CYCLOTOMIC INTEGER RINGS, IN GENERAL

Our previous writeup showed, by fairly elementary means, that the cyclotomic field $\mathbb{Q}(\zeta_{p^e})$ has integer ring $\mathbb{Z}[p^e]$ for every prime power p^e. This writeup builds on that result to show, now using the discriminant, that $\mathbb{Q}(\zeta_n)$ has integer ring $\mathbb{Z}[\zeta_n]$ for every positive integer n. Section 1 gives some basic facts about discriminants. Section 2 notes that if two positive integers n and m are coprime then so are the discriminants of the nth and mth cyclotomic polynomials. A slightly general argument in section 3 specializes to two results that bound the denominators occurring in integer rings. Section 4 completes the argument that the cyclotomic integer ring is as claimed, although we make one invocation. The optional section 5 continues on to compute the discriminant of the nth cyclotomic polynomial for any n, even though doing so is unnecessary for this writeup's main result.

Contents

1. Discriminants: some basic facts

Let F be a number field, meaning an extension field of $\mathbb{Q}$ having finite degree $d = [F : \mathbb{Q}]$, this degree being the dimension of F as a vector space over $\mathbb{Q}$. There exist d field embeddings $\sigma_1, \dots, \sigma_d$ of F into the complex number field $\mathbb{C}$. For some nonnegative integers r and s such that $r + 2s = d$, r of these embeddings take F into $\mathbb{R}$, and the remaining $2s$ embeddings are s complex conjugate pairs that take F to nonreal subfields of $\mathbb{C}$.

Consider a vector $\vec{\alpha} = (\alpha_1, \dots, \alpha_d)$ with each α_j in F. Its *discriminant* is

$$\mathrm{disc}(\vec{\alpha}) = (\det[\sigma_i(\alpha_j)])^2 \qquad \text{where } [\sigma_i(\alpha_j)] = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_d) \\ \vdots & \ddots & \vdots \\ \sigma_d(\alpha_1) & \cdots & \sigma_d(\alpha_d) \end{bmatrix}.$$

Each complex conjugate pair $\vec{x} + i\vec{y}, \vec{x} - i\vec{y}$ of rows in the matrix of the previous display linearly recombines to give the rows $2\vec{x}, i\vec{y}$. Thus the squared determinant $\mathrm{disc}(\vec{\alpha})$ is real with sign $(-1)^s$.

Let $\alpha \in K$ be a generator, meaning that $K = \mathbb{Q}(\alpha)$. Let $\vec{\alpha} = (1, \alpha, \alpha^2, \dots, \alpha^{d-1})$. Define $\alpha_i = \sigma_i(\alpha)$ for $i = 1, \dots, d$ and compute that because each σ_i is a ring homomorphism,

$$\mathrm{disc}(\vec{\alpha}) = (\det[\sigma_i(\alpha^{j-1})])^2 = (\det[\sigma_i(\alpha)^{j-1}])^2 = (\det[\alpha_i^{j-1}])^2.$$

Here we have a Vandermonde determinant $(-1)^{\lfloor d/2\rfloor}\det[\alpha_i^{j-1}] = \prod_{i<j}(\alpha_i-\alpha_j)$, such as

$$-\det\begin{bmatrix}1 & a & a^2\\ 1 & b & b^2\\ 1 & c & c^2\end{bmatrix} = (a-b)(a-c)(b-c).$$

Thus

$$\operatorname{disc}(1,\alpha,\alpha^2,\dots,\alpha^{d-1}) = \prod_{i<j}(\alpha_i-\alpha_j)^2, \qquad \alpha_i=\sigma_i(\alpha) \text{ for all } i.$$

This product of squares of differences is also by definition the polynomial discriminant of the minimal polynomial $f_\alpha(x)=\prod_{i=1}^d(x-\alpha_i)$ of α, and so

$$\operatorname{disc}(1,\alpha,\alpha^2,\dots,\alpha^{d-1}) = \operatorname{disc}(f_\alpha).$$

We review the fact that the discriminant of a monic polynomial is, up to sign, the product of the polynomial's derivative-values at its roots. Indeed, for any polynomial

$$f(X)=\prod_j(X-\alpha_j)$$

we have

$$f'(X)=\sum_k\prod_{j\neq k}(X-\alpha_j),$$

so that $f'(\alpha_i)=\prod_{j\neq i}(\alpha_i-\alpha_j)$ and then

$$\prod_i f'(\alpha_i) = \prod_{i,j:i\neq j}(\alpha_i-\alpha_j).$$

So with $d=\deg(f)$, noting that $\binom{d}{2}$ and $\lfloor d/2\rfloor$ have the same parity,

$$\prod_i f'(\alpha_i) = (-1)^{\lfloor d/2\rfloor}\operatorname{disc}(f).$$

For degree $d=1$, the product and the discriminant are both 1 and the exponent of -1 is 0. Although the formula in the previous display is not immediately useful numerically unless we know the roots of f, it is useful theoretically and also we will indeed know the roots of the polynomials in this writeup, these being X^n-1 with roots ζ_n^i for $i\in\mathbb{Z}/n\mathbb{Z}$ and the cyclotomic polynomials $\Phi_n(X)$ with roots ζ_n^i for $i\in(\mathbb{Z}/n\mathbb{Z})^\times$.

Now we show:

If $f(X)\mid g(X)$ *in* $\mathbb{Z}[X]$ *then* $\operatorname{disc}(f)\mid\operatorname{disc}(g)$ *in* $\mathbb{Z}$.

Indeed, the assumed divisibility is

$$g(X)=f(X)h(X) \quad \text{for some } h(X)\in\mathbb{Z}[X],$$

from which

$$g'(X)=f'(X)h(X)+f(X)h'(X).$$

Thus for any root α of f,

$$g'(\alpha)=f'(\alpha)h(\alpha),$$

and multiplying over all such roots gives, with $d=\deg(f)$,

$$\prod_\alpha g'(\alpha) = (-1)^{\lfloor d/2\rfloor}\operatorname{disc}(f)\cdot\prod_\alpha h(\alpha).$$

Both products lie in the ring of integers of the splitting field of f over $\mathbb{Q}$, and also they are invariant under the Galois group, so they lie in $\mathbb{Q}$; that is, they lie in $\mathbb{Z}$. Because $\mathrm{disc}(g)$ is a multiple of $\prod_\alpha g'(\alpha)$ in $\mathbb{Z}$ (recall that this product is taken over the roots of f, a subset of the roots of g), this gives the result.

Returning to our number field F, suppose that we have vectors $\vec{\alpha}$ and $\vec{\beta} = M\vec{\alpha}$ where $M \in \mathbb{Q}^{d\times d}$; for this equality we treat the vectors as columns. Compute

$$[\sigma_i(\vec{\beta})] = [\sigma_i(M\vec{\alpha})] = [M\sigma_i(\vec{\alpha})] = M[\sigma_i(\vec{\alpha})],$$

and so

$$\mathrm{disc}(\vec{\beta}) = (\det[\sigma_i(\vec{\beta})])^2 = (\det M[\sigma_i(\vec{\alpha})])^2 = (\det M)^2\,\mathrm{disc}(\vec{\alpha}).$$

The relation $\mathrm{disc}(\vec{\beta}) = (\det M)^2\,\mathrm{disc}(\vec{\alpha})$ has two quick consequences:

- If $\vec{\alpha}$ and $\vec{\beta}$ are $\mathbb{Z}$-bases of the integer ring $\mathcal{O}_F$ then the matrix M has entries in $\mathbb{Z}$ and determinant ± 1, and so $\mathrm{disc}(\vec{\beta}) = \mathrm{disc}(\vec{\alpha})$. The common value of $\mathrm{disc}(\vec{\alpha})$ for all $\mathbb{Z}$-bases $\vec{\alpha}$ of $\mathcal{O}_F$ is the *field discriminant* of F, written $\mathrm{disc}(F)$.
- If $\vec{\alpha}$ is a basis of $\mathcal{O}_F$ and $\vec{\beta} = (1, \beta, \beta^2, \ldots, \beta^{d-1})$ where $F = \mathbb{Q}(\beta)$ and $\beta \in \mathcal{O}_F$ then the matrix M has entries in $\mathbb{Z}$ and nonzero determinant, so the discriminant $\mathrm{disc}(\vec{\beta}) = \mathrm{disc}(f_\beta)$ is a nonzero square multiple of $\mathrm{disc}(\vec{\alpha})$ in $\mathbb{Z}$. Thus any prime that divides $\mathrm{disc}(f_\beta)$ once also divides $\mathrm{disc}(F)$ once, and any prime that divides $\mathrm{disc}(f_\beta)$ an odd number of times also divides $\mathrm{disc}(F)$ an odd number of times though possibly fewer. Computing $\mathrm{disc}(f_\beta)$ for various β can narrow down the possible values of $\mathrm{disc}(F)$ or even determine it.

2. Cyclotomic coprimality result

For any positive integer n, let $\Phi_n(X)$ denote the nth cyclotomic polynomial. The divisibility $\Phi_n(X) \mid X^n - 1$ in $\mathbb{Z}[X]$ says that $\mathrm{disc}(\Phi_n) \mid \mathrm{disc}(X^n - 1)$ in $\mathbb{Z}$, and by the product formula from the previous section, the latter discriminant is

$$\mathrm{disc}(X^n - 1) = (-1)^{\lfloor n/2\rfloor} \prod_{i=0}^{n-1} n\zeta_n^{(n-1)i} = (-1)^{\lfloor n/2\rfloor} n^n \prod_{i=0}^{n-1} \zeta_n^i = -(-1)^{\lfloor (n+1)/2\rfloor} n^n.$$

Although the sign of this discriminant doesn't particularly matter to us, we may note that it is 1 if $n = 1, 2 \bmod 4$, and -1 if $n = 3, 4 \bmod 4$. Because $\mathrm{disc}(\Phi_n)$ divides a power of n, we have the following result:

For positive integers n and m with $\gcd(n, m) = 1$, also $\gcd(\mathrm{disc}(\Phi_n), \mathrm{disc}(\Phi_m)) = 1$.

We will use this result later in this writeup.

3. Two results on integer rings and discriminants

Consider two number fields, of degrees n and m,

$$F = \mathbb{Q}(\vec{\alpha}) \quad \text{where } \vec{\alpha} = (\alpha_1, \ldots, \alpha_n),\text{ each } \alpha_j \in \mathcal{O}_F$$
$$K = \mathbb{Q}(\vec{\beta}) \quad \text{where } \vec{\beta} = (\beta_1, \ldots, \beta_m),\text{ each } \beta_k \in \mathcal{O}_K.$$

Suppose further that

$$F \cap K = \mathbb{Q},$$

and introduce the composite field

$$L = FK = \mathbb{Q}(\vec{\alpha}, \vec{\beta}).$$

Every element γ of $\mathcal{O}_L$ takes the form

$$\begin{aligned}\gamma &= \sum_{j,k} \alpha_j \beta_k x_{jk} \quad \text{with all } x_{jk} \in \mathbb{Q} \\ &= \sum_j \alpha_j \kappa_j \qquad\quad \text{where } \kappa_j = \sum_k \beta_k x_{jk} \in K \text{ for each } j.\end{aligned}$$

Let $\sigma_1, \dots, \sigma_n$ denote the embeddings of F in $\mathbb{C}$, extended trivially on K to L; here we are using the condition $F \cap K = \mathbb{Q}$. We have a linear system

$$\begin{bmatrix} \sigma_1\gamma \\ \vdots \\ \sigma_n\gamma \end{bmatrix} = \begin{bmatrix} \sigma_1\alpha_1 & \dots & \sigma_1\alpha_n \\ \vdots & \ddots & \vdots \\ \sigma_n\alpha_1 & \dots & \sigma_n\alpha_n \end{bmatrix} \begin{bmatrix} \kappa_1 \\ \vdots \\ \kappa_n \end{bmatrix},$$

or, more concisely,

$$\vec{\sigma}\gamma = A\vec{\kappa}.$$

Here $(\det A)^2 = \mathrm{disc}(\vec{\alpha})$. Multiply through from the left by $\mathrm{disc}(\vec{\alpha})^{-1}\det(A)A^{\mathrm{adj}} = A^{-1}$, where *adj* denotes the classical adjoint, to get

$$\mathrm{disc}(\vec{\alpha})^{-1}\det(A)A^{\mathrm{adj}}\vec{\sigma}\gamma = \vec{\kappa}.$$

This equality of vectors shows that each κ_j lies in $\mathrm{disc}(\vec{\alpha})^{-1}\overline{\mathbb{Z}} \cap K = \mathrm{disc}(\vec{\alpha})^{-1}\mathcal{O}_K$.

For one consequence of this reasoning, specialize to $K = \mathbb{Q}$, so that $\vec{\beta} = 1$ and $\kappa_j = x_j$ for all j with no reason for a k-index, and make no assumption that $\vec{\alpha}$ is a $\mathbb{Z}$-basis of the entire integer ring $\mathcal{O}_F$. Certainly $\mathbb{Z}[\vec{\alpha}] \subset \mathcal{O}_F$, but also the work has shown that each x_j lies in $\mathrm{disc}(\vec{\alpha})^{-1}\mathbb{Z}$, giving an outer containment of $\mathcal{O}_F$ as well,

$$\boxed{\mathcal{O}_F \subset \mathrm{disc}(\vec{\alpha})^{-1}\mathbb{Z}[\vec{\alpha}].}$$

For a second consequence, drop the specialization of K, but now assume that $\mathcal{O}_F = \mathbb{Z}[\vec{\alpha}]$ and $\mathcal{O}_K = \mathbb{Z}[\vec{\beta}]$. Each $\kappa_j = \sum_k \beta_k x_{jk}$ of $\vec{\kappa}$ lies in $\mathrm{disc}(\vec{\alpha})^{-1}\mathbb{Z}[\vec{\beta}]$, and so $\{x_{jk}\} \subset \mathrm{disc}(\vec{\alpha})^{-1}\mathbb{Z}$. Symmetrically $\{x_{jk}\} \subset \mathrm{disc}(\vec{\beta})^{-1}\mathbb{Z}$, and so, because $\gamma = \sum_{j,k} \alpha_j\beta_k x_{jk}$ is an arbitrary element of $\mathcal{O}_L$, we have shown the containment

$$\boxed{\mathcal{O}_L \subset \gcd(\mathrm{disc}(\vec{\alpha}), \mathrm{disc}(\vec{\beta}))^{-1}\mathbb{Z}[\vec{\alpha}, \vec{\beta}] \quad \text{if } \mathcal{O}_F = \mathbb{Z}[\vec{\alpha}] \text{ and } \mathcal{O}_K = \mathbb{Z}[\vec{\beta}].}$$

In particular, if $\mathcal{O}_F = \mathbb{Z}[\vec{\alpha}]$ and $\mathcal{O}_K = \mathbb{Z}[\vec{\beta}]$ and $\gcd(\mathrm{disc}(\vec{\alpha}), \mathrm{disc}(\vec{\beta})) = 1$ then $\mathcal{O}_L = \mathbb{Z}[\vec{\alpha}, \vec{\beta}]$.

4. $\mathbb{Q}(\zeta_n)$ has integer ring $\mathbb{Z}[\zeta_n]$

Recall that we have established that for positive n and m with $\gcd(n, m) = 1$, also $\gcd(\mathrm{disc}(\Phi_n), \mathrm{disc}(\Phi_m)) = 1$. For such n and m set

$$F = \mathbb{Q}(\zeta_n) \qquad K = \mathbb{Q}(\zeta_m),$$

and suppose that $\mathcal{O}_F = \mathbb{Z}[\zeta_n]$ and $\mathcal{O}_K = \mathbb{Z}[\zeta_m]$. We have $\zeta_n = \zeta_{nm}^m$ and $\zeta_m = \zeta_{nm}^n$, and because $Nn + Mm = 1$ for some N and M also $\zeta_{mn} = \zeta_{mn}^{Nn+Mm} = \zeta_m^N\zeta_n^M$, so

$$\mathbb{Z}[\zeta_n, \zeta_m] = \mathbb{Z}[\zeta_{nm}].$$

By results beyond the limited scope of this writeup, the intersection $F \cap K$ is $\mathbb{Q}$. (A formula for field discriminants shows that $\mathrm{disc}(F \cap K)$ divides $\mathrm{disc}(F)$ and $\mathrm{disc}(K)$, which divide n^n and m^m, so that $\mathrm{disc}(F \cap K) = 1$, and then it is a fact of algebraic number theory that this gives $F \cap K = \mathbb{Q}$.) And the composite field $L = FK = \mathbb{Q}(\zeta_n, \zeta_m)$ is $L = \mathbb{Q}(\zeta_{nm})$. Because $\mathrm{disc}(F)$ and $\mathrm{disc}(K)$ are coprime, the last sentence of the previous section of this writeup and the previous display together say that

$$\mathcal{O}_L = \mathbb{Z}[\zeta_{nm}].$$

Because we know that the integer ring of $\mathbb{Q}(\zeta_n)$ is indeed $\mathbb{Z}[\zeta_n]$ when n is a prime power, the work here extends the result to all positive integers n.

5. Cyclotomic polynomial discriminant

This section is optional. We compute the discriminant of the nth cyclotomic polynomial $\Phi_n(X)$ for the reader who wants to see it as a matter of practice, even though this computation is not necessary for this writeup's main goal of proving that the nth cyclotomic field $\mathbb{Q}(\zeta_n)$ has integer ring $\mathbb{Z}[\zeta_n]$. With this fact proved, we know that $\mathrm{disc}(\Phi_n) = \mathrm{disc}(\mathbb{Q}(\zeta_n))$. Because $\mathbb{Q}(\zeta_n)$ has no complex embeddings for $n = 1, 2$ and $\phi(n)$ complex embeddings for $n \geq 3$, and this number of complex embeddings is $2s = 2\lfloor \phi(n)/2 \rfloor$ in all cases, the sign of $\mathrm{disc}(\Phi_n)$ is $(-1)^{\lfloor \phi(n)/2 \rfloor}$. If n is a prime p then this sign is

$$\mathrm{sgn}(\mathrm{disc}(\Phi_p)) = \begin{cases} 1 & \text{if } p = 2 \text{ or } p = 1 \bmod 4 \\ -1 & \text{if } p = 3 \bmod 4. \end{cases}$$

If n is a prime power p^e then it is

$$\mathrm{sgn}(\mathrm{disc}(\Phi_{p^e})) = \begin{cases} 1 & \text{if } p^e = 2^e \text{ with } e \neq 2 \text{ or if } p = 1 \bmod 4 \\ -1 & \text{if } p^e = 4 \text{ or if } p = 3 \bmod 4. \end{cases}$$

Because ϕ is multiplicative, $\mathrm{sgn}(\mathrm{disc}(\Phi_n))$ in general is 1 when some 2^e with $e \neq 2$ exactly divides n or if $p \mid n$ for some $p = 1 \bmod 4$. Thus we need only to compute the absolute value of $\mathrm{disc}(\Phi_n)$. The sign of $\mathrm{disc}(\Phi_n)$ can be computed directly, without using the fact that $\mathrm{disc}(\Phi_n) = \mathrm{disc}(\mathbb{Q}(\zeta_n))$, but doing so makes the calculation more cluttered and so we omit it.

The prime power cyclotomic polynomial is

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

Thus $(X^{p^{e-1}} - 1)\Phi_{p^e}(X) = X^{p^e} - 1$, and then differentiating gives

$$(X^{p^{e-1}} - 1)\Phi'_{p^e}(X) + p^{e-1}X^{p^{e-1}-1}\Phi_{p^e}(X) = p^e X^{p^e-1}.$$

Substitute $X = \zeta_{p^e}^i$ for any $i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ to get $(\zeta_{p^e}^{ip^{e-1}} - 1)\Phi'_{p^e}(\zeta_{p^e}^i) = p^e \zeta_{p^e}^{i(p^e-1)}$, or

$$(\zeta_p^i - 1)\Phi'_{p^e}(\zeta_{p^e}^i) = p^e \zeta_{p^e}^{-i}.$$

Multiply over all $i \in (\mathbb{Z}/p^e\mathbb{Z})^\times$,

$$\pm \prod_{i \in (\mathbb{Z}/p^e\mathbb{Z})^\times} (\zeta_p^i - 1) \cdot \mathrm{disc}(\Phi_{p^e}) = p^{e\phi(p^e)} \prod_{i \in (\mathbb{Z}/p^e\mathbb{Z})^\times} \zeta_{p^e}^i.$$

If $p^e = 2$ then the last product is -1, otherwise its terms cancel pairwise to give 1. Thus we have

$$\pm \prod_{i \in (\mathbb{Z}/p^e\mathbb{Z})^\times} (1 - \zeta_p^i) \cdot \mathrm{disc}(\Phi_{p^e}) = p^{e\phi(p^e)},$$

which is to say, noting that the product is $\Phi_p(1)^{p^{e-1}}$ because the natural surjection $(\mathbb{Z}/p^e\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ has degree $\phi(p^e)/\phi(p) = p^{e-1}$,

$$\mathrm{disc}(\Phi_{p^e}) = \pm p^{(e(p-1)-1)p^{e-1})}.$$

As above, the sign is $(-1)^{\lfloor \phi(p^e)/2 \rfloor}$. That is,

$$\boxed{\mathrm{disc}(\Phi_{p^e}) = (-1)^{\lfloor \phi(p^e)/2 \rfloor} (p^e)^{\phi(p^e)} / p^{\phi(p^e)/(p-1)}.}$$

Especially $\mathrm{disc}(\Phi_p)$ is a proper divisor of $\mathrm{disc}(X^p - 1) = -(-1)^{\binom{p+1}{2}} p^p$ from above,

$$\boxed{\mathrm{disc}(\Phi_p) = (-1)^{\lfloor (p-1)/2 \rfloor} p^{p-2}.}$$

Now consider the case that n is divisible by at least two primes. First we show:

If $n = \prod_{i=1}^g p_i^{e_i}$ ($g \geq 2$, each $e_i \geq 1$) then $\prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} (1 - \zeta_n^j) = 1$.

Indeed, for every positive integer m the polynomial equality $\prod_{j=1}^{m-1}(X - \zeta_m^j) = \sum_{i=1}^{m-1} X^i$ gives for $X = 1$ the relation $\prod_{j=1}^{m-1}(1 - \zeta_m^j) = m$. Especially, this holds for $m = n$ and for $m = p_i^{e_i}$,

$$\prod_{j=1}^{n-1}(1 - \zeta_n^j) = n, \qquad \prod_{j=1}^{p_i^{e_i}-1}(1 - \zeta_{p_i^{e_i}}^j) = p_i^{e_i}.$$

If $j \in \{1, \dots, n-1\}$ takes the form $j = j'n/p_i^{e_i}$, $j' \in \{1, \dots, p_i^{e_i} - 1\}$, then $\zeta_n^j = \zeta_{p_i^{e_i}}^{j'}$ and i is unique to j. So the product $\prod_{j=1}^{n-1}(1 - \zeta_n^j)$ is a multiple of the product $\prod_{i=1}^g \prod_{j'=1}^{n/p_i^{e_i}-1}(1 - \zeta_{p_i^{e_i}}^{j'})$, and both of these products equal n. This says that with

$$S = \{j \in \{1, \dots, n-1\} \text{ not of the form } j'n/p_i^{e_i} \text{ for any } j' \text{ and } i\},$$

we have $\prod_{j \in S}(1 - \zeta_n^j) = 1$. The set S contains all values $j \in \{1, \dots, n-1\}$ coprime to n, because n and $j'n/p_i^{e_i}$ share at least the factor $\prod_{k \neq i} p_k^{e_k}$; here we use the condition that n is not a prime power. This shows that the rational integer $\prod_{(j,n)=1}(1 - \zeta_n^j)$, which divides 1 in $\mathbb{Z}[\zeta_n]$ and therefore in $\mathbb{Z}$, is ± 1. Finally, it is 1 because it consists of products of pairs of complex conjugate terms $1 - \zeta_n^j$ and $1 - \zeta_n^{-j}$, and each such product is positive.

Now we can compute the discriminant of $\Phi_n(X)$. The relation

$$\Phi_n(X) = \frac{(X^n - 1) \prod_{p,q|n}(X^{n/pq} - 1) \cdots}{\prod_{p|n}(X^{n/p} - 1) \prod_{p,q,r|n}(X^{n/pqr} - 1) \cdots}$$

differentiates at $X = \zeta_n$ to (noting that $\zeta_n^{n/d} = \zeta_d$)

$$\Phi_n'(\zeta_n) = \frac{n\zeta_n^{-1} \prod_{p,q|n}(\zeta_{pq} - 1) \cdots}{\prod_{p|n}(\zeta_p - 1) \prod_{p,q,r|n}(\zeta_{pqr} - 1) \cdots}.$$

The same calculation holds with ζ_n replaced by ζ_n^i for each $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. Multiply the equalities together, recalling that $\prod_{i\in(\mathbb{Z}/p\mathbb{Z})^\times}(1-\zeta_p^i) = p$ while if at least two primes divide d then $\prod_{i\in(\mathbb{Z}/d\mathbb{Z})^\times}(1-\zeta_d^i) = 1$,

$$\boxed{\operatorname{disc}(\Phi_n) = (-1)^{\lfloor\phi(n)/2\rfloor} n^{\phi(n)} / \prod_{p|n} p^{\phi(n)/(p-1)}.}$$