1. Prove that a UFD is normal.

Proof: Let A be a UFD, K its field of fractions. Given $x \in K$, we can write $x = a/b$ with $a \in A$ and $b \in A \setminus \{0\}$, and the factorizations of a and b not having any prime in common (by canceling any common primes). Then if x is integral over A, we have

$$x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 = 0$$

for some n and $c_i \in A$. Clearing denominators gives

$$a^n + c_{n-1}a^{n-1}b + \ldots + c_1 a b^{n-1} + c_0 b^m = 0,$$

which shows that b divides a^n. But then any prime in b's factorization would also be in a^n's, and hence in a's; we avoid a contradiction only if b's factorization has no primes, i.e. b is a unit, which means $x \in A$.

2. What is the normalization of $A = k[x, y]/(y^2 - x^3)$? Here k is a field.

Answer: First we give an injection of A into $k[t]$: define $\varphi : A \to k[t]$ by $x \mapsto t^2$, $y \mapsto t^3$ (which is well-defined since $(t^3)^2 - (t^2)^3 = 0$). We will show injectivity by exhibiting a collection of elements of A which span A and whose images under φ are linearly independent (as a bonus, this will simultaneously show that our collection is in fact a basis). The desired collection consists of the

$$\overline{x}^i \overline{y}^j \text{ for } i \geq 0 \text{ and } j = 0 \text{ or } 1.$$

These span A: indeed, certainly the $\overline{x}^i\overline{y}^j$ for $i, j \geq 0$ span, and we can reduce the j below 2 by successively applying the relation $\overline{y}^2 = \overline{x}^3$. And their images, namely 1 together with the t^n for $n \geq 2$, are indeed linearly independent.

So A is isomorphic to its image $A' = \varphi(A)$ (which, explicitly, is the span of 1 and the x^n for $n \geq 2$). Let's think about the normalization of A'. The field of fractions of A' is $k(t)$, the same as that of $k[t]$, since $t = t^3/t^2$. And $k[t]$ is integral over A', since $t^2 - t^2 = 0$. And $k[t]$ is a UFD, hence integrally closed by the first problem. Thus $k[t]$ is the normalization of A'; that is, the normalization of A' is obtained by adjoining the element t^3/t^2 to A' inside its field of fractions. Translating via the above isomorphism, we see that the normalization of A is obtained by adjoining $\overline{y}/\overline{x}$ inside the field of fractions, and that the result is just a polynomial ring in $\overline{y}/\overline{x}$.

3. Let I be an ideal in a ring A. Is $\mathrm{Ann}(I/I^2) = \mathrm{Ann}(I) + I$?

Answer: No. Many of of you gave the following good example: let $A = \prod_{i=1}^{\infty} \mathbf{Z}/2\mathbf{Z}$, and I be the ideal $\oplus_{i=1}^{\infty}\mathbf{Z}/2\mathbf{Z}$. Then $I = I^2$, so $\mathrm{Ann}(I/I^2) = A$; but $\mathrm{Ann}(I) = 0$, so $\mathrm{Ann}(I) + I = I \neq A$.

In this example, I is not finitely generated. Even if I is finitely generated, we don't necessarily have equality; Tiankai and Nike gave the following example: let $A = k[x, y, z]/(y^2 - xz, x^2 - yz)$ and $I = (x, y)$. Then $z \in \mathrm{Ann}(I/I^2)$, but the claim is that $z \notin \mathrm{Ann}(I) + I$. This claim is not easy to check, because it can be tricky to get a handle on modding out by $y^2 - xz$ and $x^2 - yz$. There is a technique one can use, that of Groebner bases, which I won't explain here, but maybe will in section some day.

The reason the finitely generated case is different is that for I finitely generated, one necessarily has that the radicals of $\mathrm{Ann}(I/I^2)$ and of $\mathrm{Ann}(I)+I$ coincide. You might not understand this argument yet, but you soon will:

Indeed, It suffices to see that $V(\mathrm{Ann}(I/I^2)) = V(\mathrm{Ann}(I)+I) = V(\mathrm{Ann}(I)) \cap V(I)$. Since $I = \mathrm{Ann}(A/I)$ and I/I^2 is isomorphic to $I \otimes_A A/I$ (see the next problem), this will follow from the following more general claim: let M and N be finitely generated modules over A. Then $V(\mathrm{Ann}(M \otimes_A N)) = V(\mathrm{Ann}(M)) \cap V(\mathrm{Ann}(N))$.

For this I first claim that $\mathfrak{p} \notin V(\mathrm{Ann}(M))$ if and only if $M_{\mathfrak{p}} = 0$. For "if", note that the condition implies that, $m_1, \ldots, m_n$ being generators, there are $a_1, \ldots, a_n \in A \setminus \mathfrak{p}$ with $a_i m_i = 0$. Then the product of the a_i will be in $\mathrm{Ann}(M)$ but not $\mathfrak{p}$. "Only if" is easier, and I leave it to you.

Thus what we need to prove is that $(M \otimes_A N)_{\mathfrak{p}} = 0$ if and only if either $M_{\mathfrak{p}} = 0$ or $N_{\mathfrak{p}} = 0$. But (and here by $=$ I mean canonical isomorphisms of $A_{\mathfrak{p}}$-modules) we have

$$(M \otimes_A N)_{\mathfrak{p}} = (M \otimes_A N) \otimes_A A_{\mathfrak{p}} = (M \otimes_A A_{\mathfrak{p}}) \otimes_{A_{\mathfrak{p}}} (N \otimes_A A_{\mathfrak{p}}) = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}},$$

so the claim follows from 2.3 below (certainly if M is finitely generated over A, so is $M_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$). Here the second $=$ follows from a general claim made in the proof of that exercise, and the other $=$'s are instances of the same general fact $M_{\mathfrak{p}} = M \otimes_A A_{\mathfrak{p}}$, which I invite you to check.

2.2 Let A be a ring, I an ideal, and M an A-module. Show that $(A/I) \otimes_A M$ is isomorphic to M/IM.

Proof: Consider the short exact sequence

$$0 \to I \to A \to A/I \to 0.$$

Tensoring with M is right exact, so we get an exact sequence

$$I \otimes M \to A \otimes M \to (A/I) \otimes M \to 0.$$

This shows that $(A/I) \otimes M$ is isomorphic to $A \otimes M$ modulo the image of $I \otimes M \to A \otimes M$. However, I claim that $A \otimes M$ is isomorphic to M via $a \otimes m \mapsto am$. Indeed, this is certainly bilinear, so gives a good map from the tensor product $A \otimes M$; and $m \mapsto 1 \otimes m$ is an obvious inverse. So $(A/I) \otimes M$ is isomorphic to M modulo the image of $I \otimes M \to A \otimes M \to M$, which is IM if you just remember the maps.

2.3 Let A be a local ring, M and N finitely generated A-modules. Prove that if $M \otimes_A N = 0$, then $M = 0$ or $N = 0$.

Proof: First I claim that if A is an arbitrary ring and B an A-algebra, and M and N are arbitrary A-modules, we have a canonical isomorphism of B-modules $(M \otimes_A N) \otimes_A B = (M \otimes_A B) \otimes_B (N \otimes_A B)$. As a lemma, I claim that $M \otimes_A B$ has the following universal property: for any B-module P, the sets $\mathrm{Hom}_B(M \otimes_A B, P)$ and $\mathrm{Hom}_A(M, P)$ are in canonical one-to-one correspondence (we can consider P as an A-module through the map $A \to B$: have $a \in A$ act through its image). Indeed, to $f : M \otimes_A B \to P$ we can associate an $M \to P$ by $m \mapsto f(m \otimes 1)$, and to $g : M \to P$ we can associate $M \otimes_A B \to P$ by $m \otimes b \mapsto bg(m)$, and these are easily seen to be inverse. Then the following chain of canonical bijections shows that the two modules we want to be isomorphic satisfy the same universal property:

$$\begin{aligned} Hom_B((M \otimes_A N) \otimes_A B, P) &= Hom_A(M \otimes_A N, P) \\ &= Hom_A(M, Hom_A(N, P)) \\ &= Hom_A(M, Hom_B(N \otimes_A B, P)) \\ &= Hom_B(M \otimes_A B, Hom_B(N \otimes_A B, P)) \\ &= Hom_B((M \otimes_A B) \otimes_B (N \otimes_A B), P). \end{aligned}$$

(To get the explicit isomorphism and its inverse from this argument, one should take $P = (M \otimes_A N) \otimes_A B$ in the above and trace $id_{(M\otimes_A N)\otimes_A B}$ through; then do the reverse with $P = (M \otimes_A B) \otimes_B (M \otimes_A B)$ and $id_{(M\otimes_A B)\otimes_B (M\otimes_A B)}$).

Now we apply this in our situation with $B = A/\mathfrak{m}$. We see that $M \otimes_A N = 0$ implies, on tensoring with B, that $M/\mathfrak{m}M \otimes_{A/\mathfrak{m}} N/\mathfrak{m}N = 0$ (we have also used the previous exercise). But $M/\mathfrak{m}M$ and $N/\mathfrak{m}N$ are vector spaces over the field $A/\mathfrak{m}$, so this means that one must be zero (count dimensions if you like; dim takes tensor to product). Then Nakayama's lemma implies that one of M and N is zero, as desired.

5.8. Let A be a subring of a ring B, and let C be the integral closure of A in B. Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Prove that $f, g \in C[x]$.

Proof: First some building lemmas.

Lemma: Let R be a ring, $f \in R[x]$, and $a \in R$ such that $f(a) = 0$. Then there is a $g \in R[x]$ with $f(x) = g(x)(x - a)$. If $f \neq 0$ then the degree of f is one less than that of g (this is obvious).

Proof: Expand out $f(x) = f(x - a + a)$ as a polynomial in $x - a$ (e.g. using binomial theorem); the constant term is $f(a) = 0$.

Lemma: Let R be a ring, $f \in R[x]$ monic. Then there is a ring S and an injection $R \to S$ such that f has a root in S.

Proof: Take $S = R[x]/(f)$. Clearly f has the root $\overline{x}$ in S, and $R \to S$ is injective since everything nonzero in (f) has degree $\geq \deg(f) > 0$ (here we use monicity).

Lemma: Let R be a ring, $f \in R[x]$ monic. Then there is a ring S and an injection $R \to S$ such that f splits into linear factors in S.

Proof: Use the previous two lemmas and induction.

Now for the proof proper. Apply the last lemma to get a ring S containing B in which both f and g split completely (it's not enough to get fg to split completely; consider $f = g = x^2+2$ in $\mathbf{Z}/4\mathbf{Z}[x]$), say as $f(x) = \prod(x-\alpha_i)$ and $g(x) = \prod(x-\beta_j)$. Then each α_i and β_j is a root of fg, which is monic with coefficients in C; thus each is integral over C. Hence so is every polynomial in the α_i and β_j, in particular the coefficients of f and g. But these also lie in B, in which C is integrally closed; hence $f, g \in C[x]$ as desired.

5.9. Let A be a subring of a ring B, and C the integral closure of A in B. Show that $C[x]$ is the integral closure of $A[x]$ in $B[x]$.

Proof: Firstly, $C[x]$ is integral over $A[x]$, since obviously both C and x are. For the converse, suppose $f \in B[x]$ with

$$f^n + g_{n-1}f^{n-1} + \ldots + g_1 f + g_0 = 0$$

for some $g_i \in A[x]$. Take r larger than the degree of everything in sight, and let $f' = f - x^r$. Then replacing f by $f' + x^r$ in the above and expanding as a polynomial in f' gives something like

$$f'^n + h_{n-1}f'^{n-1} + \ldots + h_1 f' + h_0 = 0,$$

with $h_0 = x^{rn} + g_{n-1}h^{r(n-1)} + \ldots + g_1 h^r + g_0 \in A[x]$. We deduce from the above inset equation that

$$(-f') \cdot (\textit{something in } B[x]) = h_0;$$

by our choice of r, both $-f'$ and h_0 are monic; hence so is (*something*); the previous exercise lets us conclude that $f' \in C[x]$; hence $f = f' + x^r$ is too.