Math 154. Integer ring of prime-power cyclotomic field

Let $p > 0$ be a prime number, and consider the splitting field K of $X^{p^r} - 1$ over $\mathbf{Q}$ for a fixed $r \geq 1$. We saw in class that $K = \mathbf{Q}(\zeta_{p^r})$ for any primitive p^rth root of unity ζ_{p^r}, $[K : \mathbf{Q}] = \varphi(p^r) = p^{r-1}(p-1)$, and that the natural map of groups

$$\mathrm{Gal}(K/\mathbf{Q}) \to (\mathbf{Z}/p^r\mathbf{Z})^\times$$

given by sending any $g \in \mathrm{Gal}(K/\mathbf{Q})$ to the exponent m_g by which it acts on *all* p^rth roots of unity (primitive or not) – that is, $g(\zeta) = \zeta^{m_g}$ whenever $\zeta^{p^r} = 1$ – is an isomorphism of groups.

Observe that $\mathbf{Z}[\zeta_{p^r}] \subseteq \mathscr{O}_K$, and this subring already has full rank over $\mathbf{Z}$ (i.e., it is finite free of rank $p^{r-1}(p-1)$ as a $\mathbf{Z}$-module), so it is finite index in $\mathscr{O}_K$. In this handout, we aim to prove that this inclusion is an equality, and a bit more:

Theorem 0.1. *Let ζ be a primitive p^rth root of unity over $\mathbf{Q}$. The inclusion $\mathbf{Z}[\zeta] \subseteq \mathscr{O}_K$ is an equality, and $\mathrm{disc}(K)$ is a nontrivial power of p up to a sign except when $p^r = 2$ (in which case $K = \mathbf{Q}$, so the discriminant is 1). Explicitly, this discriminant is $\pm p^{p^{r-1}(r(p-1)-1)}$.*

The value of the annoying sign for the discriminant will not be relevant for us, and there are better ways to figure it out than being attentive during the calculation. So we will ignore the sign issue. But note from the explicit formula that $d = \pm 1$ precisely when $p^r = 2$ (as one sees with a bit of fiddling around depending on whether $p = 2$ or $p > 2$).

Let $n = p^{r-1}(p-1) = [K : \mathbf{Q}]$. The two-step strategy for the proof was presented in class: for $d = D(1, \zeta, \ldots, \zeta^{n-1})$ we have $\mathscr{O}_K \subseteq (1/d)\mathbf{Z}[\zeta]$, so once it is shown that d is a p-power up to a sign (we will actually compute d exactly) then it will remain to show that $\mathbf{Z}[\zeta] \cap p\mathscr{O}_K = p\mathbf{Z}[\zeta]$. This latter equality amounts to the assertion that if $z \in \mathbf{Z}[\zeta]$ and z/p is an algebraic integer then in fact $z \in p\mathbf{Z}[\zeta]$.

Let's first compute d. As we noted in class, the discriminant formula for rings generated by a single algebraic integer gives

$$d = (-1)^{n(n-1)/2}\mathrm{N}_{K/\mathbf{Q}}(f'(\zeta))$$

where $f = \Phi_{p^r} = (X^{p^r} - 1)/(X^{p^{r-1}} - 1) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 \in \mathbf{Z}[X]$ is the minimal polynomial of ζ over $\mathbf{Q}$. The description of f as a quotient is much more suitable for evaluating $f'(\zeta)$, since the quotient rule gives

$$f'(X) = \frac{(X^{p^{r-1}} - 1)p^r X^{p^r - 1} - (X^{p^r} - 1)p^{r-1}X^{p^{r-1}-1}}{(X^{p^{r-1}} - 1)^2}$$

and the second term in the numerator vanishes at ζ. Thus,

$$f'(\zeta) = \frac{(\zeta^{p^{r-1}} - 1)p^r\zeta^{p^r-1}}{(\zeta^{p^{r-1}} - 1)^2} = \frac{p^r\zeta^{-1}}{(\zeta_p - 1)}$$

where $\zeta_p := \zeta^{p^{r-1}}$ is a primitive pth root of unity.

Since we know $\mathrm{Gal}(K/\mathbf{Q})$ rather explicitly, especially how it acts on roots of unity, computing norms relative to $K/\mathbf{Q}$ will be quite tractable. Since ζ^{-1} is an integral unit, its norm into $\mathbf{Q}$ lies in $\mathbf{Z}^\times = \pm 1$, so since we are ignoring sign issues we can suppress the appearance of ζ^{-1} when computing $\mathrm{N}_{K/\mathbf{Q}}(f'(\zeta))$. Thus, we aim to prove that $\mathrm{N}_{K/\mathbf{Q}}$ applied to $p^r/(\zeta_p - 1)$ yields the asserted p-power up to a sign. Since the norm is multiplicative, and its effect on the ground field is the nth power (where n is the degree of the field extension involved), we have

$$\mathrm{N}_{K/\mathbf{Q}}(p^r/(\zeta_p - 1)) = \frac{p^{rp^{r-1}(p-1)}}{\mathrm{N}_{K/\mathbf{Q}}(\zeta_p - 1)} = \frac{p^{rp^{r-1}(p-1)}}{\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta - 1)^{p^{r-1}}},$$

where the second equality uses the transitivity relation $\mathrm{N}_{K/\mathbf{Q}} = \mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}} \circ \mathrm{N}_{K/\mathbf{Q}(\zeta_p)}$ and the fact that the effect of $\mathrm{N}_{K/\mathbf{Q}(\zeta_p)}$ on an element of $\mathbf{Q}(\zeta_p)$ is raising to the exponent $[K : \mathbf{Q}(\zeta_p)] = p^{r-1}$. Already this shows that up to a sign either d is 1 or a power of p, which is all we need for the purpose of determining the ring of integers. To complete the determination of d up to sign (and in particular, to verify that it really is not ± 1 when $p^r \neq 2$, which is to say that it is divisible by p when $K \neq \mathbf{Q}$), it remains to show that

$\mathrm{N}_{\mathbf{Q}(\zeta_p)/\mathbf{Q}}(\zeta_p - 1) = \pm p$. This is a special case of the following lemma that applies to *all* prime-power roots of unity (not just primitive pth roots of unity) and will be useful for another purpose later in the argument:

Lemma 0.2. *For any prime power p^r and the associated cyclotomic field $K = \mathbf{Q}(\zeta_{p^r})$, $\mathrm{N}_{K/\mathbf{Q}}(1 - \zeta_{p^r}) = p$.*

The order of subtraction within the norm is designed to make the right side involve no sign, regardless of whether or not $p = 2$. Note also that this lemma applies even when $p^r = 2$, in which case $K = \mathbf{Q}$ and $1 - \zeta_{p^r} = 1 - (-1) = 2$.

Proof. Let $f = \Phi_{p^r} \in \mathbf{Z}[X]$, so $f(1) = p$. Since $\mathrm{Gal}(K/\mathbf{Q}) = (\mathbf{Z}/p^r\mathbf{Z})^\times$, for $\zeta := \zeta_{p^r}$ the Galois conjugates of ζ over $\mathbf{Q}$ are precisely the powers ζ^j as j varies through $(\mathbf{Z}/p^r\mathbf{Z})^\times$. Hence, $f(X) = \prod_j (X - \zeta^j)$ and the Galois-theoretic formula for the norm gives $\mathrm{N}_{K/\mathbf{Q}}(1 - \zeta) = \prod_{j \in (\mathbf{Z}/p^r\mathbf{Z})^\times}(1 - \zeta^j) = f(1) = p$. ∎

Now we turn to the other part of the argument, which is to show that $\mathbf{Z}[\zeta] \cap p\mathscr{O}_K = p\mathbf{Z}[\zeta]$. Observe that we may use the power basis $\{(1 - \zeta)^j\}$ rather than $\{\zeta^j\}$ (corresponding to the fact that $X \mapsto 1 - X$ induces an automorphism of the ring $\mathbf{Z}[X]$, so any polynomial expression in ζ over $\mathbf{Z}$ can be rewritten as a polynomial in $1 - \zeta$, and vice-versa). This will be much more convenient for our purposes, mainly due to the preceding Lemma. It is elementary to check that the powers $(1 - \zeta)^j$ for $0 \leq j \leq n - 1$ are a $\mathbf{Z}$-basis of $\mathbf{Z}[\zeta]$ (with $n = [K : \mathbf{Q}] = p^{r-1}(p - 1)$).

Consider an element $z = \sum_{j=0}^{n-1} c_j(1 - \zeta)^j$ with $c_j \in \mathbf{Z}$, and assume $z \in p\mathscr{O}_K$. Our goal is to prove that $c_j \in p$ for all j, so then $z \in p\mathbf{Z}[\zeta]$ as desired. Since p lies in the ideal $(1 - \zeta)$ (because the Lemma above expresses p explicitly as a product of Galois conjugates of $1 - \zeta$), the inclusion $z \in p\mathscr{O}_K \subset (1 - \zeta)$ implies that $c_0 \in (1 - \zeta)$. Hence, $c_0 \in (1 - \zeta) \cap \mathbf{Z}$. This intersection is given by:

Lemma 0.3. $(1 - \zeta) \cap \mathbf{Z} = p\mathbf{Z}$.

Proof. Clearly the right side is contained in the left side. For the reverse inclusion, we have to show that if $a \in \mathbf{Z}$ is divisible by $1 - \zeta$ in $\mathscr{O}_K$ then $p|a$ in $\mathbf{Z}$. Writing $a = (1 - \zeta)\alpha$ for some $\alpha \in \mathscr{O}_K$, applying $\mathrm{N}_{K/\mathbf{Q}}$ gives

$$a^n = \mathrm{N}_{K/\mathbf{Q}}(a) = \mathrm{N}_{K/\mathbf{Q}}(1 - \zeta)\mathrm{N}_{K/\mathbf{Q}}(\alpha) = p\mathrm{N}_{K/\mathbf{Q}}(\alpha)$$

with $\mathrm{N}_{K/\mathbf{Q}}(\alpha) \in \mathbf{Z}$ (since $\alpha \in \mathscr{O}_K$). Here we have used the preceding Lemma. We conclude that in $\mathbf{Z}$, a^n is divisible by p. Since p is prime, it follows that a itself is divisible by p (in $\mathbf{Z}$). ∎

To summarize, we have shown that if $z \in p\mathscr{O}_K$ then $c_0 \in p\mathbf{Z}$. It is therefore harmless to replace z with $z - c_0$ for the purpose of proving $z \in p\mathbf{Z}[\zeta]$, and if $c_1 \in p\mathbf{Z}$ then we may similarly subtract off $c_1(1 - \zeta)$ without harm. Continuing in this way, we may assume $z = c_{i_0}(1 - \zeta)^{i_0} + \cdots + c_{n-1}(1 - \zeta)^{n-1} \in p\mathscr{O}_K$ with $i_0 \leq n - 1$ and we just have to show that $c_{i_0} \in p\mathbf{Z}$. We will prove below that p is actually an $\mathscr{O}_K^\times$-multiple of $(1-\zeta)^n$ in $\mathscr{O}_K$, so $p\mathscr{O}_K = (1-\zeta)^n\mathscr{O}_K$ and hence the hypothesis $z \in p\mathscr{O}_K$ implies $c_{i_0}(1-\zeta)^{i_0} \in (1-\zeta)^{i_0+1}\mathscr{O}_K$ (since the "higher order" terms $c_j(1 - \zeta)^j$ for $i_0 < j \leq n - 1$ all lie in $(1 - \zeta)^{i_0+1}\mathscr{O}_K$). But then dividing out by $(1 - \zeta)^{i_0}$ gives $c_{i_0} \in (1 - \zeta)\mathscr{O}_K \cap \mathbf{Z}$, and we have seen above that this intersection is exactly $p\mathbf{Z}$ (so $c_{i_0} \in p\mathbf{Z}$ and we can continue as desired).

It now remains to prove that $p\mathscr{O}_K = (1 - \zeta)^n\mathscr{O}_K$. Since $p = \mathrm{N}_{K/\mathbf{Q}}(1 - \zeta) = \prod_j(1 - \zeta^j)$ as j runs through the group $(\mathbf{Z}/p^r\mathbf{Z})^\times$ of size $[K : \mathbf{Q}] = n$, it suffices to show that the Galois conjugates $1 - \zeta^j$ are all $\mathscr{O}_K^\times$-multiples of $1 - \zeta$. This is recorded as our final lemma:

Lemma 0.4. *For all $j \in (\mathbf{Z}/p^r\mathbf{Z})^\times$, $(1 - \zeta^j)/(1 - \zeta) \in \mathscr{O}_K^\times$.*

Proof. Fix a representative for j in $\mathbf{Z}^+$. Since $(1 - Y^j)/(1 - Y) \in \mathbf{Z}[Y]$, clearly the ratio $(1 - \zeta^j)/(1 - \zeta)$ lies in $\mathbf{Z}[\zeta] \subseteq \mathscr{O}_K$. It remains to show that the reciprocal $(1 - \zeta)/(1 - \zeta^j) \in \mathbf{Q}(\zeta) = K$ also lies in $\mathbf{Z}[\zeta]$. The action of $\mathrm{Gal}(K/\mathbf{Q})$ on K carries $\mathbf{Z}[\zeta]$ isomorphically onto itself, so it is sufficient to find some $g \in \mathrm{Gal}(K/\mathbf{Q}) = (\mathbf{Z}/p^r\mathbf{Z})^\times$ such that applying g to this ratio gives a result in $\mathbf{Z}[\zeta]$. Take g to be the class of j^{-1} mod p^r. That is, consider the residue class modulo p^r of a positive integer k that satisfies $kj \equiv 1$ mod p^r. This carries the ratio of interest to $(1 - \zeta^k)/(1 - \zeta)$ (!), which is visibly in $\mathbf{Z}[\zeta]$. ∎