curve itself may be defined in projective space, or an affine open set may be defined by a single polynomial equation

$$\Phi(x, y) = 0,$$

where Φ is a polynomial in the two affine coordinates x, y. If the coefficients of Φ lie in a field k, we say that the curve is **defined** over k. Important curves for us later will be defined over $\mathbf{Q}$ or over other interesting algebraic number fields, namely finite extensions of the rational numbers. Among these curves will be the so-called modular curves, discussed at greater length in §3. Certain subgroups of the divisor class group for these curves at first present a striking analogy with ideal class groups in algebraic number theory, and recent discoveries have actually established precise connections which will provide much of the substance of these lectures.

Let X be a curve defined over a number field K. Associated with this curve is what is known as its Jacobian variety $J = J(X)$, which gives an algebraic representation of the Picard group $\mathrm{Pic}(X)$. Indeed, the analytic manifold $\mathrm{Pic}(X)_{\mathbf{C}} \approx \mathbf{C}^g/\Lambda$ (complex torus of dimension g) admits a projective embedding so that the group law on the torus corresponds to an algebraic group law. The image of $\mathbf{C}^g/\Lambda$ in projective space is called the **Jacobian variety**. Of course, there exist many such projective embeddings, and all such are algebraically isomorphic. Let us suppose that X has a rational point O in K (that is, X is coordinatized, defined over K, and there is a point all of whose coordinates lie in K). Then there is a projective model for J which is defined over K, and an embedding

$$X \to J$$

such that O (in X) goes to the origin in J. The embedding of X in J is in fact given by the map

$$P \mapsto \text{class of } (P) - (O) \text{ in } \mathrm{Pic}(X) \approx J;$$

furthermore X, identified with its image in J, generates J.

Having coordinatized J in that fashion, we may then speak of **rational points of J in some extension L of K**. They are the points whose affine coordinates lie in L. Such points form a group, denoted by J_L. The group of complex points $J_{\mathbf{C}}$ is complex analytically isomorphic to $\mathbf{C}^g/\Lambda$. If L is a number field, the theorem of Mordell-Weil asserts that J_L is finitely generated. We are interested here in the subgroup of torsion points J_{tor}.

For a given positive integer N, the group of points of order N in J will be denoted by J_N or $J[N]$. This is a finite subgroup, consisting of points which are algebraic over K (all their coordinates are algebraic over K). Let us denote by

$$K(J_N)$$

the field generated by the coordinates of all points in J_N over K. Then $K(J_N)$ is a Galois extension of K, and the effect of any automorphism $\sigma \in \mathrm{Gal}(K(J_N)/K)$ is determined by its effect on the points in J_N. Since we have an isomorphism $J_N \approx (\mathbf{Z}/N\mathbf{Z})^{2g}$, where g is the genus of X, we obtain a representation of this Galois group in $GL_{2g}(\mathbf{Z}/N\mathbf{Z})$. To determine the image of this representation in general is a fundamental problem relating number theory and algebraic geometry. When $g = 1$, so $X = J$, fundamental results have been obtained by Serre [**Se**], but here we want to concentrate on other cases which affect the theory of cyclotomic fields, and give rise to abelian unramified extensions.

In fact, it is necessary to consider certain special subgroups $\mathfrak{g}$ of J. We denote by $K(\mathfrak{g})$ the extension obtained by adjoining to K all coordinates of all points of $\mathfrak{g}$. For special choice of curve X and group $\mathfrak{g}$, we get interesting extensions. This is part of the general framework of giving explicit irrationalities via algebraic geometric objects for the generators of extensions predicted from purely internal structures of algebraic number theory, like ideal class groups. In other words, we want to construct (parametrize) explicitly the algebraic extensions of a given number field. For our purposes, we limit ourselves to abelian extensions, and even to special number fields like cyclotomic fields, for instance fields generated by roots of unity over the rational numbers, since the general problems are already very substantial in those cases.

In §2, §3, §4, §5, and §7 you will see examples of a situation with a group $\mathfrak{g}$ of order p, in a Jacobian variety or in the multiplicative group, admitting a group of automorphisms of order $p - 1$. This situation is represented in different (but related) contexts, with a Galois group having a representation by 2×2 matrices

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad \text{with } a,\ d \in (\mathbf{Z}/p\mathbf{Z})^*,\ b \in \mathbf{Z}/p\mathbf{Z}.$$

Thus the study of abelian coverings leads to non-abelian coverings.

One particular way of obtaining interesting subgroups $\mathfrak{g}$ as mentioned above is the following, which ties up divisor class groups with units in the context of Riemann surfaces.

Let X be a Riemann surface again. Let S be a finite non-empty set of points. Let R be the ring of functions on X which have no poles outside S, that is functions whose poles lie in S. Then the points of S may be viewed as points at infinity, and we may say that the elements of R are the functions with poles only at infinity. Let R^* denote the group of units in R (invertible elements). Then R^* is the group of functions whose zeros and poles are at infinity. Consider the map

$$f \mapsto (f) = \sum_{P \in S} (\operatorname{ord}_P f)(P).$$

Let $s = |S|$ be the cardinality of S. The above map is a homomorphism of R^* into a free group of rank s generated by the points in S. Its kernel is precisely the group of constant functions (a function without zeros and poles on a compact Riemann surface is constant); and its image is contained in the group of divisors of degree 0, so its image has rank at most $s - 1$. "Usually" this image will have much smaller rank. We shall meet later a special situation when for suitable choice of X and S, this rank is precisely $s - 1$. Let $D^S = D^S(X)$ be the group of divisors with support in S. Then the group

$$D_0^S / D_l^S = \operatorname{Pic}^S(X) \subset \operatorname{Pic}(X)$$

is the subgroup of the divisor classes with support in S, or at infinity. When the above rank is $s - 1$, then this subgroup is finite, and provides a very interesting object. For the modular curves considered in §2, they provide geometric counterparts for the ideal class groups in algebraic number theory. The interplay of the algebraic number theory and the theory of divisor classes for certain special number fields and special curves is precisely the topic of these lectures. These modular curves will be obtained as a quotient of the upper half plane by a subgroup of $SL_2(\mathbf{Z})$, of finite index. Such a quotient turns out to be the "affine part" of the complex points on a curve, and the points at infinity, classically called the cusps, furnish the set S. In this way, both the classical and contemporary theory of modular functions enter the picture.

Remark. The word "usually" used above can be made more precise as follows. The **Manin-Mumford conjecture** asserts that fixing a point O on X, there is only a finite number of points P such that the divisor $(P) - (O)$ is of finite order in the Picard group $\mathrm{Pic}(X)$. Essentially this gives a bound on the size of the set S for which the S-units have maximal rank. The conjecture was reduced to a Galois theoretic statement in [**L 3**], and Shimura observed that this statement can be proved in a case known as the complex multiplication case, so the conjecture is true in that case. For a partial result in the general direction, cf. Bogomolov [**Bo**]. [*Raynaud recently proved the conjecture.*]

The above concepts are partly topological and partly geometric, over the complex numbers. However, they can be viewed as being merely the "local" concepts associated with more global concepts of geometric objects over rings of finite type over the integers. In that case, reduction mod primes p, or the associated objects over p-adic fields give other local objects, and gives the possibility for p-adic local results. Putting all these results together for various p and also the archimedean places gives rise to global results. So far, a few results and conjectures are known in various directions. Starting from a very classical situation, I shall expand the range of considerations throughout these lectures to arrive at a more encompassing outlook, pointing to broader directions in which each one of these considerations merely represents one facet of what eventually will become one huge theory.

I shall start with what I hope is a self contained and reasonably accessible level of exposition for a broad audience. As things move forward, the level will rise unavoidably. The actual lectures covered only the first part of the material. There was no reason why the written exposition should abide by the same limitations as the oral exposition.

§2. Cyclotomic Fields

(a) **The basic objects.** As good a point as any to start is the Fermat problem about the solutions to the equation

$$x^N - y^N = 1.$$

The left hand side factorizes as

$$\prod_{\zeta} (x - \zeta y)$$

where the product is taken over all N-th roots of unity. This immediately leads into the study of **cyclotomic fields**, namely the field $\mathbf{Q}(\boldsymbol{\mu}_N)$, where $\boldsymbol{\mu}_N$ denotes the group of N-th roots of unity. By a number field we shall mean a finite extension of the rational numbers. If K is a finite extension of $\mathbf{Q}$, we denote by $\mathfrak{o}_K$ (or $\mathfrak{o}$ if the reference to K is clear) the subring of algebraic integers. When $K = \mathbf{Q}(\boldsymbol{\mu}_N)$, then

$$\mathfrak{o}_K = \mathbf{Z}[\boldsymbol{\mu}_N]$$

is the ring generated over the ordinary integers $\mathbf{Z}$ by the roots of unity. If R is any ring, we let R^* be the group of units (invertible elements) in that ring. In the early study of the Fermat curve, many mistakes were made because people thought that ring had unique factorization into irreducible (prime) elements, which turned out to be false. For instance, a recent issue of the *Mathematical Intelligencer* (1979) reproduces a page of the *Compte Rendu des Séances de l'Académie des Sciences* of 1 March 1847 where Lamé announces a proof of the Fermat problem. (Cf. the Lenstra article, p. 6.) This announcement is followed by critical remarks of Liouville, pointing out that Lamé's paper is deficient in not taking into account the lack of unique factorization.

The obstruction to unique factorization of course lies in the ideal class group, which is defined as follows. Let $\mathfrak{a}, \mathfrak{b}$ be two ideals ($\neq 0$) of $\mathfrak{o}$. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are **linearly equivalent**, or lie in the same **ideal class**, if there exists an element α of K such that $\mathfrak{a} = \alpha\mathfrak{b}$. Under this equivalence relation, the ideals form a group called the **ideal class group** $\mathrm{Cl}(K)$ of K, and this group is finite. Its order is denoted by h_K and is called the **class number**.

Kummer proved that if the class number of $\mathbf{Q}(\mu_p)$ is not divisible by p, then the Fermat problem is solved affirmatively for p. We shall describe below other deeper considerations of Kummer concerning this class number and the Fermat problem.

A fundamental problem about number fields is the determination of the class number and of the structure of the ideal class group. For instance: how large is h_K? By what primes is it divisible? How does it behave asymptotically with N when $K = \mathbf{Q}(\mu_N)$? Or $K = \mathbf{Q}(\mu_{p^n})$ with a fixed prime p and n variable?

The ideal class group is directly related to unramified coverings as follows. For any extension L of K, the primes $\mathfrak{p}$of K may decompose in this extension:

$$\mathfrak{p}\mathfrak{o}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},$$

where the right hand side is the unique factorization of $\mathfrak{p}\mathfrak{o}_L$ into power products of prime *ideals*. If the exponents $e_1, \ldots, e_r$ are all equal to 1, we say that $\mathfrak{p}$ is **unramified**. If every prime $\mathfrak{p}$ of K is unramified, and if in addition every embedding of K into the real numbers extends only to real embeddings of L, then we say that L is **unramified** over K. A fundamental fact of **class field theory** asserts:

Let L be the maximal abelian unramified extension of K.

Then there is a canonical isomorphism

$$C_K \approx \mathrm{Gal}(L/K)$$

of the ideal class group of K with the Galois group of L over K.

Another difficulty encountered in analyzing the Fermat curve, besides the ideal class group, was due to the units of $\mathfrak{o}_K$. Kummer had understood the deeper significance of the units, and of a distinguished subgroup of the units which he could write down immediately. Indeed, let ζ be a primitive N-th root of unity, and let i, j be positive integers prime to N. Then

$$\frac{1-\zeta^i}{1-\zeta^j}$$

is a unit. This is easily seen. First we note that

$$\frac{1-\zeta^i}{1-\zeta} = 1 + \zeta + \cdots + \zeta^{i-1},$$

so $1 - \zeta$ divides $1 - \zeta^i$. But we can find a positive integer a such that $aj \equiv 1 \bmod N$ since j is assumed relatively prime to N, so we get also that $1 - \zeta^j$ divides $1 - \zeta$, as asserted.

Let $K = \mathbf{Q}(\mu_N)$. We let $E_{\mathrm{cyc}}(K)$ be the group generated by all roots of unity in K and all the units of the form

$$\prod_{1 \leq a < N} (1 - \zeta^a)^{n(a)}.$$

We call $E_{\mathrm{cyc}}(K)$ the group of **cyclotomic units**. It is a subgroup of the units $E(K)$. A classical theorem of Dirichlet asserts that $E(K)$ (so $E_{\mathrm{cyc}}(K)$) are finitely generated, of the same rank. In fact, we have

$$\operatorname{rank} E(K) = \frac{[K : \mathbf{Q}]}{2} - 1,$$

where $[K : \mathbf{Q}]$ is the degree of K over $\mathbf{Q}$, which is known to be equal to $\phi(N)$ (ϕ is the Euler function). Although one knows the group $E_{\mathrm{cyc}}(K)$, the structure of $E(K)$, and especially the factor group E/E_{cyc} remains a mystery.

It is clear that the essential aspects of the units have to do with the real subfield K^+ of K. Indeed, let E^+ denote the group of units in K^+. With Hasse, define the index

$$Q = (E : \mu_K E^+).$$

Then it is easy to show that $Q = 1$ if N is a prime power, and $Q = 2$ if N is composite. In addition, concerning the cyclotomic units, suppose for simplicity that N is odd. If ζ is an N-th root of unity, we can write $\zeta = \lambda^2$ for some N-th root of unity λ, and then

$$1 - \lambda^2 = \lambda(\lambda^{-1} - \lambda).$$

This immediately shows that up to roots of unity, the cyclotomic units are real.

In the formula for the rank given above, the factor of $1/2$ is due to the fact that up to roots of unity, the units come from the real subfield; and we subtract 1 because there is a relation analogous to the property in function fields that a function has the same number of zeros and poles, counting multiplicities. In the present instance, the places at infinity are simply the embeddings of a number field into the complex numbers. If v denotes such an embedding, and $| \ |_v$ denotes the absolute value induced by the embedding, then one has the relation for any unit ϵ:

$$\sum_v \log |\epsilon|_v = 0.$$

If r_1 denotes the number of real embeddings and $2r_2$ the number of complex embeddings, then it is clear that the rank of the units is at most $r_1 + r_2 - 1$, and Dirichlet's theorem implies that the rank is precisely equal to this number. In the cyclotomic case $K = \mathbf{Q}(\mu_N)$ with $N \geq 3$ there is of course no real embedding of K.

We shall now see more precisely what is known and what is conjectured about the ideal class group and unit group in the cyclotomic fields.

We must view the various groups we have introduced as representation spaces for the Galois group

$$G = \mathrm{Gal}(\mathbf{Q}(\mu_N)/\mathbf{Q}).$$

This group G is isomorphic to $(\mathbf{Z}/N\mathbf{Z})^*$, under the association

$$a \mapsto \sigma_a.$$

If a is an integer prime to N, then σ_a is the automorphism of $\mathbf{Q}(\mu_N)$ such that

$$\sigma_a \zeta = \zeta^a.$$

The group of principal ideals is stable under G, so G acts on C_K with $K = \mathbf{Q}(\mu_N)$. It is also clear that the group of cyclotomic units is stable under G, so G acts on E/E_{cyc}. What is the structure of these groups as G-modules?

In any representation theory, one tries to decompose representation spaces into eigenspaces for the characters of the group. The first immediate such decomposition that we deal with is that arising from complex conjugation. Note the element σ_{-1} in G such that

$$\sigma_{-1}\zeta = \zeta^{-1}.$$

If A is any G-module we let A^+ be the $(+1)$-eigenspace for σ_{-1}, that is the subgroup of elements fixed by σ_{-1}. We let A^- be the (-1)-eigenspace, that is the subgroup of elements x such that $\sigma_{-1}x = -x$ for $x \in A$ (writing the operation of A additively). If multiplication by 2 is invertible on A, then we have a direct sum decomposition

$$A = A^+ \oplus A^-.$$

Consider the group of ideal classes $C = C_K$. Let K^+ denote the real subfield of K. An ideal $\mathfrak{a}$ in K^+ lifts to an ideal of K, namely

$$\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{o}_K.$$

This induces a homomorphism on the ideal class groups

$$C_{K^+} \to C_K$$

which can be proved to be injective. Likewise, we have a norm map

$$N_{K/K^+} : C_K \to C_{K^+}$$

given by $c \mapsto cc^\rho$, where $\rho = \sigma_{-1}$ is complex conjugation. It can be shown that this norm map is surjective. By definition, the kernel of the norm map consists of those ideal classes c such that $c^{1+\rho} = 1$, or in other words $c^\rho = c^{-1}$. This kernel is precisely the (—1)-eigenspace for complex conjugation. Thus we have an exact sequence

$$1 \to C_K^- \to C_K \to C_{K^+} \to 1.$$

(For proofs, cf. [**L 1**], Chapter 3, §4.) We let:

$$h^+ = \text{order of } C^+ \quad \text{and} \quad h^- = \text{order of } C^-.$$

Then h^+ is the class number of the real subfield, and we have

$$h = h^- h^+.$$

We are thus led to study h^+ and h^- separately.

(b) **Plus eigenspaces.** Let us begin with h^+. First there is a relation of this number with units. We assume for simplicity that $N = p$ is a prime ≥ 3 and $K = \mathbf{Q}(\mu_p)$. We then have a coincidence of orders:

Theorem 2.1. $h^+ = (E : E_{\text{cyc}})$.

This theorem is due to Kummer. Its proof today is viewed as elementary, and results from the factorization of the zeta function into Dirichlet L-series. There is no need to go into the proof here. Kummer made the first basic discoveries concerning these class numbers, and made the first basic conjectures. Especially:

Conjecture 1. *For* $\mathbf{Q}(\mu_p)$, h^+ *is prime to* p.

The history of that conjecture is interesting. Kummer made it in no uncertain terms in a letter to Kronecker dated 28 December 1849. Kummer first tells Kronecker off for not understanding properly what he had previously written about cyclotomic fields and Fermat's equation, by stating "so liegt hierin ein grosser Irrthum deinerseits..."; and then he goes on (Collected Works, Vol. 1, p. 84):

> Deine auf dieser falschen Ansicht berühenden Folgerungen fallen
> somit von selbst weg. Ich gedenke vielmehr den Beweis des
> Fermatschen Satzes auf folgendes zu grunden:
>
> 1. Auf den noch zu beweisenden Satz, dass es für die Ausnahmszahlen λ stets Einheiten giebt, welche ganzen Zahlen congruent sind für den Modul λ, ohne darum λte Potenzen anderer Einheiten zu sein, oder was dasselbe ist, dass hier niemals D/Δ durch λ theilbar wird.

In our notation: $\lambda = p$ and $D/\Delta = h^+$. Writing h^+ in this form is explainable in terms of the expression in Theorem 2.1. The quotient D/Δ represents the order of the factor group E/E_{cyc}. Thus Kummer rather expected to prove the conjecture. According to Barry Mazur, who reviewed Kummer's complete works when they were published recently by Springer-Verlag, Kummer never mentioned the conjecture in a published paper, but he mentioned it once more in another letter to Kronecker on 24 April 1853 (loc cit p. 93):

> Hierein hängt auch zusammen, dass eines meiner Haupresultate auf
> welches ich seit einem Vierteljahre gebaut hatte, dass der zweite
> Faktor der Klassenzahl D/Δ niemals durch λ theilbar
> ist, falsch ist oder wenigstens unbewiesen...Ich werde
> also vorlaufig hauptsachlich meinen Fleiss nur auf die Weiterführung
> der Theorie der complexen Zahlen wenden, und dann sehen ob
> etwas daraus entsteht, was auch uber jene Aufgabe
> Licht verbreitet.

So the situation was less clear than Kummer thought at first. Much later, Vandiver made the same conjecture, and wrote [**Va 1**]:

> ...However, about twenty-five years ago I conjectured that this number was never divisible by p [referring to h^+]. Later on, when I discovered how closely the question was related to Fermat's Last Theorem, I began to have my doubts, recalling how often conjectures concerning the theorem turned out to be incorrect. When I visited Furtwängler in Vienna in 1928, he mentioned that he had conjectured the same thing before I had brought up any such topic with him. As he had probably more experience with algebraic numbers than any mathematician of his generation, I felt a little more confident...

Vandiver, like others before him, wanted to have such a result for the application to what is called the *first case* of Fermat's theorem: there are no solutions other than the trivial ones to the equation

$$x^p + y^p = z^p$$

in relatively prime integers x, y, z which are also prime to p. Many years ago, Feit was unable to understand a step in Vandiver's "proof" that $p \nmid h^+$ implies the first case of Fermat's Last Theorem [**Va 2**], and stimulated by this, Iwasawa found a precise gap which is such that there is no proof.

In number theory, or elsewhere, when two groups arising naturally in the course of a theory have the same order, one immediately asks whether this coincidence is not due to the fact that the groups are isomorphic. Iwasawa has an example showing that C^+ and E/E_{cyc} are not isomorphic as G-modules. It is generally believed that the two groups are not always isomorphic, even as abelian groups. However, in this direction, one has the next best thing.

Theorem 2.2. *For any prime l not dividing the degree $[K : \mathbf{Q}]$ with $K = \mathbf{Q}(\boldsymbol{\mu}_p)$ the l-primary parts of C^+ and E/E_{cyc} have isomorphic semisimplications.*

Recall that the l-primary part $A^{(l)}$ of a torsion abelian group A is the subgroup generated by all elements whose order is a power of l.

We also recall briefly the definition of semisimplification. Let A be a representation module for G. We say that A is **simple** (or gives a simple, or irreducible representation of G) if $A \neq \{0\}$, and if A has no G-submodules other than 0 or itself. The module A may of course have a coefficient ring or field acting on it, commuting with the action of G. If A is a finite group, we may take this ring to be $\mathbf{Z}$. Suppose that A is finite, or finite dimensional over a field. Then A has a chain of submodules

$$A = A_0 \supset A_1 \supset \cdots \supset A_r$$

such that every A_i/A_{i+1} is simple. The direct sum

$$\bigoplus_{i=0}^{r-1} A_i/A_{i+1}$$

is uniquely determined as a G-module, up to isomorphism, and is called the **semisimplification**. In earlier terminology, the simple components A_i/A_{i+1} are called the **Jordan-Hölder** factors.

Theorem 2.2 was conjectured for several years, stemming from the work of Leopoldt [**Le 2**]. The conjecture is made explicit in Gras [**Gra**]. A related conjecture appears as a "Remark" in Coates-Lichtenbaum [**Co-L**], p. 520. Greenberg [**Gr 2**] showed that the statement of Theorem 2.2 was a consequence of a standard conjecture concerning certain infinite extensions, now proved by Mazur-Wiles, see below Theorem 2.10.

By going up the tower of p^n-th roots of unity, one can make a conjecture concerning the limiting behavior of units and ideal classes as modules over the infinite Galois group. This is more elaborate to state, and we shall touch on that aspect of the question at the end of this section.

The group theoretic situation in the case when N is composite was unclear for a long time. Sinnott [**Si 1**], [**Si 2**] made a breakthrough when he discovered the appropriate group-ring formulation needed to handle the analogue of Theorem 2.1 in the composite case. In this case, the reader should be warned of at least one important new phenomenon: the presence of a power of 2 in the relation of Theorem 1.1, between h^+ and the index $(E : E_{\text{cyc}})$, namely

$$(E : E_{\text{cyc}}) = (E^+ : E^+_{\text{cyc}}) = 2^\nu h^+,$$

where $\nu = 2^{t-2} + 1 - t$, and t is the number of prime factors of N, whenever $t \geq 2$. Thus when $t = 1$ or 2, $2^\nu = 1$, but $\nu > 0$ otherwise.

(c) **A topological interlude.** Let G be a finite group operating freely on the n-sphere S^n with $n \geq 3$, and let S^n/G be the quotient space. Then $G = \pi_1(S^n/G)$ is the fundamental group. Such operations therefore give rise to maximal unramified coverings, which are even finite. One wishes to classify such actions up to various equivalence relations. Two representations R_1, R_2 of a group G in the group of topological automorphisms of a space X are called topologically conjugate if there exists a topological automorphism T of X such that $TR_1(g)T^{-1} = R_2(g)$ for all $g \in G$. A folklore conjecture asserts that:

> a topologically free action of a finite group on the 3-sphere S^3
> is topologically conjugate to a free linear action.

Seifert must have known this possibility. Milnor drew attention to the problem in the late fifties, and solved a special case. The problem is stated in Thurston's Lecture Notes from Princeton (in circulation). For background material, see J. Hempel's book on 3-Manifolds (Ann. of Math. Studies 96, 1976).

In higher dimensions, there is of course always the linear action of finite subgroups of $O(n)$ on S^n. For such linear theory, cf. for instance J. Wolf, *Spaces of Constant Curvature*, 2nd Edition, Publish or Perish. I am indebted to C. B. Thomas for drawing my attention to the above literature, and to forthcoming papers of his, concerning the classification of free actions of finite groups on S^n which C. T. C. Wall has already shown to depend in part on the 2-primary component of the ideal class group in real cyclotomic fields $\mathbf{Q}(\boldsymbol{\mu}_N)^+$ for suitable N.

In particular, Thomas tells me that given any free action of a finite group G on S^n with $n \geq 5$, there exist infinitely many distinct topological conjugacy classes of actions of G on S^n, and there are only finitely many topological conjugacy classes of linear actions. Using the algebraic background of a paper of Wall [**Wa**], applied to the surgery exact sequence, Thomas gives examples for the binary dihedral group D_{4p} of order $4p$ operating freely on S^{4k-1}

with $k \geq 2$, when p is a prime such that h_p^+ is odd, e.g. $p < 163$. These operations are even homotopically distinct from the classical linear actions. [For the convenience of the reader, I reproduce a definition of D_{4p}. It can be represented as the group generated by the matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } \begin{pmatrix} \varsigma & 0 \\ 0 & \varsigma^{-1} \end{pmatrix}$$

where ς is a primitive p-th root of unity. It is one of the extensions of the cyclic group of order p by the cyclic group of order 4. In the above representation, it acts linearly on $\mathbf{C}^2$, whence on S^3 which is naturally contained in $\mathbf{C}^2$.]

Furthermore, according to Thomas, there exist free actions by D_{4p} which can be topologically distinguished only by an invariant in the 2-primary part of the ideal class group of $\mathbf{Q}(\boldsymbol{\mu}_p)^+$. A paper of Kubert [**Ku 1**] shows the existence of a large 2-primary component in $\mathbf{Q}(\boldsymbol{\mu}_N)$ when N is divisible by many primes, but says nothing about the 2-primary part for $\mathbf{Q}(\boldsymbol{\mu}_p)$.

In the above context, the ideal class group (2-primary part) intervenes. I am indebted to J. Milgram for pointing out to me the existence of a substantial literature which relates the existence of free action of finite groups on spheres to units in cyclotomic fields, and especially cyclotomic units. For example in [**Mi 1**], [**Mi 2**] Milgram reduces questions of which groups act on S^n $(n > 3)$ to explicit questions involving the structure of such units. Since my main interest here was only to point out briefly a connection of units and ideal class groups with topology, and constitute an aside for the main topics of these lectures, I refer interested readers to the discussions and bibliographies at the end of Milgram's papers for further information.

(d) **The minus eigenspaces.** So much for the plus part of the class number and the units at this time. Let us look at the minus part. The situation is now radically different. We are seeking all relations for the ideal classes C^- in the group ring $R = \mathbf{Z}[G]$. Classical relations are provided by a construction of Kummer and Stickelberger, as follows.

Given a real number mod $\mathbf{Z}$, say $x \in \mathbf{R}/\mathbf{Z}$, we let $\langle x \rangle$ denote its unique representative in $\mathbf{R}$ such that

$$0 \leq \langle x \rangle < 1.$$

We define the first **Bernoulli polynomial**

$$\mathbf{B}_1(X) = X - \frac{1}{2}.$$

(There will be a second Bernoulli polynomial later.) We then define the **Stickelberger element** in $\mathbf{Q}[G]$:

$$\theta = \sum_{a=1}^{p-1} \mathbf{B}_1\left(\frac{a}{p}\right)\sigma_a^{-1} = \sum_{a \in \mathbf{Z}(p)^*} \mathbf{B}_1\left(\left\langle\frac{a}{p}\right\rangle\right)\sigma_a^{-1}.$$

This element θ has rational coefficients in the group algebra. How to integralize it? Note that for any positive integer c odd and prime to p, the rational numbers

$$\left\langle\frac{ca}{p}\right\rangle - c\left\langle\frac{a}{p}\right\rangle \quad \text{and} \quad \frac{c-1}{2}$$

are integers. From this it follows at once that $(\sigma_c - c)\theta \in \mathbf{Z}[G]$. In other words, let I be the ideal in the group ring $\mathbf{Z}[G]$ generated by all elements $\sigma_c - c$ with c prime to $2p$. Then

$$I\theta \subset \mathbf{Z}[G],$$

and in fact, if we let $R = \mathbf{Z}[G]$, then

$$R\theta \cap R = I\theta.$$

Furthermore, $\theta = \theta^-$. We call $I\theta$ the **Stickelberger ideal** S.

Theorem 2.3. *The elements of the Stickelberger ideal annihilate C^-. (Actually, they also annihilate C.)*

This theorem of Kummer and Stickelberger is proved by showing that for any ideal $\mathfrak{a}$, the ideal $\mathfrak{a}^\alpha$ is principal when $\alpha = (\sigma_c - c)\theta$, and by exhibiting explicitly the algebraic number generating this ideal, which is a quotient of Gauss sums. We do not go into this explicit determination here since we want to emphasize other aspects of the theory. For a general context, see Conjecture 8.3. Kummer had already proved the theorem by getting the relation for prime ideals of degree 1 over $\mathbf{Q}$, see [**Kum 2**], p. 628, and by using the "Stickelberger element" in special cases.

Iwasawa [**Iw 3**] proved:

Theorem 2.4. $(R^- : S) = h^-$.

As for the cyclotomic units, this relation holds without extra factor when dealing with N equal to a prime power, and with an extraneous power of 2, as determined by Sinnott, when N is composite. We stick to the prime case for simplicity.

Iwasawa and Leopoldt emphasized repeatedly the problem of determining the relation between the factor module R^-/S and C^-.

Theorem 2.5. *Let $K = \mathbf{Q}(\mu_p)$. For any prime l not dividing the degree $[K : \mathbf{Q}]$, the l-primary parts of C^- and R^-/S have isomorphic semisimplifications. (Here we may have $l = p$.)*

Theorem 2.5 was conjectured by Leopoldt [**Le 2**], [**Le 3**], and like its plus counterpart, follows from the Mazur-Wiles general theorems. For the p-primary part, one has in addition:

Conjecture 2. *The p-primary part of C^- is cyclic over the group ring, namely it is generated by one element, and consequently there is an isomorphism*

$$(R^-/S)^{(p)} \approx C^{-(p)},$$

where the superscript (p) indicates p-primary part.

In this manner, the study of the minus p-primary part of the class group would be reduced to the study of the Stickelberger ideal.

Note. Conjecture 2 stems from the work of Iwasawa and Leopoldt, but neither have explicitly stated it as a conjecture. They certainly drew attention to its possibility, and for convenience, it may be useful to refer to it as the Iwasawa-Leopoldt conjecture. If it is true, they should get the credit, and if it is false, I should get the blame.

When studying the eigenspaces for the characters of G (after a suitable extension of scalars), one encounters the character values

$$\chi(\theta) = \sum_{a=1}^{p-1} \mathbf{B}_1\left(\frac{a}{p}\right)\bar{\chi}(a) = B_{1,\bar{\chi}} \quad \text{by definition,}$$

identifying σ_a with a in $(\mathbf{Z}/p\mathbf{Z})^*$. Following Iwasawa, Leopoldt, and Mazur, this sum can be written as an integral

$$B_{1,\bar{\chi}} = \int_{\mathbf{Z}/p\mathbf{Z}} \bar{\chi}\, d\mu_{\mathbf{B}_1},$$

but we do not discuss this aspect of the question. However, we note that the divisibility properties of h^- depend on the divisibility properties of these sums $\chi(\theta)$, which are still very difficult to determine. Indeed, it is shown classically also by elementary L-series considerations that one has the explicit formula:

Theorem 2.6. $h^- = w \prod_{\chi\ odd} -\frac{1}{2}B_{1,\chi}.$

Here w is the number of roots of unity in $\mathbf{Q}(\mu_p)$, namely $2p$. The product is taken over odd characters χ, meaning characters such that $\chi(-1) = -1$. Thus the divisibility properties of h^- are determined by the divisibility properties of the numbers $B_{1,\chi}$, the "generalized Bernoulli numbers" of Leopoldt [**Le 1**] who investigated their congruence properties, picking things up where Kummer left them a century before.

So we look at characters χ of $(\mathbf{Z}/p\mathbf{Z})^*$, even or odd since we are going to deal with the cyclotomic fields and the modular curves. The group $(\mathbf{Z}/p\mathbf{Z})^*$ is merely the multiplicative group of the prime field $\mathbf{Z}/p\mathbf{Z}$, and consists of $(p-1)$th roots of unity. On the other hand, the p-adic integers $\mathbf{Z}_p$ contain the $(p-1)$th roots of unity as a subgroup of $\mathbf{Z}_p^*$, and reduction mod p gives an isomorphism

$$\mu_{p-1} \to (\mathbf{Z}/p\mathbf{Z})^*$$

of the group of $(p-1)$th roots of unity in characteristic 0 with the $(p-1)$th roots of unity in characteristic p. The inverse of this isomorphism,

$$\omega : (\mathbf{Z}/p\mathbf{Z})^* \to \mu_{p-1}$$

is called the **Teichmuller character**. So $\omega(a)$ is the unique root of unity congruent to $a \bmod p$.

Instead of the group ring $\mathbf{Z}[G]$, let us look at the group ring $\mathbf{Z}_p[G]$ over the p-adic integers. We lose nothing in so widening the coefficients when we look at representations of G in finite abelian groups whose order is a power of p; and we gain a lot, because the usual idempotent projecting on the χ-eigencomponents can now be written with coefficients in $\mathbf{Z}_p$, namely

$$e_\chi = \frac{1}{|G|} \sum_{\sigma \in G} \bar{\chi}(\sigma)\sigma.$$

As usual, $|G|$ denotes the order of G, namely $p - 1$ in the present case. Note that $p - 1$ is invertible in $\mathbf{Z}_p^*$, so $e_\chi \in \mathbf{Z}_p[G]$. Let M be a G-module on which multiplication by $p - 1$ is invertible. Then $e_\chi M$ is the χ-eigenspace, namely the subgroup of all elements x such that

$$\sigma x = \chi(\sigma)x.$$

This eigenspace will be denoted by $M(\chi)$.

Here we let M be the co-Stickelberger module,

$$M = \mathbf{Z}_p[G]^- / \mathbf{Z}_p S.$$

According to Conjecture 2, we have $M \approx C^{-(p)}$. In any case, one can ask two questions: what is the structure of M, and how closely does it approximate $C^{-(p)}$.

Theorem 2.7. (i) *If* $\chi = \omega$, *then* $M(\chi) = 0$.

(ii) χ *is an odd character,* $\chi \neq \omega$ *then* $M(\chi)$ *is cyclic,*

$$M(\chi) \approx \mathbf{Z}_p / B_{1,\bar{\chi}} \mathbf{Z}_p.$$

In particular, $\operatorname{ord}_p M(\chi) = \operatorname{ord}_p B_{1,\bar{\chi}}$.

This theorem is an immediate consequence of the definitions. Theorem 2.5 then implies that

$$\operatorname{ord}_p C^{-(p)}(\chi) = \operatorname{ord}_p B_{1,\bar{\chi}},$$

and Conjecture 2 predicts that $C^{-(p)}(\chi)$ is cyclic, for an odd character $\chi \neq \omega$, of order $p^{m(\chi)}$, where $m(\chi) = \operatorname{ord}_p B_{1,\bar{\chi}}$. Thus the study of M is reduced to the study of p-divisibility of the Bernoulli numbers.

The above conjectures and theorems constitute an essential part of the present vision of what the structure of units and class numbers should be like. It can be shown that the Kummer-Vandiver conjecture h^+ prime to p is true implies all the theorems and conjectures of this section. Thus the conjectures are related, and in fact are related via Kummer theory and class field theory as follows.

Consider the maximal abelian unramified extension of $K = \mathbf{Q}(\mu_p)$ which is of exponent p, meaning that if $\mathcal{G}$ is its Galois group, then $\sigma^p = 1$ for all $\sigma \in \mathcal{G}$. By Kummer theory, if L is a cyclic subextension of degree p, then

$$L = K(\epsilon^{1/p})$$

for some element ϵ. The Kummer-Vandiver conjecture implies that ϵ can be taken to be a cyclotomic unit. But then the representation of $\mathrm{Gal}(K/\mathbf{Q})$ on the cyclotomic units is sufficiently explicit so that by mixing Kummer theory and class field theory one obtains the cyclicity of C^- over the group ring. Actually, the situation is more involved, because as described above, we are only dealing with the subgroup of elements of order p, and to get the full structure, one has to consider higher cyclotomic fields of p^n-th roots of unity, for n tending to infinity. In other words, one has to go up the cyclotomic tower. This requires a more elaborate foundation and the introduction of new concepts which are more technical. In any case, one is led to consider double decked extensions

$$\begin{tikzcd}
K(\epsilon^{1/p}) \arrow[d, dash] \\
K = \mathbf{Q}(\boldsymbol{\mu}_p) \arrow[d, dash] \\
\mathbf{Q}
\end{tikzcd}$$

such that each layer is abelian, but the composite layer is not; and similarly when p is replaced by p^n for arbitrarily large n. Attempts to recognize directly which extensions $K(\epsilon^{1/p})$ are unramified over $\mathbf{Q}(\boldsymbol{\mu}_p)$ have failed for a century. The newly developed methods via algebraic geometry replace the ordinary p-th root of a unit by another p-th root, namely the root taken relative to the group law on Jacobian varieties, where the additional structure is more complicated, richer and leads to results which so far were unobtainable otherwise.

In the tower, we should note a theorem of Washington [**Wash**].

Theorem 2.8. *Let C_n^- be the minus part of the ideal class group in $\mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})$. Let l be a prime $\neq p$. Then the powers of l dividing the orders of C_n^- are bounded.*

One asks not only for the behavior of class numbers "vertically", that is in the tower of fields $\mathbf{Q}(\boldsymbol{\mu}_{p^n})$ for n tending to infinity, but one also asks for the "horizontal" behavior of these class numbers. This amounts to the horizontal behavior of $B_{1,\chi}$ from the point of view of divisibility, when χ is a character of $(\mathbf{Z}/p\mathbf{Z})^*$, and p is viewed as variable. As far as I know, there are no results in this direction. Computations indicate a perturbation of random behavior. For instance, Trotter has done some computations for the class number

$$h = -B_{1,\chi}$$

of an imaginary quadratic field $F = \mathbf{Q}(\sqrt{-p})$, where χ is the associated quadratic character. Consider the primes $\equiv 3 \bmod 4$, with $7 \leq p < 48,611$. There are 2,512 such primes. We have mod 3:

$h \equiv 0$ for 964 (out of 2,512) or 38.4 o/o,

$h \equiv 1$ for 761 (out of 2,512) or 30.3 o/o,

$h \equiv 2$ for 787 (out of 2,512) or 31.3 o/o.

As Trotter remarks, the evidence is strong that $h \equiv 0 \bmod 3$ occurs more often than a third of the time, quite strong that $h \equiv 0 \bmod 5$ occurs more than one fifth of the time, and definitely suggests that $h \equiv 0 \bmod 7$ occurs more than one seventh of the time. One awaits more precise conjectures and proofs.

However, the distribution over all quadratic fields $\mathbf{Q}(\sqrt{-D})$ appears to be random, cf. Davenport and Heilbronn [**Da-H**], cf. see also Kuroda-Leopoldt in [**Zi**], p. 42.

When the quadratic subfield F is contained in the cyclotomic field $\mathbf{Q}(\boldsymbol{\mu}_p)$, then the ideal class group of F occurs as a quotient group of the ideal class group of $\mathbf{Q}(\boldsymbol{\mu}_p)$, by considerations of class field theory, so the class numbers of subfields of $\mathbf{Q}(\boldsymbol{\mu}_p)$ are important components of the class numbers of the full cyclotomic field itself.

(e) **The cyclotomic p-tower.** In this last part I shall summarize briefly the way one formulates results in the infinite tower of p-extensions, first investigated by Iwasawa. The algebra becomes a little heavier. The reader might omit this part at first, in order to minimize the obstacles preceding the discussion of geometric connections of number theory and groups of finite order on Jacobian varieties, given in §3 and §4 for $\mathbf{Q}(\boldsymbol{\mu}_p)$.

I limit the discussion to the standard cyclotomic case, so let p be an odd prime, and let

$$K_n = \mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}}), \qquad K_\infty = \bigcup_{n=1}^{\infty} K_n.$$

Let:

$\mathcal{G}_n = \mathrm{Gal}(K_n/K_0)$,

$\mathcal{G}_\infty = \mathrm{Gal}(K_\infty/K_0) =$ projective limit of the groups $\mathcal{G}_n$. Then

$$\mathcal{G}_\infty \approx \mathbf{Z}_p.$$

$\gamma =$ topological generator of $\mathcal{G}_\infty$, for instance $\gamma = \sigma_{1+p}$.

$\Lambda =$ projective limit of $\mathbf{Z}_p[\mathcal{G}_n]$. Then there is a unique isomorphism

$$\Lambda \approx \mathbf{Z}_p[[X]]$$

with the power series in one variable over $\mathbf{Z}_p$, such that $1 + X$ corresponds to the chosen generator γ. This means that the image of $1 + X$ in $\mathbf{Z}_p[\mathcal{G}_n]$ is equal to the image of γ in $\mathcal{G}_n$ for all n. We call Λ the **Iwasawa algebra**. Cf. [**Iw 1**] and [**Se 2**]. Let:

$\mathcal{A}_n = p$-primary part of $\mathrm{Cl}(K_n)^-$ and

$\mathcal{A} = \varprojlim \mathcal{A}_n$.

Then $\mathcal{A}$ is a Λ-module, which can be proved to be torsion and finitely generated, and $\mathcal{A}$ is also a topological γ-module. Cf. Iwasawa [**Iw 1**] and Serre [**Se 2**]. Let further:

$G_n = \mathrm{Gal}(K_n/\mathbf{Q})$.

Then $\mathcal{A}$ is a G_0-module. Since $\boldsymbol{\mu}_{p-1} \subset \mathbf{Z}_p$, if χ denotes odd characters of G_0, we may form the decomposition

$$\mathcal{A} = \bigoplus_{\chi} \mathcal{A}(\chi).$$

For each n there is a Stickelberger ideal S_n, and the **co-Stickelberger module at level** n:

$$M_n = \mathbf{Z}_p[G_n]^- / \mathbf{Z}_p S_n.$$

We let the **co-Stickelberger module** be the projective limit

$$M = \varprojlim M_n.$$

If the Iwasawa-Leopoldt conjecture is true, then we have an isomorphism for each odd $\chi \neq \omega$:

$$\mathcal{A}(\chi) \approx M(\chi).$$

We wish to describe the Mazur-Wiles theorem concerning the structure of $\mathcal{A}$ as Λ-module.

Two modules M_1 and M_2 are called **quasi-isomorphic** if there is a homomorphism $h : M_1 \to M_2$ with finite kernel and finite cokernel. It is a theorem of Serre [**Se 2**] that any finitely generated torsion module over Λ is quasi-isomorphic to a direct sum

$$\bigoplus_i \Lambda/p^{r_i}\Lambda \oplus \bigoplus_j \Lambda/f_j\Lambda$$

where each f_j is a **Weierstrass polynomial**, namely a polynomial in X with leading coefficient 1, and all other coefficients congruent to $0 \bmod p$. Such a module will be said to be of **Jacobian type** if there are no factors of type $\Lambda/p^r\Lambda$.

Theorem 2.9. **(Ferrero-Washington)** *The module $\mathcal{A}$ and the co-Stickelberger module are of Jacobian type.*

The proof in [**Fe-W**] relies on p-adic measure theoretic considerations, and we do not go into it here. If f is a Weierstrass polynomial, then $\Lambda/f\Lambda$ is free of dimension $\deg f$ over $\mathbf{Z}_p$. For a module of Jacobian type, we define the **characteristic polynomial** to be

$$\prod f_j.$$

It is the characteristic polynomial of $\gamma - 1$ acting on the $\mathbf{Q}_p$-vector space obtained by. tensoring with $\mathbf{Q}_p$.

Theorem 2.10. **(Mazur-Wiles)** *For any odd character $\chi \neq \omega$, $\chi \neq \bar{\omega}$, the modules $\mathcal{A}(\chi)$ and $M(\chi)$ have the same characteristic polynomials. Equivalently, the $\mathbf{Q}_p$-vector spaces $\mathbf{Q}_p\mathcal{A}(\chi)$ and $\mathbf{Q}_pM(\chi)$ have isomorphic semi-simplifications as Λ-modules.*

A generator of the ideal formed with the characteristic polynomial is determined only up to a unit in Λ. Another generator of independent interest arises in the theory and illuminates Theorem 2.10, namely a power series g_χ having the following property. Let ψ be a character of $1+p\mathbf{Z}_p$, and let n be the smallest positive integer such that $1+p^n\mathbf{Z}_p$ is contained in the kernel of ψ. Such p^n is called the conductor of ψ. One can define generalized Bernoulli numbers $B_{1,\chi\psi}$. Identifying $\mathcal{G}_\infty$ with $1+p\mathbf{Z}_p$ by using the topological generator γ, we may view ψ as a character on $\mathcal{G}_\infty$. Then $\psi(\gamma)$ is a primitive p^{n-1}-th root of unity. There exists a unique power series $g_\chi = g_{\chi,\gamma}$ (of Kubota-Leopoldt) such that for all ψ, we have

$$g_\chi(\psi(\gamma)-1) = -B_{1,\bar{\chi}\bar{\psi}}.$$

The Ferrero-Washington theorem is equivalent with the property that the coefficients of g_χ are not all divisible by p, and hence that

$$g_\chi(X) = c_0 + c_1X + \cdots + c_\lambda X^\lambda + \text{higher terms},$$

where $c_\nu \equiv 0 \bmod p$ for $\nu < \lambda$, and c_λ is a p-adic unit. The Weierstrass preparation theorem states that g_χ differs from a Weierstrass polynomial by a unit in $\mathbf{Z}_p[[X]]$. The following theorem is a direct consequence of the definitions and p-adic interpolation, belonging to the basic theory of p-adic L-functions due to Iwasawa.

Theorem 2.11. *The characteristic polynomial of* $\gamma - 1$ *on the co-Stickelberger module* $M(\chi)$ *is the Weierstrass polynomial of the Kubota-Leopoldt power series* $g_{\chi,\gamma}$.

Although the Mazur-Wiles theorem does not completely elucidate the module structure of $\mathcal{A}$, or at the first level of $\mathrm{Cl}^-(K_0)^{(p)}$, it is sufficient to imply consequences for the orders of these groups. We shall state such a consequence in a later section in connection with the algebraic-geometric considerations entering in its proof.

The Iwasawa-Leopoldt conjecture would be more precise than the Mazur-Wiles theorem for the classical cyclotomic tower that we have considered. It is related to the simplicity of the roots of the characteristic polynomials involved.

On the other hand, Mazur-Wiles treat more general ground fields than the rationals, namely any abelian field (a subfield of a cyclotomic field); and thereby they deal with a more general character decomposition than that of the group $\mathrm{Gal}(K_0/\mathbf{Q})$. For these more general ground fields, the analogue of the Iwasawa-Leopoldt conjecture is definitely not always true. It is still a problem, even in the most classical tower over $\mathbf{Q}$, to determine the extent to which the modules $M(\chi)$ and $\mathcal{A}(\chi)$ differ, for instance: is $\mathcal{A}(\chi)$ quasi-cyclic, or equivalently are $M(\chi)$ and $\mathcal{A}(\chi)$ quasi-isomorphic? To what extent are the characteristic roots simple?

One should not miss the importance of having these more general ground fields and characters, and I want to add a few words about that. Let F be an abelian extension of the rationals, contained in some cyclotomic field. For each prime number p, the Galois group $\mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q})$ has a finite torsion subgroup, whose fixed field Z_p is a $\mathbf{Z}_p$-extension of $\mathbf{Q}$, that is

$$\mathrm{Gal}(Z_p/\mathbf{Q}) \approx \mathbf{Z}_p.$$

Let FZ_p be the composite. Then FZ_p is called the **cyclotomic $\mathbf{Z}_p$-extension** of F. Let γ_p be a topological generator of $\mathrm{Gal}(FZ_p/F)$. For odd character χ with conductor divisible at most by the first power of p, one may form the projective limits $\mathcal{A}_{F,p}(\chi)$ and $M_{F,p}(\chi)$ as before using the appropriate generalized Bernoulli numbers. The Mazur-Wiles theorem asserts that these two Λ_p-modules have the same characteristic polynomial $f_{p,\chi}$ for $\gamma_p - 1$.

For almost all p we can make a canonical choice of γ_p. Indeed, if p is odd, then $\mathrm{Gal}(Z_p/\mathbf{Q})$ is generated by σ_{1+p}, and if $p = 2$, then by σ_{1+4}. For almost all p, F is disjoint from Z_p, so σ_{1+p} may be viewed as a generator of $\mathrm{Gal}(FZ_p/F)$. For this choice of generator one may then ask more refined questions concerning the coefficients and the roots of the characteristic polynomial, for a given character χ, or after taking a product over χ for the characteristic polynomial f_p of $\sigma_{1+p} - 1$ on $\mathbf{Q}_pM_{F,p}$. One may also ask questions concerning the behavior of f_p for varying p, for instance: are the degrees bounded as a function of p; how do they vary with p; what is the nature of the roots; what is the distribution of p for which the roots are simple; etc. Some of these questions are now being thought about by those active in the field, but nothing is known at present. This leads into the consideration of extensions of type

$$FZ_{p_1}\cdots Z_{p_t}$$

for a finite set of primes $p_1, \ldots, p_t$, and in general passing to the limit. Such extensions have recently been considered by Greenberg and Friedman following Iwasawa.

Finally, I should also emphasize that one can take much more general ground fields than abelian fields, and one can define a Stickelberger element and ideal via the zeta function instead of doing it ad hoc as we did here with Bernoulli polynomials. Cf. §8, where this will be done in a different context. Similar questions then arise for arbitrary $\mathbf{Z}_p$-extensions: we are faced with (at least) two modules, the projective limit of the ideal class group (p-primary part) and the co-Stickelberger module, so that the investigation of their relation can be posed as a problem in this generality. Cf. [**Co 1**].

§3. Modular curves

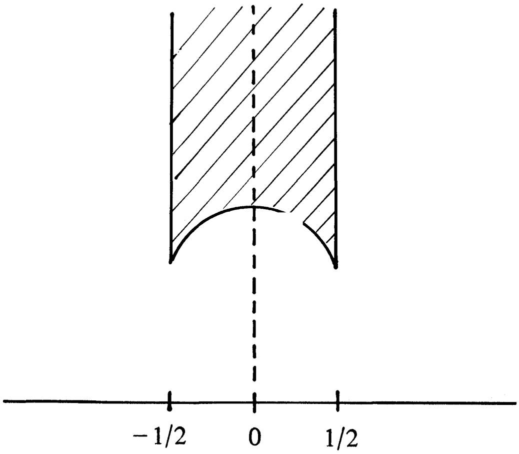
Let $\mathfrak{H}$ be the upper half plane, that is the set of complex numbers $\tau = x + iy$ with $y > 0$. Let $\Gamma(1) = SL_2(\mathbf{Z})$ be the **modular group**, that is the group of matrices

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with integer coefficients, determinant 1. Then $\Gamma(1)$ operates on $\mathfrak{H}$ by

$$\tau \mapsto \frac{a\tau + b}{c\tau + d} = \gamma(\tau),$$

and ± 1 operates trivially, so we get a faithful representation of $\Gamma(1)/\pm 1$. The coset space $\Gamma(1)\backslash\mathfrak{H}$ has a representative fundamental domain which has the well-known shape pictured below.



There is a classical function, holomorphic on $\mathfrak{H}$ and invariant under $\Gamma(1)$, called the j-function, which gives a complex analytic isomorphism

$$j : \Gamma(1)\backslash\mathfrak{H} \to \mathbf{P}^1_{\mathbf{C}} - \{\infty\}$$

with the affine line (projective one-dimensional space from which infinity is deleted). If one takes $q = e^{2\pi i\tau}$ as a local uniformizing parameter at infinity, then one can compactify $\Gamma(1)\backslash\mathfrak{H}$ by adjoining one point at infinity, thus obtaining a compact Riemann surface namely $\mathbf{P}^1_{\mathbf{C}}$. In terms of q, the function j has a Laurent expansion

$$j = \frac{1}{q} + 744 + 196884q + \text{higher terms.}$$

One can characterize j analytically by stating that $j(i) = 1728$ and $j(e^{2\pi i/3}) = 0$, while $j(\infty) = \infty$. This is rather ad hoc. A better way to conceive of j is in terms of isomorphism classes of complex toruses as follows.

Let $\Lambda = [\omega_1, \omega_2]$ be a lattice in $\mathbf{C}$, with basis ω_1, ω_2 over the integers. This means that Λ is the abelian group generated by ω_1, ω_2, and that these two elements are linearly independent over the real numbers. In addition, we shall always suppose that ω_1/ω_2 lies in the upper half plane, so we put $\omega_1/\omega_2 = \tau$. Then the invariance of j under $SL_2(\mathbf{Z})$ shows that the value $j(\tau)$ is independent of the choice of basis as above, and in addition, is the same if we replace $[\omega_1, \omega_2]$ by $[c\omega_1, c\omega_2]$ for any complex number $c \neq 0$. Thus we may define

$$j(\Lambda) = j(\tau),$$

and we have $j(c\Lambda) = j(\Lambda)$. But $\mathbf{C}/\Lambda$ is a complex torus of dimension 1, and the above arguments show that j is the single invariant for isomorphism classes of such toruses. The value 1728 is selected for usefulness in arithmetic applications. One can give many analytic expressions for j, arising from the theory of elliptic functions. For instance, associated with the lattice are the two invariants

$$g_2(\Lambda) = 60 \sum \omega^{-4} \quad \text{and} \quad g_3(\Lambda) = 140 \sum \omega^{-6},$$

where the sums are taken for $\omega \in \Lambda$, $\omega \neq 0$. Then

$$j = 1728 g_2^3/(g_2^3 - 27 g_3^2).$$

Now let Γ be a subgroup of $\Gamma(1)$, of finite index. Then $\Gamma \setminus \mathfrak{H}$ is a finite (possibly ramified) covering of $\Gamma(1) \setminus \mathfrak{H}$. We shall be specifically interested in some very special subgroups Γ, which we now describe. Let N be a positive integer. We define:

$$\Gamma(N) = \text{subgroup of elements } \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N;$$
$$\Gamma_1(N) = \text{subgroup of elements } \gamma \equiv \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \bmod N \text{ with arbitrary } b;$$
$$\Gamma_0(N) = \text{subgroup of elements } \gamma \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \bmod N \text{ with arbitrary } a, b.$$

Since $\det \gamma = 1$ and a, b, c, d are integers, we must have

$$d \equiv a^{-1} \bmod N,$$

and a, d are prime to N. It is then easily seen that

$$\Gamma_0(N)/\Gamma_1(N) \approx (\mathbf{Z}/N\mathbf{Z})^*.$$

In fact we get two exact sequences:

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

where the right hand map is reduction mod N; and

$$1 \to \Gamma_1(N) \to \Gamma_0(N) \to (\mathbf{Z}/N\mathbf{Z})^* \to 1$$

where the right hand map is the projection on $a \bmod N$.

If $\Gamma_1 \subset \Gamma_2$ then we have a covering (possibly ramified):

$$\Gamma_1 \setminus \mathfrak{H} \to \Gamma_2 \setminus \mathfrak{H}.$$

For any Γ, the projective embedding j of $\Gamma(1) \setminus \mathfrak{H}$ can be lifted to a projective embedding

$$\Gamma \setminus \mathfrak{H} \xrightarrow{f_\Gamma} \text{some projective space}$$

such that the image of f_Γ is an affine curve, denoted by $Y(\Gamma)_{\mathbf{C}}$. The coordinate functions of f_Γ can be chosen in many ways, suited for different applications, and exhibiting different properties of this affine curve, which is called a modular curve. The discussion of such functions becomes technical, and will be omitted, except that in §6 we discuss one possible generator for projective coordinates. Cf. Klein [**Kl**] and [**Ku-L 1**].

When Γ is one of the three groups defined above, then the corresponding affine curve is denoted by

$$Y(N), \quad Y_1(N), \quad Y_0(N) \text{ respectively,}$$

with the subscript **C** when we refer to the Riemann surface of its complex points. Thus we have a commutative diagram of coverings:

$$\begin{tikzcd}
\Gamma_1(N)\backslash\mathfrak{H} \arrow[r] \arrow[d] & Y_1(N)_{\mathbf{C}} \arrow[d] \\
\Gamma_0(N)\backslash\mathfrak{H} \arrow[r] & Y_0(N)_{\mathbf{C}}
\end{tikzcd}$$

To slide into the algebraic terminology, we shall speak more systematically of elliptic curves rather than complex toruses $\mathbf{C}/\Lambda$. The curves $Y_1(N)$ and $Y_0(N)$ have an interpretation as parametrizing certain isomorphism classes of objects, similar to $Y(1)$ (that is $\Gamma(1)\backslash\mathfrak{H}$) parametrizing isomorphism classes of elliptic curves, as follows:

$Y_0(N)$ parametrizes isomorphism classes of pairs (A, Z), where A is an elliptic curve (complex torus) and Z is a cyclic subgroup of order N.

$Y_1(N)$ parametrizes isomorphism classes of pairs (A, P), where A is an elliptic curve and P is a point of order exactly N.

In terms of the analytic objects, if $A = \mathbf{C}/[\tau, 1]$, we take P to be the point represented by $1/N$, and we take Z to be the subgroup generated by P. The invariance under the groups $\Gamma_0(N)$ and $\Gamma_1(N)$ gives the bijection between $\Gamma_0(N)\backslash\mathfrak{H}$ resp. $\Gamma_1(N)\backslash\mathfrak{H}$ and isomorphism classes of pairs as stated above.

However, using the algebraic language and formulation has one advantage: it can be used in an arithmetic context, because relative to a suitable choice of coordinatization, the curves $Y_1(N)$ and $Y_0(N)$ are defined over the rational numbers.

In terms of the above representation, the covering map $Y_1(N) \to Y_0(N)$ associates to each pair (A, P) the pair (A, Z) where Z is the cyclic group generated by P.

Now let us look at the points at infinity.

The affine curve $Y(\Gamma)$ can be compactified, and the points in the inverse image of ∞ on the j-line are called the **points at infinity**, or the **cusps**. The projective curve consisting of $Y(\Gamma)$ and the points at infinity is denoted by $X(\Gamma)$. Thus we have

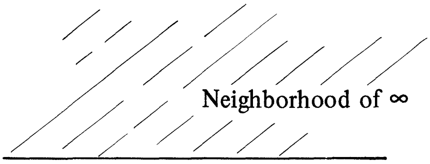
$$X(\Gamma) = Y(\Gamma) \cup X^\infty(\Gamma)$$

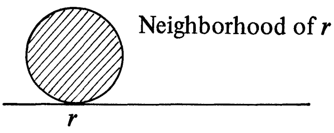
where $X^\infty(\Gamma)$ is the set of cusps.

The cusps have a simple model as follows. Let

$$\mathfrak{H}^* = \mathfrak{H} \cup \mathbf{Q} \cup \{\infty\}.$$

Then $SL_2(\mathbf{Z})$ operates on $\mathbf{Q} \cup \{\infty\}$. One can give a topology and complex analytic structure to $\mathfrak{H}^*$ such that $\Gamma \setminus \mathfrak{H}^*$ is a compact Riemann surface. A typical neighborhood of a rational number r is a disc in the upper half plane tangent to r; and a typical neighborhood of ∞ is the part of the upper half plane lying above a horizontal line, as shown in the figure.





Then $X^{\infty}(\Gamma)$ is the set of equivalence classes of $\mathbf{Q} \cup \{\infty\}$ with respect to the action of Γ.

Again, when Γ is one of the three special subgroups defined above, the corresponding projective curve is denoted by

$$X(N), \quad X_1(N), \quad X_0(N) \text{ respectively.}$$

The (ramified) covering $Y_1(N) \to Y_0(N)$ extends to a (ramified) covering

$$X_1(N) \to X_0(N).$$

If, as before, we let $G \approx (\mathbf{Z}/N\mathbf{Z})^*$, then this covering has a group of covering transformations $G/\pm 1$, under the association

$$a \mapsto \gamma_a$$

where γ_a is any element of $\Gamma_0(N)$ satisfying

$$\gamma_a \equiv \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \bmod N.$$

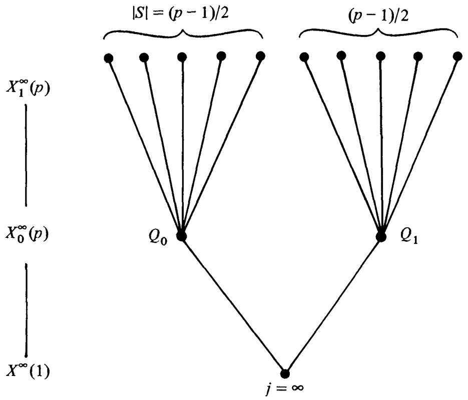
Now take $N = p$ *prime* ≥ 3. It turns out first that there are precisely two cusps on $X_0(N)$ lying above $j = \infty$. The degree of the covering is given by

$$[X_1(N) : X_0(N)] = \frac{N-1}{2},$$

and it is easily seen that the covering is unramified over the cusps. Therefore, if we denote by Q_0 and Q_1 the two cusps of $X_0(N)$, then there are precisely $(N-1)/2$ distinct points on $X_1(N)$ lying above each of these two points. We now let:

$$S = \text{set of } (N-1)/2 \text{ points on } X_1(N) \text{ lying above } Q_0.$$

We take this as a particularly interesting set of points at infinity, according to the general situations mentioned in the introductory remarks. More precisely, Q_0 and the set of points in S are chosen to be the rational cusps (rational points in $\mathbf{Q}$).



Just as in the case of ideal classes, we seek all relations in the cuspidal divisor class groups $\mathcal{C}^\infty(\Gamma) = \mathrm{Pic}^\infty(X(\Gamma))$ for the Γ introduced above. The finiteness of this group was originally proved by Manin-Drinfeld [**Dr**], but the investigation of its structure in more explicit form was begun and carried out in the Kubert-Lang series of papers. Cf. also [**Ku-L 1**]. Here we shall limit ourselves to describing some results from that series which give a striking analogy with the cyclotomic case, and lead into the deeper connections established subsequently by Wiles and Mazur-Wiles. These results pertain to the group $\mathcal{C}_1^S(N)$ for N prime, where $\mathcal{C}_1^S(N) = \mathrm{Pic}^S(X_1(N))$.

We are dealing again with the group ring $\mathbf{Z}[G]$, or rather $\mathbf{Z}[G/\pm 1]$. Let

$$\mathbf{B}_2(x) = x^2 - x + \frac{1}{6}$$

be the **second Bernoulli polynomial**. Note that $\mathbf{B}_2(1-x) = \mathbf{B}_2(x)$ for $0 \leq x \leq 1$. We let

$$\theta^{(2)} = N \sum_{a \in \mathbf{Z}(N)^*/\pm 1} \frac{1}{2}\mathbf{B}_2\left(\left\langle \frac{a}{N} \right\rangle\right)\sigma_a^{-1}$$

be the **Stickelberger element of order** 2. Let:

$I^{(2)}=$ ideal of $\mathbf{Z}[G/\pm 1]$ generated by the elements $\sigma_c - c^2$ with c prime to $6N$.

$R=\mathbf{Z}[G/\pm 1]=$ the group ring.

$R_0=$ ideal of elements in R of degree 0, and $I_0=I\cap R_0$.

We let the **Stickelberger ideal** $S^{(2)}$ be the ideal

$$S^{(2)}=R\theta^{(2)}\cap R_0=I_0^{(2)}\theta^{(2)},$$

and we then get the **co-Stickelberger module** $R_0/S^{(2)}$. For the rest of this section we omit the superscripts (2) since we deal only with them. Otherwise, we have to have a notation to distinguish the present situation from that dealing with the first Bernoulli polynomials.

Theorem 3.1. (i) *There is a natural isomorphism*

$$R_0/S\approx C_1^S(N).$$

(ii) *We have the class number formula*

$$(R_0:S)=N\prod_{\chi\neq 1}\pm\frac{1}{2}B_{2,\chi}$$

where

$$B_{2,\chi}=N\sum_a \mathbf{B}_2\left(\left\langle\frac{a}{N}\right\rangle\right)\chi(a).$$

Here χ ranges over the characters of $(\mathbf{Z}/N\mathbf{Z})^*/\pm 1$, or what is the same, the even characters of $(\mathbf{Z}/N\mathbf{Z})^*$.

When N is a prime power, the situation is somewhat more complicated, since the Stickelberger ideal needs to be refined, cf. the [**Ku-L**] series; and when N is composite, Jing Yu [**Yu**] has applied the Sinnott methods to get corresponding structure theorems for $C_1^S(N)$ and $C^\infty(N)$.

It is at the moment a problem to give similar geometric interpretations for the co-Stickelberger module formed with the higher degree Bernoulli polynomials, defined by the generating series

$$\frac{te^{tX}}{e^t-1}=\sum\mathbf{B}_k(X)\frac{t^k}{k!}.$$

Cf. Kubert-Lang, as in [**L 1**], Chapter 2 and Bergelson [**Be**] for purely algebraic index computations of Stickelberger ideals involving such polynomials.

The proof of Theorem 3.1 is done by a complete characterization of the group of functions (modulo constants) which have zeros and poles only at the cusps, or in the set S as stated above. Such functions can be constructed explicitly in terms of "modular forms", but such a discussion gets more technical and we wish to proceed with our general survey rather than go into these more elaborate constructions.

In any case, what was Conjecture 2 in the cyclotomic theory is a theorem in the context of the cuspidal divisor class group on the modular curve. The analogue of the theorem on eigenspces, namely the analogue of Theorem 2.7, is then true not only for the group ring modulo the Stickelberger ideal, but for the cuspidal group itself. We suppose that $p\geq 5$.

Theorem 3.2. *Let χ be an even character of G and let*

$$M = \mathbf{Z}_p[G]_0/S_p^{(2)} \quad \textit{where } S_p^{(2)} = \mathbf{Z}_p S^{(2)}.$$

Then

$$C_1^S(p)^{(p)} \approx M,$$

and we have the following eigenspace descriptions.

(i) *If χ is trivial, or $\chi = \omega^2$ then $M(\chi) = 0$.*

(ii) *If $\chi \neq 1$ and $\chi \neq \omega^2$ then*

$$M(\chi) \approx \mathbf{Z}_p/B_{2,\bar{\chi}}\mathbf{Z}_p,$$

so this group is cyclic of order $p^{n(\chi)}$, where $n(\chi) = \operatorname{ord}_p B_{2,\bar{\chi}}$.

§4. The Wiles and Mazur-Wiles connection

So far, we have described two analogous theories. The possibility that the geometric theory would affect the cyclotomic theory was immediately apparent (cf. [**L 1**], p. 53), but it was Wiles who first showed precisely how this connection would come about, following work of Ribet. The situation is now going to get more complicated, and we have to expand very considerably the range of notions which intervene.

We are concerned with the p-primary component of the group of ideal classes in $\mathbf{Q}(\boldsymbol{\mu}_p)$, say; by class field theory this corresponds to an abelian unramified extension. Can one obtain this extension "geometrically", by means of certain finite groups on appropriately selected Jacobians of curves as in the introduction? Indeed, let us go back to Theorem 2.10, which implies a conjectural existence of a certain abelian unramified extension of $K = \mathbf{Q}(\boldsymbol{\mu}_p)$, of order p^m where

$$m = m(\chi) = \operatorname{ord}_p B_{1,\bar{\chi}},$$

for $\chi \neq \omega$. Ribet [**Ri**] proved that if p divides $B_{1,\bar{\chi}}$, then there exists a cyclic unramified abelian extension of degree p, of the appropriate character, so that p divides $|C^{-(p)}(\chi)|$.

He introduced the theory of modular functions, and especially the curve $X_1(p)$, via a fundamental theorem of Shimura [**Sh 1**], Theorem 7.14. Ribet showed that by selecting an appropriate finite subgroup of torsion points in a quotient of the Jacobian $J_1(p)$ of $X_1(p)$, he could generate a cyclic extension of degree p,

$$\mathbf{Q}(\boldsymbol{\mu}_p)(\mathfrak{g}),$$

by adjoining the coordinates of the points in this group. However, more has now been proved:

Theorem 4.1. *Suppose that χ is an odd character, and $\chi \neq \omega, \chi \neq \bar{\omega}$. Then the order of $C^{-(p)}(\chi)$ is exactly $p^{m(\chi)}$.*

With the additional hypothesis that $C^{-(p)}(\chi)$ is cyclic, this theorem was proved by Wiles [**Wi**]. By an extension of the methods, it was proved as stated by Mazur-Wiles [**Ma-W**]. These methods link the algebraic geometry of the modular curves in §2 with the arithmetic of the cyclotomic fields, and are based extensively on deep, original and far reaching results of Mazur concerning the arithmetic properties of these modular curves and their Jacobians, via his theory of the "Eisenstein ideal" in [**Ma 1**]. I am going to try to explain how this comes about, following the introduction and first section of Wiles' paper [**Wi**].

Note that if χ is an odd character $\neq \omega$, $\neq \bar{\omega}$, then $\chi\omega$ is an even character $\neq 1$, ω^2. Let Z be the cyclic cuspidal group

$$Z = C_1^S(p)(\chi\omega)^{(p)} \approx \mathbf{Z}_p/B_{2,\overline{\chi\omega}}\mathbf{Z}_p.$$

In other words, Z is the p-primary part of the cuspidal group on $X_1(p)$, with support in the set of cusps S described in §2, and forming the $\chi\omega$-eigenspace. The algebra of endomorphisms of $J_1(p)$ contains a subalgebra $\mathbf{T}$, called the **Hecke algebra**, which we shall describe very briefly below. For purposes of this section, the Hecke algebra $\mathbf{T}$ is assumed to have coefficients in $\mathbf{Z}_p$.

Theorem 4.2. *Let χ be an odd character $\neq \omega$, $\neq \bar{\omega}$. Let $\mathbf{I}_{\chi\omega} = \mathbf{I}$ be the ideal in $\mathbf{T}$ annihilating the cyclic group Z above, and let $\mathfrak{g}$ be the finite group of zeros of $\mathbf{I}$ in $J_1(p)$, namely the group of points $x \in J_1(p)$ such that $\mathbf{I}x = 0$. Let $p^n = |Z|$ be the order of Z. Then*

$$\mathbf{Q}(\boldsymbol{\mu}_{p^n})(\mathfrak{g})$$

is an unramified abelian extension of $\mathbf{Q}(\boldsymbol{\mu}_{p^n})$, of degree p^n.

This theorem describes how to construct certain abelian unramified extensions by means of torsion points on the Jacobian of the modular curve. Even though Z is a cuspidal group, $\mathfrak{g}$ is not. Note that Theorem 4.2 constructs an abelian extension of $\mathbf{Q}(\boldsymbol{\mu}_{p^n})$ but not of $\mathbf{Q}(\boldsymbol{\mu}_p)$, which is what we wanted in the first place. Thus it is still a complicated matter to "descend" the above construction back to $\mathbf{Q}(\boldsymbol{\mu}_p)$. The matter is sufficiently complicated that I shall limit myself to describe in general terms what is done in the papers of Wiles and Mazur. This involves the following steps.

(i) For arbitrary "levels", that is for arbitrary curves $X_1(p^\nu)$ and appropriate cuspidal divisor class groups, construct abelian unramified extensions of cyclotomic fields $\mathbf{Q}(\boldsymbol{\mu}_{p^n})$ with suitable, and arbitrarily large prime powers p^n, in a way similar to the construction of Theorem 4.2.

(ii) Express the limiting result (injective limit or projective limit) in the category of continuous modules over the Galois group $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^\infty})/\mathbf{Q}(\boldsymbol{\mu}_p))$; or alternatively of modules over the "Iwasawa algebra", equal to the projective limit of the group rings formed at finite levels, namely

$$\Lambda = \lim \mathbf{Z}_p[\mathcal{G}_n]$$

where $\mathcal{G}_n = \mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_{p^{n+1}})/\mathbf{Q}(\boldsymbol{\mu}_p))$; and do this for the eigenspaces relative to the characters of $\mathrm{Gal}(\mathbf{Q}(\boldsymbol{\mu}_p)/\mathbf{Q})$, as in §2.

(iii) Elaborate the algebraic theory of the "twist" which allows one to shift from eigencomponents of even characters, arising from the algebraic geometry, to the odd characters arising from the ideal-class-group theory; and follow this twist by taking Galois invariants to recover the structure (as far as possible) of the ideal class group of $\mathbf{Q}(\boldsymbol{\mu}_p)$. See [**L 1**], Chapter 2, §7; and [**Ma-W**], as well as the end of [**Wi**], p. 33 where Wiles goes from "p^n" to "p^m".

For these lectures, I preferred to emphasize the connection between the algebraic number theory and the algebraic geometry; and to give the flavor of the geometric construction used to obtain unramified abelian extensions of cyclotomic fields, rather than to enter into the relatively heavy algebra needed to describe more precisely the above three steps, except for the last part of §2.

We finish this section with a few words concerning the Hecke algebra. It is generated by endomorphisms denoted T_l (for $l \neq p$), $U_p, \langle a \rangle$ (for a prime to p), and w_ς. Their descriptions can be given in various contexts, especially as correspondences on the modular curve $X_1(p)$, whose points are viewed as pairs (E, P) where E is an elliptic curve, and P is a point of order p; or in analytic terms, as function of the variable τ in the upper half plane. To keep this discussion brief, we use the first context.

T_l is the correspondence

$$(E,P) \mapsto \sum_B (E/B, (P+B)/B)$$

which to each pair (E, P) associates the formal sum shown above, taken over all subgroups B of order l in E.

U_p is the correspondence

$$(E,P) \mapsto \sum_B (E/B, (P+B)/B)$$

where the sum is now taken over the subgroups of order p but unequal to the subgroup generated by P itself.

$\langle a \rangle$, for an integer in $(\mathbf{Z}/p\mathbf{Z})^*$, is the correspondence

$$(E,P) \mapsto (E, aP).$$

Finally, to describe w_ς, one needs to know that there is a canonical pairing

$$e_p : E_p \times E_p \to \boldsymbol{\mu}_p,$$

which makes E_p self dual, and is alternating. Fix a primitive p-th root of unity ς. To each point P of order p, we let P' be a point (well determined in $E/(P)$ by the alternating property) such that

$$e_p(P, P') = \varsigma.$$

Then w_ς is the correspondence such that

$$(E,P) \mapsto (E/(P), P').$$

Mazur [**Ma 1**] had studied extensively this algebra in relation to the cuspidal points on $X_0(p)$. By extending this study to $X_1(p)$, Wiles was led to his theorems, subsequently completed and extended by Mazur-Wiles.

For the convenience of the reader, I also give explicitly generators for the ideal $\mathbf{I}_{\chi\omega}$ (the Eisenstein ideal, better called the $(S, \chi\omega)$-**cuspidal ideal.**)

Theorem 4.3. *Let χ be an odd character $\neq \omega$, $\neq \bar{\omega}$. Then the cuspidal ideal $\mathbf{I}_{\chi\omega}$ of Theorem 4.2 is generated by the elements*

$$T_l - (1 + l\langle l\rangle), \quad U_p - 1, \quad \langle a\rangle - \chi\omega(a), \quad p^n$$

where p^n is the exact power of p dividing $B_{2,\overline{\chi\omega}}$.

Remark. The above generators for the cuspidal ideal correspond to the choice of rational cusps which we have made, and is therefore a slight variation of the choice made in [**Wi**] relative to the other set of cusps lying above Q_1.

The situation is obviously deep and complicated. I want to emphasize that the techniques and ideas used to solve certain concrete classical problems bring out the full panoply of commutative algebra-algebraic geometry over rings of Grothendieck and his school, put to work in concrete contexts (especially of modular curves). In particular, to show that extensions obtained by adjoining coordinates of certain torsion points are unramified, one needs the general theory of commutative group schemes of Oort-Tate and Raynaud [**O-T**], [**Ray**]; the general theory of modular schemes over **Z**, as in Deligne-Rapoport [**De-Rap**]; all based extensively on assorted EGA and SGA to the tune of several thousand pages, cf. for instance the bibliography at the end of Wiles' paper listing four of these volumes. Not only that, but Mazur-Wiles also use the Langlands Antwerp paper [**Lgds**] based on representation theory-trace formula techniques to be able to handle the ramification for $J_1(p^\nu)$ for arbitrarily large powers p^ν. However, the applicability of these last techniques is itself based on a good understanding of the algebraic geometry of the various moduli schemes involved. The appeal to representation theory can be replaced by a direct appeal to the work of Katz-Mazur [**Ka-M**] on these moduli schemes.

My listing of the above items is not meant to discourage anyone from reading the Mazur-Wiles papers. I merely did not want to hide what was involved. However, it should also be understood that few people have a complete grasp of all the elements put together by Mazur-Wiles. Some people may have the ability to take much for granted; to make just the right selection of items culled from more extensive works, and be comfortable with this selection; and to develop their intuition from carefully worked out special cases, for instance $X_0(37)$ and $X_1(37)$. To each his own.

§5. Geometric class field theory

It is possible to give a geometric context for some problems of class field theory. I shall select here a special case which can be easily formulated, and I follow a joint paper with Katz [**Ka-L**]. (For varieties over finite fields, cf. [**L 4**] and [**L 5**].) Although [**Ka-L**] deals with varieties in general, I limit myself to curves here for simplicity of language. (In higher dimensions, the Jacobian must be replaced by the Albanese variety or its dual.)

Let X be a projective non-singular curve defined over a number field k. Unramified coverings of X are usually defined over an algebraic extension of k. One may ask for those which are defined over k, and which, furthermore, are abelian over k: the elements of the group of covering transformations are defined over k also. The following theorem is an analogue of the finiteness of the class number.

Theorem 5.1. *Let x_0 be a rational point of X in k. There exists a maximal abelian unramified covering*

$$\pi : X' \to X,$$

also defined over k, such that x_0 splits completely in the covering, that is $\pi^{-1}(x_0)$ consists of d distinct k-rational points, where $d = [X' : X]$ is the degree of the covering.

Note that implicit in the statement of Theorem 5.1 is the fact that the maximal abelian unramified covering in which x_0 splits completely is actually finite. The proof is done by reducing mod good primes, to the case of curves over finite fields, where the situation is known by more classical class field theory.

We can generalize the notion of covering to include constant field extensions of k, which are then regarded as "unramified" over k. Then from **[Ka-L]** we have:

Theorem 5.2. *The maximal abelian unramified covering of $k(X)$ is the composite of the maximal abelian extension k^{ab} of k and the geometric covering whose existence is asserted in Theorem* 5.1.

This geometric covering is in fact obtained by pull-back from the Jacobian: there exists a corresponding covering $J' \to J$ of the Jacobian of X, defined over k, such that X' is the pull-back of J':

$$\begin{tikzcd}
X' \arrow[r] \arrow[d] & J' \arrow[d] \\
X \arrow[r] & J.
\end{tikzcd}$$

In the canonical map of X in J, the point x_0 is assumed to map on the origin of J which splits completely in J'. Thus the problem of determining unramified abelian extension of X is reduced to the same problem over the Jacobian. The group of covering transformations $\mathrm{Aut}(J'/J)$ can be identified with a group of translations by rational points of J' in k; that is an element $T \in \mathrm{Aut}(J'/J)$ acts as T_a for some $a \in J'_{\mathrm{tor}}(k)$, where

$$T_a(y) = y + a.$$

Then J can be viewed as the quotient of J' by a finite subgroup $\mathfrak{g} \subset J'(k)$ of k-rational points of J'.

By an elementary duality, the group of rational points on a covering J' of J correspond to a certain group on J itself as follows. Let $x \in J_N$ be a point of order N on J, rational over some finite extension of k. Let k^{a} denote the algebraic closure of k (the field of all algebraic numbers), and $\mathrm{Gal}(k^{\mathrm{a}}/k) = G_k$ the Galois group of k^{a} over k. We shall say that x is a **μ-point** if the cyclic group generated by x is G_k-isomorphic to the group μ_N of all N-th roots of unity. In particular, x is rational over $k(\mu_N)$. A finite subgroup of J is called a **μ-group** if all its points are μ-points. Then it can be shown by duality that finite k-rational subgroups of points on a covering J' of J as above are in bijection with μ-groups on J.

Theorem 5.3. *The maximal μ-subgroup is finite.*

This statement is equivalent with the finiteness of the maximal geometric unramified abelian covering of J (or X) over k, and follows from Theorem 5.1. This led to the conjecture that not only is the maximal μ-subgroup finite, but so is the group of torsion points of J in the maximal cyclotomic extension of k. This conjecture was proved in [**Ka-L**] in the case of complex multiplication, and was extended to the general case by Ribet (see the appendix to [**Ka-L**]). Since Theorem 5.3 can thus be proved ab ovo, it provides an alternative proof for the finiteness of the maximal covering in Theorem 5.1.

For each curve X it is then interesting to determine precisely the nature of this maximal μ-type group, especially for the modular curves which have proved so important in other contexts. Let us return to the ramified covering

$$X_1(p) \to X_0(p)$$

discussed in §3. It is cyclic of degree $(p-1)/2$. Let

$$n = \text{numerator of } \frac{p-1}{12}.$$

Let G be the group of covering transformations. Then G has a unique factor group of order n, which corresponds to an intermediate covering denoted by $X_2(p)$, so $X_1(p) \to X_2(p)$ is cyclic of degree $(p-1)/2n$, and the covering

$$\pi : X_2(p) \to X_0(p),$$

which is cyclic of degree n, is called the **Shimura covering**. Mazur had determined the maximal μ-subgroup of $J_0(p)$ in [**Ma 1**]. In the general framework of [**Ka-L**], this was interpreted as an explicit determination for $X_0(p)$ of the notion arising in Theorem 5.1:

Theorem 5.4. *The Shimura covering is the maximal abelian unramified covering of $X_0(p)$, defined over* $\mathbf{Q}$, *in which the rational cusp at infinity splits completely.*

On the other hand, one may consider models for $X_0(p)$ (or an arbitrary curve X) over the ring of integers of k. For the modular scheme as above, it is remarked in [**Ka-L**] that there is total ramification over one of the components at p, and therefore that scheme-theoretically, there is no unramified covering as in Theorem 5.4. One may also ask for the decomposition laws of "primes"–in this case, maximal ideals locally, in rings of dimension 2–in such coverings. Such decomposition laws would amount to higher dimensional "reciprocity laws", cf. [**L 4**] and [**L 5**], where the problem is raised in a general context of schemes over the integers (not yet called by that name). For instance in [**L 5**] I pointed out the surjectivity of the reciprocity law mapping from 0-cycles of the base space into the Galois group. Recently, Spencer Bloch [**B**] has made a great advance in this direction, by discovering how to formulate such laws for curves having everywhere non-degenerate reduction, following work of Kato [**Kato**] and Parshin [**Pa**]. Bloch formulates the decomposition laws in terms of the K-group of the base space. It remains to extend his results to more general cases (the modular curves have degenerate reduction at p, for instance), and to make his results explicit in the case of the modular curves. In any case, the maximal μ-subgroup can then be interpreted as a "class number", the number of classes being those in a suitable group of K-theory, in the unramified case of Bloch, and ultimately in the ramified case with conductor.

§6. Modular units

In this section, we describe briefly how one constructs the units in the modular function field, i.e. the meromorphic functions on $X(N)$ which have zeros and poles only at the points at infinity. We then show how one obtains units in the rings of integers in abelian extensions of imaginary quadratic fields.

(a) The function field

First consider an arbitrary lattice Λ in the complex plane $\mathbf{C}$. Then $\mathbf{C}/\Lambda$ is a complex torus, of complex dimension 1, real dimension 2. It admits a projective embedding in the projective plane, by means of the classical Weierstrass $\wp$-function and its derivative, which provide affine coordinates:

$$z \mapsto (\wp(z), \wp'(z)),$$

where

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \neq 0} \left[\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right],$$

$$\wp'(z) = \sum_{\omega} \frac{-2}{(z-\omega)^3}$$

and the sums are taken for $\omega \in \Lambda$, or $\omega \neq 0$ as indicated. The series for the $\wp$-function is concocted so as to make $\wp$ periodic with respect to Λ, and to insure convergence. Lattice points go to the point at infinity. If we put $x = \wp(z)$ and $y = \wp'(z)$, then

$$y^2 = 4x^3 - g_2 x - g_3,$$

where g_2, g_3 were already mentioned in §3.

We shall describe another type of projective coordinate.

First, we want an entire function which has a zero of order 1 at each lattice point and no other zero. The simplest normalization is that of the **sigma function** of Weierstrass,

$$\sigma(z,\Lambda) = z \prod_{\omega\neq 0}\left(1-\frac{z}{\omega}\right)\exp\left(\frac{z}{\omega}+\frac{1}{2}\left(\frac{z}{\omega}\right)^2\right).$$

We then define the **Weierstrass zeta function** to be the logarithmic derivative

$$\zeta(z,\Lambda) = \sigma'/\sigma(z,\Lambda).$$

This function has the property that for any period $\omega \in \Lambda$ we have

$$\zeta(z+\omega,\Lambda) - \zeta(z,\Lambda) = \eta(\omega,\Lambda),$$

where $\eta(z,\Lambda)$ is a function which is **R**-linear in the variable z, and homogeneous of degree —1 in the pair (z,Λ), that is

$$\eta(cz,c\Lambda) = c^{-1}\eta(z,\Lambda) \quad \text{for } c \in \mathbf{C},\ c \neq 0.$$

We then define the **Klein form**

$$\mathfrak{k}(z,\Lambda) = e^{-\eta(z,\Lambda)z/2}\sigma(z,\Lambda),$$

which is homogeneous of degree 1 in (z,Λ). This function will be used to parametrize algebraic numbers analogous to the cyclotomic numbers $e^{2\pi iz}-1$ when z ranges over division values of the lattice: rational multiples of $2\pi i$ in the cyclotomic case; rational multiples of elements in Λ in the elliptic case. Note that $\mathfrak{k}(z,\Lambda)$ is not holomorphic in z.

We recall that

$$\Delta = g_2^3 - 27g_3^2.$$

There is a natural 12th root, which is also denoted by $\eta(\tau)$, as a function of a variable in the upper half plane, and is called the **Dedekind** eta function (not to be confused with the Weierstrass eta function introduced above). The Dedekind eta function has a q-expansion given by the product

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

where as before, $q = e^{2\pi i\tau}$. Let ω_1, ω_2 be a basis for the lattice Λ over the integers **Z**. Then we can write any complex number z as a linear combination

$$z = a_1\omega_1 + a_2\omega_2,$$

with real numbers a_1, a_2. We let $a = (a_1, a_2)$ be a pair in $\mathbf{Q}^2$, and we suppose that $a \notin \mathbf{Z}^2$. We define the function

$$g_a(\tau) = \eta(\tau)^2 \mathfrak{k}_a(\tau),$$

where

$$\mathfrak{k}_a(\tau) = \mathfrak{k}(a_1\tau + a_2, [\tau, 1])$$

and $[\tau, 1]$ is the lattice generated by τ and 1 over the integers. Then g_a is a meromorphic function on $X(2N^2)$ if

$$a \in \frac{1}{N}\mathbf{Z}^2 \quad \text{but } a \notin \mathbf{Z}^2.$$

In [**Ku-L 1**] all the modular units are shown to be suitable power products of these functions g_a, which have zeros and poles only at the points at infinity, and one can describe precisely which power products have exact level N, that is, are invariant under the group of automorphisms $\Gamma(N)$ (or $\Gamma_1(N)$ for that matter). This precise determination leads to the structure of the cuspidal divisor class group $\mathcal{C}_1^S(N)$ mentioned in §3.

(b) Fields of complex multiplication

Ever since the last century, it has been realized that abelian extensions of an imaginary quadratic field behave in a manner analogous to that of cyclotomic fields over the rationals, and basic theorems of class field theory were known in this case before they were known over arbitrary number fields. The reason for this was that one has explicit algebraic and analytic parametrizations for such abelian extensions. I shall summarize some aspects and concentrate on a selection of problems fitting into the general pattern considered in these lectures.

Suppose that K is an imaginary quadratic field, say $K = \mathbf{Q}(\sqrt{-D})$ where D is a positive integer, assumed square free, and let $\mathfrak{o} = \mathfrak{o}_K$ be the ring of algebraic integers in K. For example, if $K = \mathbf{Q}(\sqrt{-1})$, then $\mathfrak{o} = \mathbf{Z}[i]$. If $K = \mathbf{Q}(\sqrt{-3})$, then $\mathfrak{o} = \mathbf{Z}[\mu_3]$. Take $\Lambda = \mathfrak{o}$. Then $\mathbf{C}/\mathfrak{o}$ admits as endomorphisms multiplication by elements of $\mathfrak{o}$. Indeed, if $\alpha \in \mathfrak{o}$, then $\alpha\mathfrak{o} \subset \mathfrak{o}$ so we get an induced map

$$\alpha : \mathbf{C}/\mathfrak{o} \to \mathbf{C}/\mathfrak{o}$$

sending $z \mapsto \alpha z (\operatorname{mod} \mathfrak{o})$. More generally, if $\mathfrak{a}$ is any (non zero) ideal of $\mathfrak{o}, \mathbf{C}/\mathfrak{a}$ again admits endomorphisms as above. We shall refer to the case when Λ is equal to such an ideal as the **complex multiplication** case.

In the two special cases of $\mathbf{Q}(i)$ and $\mathbf{Q}(\sqrt{-3})$ mentioned above, the ring of endomorphisms is generated by automorphisms of the curve. For instance,

$$y^2 = x^3 + ax$$

admits as automorphism $(x, y) \mapsto (-x, iy)$; while the curve

$$y^2 = x^3 + b$$

admits as automorphism $(x, y) \mapsto (\varsigma x, y)$ where $\varsigma^3 = 1$.

The values $\wp(z)$ and $\wp'(z)$ generate an abelian extension of $K(g_2, g_3)$ when z is a point of finite period with respect to $\mathfrak{a}$, or equivalently stated, when z is a torsion point in $\mathbf{C}/\mathfrak{a}$. However, the coordinates given by the Weierstrass functions are defined by means of "additive" expressions (just look at the series) and are inappropriate for the construction of units in abelian extensions of K. For that purpose, one has to use the Klein forms.

We must summarize some facts about ramified abelian extensions of K. Let $\mathfrak{f}$ be an ideal $\neq \mathfrak{o}$. There is a unique abelian extension $K(\mathfrak{f})$ of K, characterized by the following property. A prime ideal $\mathfrak{p}$ of K, $\mathfrak{p} \nmid \mathfrak{f}$, splits completely in $K(\mathfrak{f})$ if and only if $\mathfrak{p}$ is principal, $\mathfrak{p} = (\alpha)$, and a generator α (a priori determined only up to a unit of $\mathfrak{o}_K$) exists which satisfies $\alpha \equiv 1 \bmod \mathfrak{f}$. This extension $K(\mathfrak{f})$ is called the **ray class field**, of **conductor** $\mathfrak{f}$. "Split completely" in the present case means that if $\mathfrak{O}$ is the ring of algebraic integers in $K(\mathfrak{f})$, then $\mathfrak{p}\mathfrak{O}$ decomposes into a product of $[K(\mathfrak{f}) : K]$ distinct prime ideals:

$$\mathfrak{p}\mathfrak{O} = \mathfrak{P}_1 \cdots \mathfrak{P}_r \quad \text{where } r = [K(\mathfrak{f}) : K].$$

We are going to define a group of units in $K(\mathfrak{f})$ analogous to the cyclotomic units in $\mathbf{Q}(\boldsymbol{\mu}_N)$.

Although their origin lies in Kronecker's limit formula, the construction of such units was revived and extended in Siegel's Tata Institute Notes [**Sie**], and in the subsequent paper of Ramachandra [**Ra**]. A key step forward was made by Robert [**Ro 1**], who saw how to enlarge the known group by taking roots, so that the index of this unit group in the group of all units in the prime power case became essentially equal to the class number of $K(\mathfrak{f})$, (up to relatively large powers of 2 and 3) in analogy to the formula relating h^+ and E/E_{cyc} in the cyclotomic case. Here we shall follow the procedure developed by Kersey, Kubert and myself. See [**Ku-L**], Chapters 12 and 13, as well as [**Ke 2**].

Let $\mathbf{I}$ be the free abelian group on the ideals, so an element $\mathbf{a}$ of $\mathbf{I}$ can be written as a formal linear combination

$$\mathbf{a} = \sum n(\mathfrak{a})\mathfrak{a}$$

with integer coefficients $n(\mathfrak{a})$, almost all of which are equal to 0. Given $\mathfrak{f}$, and such $\mathbf{a}$ so that if $n(\mathfrak{a}) \neq 0$ then $\mathfrak{f}$ does not divide $\mathfrak{a}$, we define

$$\mathfrak{k}_{\mathfrak{f}}(\mathbf{a}) = \prod_{\mathfrak{a}} \mathfrak{k}(1, \mathfrak{f}\mathfrak{a}^{-1})^{n(\mathfrak{a})}.$$

This is an analogue to the cyclotomic numbers $\prod(\mathbf{e}(a/f) - 1)^{n(a)}$, but in order to obtain the "right" algebraic numbers, we have to impose some conditions. Let the degree of $\mathbf{a}$ be

$$\deg \mathbf{a} = \sum n(\mathfrak{a}).$$

We shall always require that $\deg \mathbf{a} \equiv 0 \bmod w$, where w is the number of roots of unity in K. Let $N(\mathfrak{f})$ be the smallest positive integer lying in $\mathfrak{f}$. The most important condition that we require is that

$$\sum n(\mathfrak{a})\mathbf{N}\mathfrak{a} \equiv 0 \bmod N(\mathfrak{f}).$$

As usual in number theory, $\mathbf{N}\mathfrak{a}$ denotes the absolute norm of $\mathfrak{a}$, namely the index $(\mathfrak{o} : \mathfrak{a})$. In addition to that, we require additional technical conditions to take care of problems with the prime 2 which we do not make explicit here. The abelian group generated by elements $\mathbf{a}$ satisfying these conditions is denoted by $\mathbf{I}_w(\mathfrak{f})$.

In addition to a formal linear combination $\mathbf{a}$ as above, we require other similar elements as follows. Let:

$S =$ a finite set of primes $\mathfrak{p}$ relatively prime to 6,

$R(\mathfrak{p}) =$ a set of representatives for $(\mathfrak{o}/\mathfrak{p})^*/\mathfrak{o}^*$;

for each $\mathfrak{p} \in S$ let $\mathbf{a}_\mathfrak{p} \in \mathbf{I}_w(\mathfrak{p})$.

If $\alpha \in \mathfrak{o}$ and $\mathbf{a}_\mathfrak{p} = \sum n_\mathfrak{p}(\mathfrak{a})\mathfrak{a}$, we denote $\alpha\mathbf{a}_\mathfrak{p} = \sum n_\mathfrak{p}(\mathfrak{a})(\alpha\mathfrak{a})$. Let

$$\beta = \mathfrak{k}_\mathfrak{f}(\mathbf{a}) \prod_{\mathfrak{p}\in S} \prod_{\alpha\in R(\mathfrak{p})} \mathfrak{k}_\mathfrak{p}(\alpha\mathbf{a}_\mathfrak{p}).$$

If we assume that the total degree in this product is 0, that is

$$\deg \mathbf{a} + \sum_{\mathfrak{p}\in S} \frac{\mathbf{N}\mathfrak{p} - 1}{w} \deg \mathbf{a}_\mathfrak{p} = 0,$$

then the element β above is an algebraic number, which can be shown to lie in $K(\mathfrak{f})$. The group generated by all such numbers is called the group of **modular numbers** in $K(\mathfrak{f})$, and denoted by $\mathfrak{K}(\mathfrak{f})$. The group generated by the roots of unity $\boldsymbol{\mu}_{K(\mathfrak{f})}$ and by the subgroup of units in $\mathfrak{K}(\mathfrak{f})$ is called the group of **modular units** in $\mathfrak{K}(\mathfrak{f})$. Thus

$$E_{\text{mod}}(K(\mathfrak{f})) = \boldsymbol{\mu}_{K(\mathfrak{f})}(\mathfrak{K}(\mathfrak{f}) \cap E),$$

where E denotes the group of all units.

If H denotes a subfield of $K(\mathfrak{f})$ containing K, then essentially one defines the group of modular units $E_{\text{mod}}(H)$ in H to be the group generated by $\boldsymbol{\mu}_H$ and by the norms down to $H \cap K(\mathfrak{g})$ of the modular units $E_{\text{mod}}(K(\mathfrak{g}))$, for all $\mathfrak{g} \mid \mathfrak{f}$.

The definition is somewhat elaborate and some aspects are fairly technical. The main point is that we define a rather large group of units in a canonical manner, expressed in terms of values of a single function $\mathfrak{k}(z, \Lambda)$, and containing all groups defined by other authors as mentioned above in a similar context. This latter inclusion property may be viewed as one possible reason for calling the group of modular units "large". Another is given more precisely by Kersey's index computation [**Ke 2**], the most precise result known today.

Theorem 6.1. $(E(K(\mathfrak{f})) : E_{\text{mod}}(K(\mathfrak{f}))) = \lambda h_{K(\mathfrak{f})}$ *where* λ *is a power of* 2 *depending on the number of prime factors of* $\mathfrak{f}$; $\lambda = 1$ *if* $\mathfrak{f}$ *is a prime power, relatively prime to* 6, *in particular if* $\mathfrak{f} = (1)$.

Kersey's proof is based in part on the same group theoretical considerations as Sinnott [**Si**] in the cyclotomic case, but the situation he faces is much more complicated for a variety of reasons: more complicated analytic functions to express units; more complicated structure of the Galois group; etc.

§7. The Coates-Wiles connection

Instead of starting from the diophantine problem posed by the higher degree Fermat equations, let us start over again now with the diophantine problem arising from cubic equations, say

$$y^2 = x^3 + ax + b,$$

where a, b are integers. We assume that the discriminant of the right hand side is not equal to 0. Then the set of complex points of this equation, together with one point at infinity, form a Riemann surface of genus 1, isomorphic to a complex torus. The curve is equal to its own Jacobian, taking as origin the point at infinity. Let A denote the curve, and $A(\mathbf{Q})$ its group of rational points. Classical questions concerning $A(\mathbf{Q})$ ask:

What is the structure of the group of torsion points $A(\mathbf{Q})_{\mathrm{tor}}$?

Is there a rational point of infinite order? If so, what is the rank over $\mathbf{Z}$ of $A(\mathbf{Q})$ (which is finitely generated according to a celebrated theorem of Mordell)?

Again, I don't want to go into extensive terminology, and among an open ended choice of topics, I shall select one which establishes a relation between these diophantine questions and units in suitable number fields.

I shall also limit myself to even more special curves of type

$$y^2 = x^3 + b,$$

where b is an integer. We have seen in the last section that these curves admit $\boldsymbol{\mu}_3$ as a group of automorphisms, and belong to the "complex multiplication" category. Over the complex numbers, any two such curves become isomorphic, but over the rational numbers, they may exhibit completely different behavior. For instance, one curve may have rational points other than ∞, while another may not. We are interested to give a criterion when there is a rational point of infinite order, and we shall relate this question to the existence of certain (ramified) extensions of number fields.

Let $K = \mathbf{Q}(\sqrt{-3}) = \mathbf{Q}(\boldsymbol{\mu}_3)$. Let p be a prime number relatively prime to $6b$. We shall suppose in the sequel that p splits completely in K, that is

$$p\mathfrak{o}_K = \mathfrak{p}\bar{\mathfrak{p}}, \qquad \mathfrak{p} \neq \bar{\mathfrak{p}}.$$

Since $\mathfrak{o}_K$ has unique factorization, there is a generator π for $\mathfrak{p}$, that is $\mathfrak{p} = \pi\mathfrak{o}$, and π is well-defined up to a root of unity. We have $p = \pi\bar{\pi}$. Furthermore, $K_{\mathfrak{p}} = \mathbf{Q}_p$, where $K_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic completion of K.

For an element $\alpha \in \mathfrak{o}$ we let $[\alpha] = [\alpha]_A$ be the endomorphism of A induced by α. Let $\mathbf{Q}^{\mathrm{a}}$ denote the algebraic closure of $\mathbf{Q}$. For any field F, A_F or $A(F)$ denotes the group of points on A rational over F.

We assume that A has good reduction at $\mathfrak{p}$, and that the generator π is selected so that the reduction mod $\mathfrak{p}$ of $[\pi]_A$ is the Frobenius endomorphism $\mathrm{Fr}_{\mathfrak{p}}$. This means that for any point $(x, y) \in A(\mathbf{Q}^{\mathrm{a}})$ and any prime $\mathfrak{P}$ of $\mathbf{Q}^{\mathrm{a}}$ over $\mathfrak{p}$, we have

$$[\pi](x, y) \equiv (x^p, y^p) \bmod \mathfrak{P}.$$

Let A_π be the group of points t in $A(\mathbf{Q}^{\mathrm{a}})$ such that

$$[\pi]t = 0.$$

We could also write $A_\pi = A[\pi]$ or $A[\mathfrak{p}]$, to be the set of points t such that $[\alpha]t = 0$ for all $\alpha \in \mathfrak{p}$. Then A_π is a cyclic group of order p, and in fact, $K(A_\pi)$ is a cyclic extension of K, of degree $p - 1$ with Galois group $G \approx (\mathbf{Z}/p\mathbf{Z})^*$ in analogy with the cyclotomic theory. The action of G is determined by the representation on A_π, namely for $a \in \mathfrak{o}$,

$$\sigma_a t = [a]t,$$

analogous to the formula $\sigma_a \zeta = \zeta^a$ if $\zeta \in \boldsymbol{\mu}_p$.

The theory of the extension $K(A_\pi)$ over K can be carried out in analogy with the p-adic theory of Kummer for $\mathbf{Q}(\boldsymbol{\mu}_p)$ over $\mathbf{Q}$. As usual, we have to look at eigenspaces. We let χ be the character such that for $\sigma \in G$ we have

$$\sigma t = \chi(\sigma)t, \quad \text{with } \chi(\sigma) \in (\mathbf{Z}/p\mathbf{Z})^*.$$

One may view χ as a character $\chi : \mathrm{Gal}(K^{\mathrm{a}}/K) \to (\mathbf{Z}/p\mathbf{Z})^*$, where K^{a} is the algebraic closure of K, and χ factors through $G = \mathrm{Gal}(K(A_\pi)/K)$.

Suppose, as in Coates-Wiles, that A has a rational point P of infinite order, and take P not in $[\pi]A(K)$. Then one may extract a π-th root of P, namely a point

$$Q \in \pi^{-1}(P)$$

such that $[\pi]Q = P$. This is analogous to extracting a p-th root in the multiplicative group when dealing with the cyclotomic theory. Then we have another example of double-decked extensions:

$$\begin{tikzcd}
K(A_\pi, \pi^{-1}(P)) \arrow[d, dash] \\
K(A_\pi) \arrow[d, dash] \\
K
\end{tikzcd}$$

Let t be a generator for A_π over $\mathbf{Z}/p\mathbf{Z}$. Then we obtain a 2-dimensional representation of $\mathrm{Gal}(K^{\mathrm{a}}/K)$ arising from the action:

$$\sigma t = \chi(\sigma)t$$
$$\sigma Q = b(\sigma)t + Q$$

with $b(\sigma) \in \mathbf{Z}/p\mathbf{Z}$, thus giving the matrix representation

$$\sigma \mapsto \begin{pmatrix} \chi(\sigma) & b(\sigma) \\ 0 & 1 \end{pmatrix}.$$

Conversely, one may consider Galois extensions of K cyclic of degree p over $K(A_\pi)$ whose Galois group admits such a matrix representation with character χ, and ask if the existence of such extensions can arise only through the above construction with a point of infinite order. We shall say that p is **special** if $\pi + \bar{\pi} = 1$. Otherwise, we call p **non-special.**

Conjecture 7.1. *Assume that for infinitely many non-special primes p, there exists a Galois extension of K over $K(A_\pi)$ whose Galois group admits a representation in $GL_2(\mathbf{Z}/p\mathbf{Z})$, with matrices as above, and character χ. Then there exists a point P of infinite order in A_K, and all but a finite number of these extensions and representations are obtained as described above, by extracting a π-th root of some such P.*

The conjecture can be made somewhat more quantitative. For instance, extracting π-th roots of $A_K/[\pi]A_K$ gives rise to r independent p-extensions of $K(A_\pi)$, where r is the rank of A_K (for all but a finite number of primes p). We leave this aside, but we note that the conjecture essentially asserts that the existence of such extensions can only be explained as arising from a point of infinite order as described in the Coates-Wiles way, except in a finite number of cases. These "exceptional" cases are related to other more subtle invariants of the elliptic curve (something called the Tate-Shafarevitch group, which is beyond the level at which I wish to keep this exposition).

We turn to the local considerations of Coates-Wiles. Let:

$K_0 = K(A_\pi)$;

F_0 = completion of K_0 at some prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$.

Then $F_0 = K_{\mathfrak{p}}(A_\pi) = \mathbf{Q}_p(A_\pi)$.

U_0 = group of $\mathfrak{p}$-adic units in F_0.

$\mathcal{E}_0$ = group of modular units in K_0.

$\bar{\mathcal{E}}_0$ = closure of $\mathcal{E}_0$ in U_0.

Since the $(p-1)$th roots of unity are contained in $\mathbf{Z}_p$, and a fortiori in $\mathbf{Q}_p$, it follows that the cyclic extension F_0 of $\mathbf{Q}_p$, which is of degree $p-1$, is a Kummer extension, that is

$$F_0 = \mathbf{Q}_p(w_0) \quad \text{where } w_0^{p-1} \in \mathbf{Q}_p.$$

The lattice of fields is shown on the figure.

$$\begin{tikzcd}[column sep=small]
 & & \mathbf{Q}_p(A_\pi) = F_0 \arrow[dd, dash] & \\
 & K(A_\pi) \arrow[ur, dash] \arrow[dd, dash] & & G \\
G & & K_p = \mathbf{Q}_p & \\
 & K \arrow[ur, dash] & &
\end{tikzcd}$$

It might happen that $\mathbf{Q}_p(A_\pi) = \mathbf{Q}_p(\boldsymbol{\mu}_p)$. It is an easy technical matter to show that this happens if and only if $\pi + \bar{\pi} = 1$, in other words, π is special (provided $p > 5$). It can be shown that the set of special primes has density zero, so there are plenty of non-special primes. We assume p is non-special.

In dealing with the local extension over $\mathbf{Q}_p$, we can now view the character χ as the Kummer character of G, namely the character such that

$$\sigma w_0 = \chi(\sigma) w_0.$$

The double-decked extension can be viewed locally by extending the base field to $K_{\mathfrak{p}}$:

$$\begin{tikzcd}
& F_0(\pi^{-1}(P)) \arrow[dd, no head] \\
K_0(\pi^{-1}(P)) \arrow[ur, no head] \arrow[dd, no head] & \\
& F_0 \arrow[dd, no head] \\
K_0 \arrow[ur, no head] \arrow[dd, no head] & \\
& K_p \\
K \arrow[ur, no head] &
\end{tikzcd}$$

The extension $K_0(\pi^{-1}(P))$ of K_0 is a cyclic extension of degree p, closely related by class field theory to the factor group of local units modulo the closure of the global units.

If C is an abelian group on which G operates, we denote:

$C(p) = C/C^p$ (writing C multiplicatively);

$C(p, \chi) = (C/C^p)(\chi) = \chi$-eigenspace of $C(p)$.

Kummer had already studied the p-adic properties of the cyclotomic units, which in modern language amounts to the factor group of local units in $\mathbf{Q}(\boldsymbol{\mu}_p)$ by the closure of the cyclotomic units. A similar study can be made in the present context, but I shall limit myself to only one aspect. Motivated by the "Birch-Swinnerton-Dyer Conjecture", Coates-Wiles arrive at the following result.

Theorem 7.2. *Suppose that p is non-special and that there exists a rational point P of infinite order in $A(K)$. Then*

$$(U_0/\overline{\mathcal{E}}_0)(p, \chi) \neq 0.$$

The proof of that theorem is carried out by methods of class field theory, related to a p-adic "Kummer criterion", see **[Co-W]**, **[Co 2]**. Robert **[Ro 2]** had also considered the analogue of Kummer's criterion in the context of elliptic curves.

Conjecture 7.3. *Conversely, assume that $(U_0/\overline{\mathcal{E}}_0)(p, \chi) \neq 0$ for infinitely many non-special primes. Then there exists a rational point on A of infinite order.*

This conjecture is a transformation of a special case of the Birch-Swinnerton Dyer conjecture. By class field theory, the hypothesis guarantees the existence of certain abelian extensions (subject to a certain eigenspace condition) of $K(A_\pi)$.

In any case, we see here once more how (possibly conjecturally) abelian extensions of number fields can be parametrized by extracting "roots", except that the roots occur on the group of an elliptic curve as well as the multiplicative group.

Of course, everything we have stated for K_0 can be extended by taking powers of π, and looking at the extensions

$$K_n = K(A[\pi^{n+1}]) \quad \text{and} \quad \Omega_n = K_n(\pi^{-(n+1)}P)$$

if P is a point of infinite order. Even to consider K_0 and Ω_0 as we have done above, it is necessary to pass to the limit in this tower of extensions to apply Iwasawa theory of $\mathbf{Z}_p$-extensions, which leads to the "right" statements concerning the quantitative description of the extensions one obtains by dividing not only torsion points but points of infinite order. This is a massive undertaking which goes beyond the scope of our discussion, but I want to emphasize that the formalism of the characteristic polynomial as in the appendix of §2, and the questions related to it, can be formulated in the present context also. For example, let C_n be the p-primary part of the ideal class group in K_n. We can form the same type of projective limit as in the cyclotomic $\mathbf{Z}_p$-extension. Is the projective limit of Jacobian type (analogue of the Ferrero-Washington theorem)? The answer is not known today.

§8. Stark units

Let us go back to cyclotomic fields, and to the cyclotomic units. Consider the real subfield $K = \mathbf{Q}(\mu_m)^+$ where m is an integer ≥ 3, odd or divisible by 4. We have one archimedean absolute value v_0 on $\mathbf{Q}$, the ordinary absolute value. The field K is totally real, meaning that any embedding of K into the complex numbers actually lies in the real numbers. We can find a cyclotomic number generating K, namely $K = \mathbf{Q}(\epsilon)$, where

$$\epsilon = (1 - \zeta)(1 - \zeta^{-1})$$

and $\zeta = e^{2\pi i/m}$. The Galois group of K over $\mathbf{Q}$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^* / \pm 1$, under the map $a \mapsto \sigma_a$.

We may define the **partial zeta function** relative to $K/\mathbf{Q}$:

$$\zeta(\sigma_a, s) = \sum_{\substack{n=1 \\ n \equiv \pm a(m)}}^{\infty} n^{-s}.$$

Classically, we have $\zeta(\sigma_a, 0) = 0$ and

$$\zeta'(\sigma_a, 0) = -\frac{1}{2}\log|\sigma_a \epsilon|.$$

Of course, we could replace ϵ by ϵ^{-1} to get rid of the minus sign in that equation. Stark [**St IV**] interprets these relations as defining analytically a "unit" which becomes the generator of an abelian (ramified) extension of the rationals. Indeed, if m is composite, then ϵ is a unit, and if $m = p^{\nu}$ is a prime power, then ϵ is divisible only by the prime lying above p (p-unit).

Finally, Stark notes that $K(\epsilon^{1/2})$ is abelian over $\mathbf{Q}$. Indeed, if we write $K = K_m = \mathbf{Q}(\mu_m)$, then

$$K(\epsilon^{1/2}) = \begin{cases} K_{4m} & \text{if } m \text{ is odd,} \\ K_{2m} & \text{if } m \text{ is even.} \end{cases}$$

Stark has conjectured the existence of a similar situation, involving units, which can be used to generate "class fields" (ramified abelian extensions) of a number field. He has given proofs only in those cases when we know how to parametrize units as values of classical analytic functions of "exponential" type (parametrizing the exponential map on algebraic Lie groups), namely the cyclotomic case as above, and the case of modular units over imaginary quadratic fields, as mentioned in the last two sections. I shall briefly summarize the general situation envisioned by Stark. I base the exposition on lectures of Tate, and also on [**Ta 1**] and [**Ta 2**].

Let k be a number field and K an abelian extension with Galois group G. Denote by v an archimedean place of k. Then v denotes either an embedding of k in the real numbers, or in the complex numbers (up to complex conjugation). We let k_v denote the completion of k at v, which is isomorphic to either $\mathbf{R}$ or $\mathbf{C}$ as the case may be. Let v' be an archimedean place of K lying above v. Then the completion $K_{v'}$ is also equal to $\mathbf{R}$ or $\mathbf{C}$, and $K_{v'}$ is an extension of k_v of degree 1 or 2. If $K_{v'}$ is an extension of degree 2 of k_v, then the local Galois group G_v is cyclic of order 2, generated by complex conjugation. These are the archimedean analogues of the p-adic places which correspond to embeddings in the field $\mathbf{C}_p$, completion of the algebraic closure of $\mathbf{Q}_p$. Let $[K_{v'} : k_v] = n_v$ be the local degree. We define

$$\|\alpha\|_{v'} = |\alpha|_{v'}^{n_v}$$

where $|\alpha|_{v'}$ is the absolute value on K induced by the embedding v'.

As with prime ideals, we say that v splits completely in K if the number of distinct embeddings of K in $\mathbf{C}$ lying above v is equal to the degree $[K : k]$. Equivalently, we could say that for any extension v' of v to K, v' is real if and only if v is real. If v is real and v' is complex, then we say that v ramifies in K, or that v' is ramified over v.

Let R = set of primes of k ramified in K. Let

$$S \supset R \cup S^{\infty}(k)$$

be a finite set of places with at least two elements.

Let $\mathfrak{p}$ be a prime of k unramified in K, and let $\mathfrak{P}$ be a prime ideal of K lying above $\mathfrak{p}$. Let $G_{\mathfrak{P}}$ be the decomposition group of $\mathfrak{P}$, meaning the subgroups of elements $\sigma \in G$ such that $\sigma\mathfrak{P} = \mathfrak{P}$. Since we assumed that G is abelian, it follows that $G_{\mathfrak{P}}$ depends only on $\mathfrak{p}$, not on the choice of $\mathfrak{P}$, and $G_{\mathfrak{P}}$ is therefore denoted by $G_{\mathfrak{p}}$. Furthermore, $G_{\mathfrak{p}}$ acts on the residue class field $\mathfrak{o}_K/\mathfrak{P}$ over $\mathfrak{o}_k/\mathfrak{p}$, and is cyclic, with a canonical generator, the Frobenius element $\sigma_{\mathfrak{p}}$ such that

$$\sigma_{\mathfrak{p}}\, x \equiv x^{\mathbf{N}\mathfrak{p}} \bmod \mathfrak{P}.$$

The **partial zeta function** associated with a given $\sigma \in G$ is defined to be the partial sum

$$\zeta_S(\sigma, s) = \sum_{\substack{(\mathfrak{a},S)=1 \\ \sigma(\mathfrak{a})=\sigma}} \mathbf{N}\mathfrak{a}^{-s}\,.$$

Remark: If $S = \mathcal{R} \cup S^{\infty}(k)$, then we omit the subscript S, and we write $\zeta_S(\sigma, s) = \zeta(\sigma, s)$. *Let us assume*:

there is one archimedean place v_0 of k which splits completely in K.

Then basic analytic number theory shows that the partial zeta function vanishes of order ≥ 1 at $s = 0$. We are interested in the derivative of $\zeta_S(\sigma, s)$ at $s = 0$ following Stark, who observed that the formulas for this derivative at $s = 0$ are structurally more transparent than the analogous formulas for $\zeta_S(\sigma, s)$ at $s = 1$, considered more classically. (These formulas can be obtained from the functional equation of Hurwitz zeta functions.)

We shall say that we are in the **special case** if S has exactly two elements; then

$$\{S^{\infty}(k) - v_0\} \cup \mathcal{R}$$

has precisely one element (which may therefore be archimedean, or may be a single ramified prime) v_1, called **special.** By a (v_0, S)**-unit** we shall mean an element ϵ of K^* such that in non-special cases:

$$\|\epsilon\|_v = 1 \text{ for any place } v \text{ of } K, v \nmid v_0.$$

In the special case, then the above condition should hold for $v \nmid v_0, v \nmid v_1$, and then we require in addition that the values

$$\|\epsilon\|_v \text{ for } v \mid v_1$$

are equal to 'each other.

In particular, if we are not in the special case, then such ϵ are units; and in the special case, if the special element v_1 corresponds to a prime ideal, then such ϵ are $\mathfrak{p}$-adic units for all other primes $\mathfrak{p}$, i.e. they are what is usually called S-units. Note that the special case is rare, but that the classical cases $k = \mathbf{Q}$ or $k =$ imaginary quadratic field often give rise to special cases.

Conjecture 8.1. *Denote by v some extension of v_0 to K. Let $W = w_K$ be the number of roots of unity in K. Then there exists a (v_0, S)-unit ϵ in K, well-determined up to a root of unity in $\boldsymbol{\mu}_K$, such that*

(i) $\zeta'_S(\sigma, 0) = -\frac{1}{W} \log \|\sigma\epsilon\|_v$ *for all* $\sigma \in G$.

(ii) $K(\epsilon^{1/W})$ *is abelian over* k.

In the special case when k is an imaginary quadratic field, the case of complex multiplication, Stark proved his conjecture by using the classical theory of L-series (Kronecker limit formula in this case), as well as the theory of modular units in a fairly precise form since we want ϵ itself, not just some power of ϵ, to fit the Stark formula giving the derivative of the partial zeta function at $s = 0$. At this point it becomes important to have as large a group of modular units as possible. Note that usually one expects to have $K = k(\epsilon)$, but one has to impose some conditions to insure this.

Despite attempts by Stark and by Shintani [**Sh**], even the case when k is a real quadratic field is still unknown. Stark's paper [**St IV**] contains numerical computations which confirm the conjecture strikingly in special fields, and some cubic extensions. Shintani [**Sh 2**] proves the conjecture in special, and non-trivial cases.

Gross [**Gro 1**] has formulated conjectures as above for p-adic L-functions. Also Tate pointed out that instead of taking an archimedean absolute value v_0, one could take a prime $\mathfrak{p}_0$ of k, also splitting completely in K, to obtain a new case for the complex zeta function, as follows [**Ta 2**].

Let $\mathfrak{p} \mid \mathfrak{p}_0$ in K. For simplicity, we assume that the set

$$S = R \cup S^{\infty}(k) \cup \{\mathfrak{p}_0\}$$

has ≥ 3 elements, so $R \cup S^{\infty}(k)$ has ≥ 2 elements. This assumption amounts to omitting the special case, which is so degenerate as to be of no interest here.

Conjecture 8.2. *Let $\mathfrak{p}$ be a prime of K lying above $\mathfrak{p}_0$. There exists a $\mathfrak{p}_0$-unit ϵ such that*

(i) $\zeta(\sigma, 0) = \frac{1}{W} \operatorname{ord}_{\mathfrak{p}}(\sigma\epsilon)$;

(ii) $K(\epsilon^{1/W})$ *is abelian over k.*

The absence of the derivative is due to a technical transformation as follows. Let

$$\zeta_{[\mathfrak{p}]}(\sigma, s) = (1 - \mathrm{N}\mathfrak{p}^{-s})\zeta(\sigma, s)$$

be the zeta function from which the $\mathfrak{p}$-Euler factor has been deleted. Then

$$\begin{aligned} \zeta'_{[\mathfrak{p}]}(\sigma, 0) &= (\log \mathrm{N}\mathfrak{p}_0)\zeta(\sigma, 0) \\ &= -\frac{1}{W}\log\|\sigma\epsilon\|_{\mathfrak{p}} \quad \text{(conjecturally)} \\ &= \frac{1}{W}\operatorname{ord}_{\mathfrak{p}}(\sigma\epsilon)(\log \mathrm{N}\mathfrak{p}), \end{aligned}$$

and $\mathrm{N}\mathfrak{p}_0 = \mathrm{N}\mathfrak{p}$ since we assumed that $\mathfrak{p}_0$ splits completely in K; so the formula for $\zeta(\sigma, 0)$ drops out.

Following Brumer, one defines the **Stickelberger element** associated with the extension K/k to be

$$\theta = \sum_{\sigma \in G} \zeta(\sigma, 0)\sigma^{-1}.$$

Siegel has shown that $\theta \in \mathbf{Q}[G]$, i.e. that $\zeta(\sigma, 0)$ is a rational number. If there is more than one ramified prime, then one gets the formal factorization

$$(\epsilon) = \mathfrak{p}^{W\theta},$$

and if there is exactly one ramified prime, then a power of that prime may occur additonally in the factorization of ϵ.

As in the cyclotomic case, define the **integralizing ideal** I to be the ideal of $\mathbf{Z}[G]$ generated by W and elements of the form $\sigma_{\mathfrak{c}}$ — $\mathbf{N}\mathfrak{c}$ for ideals $\mathfrak{c}$ prime to W and to the ramified primes. This is the annihilator in $\mathbf{Z}[G]$ of $\boldsymbol{\mu}(K)$. It is known by Deligne-Ribet [**De-R**] or Barsky-Cassou-Nogues [**CN**] that $I\theta \subset \mathbf{Z}[G]$. (This is a much more difficult result than in the cases we encountered previously.)

Conjecture 8.3. *The ideal $I\theta$ annihilates the class group* $\mathrm{Cl}(K)$. *If $x \in I$ and $\mathfrak{a}$ is an ideal of K, then*

$$\mathfrak{a}^{x\theta} = (\alpha_x)$$

where α_x satisfies $\|\alpha_x\|_v = 1$ for any archimedean absolute value v of K, and so α_x is well-defined up to a root of unity. Furthermore, if $\mathfrak{a}^{W\theta} = (\epsilon)$, then $K(\epsilon^{1/W})$ is abelian over k. Finally, if $(W\mathfrak{a}, \mathfrak{p}) = 1$, then

$$\mathfrak{a}^{(\sigma_{\mathfrak{p}} - \mathbf{N}\mathfrak{p})\theta} = (\alpha_{\mathfrak{p}}) \quad \textit{with}\, \alpha_{\mathfrak{p}} \equiv 1 \bmod \mathfrak{p}.$$

The annihilation of the ideal class group by the Stickelberger ideal $I\theta$ has been conjectured for some time by Brumer. The rest was formulated by Stark and Tate, who pointed out that Conjecture 8.2 implies Conjecture 8.3, which is the analogue of the Stickelberger theorem for cyclotomic fields. For related questions, see Coates-Sinnott [**Co-Si**] and [**Co 2**].

§9. Higher regulators: number fields

Stark [**St II**] has also formulated a non-abelian theory, with arbitrary representation of the Galois group G, starting from the Artin formalism of L-functions. This leads into higher dimensional regulators (determinants formed with the logarithms of units).

In this theory, we deal with two naturally defined $\mathbf{Q}$-vector spaces which become isomorphic over the complex numbers. The $\mathbf{Q}$-spaces give natural representations of a Galois group. After extending the scalars to $\mathbf{C}$, and choosing bases over $\mathbf{Q}$, the isomorphism between the spaces can be represented by a square matrix, whose determinant is well defined modulo a non-zero *rational number*, because changing bases over $\mathbf{Q}$ introduces only changes by rational matrices. A representation of G then leads to a determinant which conjecturally can be expressed as a transcendental number, times an algebraic number which transforms in a "functorial" way under the action of the Galois group. This algebraic number is the analogue of the Stark unit mentioned in §8, where the "determinant" was a one by one determinant.

The exposition in this section is based on lectures by Tate on Stark's conjectures, especially [**Ta 1**], [**Ta 2**].

Let K/k be a finite Galois extension of a number field, with $\mathrm{Gal}(K/k) = G$. Let V denote a $\mathbf{C}$-linear representation of G, or the finite dimensional vector space associated with it. Let:

$S^{\infty}(K)$ = set of archimedean places of K; elements v range over $S^{\infty}(K)$.

$U(K)$ = free abelian group on $S^{\infty}(K)$.

$U_0(K)$ = elements of $U(K)$ of degree 0 (the augmentation module).

$E(K)$ = group of units of $K = \mathfrak{o}_K^*$.

The groups $U(K), U_0(K), E(K)$ are G-modules. A theorem of Herbrand asserts that the units $E(K)$ contain a subgroup of finite index which is G-isomorphic to $U_0(K)$. Then the $\mathbf{Q}$-vector spaces are isomorphic:

$$\mathbf{Q} \otimes U_0(K) \approx \mathbf{Q} \otimes E(K).$$

To begin with some algebraic considerations, we first look at $\mathbf{C}U_0(K)$. We shall deal with the units afterward.

Let $U_0 = U_0(K)$, and let

$$\theta : \mathbf{C}U_0 \to \mathbf{C}U_0$$

be an automorphism (of $\mathbf{C}$-vector spaces). Then θ induces an endomorphism

$$\theta^* : \mathrm{Hom}_G(V^*, \mathbf{C}U_0) \to \mathrm{Hom}_G(V^*, \mathbf{C}U_0),$$

where V^* is the dual space of V. We define

$$\delta(V, \theta) = \det(\theta^*, \mathrm{Hom}_G(V^*, \mathbf{C}U_0)).$$

Then $V \mapsto \delta(V, \theta)$ satisfies the formalism of Artin, which we recall. Let H be a subgroup of G. Let Ind_G^H denote the induced representation, characterized by the formula

$$\mathrm{Hom}_G(\mathrm{Ind}_G^H(V), W) = \mathrm{Hom}_G(V, \mathrm{Res}_H^G(W)),$$

for any G-space W and H-space V, so induction is the adjoint of restriction. Let Inf denote inflation from G/H to G if H is normal. We have:

(1) $\delta(V_1 \oplus V_2, \theta) = \delta(V_1, \theta)\delta(V_2, \theta)$;

(2) $\delta(\mathrm{Ind}_G^H V, \theta) = \delta(V, \theta)$ if V is a representation of a subgroup H;

(3) $\delta(\mathrm{Inf}_G^{G/H} V, \theta) = \delta(V, \theta \mid (\mathbf{C}U_0)^H)$ if V is a representation of G/H;

(4) $\delta(V, \theta_1\theta_2) = \delta(V, \theta_1)\delta(V, \theta_2)$;

(5) $\delta(V, \theta)^{\sigma} = \delta(V^{\sigma}, \theta^{\sigma})$ for any $\sigma \in \mathrm{Aut}(\mathbf{C})$.

The first four are easily proved. The fifth also once we make the following remarks. The number $\delta(V,\theta)$ depends only on the isomorphism class of V. An automorphism σ operates on V, say after a choice of basis so that σ operates on the coordinates of $\mathbf{C}^{\dim V}$. Thus V^{σ} is well defined up to an isomorphism. With this explanation, (5) is also easy.

Next, we need the regulator map

$$\lambda : \mathbf{C}E(K) \to \mathbf{C}U_0(K)$$

defined on units by

$$\lambda(\epsilon) = \sum_{v} \log \|\epsilon\|_v \cdot [v],$$

and extended by **C**-linearity to a **C**-isomorphism. If

$$\varphi : \mathbf{C}U_0 \to \mathbf{C}E(K)$$

is an isomorphism, then

$$\theta = \lambda \circ \varphi : \mathbf{C}U_0 \to \mathbf{C}U_0$$

is a possible automorphism.

If φ is the **C**-linear extension of a G-embedding

$$U_0 \to E(K),$$

then one has the special value

$$\delta(1_k, \lambda \circ \varphi) = \pm(E(K) : \varphi(U_0(k)))R_k/w_k \tag{6}$$

where R_k is the regulator of k and w_k the number of roots of unity in k.

Finally, we need to recall the definition of the Artin L-function associated with the representation V of $G = \mathrm{Gal}(K/k)$. For each prime $\mathfrak{p}$ of k the conjugacy class of a Frobenius element $\sigma_{\mathfrak{p}}$ in G is well defined modulo the inertia group $I(\mathfrak{p})$, defined up to conjugacy. The **Artin L-function** is defined for $\mathrm{Re}(s) > 1$ by the product

$$L(s,V) = \prod_{\mathfrak{p}} \det(1 - \sigma_{\mathfrak{p}} \mathrm{N}\mathfrak{p}^{-s} \mid V^{I(\mathfrak{p})}),$$

where $V^{I(\mathfrak{p})}$ is the part of V fixed by $I(\mathfrak{p})$. We let $c(V)$ be the coefficient of the leading term at $s = 0$, that is

$$L(s,V) \sim c(V)s^{r(V)}, \quad \text{for } s \to 0,$$

where $r(V)$ is the order of the zero of $L(s,V)$ at $s = 0$.

Define

$$A(V,\varphi) = \frac{\delta(V, \lambda \circ \varphi)}{c(V)}.$$

Then $A(V,\varphi)$ depends only on the isomorphism class of the complex representation V, for fixed φ, and so may be written $A(\chi,\varphi)$. We may now state Stark's conjecture.

Conjecture 9.1. *For any $\sigma \in \mathrm{Aut}(\mathbf{C})$, we have*

$$A(V,\varphi)^{\sigma} = A(V^{\sigma},\varphi^{\sigma}).$$

By (4) and (5), if the conjecture is true for some φ, then it is true for every φ.

Property (6) shows that the conjecture is true for trivial V. Stark in [**St II**] has shown that if the character of V is rational valued, then there is some positive integer m such that the conjecture is true for $m.V$, in other words,

$$(A(V,\varphi)^{m})^{\sigma} = (A(V^{\sigma},\varphi^{\sigma}))^{m}.$$

The proof is obtained by using the induction property, and the fact that any representation with rational character has an integral multiple which is a sum of induced representations of trivial characters on some subgroups of G. Then one uses the theorem for trivial representations, together with the Artin formalism (2) and (3). Tate has proved Conjecture 9.1 when the character of V is rational valued.

It is then possible to obtain units (conjecturally) in a manner similar to that of the preceding section, as follows.

Assume that V is irreducible and non-trivial, and that $r(V) = 1$, so the L-function vanishes of order 1 at the origin.

Then $\mathrm{Hom}_G(V, \mathbf{C}U_0)$ is 1-dimensional, and there is an embedding

$$V \to \mathbf{C}U_0$$

unique up to a scalar multiple.

Let φ satisfy Conjecture 9.1, and assume in addition that φ is the $\mathbf{C}$-linear extension of a G-embedding

$$U_0 \to E(K).$$

If x is in the image of V under this embedding, then we have

$$\lambda \circ \varphi(x) = \delta(V, \lambda \circ \varphi)x.$$

Let F be the field generated over the rationals by the character values of G. Then $A(V,\varphi)$ lies in F.

By Frobenius reciprocity and the functional equation for the L-function, one sees that there is one archimedean place v of k such that

$$\dim V^{G_v} = 1, \text{ but } V^{G_{v'}} = 0 \quad \text{for } v' \in S^{\infty}(k), v' \neq v.$$

We denote by this same letter v an extension of the place to K. Let $\chi = \chi_V$ be the character of V. Then an element x can be taken to be

$$x = \sum_{\sigma \in G} \chi(\sigma^{-1})(\sigma[v] - [v]).$$

Let

$$\epsilon_{\sigma,\varphi} = \varphi(\sigma[v] - [v]).$$

If Y is any subset of G, let $\chi(Y) = \sum \chi(y)$, where the sum is taken for $y \in Y$.

Theorem 9.2. *Assume Conjecture 9.1. Suppose that V is irreducible, non-trivial; that $r(V) = 1$; and φ is the* **C**-*linear extension of a G-embedding $U_0 \to E(K)$. Then*

$$L'(0,V) = (A(V,\varphi)\chi(G_v))^{-1} \sum_{\sigma \in G} \chi(\sigma^{-1}) \log \|\epsilon_{\sigma,\varphi}\|.$$

The above theorem gives an expression in the non-abelian case analogous to that of the preceding section in the abelian case. Stark gives proofs of such a formula in special cases in [**St II**] and [**St B**]. The theorem is proved by juggling with the orthogonality relations of characters. It then gives rise to:

Theorem 9.3. *Assume in addition that V gives a faithful representation of G. Let*

$$c(\sigma) = \mathrm{Tr}_{F/\mathbf{Q}}\, \chi(\sigma)/A(V,\varphi),$$

and let m be a positive integer such that $mc(\sigma) \in \mathbf{Z}$ for all $\sigma \in G$. Let

$$\epsilon_m = \prod_{\sigma \in G} \epsilon_\sigma^{mc(\sigma^{-1})}.$$

Then K is the smallest Galois extension of k which contains ϵ_m.

These two statements summarize Stark's insight into the possibility of generating non-abelian extensions by units appearing in Artin L-functions derivatives at $s = 0$. Stark has proved special cases which could be reduced to the complex multiplication situation by induced characters. Chinburg (Thesis, Harvard, 1980) has made computations confirming the existence of the expected units to 13 decimal places in tetrahedral cases over the rationals.

§10. Higher regulators: curves (da capo)

We shall now describe results of Anderson [**An 1**], [**An 2**] giving a geometric context for the same formalism as in the preceding section.

Let X be a projective non-singular curve defined over a number field k. Then we have the De Rham cohomology group

$$H^1_{DR}(X,k)$$

of differential forms of second kind modulo exact forms. For every embedding $\tau : k \to \mathbf{C}$ of k into the complex numbers, the curve X^τ is defined over k^τ, and we have the corresponding space $H^1_{DR}(X^\tau, k^\tau)$, as well as $H^1_{DR}(X^\tau, \mathbf{C})$ obtained by extension of scalars from k^τ to $\mathbf{C}$. There is a natural isomorphism

$$\lambda = \lambda_\tau : H^1_{DR}(X^\tau, \mathbf{C}) \to H^1_{\mathrm{top}}(X^\tau, \mathbf{C})$$

which to each differential form ω associates the functional

$$\gamma \mapsto \int_\gamma \omega$$

for every cycle γ. This will play a role analogous to the regulator map of §9.

Now suppose G is a finite group of automorphisms of X, also defined over k. Then G gives rise to a finite covering

$$X \to X/G,$$

and G operates on $H^1_{DR}(X, k)$.

For each τ we let

$$\varphi_\tau : H^1_{\text{top}}(X^\tau, k^\tau) \to H^1_{DR}(X^\tau, k^\tau)$$

be an isomorphism of k^τ-vector spaces. Then $\lambda \circ \varphi_\tau$ is an automorphism of $H^1_{\text{top}}(X^\tau, \mathbf{C})$, after extending φ_τ by $\mathbf{C}$-linearity.

Let V be a representation of G over k, so V^τ is a representation of V over k^τ, whence over $\mathbf{C}$. Let θ_τ be any automorphism of $H^1_{\text{top}}(X^\tau, \mathbf{C})$. Then θ_τ induces an automorphism θ^*_τ of $\text{Hom}_G(V^*, H^1_{\text{top}}(X^\tau, \mathbf{C}))$, where V^* is the dual space. Define

$$\delta(X^\tau, V^\tau, \theta_\tau) = \det(\theta^*_\tau : \text{Hom}_G(V^*, H^1_{\text{top}}(X^\tau, \mathbf{C}))).$$

This symbol satisfies the Artin formalism, as listed in the preceding section. Cf. [**L 6**]. In practice, we shall take $\theta_\tau = \lambda \circ \varphi_\tau$.

On the other hand, Anderson defines a constant $c(X, V)$ with the gamma function as follows. Let $x \in X$ be a point of X in a fixed algebraic closure of k, and let $G(x)$ be the isotropy group of x in G; let $e(x)$ be the order of $G(x)$, namely the ramification index of x. Let $T(x)$ be the tangent space of x, as one-dimensional $G(x)$-module. Define

$$c(X, V) = (2\pi i)^{d(X,V)} \prod_x \prod_{i=1}^{e(x)} \Gamma\left(\frac{i}{e(x)}\right)^{d(i,x,V)}$$

where

$$d(X, V) = (g(X/G) - 1)\dim V + \dim V^G$$

and

$$d(i, x, V) = \dim \text{Hom}_{G(x)}(T(x)^{\otimes i}, V).$$

Also define

$$A(X^\tau, V^\tau, \varphi_\tau) = \frac{\delta(X^\tau, V^\tau, \lambda \circ \varphi_\tau)}{c(X, V)}.$$

Then Anderson proves:

Theorem 10.1. *For any automorphism $\sigma \in \text{Aut}(\mathbf{C})$, we have*

$$A(X^\tau, V^\tau, \varphi_\tau)^\sigma = A(X^{\tau\sigma}, V^{\tau\sigma}, \varphi_{\tau\sigma})\alpha(\sigma, \tau),$$

with some element $\alpha(\sigma, \tau) \in k^{\tau\sigma}$. [Notation: $k^{\tau\sigma} = (k^\tau)^\sigma$.] Furthermore, if $w = w(k)$ is the number of roots of unity in k, then

$$A(X^\tau, V^\tau, \varphi_\tau)^w \in k^\tau.$$

This last assertion shows that the number $A(X^{\tau}, V^{\tau}, \varphi_{\tau})$ in fact generates a Kummer extension of k^{τ}, and by appropriate choice of φ_{τ}, Anderson can make the factor $\alpha(\sigma, \tau)$ equal to a root of unity. For this and further aspects of $\alpha(\sigma, \tau)$, cf. [**An 2**].

The expressions for the "periods" in Anderson's theory form a geometric counterpart to the arithmetic conjectures of Stark. Ultimately, these two extremes will be covered by the general theory of schemes of finite type over **Z**.

Say R is a finitely generated subring of a finitely generated extension of the rational numbers. Assume that R is regular (all its local rings are regular) for simplicity. The prime ideals of R constitute the spectrum $X = \operatorname{spec} R$, and the maximal ideals P are called the closed points. Let $\mathrm{N}P$ denote the number of elements in the residue class field R/P, necessarily finite. One defines the **Hasse-Weil zeta function**

$$\varsigma(X, s) = \prod_P (1 - \mathrm{N}P^{-s}).$$

Such a function provides a way to reflect many arithmetic and geometric properties of X. if R is the ring of integers of a number field, then this function is the Dedekind zeta function. It can be defined for a scheme, covered by a finite number of such affine pieces.

Both in §9 and §10 the theorems or conjectures were formulated for number fields. Ultimately, they will be generalized to schemes of finite type. At the present time, only very special cases have been handled, mostly concerning elliptic curves with complex multiplication, modular curves, and Fermat type curves. However, one has already a good view of conjectural statements which started from the Birch-Swinnerton Dyer conjecture for elliptic curves, as given by Tate in two very valuable papers [**Ta 3**] and [**Ta 4**]. See also [**Ta 5**]. Just to make the link with these papers, I reproduce one of his conjectures as follows:

Conjecture 10.2. *If X is a regular ring R of finite type over* **Z**, *then the order of $\varsigma(X, s)$ at the point $s = \dim X - 1$ is equal to*

$$\operatorname{rank} R^* - \operatorname{rank} \mathrm{Cl}(R),$$

where R^* is the group of units of R, and $\mathrm{Cl}(R)$ *is the group of divisor classes.*

One needs to go further and give a description of the coefficient of $(s - d + 1)^r$ in the expansion

$$\varsigma(X, s) = c(X)(s - d + 1)^r + \text{lower order terms}$$

at $s = d - 1$, where $d = \dim X$. Deligne [**De**] gives the value of the zeta function suitably normalized at the "critical point" in the context of "motives", when the zeta function does not vanish. To cover the cases considered by Birch-Swinnerton-Dyer-Stark-Tate with $r > 0$, there still remains to fit the considerations of §9, and the period considerations of §10 into this pattern, for regular schemes of finite type over **Z**, especially the modular scheme (cf.

Beilenson [**Be**]). But I hope I have fulfilled my objective to lead the reader (who has come this far) into the unknown, concerning units and class groups in number theory and algebraic geometry.

Appendix: Distributions

Because of special interest shown in this topic, and some questions asking "why the Bernoulli polynomials and not others" in the theory described in §2 and §3, I have extracted here some general remarks from my AMS talk at the summer meeting.

Let

$$\varphi : \mathbf{Q}/\mathbf{Z} \to A$$

be a mapping into some abelian group which satisfies the relation for every positive integer N:

$$N^k \sum_{j=1}^{N-1} \varphi\left(x + \frac{j}{N}\right) = \varphi(Nx).$$

Here k is some positive integer. Then φ is said to be a **distribution of degree** k. Relations as above are satisfied by many functions in classical analysis and number theory, and I shall list a series of examples.

Note that if $\psi : \mathbf{Q}/\mathbf{Z} \to B$ is another distribution, then a homomorphism of φ to ψ is defined to be a homomorphism $h : A \to B$ making the following diagram commutative:

$$\begin{tikzcd}
 & A \arrow[dd, "h"] \\
\mathbf{Q}/\mathbf{Z} \arrow[ur] \arrow[dr] & \\
 & B
\end{tikzcd}$$

Some of the examples which we shall give will be homomorphic images of each other, but appearing under different disguises.

A distribution is called **odd** or **even** according as the function is odd or even. If multiplication by 2 is invertible on A, then any A-valued distribution can be uniquely decomposed as a direct sum of an even and an odd distribution. In the subsequent examples, each distribution is naturally equipped with a parity.

Bernoulli distribution. For each positive integer k, there exists a unique polynomial $\mathbf{B}_k$ with complex coefficients, leading coefficient 1, of degree k, such that the map

$$x \mapsto \frac{1}{k}\mathbf{B}_k(\langle x \rangle)$$

is a distribution of degree $k - 1$. This polynomial is the Bernoulli polynomial, which has rational coefficients, and can be given by the generating series

$$\frac{te^{tX}}{e^t - 1} = \sum_{k=0}^{\infty} \mathbf{B}_k(X)\frac{t^k}{k!}.$$

If you check back to §2 or §3, you note that we discussed the Stickelberger element only at first level p, although we alluded to the necessity of considering all levels p^n. Let

$$G_n \approx (\mathbf{Z}/p^n\mathbf{Z})^*.$$

Then there is a natural homomorphism of group rings

$$\mathbf{Z}[G_{n+1}] \to \mathbf{Z}[G_n].$$

If one writes down the Stickelberger element at level $n+1$, then one expects its image under this homomorphism to be the Stickelberger element at level n. It is immediately seen that this compatibility condition amounts to the distribution relations for powers of p. This explains "why" the Bernoulli polynomials were forced in the context of the p-towers. Note that the Bernoulli distribution has parity $(-1)^k$.

The Fourier-Bernoulli distribution. Let

$$f_k(x) = \sum_{k=1}^{\infty} \frac{e^{2\pi i n x}}{n^k}.$$

Then it is immediately verified that f_k defines a distribution of degree $k-1$. In fact, the variable x can be taken to be in $\mathbf{R}/\mathbf{Z}$ rather than $\mathbf{Q}/\mathbf{Z}$. Furthermore, we have the following lemma of Rohrlich.

Lemma. *Let f be in $L^2(\mathbf{R}/\mathbf{Z})$, and assume that f satisfies the distribution relations of degree $k-1$. Let*

$$f(x) = \sum_{-\infty}^{\infty} c_n e^{2\pi i n x}$$

be the Fourier series of f. Then: $c_0 = 0$; $c_n = c_1/n^k$ for $n > 0$; $c_{-n} = c_{-1}/n^k$ for $n > 0$.

Proof. By definition, and using simple transformations, we have:

$$\begin{aligned}
c_n &= \int_0^1 f(x)e^{-2\pi i n x}\,dx \\
&= N^{k-1}\int_0^1 \sum_{j=0}^{N-1} f\left(\frac{x}{N}+\frac{j}{N}\right)e^{-2\pi i n x}\,dx \\
&= N^k \sum_{j=0}^{N-1} f\left(u+\frac{j}{N}\right)e^{-2\pi i n N u}\,du \\
&= N^k \int_0^1 f(u)e^{-2\pi i n N u} \\
&= N^k c_{nN}.
\end{aligned}$$

For $n = 0$, pick $N \neq 0$ to conclude $c_0 = 0$. Then take $n = 1$ or $n = -1$ to conclude the proof.

In view of the uniqueness theorem, the Fourier series for the Bernoulli distribution must be a linear combination of the above Fourier series and its conjugate. In fact, one knows classically that

$$\mathbf{B}_k(\langle x\rangle) = -\frac{k!}{(2\pi i)^k}\sum_{n\neq 0}\frac{e^{2\pi i n x}}{n^k}.$$

The Hurwitz zeta function. For $0 < u \leq 1$ let

$$\zeta(s,u) = \sum_{n=0}^{\infty}\frac{1}{(n+u)^s}.$$

This expression defines an analytic function of the complex variable s for $\mathrm{Re}(s) > 1$, and can be analytically continued into the whole plane, except for a simple pole at $s = 1$. For each real number t, let $\{t\}$ be the unique number congruent to $t \bmod \mathbf{Z}$, and such that

$$0 < \{t\} \leq 1.$$

Then one verifies at once that the map into the additive group of meromorphic functions given by

$$x \mapsto \zeta(s, \{x\})$$

is a distribution of degree $-s$. Here we can take s to be any complex number by analytic continuation. The Bernoulli distribution is a homomorphic image of the Hurwitz distribution, via the homomorphism evaluation at $s = 1 - k$, because of the classical Hurwitz relation:

$$\zeta(1-k, u) = -\frac{1}{k}\mathbf{B}_k(u).$$

The gamma distribution. Define

$$G(z) = \frac{1}{\sqrt{2\pi}}\Gamma(z).$$

We view G as defined on $\mathbf{Q}/\mathbf{Z}$ with the origin deleted, but then with values in the factor group

$$G : \mathbf{Q}/\mathbf{Z} \to \mathbf{C}^*/\mathbf{Q}_{\mathrm{a}}^*$$

of the multiplicative group of complex numbers modulo the group of nonzero algebraic numbers. The classical identity

$$\prod_{j=0}^{N-1}\frac{1}{\sqrt{2\pi}}\Gamma\left(z+\frac{j}{N}\right) = \frac{1}{\sqrt{2\pi}}\Gamma(Nz)N^{1/2-Nz}$$

shows that G defines a distribution.

Furthermore, this distribution also depends on the Hurwitz distribution. If we take the power series expansion of the Hurwitz zeta function at any complex number s_0, then the value defines a distribution. But we may also take the coefficients of higher powers $(s - s_0)^m$ for $m \geq 1$. Then we get the distribution relations, and in addition other terms coming from the overflow from lower terms. In particular, we have the classical expansion at $s = 0$, namely

$$\zeta(s,u) = \frac{1}{2} - u + \log\left(\frac{1}{\sqrt{2\pi}}\Gamma(u)\right)s + O(s^2).$$

The distribution relations for $\log \frac{1}{\sqrt{2\pi}}\Gamma$ follows from the distribution relations for the Hurwitz zeta function. The extra term $N^{1/2-Nz}$ is explainable structurally from the constant term in the expansion, which is none other than $-\mathbf{B}_1(u)$, itself the first Bernoulli distribution. The next coefficient (that of s^2) would also satisfy the distribution relations, modulo the expressions due to the preceding terms.

We note that the gamma distribution is odd, because of the classical relation

$$\frac{1}{\sqrt{2\pi}}\Gamma(z)\frac{1}{\sqrt{2\pi}}\Gamma(1-z) = \frac{1/2}{\sin \pi z}.$$

Here of course we take z rational, so $\sin \pi z$ is algebraic.

Cyclotomic numbers. The function

$$x \mapsto e^{2\pi i x} - 1$$

defines a distribution into the multiplicative group of complex numbers (except at $x = 0$). This is immediate from the relation

$$\prod_{\zeta^N=1} (1 - \zeta X) = 1 - X^N.$$

If x ranges over rational numbers, then $e^{2\pi i x} - 1$ is just the numerator of the cyclotomic units, and may be called the cyclotomic numbers distribution. If the values are viewed as in $\mathbf{C}^*/\boldsymbol{\mu}$, then the distribution is even.

Modular units. In §6 we had defined the functions g_a with $a \in \mathbf{Q}^2$, $a \notin \mathbf{Z}^2$. It can easily be shown that if one changes a by a pair in $\mathbf{Z}^2$, then g_a changes by multiplication with a root of unity. We view the association

$$a \mapsto g_a$$

as a map of $\mathbf{Q}^2/\mathbf{Z}^2$ into the multiplicative group of meromorphic functions, modulo constants. Then this map satisfies the analogue of the distribution relations on $\mathbf{Q}^2/\mathbf{Z}^2$. It is an even distribution.

The Lobatchevski distribution. Define the Lobatchevski function

$$\lambda(x) = -\int_0^x \log\left|e^{2\pi i t} - 1\right| dt.$$

Then λ is a distribution, being composed of the cyclotomic numbers distribution, the absolute value, the logarithm (which are homomorphisms), and the integral which is easily seen to preserve the distribution relations. Milnor has investigated this distribution in connection with hyperbolic geometry as follows. Let H be hyperbolic 3-space. This is the set of points

$$(x_1, x_2, y) \in \mathbf{R} \times \mathbf{R} \times \mathbf{R}^+$$

so (x_1, x_2) is an ordinary point in the plane, and $y > 0$. We endow H with the metric

$$\frac{dx_1^2 + dx_2^2 + dy^2}{y^2}.$$

Select four distinct points in the plane, and let T be the tetrahedron in H whose vertices are at these points. Then it can be shown that opposite dihedral angles are equal. (The dihedral angles are the angles between the faces of the tetrahedron.) Let α, β, γ be the dihedral angles. Then

$$\alpha + \beta + \gamma = \pi,$$

and the volume of the tetrahedron is precisely given in terms of the Lobatchevski function, by

$$\mathrm{Vol}(T) = \iiint_T \frac{dx_1\, dx_2\, dy}{y^3} = \lambda(\alpha) + \lambda(\beta) + \lambda(\gamma).$$

The search for relations among such volumes had led Milnor to consider the Lobatchevski function and its relations, now known as the distribution relations, and to show that it had the maximum rank (its values being viewed as generated a vector space over the rationals). We discuss this systematically below.

The Stickelberger distribution. Let $h : \mathbf{Q}/\mathbf{Z} \to \mathbf{C}$ be a distribution. Let $G(N) \approx (\mathbf{Z}/N\mathbf{Z})^*$ under an association $a \mapsto \sigma_a$, as in cyclotomic theory. Define

$$g_N(x) = \frac{1}{|G(N)|} \sum_{a \in (\mathbf{Z}/N\mathbf{Z})^*} h(xa)\sigma_a^{-1},$$

for $x \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}$. Then g_N takes values in the group algebra $\mathbf{C}[G(N)]$, and if $M \mid N$, then the image of $g_N(x)$ under the canonical homomorphism $G(N) \to G(M)$ is equal to $g_M(x)$. Thus we may define

$$\mathrm{St}_h(x) = \lim g_N(x)$$

in the injective limit of the group algebras (as vector spaces over $\mathbf{C}$), ordered by divisibility, with the injection from one level to the next given by sending one group element to the sum of all the group elements lying above it under the canonical homomorphism. Then one sees that $x \mapsto \mathrm{St}_h(x)$ is a distribution, called the Stickelberger distribution St_h associated with h.

The universal distribution. Fix an integer $N > 1$, and consider the subgroup of $\mathbf{Q}/\mathbf{Z}$ consisting of those elements with order N, that is

$$\frac{1}{N}\mathbf{Z}/\mathbf{Z} = (\mathbf{Q}/\mathbf{Z})_N = Z_N \quad \text{(by definition).}$$

One can then form the universal distribution (restricted to Z_N) in the obvious way. We start with the free abelian group $Fr(Z_N)$, and factor out the distribution relations (say of degree 0 for simplicity) with level M dividing N. If we denote the subgroup of these relations by $DR(N)$, then the universal distribution is simply the factor group $\mathbf{U}(N) = Fr(Z_N)/DR(N)$, with the natural map of Z_N into this factor group. A theorem of Kubert [**Ku 2**] (see [**Ku-L 1**] or [**L 1**], Chapter 2 and Yamamoto [**Ya**]) asserts:

The universal distribution $U(N)$ is a free abelian group on $\phi(N)$ generators. Let

$$N = \prod p_i^{n_i}$$

be the factorization of N into prime powers. A free basis for $\mathbf{U}(N)$ is given by the elements

$$\sum \frac{a_i}{p_i^{n_i}}$$

with $a_i \in (\mathbf{Z}/p_i^{n_i}\mathbf{Z})^*$ (so a_i prime to p_i) and $a_i \neq 1$, or $a_i = 0$.

The general philosophy is that if a distribution arises naturally, and is not "obviously" special, then it is in fact universal, possibly with the parity odd or even. For example, the Bernoulli distribution is obviously not universal since it is rational valued, but it can be shown that its associated Stickelberger distribution is universal of the appropriate parity (for values into abelian groups where 2 is invertible). The cyclotomic number distribution is universal even (with values as above). This is a reformulation of a theorem of H. Bass. The modular units give a universal even distribution, cf. [**Ku-L 1**]. Rohrlich conjectured that the gamma distribution is universal odd. Since the values are in the group $\mathbf{C}^*$ modulo non-zero algebraic numbers, this would amount to a theorem in the theory of transcendental numbers. Similarly, Milnor conjectured that the Lobatchevski distribution is universal odd (values in the additive group of complex numbers). For a general discussion of distributions, cf. Chapter 1 of [**Ku-L 1**], and the bibliography contained in that book, as well as [**L 1**], Chapter 2, containing proofs for all the theorems mentioned here. Distributions on projective systems arose in number theory through the work of Iwasawa, reformulated by Mazur. The point of view on injective systems taken here stems from the Kubert-Lang series of papers. The subtleties involving 2-torsion in the universal distribution have been dealt with systematically by Kubert, cf. [**Ku 3**] and the bibliography at the end of [**Ku-L 1**]. They involve the cohomology of ± 1 in the universal distribution, and have applications to modular functions, and possibly to algebraic topology.

In this Appendix, I did not want to go systematically into the study of distributions. I merely wanted to point out the general pattern underlying much of the formalism which arises in connection with §2, §3, §4, §8 and in other parts of mathematics.

Note: The author wishes to point out to the reader that some errors may have been introduced in this paper during the corrections process, after the material had been proofread.

BIBLIOGRAPHY

[An 1] G. ANDERSON, Logarithmic derivatives of Dirichlet L-functions and the periods of abelian varieties, to appear.

[An 2] G. ANDERSON, to appear.

[Be] N. BEILINSON, Higher regulators and values of L-functions of curves, Functional Analysis 14 No. 2 (1980), pp. 46–47.

[Be] R. BERGELSON, The index of the Stickelberger ideal of order k on $C^k(N)$, to appear, Annals of Math.

[Bl] S. BLOCH, Algebraic K-theory and class field theory for arithmetic surfaces, to appear.

[Bo] F. A. BOGOMOLOV, On the algebraicity of l-adic representations, CR Acad. Sci. Paris 290 No. 15 (1980) pp. 701–703.

[CN] P. CASSOU-NOGUÈS, Valeurs aux entiers négatifs des fonctions zeta et fonctions zeta p-adiques, Invent. Math. 51 (1979) pp. 29–59.

[Co 1] J. COATES, p-adic L-functions and Iwasawa's theory, Durham Conference on algebraic number theory and class field theory, 1976.

[Co 2] J. COATES, Fonctions zeta partielles d'un corps de nombres totalement réel, Seminaire Delange-Pisot-Poitou, 1974–1975.

[Co-L] J. COATES and S. LICHTENBAUM, On l-adic zeta functions, Ann. of Math. 98 (1973) pp. 498–550.

[Co-Si 1] J. COATES and W. SINNOTT, On p-adic L-functions over real quadratic fields, Invent. Math 25 (1974) pp. 253–279.

[Co-Si 2] J. COATES and W. SINNOTT, Integrality properties of the values of partial zeta functions, Proc. London Math. Soc. (1977) pp. 365–384.

[Co-Wi 1] J. COATES and A. WILES, On the conjecture of Birch and Swinnerton-Dyer, Invent. Math. 39 (1977) pp. 223–251.

[Co-Wi 2] J. COATES and A. WILES, Kummer's criterion for Hurwitz numbers, Kyoto Conference on Algebraic Number Theory, 1977.

[Co-Wi 3] J. COATES and A. WILES, On p-adic L-functions and elliptic units, J. Austr. Math. Soc. 26 (1978) pp. 1–25.

[Da-H] H. DAVENPORT and H. HEILBRONN, On the density of discriminants of cubic fields II, Proc. Royal Soc. 322 (1971) pp. 405–420.

[De] P. DELIGNE, Valeurs de fonctions L et periodes d'integrales, Proc. Symp. Pure Math. Vol. 33 (1979) pp. 313–346.

[De-Ra] P. DELIGNE and M. RAPOPORT, Schémas de modules des courbes élliptiques, Springer Lecture Notes 349 (1973).

[Dr] V. G. DRINFELD, Two theorems on modular curves, Functional analysis and its applications, Vol. 7 No. 2 translated from the Russian April–June 1973 pp. 155–156.

[Fe-W] B. FERRERO and L. WASHINGTON, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. Math. 109 (1979) pp. 377–395.

[Gra] G. GRAS, Classes d'idéaux des corps abéliens et nombres de Bernoulli généralisés, Annales Institut Fourier Université de Grenoble, Tome XXVII, Fasc. 1 (1977) pp. 1–66.

[**Gre 1**] R. GREENBERG, On p-adic L-functions and cyclotomic fields I, Nagoya Math. J. No. 56 (1974) pp. 61–77.

[**Gre 2**] R. GREENBERG, On p-adic L-functions and cyclotomic fields II, Nagoya Math. J. No. 67 (1977) pp. 139–158.

[**Gro 1**] B. GROSS, p-adic L-series at $s = 0$, to appear.

[**Gro 2**] B. GROSS, On the periods of Abelian integrals and a formula of Chowla and Selberg, Invent. Math. 45 (1978) pp. 193–211.

[**Iw 1**] K. IWASAWA, On Γ-extensions of algebraic number fields, Bull. AMS 65 (1959) pp. 183–192.

[**Iw 2**] K. IWASAWA, On p-adic L-functions, Ann. of Math. 89 (1969) pp. 198–205.

[**Iw 3**] K. IWASAWA, A class number formula for cyclotomic fields, Ann. of Math. 76 (1962) pp. 171–179.

(For a more complete list of eighteen papers by Iwasawa on the subjects of concern here, cf. the bibliography at the end of my *Cyclotomic Fields* Vol. 2.)

[**Kato**] K. KATO, Higher Local Class Field Theory, Proc. Japan Acad. 53 (1977) pp. 140–143 and 54 (1978) pp. 250–255.

[**Ka-L**] N. KATZ and S. LANG, Finiteness Theorems in Geometric Class Field Theory, to appear in l'Enseignement Mathematique, 1982.

[**Ka-M**] N. KATZ and B. MAZUR, to appear.

[**Ke 1**] D. KERSEY, Modular units inside cyclotomic units, Ann. of Math. 112 (1980) pp. 361–380.

[**Ke 2**] D. KERSEY, The index of modular units, to appear.

[**Kl**] F. KLEIN, Uber die elliptischen Normalkurven der n-ten Ordnung, Abh. math.-phys. Klasse Sächsischen Kgl. Gesellschaft Wiss. Bd 13, Nr. IV (1885) pp. 198–254.

[**Ku 1**] D. KUBERT, The 2-primary component of the ideal class group in cyclotomic fields, to appear.

[**Ku 2**] D. KUBERT, The universal ordinary distribution, Bull. Soc. Math. France **107** (1979), 179–202.

[**Ku 3**] D. KUBERT, The $\mathbf{Z}/2\mathbf{Z}$ cohomology of the universal ordinary distribution, Bull. Soc. Math. France **107** (1979), 203–224.

[**Ku-L 1**] D. KUBERT and S. LANG, Modular Units, Springer Verlag, 1981.

[**Ku-L 2**] D. KUBERT and S. LANG, Modular units inside cyclotomic units, Bull. Soc. Math. France 107 (1979) pp. 161–178.

[**Kum 1**] E. KUMMER, Mémoire sur la théorie des nombres complexes composeés de racines de l'unité et de nombres entiers, J. Math. Pure et Appliquees, XVI (1851) pp. 377–498 (=Collected Works I, especially p. 452).

[**Kum 2**] E. KUMMER, Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, Math. Abh. Konig. Akad. Wiss. Berlin (1856) pp. 1–47, (Collected Works I, especially p. 583). *Note*: In CW I, p. 626, Kummer gives what is known as the Stickelberger congruence for Gauss sums in terms of factorials.

[**L 1**] S. LANG, Cyclotomic Fields Vols. 1 and 2, Springer Verlag 1979 and 1980.

[**L 2**] S. LANG, Elliptic functions, Addison Wesley, 1974.

[**L 3**] S. LANG, Division points on curves, Ann. Mat. Pura Appl. IV, Tomo LXX (1965) pp. 229–234.

[**L 4**] S. LANG, Unramified class field theory over function fields in several variables, Ann. of Math. 64 (1956) pp. 286–325.

[**L 5**] S. LANG, Sur les séries L d'une variété algébrique, Bull. Soc. Math. France 84 (1956) pp. 385–407.

[**L 6**] S. LANG, L-series of a covering, Proc. Nat. Acad. Sci. USA (1956).

[**Lgds**] R. LANGLANDS, Modular forms and l-adic representations, Springer Lecture Notes 349 (1973) pp. 361–500.

[**Le 1**] H. W. LEOPOLDT, Eine Verallgemeinerung der Bernoullische Zahlen, Abh. Math. Sem. Hamburg (1958) pp. 131–140.

[**Le 2**] H. W. LEOPOLDT, Uber Einheitengruppe und Klassenzahl reeler abelscher Zahlkörper, Abh. Deutsche Akad. Wiss. Berlin Math. 2 (1954) Akademie Verlag.

[**Le 3**] H. W. LEOPOLDT, Uber die Arithmetik algebraischen Zahlkörper, J. reine angew. Math 209 (1962) pp. 54–71.

(For a more complete list of eleven papers of Leopoldt on cyclotomic fields and p-adic L-functions, cf. the bibliography at the end of *Cyclotomic Fields* Vol. 2.)

[**Ma 1**] B. MAZUR, Modular curves and the Eisenstein ideal, Pub. IHES No. 47 (1977) pp. 33–186.

[**Ma 2**] B. MAZUR, Rational isogenies of prime degree, Invent. Math. 44 (1978) pp. 129–162.

[**Ma-W**] B. MAZUR and A. WILES, to appear.

[**Mi 1**] J. MILGRAM, Odd index subgroups of units in cyclotomic fields and applications, Springer Lecture Notes no. 854 (1981).

[**Mi 2**] J. MILGRAM, Patching techniques in surgery and the solution of the compact space form problem, to appear.

[**O-T**] F. OORT and J. TATE, Group schemes of prime order, Ann. Scient. Ec. Norm. Sup. serie 4, 3 (1970) pp. 1–21.

[**Pa**] A. M. PARSHIN, Class field theory for arithmetical schemes, preprint, and also Uspekhi Matem. Nauk 39 (1975) p. 253 and Izvestija Acad. Nauk. SSSR Ser. Matem. 40 (1976) pp. 736–773.

[**Ra**] K. RAMACHANDRA, Some applications of Kronecker's limit formula, Ann. of Math. 80 (1964) pp. 104–148.

[**Ray 1**] M. RAYNAUD, Schémas en groupes de type $(p,\ldots,p)$, Bull. Soc. Math. France 102 (1974) pp. 241–280.

[**Ray 2**] M. RAYNAUD, Faisceaux amples sur les schémas en groupes et les éspaces homogènes, Springer Lecture Notes 119 (1970).

[**Ri**] K. RIBET, A modular construction of unramified p-extensions of $\mathbf{Q}(\mu_p)$, Invent. Math. 34 (1976) pp. 151–162.

[**Ro 1**] G. ROBERT, Unités élliptiques, Bull. Soc. Math. France Supplément, Décembre 1973 No. 36.

[**Ro 2**] G. ROBERT, Nombres de Hurwitz et unités élliptiques, Ann. Scient. Ec. Norm. Sup. 4e serie t. 11 (1978) pp. 297–389.

[**Se 1**] J. P. SERRE, Propriétés Galoisiènnes des points d'ordre fini des courbes élliptiques, Invent. Math. 15 (1972) pp. 259–331.

[**Se 2**] J. P. SERRE, Classes des corps cyclotomiques d'après Iwasawa, Bourbaki Seminar 1958.

[**Shim**] G. SHIMURA, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten and Princeton University Press 1971.

[**Shin 1**] T. SHINTANI, On a Kronecker limit formula for real quadratic fields, J. Fac. Sci. Univ. Tokyo Sec. IA, 24 (1977) pp. 167–199.

[**Shin 2**] T. SHINTANI, On certain ray class invariants of real quadratic fields, J. Math. Soc. Japan Vol. 30 No 1 (1978) pp. 139–167.

[Sie] C. L. SIEGEL, Lectures on advanced analytic number theory, Tata Institute Lecture Notes 1961.

[Sin 1] W. SINNOTT, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math. 108 (1978) pp. 107–134.

[Sin 2] W. SINNOTT, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980) pp. 181–234.

[St] H. STARK, L-functions at $s = 1$:

I: Advances in Math. 7 (1971) pp. 301–343,

II: Ibid. 17 (1975) pp. 60–92,

III: Ibid 22 (1976) pp. 64–84,

IV: Ibid 35 (1980) pp. 197–235.

[St B] H. STARK, Class fields and modular forms of weight 1, Springer Lecture Notes 601, 1976; (Bonn conference on modular forms in one variable).

[Ta 1] J. TATE, On Stark's conjectures on the behavior of $L(s, \chi)$ at $s = 0$, to appear, Shintani Memorial Volume, J. Fac. Sci. Tokyo 1982.

[Ta 2] J. TATE, Les conjectures de Stark sur les fonctions L d'Artin en $s = 0$, notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher, Lecture Notes to appear in the Birkhauser Boston Series.

[Ta 3] J. TATE, Algebraic cycles and poles of zeta functions, in Arithmetical Algebraic Geometry, Conference held at Purdue University, 1963, Harper and Row, New York 1965.

[Ta 4] J. TATE, The conjecture of Birch and Swinnerton-Dyer and a geometric analogue, Dix exposés sur la cohomologie des schémas, North Holland, 1968 (=Seminaire Bourbaki 352, 1966).

[Ta 5] J. TATE, Arithmetic of Elliptic Curves, Invent. Math. 23 (1974) pp. 179–206.

[Va 1] H. S. VANDIVER, Fermat's last theorem and the second factor in the cyclotomic class number, Bull. AMS 40 (1934) pp. 118–126.

[Va 2] H. S. VANDIVER, Fermat's last theorem, Am. Math. Monthly 53 (1946) pp. 555–576.

[Wall] C. T. C. WALL, Classification of hermitian forms VI, Ann. of Math. 103 (1976) pp. 1–80.

[Wash] L. WASHINGTON, The non-p-part of the class number in a cyclotomic $\mathbf{Z}_p$-extension, Invent. Math. 49 (1978) pp. 87–97.

[Wi] A. WILES, Modular curves and the class group of $\mathbf{Q}(\zeta_p)$, Invent. Math. 58 (1980) pp. 1–35.

[Ya 1] K. YAMAMOTO, The Gap group of multiplicative relationships of Gaussian sums, Symposia Mathematica No. 15 (1975) pp. 427–440.

[Ya 2] K. YAMAMOTO, On a conjecture of Hasse concerning multiplicative relations, of Gaussian sums, J. Combin. Theory 1 (1966) pp. 476–489.

[Yu] JING YU, A cuspidal class number formula for the modular curves $X_1(N)$, Math. Ann. 252 (1980) pp. 197–216.

[Zi] H. ZIMMER, Lecture Notes in Math., vol. 262, Springer-Verlag, New York, 1972.

Current address: Department of Mathematics, Box 2155 Yale Station, Yale University, New Haven, Connecticut 06520