1.
2. Suppose that $\mathfrak{a}$ and $\mathfrak{b}$ have a common prime divisor, i.e., let $\mathfrak{p} \subseteq A$ a prime ideal such that $\mathfrak{a} \cup \mathfrak{b} \subseteq \mathfrak{p}$. Since $\mathfrak{a} + \mathfrak{b}$ is the ideal generated by $\mathfrak{a} \cup \mathfrak{b}$, this is equivalent to $\mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{p}$. In particular, we have shown that $\mathfrak{a} + \mathfrak{b}$ is a proper ideal if and only if $\mathfrak{a}$ and $\mathfrak{b}$ have a common prime divisor.
3. Let $0 < e \leqslant v_{\mathfrak{P}}(\mathfrak{p}.A)$. Since $\mathfrak{P}^{v_{\mathfrak{P}}(\mathfrak{p}.A)} \subseteq \mathfrak{P}^e \subseteq \mathfrak{P}$, using $\mathfrak{p} = \mathfrak{P} \cap A$ (which was proven in class), we find that

$$\mathfrak{P} \cap A = \mathfrak{p} \subseteq \mathfrak{P}^e \cap A \subseteq \mathfrak{P} \cap A$$

and hence the desired equality follows.
4. a) By the classification of finitely generated groups over $\mathbb{Z}$, there must exist $\xi \in \mathcal{O}_K$ such that its equivalence class $\xi + \mathbb{Z}[\theta]$ is of order p in $\mathcal{O}_K/\mathbb{Z}[\theta]$. In other words, we have $\xi \notin \mathbb{Z}[\theta]$ but $p\xi \in \mathbb{Z}[\theta]$.
   b) Since $p\xi \in \mathbb{Z}[\theta]$, we can write it in the form

$$p\xi = b_0 + b_1\theta + \ldots + b_{d-1}\theta^{d-1}$$

for some $b_0, \ldots, b_{d-1} \in \mathbb{Z}$. Furthermore note that not all b_i are divisible by p, since otherwise we would have $\xi \in \mathbb{Z}[\theta]$. So there is a smallest index j such that $p \nmid b_j$. Then we can write $b_j\theta^{d-1}$ in the following way,

$$b_j\theta^{d-1} = \left(p\xi - b_0 - \ldots - b_{j-1}\theta^{j-1}\right)\theta^{d-j-1} - \left(b_{j+1} + \ldots + b_{d-1}\theta^{j-d-2}\right)\theta^d.$$

By definition of b_j we have

$$p\xi - b_0 - b_1\theta - \ldots - b_{j-1}\theta^{j-1} \in p\mathcal{O}_K,$$

and since P is Eisenstein at p we also have

$$\theta^d = -a_{d-1}\theta^{d-1} - \ldots - a_1\theta - a_0 \in p\mathcal{O}_K.$$

Thus

$$b_j\theta^{d-1} \in p\mathcal{O}_K,$$

as we wanted to show.
   c) We have

$$\mathrm{N}_{K/\mathbb{Q}}\left(\frac{b_j\theta^{d-1}}{p}\right) = \frac{{b_j}^d}{p^d}\,\mathrm{N}_{K/\mathbb{Q}}(\theta)^{d-1} = \frac{{b_j}^d {a_0}^{d-1}}{p^d} \notin \mathbb{Z},$$

since $p \nmid b_j$ and $p^2 \nmid a_0$.
   d) As we have shown in 4b, $b_j\theta^{d-1}/p \in \mathcal{O}_K$ and thus

$$\mathrm{N}_{K/\mathbb{Q}}\left(\frac{b_j\theta^{d-1}}{p}\right) \in \mathbb{Z}.$$

This contradicts 4c. Hence we can conclude that p does not divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$.
5. a) First of all note that

$$\Phi(X) = 1 + X^{p^{\ell-1}} + X^{2p^{\ell-1}} + X^{3p^{\ell-1}} + \ldots + X^{(p-1)p^{\ell-1}},$$

so $\Phi(X)$ is indeed a polynomial in $\mathbb{Z}[X]$ of degree $\phi(p^\ell) = p^{\ell-1}(p-1)$. Now, since ζ is a primitive p^ℓ-th root of unity, we have that

$$\zeta^{p^\ell} = 1 \qquad \text{and} \qquad \zeta^{p^{\ell-1}} \neq 1,$$

and thus

$$\Phi(\zeta) = \frac{\zeta^{p^\ell} - 1}{\zeta^{p^{\ell-1}} - 1},$$

which shows that ζ is indeed a root of $\Phi(X)$.

In order to show irreducibility, we will apply Eisenstein's criterion on the polynomial $\Phi(X+1)$. Let $\overline{\Phi}(X) \in \mathbb{F}_p[X]$ be the reduction of $\Phi(X)$ mod p. Because of

$$X^{p^j} = (X+1)^{p^j} - 1 \quad \text{for} \quad j \geqslant 0$$

in $\mathbb{F}_p[X]$, it follows that

$$\overline{\Phi}(X+1)X^{p^{\ell-1}} = \overline{\Phi}(X+1)((X+1)^{p^{\ell-1}} - 1) = (X+1)^{p^\ell} - 1 = X^{p^\ell},$$

and thus

$$\overline{\Phi}(X+1) = X^{(p-1)p^{\ell-1}}.$$

This shows that all but the leading coefficients of the polynomial $\Phi(X+1)$ are divisible by p. Furthermore, a direct calculation shows that the constant coefficient of $\Phi(X+1)$ is equal to p. Hence we can apply the Eisenstein criterion and we see that $\Phi(X+1)$ is indeed irreducible. By consequence, so is $\Phi(X)$.

b) By what we have shown in 5a, the minimal polynomial of ξ (which is a p-th root of unity) over $\mathbb{Q}$ is given by

$$1 + X + X^2 + \ldots + X^{p-1}.$$

Thus the minimal polynomial of $\xi - 1$ is

$$1 + (X+1) + (X+1)^2 + \ldots + (X+1)^{p-1},$$

and since the constant coefficient of this polynomial is equal to p, we get

$$\mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1) = p.$$

Using this result we can also deduce

$$\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}}(\xi - 1) = \mathrm{N}_{\mathbb{Q}(\xi)/\mathbb{Q}}(\xi - 1)^{[\mathbb{Q}(\zeta):\mathbb{Q}(\xi)]} = p^{p^{\ell-1}},$$

where we have made use of the fact that $[\mathbb{Q}(\zeta) : \mathbb{Q}(\xi)] = p^{\ell-1}$.

c) We have

$$(X^{p^{\ell-1}} - 1)\Phi(X) = X^{p^\ell} - 1$$

which by taking the derivative with respect to X gives

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

The identity in question follows immediately by evaluating both sides at ζ.

d) By Sheet 6, Exercise 3(c) we have

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^\ell)-1}\right)\right| = \mathrm{N}_{K/\mathbb{Q}}(\Phi'(\zeta)).$$

so that by the identity proven in 5c,

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^\ell)-1}\right)\right| = \mathrm{N}_{K/\mathbb{Q}}\left(\frac{p^\ell}{\zeta(\xi-1)}\right) = \frac{\mathrm{N}_{K/\mathbb{Q}}(p^\ell)}{\mathrm{N}_{K/\mathbb{Q}}(\zeta)\,\mathrm{N}_{K/\mathbb{Q}}(\xi-1)}.$$

Noting that

$$\mathrm{N}_{K/\mathbb{Q}}(p^\ell) = p^{\ell\phi(p^\ell)}, \qquad \mathrm{N}_{K/\mathbb{Q}}(\zeta) = 1 \qquad \text{and} \qquad \mathrm{N}_{K/\mathbb{Q}}(\xi - 1) = p^{p^{\ell-1}}$$

the identity in question follows.

e) Let $\mathcal{B}$ be a basis of $\mathcal{O}_K$, and let M be the matrix representing the tuple

$$1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^\ell)-1}$$

in this basis. Then we have the relation

$$\operatorname{disc}_{K/\mathbb{Q}}\left(1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^\ell)-1}\right) = (\det M)^2 \operatorname{disc}_{K/\mathbb{Q}}(\mathcal{B}).$$

By Sheet 2 we have

$$|\det(M)| = |\mathcal{O}_K/\mathbb{Z}[\zeta]|,$$

and by 5d,

$$\left|\operatorname{disc}_{K/\mathbb{Q}}\left(1, \zeta, \zeta^2, \ldots, \zeta^{\phi(p^\ell)-1}\right)\right| = p^s,$$

for some positive integer s. Together this shows that the only prime divisor of $|\mathcal{O}_K/\mathbb{Z}[\zeta]|$ is p.

On the other hand, as shown in 5a, the polynomial $\Phi(X+1)$ satisfies the Eisenstein condition at p. By the previous exercise, it follows that p doesn't divide

$$\left|\mathcal{O}_{\mathbb{Q}(\zeta-1)}\big/\mathbb{Z}[\zeta-1]\right|,$$

and since obviously $\mathbb{Q}(\zeta-1) = \mathbb{Q}(\zeta)$ and $\mathbb{Z}[\zeta-1] = \mathbb{Z}[\zeta]$, we see that p does also not divide $|\mathcal{O}_K/\mathbb{Z}[\zeta]|$. So, we must have

$$|\mathcal{O}_K/\mathbb{Z}[\zeta]| = 1,$$

or, in other words, $\mathcal{O}_K = \mathbb{Z}[\zeta]$.