0. Read the proof of Proposition 2 in §2.1 of the text (“integrality of ring extensions is transitive”).

(i) Deduce that if $K'/K$ is an extension of number fields then not only is $\mathcal{O}_{K'}$ integral over $\mathcal{O}_K$ (even over $\mathbb{Z}$!) but it is the integral closure of $\mathcal{O}_K$ in $K'$. This is important in the relative theory of number fields (viewing one number field as an extension of another). Taking $K' = K$, this proves $\mathcal{O}_K$ is integrally closed!

(ii) In the setup of (i), prove that the norm and trace maps $K' \to K$ carry $\mathcal{O}_{K'}$ into $\mathcal{O}_K$. (Hint: Compute the norm and trace in a Galois closure of $K'$ over $K$).

**Remark.** Whereas $\mathcal{O}_K$ is a finitely generated and free $\mathbb{Z}$-module (so it is also a finitely generated $\mathcal{O}_K$-module, by using the same generating set as over $\mathbb{Z}$), it often happens that $\mathcal{O}_{K'}$ is not a free $\mathcal{O}_K$-module (so in such cases $\mathcal{O}_K$ is certainly not a PID). An example is $K = \mathbb{Q}(\sqrt{-5})$ and $K' = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.

1. Let $K = \mathbb{Q}(\sqrt{3}, \sqrt{5})$ be a splitting field for $(X^2 - 3)(X^2 - 5)$ over $\mathbb{Q}$. Prove that $\alpha = \sqrt{3} + \sqrt{5}$ is a primitive element, and compute $D(1, \alpha, \alpha^2, \alpha^3)$ in two different ways: use the definition as a determinant of traces, and alternatively (since it is easy to “write down” the conjugates of $\alpha$ over $\mathbb{Q}$) use the formula $(-1)^{(n-1)/2} \prod_{\sigma \neq \tau} (\sigma(\alpha) - \tau(\alpha))$ (with $n = [K : \mathbb{Q}] = 4$ here).

2. A pair of ideals $I$ and $J$ in a ring $A$ are said to be coprime if $I + J = A$. For example, if $I$ is a maximal ideal and $J$ is not contained in $I$ then $I$ and $J$ are coprime.

(i) If $A$ is a PID, prove that nonzero ideals $(a)$ and $(a')$ are coprime if and only if $a$ and $a'$ share no common irreducible factor. Give a counterexample in a UFD that is not a PID. (Hint: $A = k[X,Y]$ for a field $k$, which you may accept is UFD.)

(ii) If $I$ and $J$ are coprime, prove that the inclusion $IJ \subseteq I \cap J$ is an equality.

(iii) If $I_1, \ldots, I_k$ are ideals that are pairwise coprime with $k \geq 2$, prove that $I_1$ and $\prod_{j=2}^k I_j$ are coprime, and deduce by induction on $k$ and (ii) that $\cap_{j=1}^k I_j = \prod_{j=1}^k I_j$.

(iv) Prove the Chinese Remainder Theorem for pairwise coprime ideals: if $I_1, \ldots, I_k$ are pairwise coprime (with $k \geq 2$) then the natural map of rings

$$ A/(\prod_{j=1}^k I_j) \to (A/I_1) \times \cdots \times (A/I_k) $$

is an isomorphism, and so in particular the natural map $A \to \prod_{j=1}^k (A/I_j)$ is surjective. (Hint: induction)

3. Let $d \in \mathbb{Z} - \{0, 1\}$ be squarefree. Let $K = \mathbb{Q}(\sqrt{d})$. Let $D = \text{disc}(K/\mathbb{Q})$ (so $D \equiv 0, 1 \mod 4$, and $2|D$ if and only if $d \equiv 2, 3 \mod 4$).

(i) Construct an isomorphism of rings $\mathbb{Z}[X]/(X^2 - DX + (D^2 - D)/4) \cong \mathcal{O}_K$.

(ii) Passing to the quotient modulo $p$, describe $\mathcal{O}_K/p\mathcal{O}_K$ as a quotient of $\mathbb{F}_p[X]$, and for odd $p$ (resp. $p = 2$) deduce that $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ (i.e., $\mathcal{O}_K/p\mathcal{O}_K$ is a domain) if and only if $p \nmid D$ and $D$ is a nonsquare modulo $p$ (resp. $D \equiv 3 \mod 8$), in which case $\mathcal{O}_K/p\mathcal{O}_K$ is a finite field with size $p^2$. Prove that if $p|D$ then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[t]/(t^2)$ and that if $p \nmid D$ but $D$ is a square modulo $p$ for odd $p$ (resp. $D \equiv 1 \mod 8$ for $p = 2$) then $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p \times \mathbb{F}_p$ as rings.

4. (i) Let $R$ be a domain whose underlying set is finite. Prove that $R$ is a field. (Hint: using counting to prove surjectivity of the multiplication map $R \to R$ against a nonzero element of $R$.)

(ii) Let $F$ be a field and $F \to A$ a map of rings making $A$ finite-dimensional as an $F$-vector space. Prove that $A$ is a domain if and only if it is a field. (Hint: use $F$-dimension reasons to prove surjectivity of the multiplication map $A \to A$ against a nonzero element of $A$, a map you must check is $F$-linear.)

5. (i) Read §2.2 and then the statement and proof of Eisenstein’s irreducibility criterion (for PID’s) in §2.9. Prove that $X^7 + 6X + 12 \in \mathbb{Q}[X]$ is irreducible. Also prove that if $\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 \in \mathbb{Q}[X]$ for a prime $p$ then $\Phi_p(X^e)$ is irreducible over $\mathbb{Q}$ for any $e \geq 0$ (hint: replace $X$ with $X + 1$).

(ii) Let $A$ be a PID with fraction field $K$. **Gauss’ Lemma** says that if a monic $f \in A[X]$ is reducible over $K$ then it admits a nontrivial monic factorization over $A$: see Wikipedia for a proof. Deduce that if $f \bmod m \in (A/m)[X]$ is irreducible for some maximal ideal $m$ of $A$ then $f$ is irreducible over $K$. Apply it to prove $X^3 - X^2 - 2X - 8 \in \mathbb{Q}[X]$ is irreducible by working in $\mathbb{F}_p[X]$ for some small prime $p$. 
