THE RING OF CYCLOTOMIC INTEGERS

RITIK JAIN

In this note, we use p-adic numbers to prove that $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})} = \mathbb{Z}[\zeta_{p^r}]$ for a prime power p^r.[1] The proof proceeds in two steps: first, we reduce the problem to proving the statement over $\mathbb{Q}_p$, then establish the result locally. This approach is less computationally intensive than the standard proofs, and moreover provides a nice illustration of the technique of "passing to local fields".

Lemma 1. Let $A \subseteq B$ be two finitely generated, torsion-free abelian groups of rank $n \in \mathbb{N}$. Then for each prime p,

$$[B \otimes_{\mathbb{Z}} \mathbb{Z}_p : A \otimes_{\mathbb{Z}} \mathbb{Z}_p] = p^{v_p([B:A])},$$

where left-hand side is the cardinality of the $\mathbb{Z}_p$-module $(B \otimes_{\mathbb{Z}} \mathbb{Z}_p)/(A \otimes_{\mathbb{Z}} \mathbb{Z}_p)$, and v_p denotes the p-adic valuation.

Proof. Choose $\mathbb{Z}$-bases so that the inclusion $A \hookrightarrow B$ is represented by a matrix $T \in M_n(\mathbb{Z})$ with determinant $d \neq 0$, so $[B : A] = |d|$. After tensoring by $\mathbb{Z}_p$, the inclusion $A \otimes_{\mathbb{Z}} \mathbb{Z}_p \hookrightarrow B \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is still represented by T (now viewed as a matrix over $\mathbb{Z}_p$), thus over the PID $\mathbb{Z}_p$, we can put T into Smith normal form as follows:

$$U\,T\,V = \operatorname{diag}(p^{a_1}, \ldots, p^{a_n}), \qquad U, V \in \mathrm{GL}_n(\mathbb{Z}_p), \quad a_i \geq 0.$$

The cokernel of $T : A \otimes \mathbb{Z}_p \to B \otimes \mathbb{Z}_p$ is thus

$$(B \otimes \mathbb{Z}_p)/(A \otimes \mathbb{Z}_p) \;\cong\; \bigoplus_{i=1}^{n} \mathbb{Z}_p/(p^{a_i}) \;\cong\; \bigoplus_{i=1}^{n} \mathbb{Z}/p^{a_i}\mathbb{Z},$$

so

$$[B \otimes \mathbb{Z}_p : A \otimes \mathbb{Z}_p] = p^{a_1 + \cdots + a_n} = p^{v_p(\det T)} = p^{v_p([B:A])}.$$

□

Lemma 2. For a prime power p^r, $\mathbb{Z}_p[\zeta_{p^r}]$ is a discrete valuation ring.

Proof. Using

$$\Phi_{p^r}(x) = \prod_{\substack{1 \leq a \leq p^r \\ (a, p^r) = 1}} (x - \zeta_{p^r}^a),$$

Date: November 2025.

[1]The inspiration for this proof was a comment written by Keith Conrad on MathOverflow.

we obtain

$$\Phi_{p^r}(1) = p = \prod_{\substack{1\leq a\leq p^r \\ (a,p^r)=1}} (1-\zeta_{p^r}^a).$$

The factors $(1-\zeta_{p^r}^a)$ are Galois conjugates of $1-\zeta_{p^r}$, so they all generate the same prime ideal $(1-\zeta_{p^r})$ above p. That is, (p) is a power of $(1-\zeta_{p^r})$. But every maximal ideal in $\mathbb{Z}_p[\zeta_{p^r}]$ contains (p), hence $(1-\zeta_{p^r})$ is the unique maximal ideal in $\mathbb{Z}_p[\zeta_{p^r}]$. In particular, $\mathbb{Z}_p[\zeta_{p^r}]$ is a local ring. But $\mathbb{Z}_p[\zeta_{p^r}]$ is also finite over the DVR $\mathbb{Z}_p$, so in particular $\mathbb{Z}_p[\zeta_{p^r}]$ is a local Dedekind domain. Since every local Dedekind domain is a DVR, we have the result. □

Having established these two lemmas, the proof becomes relatively straightforward.

Theorem. Let $K := \mathbb{Q}(\zeta_{p^r})$ for a prime power p^r. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$.

Proof. Since the inclusion $\mathbb{Z}[\zeta_{p^r}] \subseteq \mathcal{O}_K$ is clear, it suffices to show that

$$[\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}]] = 1,$$

where $\mathcal{O}_K$ and $\mathbb{Z}[\zeta_{p^r}]$ are viewed as free $\mathbb{Z}$-modules. By Marcus, Ch. 1, Exercise 27(c), we have

$$\operatorname{disc}(\mathbb{Z}[\zeta_{p^r}]) = \operatorname{disc}(\mathcal{O}_K)\cdot[\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}]]^2. \tag{1}$$

Since it is known that $\operatorname{disc}(\mathbb{Z}[\zeta_{p^r}])$ is a signed power of p, (1) implies that $[\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}]]$ is a power of p. That is,

$$[\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}]] = p^{v_p([\mathcal{O}_K:\mathbb{Z}[\zeta_{p^r}]])}, \tag{2}$$

Now, tensoring by $\mathbb{Z}_p$, we have

$$\mathbb{Z}[\zeta_{p^r}]\otimes_{\mathbb{Z}}\mathbb{Z}_p \cong \mathbb{Z}_p[\zeta_{p^r}], \qquad \mathcal{O}_K\otimes_{\mathbb{Z}}\mathbb{Z}_p \cong \mathcal{O}_{K_p},$$

where $K_p := \mathbb{Q}_p(\zeta_{p^r})$. By Lemma 1,

$$[\mathcal{O}_{K_p} : \mathbb{Z}_p[\zeta_{p^r}]] = p^{v_p([\mathcal{O}_K:\mathbb{Z}[\zeta_{p^r}]])},$$

thus by (2),

$$[\mathcal{O}_K : \mathbb{Z}[\zeta_{p^r}]] = [\mathcal{O}_{K_p} : \mathbb{Z}_p[\zeta_{p^r}]].$$

Therefore, it suffices to show that $\mathcal{O}_{K_p} = \mathbb{Z}_p[\zeta_{p^r}]$. By Lemma 2, $\mathbb{Z}_p[\zeta_{p^r}]$ is a discrete valuation ring in K_p, hence it is integrally closed in K_p. Since $\mathbb{Z}_p \subseteq \mathbb{Z}_p[\zeta_{p^r}]$, we have that $\mathbb{Z}_p[\zeta_{p^r}]$ must be the integral closure of $\mathbb{Z}_p$ in K_p. But $\mathcal{O}_{K_p}$ is the unique subring of K_p with this property, thus $\mathcal{O}_{K_p} = \mathbb{Z}_p[\zeta_{p^r}]$ as desired. □