CYCLOTOMIC INTEGERS

TREVOR HYDE

Let p be a prime number and ζ be a primitive p^nth root of unity. We show the following:

Proposition 1. *If $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\zeta)$, then $\mathcal{O} = \mathbb{Z}[\zeta]$.*

If we let $\pi = \zeta - 1$, then what we really show is that $\mathbb{Z}[\pi]$ is the ring of integers, although this amounts to the same thing. The key to Proposition 1 is ramification. The special properties of the extension $\mathcal{O}/\mathbb{Z}$ we use are:

(1) $\mathcal{O}/\mathbb{Z}$ has a totally ramified prime (π), and
(2) No other prime of $\mathcal{O}/\mathbb{Z}$ ramifies.

The ring of integers $\mathcal{O}$ is a global object but is computed locally. Property (1) of $\mathcal{O}/\mathbb{Z}$ suffices to compute $\mathcal{O}$ locally at (π). The value of Property (2) comes from the following Lemma:

Lemma 2. *If $\mathcal{O}$ is the ring of integers in a number field $K = \mathbb{Q}(a)$ with $a \in \mathcal{O}$, then*

$$\mathcal{O} \subseteq \frac{1}{\operatorname{disc}(a)}\mathbb{Z}[a].$$

Property (2) tells us that $\operatorname{disc}(\pi) \in \mathcal{O}_Q^\times$ for any other prime $Q \subseteq \mathcal{O}$, hence $\mathcal{O}_Q = \mathbb{Z}[\pi]_Q$. Thus our proof consists of an entirely local analysis of $\mathcal{O}$ at (π) combined with the global information coming from $\operatorname{disc}(\pi)$.

Lemma 3. *Let ζ be a primitive p^nth root of unity, $\pi = \zeta - 1$, and φ be Euler's function. Then*

$$(p) = (\pi)^{\varphi(p^n)}$$

as ideals in $\mathcal{O}$ and

$$\sqrt{\big(\operatorname{disc}(\pi)\big)} = (p)$$

as ideals of $\mathbb{Z}$.

Proof. From $x^{p^n} - 1 \equiv (x-1)^{p^n} \bmod p$ it follows that the minimal polynomial of $\pi = \zeta - 1$ is Eisenstein and of degree $\varphi(p^n)$, giving us the factorization of ideals

$$(p) = (\pi)^{\varphi(p^n)}.$$

Let $\ell \neq p$ be a prime. Then $p^n \mid \ell^{\varphi(p^n)} - 1$, hence the cyclic group $\mathbb{F}^\times_{\ell^{\varphi(p^n)}}$ of order $\ell^{\varphi(p^n)} - 1$ contains p^n distinct p^nth roots of unity. So $x^{p^n} - 1$ is separable modulo ℓ and thus ℓ does not divide $\operatorname{disc}(\zeta) = \operatorname{disc}(\pi)$. □

It is not difficult to compute the discriminant precisely in this case, but here we emphasize that this is unnecessary for the proof of Proposition 1. A computation of the discriminant when $n = 1$ is demonstrated at the end of this note.

Date: October 22nd, 2016.

Lemma 4. *Suppose π is an algebraic integer, $\mathcal{O}$ is the ring of integers in $\mathbb{Q}(\pi)$, and $\mathfrak{p} = (\pi)$ is a prime ideal of $\mathcal{O}$ totally ramified in $\mathcal{O}/\mathbb{Z}$. Then $\mathcal{O}_\mathfrak{p} = \mathbb{Z}[\pi]_\mathfrak{p}$.*

Proof. Let $d = [\mathbb{Q}(\pi) : \mathbb{Q}]$. Lemma 2 tells us that any $b \in \mathcal{O}_\mathfrak{p}$ may be written as

$$b = \big(a_0 + a_1\pi + a_2\pi^2 + \ldots + a_{d-1}\pi^{d-1}\big)/\mathrm{disc}(\pi),$$

with $a_i \in \mathbb{Z}_\mathfrak{p}$. We show that each a_k is divisible by $\mathrm{disc}(\pi)$, implying that $b \in \mathbb{Z}[\pi]_\mathfrak{p}$. Let v be the normalized valuation at the prime $\mathfrak{p}$. Then, for example, $v(\pi) = 1$ and $v(\mathbb{Z}_\mathfrak{p}) \subseteq d\mathbb{Z}$ by our assumption that $\mathfrak{p}$ is totally ramified. Let us compute the valuation of each term in b.

$$v\big(a_k\pi^k/\mathrm{disc}(\pi)\big) = v(a_k) + k - v\big(\mathrm{disc}(\pi)\big). \tag{1}$$

Since $v(a)$ is divisible by d for any $a \in \mathbb{Z}_\mathfrak{p}$, we have for each k,

$$v\big(a_k\pi^k/\mathrm{disc}(\pi)\big) \equiv k \bmod d.$$

Hence all the terms in b have distinct valuations modulo d, and then $0 \leq k < d$ implies all terms in b have distinct valuations in $\mathbb{Z}$ (this is my favorite part of the argument!) From $b \in \mathcal{O}_\mathfrak{p}$, the distinctness of valuations, and the non-archimedean property of v, we have for each k,

$$0 \leq v(b) = \min_j v\big(a_j\pi^j/\mathrm{disc}(\pi)\big) \leq v\big(a_k\pi^k/\mathrm{disc}(\pi)\big). \tag{2}$$

Combining (1) and (2) we have

$$0 \leq v(a_k) + k - v\big(\mathrm{disc}(\pi)\big) \Longrightarrow \frac{v\big(\mathrm{disc}(\pi)\big)}{d} - \frac{k}{d} \leq \frac{v(a_k)}{d}. \tag{3}$$

Both $v\big(\mathrm{disc}(\pi)\big)/d$ and $v(a_k)/d$ are integers. On the other hand, $0 \leq k < d$, so that $\frac{k}{d} < 1$. It follows that (3) can be strengthened to

$$\frac{v\big(\mathrm{disc}(\pi)\big)}{d} \leq \frac{v(a_k)}{d} \Longrightarrow v\big(\mathrm{disc}(\pi)\big) \leq v(a_k),$$

which is equivalent to $\mathrm{disc}(\pi)$ dividing a_k in $\mathbb{Z}_\mathfrak{p}$, as we wished to show. □

We now prove Proposition 1.

Proof. Lemma 2 and Lemma 3 imply that for all prime ideals $\mathfrak{q} \neq \mathfrak{p} = (\pi)$,

$$\mathbb{Z}[\pi]_\mathfrak{q} \subseteq \mathcal{O}_\mathfrak{q} \subseteq \frac{1}{\mathrm{disc}(\pi)}\mathbb{Z}[\pi]_\mathfrak{q} = \mathbb{Z}[\pi]_\mathfrak{q} \Longrightarrow \mathcal{O}_\mathfrak{q} = \mathbb{Z}[\pi]_\mathfrak{q}.$$

Then Lemma 4 implies $\mathcal{O}_\mathfrak{p} = \mathbb{Z}[\pi]_\mathfrak{p}$, hence $\mathcal{O} = \mathbb{Z}[\pi]$. □

We conclude this note with a computation of $\mathrm{disc}(\zeta)$ when ζ is a pth root of unity. There is a quick derivation using norms and derivatives which may be found in essentially every textbook. We give an alternative derivation for the sake of a fresh perspective. A similar approach works for p^nth roots of unity, but requires more book-keeping.

Lemma 5. *Let ζ be a primitive pth root of unity. Then, as ideals of $\mathbb{Z}$, we have*

$$\big(\mathrm{disc}(\zeta)\big) = (p)^{p-2}.$$

Proof. It follows from Lemma 3 that $\big(\mathrm{disc}(\zeta)\big)$ is a power of (p). To determine the power we consider the local expansion of the pth roots of unity at (π). Since $x^p - 1 \equiv (x-1)^p \bmod p$, we see that the pth roots of unity are all congruent to 1 modulo π. The binomial theorem implies

$$(1 + a\pi)^p \equiv 1 \bmod \pi^2,$$

for each $a \in \mathbb{Z}/(p)$, which tells us that all the pth roots of unity are distinct modulo π^2. Hence, if v is the normalized valuation at (π), then $v(\zeta_1 - \zeta_2) = 1$ for any pair of distinct pth roots of unity. Recall that $\mathrm{disc}(\zeta)$ is the discriminant of the minimal polynomial $f(x)$ of ζ defined by

$$\mathrm{disc}(f) = \prod_{\alpha,\beta} (\alpha - \beta)^2,$$

where the product is taken over all pairs of roots of f in a splitting field. There are $\binom{p-1}{2} = \frac{(p-1)(p-2)}{2}$ pairs of roots, and $(p) = (\pi)^{p-1}$ as ideals of $\mathcal{O}$, hence

$$\big(\mathrm{disc}(\zeta)\big) = (\pi)^{2\binom{p-1}{2}} = (p)^{p-2},$$

as ideals of $\mathbb{Z}$. □

DEPT. OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,
E-mail address: tghyde@umich.edu