

KUMMER'S CRITERION ON CLASS NUMBERS OF CYCLOTOMIC FIELDS

SEAN KELLY

ABSTRACT. Kummer's criterion is that p divides the class number of $\mathbb{Q}(\mu_p)$ if and only if it divides the numerator of some Bernoulli number B_k for $k = 2, 4, \dots, p-3$. This talk will start with explaining how finite groups of Dirichlet characters are in bijection with finite Abelian extensions of \mathbb{Q} , and why the class number of an Abelian CM field is "almost" computable. This computation involves the generalized Bernoulli numbers, giving a partial result similar to Kummer's criterion.

In the second half of the talk I will discuss a "Kummer-like" criterion, Herbrand's theorem. It is a refinement of previous result in the sense that it tells us more about the structure of the ideal class group of $\mathbb{Q}(\mu_p)$ as a $\text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ -module. If there's time, I'll discuss the first step of Ribet's proof of the converse of Herbrand's theorem.

CONTENTS

| | |
|--|----|
| 1. Introduction | 2 |
| 2. Kummer's Criterion | 2 |
| 2.1. Finite Abelian extensions of \mathbb{Q} | 2 |
| 2.2. Generalized Bernoulli Numbers | 5 |
| 2.3. L-functions | 6 |
| 2.4. CM fields have "almost" computable class number | 8 |
| 2.5. Kummer's criterion | 9 |
| 3. Herbrand's theorem and its converse | 10 |
| 3.1. Galois groups acting on the ideal class group | 10 |
| 3.2. Stickelberger's Theorem | 12 |
| 3.3. Some class field theory | 13 |
| 3.4. The first step of Ribet's proof | 13 |
| 4. References | 14 |

Throughout, p is an odd prime.

1. INTRODUCTION

Let h_p denote the number field $\mathbb{Q}(\mu_p)$, where μ_p denotes the group of p th roots of unity. Then $\mathbb{Q}(\mu_p)$ is an Abelian CM field with maximal totally real subfield $\mathbb{Q}(\mu_p + \mu_p^{-1})$.

Date: October 1, 2009.

Historically, we are interested in the class numbers of the fields $\mathbb{Q}(\mu_p)$ because they tell us when we can prove special cases Fermat's Last Theorem using elementary methods from algebraic number theory. We denote by h_p the class number of $\mathbb{Q}(\mu_p)$. Similarly denote by h_p^+ the class number of $\mathbb{Q}(\mu_p + \mu_p^{-1})$, and let

$$h_p^- = \frac{h_p}{h_p^+}$$

be what's called the relative class number. Note that even though we use the letter h to denote it, it isn't actually the class number of anything in particular. We define a prime to be **irregular** if $p \mid h_p$.

The **Bernoulli numbers** are defined by,

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}$$

So $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, and $B_i = 0$ for odd i . Some people set $B_0 = B_1 = 0$. The Bernoulli numbers appear as special values of the Riemann zeta function at the negative integers, $\zeta(1-k) = -\frac{1}{k} B_k$, $k = 2, 4, \dots$

Kummer's criterion is the following,

Theorem 1. *p is irregular if and only if p divides the numerator of some Bernoulli number B_k , $k = 2, 4, \dots, p-3$.*

2. KUMMER'S CRITERION

In this section we derive a weaker form of Kummer's Criterion,

Theorem 2. *$p \mid h_p^-$ if and only if p divides the numerator of some Bernoulli number B_k , $k = 2, 4, \dots, p-3$.*

2.1. Finite Abelian extensions of \mathbb{Q} . By the Kronecker-Weber theorem, every finite Abelian extension of \mathbb{Q} is contained in some cyclotomic field $\mathbb{Q}(\mu_n)$. Put another way,

$$\mathbb{Q}^{ab} = \mathbb{Q}(\mu_\infty) = \bigcup_n \mathbb{Q}(\mu_n)$$

Theorem 3. *The Galois group of $\mathbb{Q}(\mu_n)$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$ by sending $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ to the automorphism*

$$\sigma_m : \zeta_n \mapsto \zeta_n^m \quad \forall \zeta_n \in \mu_n$$

It follows that

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{ab} = \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times = (\widehat{\mathbb{Z}})^\times.$$

By the Galois correspondence, to understand finite abelian extensions of \mathbb{Q} we simply need to understand closed and open subgroups of $(\widehat{\mathbb{Z}})^\times$, and the easiest way to work with these are via the 1-dimensional representation, or characters, of $(\widehat{\mathbb{Z}})^\times$.

A **Dirichlet character** is a map $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$, although this is an oversimplification. Really a Dirichlet character is a character on $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that factors through the quotients,

$$\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \rightarrow \mathbb{C}^\times$$

Also, it is useful to consider Dirichlet character having as its codomain a field other than \mathbb{C} , as the following example illustrates.

Example 4.

Let $m \in (\mathbb{Z}_p/p\mathbb{Z}_p)^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times$. Then $m^{p-1} \equiv 1$ and since $p \nmid (p-1)$, m lifts by Hensel's lemma to a unique $\omega(m) \in \mathbb{Z}_p$ such that $(\omega(m))^{p-1} = 1$ and

$$\omega(m) \equiv m \pmod{p\mathbb{Z}_p}$$

The **Teichmüller character** is the character which assigns $m \mapsto \omega(m)$. Without confusion, can also consider it as a character $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \rightarrow \mathbb{Z}_p$ as the need arises.

Also notice that the Teichmüller character generates the entire group of characters on $(\mathbb{Z}/p\mathbb{Z})^\times$.

There is a smallest number $f \mid n$ such that χ factors through the quotient $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \rightarrow (\mathbb{Z}/f\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. This number is called the **conductor** of χ and is denoted f_χ .

The **parity** of a character is defined to be odd (or 1) if $\chi(-1) = -1$ and even (or 0) if $\chi(-1) = 1$.

There is a group law on Dirichlet characters, but it is not given by pointwise multiplication. However for our purposes we only need to know the following facts. 1. If χ, ψ are Dirichlet characters and $(f_\chi, f_\psi) = 1$, then $(\chi\psi)(m) = \chi(m)\psi(m)$. 2. If χ is a Dirichlet character then $(\chi^i)(m) = (\chi(m))^i$.

Now let X be a finite group of Dirichlet characters, and let f be the lcm of their conductors. Then we can define $H \subset (\mathbb{Z}/f\mathbb{Z})^\times$ as the intersection of all their kernels, $H = \bigcap_{\chi \in X} \ker \chi$. Under the Galois correspondence this gives a field $K \subset \mathbb{Q}(\mu_f)$, and all Abelian extensions of \mathbb{Q} arise this way. This gives a *covariant* bijection

$$\left\{ \begin{array}{c} \text{finite Abelian extensions} \\ K/\mathbb{Q} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finite groups } X \text{ of} \\ \text{Dirichlet characters} \end{array} \right\}$$

The benefit of working with groups of Dirichlet characters is first illustrated by the following formula, and later by the relative class number formula.

Theorem 5 (Conductor-discriminant formula). *Let X be a finite group of Dirichlet characters corresponding to a field K/\mathbb{Q} . Then*

$$|d_K| = \prod_{\chi \in X} f_\chi$$

where f_χ is the conductor of χ , d_K is the discriminant of K .

Example 6.

Let ρ be the unique character of order 2 on $(\mathbb{Z}/p\mathbb{Z})^\times$. Then ρ is the quadratic character mod p ,

$$\rho(m) = \left(\frac{m}{p}\right) = \begin{cases} 1, & m \text{ is a quadratic residue mod } p \\ -1, & \text{otherwise.} \end{cases}$$

Let $X = \{1, \rho\}$, and K the corresponding field. If $p \equiv 1 \pmod{4}$ then -1 is a quadratic residue, so ρ is an even character. Otherwise, ρ is an odd character. In the former case, $\ker \rho$ contains complex conjugation, and therefore K is real quadratic. Otherwise, K is imaginary quadratic. From the formula, $|d_K| = p$, so $K = \mathbb{Q}(\sqrt{\pm p})$.

Example 7.

Let X be the group generated by the Teichmüller character above, so $K = \mathbb{Q}(\mu_p)$. Then X contains $p-1$ elements of conductor p and the identity, which has conductor 1. Therefore the discriminant of $\mathbb{Q}(\mu_p)$ is p^{p-1} .

REFERENCE: [Was] Chapter 3.

2.2. Generalized Bernoulli Numbers. Let χ be a Dirichlet character of conductor f . The **generalized Bernoulli numbers** $B_{n,\chi}$ are defined by the expression

$$\sum_{m=1}^f \frac{\chi(m)te^{mt}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}$$

It turns out the generalized Bernoulli numbers are all polynomials in f , χ , and the plain old Bernoulli numbers. For most applications, we only need the first few generalized Bernoulli which are,

$$\begin{aligned} B_{0,\chi} &= \frac{1}{f} \sum_{m=1}^f \chi(m) = 0 \\ B_{1,\chi} &= \frac{1}{f} \sum_{m=1}^f \chi(m)m \\ B_{2,\chi} &= \frac{1}{f} \sum_{m=1}^f \chi(m)(m^2 - mf). \end{aligned}$$

Also, $B_{i,\chi} = 0$ if the parity of i and χ are different.

Example 8.

Let $p = 7$. Since

$$3^3 \equiv -1 \pmod{7}$$

by Hensel's lemma there is unique number $\alpha \in \mathbb{Z}_7$ such that $\alpha^3 = -1$ and $\alpha \equiv 3 \pmod{7\mathbb{Z}_7}$. It is easy to see that α generates $\mu_6 \subset \mathbb{Z}_7^\times$.

Thus we can write the standard character ω explicitly as

$$\begin{aligned} \omega(1) &= 1, & \omega(2) &= \alpha^2, & \omega(3) &= \alpha \\ \omega(4) &= -\alpha, & \omega(5) &= -\alpha^2, & \omega(6) &= -1. \end{aligned}$$

Then

$$B_{1,\omega} = \frac{1}{7}(1 + 2\alpha^2 + 3\alpha - 4\alpha - 5\alpha^2 - 6) = \frac{1}{7}(-5 - \alpha - 3\alpha^2)$$

and you can verify that $B_{1,\omega^2} = B_{1,\omega^4} = 0$ and $B_{1,\omega^3} = -1$.

Kummer's condition is a requirement on how divisible certain Bernoulli numbers are by p . You might suspect there is a relation between the divisibility of the Bernoulli numbers and the generalized Bernoulli numbers. Let's look at our example,

Example 9.

Let ω be the standard character as before. You can check that,

$$\alpha \equiv 31 \pmod{49\mathbb{Z}_7}.$$

that is, the 7-adic expansion of α is $7 + 4 \cdot 7 + O(49)$. Thus

$$-5 - \alpha - 3\alpha^2 \equiv -5 - 31 - 3 \cdot 31^2 \equiv 21 \pmod{49\mathbb{Z}_7}$$

and therefore

$$B_{1,\omega} \equiv 3 \pmod{7\mathbb{Z}_7}$$

Similarly, $B_{1,\omega^3} \equiv 6 \pmod{7\mathbb{Z}_7}$.

Notice that $\frac{1}{2}B_2 = \frac{1}{12} \equiv 3 \pmod{7}$, and $\frac{1}{4}B_4 = -\frac{1}{120} \equiv 6 \pmod{7}$.

In general we have the following,

Theorem 10. Let $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{Z}_p^\times$ be the Teichmüller character of conductor p . Let $k = 2, 4, \dots, p - 3$. Then

$$B_{1,\omega^{k-1}} \equiv \frac{1}{k} B_k \pmod{p\mathbb{Z}_p}.$$

and both sides are p -integral.¹ $B_{1,\omega^{p-2}}$ is not p -integral, but $pB_{1,\omega^{p-2}}$ is and

$$pB_{1,\omega^{p-2}} \equiv -1 \pmod{p\mathbb{Z}_p}$$

[Was] uses p -adic L-functions to prove a limited version of this theorem, while [La] uses Bernoulli distributions.

The last equivalence comes from the definition of ω : it is the character such that $\omega(m) \equiv m \pmod{p\mathbb{Z}_p}$. Therefore,

$$\sum_{m=1}^{p-1} m\omega^{-1}(m) \equiv \sum_{m=1}^{p-1} 1 \equiv -1 \pmod{p\mathbb{Z}_p}$$

¹in general,

$$\frac{1}{n} B_{n,\omega^{k-n}} \equiv \frac{1}{k} B_k \pmod{p\mathbb{Z}_p}.$$

Also both sides are 0 when k is odd.

REFERENCE: [Was] Chapters 4-5, [La] Chapters 1-2.

2.3. L-functions. The **Dedekind zeta function**, defined for any number field K , is

$$\zeta_K(s) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{1}{(\mathbb{N} \mathfrak{a})^s}$$

where \mathbb{N} denote the ideal norm induced by $\text{Nm}_{K/\mathbb{Q}}$, and the sum is taken over all ideals of K . This series converges uniformly for $\text{Re } s > 1$, and a functional equation extends ζ_K to a meromorphic function on the entire complex plane. At $s = 1$, there is a simple pole with residue

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{w\sqrt{|d|}}$$

Now suppose X is a finite group of Dirichlet characters corresponding to the Abelian extension K/\mathbb{Q} . Then the Dedekind zeta function decomposes into a product of **Dirichlet L-functions**,

$$\zeta_K(s) = \prod_{\chi \in X} L(s, \chi)$$

where

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for $\text{Re } s > 1$.

The upshot of all this is that knowledge of the Dirichlet characters gives us a tremendous amount of information about the field without having to know its elements. We have two important theorems from ANT.

Theorem 11. *Let X be a finite group of Dirichlet characters corresponding to a field K/\mathbb{Q} . Then the Dedekind zeta function of K has a pole at $s = 1$ with residue*

$$\frac{2^{r_1}(2\pi)^{r_2}hR}{|W|\sqrt{|d|}} = \prod_{\substack{\chi \in X \\ \chi \neq 1}} L(1, \chi).$$

Where r_1, r_2, R, W are the number of real embeddings, pairs of complex embeddings, regulator, and group of roots of unity of K

Let $\tau(\chi)$ denote the Gauss sum,

$$\tau(\chi) = \sum_{a=1}^f \chi(a)e^{2\pi ia/f}$$

Then we have the following.

Theorem 12. *1. The Dirichlet L functions satisfy a functional equation,*

$$\Lambda(s, \chi) = \frac{\tau(\chi)}{\sqrt{f}i^\delta} \Lambda(1-s, \bar{\chi})$$

where

$$\Lambda(s, \chi) = (f/\pi)^{s/2} \Gamma\left(\frac{s+\delta}{2}\right) L(s, \chi)$$

and $\delta = \frac{1}{2}$ parity of χ .

2. The Dirichlet L functions have special values at the negative integers,

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

3. If χ is an odd character (i.e., $\chi(-1) = -1$) then

$$L(1, \chi) = \frac{\pi i \tau(\chi)}{f_\chi} B_{1, \bar{\chi}}$$

Notice that 2. is in analogy with the special values of the Riemann zeta function at the negative integers given in the introduction.

Finally, we need one last lemma,

Lemma 13.

$$\prod_{\chi \in X} \tau(\chi) = \sqrt{|d|}$$

REFERENCE: [Mar] Chapter 7 for a self contained presentation of L -functions. Thm 12 is in [Was] Chapter 4.

2.4. CM fields have “almost” computable class number. Our endeavor is to understand the class groups of cyclotomic fields. What this formula is telling is that we can reduce the problem of computing the class number to the problem of understanding the units, which determine the regulator. The problem is that understanding the units of cyclotomic fields is as elusive as understanding the class number.

However, our saving grace is that the fields we are interested in are also CM fields, and the units of CM fields have a special property.

The goal of this section is to explain the relative class number formula,

Theorem 14. *Let K be a CM Abelian extension of \mathbb{Q} with associated characters $\{\chi\}$, K^+ its maximal real subfield. Let h, h^+ be their class numbers and $h = h^+ h^-$. Then*

$$h^- = Qw \prod_{\chi \text{ odd}} (-\frac{1}{2} B_{1, \chi})$$

First some examples.

Example 15.

Let $K = \mathbb{Q}(\sqrt{-23})$, an Abelian CM field. Since $-23 \equiv 1 \pmod{4}$, $K \subset \mathbb{Q}(\mu_{23})$ and has conductor 23. Notice that in this case, $h^- = h$, since the maximal real subfield is \mathbb{Q} . The associated group of Dirichlet characters is the order 2 group generated by the quadratic character χ , given in the example in the first section.

Since 1, 2, 3, 4, 6, 8, 9, 12, 13, 16, and 18 are the quadratic residues mod 23,

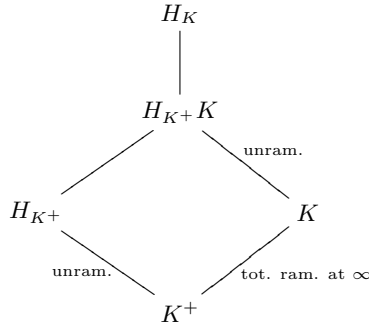
$$\begin{aligned} h &= h^- = 1 \cdot 2 \cdot -\frac{1}{2}B_{1,X} \\ &= -(1 + 2 + 3 + 4 - 5 + 6 - 7 + 8 + 9 - 10 - 11 + 12 \\ &\quad + 13 - 14 - 15 + 16 - 17 + 18 - 19 - 20 - 21 - 22) \\ &= 3 \end{aligned}$$

Theorem 16. Let K be a CM field and K^+ its maximal real subextension with rings of integers \mathcal{O}_K and \mathcal{O}_{K^+} . Denote by W the roots of unity of \mathcal{O}_K .

Then the following is true.

- (1) The class number of K^+ divides the class number of K .
- (2) $Q = [\mathcal{O}_K^\times : W\mathcal{O}_{K^+}^\times] = 1$ or 2. If $K = \mathbb{Q}(\mu_n)$ then $Q = 2$.
- (3) $R_K/R_{K^+} = 2^r/Q$ where $r = [K^+ : \mathbb{Q}] - 1$.
- (4) If K corresponds to the group of characters X , then K^+ corresponds to the subgroup of even characters $X^+ \subset X$.

Pf: The first statement follows from class field theory. Since K/K^+ is totally ramified at the infinite primes, the Hilbert class field of K^+ , H_{K^+} , is linearly disjoint from K (∞ is simultaneously ramified and unramified in $K \cap H_{K^+}$?). So we have a tower,



and recall that the index $[H_K : K]$ is equal to the class number of K . ■

Pf: Theorem 14 follows from combining the previous theorem and the results of the previous section ■

REFERENCE: [Was] Chapter 4.

2.5. Kummer's criterion. Now let $K = \mathbb{Q}(\mu_p)$, so the associated group of Dirichlet characters is the cyclic group of order $p-1$ generated by the Teichmüller character ω (see above). There are exactly $2p$ roots of unity in K , and $Q = 1$. Therefore,

$$h_p^- = 2p \prod_{\substack{1 \leq k < p \\ k \text{ odd}}} (-\frac{1}{2}B_{1,\omega^k}) = \frac{1}{2^{(p-3)/2}} B_{1,\omega} B_{1,\omega^3} \cdots B_{1,\omega^{p-4}} (-pB_{1,\omega^{p-2}})$$

Using the congruences of the previous section, we get,

$$h_p^- \equiv \frac{1}{2^{(p-3)/2}} B_2 B_4 \cdots B_{p-3} \pmod{p}$$

Therefore

Theorem 17. *p divides the relative class number if and only if p divides B_k for some $k = 2, 4, \dots, p-3$. As a result,*

$$p \text{ divides } B_k \text{ for some } k = 2, 4, \dots, p-3 \implies p \text{ is irregular}$$

To get the full Kummer condition requires a bit more work. The problem is with the real class number h_p^+ . Interestingly, we have the following conjecture.

Conjecture 18 (Vandiver).

$$p \nmid h_p^+.$$

This conjecture has only been verified for a relatively small (in the world of computational number theory) number of primes, is generally accepted to probably be true, but has no known methods that will work towards a proof.

REFERENCE: [Was] Chapter 5 for $p \mid h_p \iff p \mid h_p^-$

3. HERBRAND'S THEOREM AND ITS CONVERSE

3.1. Galois groups acting on the ideal class group. Let K/k be a Galois extension of number fields, $G = \text{Gal}(K/k)$. Let C be the ideal class group of K . You can check that G acts on the prime ideals $\mathfrak{p} \subset \mathcal{O}_K$, by

$$\mathfrak{p}^\sigma = \sigma\mathfrak{p} = \{\sigma x \mid x \in \mathfrak{p}\}.$$

Therefore G acts on the free abelian group on the prime ideals of K , and therefore on its quotient C .

Since we are interested in the p -part of the ideal class group, we also have the following

1. C/C^p , is a $\mathbb{F}_p[G]$ module. 2. If P is the p -Sylow subgroup of C , then P is a $\mathbb{Z}_p[G]$ module.

1: C/C^p is a group of type (p, \dots, p) so is also an \mathbb{F}_p vector space. 2: P is p -primary, and any p -primary group has a natural \mathbb{Z}_p action. (Let $x \in P$, $y \in \mathbb{Z}_p$. Choose r , $x^{p^r} = 1$, then choose $n \in \mathbb{Z}$ such that $n \equiv y \pmod{p^r \mathbb{Z}_p}$ and set $y \cdot x = x^n$. Check this is well defined.)

We need the following theorem.

For the moment, let G be any finite group, $|G| = n$. Recall the dual, \widehat{G} , is non-canonically isomorphic to G , and $|\widehat{G}| = |G|$.

Theorem 19. *Denote by μ_n the group of n th roots of unity. Let k be any field satisfying*

$$\text{char } k \nmid n, \quad \text{and,} \quad \mu_n \subset k^\times.$$

Then any $k[G]$ -module A decomposes as,

$$A = \bigoplus_{\chi \in \widehat{G}} A_\chi$$

where the action of G on A_χ is given by

$$\sigma x = \chi(\sigma)x \quad \text{for all } \sigma \in G \text{ and } x \in A_\chi$$

Pf: For each $\chi \in \widehat{G}$ define

$$e_\chi = \frac{1}{n} \sum_{\sigma \in G} \chi(\sigma)\sigma^{-1},$$

which is an element in $k[G]$ by hypothesis. You can compute directly that the collection of elements $\{e_\chi\}$ are a k -basis of orthogonal idempotents for $k[G]$.

Finally define

$$A_\chi = e_\chi A.$$

■

The Herbrand-Ribet theorem is the following.

Theorem 20. *Let $K = \mathbb{Q}(\mu_p)$ and ω the standard character that generates the Dirichlet characters corresponding to K . Let P be the p -primary part of its ideal class group, which decomposes $P = \bigoplus_i P_{\omega^i}$. Then for $k = 2, 4, \dots, p-3$,*

$$P_{\omega^{1-k}} \text{ is non-trivial} \iff p \mid B_k$$

The forward implication is due to Herbrand (1932) and the converse is due to Ribet ([Rib] 1976).

REFERENCE: Any text on rep theory? Or, [Was].

3.2. Stickelberger's Theorem. Now let's return to the case we are interested in. Here, our field is $\mathbb{Q}(\mu_p)$ whose Galois group $\{\sigma_m\}_{m \in (\mathbb{Z}/p\mathbb{Z})^\times}$ and character group $\{\omega^i\}_{i=1}^{p-1}$ we defined previously.

Since $|G| = p-1$, any of the fields $\mathbb{Q}(\mu_{p-1})$, or \mathbb{Z}_p , or \mathbb{F}_p will satisfy the hypotheses of the theorem.

Let θ be the element

$$\theta = \frac{1}{p} \sum_{m=1}^{p-1} m\sigma_m^{-1} \in \mathbb{Q}[G].$$

Theorem 21 (Stickelberger). *1. For all $i = 2, \dots, p-1$, the element $(i-\sigma_i)\theta \in \mathbb{Z}[G]$.
2. Let I be the ideal generated by all these elements. Then I annihilates the ideal class group of $\mathbb{Q}(\mu_p)$.*²

²**Remark:** This theorem is true for any Abelian extension K/\mathbb{Q} . Here we have to replace the element θ by

$$\theta = \sum_{a \in (\mathbb{Z}/f\mathbb{Z})^\times} (a/p)\underline{\sigma}_a^{-1} \in \mathbb{Q}[G]$$

where f is the conductor of K , (a/p) means a'/p if we choose the representative a' of a such that $1 \leq a' \leq f$, and $\underline{\sigma}_a$ means the restriction of $\sigma_a \in \text{Gal}(\mathbb{Q}(\mu_f)/\mathbb{Q})$ to K .

Pf:[Of the forward direction of the Herbrand-Ribet theorem] Recall the decomposition of the p -primary part of the ideal class group A ,

$$P = \bigoplus_{\chi \in X} P_\chi = \bigoplus_{i=1}^{p-1} P_{\omega^i}.$$

Let $x \in P_{\omega^i}$, $2 \leq c \leq p$ Then,

$$(c - \sigma_c)\theta x = (c - \omega^i(\sigma_c)) \left(\frac{1}{p} \sum_{m=1}^{p-1} m\omega^i(\sigma_m^{-1}) \right) x = (c - \omega^i(\sigma_c))B_{1,\omega^{-i}}x$$

That is, elements of the Stickelberger ideal act as multiplication by $(c - \omega^i(c))B_{1,\omega^{-i}} \in \mathbb{Z}_p$. Since ω has order $p - 1$, so, $B_{1,\omega^{-i}} = B_{1,\omega^{p-1-i}}$. By Kummer's congruences,

$$B_{1,\omega^{p-i}} \equiv \frac{1}{p-i} B_{p-i} \pmod{p\mathbb{Z}_p}$$

Also, it is easy to check that if $i \neq 1$,

$$c \not\equiv c^i \pmod{p}$$

so that $(c - \omega^i(c))$ is not divisible by p .

But P_{ω^i} is a p -group. Thus the only way that it can be annihilated by an element of \mathbb{Z}_p is if it is divisible by p . ■

Remark: Show that P_ω has to be 0 by computing the action of the Stickelberger ideal mod $p\mathbb{Z}_p$.

REFERENCE: [La] Chapters 1-2.

3.3. Some class field theory. Let K/k be Galois, and consider an Abelian extension E/K . Class field theory describes the possible extensions E in terms of the ideal class group of K . The statements are generally complicated, but in our case we can state a special case of the theorems of class field theory.

Theorem 22. *There is a covariant bijection between subgroups $B \leq A$ of the ideal class group of K and unramified³ Abelian extensions E/K . Under this correspondence,*

$$B \simeq \text{Gal}(E/K).$$

As an application, notice we have the following

Corollary 23. *Let h be the class number of K . Then $p \mid h$ if and only if there exists an unramified extension E/K such that $\text{Gal}(E/K)$ is a (nontrivial) Abelian p -group.*

Remark: The maximal such E is called the p -Hilbert class field.

The isomorphism in the theorem above is called the Artin map. It is actually very easy to define, assuming you've been given the field E/L . Take a prime ideal

³at all primes including the infinite ones

\mathfrak{p} of L . Since \mathfrak{p} is unramified in E , there is a unique element $Frob_{\mathfrak{p}} \in \text{Gal}(E/L)$ which generates the decomposition group of \mathfrak{p} and satisfies

$$Frob_{\mathfrak{p}}(x) \equiv x^{\mathbb{N}\mathfrak{p}} \pmod{\mathfrak{p}}$$

for all $x \in \mathcal{O}_E$. The Artin map is then the induced map $\mathfrak{p} \mapsto Frob_{\mathfrak{p}}$ on the ideal class group. It satisfies an important property, that for any $\sigma \in \text{Gal}(E/L)$,

$$Frob_{\sigma\mathfrak{p}} = \sigma Frob_{\mathfrak{p}} \sigma^{-1}$$

Note this doesn't apply to the theorem since our Galois group is Abelian, but this is an important property of Frobenius.

REFERENCE: See [Mil].

3.4. The first step of Ribet's proof. Now suppose we have a tower of fields

$$\begin{array}{c} E \\ \left| \right) \text{Gal}(E/K) \\ K \\ \left(\left| \right. \\ k \end{array}$$

such that E/K is Abelian and E/k is Galois. Recall that the ideal class group of K , C , is a G module. I claim that $\text{Gal}(E/K)$ is also a G -module. The action is defined as follows: if $\sigma \in G$, choose any $\tilde{\sigma} \in \text{Gal}(E/k)$ such that $\tilde{\sigma}|_K = \sigma$. The action on $\text{Gal}(E/K)$ is defined to be $\tau \in \text{Gal}(E/K)$,

$$\tau^\sigma = \tilde{\sigma}\tau\tilde{\sigma}^{-1}.$$

You can check this is well defined, using the fact that $\text{Gal}(E/K)$ is Abelian.

Theorem 24. *Take the tower as above, and suppose E/K is also unramified, and let $B \leq A$ be the corresponding class group. Then the Artin map*

$$B \rightarrow \text{Gal}(E/K)$$

is a G -module isomorphism.

Pf: It is already a group isomorphism, so we just need to check that it's a G -module homomorphism. Let $\sigma \in G$. Take any class in B represented by a prime ideal \mathfrak{p} of K , and choose $\tilde{\sigma} \in \text{Gal}(E/k)$ as above. Then $Frob_{\mathfrak{p}\sigma}$ is an element of $\text{Gal}(E/K)$, but think of it as an element of $\text{Gal}(E/k)$. Then

$$Frob_{\mathfrak{p}\sigma} = Frob_{\mathfrak{p}\tilde{\sigma}} = \tilde{\sigma}(Frob_{\mathfrak{p}})\tilde{\sigma}^{-1} = (Frob_{\mathfrak{p}})^\sigma.$$

■

Using this theorem, it is clear that in order to prove the converse direction of the Herbrand-Ribet theorem, it suffices to prove the following:

Theorem 25. *Suppose there exists a tower as above, with $K = \mathbb{Q}(\mu_p)$ and $k = \mathbb{Q}$, such that,*

1. $\text{Gal}(E/\mathbb{Q}(\mu))$ is an Abelian p -group.

2. E/K is unramified at all primes.

3. The action of G on $\text{Gal}(E/K)$ is given by

$$\tau^\sigma = \omega_i(\sigma) \cdot \tau, \quad \text{for all } \sigma \in G, \tau \in \text{Gal}(E/K).$$

Then P_{ω_i} is nontrivial.

Ribet then uses modular forms to construct the field E under the assumption that $p \mid B_k$ (Actually in Ribet's paper (1) is slightly different because he is using C/C^p instead of P).

4. REFERENCES

[La] Lang, S. Cyclotomic Fields I and II. Springer, 1990.

[Mar] Marcus, D. Number Fields. Springer, 1995.

[Mil] Milne, J.S. Class Field Theory and Algebraic Number Theory (CFT and ANT). Available from www.jmilne.org/math/.

[Rib] Ribet, K. A modular construction of unramified p -extensions of $\mathbb{Q}(\mu_p)$. *Invent. math.*, 34 (1976), 151-162.

[Was] Washington, L. Introduction to Cyclotomic Fields. Springer, 1982.