Class groups and Galois representations

Kenneth A. Ribet

UC Berkeley

ENS
February 15, 2008

For the J. Herbrand centennaire, I will revisit a subject that I studied when I first came to Paris as a mathematician, in 1975–1976. At the time, I was working on a problem that was posed to me by J-P. Serre, who encountered a variant of the problem in connection with the Ramanujan τ-function ("Une interprétation des congruences relatives à la fonction τ de Ramanujan").

In my work, I explained how to construct, using modular forms, unramified extensions of cyclotomic fields whose existence I believed to be well known.

I realized only in discussions with Coates and Serre that the extensions that I constructed had been known only conjecturally. My construction provided the first proof that they existed.

I learned around the same time that my construction provided a converse to a theorem of Herbrand. In “Cyclotomic Fields,” Lang provided a proof of Herbrand’s theorem and mentioned that I had proved the converse. I am deeply grateful that my name is associated with that of Herbrand.

Not long after 1976, my method was adapted by Mazur and Mazur–Wiles to prove the “Main Conjecture” of Iwasawa theory.

Some years later, a radically different proof of the Main Conjecture was given by Thaine, Kolyvagin and Rubin. Because their proof was simpler than the original, the modular forms technique received less attention than before.

In recent times, however, it has re-surfaced in new contexts.

Presentation of the Problem

Start with a number field K: this is a finite extension of $\mathbf{Q}$. We view K as a subfield of the field $\overline{\mathbf{Q}}$ of all complex algebraic numbers.

Algebraic number theory began with the study of unique factorization—and its failure—in the ring of integers $\mathcal{O}_K$ of K.

The extent to which unique factorization fails is measured by a finite group C_K, the class group of K. This group may be defined by taking the group of fractional ideals of K, i.e., the free abelian group on the set of maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$, and dividing by the group of principal fractional ideals.

Let H be the maximal abelian unramified extension of K in $\overline{\mathbf{Q}}$ (the Hilbert class field of K). The Artin map of class field theory furnishes an isomorphism

$$C_K \xrightarrow{\sim} \mathrm{Gal}(H/K), \qquad \mathfrak{p} \mapsto \mathrm{Frob}_{\mathfrak{p}}\,.$$

Here, $\mathrm{Frob}_{\mathfrak{p}}$ is the *Frobenius* element of the Galois group that corresponds to the prime $\mathfrak{p}$ of K.

The Artin isomorphism, in particular, enables us to view $C_K \approx \mathrm{Gal}(H/K)$ as a quotient of the abelianization of $G_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$.

Equivalently, the abelian group $\mathrm{Hom}(C_K, \mathbf{C}^*)$ dual to C_K becomes a subgroup of the group $\mathrm{Hom}(G_K, \mathbf{C}^*)$ of continuous characters of the Galois group of K.

The subgroup in question is the group of *unramified* characters of the Galois group G_K. As such, it can be viewed as the first example of a *Selmer group*.

In general, Selmer groups are tough nuts to crack. Much is known about the class groups C_K, but it would not be out of place to say that already these Selmer groups present mysteries to us. For example, it is unknown whether or not there are infinitely many quadratic fields K for which C_K is trivial.

Nevertheless, partial information about groups C_K can often be extracted from analytic formulas that are related to the Dedekind zeta function

$$\zeta_K = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}, \quad \Re s > 1.$$

The function ζ_K may be continued analytically to a meromorphic function on the complex plane with a simple pole at $s = 1$ and no other poles. The residue of the pole is given by a formula that involves the class number $h_K = \# C_K$, as well as invariants derived from the unit group $\mathcal{O}_K^*$ of K.

The residue also involves various powers of π. As Serre has stressed, it is cleaner to use the functional equation of ζ_K and look at its behavior around $s = 0$ instead of $s = 1$. This tends to lead to simpler formulas!

If K is an abelian extension of $\mathbf{Q}$ and $K^+ = K \cap \mathbf{R}$ is the real subfield of K, then the unit groups of K and K^+ are sufficiently alike that one obtains a very useful formula for the ratio

$$h_K^- := h_K / h_{K^+}$$

between the class numbers of K and K^+, which is called the *first factor* of h_K. (The second factor is then $h_K^+ = h_{K^+}$.)

This is especially true if $K = K^+$.

When $K = \mathbf{Q}(\mu_p)$ is the field of pth roots of unity ($p > 3$, say), we obtain in particular the concrete expression

$$h_k^- = 2^{\frac{p-3}{2}} p \prod_{\epsilon} L(0, \epsilon)$$

expressing the "first factor" of the class number of K in terms of finite character sums. In this formula, the product runs over the *odd* complex-valued characters of the Galois group

$$\Delta = (\mathbf{Z}/p\mathbf{Z})^* = \mathrm{Gal}(K/\mathbf{Q}),$$

i.e., those characters ϵ satisfying $\epsilon(-1) = -1$. The L-value, obtained by analytic continuation, is simply

$$L(0, \epsilon) = \frac{-1}{p} \sum_{a \bmod p} \epsilon(a) a.$$

Kummer

The field $K = \mathbf{Q}(\mu_p)$ is perhaps the birthplace of modern number theory. Recall that Kummer proved Fermat's Last Theorem for exponent p whenever the prime p is *regular* in the sense that h_K is prime to p.

Further, he proved that $h_K = h_K^- h_K^+$ is prime to p if and only if h_k^- is prime to p. In other words: if p divides $h_K^+ = h_{K^+}$, then p divides h_k^- as well.

Kummer's criterion states that p is regular if and only if p divides the numerator of none of the Bernoulli numbers B_2, B_4, $B_6, \ldots, B_{p-3}$. It derives from a mod p relation between the factors $L(0, \epsilon)$ and Bernoulli numbers.

To see how Kummer's criterion is related to our formula for h_K^-, we view the characters ϵ as taking values in $\mathbf{Q}_p^*$ instead of $\mathbf{C}^*$. Also, we write these characters as odd powers of the standard Teichmüller character ω whose mod p reduction is the identity map $\Delta = (\mathbf{Z}/p\mathbf{Z})^* \to (\mathbf{Z}/p\mathbf{Z})^*$. The term $2^{\frac{p-3}{2}} pL(0, \omega^{-1})$ is a p-adic unit, while the remaining factors $L(0, \epsilon)$ in the product for h_k^- are p-adic integers.

These factors may be written $L(0, \omega^{k-1})$ for k even, $2 \leq k \leq p-3$. A simple congruence due to Kummer proves that p divides $L(0, \omega^{k-1})$ if and only if p divides the Bernoulli number B_k.

To summarize: p divides h_K if and only p divides h_k^-, and p divides h_k^- if and only if p divides one of the $L(0, \omega^{k-1})$. Finally, p divides a given $L(0, \omega^{k-1})$ if and only if it divides the corresponding Bernoulli number B_k.

Assembling this information, we see that p is regular if and only if it divides none of the B_k and irregular if and only if it divides at least one of them.

Galois action

Structually, p is regular if and only if the p-Sylow subgroup A of the class group of $\mathbf{Q}(\mu_p)$ is zero. The p-primary torsion abelian group A is naturally a $\mathbf{Z}_p$-module. Further, it carries a functorial action of the Galois group $\Delta = \mathrm{Gal}(K/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^*$.

Canonically,

$$A = \bigoplus_{\epsilon} A(\epsilon),$$

where $A(\epsilon)$ is the subgroup of A on which Δ acts as ϵ; the direct sum is over the $\mathbf{Z}_p^*$-valued characters ϵ of Δ.

By the middle of the last century, a tremendous amount of information about the components $A(\epsilon)$ had been amassed.

Herbrand proved that $A(\omega)$ vanishes and also, for $k = 2, 4, \ldots, p-3$, that $A(\omega^{1-k})$ is annihilated by the p-adic integer $L(0, \omega^{k-1})$. In particular, if $L(0, \omega^{k-1})$ is a p-adic unit (i.e., if p doesn't divide B_k), then $A(\omega^{1-k}) = 0$.

Leopoldt proved for odd characters ϵ that the vanishing of $A(\epsilon)$ implies the vanishing of $A(\omega\epsilon^{-1})$; this statement refines Kummer's implication $p|h^+ \Longrightarrow p|h_k^-$.

The odd part of A decomposes as the direct sum

$$\bigoplus A(\omega^{1-k}), \qquad k = 2, 4, \ldots, p-3.$$

Meanwhile, the *order of* the odd part A^- of A is the "p-part" of the integer h_K^-, which decomposes as the product of terms $L(0, \omega^{k-1})$.

Is the decomposition of the order of the group A^- a reflection of the decomposition of A^- itself?

Despite the suggestive theorem of Herbrand to the effect that the individual odd eigenspaces of A are annihilated by the corresponding individual L-values, there is no a priori relationship between the direct sum decomposition of the odd part of A and the product decomposition of its order!

However, such a relationship was predicted by Iwasawa theory and established in the early 1980s by Mazur and Wiles.

A theorem of Mazur–Wiles

For each k, the order of $A(\omega^{1-k})$ is the largest power of p dividing $L(0, \omega^{k-1})$.

Because the two numbers being compared for each k are equal in the large (i.e., after multiplying together the terms of all k), to prove the above statement, one can:

- Prove, for each k, that the p-part of $L(0, \omega^{k-1})$ divides the order of $A(\omega^{1-k})$, or
- Prove, for each k, that the order of $A(\omega^{1-k})$ divides the p-part of $L(0, \omega^{k-1})$.

The first method, which amounts to showing that an eigenspace of a class group is "big," goes back to my 1976 construction of unramified extensions. This is the method of Mazur and Wiles.

In my original article, I proved only a mod p statement: if $L(0, \omega^{k-1})$ is divisible by p, then $A(\omega^{1-k})$ is nontrivial. To get the full theorem, Mazur–Wiles consider together all the fields $\mathbf{Q}(\mu_{p^n})$ ($n \geq 1$) and use the tools of Iwasawa theory.

The second method, due to Thaine and Kolyvagin, is explained by K. Rubin in his appendix to Lang's "Cyclotomic Fields." Using the language of Euler systems, one shows that ideal class groups are "not too big" by exhibiting many principal ideas. This is also the principle behind Stickelbeger's theorem!

The main idea of my 1976 article is to use the hypothesis $p|L(0,\omega^{k-1})$ to construct a reducible 2-dimensional mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ that appears as an extension of the 1-dimensional representation with character ω^{k-1} by the 1-dimensional representation with trivial Galois action. This extension gives rise to an element of

$$\mathrm{H}^1\left(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathbf{F}_p(\omega^{1-k})\right) \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(\overline{\mathbf{Q}}/K), \mathbf{F}_p)(\omega^{1-k}).$$

One proves by local arguments that this element is an *unramified* homomorphism and thereby obtains the non-triviality of $A(\omega^{1-k})$.

The method is quite flexible, but one needs some way of constructing the representation. Basically, what's required is to prove the existence of a **GL**(2)-cusp form that's congruent mod p to the Eisenstein series whose constant term is congruent to the number $L(0, \omega^{k-1})$ (which is 0 mod p by hypothesis). One can do this within the realm of modular forms (my method), think geometrically about modular curves (Wiles et. al.) or work with cohomology (Harder, . . .).

As I mentioned at the outset, the upper-bound method of Thaine and Kolyvagin seems more elementary than the lower-bound method of modular forms and Galois representations.

However, in contexts where there is no a priori formula for the order of the class group (or a Selmer group analogue), both methods (upper and lower bounds) are likely to be required if one wants to calculate the order.

For example, let E be an elliptic curve over $\mathbf{Q}$, and let $L(E, s)$ be the L-series of E. Suppose that $L(E, 1)$ is non-zero. Then Kolyvagin proved that $E(\mathbf{Q})$ is finite and moreover that the Shafarevich-Tate group $Ш(E/\mathbf{Q})$ is finite as well. Because the Mordell–Weil group $E(\mathbf{Q})$ is finite, the group $Ш$ is essentially a Selmer group.

The conjecture of Birch and Swinnerton-Dyer predicts an equality of the shape

$$\#(Ш(E/\mathbf{Q})) \stackrel{?}{=} \frac{L(E,1)}{\Omega} \frac{\#(E(\mathbf{Q}))^2}{\prod_\ell w_\ell}$$

where Ω is a period and the w_ℓ are local Tamagawa numbers (one for each prime ℓ, almost all equal to 1). Kolyvagin showed that the left-hand side divides the product of the right-hand side and a modest fudge factor. To prove something close to the desired equality, one must complement Kolyvagin's *upper* bound by a lower bound.

C. Skinner and E. Urban expect to obtain lower-bound type information by a method that is inspired by the method use to bound class groups from above. Beginning with an elliptic curve and congruences between Eisenstein series and cusp forms on $\mathbf{U}(2,2)$, they obtain 4-dimensional Galois representations that lead to non-trivial elements of Tate–Shafarevich groups.