Gauss-Jacobi Sums and Stickelberger's Theorem

S. A. Katre

In this article we shall prove Stickelberger's theorem using factorisation of Gauss sums. This theorem tells us about certain elements of the integral group ring of the Galois group of an abelian number field which annihilate the ideal class group of the number field. We shall then apply Stickelberger's theorem to prove Herbrand's theorem. Herbrand's theorem is a stronger version of Kummer's theorem : " $p \mid h(\mathbb{Q}(\zeta_p)) \Rightarrow p \mid$ some Bernoulli number". Our main reference is [8].

§ 1. Gauss and Jacobi Sums

Let p be an odd prime and q be a power of p. Let $\mathbb{F}_q$ be the finite field of q elements. Let ζ_p be a fixed primitive p^{th} root of 1. The Galois group $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is cyclic generated by the Frobenius automorphism σ_p of $\mathbb{F}_q$ given by $x \mapsto x^p$.

For $q = p^f$, let $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$ be the trace map, $\mathrm{Tr}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{f-1}}$. Then for $g(x) = x + x^p + \cdots + x^{p^{f-1}} \in \mathbb{F}_p[x]$,

$$\prod_{i=0}^{p-1}(g(x) - i) = g(x)^p - g(x) = x^q - x.$$

For every $a \in \mathbb{F}_q$, $a^q - a = 0$, so for every $i \in \mathbb{F}_p$, $g(x) - i$ has p^{f-1} zeros in $\mathbb{F}_q$. This shows that Tr is onto. Hence $\psi : \mathbb{F}_q \to \mathbb{C}^\times, \psi(x) = \zeta_p^{\mathrm{Tr}(x)}$ is a well-defined nontrivial additive character of $\mathbb{F}_q$. Let $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ be a multiplicative character of $\mathbb{F}_q^\times$. Extend χ to all of $\mathbb{F}_q$ by setting $\chi(0) = 0$ (even if χ is the trivial character[1] $\mathbf{1}$). As $\chi^{q-1} = \mathbf{1}$, the order of χ is coprime to p.

Definition 1 *Let χ, χ_1, χ_2 be multiplicative characters on $\mathbb{F}_q$. The Gauss sum corresponding to χ is defined as*

$$g(\chi) = -\sum_{a \in \mathbb{F}_q} \chi(a)\psi(a).$$

[1]This convention is different from the one in the article of S. D. Adhikari [1] in these proceedings, where $\mathbf{1}(0)$=1. Also the definition of Gauss and Jacobi sums in [1] differs from ours in sign.

The Jacobi sum corresponding to χ_1 and χ_2 is defined as

$$J(\chi_1, \chi_2) = -\sum_{a \in \mathbb{F}_q} \chi_1(a)\chi_2(1-a).$$

Proposition 1 (a) $g(\mathbf{1}) = 1, J(\mathbf{1},\mathbf{1}) = 2 - q$.

(b) *If χ, χ_1, χ_2 have orders dividing m then $g(\chi) \in \mathbb{Q}(\zeta_{mp})$ and $J(\chi_1, \chi_2) \in \mathbb{Q}(\zeta_m)$. $g(\chi)$ and $J(\chi_1, \chi_2)$ are algebraic integers.*

(c) $J(\mathbf{1}, \chi) = J(\chi,\ \mathbf{1}) = 1$ *if* $\chi \neq \mathbf{1}$.

(d) $g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$.

(e) $J(\chi, \overline{\chi}) = \chi(-1)$ *if* $\chi \neq \mathbf{1}$.

(f) $\dfrac{g(\chi_1)g(\chi_2)}{g(\chi_1\chi_2)} = J(\chi_1, \chi_2)$ *if* $\chi_1\chi_2 \neq \mathbf{1}$.
$g(\chi)g(\overline{\chi}) = \chi(-1)q$ *if* $\chi \neq \mathbf{1}$.
Thus if χ_1, χ_2 are characters of order dividing m, then $g(\chi_1)g(\chi_2)/g(\chi_1\chi_2)$ is an algebraic integer in $\mathbb{Q}(\zeta_m)$.

(g) *If* $\chi \neq \mathbf{1}, g(\chi)\overline{g(\chi)} = q$.
If $\chi_1, \chi_2, \chi_1\chi_2 \neq \mathbf{1}, J(\chi_1, \chi_2)\overline{J(\chi_1, \chi_2)} = q$.

(h) *If χ^m is trivial and $(b, m) = 1$,*

$$g(\chi)^{b-\sigma_b} := \frac{g(\chi)^b}{g(\chi)^{\sigma_b}} \in \mathbb{Q}(\zeta_m)$$

where $\sigma_b \in Gal(\mathbb{Q}(\zeta_m, \zeta_p))/\mathbb{Q}$ is defined by $\zeta_p \mapsto \zeta_p$ and $\zeta_m \mapsto \zeta_m^b$. In particular taking $b = 1 + m$, $g(\chi)^m \in \mathbb{Q}(\zeta_m)$.

(i) $g(\chi^p) = g(\chi)$.

Proof.

(e) For $\chi \neq \mathbf{1}$, $J(\chi, \overline{\chi}) = -\sum \chi(c)\overline{\chi}(1-c) = -\sum_{c \neq 1} \chi\left(\dfrac{c}{1-c}\right) = \chi(-1)$.

(f)
$$\begin{aligned} g(\chi_1)g(\chi_2) &= \sum_{a,b} \chi_1(a)\chi_2(b)\psi(a+b) \\ &= \sum_{a,b} \chi_1(a)\chi_2(b-a)\psi(b) \\ &= \sum_{\substack{a,\,b \\ b \neq 0}} \chi_1(a)\chi_2(b-a)\psi(b) + \sum_a \chi_1(a)\chi_2(-a) \\ &= S_1 + S_2 \text{ say.} \end{aligned}$$

If $\chi_1\chi_2 \neq \mathbf{1}$, $S_2 = 0$. If $\chi_1\chi_2 = \mathbf{1}$, $S_2 = \chi_1(-1)(q-1)$.
In S_1, put $a = bc$. Then

$$S_1 = \sum_{\substack{b,\,c \\ b \neq 0}} \chi_1(b)\chi_2(b)\chi_1(c)\chi_2(1-c)\psi(b) = g(\chi_1\chi_2)J(\chi_1,\chi_2).$$

If $\chi_1\chi_2 = \mathbf{1}$, $S_1 = g(\mathbf{1})J(\chi_1,\overline{\chi_1}) = \chi_1(-1)$ and so $g(\chi)\overline{g(\chi)} = \chi(-1)q$.

(h) First, $g(\chi)^{\sigma_b} = g(\chi^b)$. Also, if for $(c,p) = 1, \tau_c \in \mathrm{Gal}(\mathbb{Q}(\zeta_m,\zeta_p)/\mathbb{Q})$ is defined by $\zeta_m \mapsto \zeta_m,\ \zeta_p \mapsto \zeta_p^c$, then $g(\chi)^{\tau_c} = \chi(c)^{-1}g(\chi)$ and similarly for $g(\chi^b)$. Hence τ_c fixes $g(\chi)^{b-\sigma_b}$.
(i) $g(\chi^p) = -\sum \chi^p(a)\zeta_p^{\mathrm{Tr}(a)} = -\sum \chi(a^p)\zeta_p^{\mathrm{Tr}(a^p)} = g(\chi)$. □

§ 2. Stickelberger's Theorem.

Let ζ_m denote a primitive m^{th} root of unity. Let $M/\mathbb{Q}$ be a finite abelian extension, so by Kronecker-Weber theorem, $M \subset \mathbb{Q}(\zeta_m)$ for some m. Assume m minimal. $G = \mathrm{Gal}(M/\mathbb{Q})$ may be regarded as a quotient of $(\mathbb{Z}/m\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$.

For $(a,m) = 1, \sigma_a$ denotes the element $\zeta_m \mapsto \zeta_m^a$ of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ as well as its restriction to M. For $x \in \mathbb{R}$, let $\{x\}$ = the fractional part of x, so $x - \{x\} \in \mathbb{Z}$ and $0 \leq \{x\} < 1$. Define the Stickelberger element θ in the group-ring $\mathbb{Q}[G]$ by

$$\theta = \theta(M) = \sum_{\substack{a \pmod m \\ (a,m)=1}} \left\{\frac{a}{m}\right\}\sigma_a^{-1} = \sum_{\substack{1 \leq a \leq m \\ (a,m)=1}} \frac{a}{m}\sigma_a^{-1}.$$

Let $I(M) = \mathbb{Z}[G] \cap \theta\mathbb{Z}[G]$ consist of $\mathbb{Z}[G]$-multiples of θ which have integer coefficients. Then $I(M)$ is an ideal of the group-ring $\mathbb{Z}[G]$ and is called the Stickelberger ideal. Clearly, $m\theta \in I(M)$.

Lemma 1 *Let I' be the ideal of $\mathbb{Z}[G]$ generated by all the elements of the form $c - \sigma_c$ with $(c,m) = 1$. Equivalently I' is (finitely) generated by m and $c - \sigma_c$ with $(c,m) = 1,\ 1 \leq c < m$. Let $\beta \in \mathbb{Z}[G]$. If $\beta \in I'$ then $\beta\theta \in \mathbb{Z}[G]$, so that $I'\theta \subset I$. If, moreover, $M = \mathbb{Q}(\zeta_m)$, then $I = I'\theta$.*

Proof. We have

$$(c - \sigma_c)\theta = \sum_a \left(c\left\{\frac{a}{m}\right\} - \left\{\frac{ac}{m}\right\}\right)\sigma_a^{-1}.$$

$$\text{This is in } \mathbb{Z}[G], \text{ as } c\left\{\frac{a}{m}\right\} - \left\{\frac{ac}{m}\right\} \equiv c\cdot\frac{a}{m} - \frac{ac}{m} \pmod 1$$
$$\equiv 0 \pmod 1.$$

Hence $I'\theta \subset I$.

Note also that $m = (1+m) - \sigma_{1+m} \in I'$, so that I' is generated by m and $c - \sigma_c$ with $(c, m) = 1,\ 1 \le c < m$.

Next consider the case $M = \mathbb{Q}(\zeta_m)$. Suppose

$$(\sum_a x_a\sigma_a)\theta \in \mathbb{Z}[G],$$

where $x_a \in \mathbb{Z}$. The coefficient of identity in $\left(\sum_a x_a\sigma_a\right)\left(\sum_c \left\{\frac{c}{m}\right\}\sigma_c^{-1}\right)$ is $\sum_a x_a\left\{\frac{a}{m}\right\}$ and this $\in \mathbb{Z}$. Hence $\sum x_a\cdot\frac{a}{m}$ is in $\mathbb{Z}$, i.e. $m \mid \sum x_a\cdot a$, so that $\sum x_a\cdot a \in I'$. Hence $\sum x_a\sigma_a = \sum x_a(\sigma_a - a) + \sum x_a a \in I'$.
Thus $I \subset I'\theta$. □

Example. The above result $I = I'\theta$ is not necessarily true for a proper subfield of $\mathbb{Q}(\zeta_m)$. Let $M = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\zeta_{12}+\zeta_{12}^{11})$ (the maximal real subfield) $\subset Q(\zeta_{12})$. Then on M, $\sigma_1 = \sigma_{11} = 1$ and $\sigma_5 = \sigma_7 = \sigma$, say. Then $\theta(M) = 1+\sigma$ itself is in $\mathbb{Z}[G]$, i.e. $1\cdot\theta \in \mathbb{Z}[G]$, so $\theta \in I$. But I' is generated by $5-\sigma$, $7-\sigma$ and $11-1$ i.e. by 2 and $1+\sigma$, hence $I'\theta$ is generated by 2θ and $\theta^2 = 2+2\sigma = 2\theta$ i.e. by 2θ. Hence $\theta = 1+\sigma \notin I'\theta$, i.e. $I'\theta \subsetneq I$.

This example also tells us that although θ corresponding to a cyclotomic field does not belong to the corresponding Stickelberger ideal, θ corresponding to a proper subfield M of $\mathbb{Q}(\zeta_m)$ may belong to $I(M)$.

Action of $\mathbb{Z}[G]$ on ideals and ideal classes : If $x = \sum x_\sigma\sigma \in \mathbb{Z}[G]$, then x acts on ideals of M by

$$A^x := \Pi(A^\sigma)^{x_\sigma}$$

This also gives rise to an action on ideal classes.

Stickelberger's Theorem. *The Stickelberger ideal of an abelian number field M annihilates the ideal class group of M. In other words, if A is an ideal of M and $x \in I(M)$, the Stickelberger ideal of M, then A^x is a principal ideal of M.*

§ 3. Prime Factorisation of Gauss Sums.

Let p be an odd prime and let $q = p^f$ be a power of p. Thus $p^f \equiv 1 \pmod{q-1}$ with f least. Let $\mathcal{P}$ be one of the $\phi(q-1)/f$ prime ideals of $\mathbb{Q}(\zeta_{q-1})$ lying above p. Now $\mathbb{Z}[\zeta_{q-1}] \pmod{\mathcal{P}}$ is a finite field of p^f elements. Also the $(q-1)^{\text{st}}$ roots of unity are distinct $\pmod{\mathcal{P}}$. There is a group isomorphism

$$\omega = \omega_{\mathcal{P}} : \mathbb{F}_q^\times \to (q-1)^{\text{st}} \text{ roots of } 1$$

satisfying for $a \in \mathbb{F}_q^\times$, $\mathbb{F}_q = Z[\zeta_{q-1}]/\mathcal{P}$,

$$\omega(a) \pmod{\mathcal{P}} = a.$$

i.e. $\omega(a)$ is that $(q-1)^{\text{st}}$ root of unity which lies in the coset $\pmod{\mathcal{P}}$ corresponding to a. Then ω is a character on $\mathbb{F}_q^\times$ called the Teichmüller character (corresponding to $\mathcal{P}$) and it depends upon the model of $\mathbb{F}_q$ given by $\mathbb{Z}[\zeta_{q-1}]/\mathcal{P}$. The character $\omega : (\mathbb{Z}[\zeta_{q-1}]/\mathcal{P})^\times \to \mathbb{Q}(\zeta_{q-1})$ can thus be described by saying that for $\beta \in \mathbb{Z}[\zeta_{q-1}], \omega(\beta + \mathcal{P})$ is that unique root of unity ζ_{q-1}^k for which $\zeta_{q-1}^k \equiv \beta \pmod{\mathcal{P}}$.

As $\mathbb{F}_q^\times$ is cyclic, the characters on $\mathbb{F}_q^\times$ form a cyclic group. Now, $\omega(\zeta_{q-1} + \mathcal{P}) = \zeta_{q-1}$, so ω has order $q-1$, i.e. ω generates the character group on $\mathbb{F}_q^\times$. Any character on $\mathbb{F}_q^\times$ may be written as $\omega^{-\alpha}$ for an integer $\alpha \pmod{q-1}$. We now obtain a factorisation of the Gauss sum $g(\omega^{-\alpha})$ in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$.

Since $g(\chi)g(\overline{\chi}) = q$ for any character $\chi \neq \mathbf{1}$ on $\mathbb{F}_q^\times$, any prime divisor of $g(\omega^{-\alpha})$ for $\alpha \not\equiv 0 \pmod{q-1}$ comes from a prime divisor of p in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$. p has $\phi(q-1)/f$ distinct prime divisors in $\mathbb{Q}(\zeta_{q-1})$ ($\phi(.)$ being the Euler ϕ function) and p totally ramifies in $\mathbb{Q}(\zeta_p)$, $(p) = (1-\zeta_p)^{p-1}$. As $(p, q-1) = 1$, the cyclotomic fields $\mathbb{Q}(\zeta_{q-1})$ and $\mathbb{Q}(\zeta_p)$ are linearly disjoint, and so a prime of $\mathbb{Q}(\zeta_{q-1})$ lying above p totally ramifies in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$.

Let $\tilde{\mathcal{P}}$ be the (unique) prime of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ lying above $\mathcal{P}$. For $\alpha \in \mathbb{Z}$, we want to know the exponent, say $s(\alpha)$, of the power of this prime ideal $\tilde{\mathcal{P}}$ occurring in $g(\omega^{-\alpha})$. We have that

$$s(\alpha) = v_{\tilde{\mathcal{P}}}(g(\omega^{-\alpha})) \text{ depends only on } \alpha \pmod{q-1}.$$

We shall show that $s(\alpha) =$ the sum of the digits of α when α is expressed in base p. In terms of the function s we can also obtain the exponents corresponding to other prime ideals in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ occurring in $g(\omega^{-\alpha})$ and this will give us the prime ideal decomposition of $g(\omega^{-\alpha})$ in $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$.

Lemma 2 *Let* $\alpha,\ \beta \in \mathbb{Z}$.
(a) $s(0) = 0$.

(b) $0 \leq s(\alpha+\beta) \leq s(\alpha)+s(\beta)$.
(c) $s(\alpha+\beta) \equiv s(\alpha)+s(\beta) \pmod{p-1}$.
(d) $s(p\alpha) = s(\alpha)$.
(e) $\sum_{\alpha=1}^{q-2} s(\alpha) = (q-2)(f)(p-1)/2$.

Proof. (a) : $g(\omega^{-0}) = g(\mathbf{1}) = 1$.
(b) and (c) : By Prop. 1(f), $g(\omega^{-\alpha})g(\omega^{-\beta})/g(\omega^{-\alpha-\beta})$ is an algebraic integer in $\mathbb{Q}(\zeta_{q-1})$. Also $\mathcal{P} = \tilde{\mathcal{P}}^{p-1}$, so the values of $v_{\tilde{\mathcal{P}}}$ on $\mathbb{Q}(\zeta_{q-1})$ are divisible by $p-1$.
(d) : $g(\chi^p) = g(\chi)$.
(e) : As $g(\omega^{-\alpha})g(\omega^{\alpha}) = \pm q = \pm p^f$, we get

$$s(\alpha) + s(q-1-\alpha) = v_{\tilde{\mathcal{P}}}(p^f) = (p-1)f.$$

Adding for $\alpha = 1, 2, \cdots, q-2$ gives the result. □

Lemma 3 *$s(\alpha) > 0$ if $\alpha \not\equiv 0 \pmod{q-1}$. $s(1) = 1$.*

Proof. As $\pi = \zeta_p - 1 \in \tilde{\mathcal{P}}$, $\zeta_p \equiv 1 \pmod{\tilde{\mathcal{P}}}$, so

$$g(\omega^{-\alpha}) = -\sum \omega^{-\alpha}(a)\zeta_p^{\mathrm{Tr}(a)} \equiv -\sum \omega^{-\alpha}(a) \pmod{\tilde{\mathcal{P}}}.$$

But $\sum_{a\in\mathbb{F}_q} \omega^{-\alpha}(a) = 0$, as $\alpha \not\equiv 0 \pmod{q-1}$. Thus $g(\omega^{-\alpha}) \equiv 0 \pmod{\tilde{\mathcal{P}}}$. Hence $s(\alpha) > 0$. Next,

$$\begin{aligned} g(\omega^{-1}) &= -\sum \omega^{-1}(a)\zeta_p^{\mathrm{Tr}(a)} \\ &= -\sum \omega^{-1}(a)(1+\pi)^{\mathrm{Tr}(a)} \equiv -\sum \omega^{-1}(a)(1+\pi\mathrm{Tr}(a)) \pmod{\tilde{\mathcal{P}}^2} \\ &\equiv -\pi\sum \omega^{-1}(a)\mathrm{Tr}(a) \pmod{\tilde{\mathcal{P}}^2}. \end{aligned}$$

Regarding $\mathbb{F}_q$ as $\mathbb{Z}[\zeta_{q-1}] \pmod{\mathcal{P}}$ and noting that $a \mapsto a^p$ generates the Galois group of $\mathbb{Z}[\zeta_{q-1}] \pmod{\mathcal{P}}$ over $\mathbb{Z}/p\mathbb{Z}$, we have $\mathrm{Tr}(a) = a + a^p + \cdots + a^{p^{f-1}} \pmod{\mathcal{P}}$. Hence

$$\sum_{a\in\mathbb{F}_q} \omega^{-1}(a)\mathrm{Tr}(a) \equiv \sum_{\substack{a\not\equiv 0 \\ a \pmod{\mathcal{P}}}} a^{-1}(a + a^p + \cdots + a^{p^{f-1}}) \pmod{\mathcal{P}}.$$

For $0 < b < f$, $\sum_{a\not\equiv 0} a^{p^b-1} \equiv 0 \pmod{\mathcal{P}}$,
so this sum reduces to $\sum_{a\not\equiv 0} 1 = q-1 \equiv -1 \pmod{\mathcal{P}}$.

$$\text{This gives } g(\omega^{-1}) \equiv \pi \pmod{\tilde{\mathcal{P}}^2}.$$

But $\mathbb{Q}(\zeta_{q-1}, \zeta_p)/\mathbb{Q}(\zeta_p)$ is unramified at π. So $s(1) = v_{\tilde{\mathcal{P}}}(\pi) = 1$. □

Proposition 2 *Let $0 \le \alpha < q-1$ and let the base-p expansion of α be $\alpha = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$, $0 \le a_i \le p-1$. Then*

$$s(\alpha) = a_0 + a_1 + \cdots + a_{f-1}.$$

Proof. We have, $s(0) = 0$. As $s(1) = 1$ and $0 \le s(\alpha+\beta) \le s(\alpha) + s(\beta)$, and $s(\alpha+\beta) \equiv s(\alpha) + s(\beta) \pmod{p-1}$ we get $s(\alpha) = \alpha$ for $0 \le \alpha \le p-2$. This gives the result if $q = p$. If $q > p$, consider $s(p-1) \le p-1$ and as $s(p-1) > 0$ and $s(p-1) \equiv p-1 \pmod{p-1}$, we get $s(p-1) = p-1$.

$$\begin{aligned} \text{Also } s(\alpha) &\le s(a_0) + s(a_1 p) + \cdots + s(a_{f-1}p^{f-1}) \\ &= s(a_0) + s(a_1) + \cdots + s(a_{f-1}) \\ &= a_0 + a_1 + \cdots + a_{f-1}. \end{aligned}$$

Now as α runs over the integers from 0 to $q-1$, inclusive, each coefficient in the base-p expansion takes each of the values $0, 1, \cdots, p-1$ exactly p^{f-1} times, so

$$\sum_{\alpha=0}^{q-1}(a_0 + \cdots + a_{f-1}) = \frac{p(p-1)}{2} f p^{f-1} = \frac{p-1}{2} f q.$$

As $q-1 = (p-1) + (p-1)p + \cdots + (p-1)p^{f-1}$, omitting $\alpha = q-1$ we get

$$\sum_{\alpha=0}^{q-2}(a_0 + \cdots + a_{f-1}) = \frac{(p-1)}{2} f q - (p-1) f = (q-2) f \frac{p-1}{2} = \sum_{\alpha=0}^{q-2} s(\alpha).$$

Hence the result follows. □

In summary, given a prime divisor $\mathcal{P}$ of p in $\mathbb{Q}(\zeta_{q-1})$ and given the corresponding Teichmüller character $\omega = \omega_{\mathcal{P}}$,

$$\begin{aligned} v_{\tilde{\mathcal{P}}}(g(\omega^{-\alpha})) &= s(\alpha) = a_0 + a_1 + \cdots + a_{f-1} \\ &= \text{the sum of digits of } \alpha \text{ in its base-}p \text{ expansion.} \end{aligned}$$

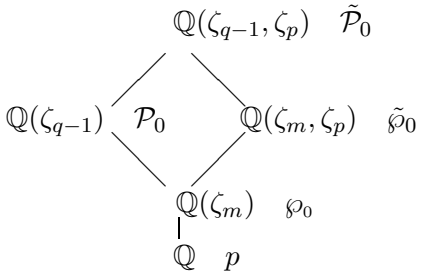
We now get the prime ideal decomposition of a Gauss sum $g(\chi)$.

Let m be a fixed positive integer, p a prime, $(p, m) = 1$. Let f be the order of $p \pmod{m}$, so m divides $p^f - 1 = q - 1$. Let $\wp_0$ be any fixed prime of $\mathbb{Q}(\zeta_m)$ lying above p. Let $\tilde{\wp}_0$ be the unique prime of $\mathbb{Q}(\zeta_m, \zeta_p)$ lying above $\wp_0$, so $\tilde{\wp}_0{}^{p-1} = \wp_0$. Let $\mathcal{P}_0$ be a prime of $\mathbb{Q}(\zeta_{q-1})$ lying above $\wp_0$, and let $\tilde{\mathcal{P}}_0$ be the prime of $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ lying above $\mathcal{P}_0$ (and $\tilde{\wp}_0$).

Let $\omega = \omega_{\mathcal{P}_0}$ be the Teichmüller character on $\mathbb{F}_q$ corresponding to $\mathcal{P}_0$. Let $\chi = \omega^{-d}$, where $d = (q-1)/m$. Then χ is a character on $\mathbb{F}_q$ of order m associated with the Teichmüller character ω obtained from $\mathcal{P}_0$. It may be observed that χ depends only on $\wp_0$ and it is in fact the reciprocal of

the character $\omega^d = \omega^{(q-1)/m}$ which can be identified with the m^{th} power residue character associated with $\wp_0$ under the natural isomorphism $\mathbb{F}_q \cong \mathbb{Z}[\zeta_{q-1}]/\mathcal{P} \cong \mathbb{Z}[\zeta_m]/\wp_0$. (See [1].)

Now $\chi^m = 1$, so $g(\chi) \in \mathbb{Q}(\zeta_m, \zeta_p)$. Since $g(\chi)\overline{g(\chi)} = q = p^f$, the factorisation of $g(\chi)$ involves only primes of $\mathbb{Q}(\zeta_m, \zeta_p)$ above p, i.e. the conjugates over $\mathbb{Q}$ of $\tilde{\wp}_0$. For $(a, m) = 1$, let $\sigma_a : \zeta_m \mapsto \zeta_m^a$ be the element of $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$. For each such a, fix an extension of σ_a to $\mathbb{Q}(\zeta_{q-1}, \zeta_p)$ such that $\zeta_p^{\sigma_a} = \zeta_p$.



As $(p, m) = 1$, p is unramified and the decomposition group for p in $(\mathbb{Z}/m\mathbb{Z})^\times$ is the cyclic group generated by $p \pmod m$, thus it is represented by $\{1, p, \cdots, p^{f-1}\}$.

Let R denote a set of representatives for $(\mathbb{Z}/m\mathbb{Z})^\times$ modulo this decomposition group. Then $\{\wp_0^{\sigma_a^{-1}} \mid a \in R\}$ is the set of conjugates of $\wp_0$. Now $\tilde{\wp}_0$ is the unique prime of $\mathbb{Q}(\zeta_m, \zeta_p)$ lying above $\wp_0$. Hence, the conjugates of $\tilde{\wp}_0$ are ${\tilde{\wp}_0}^{\sigma_a^{-1}}, a \in R$. Let $\tilde{\wp} = {\tilde{\wp}_0}^{\sigma_a^{-1}}$ be any of these. Then for $\chi = \omega^{-d}, d = \frac{q-1}{m}$,

$$v_{\tilde{\wp}}(g(\chi)) = v_{\tilde{\wp}_0}(g(\chi)^{\sigma_a}) = v_{\tilde{\wp}_0}(g(\chi^a)) = v_{\tilde{\mathcal{P}}_0}(g(\chi^a)) = v_{\tilde{\mathcal{P}}_0}(g(\omega^{ad})) = s(ad),$$

noting that $v_{\tilde{\wp}_0} = v_{\tilde{\mathcal{P}}_0}$ as $\tilde{\mathcal{P}}_0/\tilde{\wp}_0$ is unramified. We have thus proved

Proposition 3 *For $\chi = \omega^{-d}, d = \frac{q-1}{m}$, $(g(\chi)) = \tilde{\wp}_0^{\sum_R s(ad)\sigma_a^{-1}}$.*

Arguing as above we also have,

Proposition 3′.(Prime factorisation of Gauss sums) *For $k \not\equiv 0 \pmod m$,*

$$(g(\chi^k)) = \tilde{\wp}_0^{\sum_R s(kad)\sigma_a^{-1}}.$$

§ 4. Proof of Stickelberger's Theorem

We first obtain a factorisation of $(g(\chi)^m)$ in terms of the Stickelberger element θ. Recall that $g(\chi)^m \in \mathbb{Q}(\zeta_m)$ as $\chi^m = 1$.

In the following lemma we have an alternative expression for the sum $s(h)$ of the base-p digits of an integer h.

Lemma 4 *Let $0 \le h < q-1$. Then*

$$s(h) = (p-1)\sum_{i=0}^{f-1}\left\{\frac{p^i h}{q-1}\right\}.$$

Proof. Let $h = a_0 + a_1 p + \cdots + a_{f-1}p^{f-1}$, be the base-$p$ expansion of h. Then

$$p^i h \equiv a_0 p^i + a_1 p^{i+1} + \cdots + a_{f-1}p^{i-1} \pmod{(q-1)}.$$

As $h < q-1$, some digit $a_i < p-1$, so RHS $< q-1$. Hence

$$\left\{\frac{p^i h}{q-1}\right\} = \frac{1}{q-1}(a_0 p^i + \cdots + a_{f-1}p^{i-1}).$$

Summing over i, we get

$$\sum_{i=0}^{f-1}\left\{\frac{p^i h}{q-1}\right\} = \frac{1}{q-1}\left(\sum_{i=0}^{f-1} a_i\right)(1+p+\cdots+p^{f-1}) = \frac{1}{p-1}\left(\sum_{i=0}^{f-1} a_i\right).$$

This gives the result. □

Proposition 4 *If $\chi = \chi_{\wp_0}$ is the reciprocal of the m^{th} power residue character corresponding to a prime $\wp_0$ of $\mathbb{Q}(\zeta_m)$, lying above p, then*

(i) $$(g(\chi)^m) = \wp_0^{m\theta} = \wp_0^{\sum_{1\le a\le m,(a,m)=1} a\sigma_a^{-1}},$$

as ideals in $\mathbb{Q}(\zeta_m)$.

(ii) (Prime factorisation of Jacobi sums) *Let j, k be integers such that $jk(j+k) \not\equiv 0 \pmod m$. Let*

$$\theta_{j,k} = \sum_{\substack{a \pmod m \\ (a,m)=1}} \left(\left[\frac{(j+k)a}{m}\right] - \left[\frac{ja}{m}\right] - \left[\frac{ka}{m}\right]\right)\sigma_a^{-1}$$

Then $\left(J(\chi^j, \chi^k)\right) = \wp_0^{\theta_{j,k}}$ as ideals in $\mathbb{Q}(\zeta_m)$.

Proof. We have, by Lemma 4,

$$s(ad) = s(a\frac{q-1}{m}) = (p-1)\sum_{i=0}^{f-1}\left\{\frac{p^i a}{m}\right\}.$$

Hence by Proposition 3,

$$(g(\chi)^m) = \tilde{\wp}_0^{m\sum_R s(ad)\sigma_a^{-1}} = \tilde{\wp}_0^{m(p-1)\sum_{i=0}^{f-1}\sum_R\left\{\frac{p^i a}{m}\right\}\sigma_a^{-1}}.$$

As $\tilde{\wp_0}^{p-1} = \wp_0$ and $\sigma_{p^i}(\wp_0) = \wp_0$ (since $p^i \in$ the decomposition group of $\wp_0$), we get $(g(\chi)^m) = \wp_0^{m\sum_{b \pmod m,(b,m)=1}\left\{\frac{b}{m}\right\}\sigma_b^{-1}} = \wp_0^{m\theta}$ as ideals in $\mathbb{Q}(\zeta_m, \zeta_p)$.

Due to unique factorisation of ideals in $\mathbb{Q}(\zeta_m)$, $(g(\chi)^m) = \wp_0^{m\theta}$ holds also in $\mathbb{Q}(\zeta_m)$.

Next write $\theta_j = \sum_{\substack{a \pmod m \\ (a,m)=1}} \left\{\frac{ja}{m}\right\}\sigma_a^{-1}$. Then as before, $(g(\chi^j)^m) = \wp_0^{m\theta_j}$.

Let j, k be such that $j, k, j+k \not\equiv 0 \pmod m$. Then

$$m\theta_j + m\theta_k - m\theta_{j+k} = m\sum_{(a,m)=1}\left(\left[\frac{(j+k)a}{m}\right] - \left[\frac{ja}{m}\right] - \left[\frac{(ka}{m}\right]\right)\sigma_a^{-1}$$

so that, using Prop. 1(f),

$$\left(J(\chi^j, \chi^k)^m\right) = \wp_0^{m\theta_{j,k}}, \text{ where } \theta_{j,k} \in \mathbb{Z}[G].$$

Hence $(J(\chi^j, \chi^k)) = \wp_0^{\theta_{j,k}}$, by unique factorisation in $\mathbb{Q}(\zeta_m)$. □

Remark : The above proposition shows that if $\wp_0$ is a prime of $\mathbb{Q}(\zeta_m)$ such that $\wp_0 \nmid m$, taking p to be the prime of $\mathbb{Z}$ lying below $\wp_0$, $\wp_0^{m\theta}$ and $\wp_0^{\theta_{j,k}}$ are principal in $\mathbb{Q}(\zeta_m)$.

We next prove such a result for an abelian number field. We first have

Proposition 5 *Let M be a subfield of $\mathbb{Q}(\zeta_m)$. Let A be an ideal of M such that $(A, m) = 1$. Let $\theta = \theta(M)$. Then $A^{m\theta}$ is principal in $\mathbb{Z}[\zeta_m]$. Further, for $\beta \in \mathbb{Z}[G]$, $A^{\beta\theta}$ is principal in $\mathbb{Z}[\zeta_m]$.*

Proof. Let A be an ideal of $M \subset \mathbb{Q}(\zeta_m)$ such that $(A, m) = 1$. Write $A = \prod \wp_i$, $\wp_i$ being prime ideals of $\mathbb{Q}(\zeta_m)$ not necessarily distinct. Let p_i be primes of $\mathbb{Z}$ lying below $\wp_i$. Let $P =$ the square-free part of $\prod p_i$.

Then, by Proposition 4, $A^{m\theta} = \prod \wp_i^{m\theta}$ is principal in $\mathbb{Q}(\zeta_{mP})$.

Extending elements of $\mathrm{Gal}(M/\mathbb{Q})$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_{mP}/\mathbb{Q})$ by fixing ζ_P, we assume that $m\theta \in \mathbb{Z}[\mathrm{Gal}(\mathbb{Q}(\zeta_{mP})/\mathbb{Q})]$.

Let $\chi_{\wp_i}$ be the character of order m on the finite field $\mathbb{Z}[\zeta_m]/\wp_i$ defined using $\wp_i$. Then $g(\chi_{\wp_i}) \in \mathbb{Z}[\zeta_{mp_i}]$ and as ideals of $\mathbb{Z}[\zeta_{mP}]$,

$A^{m\theta} = \prod \wp_i^{m\theta} = \prod (g(\chi_{\wp_i})^m) = (\gamma^m)$ where $\gamma = \prod g(\chi_{\wp_i}) \in \mathbb{Z}[\zeta_{mP}]$.

As each $g(\chi_{\wp_i})^m \in \mathbb{Z}[\zeta_m]$, $A^{m\theta}$ is principal in $\mathbb{Z}[\zeta_m]$ itself.

Next suppose $\beta \in \mathbb{Z}[G], G = \mathrm{Gal}(M/\mathbb{Q})$ such that $\beta\theta \in \mathbb{Z}[G]$, θ being the Stickelberger element for M. Then, as above, extending the elements of $\mathrm{Gal}(M/\mathbb{Q})$ to $\mathrm{Gal}(\mathbb{Q}(\zeta_{mP})/\mathbb{Q})$ assume that $\beta\theta \in \mathrm{Gal}(\mathbb{Q}(\zeta_{mP})/\mathbb{Q})$.

Then

$$A^{m\beta\theta} = (A^{m\theta})^\beta = (\gamma^m)^\beta = (\gamma^\beta)^m$$

as ideals of $\mathbb{Z}(\zeta_{mP})$.

We next prove that γ^β in fact $\in \mathbb{Q}(\zeta_m)$, so that $A^{\beta\theta}$ is principal in $\mathbb{Z}[\zeta_m]$.

Firstly, $\gamma^{m\beta} = (\gamma^m)^\beta \in \mathbb{Q}(\zeta_m)$ and $(\gamma^{m\beta}) = (\gamma^\beta)^m = (A^{\beta\theta})^m$ is the m^{th} power of an ideal of $\mathbb{Z}[\zeta_m]$.

If $\wp$ is a prime ideal of $L = \mathbb{Q}(\zeta_m)$ such that $(\wp, m) = 1$, locally, $(\gamma^{m\beta}) = (\pi_\wp^{mt}), t \geq 0, \pi_\wp$ being a local uniformizer. So $\gamma^{m\beta} = \epsilon\pi_\wp^{mt}, \epsilon$ being a local unit. So $\gamma^\beta = \epsilon^{1/m}\pi_\wp^t$. This gives $L_\wp(\gamma^\beta) = L_\wp(\epsilon^{1/m})$ as a Kummer extension of $L_\wp$ where $\pi_\wp \not| \epsilon$. Hence the extension is unramified. Thus $\mathbb{Q}(\zeta_m, \gamma^\beta)/\mathbb{Q}(\zeta_m)$ is unramified at $\wp$.

Also $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\zeta_m, \gamma^\beta) \subset \mathbb{Q}(\zeta_m, \zeta_P)$, so ramification can occur only at primes dividing P. But $(P, m) = 1$, so the extension is unramified.

In view of the following lemma , we see that $\gamma^\beta \in \mathbb{Q}(\zeta_m)$:

Lemma 5 *Let $m, n \geq 1$ and $m|n$. If $K/\mathbb{Q}(\zeta_m)$ is unramified at all primes and $K \subset \mathbb{Q}(\zeta_n)$, then $K = \mathbb{Q}(\zeta_m)$.*

Proof. Let p be a prime dividing n/m. Then $\mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)$ is totally ramified at the primes above p. Hence $K \cap \mathbb{Q}(\zeta_{mp})/\mathbb{Q}(\zeta_m)$ is totally ramified and unramified at a prime above p. Thus, $K \cap \mathbb{Q}(\zeta_{mp}) = \mathbb{Q}(\zeta_m)$. So $[K(\zeta_{mp}) : \mathbb{Q}(\zeta_{mp})] = [K : \mathbb{Q}(\zeta_m)]$. Now a lift of an unramified extension is unramified at all primes. Hence we can argue similarly with m replaced by mp. Continuing like this, finally,

$$[K : \mathbb{Q}(\zeta_m)] = [K(\zeta_n) : \mathbb{Q}(\zeta_n)] = [\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)] = 1.$$

Hence $K = \mathbb{Q}(\zeta_m)$. □

Next to prove that $\gamma^\beta \in M$. Let $\wp_i$ be a prime divisor of A in $\mathbb{Q}(\zeta_m)$. Let p be the rational prime lying below $\wp_i$. Let $q = p^f$ where f is the residue class degree of $\wp_i$. Let $\mathcal{P}$ be a prime of $\mathbb{Q}(\zeta_{q-1})$ lying over $\wp_i$. Now $\chi_{\wp_i}$ can be defined in terms of $\mathcal{P}$ and hence write $\chi_{\wp_i} = \chi_\mathcal{P}$.

Let $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{q-1})/M)$. Then σ gives rise to a map

$$\sigma : \mathbb{Z}[\zeta_{q-1}] \pmod{\mathcal{P}} \to \mathbb{Z}[\zeta_{q-1}] \pmod{\mathcal{P}^\sigma},$$

and we have, if $\chi_\mathcal{P}(a) = \zeta$, then $\chi_{\mathcal{P}^\sigma}(a) = \zeta^\sigma$. Thus $\chi_{\mathcal{P}^\sigma} = \chi_\mathcal{P}^\sigma$. But $\chi_\mathcal{P}^m = 1$, so $\chi_{\mathcal{P}^\sigma} = \chi_\mathcal{P}$ for $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_{q-1})/\mathbb{Q}(\zeta_m))$. Thus $\chi_\mathcal{P}$ depends only on $\wp_i$, so we can in fact use the notation $\chi_{\wp_i}$.

As above, for $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m)/M)$, $\chi_{\wp_i}^\sigma = \chi_{\wp_i^\sigma}$. Extending σ to $\mathbb{Q}(\zeta_{mp})$ by letting $\zeta_p \mapsto \zeta_p$, $g(\chi_{\wp_i})^\sigma = g(\chi_{\wp_i}^\sigma) = g(\chi_{\wp_i^\sigma})$. Now for $\sigma \in \text{Gal}(\mathbb{Q}(\zeta_m)/M)$, $A^\sigma = A$, so σ permutes all the prime divisors $\wp_i$ of A in $\mathbb{Q}(\zeta_m)$.

Hence

$$\gamma^{\beta\sigma} = \prod g(\chi_{\wp_i})^{\beta\sigma} = \prod g(\chi_{\wp_i^\sigma})^\beta = \gamma^\beta.$$

But already $\gamma^\beta \in \mathbb{Q}(\zeta_m)$. Hence $\gamma^\beta \in M$. So $A^{\beta\theta} = (\gamma^\beta)$ is principal in M.

Finally, let A be any ideal of M. Write $A = BC$ where $(C, m) = 1$ and a prime $\wp$ divides B if and only if $\wp$ divides (A, m). By approximation

theorem, first get an integer $b \in M$ such that for every prime divisor $\wp$ of m in M, $v_\wp(b) = v_\wp(A)$, so that $(b) = BD$ with $(D, m) = 1$. Now there is an ideal E of M such that $(E, m) = 1$ and DE is principal $= (c)$, say, where c is an integer in M. (Use the factorisation in M of primes below D.) Then, $(b)CE = BDCE = ADE = A(c)$. Take $A_1 = CE$ and $a = b/c$. Thus we have $A = (a)A_1$, with $a \in M$, and $(A_1, m) = 1$. Then $A^{\beta\theta} = (a^{\beta\theta})A_1^{\beta\theta}$, which is principal. This completes the proof of Stickelberger's theorem .

(For a simpler proof of Stickelberger's theorem in the case of the full cyclotomic field $\mathbb{Q}(\zeta_m)$, see the article of C. S. Yogananda [9].)

§ 5. Herbrand's Theorem

Herbrand's theorem is an interesting application of Stickelberger's theorem for the cyclotomic field $\mathbb{Q}(\zeta_p)$. Herbrand's theorem and its converse characterise the Bernoulli numbers $B_2, B_4, \cdots, B_{p-3}$ divisible by p in terms of the structure of the $p-$Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$.

Bernoulli Numbers. The Bernoulli numbers $B_n,\ n \geq 0,$ were first defined by Jakob (James) Bernoulli (1654-1705) and were so designated by L. Euler. They are defined by the exponential generating function (the series being convergent for $|t| < 2\pi$)

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

$$\text{We have, } \frac{t}{e^t - 1} + \frac{t}{2} = \frac{t(e^t + 1)}{2(e^t - 1)} = \frac{t}{2} \cdot \frac{e^{t/2} + e^{-t/2}}{e^{t/2} - e^{-t/2}},$$

which is an even function of t. Hence $B_{2k-1} = 0$ for $k \geq 2$. First few values of B_n are : $B_0 = 1,\ B_1 = -\frac{1}{2},\ B_2 = \frac{1}{6},\ B_4 = -\frac{1}{30},\ B_6 = \frac{1}{42},\ B_8 = -\frac{1}{30},$ $B_{10} = \frac{5}{66},\ B_{12} = -\frac{691}{2730},\ B_{14} = \frac{7}{6}$. These can be successively obtained from the recurrence relation for Bernoulli numbers viz.

$$(m+1)B_m = -\sum_{k=0}^{m-1} \binom{m+1}{k} B_k.$$

Bernoulli proved that the sum $S_r(n)$ of r^{th} powers of first n natural numbers is given in terms of the B_m as

$$(r+1)S_r(n) = n^{r+1} - \binom{r+1}{1} B_1 n^r + \binom{r+1}{2} B_2 n^{r-1} + \cdots + \binom{r+1}{r} B_r n.$$

Euler obtained the values of the Riemann zeta function $\zeta(s)$ at positive even integral values of s in terms of Bernoulli numbers as

$$\zeta(2n) = (-1)^{n+1}\frac{2^{2n-1}B_{2n}}{(2n)!}\pi^{2n}.$$

Thus the even-indexed Bernoulli numbers are nonzero and they alternate in sign. As $\zeta(2n) > 1$ and $e^n > \frac{n^n}{n!}$ we get $|\frac{B_{2n}}{2n}| > \frac{1}{e\pi}\left(\frac{n}{e\pi}\right)^{2n-1}$, so that $|\frac{B_n}{n}| \to \infty$ as $n \to \infty, (\ n$ even).
It was proved by Von Staudt Clausen that the denominator of a Bernoulli number B_n, with n positive and even, is square-free. More precisely, he proved that for n even $> 0, B_n + \sum_{(p-1)|n}\frac{1}{p}$ is an integer, (thus 2, 3 always appear in the denominator of each such B_n). (See [2], [4], [6].)
Exercise. If $n = 2q$ where q is a prime of the form $3k+1$, then $B_n \equiv \frac{1}{6} \pmod 1$.
One also has the following congruence for Bernoulli numbers :

Kummer Congruence. Suppose m, n are positive even integers such that $m \equiv n \not\equiv 0 \pmod{(p-1)}$. Then

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod p.$$

More generally, if m, n are positive even integers and

$$m \equiv n \pmod{(p-1)p^\alpha} \text{ and } n \not\equiv 0 \pmod{(p-1)},$$

then

$$(1-p^{m-1})\frac{B_m}{m} \equiv (1-p^{n-1})\frac{B_n}{n} \pmod{p^{\alpha+1}}.$$

as $n \to \infty, (\ n$ even.)

A prime p is called irregular if $p|B_j$ for some $j = 2, 4, \cdots, p-3$. Otherwise p is called a regular prime.

As $|\frac{B_n}{n}| \to \infty$ with n (n even). Suppose $p_1, \cdots, p_r$ are irregular primes and N is large so that $m = N(p;_1 -1)\cdots(p_r - 1)$ satisfies $|\frac{B_m}{m}| > 1$. Let p be a prime in the numerator of $\frac{B_m}{m}$. Now $(p_i - 1)|m$, so all the p_i appear in the denominator of b_m; so $p \neq p_i$ for all i. Also $(p-1) \nmid m$, for otherwise p would be in the denominator of B_m. Let $m' \equiv m \pmod{p-1}$, $0 < m' < p-1$. Then by the Kummer congruence, $p|B_{m'}$. Therefore p is irregular. This shows that the number of irregular primes is infinite. At present it is not

known whether there are infinitely many regular primes or not. However, numerical evidence (W. Johnson) and probabilistic arguments (C. L. Siegel) indicate that about 61% of all primes are regular.

Kummer proved that if $p \nmid$ the class number h of $\mathbb{Q}(\zeta_p)$, then the equation $x^p + y^p = z^p$ has no positive integral solution. (See [6], [7].)

Using his results on the class number formulas for cyclotomic fields, Kummer also proved that the condition $p \nmid h(\mathbb{Q}(\zeta_p))$ is actually equivalent to the regularity of p, i.e. $p \nmid B_2, B_4, \cdots, B_{p-3}$. (See [6].)

Generalised Bernoulli Numbers. A Dirichlet character $\pmod n$ is a multiplicative homomorphism $\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$. If $n|m$, it induces a homomorphism $(\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C}^\times$ by composition with the natural map from $(\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times$. We choose n minimal which induces such a Dirichlet character $\pmod m$ and call n to be the conductor of the character denoted by f or f_χ.

The character $\chi \pmod 8$ defined by $\chi(1) = \chi(5) = 1$ and $\chi(3) = \chi(7) = -1$ has conductor 4 as it can be induced from the character $\pmod 4$ defined by $\chi(1) = 1, \chi(3) = -1$, and 4 is minimal. The character $\pmod 6$ defined by $\chi(1) = 1, \chi(5) = -1$ has conductor 3 as it can be induced from the character $\pmod 3$ defined by $\chi(1) = 1, \chi(3) = -1$, and 3 is minimal.

Given a Dirichlet character χ of modulus and conductor f, the generalised Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!}.$$

For $\chi = \mathbf{1}$, the character of conductor 1, we have $\sum_{n=0}^{\infty} B_{n,\mathbf{1}} \ \frac{t^n}{n!} = \frac{te^t}{e^t - 1} = \frac{t}{e^t - 1} + t$. Thus $B_{n,\mathbf{1}} = B_n$ except when $n = 1$, when we have $B_{1,\mathbf{1}} = \frac{1}{2}, B_1 = -\frac{1}{2}$. Also note that if $\chi \neq \mathbf{1}$, $\sum_{a=1}^{f} \chi(a) = 0$, and hence,

$$\begin{aligned} \text{i)} \quad B_{0,\chi} &= 0, \\ \text{ii)} \quad B_{1,\chi} &= \frac{1}{f} \sum_{a=1}^{f} \chi(a) a. \end{aligned}$$

Let G be a finite abelian group and $\widehat{G}$ its character group. Let R be a commutative ring with unity which contains the values of all $\chi \in \widehat{G}$ and in which $|G|$ is invertible (e.g. $R = \overline{\mathbb{Q}}$). For $\chi \in \widehat{G}$, define

$$\varepsilon_\chi = \frac{1}{|G|}\sum_{\sigma\in G}\chi(\sigma)\sigma^{-1} \in R[G].$$

Then we have

(a) $\varepsilon_\chi^2 = \varepsilon_\chi$,

(b) $\varepsilon_\chi\varepsilon_\psi = 0$ if $\chi \neq \psi$,

(c) $\mathbf{1}= \sum_{\chi\in\widehat{G}} \varepsilon_\chi$,

(d) $\varepsilon_\chi\sigma = \chi(\sigma)\varepsilon_\chi$.

ε_χ are called as the orthogonal idempotents of the group ring $R[G]$. Let M be a module over $R[G]$. Let $M_\chi = \varepsilon_\chi M$. Then

$$\varepsilon_\chi M_\chi = \varepsilon_\chi^2 M = \varepsilon_\chi M = M_\chi.$$

Using $\mathbf{1}= \sum_{\chi\in\widehat{G}}\varepsilon_\chi$, we see that $M = \sum_\chi M_\chi$. Next suppose $0 = \sum m_\chi$ with $m_\chi \in M_\chi$. Then as $m_\chi = \varepsilon_\chi m'_\chi$ with $m'_\chi \in M$, multiplying by ε_ψ we get $0 = \varepsilon_\psi m'_\psi = m_\psi$. Hence $M = \oplus M_\chi$. Also for $\sigma \in G$, and $m_\chi \in M_\chi$, writing $m_\chi = \varepsilon_\chi\ m'_\chi$ with $m'_\chi \in M$,

$$\sigma m_\chi = \sigma\varepsilon_\chi m'_\chi = \chi(\sigma)\varepsilon_\chi m'_\chi = \chi(\sigma)m_\chi.$$

Thus for the action of $\sigma \in G$ on the $R[G]$-module M, the elements of M_χ are eigenvectors with eigenvalue $\chi(\sigma)$.

Now let $R = \mathbb{Z}_p$, the ring of p-adic integers. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \approx (\mathbb{Z}/p\mathbb{Z})^\times$. As $\mathbb{Z}_p \supset \mathbb{Z}_{(p)}$ (the localization of $\mathbb{Z}$ at p), $|G| = p-1$ is invertible in $\mathbb{Z}_p$. Also $\mathbb{Z}_p$ contains all the $(p-1)^{\text{st}}$ roots of unity and these are congruent (mod p) to the elements $1, 2, \cdots, p-1$. $\widehat{G}$ denotes the group of characters of G with values in $\mathbb{Z}[\zeta_p]$.

Write elements of G as $\sigma_a : \zeta_p \mapsto \zeta_p^a, \quad (a,p) = 1$. Define $\omega \in \widehat{G}$ as follows. Write for convenience $\omega(\sigma_a)$ as $\omega(a)$. For $a \in (\mathbb{Z}/p\mathbb{Z})^\times, a$ is a $(p-1)^{\text{st}}$ root of unity. Define $\omega(a)$ to be the $(p-1)^{\text{st}}$ root of unity in $\mathbb{Z}_p$, which comes from a; i.e. $\omega(a)$ is such that $\omega(a) \equiv a \pmod p$. Then $\omega \in \widehat{G}$ and $\widehat{G} = \{\omega^i | 0 \leq i \leq p-2\}$. Then the orthogonal idempotents of $\mathbb{Z}_p[G]$ are

$$\varepsilon_i = \varepsilon_{\omega^i} = \frac{1}{p-1}\sum_{a=1}^{p-1}\omega^i(a)\sigma_a^{-1}, 0 \leq i \leq p-2.$$

Define

$$\begin{aligned}\varepsilon_- &= \sum_{i \text{ odd}} \varepsilon_i = \frac{1}{p-1}\sum_{a=1}^{p-1}\left(\sum_{i \text{ odd}} \omega^i(a)\right)\sigma_a^{-1} = \frac{1-\sigma_{-1}}{2},\\ \text{and}\\ \varepsilon_+ &= \sum_{i \text{ even}} \varepsilon_i = \frac{1+\sigma_{-1}}{2}.\end{aligned}$$

Then for any $\mathbb{Z}_p[G]$-module A, $A = A^- \oplus A^+$, where $A^- = \varepsilon_- A$ and $A^+ = \varepsilon_+ A$.

Let $\theta = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1}$ be the Stickelberger element for $\mathbb{Q}(\zeta_p)$. Using (d) above, we get,

$$\begin{aligned}\varepsilon_i\theta &= \frac{1}{p}\sum_{a=1}^{p-1} a\omega^i(a)\varepsilon_i = B_{1,\omega^{-i}}\varepsilon_i\\ \text{and } \varepsilon_i(c-\sigma_c)\theta &= (c-\omega^i(c))B_{1,\omega^{-i}}\varepsilon_i\end{aligned}$$

Any abelian p-group A is a $\mathbb{Z}_p$-module by the action $(\sum_{j=0}^{\infty} b_j p^j)a = \sum_{j=0}^{\infty} b_j(p^j a)$, since the latter sum is finite.

From now on, let A be the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$. Then the Galois group G also acts on A, so A is a $\mathbb{Z}_p[G]$-module. Write $A = \bigoplus_{i=0}^{p-2} A_i$, where $A_i = \varepsilon_i A$. By Stickelberger's theorem, for $(c,p) = 1, (c-\sigma_c)\theta$, which is in the Stickelberger ideal of $\mathbb{Q}(\zeta_p)$, annihilates in particular A, and hence each $A_i = \varepsilon_i A$. Thus, $(c-\omega^i(c))B_{1,\omega^{-i}}$ annihilates A_i.

Note. $p\theta = \sum_{(a,p)=1} a\sigma_a^{-1}$ and $(p-1)\varepsilon_1 = \sum_{(a,p)=1}\omega(a)\sigma_a^{-1}$. As $w(a) \equiv a \pmod p), p\theta \equiv (p-1)\epsilon_1 \pmod p)$. As A_i are p-groups, it may be possible to accept that $p\theta$ annihilates A_i for $i \neq 1$. We require Stickelberger's theorem to conclude that $p\theta$ annihilates A_1.

Consider $0 \leq i \leq p-2$.

Case 1. If $i \neq 0$ is even,

$$B_{1,\omega^{-i}} = \frac{1}{p}\sum_{(a,p)=1}\omega^{-i}(a)a = \frac{1}{p}\cdot\frac{1}{2}\sum_{(a,p)=1} w^{-i}(a)\{a+(p-a)\} = 0,$$

so we do not get any information in this case.

Case 2. If $i = 0, B_{1,\mathbf{1}} = \frac{1}{2}$, so $\frac{c-1}{2}$ annihilates A_0.

Taking some $1 < c \leq p-1$, $\frac{c-1}{2}$ is invertible in $\mathbb{Z}_p$, so $A_0 = 0$. This is otherwise obvious, because $A_0 = \epsilon_0 A$ and $\epsilon_0 = \text{Norm}/(p-1)$.
Case 3. Let i be odd. Suppose $i = 1$. Let $c = 1 + p$. Then

$$(c - \omega(c))B_{1,\omega^{-1}} = pB_{1,\omega^{-1}} = \sum_{a=1}^{p-1} a\omega^{-1}(a) \equiv p - 1 \not\equiv 0 \pmod{p},$$

so $(c-\omega(c))B_{1,\omega^{-1}}$ is unit of $\mathbb{Z}_p$, so that $A_1 = 0$. Next suppose $i \neq 1$. Choose an integer c (e.g. a primitive root mod p) such that $c \not\equiv c^i \equiv \omega^i(c) \pmod{p}$. Then $c - \omega^i(c)$ is a unit of $\mathbb{Z}_p$, so $B_{1,\omega^{-i}}$ is in $\mathbb{Z}_p$ and it annihilates A_i. This gives

Proposition 6 *$A_0 = A_1 = 0$. For $i = 3, 5, \cdots, p-2, B_{1,\omega^{-i}} \in \mathbb{Z}_p$ and it annihilates A_i.*

Herbrand's Theorem. *Let i be odd, $3 \leq i \leq p-2$. If $A_i \neq 0$, then $p \mid$ the Bernoulli number B_{p-i}.*

Proof. Suppose $A_i \neq 0$. Then $B_{1,\omega^{-i}}$ must be a non-unit in $\mathbb{Z}_p$, i.e. $B_{1,\omega^{-i}} \equiv 0 \pmod{p}$. Now it can be proved that (see Cor. 5.15, [6]) if n is odd and $n \not\equiv -1 \pmod{p-1}$, then $B_{1,\omega^n} \equiv \dfrac{B_{n+1}}{n+1} \pmod{p}$, and both the sides are p-integral. Hence, $B_{1,w^{-i}} \equiv \dfrac{B_{p-i}}{p-i} \pmod{p}$, Hence $p|B_{p-i}$. This proves Herbrand's theorem. □

The converse of Herbrand's theorem is

Ribet's Theorem. Let i be odd, $3 \leq i \leq p-2$. If $p|B_{p-i}$, then $A_i \neq 0$.

For an elementary proof of Ribet's Theorem see Chapter 15 of [6]. See also [5]. For irregular primes, Herbrand-Ribet give a piece-by-piece information about which Bernoulli numbers are divisible by p in terms of the $\mathbb{Z}_p[G]$-module structure of the p-Sylow subgroup of the ideal class group of $\mathbb{Q}(\zeta_p)$.

The number $i(p)$ of $B_j, j = 2, 4, \cdots, p-3$, which are divisible by p is called the index of irregularity of p. As a consequence of Ribet's theorem we get that the p-rank of the ideal class group of $\mathbb{Q}(\zeta_p)$ (i.e.the number of summands when A is written as a direct sum of cyclic groups of prime power order) is at least $i(p)$, i.e. the number of Bernoulli numbers divisible by p.

Vandiver's Conjecture. This conjecture says that $p \nmid h^+(\mathbb{Q}(\zeta_p))$, the class number of the maximal real subfield $\mathbb{Q}(\zeta_p)^+$ of $\mathbb{Q}(\zeta_p)$. The conjecture has already been checked by computer for all primes up to 4,000,000 and even if it is false it is expected to hold for most primes.

It is known that if Vandiver's conjecture holds, then the p-rank of the ideal class group of $\mathbb{Q}(\zeta_p)$ equals the number of Bernoulli numbers divisible by p. (See also the article of E. Ghate [3].)

Acknowledgements. I thank S. V. Kanetkar and Vijay Patankar for carefully going through the article and Dinesh Thakur for suggesting this topic for my lectures.

REFERENCES

1. S. D. Adhikari, The Early Reciprocity Laws: From Gauss to Eisenstein, These proceedings.
2. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Fourth Ed., Cambridge Uni. Press, 1975.
3. Eknath Ghate, Vandiver's Conjecture via K-theory, These proceedings.
4. K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, GTM 84, Springer-Verlag, New York Inc., 1982.
5. C. Khare, Notes on Ribet's Converse to Herbrand, These proceedings.
6. Paulo Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer-Verlag New York Inc., 1979.
7. Dinesh S. Thakur, Fermat's Last Theorem for Regular Primes, These proceedings.
8. L. C. Washington, Introduction to Cyclotomic Fields, Second Ed., GTM 83, Springer-Verlag New York Inc.,1997.
9. C. S. Yogananda, Stickelberger Revisited, These proceedings.

S. A. Katre
Department of Mathematics,
University of Pune,
Pune-411 007.
e-mail: sakatre@@math.unipune.ernet.in