Stickelberger Revisited

C S Yogananda

In the present article, we give the proof of the Stickelberger's Theorem in the spirit of Kummer (rediscovered by Thaine) given by Washington [4].

Theorem. *Let* $G = Gal(\mathbf{Q}(\zeta_m)/\mathbf{Q})$ *and for* $(a,m) = 1, \sigma_a : \zeta_m \mapsto \zeta_m^a$. *Let*

$$\theta = \frac{1}{m} \sum_{\substack{a=1 \\ (a,m)=1}} a\sigma_a^{-1}.$$

If $\beta \in \mathbf{Z}[G]$ *is such that* $\beta\theta \in \mathbf{Z}[G]$ *then* $\beta\theta$ *annihilates the ideal class group of* $\mathbf{Q}(\zeta_m)$.

Proof: The proof is by looking at the factorisation of certain Gauss sums. Let $\mathcal{C}$ be an ideal class in $\mathbf{Q}(\zeta_m)$. There exist infinitely many unramified primes of degree 1 in $\mathcal{C}$ (follows from Dirichlet's theorem on primes in arithmetic progression and Chebotarev density theorem). Let λ be such an ideal which is above the rational prime l; since l splits completely in $\mathbf{Q}(\zeta_m)$ we have that $l \equiv 1 \pmod{m}$. Fix a primitive root s modulo l and define a Dirichlet character mod l, $\chi : (\mathbf{Z}/l\mathbf{Z})^* \to \mathbf{C}^*$ by $\chi(s) = \zeta_m$. Consider the Gauss sum

$$g(\chi) = -\sum_{b=1}^{l-1} \chi(b)\zeta_l^b.$$

It is easy to see which are the primes dividing $g(\chi)$ in $\mathbf{Q}(\zeta_m, \zeta_l)$. First of all, since $g(\chi)g(\bar{\chi}) = l$, only primes above l occur in the factorisation of $g(\chi)$. Since l splits completely in $\mathbf{Q}(\zeta_m)$, the Galois conjugates of λ, $\sigma_a^{-1}(\lambda)$, $1 \le a \le m, (a,m) = 1$, are all the factors of l; if $\mathfrak{L}$ is the prime above λ in $\mathbf{Q}(\zeta_m, \zeta_l)$, (remember $\mathbf{Q}(\zeta_m, \zeta_l)/\mathbf{Q}(\zeta_m)$ is fully ramified above l) the prime factorisation of the principal ideal $(g(\chi))$ would look like

$$(g(\chi)) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} \sigma_a^{-1}(\mathfrak{L})^{r_a}$$

where $0 \le r_a \le l-1$ (σ_a being extended to $\mathbf{Q}(\zeta_m, \zeta_l)$.

As $g(\chi)^{l-1}$ is in $\mathbf{Q}(\zeta_m)$ and $\mathfrak{L}^{l-1} = \lambda$ we have the following factorisation in $\mathbf{Q}(\zeta_m)$:

$$(g(\chi)^{l-1}) = \prod_{\substack{a=1 \\ (a,m)=1}}^{m} \sigma_a^{-1}(\lambda)^{r_a}.$$

In other words, $\sum r_a\sigma_a^{-1}$ *annihilates the class* $\mathcal{C}$ in the ideal class group of $\mathbf{Q}(\zeta_m)$.

We now use the Galois action on $g(\chi)$ to determine the integers r_a. Consider

$$\tau \in \mathrm{Gal}(\mathbf{Q}(\zeta_m,\zeta_l)/\mathbf{Q}(\zeta_m)), \quad \tau(\zeta_l)=\zeta_l^s.$$

We have $g(\chi)^\tau = \chi(s)^{-1}g(\chi)$ and

$$(\zeta_l^s-1)/(\zeta_l-1) \equiv 1+\zeta_l+\cdots+\zeta_l^{s-1} \equiv s \pmod{\sigma_a^{-1}(\mathfrak{L})}.$$

As $\mathbf{Q}(\zeta_m,\zeta_l)/\mathbf{Q}(\zeta_m)$ is totally ramified above $\sigma_a^{-1}(\lambda)$, $1\le a\le m, (a,m)=1$, the inertia group of $\sigma_a^{-1}(\mathfrak{L})$ coincides with the full Galois group and hence τ acts trivially mod $\sigma_a^{-1}(\mathfrak{L})$. Therefore we have

$$\frac{g(\chi)}{(\zeta_l-1)^{r_a}} \equiv \frac{g(\chi)^\tau}{(\zeta_l^s-1)^{r_a}} \equiv \frac{g(\chi)}{(\zeta_l-1)^{r_a}}\frac{\chi(s)^{-1}}{s^{r_a}} \pmod{\sigma_a^{-1}(\mathfrak{L})}.$$

Since $\sigma_a^{-1}(\mathfrak{L})$ occurs to first power in (ζ_l-1) we have $g(\chi)/(\zeta_l-1)^{r_a}$ relatively prime to $\sigma_a^{-1}(\mathfrak{L})$ and hence we get

$$\zeta_m = \chi(s) \equiv s^{-r_a} \pmod{\sigma_a^{-1}(\mathfrak{L})}.$$

Since $\zeta_m \in \mathbf{Q}(\zeta_m)$ this congruence holds modulo $\sigma_a^{-1}\lambda$ and applying σ_a we obtain

$$\zeta_m^a \equiv s^{-r_a} \pmod{\lambda}.$$

Now, since the mth roots of unity are distinct mod λ, the order of ζ_m mod λ is exactly m and so,

$$\zeta_m \equiv s^{-(l-1)c/m} \pmod{\lambda}$$

where c is an integer prime to m.

Therefore

$$r_a \equiv \frac{(l-1)ac}{m} \pmod{l-1}$$

which implies that $l-1$ does not divide r_a as a and c are prime to m. Furthermore, we have $0\le r_a\le l-1$ and so

$$r_a = (l-1)\left\{\frac{ac}{m}\right\}$$

where $\{\cdot\}$ denotes the fractional part. We have

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

Thus we get that the ideal $\lambda^{(l-1)\sigma_c\theta}$ is a principal ideal generated by $g(\chi)^{l-1}$.

Let $\beta \in \mathbf{Z}[G]$ be such that $\beta\theta \in \mathbf{Z}[G]$ and $\gamma = g(\chi)^{\sigma_c^{-1}\beta}$. Then $\gamma^{l-1} \in \mathbf{Q}(\zeta_m)$ and $\lambda^{\beta\theta(l-1)} = (\gamma^{l-1})$ which implies that (γ^{l-1}) is the $(l-1)$st power of an ideal in $\mathbf{Q}(\zeta_m)$. Hence the extension $\mathbf{Q}(\zeta_m, \gamma)/\mathbf{Q}(\zeta_m)$ can be ramified only at the primes dividing $l-1$. But since $\mathbf{Q}(\zeta_m) \subseteq \mathbf{Q}(\zeta_m, \gamma) \subseteq \mathbf{Q}(\zeta_m, \zeta_l)$ it follows that $\mathbf{Q}(\zeta_m, \gamma)/\mathbf{Q}(\zeta_m)$ is totally ramified at primes above l. Therefore $\mathbf{Q}(\zeta_m, \gamma) = \mathbf{Q}(\zeta_m)$ which implies that $\gamma \in \mathbf{Q}(\zeta_m)$. We can therefore take $(l-1)$st root and obtain the following equality of ideals in $\mathbf{Q}(\zeta_m)$

$$\lambda^{\beta\theta} = (\gamma).$$

This completes the proof of the theorem. □

Actually, as we have seen in Katre's article [1], the Stickelberger's theorem holds for subfields of $\mathbf{Q}(\zeta_m)$ as well. (It would be interesting to see if the above methods can be used to give a proof of this general case.)

Thaine's Theorem

We shall state a simpler case of Thaine's theorem and give an outline of the proof to illustrate the main ideas. This account is based on Thaine's paper [3] and Washington's book [4], Chapter 15, §2.

Theorem. *Let $F = \mathbf{Q}(\zeta_p)^+$ and $\Delta = Gal(F/\mathbf{Q})$. Let E be the group of units of F, $C = C_F$, the group of cyclotomic units, A, the class group of F; put $B = E/C$. If $\theta \in \mathbf{Z}[G]$ annihilates the p-part of B then θ annihilates the p-part of A.*

An outline of the proof: Choose n large enough such that $p^n > |A|$ and $p^n > |B|$. Then the p-Sylow subgroups of A and B are, respectively, isomorphic to A/A^{p^n} and $E/E^{p^n}C$. Let $q \equiv 1 \pmod{p^n}$ be a prime; note that q splits completely in $\mathbf{Q}(\zeta_p)$. Suppose $\delta = \prod_b (\zeta_p^b - 1)^{y_b}$ is a cyclotomic unit in $\mathbf{Q}(\zeta_p)$. Let Q denote a prime above q in $\mathbf{Q}(\zeta_p)$ and $\tilde{Q}$ the unique prime in $\mathbf{Q}(\zeta_{pq})$ above Q. Put $\eta = \prod_b (\zeta_p^b \zeta_q - 1)^{y_b}$. It turns out that η is a unit in $\mathbf{Q}(\zeta_{pq})$ with some special properties: (i) η has norm 1 to $\mathbf{Q}(\zeta_p)$ (since $q \equiv 1 \pmod{p}$) and (ii) $\eta \equiv \delta$ mod primes above q. Property (1) in conjunction with Hilbert's Theorem 90 implies the existence of an $\alpha \in \mathbf{Q}(\zeta_{pq})$ such that $\eta = \alpha^\tau/\alpha$ where τ is a generator of $\mathrm{Gal}(\mathbf{Q}(\zeta_{pq})/\mathbf{Q}(\zeta_p))$. Since η is a unit the principal ideal (α) satisfies: $(\alpha)^\tau = (\alpha)$ which implies (since τ is a generator of the Galois group) that (α) is the product of an ideal I from $\mathbf{Q}(\zeta_p)$ and ramified primes:

$$(\alpha) = I \cdot \prod_\sigma \sigma(\tilde{Q})^{r_\sigma}$$

where the product is over $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. Taking norm to F we get

$$(\text{Norm } \alpha) = (I\bar{I})^{q-1} \cdot \prod_{\sigma} \sigma(Q\bar{Q})^{r_\sigma} = (I\bar{I})^{q-1} \cdot (Q\bar{Q})^{\sum \sigma r_\sigma}.$$

Thus we have that $\sum \sigma r_\sigma$ annihilates the idealclass above q in the quotient A/A^{p^n}. If s is a primitive root mod q working exactly as in section 2 we get that $s^{r_\sigma} \equiv \epsilon \equiv \delta \pmod{\sigma^{-1}\tilde{Q}}$. Since s^{r_σ} and δ are in F this congruence gives us: $s^{r_\sigma} \equiv \sigma(\delta) \pmod{Q\bar{Q}}$ which determines r_σ modulo $q-1$ and hence modulo p^n. A careful choice of the unit we start with, δ, gives us the necessary information on r_σ to conclude.

This is the essential idea behind Thaine's proof.

Generalisation to imaginary quadratic fields: There had been generalisations of Stickelberger's theorem to the case of totally real fields (see the notes at the end of the Chapter 6 in [4]) and the Thaine's theorem can also be deduced from the results of Mazur-Wiles. But the point about Thaine's work was its simplicity and adaptability to other situations. Most famously, Rubin [2] was able to obtain a generalisation to the case of abelian extensions of imaginary quadratic fields which he later used to obtain, for the first time, examples of finite Shafarevich-Tate groups of elliptic curves.

REFERENCES

1. S. A. Katre, Gauss-Jacobi sums and Stickelberger's theorem, These proceedings.

2. K. Rubin, Global units and ideal class groups, *Invent. Math.* 89 (1987), 511–526.

3. F. Thaine, On the ideal class groups of real abelian number fields, *Ann. of Math.* 128 (1988), 1–18.

4. L. C. Washington, *Introduction to Cyclotomic Fields*, GTM, Springer-Verlag.

C. S. Yogananda
MO-Cell (DAE), Dept. of Maths, IISc.
Bangalore - 560012.
e-mail: yoga@math.iisc.ernet.in