THE PRIME-POWER CYCLOTOMIC INTEGER RING BY TRACES AND NORMS

Let p be prime. For each positive integer e, let $\zeta_{p^e} = \exp(2\pi i/p^e)$ denote the usual complex primitive p^eth root of unity, and introduce the field

$$K_e = \mathbb{Q}(\zeta_{p^e}).$$

Let $\mathcal{O}_e$ denote the integer ring of K_e. The smallest candidate for $\mathcal{O}_e$ is $\mathbb{Z}[\zeta_{p^e}]$. We will show that this candidate is the full integer ring:

$$\boxed{\text{For } e \geq 1 \text{ and } K_e = \mathbb{Q}(\zeta_{p^e}) \text{ we have } \mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}].}$$

In consequence, the factorization of p in $\mathcal{O}_e$ is

$$p\mathcal{O}_e = \langle 1 - \zeta_{p^e} \rangle^{\phi(p^e)}, \quad \langle 1 - \zeta_{p^e} \rangle \text{ maximal.}$$

The equality in the previous display is not hard to establish, but the fact that $\langle 1 - \zeta_{p^e} \rangle$ is maximal is requires more; we will discuss this below. The maximality shows that the equality gives the full factorization of $p\mathcal{O}_e$, or at least *a* full factorization if we don't want to rely on the uniqueness of ideal factorization in number rings.

To establish the boxed statement, we first lay out some results about prime-power cyclotomic polynomials, in the process establishing the equality in the previous display but not the maximality, and we explain how the maximality follows from the boxed statement and a theorem. Then we prove the boxed statement by induction on e, the base case and the inductive step requiring different arguments. The only technical tools used here are the trace and the norm; in particular, we do not use the discriminant.

This writeup is derived from arguments in the books by Samuel and Marcus. Samuel proves the prime case and then writes, "The results of this section easily extend [to the prime-power case]." However, the word *easily* is context-dependent, and to extend Samuel's argument I needed to augment its methods by what would amount to further ideas for a beginning student. If indeed the prime-power case can be covered by a proof that uses only the methods—narrowly construed—of Samuel's proof for the prime case then I would appreciate learning it. On the other hand, Marcus does prove the prime-power case, but his argument uses the discriminant. Notwithstanding that every student of algebraic number theory needs to learn about the discriminant and to see it in action, my goal here is a more self-contained presentation of this writeup's result, aimed at students interested in seeing it proved without having to invest in general machinery.

Contents

1. Prime-power Cyclotomic Polynomials

The polynomial of ζ_p over $\mathbb{Q}$ is

$$\Phi_p(X) = \sum_{i=0}^{p-1} X^i = 1 + X + X^2 + \cdots + X^{p-1},$$

so that in particular $\Phi_p(1) = p$. This polynomial is well known to be irreducible via Eisenstein's criterion, and perhaps less known but more clearly shown to be irreducible via Schönemann's criterion; the latter will be reviewed below. The relation

$$(1-X)\Phi_p(X) = 1 - X^p \quad \text{in } \mathbb{Z}[X]$$

reduces modulo p to

$$(1-X)\overline{\Phi}_p(X) = (1-X)^p \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X],$$

from which

$$\overline{\Phi}_p(X) = (1-X)^{p-1} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

For general $e \geq 1$, the polynomial $\Phi_{p^e}(X)$ of ζ_{p^e} is

$$\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}}),$$

with the irreducibility of this polynomial again established by Eisenstein's criterion or Schönemann's criterion, and the previous two displays give the reduction of $\Phi_{p^e}(X)$ modulo p,

$$\overline{\Phi}_{p^e}(X) = \overline{\Phi}_p(X)^{p^{e-1}} = (1-X)^{\phi(p^e)} \quad \text{in } (\mathbb{Z}/p\mathbb{Z})[X].$$

The polynomial $\Phi_{p^e}(X)$ splits over $K_e = \mathbb{Q}(\zeta_{p^e})$ as

$$\Phi_{p^e}(X) = \prod_{j \in (\mathbb{Z}/p^e\mathbb{Z})^\times} (X - \zeta_{p^e}^j) \quad \text{in } K_e[X],$$

and so the norm of $1 - \zeta_{p^e}$ from K_e to $\mathbb{Q}$ is

$$\mathrm{N}_{K_e/\mathbb{Q}}(1-\zeta_{p^e}) = \prod_{j \in (\mathbb{Z}/p^e\mathbb{Z})^\times} (1 - \zeta_{p^e}^j) = \Phi_{p^e}(1) = \Phi_p(1^{p^{e-1}}) = \Phi_p(1) = p.$$

The relation $p = \prod_{j \in (\mathbb{Z}/p^e\mathbb{Z})^\times} (1 - \zeta_{p^e}^j)$ in the previous display combines with the finite geometric sum formula to give

$$p = (1-\zeta_{p^e})^{\phi(p^e)} \prod_{j \in (\mathbb{Z}/p^e\mathbb{Z})^\times} \sum_{i=0}^{j-1} \zeta_{p^e}^i,$$

so that $(1-\zeta_{p^e})^{\phi(p^e)}$ divides p in $\mathcal{O}_e$. Further, taking norms from K_e to $\mathbb{Q}$ in the previous display shows that the product of sums is a unit in $\mathcal{O}_e$ (in fact, that each sum is a unit), so that p and $(1-\zeta_{p^e})^{\phi(p^e)}$ are associates in $\mathcal{O}_e$; equivalently $p\mathcal{O}_e = \langle 1-\zeta_{p^e}\rangle^{\phi(p^e)}$ in $\mathcal{O}_e$.

The work so far doesn't establish that the ideal $\langle 1-\zeta_{p^e}\rangle$ of $\mathcal{O}_e$ is maximal. However, once we establish that $\mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}]$, the maximality follows from the theorem that factors $p\mathcal{O}_e$ by factoring $\Phi_{p^e}(X)$ modulo p; indeed, we have established that $\overline{\Phi}_{p^e}(X) = (1-X)^{\phi(p^e)}$ and we have established that $1-\zeta_{p^e}$ divides p in $\mathcal{O}_e$, so the theorem gives

$$p\mathcal{O}_e = \langle 1-\zeta_{p^e}\rangle^{\phi(p^e)}, \quad \langle 1-\zeta_{p^e}\rangle \text{ maximal.}$$

This repeats the equality at the end of the previous paragraph but also adds that the equality gives the complete factorization of p in $\mathcal{O}_e$. Alternatively, the theorem that the ramification, residue field degree, and decomposition index multiply to $\phi(p^e)$ gives the maximality of the ideal from the equality. For that matter, because the norm p of $\langle 1-\zeta_{p^e}\rangle$ doesn't factor in $\mathbb{Z}$, nor does $\langle 1-\zeta_{p^e}\rangle$ factor in $\mathcal{O}_e$. In the context of this writeup we emphasize the first of this paragraph's three arguments that $\langle 1-\zeta_{p^e}\rangle$ is maximal, because the writeup's goal is to establish that $\mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}]$.

We end this section by stating, applying, and proving Schönemann's criterion. David Cox's January 2011 *American Mathematical Monthly* article on this subject is highly recommended.

Proposition 1.1 (Schönemann's Criterion)**.** *Let A be a UFD, and let $f(X) \in A[X]$ be monic of positive degree n. Suppose that for some element a of A and some prime ideal $\mathfrak{p}$ of A,*

$$f(X) = (X-a)^n \bmod \mathfrak{p}[X] \qquad \text{and} \qquad f(a) \neq 0 \bmod \mathfrak{p}^2.$$

Then $f(X)$ is irreducible modulo $\mathfrak{p}^2[X]$ and hence $f(X)$ is irreducible in $A[X]$.

Immediately in consequence of Schönemann's criterion, the polynomial $\Phi_{p^e}(X)$ for p prime and $e \geq 1$ is irreducible, as follows. We have established that its reduction modulo p is $\overline{\Phi}_{p^e}(X) = (X-1)^{\phi(p^e)}$ (earlier we had $(1-X)^{\phi(p^e)}$ on the right side, but the exponent is even unless $p^e = 2$, and in that case $X-1 = 1-X$ modulo p), and also we have computed $\Phi_{p^e}(1) = p$, which is nonzero modulo p^2; so the criterion applies.

Proof of Schönemann's criterion. We show the contrapositive statement, arguing that if $f(X)$ is reducible mod $\mathfrak{p}^2[X]$ then its reduction looks enough like $(X-a)^n$ to force $f(a) = 0 \bmod \mathfrak{p}^2$. Specifically, suppose that

$$f(X) = f_1(X) f_2(X) \bmod \mathfrak{p}^2[X].$$

The reduction modulo $\mathfrak{p}^2$ agrees modulo $\mathfrak{p}$ with the reduction modulo $\mathfrak{p}$,

$$f_1(X) f_2(X) = (X-a)^n \bmod \mathfrak{p}[X],$$

and so, because we may take $f_1(X)$ and $f_2(X)$ to be monic, we have for $i = 1, 2$,

$$f_i(X) = (X-a)^{n_i} \bmod \mathfrak{p}[X], \quad n_i \in \mathbb{Z}^+.$$

Specifically, from the equality $f_1(X)f_2(X) = (X-a)^n$ in $(A/\mathfrak{p})[X]$ where the polynomials now have their coefficients reduced modulo $\mathfrak{p}$, the same equality holds in $k[X]$ where k is the quotient field of the integral domain $A/\mathfrak{p}$. Because $k[X]$ is a UFD, $f_i(X) = (X-a)^{n_i}$ in $k[X]$ for $i = 1, 2$, but these equalities stand between elements of $(A/\mathfrak{p})[X]$, giving the previous display. In consequence of the display $f_i(a) = 0 \bmod \mathfrak{p}$ for $i = 1, 2$, and so the first display in the proof gives $f(a) = 0 \bmod \mathfrak{p}^2$ as desired. □

2. Base Case: the Prime Cyclotomic Field

Let $K_1 = \mathbb{Q}(\zeta_p)$. The cyclotomic polynomial

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + 1$$

shows that $[K_1 : \mathbb{Q}] = p-1$. It also shows that ζ_p has trace -1, and hence so do its Galois conjugates, ζ_p^j for $j = 1, \ldots, p-1$, while 1 has trace $p-1$. A basis of K_1

as a vector space over $\mathbb{Q}$ is $\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}$, whereas adding ζ_p^{p-1} creates a linearly dependent set. We establish that the integer ring of K_1 is $\mathcal{O}_1 = \mathbb{Z}[\zeta_p]$.

The first step is to show that

$$(1-\zeta_p)\mathcal{O}_1 \cap \mathbb{Z} = p\mathbb{Z}.$$

To see this, recall from above that $\mathrm{N}(1-\zeta_p) = \prod_{j=1}^{p-1}(1-\zeta_p^j) = p$, and thus $1-\zeta_p$ divides p in $\mathcal{O}_1$, giving $p\mathbb{Z} \subset p\mathcal{O}_1 \cap \mathbb{Z} \subset (1-\zeta_p)\mathcal{O}_1 \cap \mathbb{Z}$; the maximality of $p\mathbb{Z}$ makes the ideal-containments equalities, because otherwise $1-\zeta_p$ divides 1 in $\mathcal{O}_1$ and then taking norms gives the false statement that p divides 1 in $\mathbb{Z}$.

Now consider any $\alpha \in \mathcal{O}_1$. Let $\{\alpha_j\}$ denote the conjugates of α in $\mathcal{O}_1$, recall as noted above that $1-\zeta_p$ divides $1-\zeta_p^j$ in $\mathcal{O}_1$ for $j = 2, \ldots, p-2$ by the finite geometric sum formula, and compute that consequently,

$$\mathrm{Tr}(\alpha(1-\zeta_p)) = \sum_{j=1}^{p-1} \alpha_j(1-\zeta_p^j) \in (1-\zeta_p)\mathcal{O}_1 \cap \mathbb{Z} = p\mathbb{Z}.$$

In coordinates we have

$$\alpha = \sum_{j=0}^{p-2} a_j \zeta_p^j, \quad a_0, \ldots, a_{p-2} \in \mathbb{Q},$$

and so also, because $\mathrm{Tr}\,\zeta_p^j = -1$ for $j = 1, \ldots, p-1$ while $\mathrm{Tr}\,1 = p-1$,

$$\mathrm{Tr}(\alpha(1-\zeta_p)) = \sum_{j=0}^{p-2} a_j \mathrm{Tr}(\zeta_p^j - \zeta_p^{j+1}) = pa_0.$$

That is, pa_0 lies in $p\mathbb{Z}$, giving $a_0 \in \mathbb{Z}$. Continuing, we now have $\zeta_p^{-1}(\alpha - a_0) \in \mathcal{O}_1$ and the same argument shows that $a_1 \in \mathbb{Z}$, and so on, so that $\alpha \in \mathbb{Z}[\zeta_p]$. This completes the proof that $\mathcal{O}_1 = \mathbb{Z}[\zeta_p]$.

3. Induction Step: Incrementing the Power of the Prime

Again let p be prime, and let $e \geq 2$ be a positive integer. We assume that

$$\text{for } K_{e-1} = \mathbb{Q}(\zeta_{p^{e-1}}) \text{ we have } \mathcal{O}_{e-1} = \mathbb{Z}[\zeta_{p^{e-1}}],$$

and we show that consequently

$$\text{for } K_e = \mathbb{Q}(\zeta_{p^e}) \text{ we have } \mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}].$$

To set up the inductive argument, note that $[K_e : K_{e-1}] = \phi(p^e)/\phi(p^{e-1}) = p$. (This differs from $[K_1 : K_0] = p-1$, where K_0 naturally denotes $\mathbb{Q}$.) The Galois group of K_e over K_{e-1} is naturally viewed as

$$\{1 + ip^{e-1} + p^e\mathbb{Z}\} \subset (\mathbb{Z}/p^e\mathbb{Z})^\times,$$

and the minimal polynomial of ζ_{p^e} over K_{e-1} is

$$f_e(X) = X^p - \zeta_{p^{e-1}}.$$

This polynomial shows that $\mathrm{Tr}_{K_e/K_{e-1}}\,\zeta_{p^e} = 0$, and $\mathrm{Tr}_{K_e/K_{e-1}}\,1 = p$. The isomorphism from $K_{e-1}[X]/\langle f_e(X)\rangle$ to K_e, taking $X + \langle f_e(X)\rangle$ to ζ_{p^e}, shows that a basis

of K_e over K_{e-1} is $\{\zeta_{p^e}^i : i = 0, \dots, p-1\}$. Generalizing the two traces just noted, compute for any integer k that

$$\mathrm{Tr}_{K_e/K_{e-1}}\, \zeta_{p^e}^k = \sum_{i=0}^{p-1} \zeta_{p^e}^{(1+ip^{e-1})k} = \zeta_{p^e}^k \sum_{i=0}^{p-1} (\zeta_p^k)^i = \begin{cases} p\zeta_{p^{e-1}}^{k/p} & \text{if } p \mid k \\ 0 & \text{if } p \nmid k. \end{cases}$$

Now we establish that $\mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}]$, assuming that $\mathcal{O}_{e-1} = \mathbb{Z}[\zeta_{p^{e-1}}]$. Consider any element of $\mathcal{O}_e$, taking the form

$$\alpha = \sum_{i=0}^{p-1} a_i \zeta_{p^e}^i, \quad a_i \in K_{e-1} \text{ for } i = 0, \dots, p-1.$$

Multiply by various units and then take traces to get

$$\mathrm{Tr}_{K_e/K_{e-1}}(\alpha \zeta_{p^e}^{-j}) = pa_j, \quad j = 0, 1, \dots, p-1.$$

That is, pa_j lies in $\mathcal{O}_{e-1}$ for each j, and so $\mathcal{O}_e \subset \frac{1}{p}\mathcal{O}_{e-1}[\zeta_{p^e}]$. Our inductive assumption that $\mathcal{O}_{e-1} = \mathbb{Z}[\zeta_{p^{e-1}}]$ makes this containment $\mathcal{O}_e \subset \frac{1}{p}\mathbb{Z}[\zeta_{p^e}]$. Because $\mathbb{Z}[\zeta_{p^e}] = \mathbb{Z}[1 - \zeta_{p^e}]$, we can rewrite the general element of $\mathcal{O}_e$ as

$$\alpha = \frac{1}{p} \sum_{i=0}^{\phi(p^e)-1} b_i (1 - \zeta_{p^e})^i, \quad b_0, \dots, b_{\phi(p^e)-1} \in \mathbb{Z}.$$

We want to show that p divides each b_i.

Let $\pi = 1 - \zeta_{p^e}$. From the beginning of this writeup, p is associate to $\pi^{\phi(p^e)}$ in $\mathcal{O}_e$, i.e., $p = u\pi^{\phi(p^e)}$ for some unit $u \in \mathcal{O}_e^\times$, and also $\mathrm{N}_{K_e/\mathbb{Q}}(\pi) = p$. Thus

$$u\pi^{\phi(p^e)}\alpha = b_0 + \sum_{i=1}^{\phi(p^e)-1} b_i \pi^i, \quad b_0, \dots, b_{\phi(p^e)-1} \in \mathbb{Z},$$

and this shows that π divides b_0 in $\mathcal{O}_e$. Take norms to $\mathbb{Q}$ to see that p divides $b_0^{\phi(p^e)}$ in $\mathbb{Z}$, and because p is prime this says that p divides b_0 in $\mathbb{Z}$.

Now we have

$$\alpha = c_0 + \frac{1}{p} \sum_{i=1}^{\phi(p^e)-1} b_i \pi^i, \quad c_0, b_1, \dots, b_{\phi(p^e)-1} \in \mathbb{Z},$$

or, letting $\alpha_1 = \alpha - c_0$, an element of $\mathcal{O}_e$,

$$u\pi^{\phi(p^e)-1}\alpha_1 = b_1 + \sum_{i=2}^{\phi(p^e)-1} b_i \pi^{i-1}, \quad b_1, \dots, b_{\phi(p^e)-1} \in \mathbb{Z},$$

and this shows that π divides b_1 in $\mathcal{O}_e$, so that p divides b_1 in $\mathbb{Z}$.

And so on. This completes the proof that $\mathcal{O}_e = \mathbb{Z}[\zeta_{p^e}]$ if $\mathcal{O}_{e-1} = \mathbb{Z}[\zeta_{p^{e-1}}]$.