

- 1.
- 2.
3. a) We first show that L_1L_2/K is a Galois extension. To this end, we note that $L_1L_2 = K(L_1 \cup L_2)$. Let $\ell \in L_i$. As was discussed in class, the K -vector space, L_1L_2 decomposes as a direct sum of $d_i = [L_1L_2 : L_i]$ subspaces $\{V_j : 1 \leq j \leq d_i\}$ which are invariant under $[\times \ell]_{L_1L_2/K}$ and admitting K -linear isomorphisms $\varphi : L_i \rightarrow V_j$ such that

$$\begin{array}{ccc} L_i & \xrightarrow{\varphi_i} & V_i \\ [\times \ell]_{L_i/K} \downarrow & & \downarrow [\times \ell]_{L_1L_2/K|V_i} \\ L_i & \xrightarrow{\varphi_i} & V_i \end{array}$$

commutes. It follows that, since L_i/K is Galois, $[\times \ell]_{L_1L_2/K}$ is diagonalizable over $L_i \subseteq L_1L_2$ for each $\ell \in L_i$. Since any collection of commuting diagonalizable maps is simultaneously diagonalizable, it follows that the K -algebra generated by $\{[\times \ell] : \ell \in L_1 \cup L_2\}$ is diagonalizable over L_1L_2 and, since $L_1L_2 = K(L_1 \cup L_2)$, this shows that $[\times x]_{L_1L_2/K}$ is diagonalizable over L_1L_2 for every $x \in L_1L_2$, i.e., L_1L_2/K is Galois.

- b) We first show that for any $\sigma \in \text{Gal}(L_1L_2/K)$ we have that $\sigma|_{L_i} \in \text{Gal}(L_i/K)$. Note that $\sigma|_{L_i} \in \text{Hom}_K(L_i, \overline{K})$. Since, by assumption, $\text{Hom}_K(L_i, \overline{K}) = \text{Hom}_K(L_i, L_i)$, i.e., since L_i/K is Galois, it follows that $\sigma|_{L_i} \in \text{Gal}(L_i/K)$. We skip the formal proof that the restriction map is a homomorphism. It follows that Ψ is a homomorphism of groups.

In order to see that Ψ is injective, suppose that $\sigma \in \text{Gal}(L_1L_2/K)$ satisfies $\sigma|_{L_i} = \text{id}_{L_i}$ for both $i = 1$ and $i = 2$. In particular, σ restricts to the identity on $L_1 \cup L_2$. Since $L_1L_2 = K(L_1 \cup L_2)$, σ is trivial.

- c) Recall that by the tower property of Galois extensions, L_2/K being Galois implies that in the sequence $L_1 \cap L_2/K$, $L_2/L_1 \cap L_2$ the latter is Galois. In particular, since $\text{Hom}_{L_2 \cap L_1}(L_2, \overline{K}) = \text{Hom}_{L_2 \cap L_1}(L_2, L_2)$ and since any L_1 -linear embedding of L_1L_2 in $\overline{K}$ restricts to a $L_1 \cap L_2$ -linear embedding of L_2 in $\overline{K}$, it follows that $\sigma(L_2) \subseteq L_2$ for any $\sigma \in \text{Gal}(L_1L_2/L_1)$.

Φ is injective: Let $\sigma \in \ker(\Phi)$. In other words, σ fixes L_2 . However, since $\sigma \in \text{Gal}(L_1L_2/L_1)$, we also know that σ fixes L_1 . Thus it must be the identity map on L_1L_2 .

Φ is surjective: By the fundamental theorem of Galois theory, we know that

$$(L_1L_2)^{\text{Gal}(L_1L_2/L_1)} = L_1.$$

Moreover, we know that for $H < \text{Gal}(L_2/L_2 \cap L_1)$ we have

$$L_2^H = L_2 \cap L_1 \iff H = \text{Gal}(L_2/L_2 \cap L_1).$$

Hence it suffices to show that $L_2^{\text{im}(\Phi)} = L_1 \cap L_2$. If $x \in L_1 \cap L_2$ and $\sigma \in \text{Gal}(L_1L_2/L_1)$, then $\sigma(x) = x$ by definition and, hence, $L_1 \cap L_2 \subseteq L_2^{\text{im}(\Phi)}$. For

the opposite inclusion, note that

$$L_2^{\text{im}(\Phi)} \subseteq (L_1 L_2)^{\text{Gal}(L_1 L_2 / L_1)} \cap L_2 = L_1 \cap L_2.$$

d) We only need to show surjectivity of Ψ . So, let

$$(\sigma_1, \sigma_2) \in \text{Gal}(L_1/K) \times \text{Gal}(L_2/K).$$

By 3c we know there exists $\tilde{\sigma}_1 \in \text{Gal}(L_1 L_2 / L_2)$ such that $\tilde{\sigma}_1|_{L_1} = \sigma_1$, and there exists $\tilde{\sigma}_2 \in \text{Gal}(L_1 L_2 / L_1)$ such that $\tilde{\sigma}_2|_{L_2} = \sigma_2$. Define $\sigma = \tilde{\sigma}_1 \circ \tilde{\sigma}_2$. Then σ is $K = L_1 \cap L_2$ -linear and, hence, $\sigma \in \text{Gal}(L_1 L_2 / K)$. It remains to show that $\sigma|_{L_i} = \sigma_i$.

Let $x \in L_1$, then $\tilde{\sigma}_2(x) = x$ since $\tilde{\sigma}_2 \in \text{Gal}(L_1 L_2 / L_1)$. Hence

$$\sigma(x) = \tilde{\sigma}_1(\tilde{\sigma}_2(x)) = \tilde{\sigma}_1(x) = \sigma_1(x).$$

Let now $x \in L_2$, then $\tilde{\sigma}_2(x) = \sigma_2(x) \in L_2$ and, using $\tilde{\sigma}_1 \in \text{Gal}(L_1 L_2 / L_2)$,

$$\sigma(x) = \tilde{\sigma}_1(\tilde{\sigma}_2(x)) = \tilde{\sigma}_2(x) = \sigma_2(x).$$

In particular, $\sigma|_{L_i} = \sigma_i$ as desired.

4. a) Using Exercise 3 and $L_1 \cap L_2 = K$, we have

$$[L_1 L_2 : \mathbb{Q}] = |\text{Gal}(L_1 L_2 / \mathbb{Q})| = |\text{Gal}(L_1 / \mathbb{Q})| \cdot |\text{Gal}(L_2 / \mathbb{Q})| = n_1 n_2.$$

In particular, $L_1 L_2$ is a number field.

By Exercise 3 we can describe the Galois group $\text{Gal}(L_1 L_2 / \mathbb{Q})$ rather explicitly in terms of $\text{Gal}(L_1 L_2 / L_2)$ and $\text{Gal}(L_1 L_2 / L_1)$. Namely, if we write

$$\text{Gal}(L_1 L_2 / L_2) = \{\sigma_1^{(1)}, \dots, \sigma_{n_1}^{(1)}\},$$

$$\text{Gal}(L_1 L_2 / L_1) = \{\sigma_1^{(2)}, \dots, \sigma_{n_2}^{(2)}\},$$

then the Galois group of $L_1 L_2 / \mathbb{Q}$ is given by

$$\text{Gal}(L_1 L_2 / \mathbb{Q}) = \{\sigma_{j_1}^{(1)} \circ \sigma_{j_2}^{(2)} : 1 \leq j_i \leq n_i\}.$$

Furthermore, note that the Galois groups of $L_1 / \mathbb{Q}$ and $L_2 / \mathbb{Q}$ are then given by

$$\text{Gal}(L_1 / \mathbb{Q}) = \{\sigma_1^{(1)}|_{L_1}, \dots, \sigma_{n_1}^{(1)}|_{L_1}\},$$

$$\text{Gal}(L_2 / \mathbb{Q}) = \{\sigma_1^{(2)}|_{L_2}, \dots, \sigma_{n_2}^{(2)}|_{L_2}\}.$$

We will use this notation through this exercise.

b) We start by observing that

$$d_2 = (\det T_2)^2 \quad \text{with} \quad T_2 = \begin{pmatrix} \sigma_1^{(2)}(z_1^{(2)}) & \cdots & \sigma_{n_2}^{(2)}(z_1^{(2)}) \\ \vdots & \ddots & \vdots \\ \sigma_1^{(2)}(z_{n_2}^{(2)}) & \cdots & \sigma_{n_2}^{(2)}(z_{n_2}^{(2)}) \end{pmatrix}.$$

Note that $T_2 \in \mathcal{O}_2^{n_2 \times n_2}$ since $L_2 / \mathbb{Q}$ is Galois by assumption. Now set

$$\alpha = \beta_1 z_1^{(2)} + \dots + \beta_{n_2} z_{n_2}^{(2)},$$

and note that we have the relation

$$(\sigma_1^{(2)}(\alpha), \dots, \sigma_{n_2}^{(2)}(\alpha)) = (\beta_1, \dots, \beta_{n_2}) T_2$$

as claimed in the hint. The inverse of T_2 can be described explicitly, e.g., by use of Cramer's rule, as

$$T_2^{-1} = \frac{1}{\det T_2} \text{adj}(T_2),$$

where $\text{adj}(T_2)$ is the adjugate of T_2 , which leads to the relation

$$(d_2\beta_1, \dots, d_2\beta_{n_2}) = \det(T_2)(\sigma_1^{(2)}(\alpha), \dots, \sigma_{n_2}^{(2)}(\alpha)) \text{adj}(T_2).$$

Since all the entries of T_2 are contained in $\mathcal{O}_2$, the same must be true for $\text{adj}(T_2)$, whose entries are polynomials in the entries of T_2 . Similarly, since $\alpha \in \mathcal{O}_{L_1L_2}$ and since $L_1L_2/\mathbb{Q}$ is Galois, we have that $\sigma_1^{(2)}(\alpha), \dots, \sigma_{n_2}^{(2)}(\alpha) \in \mathcal{O}_{L_1L_2}$. Thus it follows that

$$d_2\beta_1, \dots, d_2\beta_{n_2} \in L_1 \cap \mathcal{O}_{L_1L_2} = \mathcal{O}_{L_1},$$

which is exactly what we wanted to show.

- c) Let $\alpha \in \mathcal{O}_{L_1L_2}$. We need to express α as a $\mathbb{Z}$ -linear combination of the elements in $\mathcal{B}$. Write

$$\alpha = \sum_{\substack{1 \leq j_1 \leq n_1 \\ 1 \leq j_2 \leq n_2}} \alpha_{j_1, j_2} z_{j_1}^{(1)} z_{j_2}^{(2)} \quad \text{with} \quad \alpha_{j_1, j_2} \in \mathbb{Q}.$$

We know that this is possible since the $\mathbb{Z}$ -bases of $\mathcal{O}_i$ are $\mathbb{Q}$ -bases of L_i and, since $L_1L_2 = \mathbb{Q}(L_1 \cup L_2)$, every element in L_1L_2 is a finite $\mathbb{Q}$ -linear combination of elements in L_1 and L_2 , i.e., $\mathcal{B}$ generates L_1L_2 over $\mathbb{Q}$. Since $[L_1L_2 : \mathbb{Q}] = n_1n_2$, it follows that $\mathcal{B}$ is a $\mathbb{Q}$ -basis of L_1L_2 . We need to show that all the coefficients α_{j_1, j_2} are elements of $\mathbb{Z}$.

Consider, for $1 \leq j_2 \leq n_2$, the elements

$$\beta_{j_2} = \sum_{1 \leq j_1 \leq n_1} \alpha_{j_1, j_2} z_{j_1}^{(1)} \in L_1.$$

As of Exercise 4b we know that $d_2\beta_{j_2} \in \mathcal{O}_1$ for all $1 \leq j_2 \leq n_2$. Since $(z_1^{(1)}, \dots, z_{n_1}^{(1)})$ is a $\mathbb{Z}$ -basis of $\mathcal{O}_1$, this implies that $d_2\alpha_{j_1, j_2} \in \mathbb{Z}$ for all (j_1, j_2) . Exchanging the roles of L_1 and L_2 in this argument, the same reasoning implies that $d_1\alpha_{j_1, j_2} \in \mathbb{Z}$ for all (j_1, j_2) . Since $(d_1, d_2) = (1)$, it follows that $\alpha_{j_1, j_2} \in \mathbb{Z}$ for all (j_1, j_2) . More explicitly, let $r_1, r_2 \in \mathbb{Z}$ such that $1 = r_1d_1 + r_2d_2$, it follows that

$$\alpha_{j_1, j_2} = (r_1d_1 + r_2d_2)\alpha_{j_1, j_2} = r_1d_1\alpha_{j_1, j_2} + r_2d_2\alpha_{j_1, j_2} \in \mathbb{Z}.$$

- d) The discriminant of $\mathcal{B}$ is given by

$$\text{disc}_{L_1L_2/\mathbb{Q}}(\mathcal{B}) = (\det M)^2,$$

where M is the $n_1n_2 \times n_1n_2$ -matrix

$$M = \begin{pmatrix} M_{1,1} & \cdots & M_{1,n_2} \\ \vdots & \ddots & \vdots \\ M_{n_2,1} & \cdots & M_{n_2,n_2} \end{pmatrix},$$

with the M_{i_2, j_2} the $n_1 \times n_1$ -matrix defined as

$$M_{i_2, j_2} = \begin{pmatrix} \sigma_1^{(1)} \sigma_{i_2}^{(2)}(z_1^{(1)} z_{j_2}^{(2)}) & \cdots & \sigma_1^{(1)} \sigma_{i_2}^{(2)}(z_{n_1}^{(1)} z_{j_2}^{(2)}) \\ \vdots & \ddots & \vdots \\ \sigma_{n_1}^{(1)} \sigma_{i_2}^{(2)}(z_1^{(1)} z_{j_2}^{(2)}) & \cdots & \sigma_{n_1}^{(1)} \sigma_{i_2}^{(2)}(z_{n_1}^{(1)} z_{j_2}^{(2)}) \end{pmatrix}.$$

In order to calculate $\det(M)$, we first rewrite the latter matrix as

$$M_{i_2, j_2} = \begin{pmatrix} \sigma_1^{(1)}(z_1^{(1)}) \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) & \cdots & \sigma_1^{(1)}(z_{n_1}^{(1)}) \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) \\ \vdots & \ddots & \vdots \\ \sigma_{n_1}^{(1)}(z_1^{(1)}) \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) & \cdots & \sigma_{n_1}^{(1)}(z_{n_1}^{(1)}) \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) \end{pmatrix}$$

and therefore $M_{i_2, j_2} = T_1 S_{i_2, j_2}$, where

$$T_1 = \begin{pmatrix} \sigma_1^{(1)}(z_1^{(1)}) & \cdots & \sigma_1^{(1)}(z_{n_1}^{(1)}) \\ \vdots & \ddots & \vdots \\ \sigma_{n_1}^{(1)}(z_1^{(1)}) & \cdots & \sigma_{n_1}^{(1)}(z_{n_1}^{(1)}) \end{pmatrix},$$

and

$$S_{i_2, j_2} = \begin{pmatrix} \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) & & \\ & \ddots & \\ & & \sigma_{i_2}^{(2)}(z_{j_2}^{(2)}) \end{pmatrix}.$$

This way we can express M as follows,

$$M = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_1 \end{pmatrix} \begin{pmatrix} S_{1,1} & \cdots & S_{1,n_2} \\ \vdots & \ddots & \vdots \\ S_{n_2,1} & \cdots & S_{n_2,n_2} \end{pmatrix}.$$

Now let E_{i_1, j_2} be the $n_1 \times n_2$ -matrix whose only non-zero entry is 1 in the i_1 -th row and j_2 -th column, and set

$$P = \begin{pmatrix} E_{1,1} & \cdots & E_{n_1,1} \\ \vdots & \ddots & \vdots \\ E_{1,n_2} & \cdots & E_{n_1,n_2} \end{pmatrix}.$$

Clearly, P is a permutation matrix, so that $\det(P) \in \{-1, 1\}$. Furthermore, it is not hard to see that

$${}^t P \begin{pmatrix} S_{1,1} & \cdots & S_{1,n_2} \\ \vdots & \ddots & \vdots \\ S_{n_2,1} & \cdots & S_{n_2,n_2} \end{pmatrix} P = \begin{pmatrix} T_2 & & \\ & \ddots & \\ & & T_2 \end{pmatrix},$$

where T_2 is the matrix defined in 4b. Hence

$$M = \begin{pmatrix} T_1 & & \\ & \ddots & \\ & & T_1 \end{pmatrix} P \begin{pmatrix} T_2 & & \\ & \ddots & \\ & & T_2 \end{pmatrix} {}^t P,$$

which then gives

$$\det(M) = (\det T_1)^{n_2} (\det T_2)^{n_1}.$$

Because of $d_1 = (\det T_1)^2$ and $d_2 = (\det T_2)^2$, we thus get

$$\text{disc}_{L_1 L_2 / \mathbb{Q}}(\mathcal{B}) = (\det M)^2 = d_1^{n_2} d_2^{n_1},$$

which is exactly what we wanted to prove.

5. Clearly, it is of no relevance which specific primitive n -th root of unity we choose for ζ_n . Thus, in order to simplify the notation, we will simply assume that

$$\zeta_n = e^{\frac{2\pi i}{n}}.$$

Also, remember that for any two positive integers n_1 and n_2 , we have

$$n_1 n_2 = [n_1, n_2] (n_1, n_2).$$

a) Clearly

$$\zeta_{[n_1, n_2]}^{\frac{n_2}{(n_1, n_2)}} = \zeta_{n_1} \quad \text{and} \quad \zeta_{[n_1, n_2]}^{\frac{n_1}{(n_1, n_2)}} = \zeta_{n_2},$$

which shows that

$$\mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) \subset \mathbb{Q}(\zeta_{[n_1, n_2]}) \quad \text{and} \quad \mathbb{Z}[\zeta_{n_1}, \zeta_{n_2}] \subset \mathbb{Z}[\zeta_{[n_1, n_2]}].$$

On the other hand, we know from Bézout's lemma that there exist integers $r_1, r_2 \in \mathbb{Z}$ such that

$$\zeta_{n_1}^{r_1} \zeta_{n_2}^{r_2} = e^{2\pi i \frac{r_1 n_2 + r_2 n_1}{n_1 n_2}} = e^{\frac{2\pi i}{[n_1, n_2]}} = \zeta_{[n_1, n_2]},$$

implying that

$$\mathbb{Q}(\zeta_{[n_1, n_2]}) \subset \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) \quad \text{and} \quad \mathbb{Z}[\zeta_{[n_1, n_2]}] \subset \mathbb{Z}[\zeta_{n_1}, \zeta_{n_2}].$$

This concludes the proof.

b) We have

$$\zeta_{n_1}^{\frac{n_1}{(n_1, n_2)}} = \zeta_{(n_1, n_2)} \quad \text{and} \quad \zeta_{n_2}^{\frac{n_2}{(n_1, n_2)}} = \zeta_{(n_1, n_2)},$$

so that $\zeta_{(n_1, n_2)} \in \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})$ and hence

$$\mathbb{Q}(\zeta_{(n_1, n_2)}) \subset \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}).$$

On the other hand, by Exercise 3c, together with what we have shown in 5a, we see that

$$\text{Gal}(\mathbb{Q}(\zeta_{[n_1, n_2]})/\mathbb{Q}(\zeta_{n_1})) \cong \text{Gal}(\mathbb{Q}(\zeta_{n_2})/\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})).$$

By consequence,

$$\begin{aligned} [\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})] &= [\mathbb{Q}(\zeta_{[n_1, n_2]}) : \mathbb{Q}(\zeta_{n_1})] \\ &= \frac{[\mathbb{Q}(\zeta_{[n_1, n_2]}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{n_1}) : \mathbb{Q}]} \\ &= \frac{\phi([n_1, n_2])}{\phi(n_1)} = \frac{\phi(n_2)}{\phi((n_1, n_2))} \\ &= \frac{[\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_{(n_1, n_2)}) : \mathbb{Q}]} \\ &= [\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{(n_1, n_2)})]. \end{aligned}$$

Hence, we see that

$$[\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{(n_1, n_2)})] = \frac{[\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{(n_1, n_2)})]}{[\mathbb{Q}(\zeta_{n_2}) : \mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2})]} = 1,$$

or, in other words,

$$\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{(n_1, n_2)}),$$

as we wanted to show.

c) We use induction on the number of prime factors of n . If n has exactly one prime factor, i.e., $n = p^\ell$ for some prime p , then we know by Exercise 5 of Sheet 7 that

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n],$$

and that the discriminant $\Delta_{\mathbb{Q}(\zeta_n)}$ is only divisible by p .

Now let n be an integer with exactly $r + 1$ different prime divisors, say

$$n = p_1^{\ell_1} \cdots p_r^{\ell_r} p_{r+1}^{\ell_{r+1}}.$$

Let $n_1 = p_1^{\ell_1} \cdots p_r^{\ell_r}$ and $n_2 = p_{r+1}^{\ell_{r+1}}$, so that

$$n = n_1 n_2 \quad \text{and} \quad (n_1, n_2) = 1.$$

By our induction hypothesis, we know that, for $i = 1, 2$,

$$\mathcal{O}_{\mathbb{Q}(\zeta_{n_i})} = \mathbb{Z}[\zeta_{n_i}],$$

and that the discriminant $\Delta_{\mathbb{Q}(\zeta_{n_i})}$ is only divisible by the prime factors of n_i . Furthermore, as we have shown in 5a and 5b, we have

$$\mathbb{Q}(\zeta_{n_1}) \cap \mathbb{Q}(\zeta_{n_2}) = \mathbb{Q} \quad \text{and} \quad \mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2}) = \mathbb{Q}(\zeta_{n_1}, \zeta_{n_2}) = \mathbb{Q}(\zeta_n).$$

Hence, we can apply the results from Exercise 4 to see that

$$\begin{aligned} \mathcal{O}_{\mathbb{Q}(\zeta_n)} &= \mathcal{O}_{\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})} = \left\{ \sum_{i=1}^r a_i^{(1)} a_i^{(2)} : r \in \mathbb{N} \cup \{0\}, a_i^{(j)} \in \mathcal{O}_{\mathbb{Q}(\zeta_{n_j})} \right\} \\ &= \left\{ \sum_{i=1}^r a_i^{(1)} a_i^{(2)} : r \in \mathbb{N} \cup \{0\}, a_i^{(j)} \in \mathbb{Z}[\zeta_{n_j}] \right\} = \mathbb{Z}[\zeta_{n_1 n_2}], \end{aligned}$$

and that the discriminant $\Delta_{\mathbb{Q}(\zeta_n)} = \Delta_{\mathbb{Q}(\zeta_{n_1})\mathbb{Q}(\zeta_{n_2})}$ is only divisible by the prime factors of $n = n_1 n_2$. This concludes the proof.

- d) We will show that if $p|n$, p ramifies in $\mathbb{Z}[\zeta_n]$. The other direction was already proven in class.

Let $d \geq 1$ be such that $p^d || n$. We have $\mathbb{Z}[\zeta_{p^d}] \subseteq \mathbb{Z}[\zeta_n]$ an extension of Dedekind domains. It follows from Exercise 2d of Sheet 7 and the ramification criterion discussed in class that p ramifies in $\mathbb{Z}[\zeta_{p^d}]$, so it ramifies in $\mathbb{Z}[\zeta_n]$.