The Stickelberger Ideal

Robin Chapman

7 November 1999

I give a simple proof of the theorem of Iwasawa, that the index of an ideal defined via the Stickelberger element associated to the Galois group of $\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}$ is the minus part of the class number of $\mathbf{Q}(\zeta_{p^n})$. This is Theorem 6.19 in [1]. However I find Washington's proof to be overcomplicated and inelegant. Instead of providing a global approach he gives a local proof at each prime. In effect that he proves the result three times, each case varying with the idiosyncrasy of the prime involved. In this note I give a direct global proof, essentially a simplification of Washington's.

I am indebted to Franz Lemmermeyer for pointing out some errors in an earlier version of this note.

We need to define our notation. Let p^n be a power of the odd prime p. Let G be a group isomorphic to $(\mathbf{Z}/p^n\mathbf{Z})^*$. Let σ_a be the element of G corresponding to the integer a coprime to p. (The notation comes from the standard identification of G with the Galois group of $\mathbf{Q}(\zeta_{p^n})/\mathbf{Q}$, but we shall not need this.) Let $R = \mathbf{Z}[G]$ be the integral group ring of G. We define the *Stickelberger element* as

$$\theta = \frac{1}{p^n}\sum_{\substack{a=1\\ p\nmid a}}^{p^n} a\sigma_a^{-1}.$$

Note that $\theta \in \mathbf{Q}[G]$ but $\theta \notin R$. The *Stickelberger ideal* is defined as $I = R\theta \cap R$. Let

$$I' = \{\alpha \in R : \alpha\theta \in R\}$$

so that $I = I'\theta$. Then I' is an ideal of R which we wish to identify. To this end define a ring homomorphism $\phi : R \to \mathbf{Z}/p^n\mathbf{Z}$ by $\phi(\sigma_a) = a$. Then ϕ is surjective so its kernel has index p^n in R.

Lemma 1 *The ideal I' is the kernel of $\phi : R \to \mathbf{Z}/p^n\mathbf{Z}$.*

Proof This is a reformulation of Lemma 6.9 in [1].

Let

$$\alpha = \sum_{\substack{b=1 \\ p \nmid b}}^{p^n} x_b \sigma_b \in R.$$

Then

$$p^n \alpha\theta = \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} \sum_{\substack{b=1 \\ p \nmid b}}^{p^n} a x_b \sigma_a^{-1} \sigma_b = \sum_{\substack{c=1 \\ p \nmid c}}^{p^n} \sigma_c \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} a x_{ac}.$$

If $\alpha\theta \in R$ then the coefficient of σ_1 in $p^n \alpha\theta$ is divisible by p^n and so

$$\sum_{\substack{a=1 \\ p \nmid a}}^{p^n} a x_a \equiv 0 \pmod{p^n}$$

or equivalently $\phi(\alpha) = 0$. Conversely, if $\phi(\alpha) = 0$ then the coefficient of σ_1 in $\alpha\theta$ is an integer. But the coefficient of σ_c in $\alpha\theta$ is also the coefficient of σ_1 in $\alpha\sigma_c^{-1}\theta$. But as ϕ is a homomorphism, $\phi(\alpha) = 0$ implies that $\phi(\alpha\sigma_c^{-1}) = 0$, and so the coefficient of σ_c in $\alpha\theta$ is an integer. Hence $\alpha\theta \in R$.

To summarize, $\alpha\theta \in R$ if and only if $\phi(\alpha) = 0$, as required. $\square$

Following Washington define $J = \sigma_{-1}$, and let

$$R^- = \{\alpha \in R : J\alpha = -\alpha\}.$$

Suppose that

$$\alpha = \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} x_a \sigma_a \in R.$$

Then $\alpha \in R^-$ if and only if $x_{p^n - a} = -x_a$ for each a, equivalently, if and only if

$$\alpha = (1 - J) \sum_{\substack{a=1 \\ p \nmid a}}^{(p^n-1)/2} x_a \sigma_a.$$

Hence $R^- \subseteq (1 - J)R$, and the reverse inclusion is obvious, and so $R^- = (1 - J)R$. Define $I^- = I \cap R^-$. Theorem 6.19 of [1] states:

Theorem 1 (Iwasawa) *We have*

$$|R^- : I^-| = h^-(\mathbf{Q}(\zeta_{p^n})).$$

Here $h^-(\mathbf{Q}(\zeta_{p^n}))$ is the minus part of the class number of $\mathbf{Q}(\zeta_{p^n})$, defined to be $h(\mathbf{Q}(\zeta_{p^n}))/h(\mathbf{Q}(\zeta_{p^n} + \zeta_{p^n}^{-1}))$.

For the proof of theorem 1 we require a couple of lemmas.

Lemma 2 *We have $I' \cap R^- = (1-J)I'$ and $|R^- : (1-J)I'| = p^n$.*

Proof Certainly $(1-J)I' \subseteq I' \cap R^-$. Let $\alpha \in I' \cap R^-$. Then $\alpha = (1-J)\beta$ where $\beta \in R$, since $R^- = (1-J)R$. Then

$$0 = \phi(\alpha) = \phi((1-J)\beta) = (1-\phi(J))\phi(\beta) = 2\phi(\beta).$$

As 2 is a unit in $\mathbf{Z}/p^n\mathbf{Z}$, then $\phi(\beta) = 0$ and so $\beta \in I'$. Thus $\alpha \in (1-J)I'$ and so $I' \cap R^- = (1-J)I'$.

The set $(1-J)I'$ is thus the intersection of of R^- and the kernel of ϕ. But $1-J \in R^-$ and $\phi(1-J) = 2$, which is a unit in $\mathbf{Z}/p^n\mathbf{Z}$. Thus $\phi(R^-) = \mathbf{Z}/p^n\mathbf{Z}$ and so $|R^- : (1-J)I'| = p^n$. □

Define a homomorphism $\psi : R \to \mathbf{Z}$ by $\psi(\sigma_a) = 1$ for each a. Let

$$N = \sum_{\sigma \in G} \sigma$$

be the *norm* element of R. Then $\sigma_a N = N$ for each a, and so $\alpha N = \psi(\alpha)N$ for each $\alpha \in R$.

Lemma 3 *We have $2I^- \subseteq (1-J)I'\theta$ and $|(1-J)I'\theta : 2I^-| = 2$.*

Proof Let $\alpha \in I^-$. Then $\alpha = \beta\theta$ for some $\beta \in I'$. Also $J\alpha = -\alpha$ and so

$$2\alpha = (1-J)\alpha = (1-J)\beta\theta \in (1-J)I'\theta.$$

Hence $2I^- \subseteq (1-J)I'\theta$.

Now let $\gamma \in I'$. Then

$$2\gamma\theta = (1+J)\gamma\theta + (1-J)\gamma\theta.$$

But

$$(1+J)\theta = \frac{1}{p^n} \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} [a + (p^n - a)]\sigma_a = N.$$

Hence $1 + J \in I'$ and $N \in I$. We thus have

$$2\gamma\theta = \gamma N + (1-J)\gamma\theta = gN + (1-J)\gamma\theta$$

where $g = \psi(\gamma)$. If g is even, then $(1-J)\gamma\theta = 2\gamma\theta - gN \in 2I$ and so $(1-J)\gamma\theta \in 2I^-$. If g is odd then $(1-J)\gamma\theta - N = 2\gamma\theta - (g+1)N \in 2I$ and so $(1-J)\gamma\theta \notin 2R$ and *a fortiori* $(1-J)\gamma\theta \notin 2I^-$.

It follows that

$$2I^- = \{(1-J)\gamma\theta : \gamma \in I' \text{ and } \psi(\gamma) \text{ is even}\}.$$

As $p^n \in I'$ and $\psi(p^n)$ is odd, the set

$$\{(1-J)\gamma\theta : \gamma \in I' \text{ and } \psi(\gamma) \text{ is odd}\}$$

is nonempty, and is thus a coset of $2I^-$ disjoint from $2I^-$. Thus

$$|(1-J)I'\theta : 2I^-| = 2$$

which proves the lemma. □

Proof of Theorem 1 We calculate what we shall denote $|(1-J)I' : (1-J)I'\theta|$. It is not clear whether this is an index, as it might not be the case that $(1-J)I'\theta \subseteq (1-J)I'$. However if A and B are free abelian groups of rank r, each spanning a $\mathbf{Q}$-vector space V of dimension r, then $|A : A \cap B|$ and $|B : A \cap B|$ are both finite and if we define

$$|A : B| = \frac{|A : A \cap B|}{|B : A \cap B|}$$

then $|A : B|$ has the same formal properties as the index. In particular if $T : V \to V$ is a non-singular linear transformation, then $|A : T(A)| = |\det(T)|$. Let

$$V = \mathbf{Q}[G]^- = \{\alpha \in \mathbf{Q}[G] : J\alpha = -\alpha\}.$$

Then V is a $\mathbf{Q}$-vector space of dimension $r = |G|/2$. Also $R^- \subseteq V$ and R^- has rank r. As $|R^- : (1-J)I'| = p^n$ then $(1-J)I'$ has rank r too. Consider $T : V \to V$ given by $T(\alpha) = \alpha\theta$.

We can compute the determinant of T by extending T to a linear map on

$$\mathbf{C}[G]^- = \{\alpha \in \mathbf{C}[G] : J\alpha = -\alpha\}.$$

For a character $\chi : G \to \mathbf{C}^*$ define

$$\epsilon_\chi = \frac{1}{|G|}\sum_{\sigma\in G} \chi(\sigma)\sigma^{-1}.$$

Then $\mathbf{C}[G]^-$ has as a basis the set of ϵ_χ for the odd characters χ, those with $\chi(J) = -1$. But $\sigma\epsilon_\chi = \chi(\sigma)\epsilon_\chi$ for each σ and χ, and so

$$\epsilon_\chi\theta = B_{1,\chi}\epsilon_\chi$$

where

$$B_{1,\chi} = \frac{1}{p^n} \sum_{\substack{a=1 \\ p \nmid a}}^{p^n} a\chi(\sigma_a).$$

As these ϵ_χ form a basis of eigenvectors of T then

$$\det(T) = \prod_{\chi(J)=-1} B_{1,\chi}.$$

Let $h^- = h^-(\mathbf{Q}(\zeta_{p^n}))$. By an argument based on the analytic class number formula [1, Theorem 4.17]

$$h^- = 2p^n \prod_{\chi(J)=-1} (-B_{1,\chi}/2)$$

and so

$$|\det(T)| = \frac{2^r h^-}{2p^n} \neq 0.$$

It follows that $(1-J)I'\theta$ has rank r and $|(1-J)I' : (1-J)I'\theta| = 2^r h^-/(2p^n)$. But

$$|R^- : I^-| = |R^- : (1-J)I'||(1-J)I' : (1-J)I'\theta||(1-J)I'\theta : 2I^-||I^- : 2I^-|^{-1}.$$

We have seen that $|R^- : (1-J)I'| = p^n$ (Lemma 2), $|(1-J)I' : (1-J)I'\theta| = 2^r h^-/(2p^n)$ and $|(1-J)I'\theta : 2I^-| = 2$ (Lemma 3). As I^- has rank r then $|I^- : 2I^-| = 2^r$. Putting all these pieces together we get $|R^- : I^-| = h^-$, as required. □

Lemmermeyer has informed me that with suitable modifications this proof is also valid for $p = 2$. If $p = 2$ and $n \geq 2$ (to avoid trivialities) we find that in Lemma 2 we $|I' \cap R^- : (1-J)I'| = 2$ but that $|R^- : (1-J)I'| = 2^n$. In Lemma 3 we find that $(1-J)I'\theta = 2I^-$. Finally in the proof of Theorem 1 we need that the anlaytic class number formula gives us $|\det(T)| = 2^r h^-/2^n$.

References

[1] Lawrence C. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982, 1997.