Solutions for Chapter III. Updated November 3, 2016.

Exercise III.1. *Let $d = 4b + 1$ ($b \in \mathbb{Z}$) be square-free. Show that the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{d})$ has free $\mathbb{Z}$-basis $\{1, \alpha\}$, where $\alpha = (1 + \sqrt{d})/2$.*

[anton@math] Observation: Let R be a normal domain with fraction field K, and let L be a field extension of K. If an element $\ell \in L$ is integral over R then the minimal polynomial $p(x) \in K[x]$ of ℓ lies in $R[x]$. To see this, assume ℓ satisfies some monic $g(x) \in R[x]$. Then $p(x)$ divides $g(x)$ in $K[x]$. Then all the roots of $p(x)$ in $\overline{K}$ also satisfy g, so they are integral over R. Thus, the coefficients of p are integral R, so they are in R.

We will show that any integral element of $\mathbb{Q}(\sqrt{d})$ is in $\mathbb{Z} + \alpha\mathbb{Z}$. It is clear that 1 and α are $\mathbb{Z}$-linearly independent. Note that every element of $\mathbb{Q}(\sqrt{d})$ can be written as $\frac{r}{s} + \frac{n}{m}\sqrt{d}$, with $r, s, n, m \in \mathbb{Z}$ because we can clear denominators in the usual way. Moreover, we may assume that r and s are relatively prime, and that n and m are relatively prime. Assume such an element is integral. If $n = 0$, then we get that $\frac{r}{s}$ is integral; since $\mathbb{Z}$ is normal, it follows that $\frac{r}{s}$ is an integer. If $n \neq 0$, then the minimal polynomial is

$$\left(x - \left(\frac{r}{s} + \frac{n}{m}\sqrt{d}\right)\right)\left(x - \left(\frac{r}{s} - \frac{n}{m}\sqrt{d}\right)\right) = x^2 - \frac{2r}{s}x + \frac{r^2}{s^2} - \frac{n^2}{m^2}d.$$

By the observation, we must have $\frac{2r}{s}, \frac{r^2}{s^2} - \frac{n^2}{m^2}d \in \mathbb{Z}$. Since $gcd(r, s) = 1$, we must have $s|2$, so $s = 1$ or 2.

Case 1: $s = 1$. Then we must have $\frac{n^2}{m^2}d \in \mathbb{Z}$, so $m^2|n^2d$. Since d is square-free, any prime dividing m must divide n (with at least as much multiplicity), so $m|n$. Thus, we have $\frac{r}{s} + \frac{n}{m}\sqrt{d} \in \mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq \mathbb{Z} + \mathbb{Z}\alpha$.

Case 2: $s = 2$. In this case, r is odd, so r^2 is 1 modulo 4. We must have $\frac{1}{4} - \frac{n^2}{m^2}d \in \mathbb{Z}$, so we must have that $\frac{4n^2d}{m^2} \in 1 + 4\mathbb{Z}$. Since d is square-free and $gcd(n, m) = 1$, we must have $m = 2$, and n is odd. Thus, $\frac{r}{s} + \frac{n}{m}\sqrt{d} = \frac{r}{2} + \frac{n}{2}\sqrt{d}$, with r and n both odd. Such an element is in $\mathbb{Z} + \alpha\mathbb{Z}$. ■

Exercise III.2. *Let $R \subset S$ be rings, and let $x, y \in S$ such that $x^2, y^2 \in R$. Find a monic equation satisfied by $x + y$ over R.*

[annejls@math] Consider $p(t) = t^4 - 2(x^2 + y^2)t + (x^2 + y^2)^2 - 4x^2y^2$, which is a polynomial over R because $x^2, y^2 \in R$. We see that $p(t) = (t^2 - (x^2 + y^2))^2 - 4x^2y^2$, so $p(x + y) = ((x + y)^2 - (x^2 + y^2))^2 - 4x^2y^2 = (2xy)^2 - 4x^2y^2 = 0$. ■

Exercise III.3. *(Reciprocal polynomial trick) Show that a unit u in a ring is integral over a subring R if and only if $u \in R[u^{-1}]$.*

[anton@math] If u is integral over R, then $u^n + a_1u^{n-1} + \cdots + a_n = 0$, with $a_i \in R$. Multiplying through by u^{-n+1}, we get $u = -a_1 - a_2u^{-1} - \cdots - a_nu^{-n+1} \in R[u^{-1}]$.

Conversely, if $u = b_0 + b_1u^{-1} + \cdots + b_nu^{-n} \in R[u^{-1}]$, the multiplying through by u^n, we get $u^{n+1} + b_0u^{n-1} + \cdots + b_n = 0$, so u is integral over R. ■

In Exercises 4-11, S/R denotes an integral ring extension.

Exercise III.4. *For $u \in R$, show that $u \in U(R)$ iff $u \in U(S)$.*

[David Brown, brownda@math] Let $u \in R \cap U(S)$. As $u^{-1} \in S$ is integral over R, exercise III.3 implies that $u^{-1} \in R[u] = R$ (and thus $u \in U(R)$). Conversely, $U(R) \subset U(S)$. ■

Exercise III.5. *Show that it, if J is any regular ideal in S, then $J \cap R \neq 0$. Does this result hold if J is not regular?*

[annejls@math] Take $x \in J$ a regular element. Now, S/R is integral, so we have $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, where each $a_i \in R$. By assumption, x is regular, so $a_0 \neq 0$. But we see that a_0 is a multiple of x in S, so a_0 is in J. So, a_0 is a non-zero element of $J \cap R$.
The result does not hold if J is not regular. Trivially, if $R = S$, then $J = 0$ verifies this. For an example with proper containment, consider $R = k \subset k[x]/(x^2) = S$, where k is a field. Then, $J = (x)$ is a non-regular ideal such that $J \cap R = 0$. ■

Exercise III.6. *Let $\mathfrak{p} = \mathfrak{P} \cap R$, where $\mathfrak{P} \in \operatorname{Spec}(S)$. Show that $S_{\mathfrak{P}}/R_{\mathfrak{p}}$ may not be an integral extension.*

[ecarter@math] Let $S = \mathbb{Q}[x]$ and $R = \mathbb{Q}[t]$, where $t = x^2 - 1$. Then it is clear that S/R is an integral extension, since x is a root of the monic polynomial $X^2 - t + 1$ over R.

Let $\mathfrak{p} = (t)$ and $\mathfrak{P} = (x-1)$. Then $\mathfrak{P} \cap R$ is the kernel of the composite ring homomorphism $R \to S \to \mathbb{Q}$. Here the first map is the inclusion map, and the second map is evaluation at $x = 1$. Since this corresponds to evaluation at $t = 0$, $\mathfrak{P} \cap R = \mathfrak{p}$. Similarly, $\mathfrak{p} = (x+1) \cap R$.

Suppose $\frac{1}{x+1}$ satisfies some monic polynomial equation which, after clearing denominators, has the form

$$f_n X^n + f_{n-1}X^{n-1} + \cdots + f_0 = 0,$$

where each $f_i \in R$ and $f_n \notin \mathfrak{p}$. Then we have that

$$\frac{f_n}{(x+1)^n} = -\frac{f_{n-1} + f_{n-2}(x+1) + \cdots + f_0(x+1)^{n-1}}{(x+1)^{n-1}}$$

so that

$$f_n = (x+1)(-f_{n-1} - f_{n-2}(x+1) - \cdots - f_0(x+1)^{n-1}).$$

Thus $f_n \in (x+1)$. However, since $\mathfrak{p} = (x+1) \cap R$, $f_n \in \mathfrak{p}$, which is a contradiction. Therefore $\frac{1}{x+1}$ is not integral over R. ■

Exercise III.7. *Let $\mathfrak{p} \in \operatorname{Spec}(R)$ be such that only one prime $\mathfrak{P} \in \operatorname{Spec}(S)$ lies over $\mathfrak{p}$. Show that $S_{\mathfrak{P}} = S_{\mathfrak{p}}$. (In particular, here, $S_{\mathfrak{P}}/R_{\mathfrak{p}}$ would be an integral extension.) (**Hint.** First show that $S_{\mathfrak{p}}$ is a local ring.)*

[los@math, anton@math] The primes of $S_\mathfrak{p}$ correspond to the primes $\mathfrak{P}' \in \operatorname{Spec} S$ such that $\mathfrak{P}' \cap R \subseteq \mathfrak{p}$. In particular, $\mathfrak{P}S_\mathfrak{p}$ is the only prime lying over $\mathfrak{p}R_\mathfrak{p}$. Also, $S_\mathfrak{p}$ is integral over $R_\mathfrak{p}$ (by Corollary 1.4). Thus, we have reduced to the case where $(R, \mathfrak{p})$ is local. For any prime $\mathfrak{P}' \in \operatorname{Spec} S$, we have $\mathfrak{P}' \cap R \subseteq \mathfrak{p} = \mathfrak{P} \cap R$ because $\mathfrak{p}$ is the maximal ideal of R. By incomparability, $\mathfrak{P}' \subseteq \mathfrak{P}$, so $\mathfrak{P}$ is the unique maximal ideal of S. Thus, $S_\mathfrak{P} = S = S_\mathfrak{p}$. ■

Exercise III.8. *Suppose $_RS$ is generated by n elements.*

(1) Show that, for any $\mathfrak{m} \in \operatorname{Max} R$, at most n maximal ideals of S lie over $\mathfrak{m}$. Using this, show that, if $r = |\operatorname{Max} R| < \infty$, then $|\operatorname{Max} S| \le rn$. (Cf. the earlier result (I.5.15))

(2) Show that only finitely many prime ideals of S lie over a given prime ideal in R.

[los@math, anton@math] (1) Since $_RS$ is generated by n elements, we have that $\dim_{R/\mathfrak{m}}(S/\mathfrak{m}S) \le n$. In particular $S/\mathfrak{m}S$ is finite length over itself, so it is artinian. By Akizuki-Cohen, $S/\mathfrak{m}S \cong \prod S/\mathfrak{M}_i^t$ for some t, where the $\mathfrak{M}_i$ are the maximal ideals of $S/\mathfrak{m}S$. By incomparability, only maximal ideals can lie over a maximal ideal, so the $\mathfrak{M}_i$ correspond to the maximal ideals lying over $\mathfrak{m}$. Since each $S/\mathfrak{M}_i^t$ has dimension at least 1 over $R/\mathfrak{m}$, there are at most n of them. Again, since only maximal ideals lie over maximal ideals, we get $|\operatorname{Max} S| \le n|\operatorname{Max} R|$.

(2) If $\mathfrak{p} \in \operatorname{Spec} R$, then $S_\mathfrak{p}$ is integral over $R_\mathfrak{p}$ and $_{R_\mathfrak{p}}S_\mathfrak{p}$ is generated by n elements. By part (the solution to) (1), there are at most n prime ideals of $S_\mathfrak{p}$ over $\mathfrak{p}$. But the primes of $S_\mathfrak{p}$ lying over $\mathfrak{p}$ correspond exactly to the prime ideals of S lying over $\mathfrak{p}$. ■

Exercise III.9. *Show that it is possible for infinitely many prime ideals of S to lie over a prime $\mathfrak{p} \in Spec(R)$.*

[annejls@math] Consider $R = k[x_1^2, x_2^2, \dots] \subset k[x_1, x_2, \dots] = S$, where k is a field. Then, any $\mathfrak{q} = (x_1 - \epsilon_1, x_2 - \epsilon_2, \dots)$ where each $\epsilon_i = \pm 1$, lies over $\mathfrak{p} = (x_1^2 - 1, x_2^2 - 1, \dots)$. ■

[lam@math] *Discussion.* Oh that was pretty smart ... $^*\smile^*$. A really nice feature of Anne's counterexample is that R and S are both *normal domains.* I will strengthen Exercise 9 by demanding a counterexample of this nature!

I once said that the ring $S = k \times k \times \cdots$ gives us lots of counterexamples, so what I had in mind this time was some dumb construction like: taking k above to be $\mathbb{Z}_2$ and viewing S as an algebra over $R = k$. Surely S/R is integral (after all S is Boolean), and *all* primes of S can only lie over (0). There are infinitely many such primes, e.g. $S \cdot (1 - e_i)$ for the unit vectors e_i. Okay — S is not a domain, but a 0-dimensional counterexample deserves a consolation prize ... ■

Exercise III.10. *Show that the functorial map ϕ from* $\operatorname{Spec}(S)$ *to* $\operatorname{Spec}(R)$ *is a closed map; that is, ϕ takes closed sets to closed sets.*

[Jonah (jblasiak@math)] Let $V(I)$, $I \triangleleft S$, be a closed set in $\mathrm{Spec}(S)$. Put $J = R \cap I$, which is an ideal in R. The image of $V(I)$ is the set $\{p \cap R | I \subseteq p\}$. This is clearly a subset of $V(J)$, and we will show it is equal to $V(J)$. There is a natural inclusion $i' : R/J \hookrightarrow S/I$ since J is the kernel of the composition $R \hookrightarrow S \to S/I$. The image of $V(I)$ is equal to the image of $\mathrm{Spec}(S/I)$ under the map $\phi' : \mathrm{Spec}(S/I) \to \mathrm{Spec}(R/J)$ corresponding to i'. It is not hard to see that S/I is an integral extension of R/J: any $s \in S$ satisfies a monic polynomial with coefficients in R; just consider these coefficients mod J and this gives a monic polynomial satisfied by $\bar{s} \in S/I$. Now Going Up Theorem 1.10 (1) applies, so the image of $\mathrm{Spec}(S/I)$ under ϕ' is $\mathrm{Spec}(R/J)$ and therefore the image of $V(I)$ under ϕ is $V(J)$. ■

Exercise III.11. *For a given integral extension S/R, show that the conclusion of the Going-Down theorem 2.5 is equeivalent to each of the following statements:*

1. *for any $\mathfrak{p} \in \mathrm{Spec}(R)$, the set of primes of S lying over $\mathfrak{p}$ is the set of minimal primes over $\mathfrak{p}S$*
2. *for any $I \triangleleft R$, the set of primes of R minimal over I is the set of contractions of the primes of S minimal over IS.*

[Lars Kindler, lars_k@berkeley.edu] Let the conclusion of the Going-Down Theorem be denoted by $(*)$. First let $(*)$ hold and let $\mathfrak{p}$ be a prime of R. Let $\mathfrak{P}$ be a prime of S minimal over $\mathfrak{p}S$, denote $\mathfrak{P} \cap R$ by $\mathfrak{p}'$ and assume $\mathfrak{p} \subsetneq \mathfrak{p}'$. Then by $(*)$ there is a $\mathfrak{P}' \subsetneq \mathfrak{P}$ with $\mathfrak{p}S \subset \mathfrak{P}'$, which is a contradiction. Conversely let $\mathfrak{P} \in \mathrm{Spec}\, S$ with $\mathfrak{P} \cap R = \mathfrak{p}$, then $\mathfrak{p}S \subset \mathfrak{P}$. If $\mathfrak{P}$ is not minimal over $\mathfrak{p}S$, then there is a prime $\mathfrak{P}' \subsetneq \mathfrak{P}$ that also contains $\mathfrak{p}S$ and contracts to $\mathfrak{p}$, which contradicts the incomparability theorem, so $\mathfrak{P}$ is minimal over $\mathfrak{p}S$, which proves $(*) \Rightarrow (1)$.
Next, assume (1) holds and let $I \triangleleft R$. Let $\mathfrak{p} \in \mathrm{Spec}\, R$ be minimal over I, then there is a $\mathfrak{P} \in \mathrm{Spec}\, R$ over $\mathfrak{p}$, which by (1) is minimal over $\mathfrak{p}S \supset IS$. If there is a $\mathfrak{P}' \in \mathrm{Spec}\, S$ with $IS \subset \mathfrak{P}' \subsetneq \mathfrak{P}$, then $\mathfrak{p}S \not\subset \mathfrak{P}'$, so $\mathfrak{P}' \cap R \subsetneq \mathfrak{p}$ is a prime containing I which is a contradiction. Conversely, let $\mathfrak{P} \in \mathrm{Spec}\, S$ be minimal over IS and define $\mathfrak{p} := \mathfrak{P} \cap R \supset I$. Assume there is a $\mathfrak{p}' \in \mathrm{Spec}\, R$ with $I \subset \mathfrak{p}' \subsetneq \mathfrak{p}$, then by (1) $\mathfrak{P}$ is not minimal over $\mathfrak{p}'S$, so there is a $\mathfrak{P}' \in \mathrm{Spec}\, S$ over $\mathfrak{p}'$, with $IS \subset \mathfrak{p}'S \subset \mathfrak{P}' \subsetneq \mathfrak{P}$; a contradiction. This proves $(1) \Rightarrow (2)$.
Now let (2) hold. Given $\mathfrak{P}' \in \mathrm{Spec}\, S$ and $\mathfrak{p}' := \mathfrak{P}' \cap R$, let $\mathfrak{p} \in \mathrm{Spec}\, R$ be a prime ideal of R with $\mathfrak{p} \subsetneq \mathfrak{p}'$. Then $\mathfrak{p}S \subset \mathfrak{P}'$, and $\mathfrak{P}'$ is not minimal over $\mathfrak{p}S$, since in that case (2) would imply $\mathfrak{P}' \cap R = \mathfrak{p} \neq \mathfrak{p}'$. So there is a prime $\mathfrak{P} \subsetneq \mathfrak{P}'$ minimal over $\mathfrak{p}S$, which by assumption means $\mathfrak{P} \cap R = \mathfrak{p}$, i.e. $(*)$ holds. ■

Exercise III.12. *(New Version) Show that a domain R is normal iff, for any $a \in R$ and any domain S that is an integral extension of R, $aS \cap R = aR$.*

[Jonah (jblasiak@math)] First assume R is normal and let K be the quotient field of R. It is clear that $aR \subseteq aS \cap R$. Now suppose $r \in R$ and $r = as$

for some $s \in S$. S is an integral extension of R so there exists an equation $s^n + c_{n-1}s^{n-1} + \ldots + c_0 = 0$, with coefficients c_i in R. Multiplying by a^n we obtain $r^n + c_{n-1}ar^{n-1} + \ldots + c_0 a^n = 0$. This is now an equation in R, which can also be viewed as an equation in K, and therefore $\frac{r}{a}$ satisfies a monic polynomial with coefficients in R (we would like to just say $s = \frac{r}{a}$, but this is not an equation in K because S is not a subring of K). Since R is normal, $\frac{r}{a} = s' \in R$. This yields the equation $r - r = a(s - s')$ in S, which implies $a = 0$ or $s = s'$, as S is a domain. If $a = 0$, the result is easy, and if $s = s'$, then $r = as' \in aR$.

Conversely, let S be the integral closure of R in K. Suppose $s = \frac{r}{a}$ is an element of S, with $r, a \in R$. Since $aS \cap R = aR$, $as = r$ is in aR. Thus $as = as'$, for some $s' \in R$, which implies $s = s' \in R$ since S is a domain. Therefore $S = R$, so R is normal. ■

Exercise III.13. *Let $T = \mathbb{Z}[x]/(x^2 - x, 2x)$. Referring to the notations of (2.14), show that $\varphi(\bar{x}) = (0, \bar{1}) \in S$ defines a ring isomorphism from T to S. Compute the ideals $\varphi^1(\mathfrak{P})$ and $\varphi^{-1}(\mathfrak{P}')$, and show* directly *that $\varphi^{-1}(\mathfrak{P}')$ is a minimal in Tthat provides a counterexample to "Going Down" for the integral extension $T/\mathbb{Z}$.*

[los@math, anton@math] Recall that $S = \mathbb{Z} \times \mathbb{Z}/2$, $\mathfrak{P} = 0 \times \mathbb{Z}/2$, and $\mathfrak{P}' = \mathbb{Z} \times 0$. Since $\varphi(\bar{x})$ satisfies the appropriate relations in S, φ is a homomorphism. Since $(n, \bar{n} + \bar{k}) = \varphi(n + k\bar{x})$, φ is surjective. Every element of T can clearly be written as n or $n + \bar{x}$, and it is immediate that none of these (except zero) is sent to zero, so φ is injective. Note that $\varphi^{-1}(0, \bar{1}) = \bar{x}$ and $\varphi^{-1}(1, 0) = 1 - \bar{x}$.

We have that $\varphi^{-1}(\mathfrak{P}) = (\bar{x})$, and $\varphi^{-1}(\mathfrak{P}') = (1 - \bar{x})$. Since $\bar{x}(1 - \bar{x}) = 0$, any prime in T contains either $\bar{x}$ or $1 - \bar{x}$. So any prime properly contained in $(1 - \bar{x})$ must contain $\bar{x}$, contradicting $\bar{x} \notin (1 - \bar{x})$. Thus, $(1 - \bar{x})$ is minimal.

$(1 - \bar{x}) \cap \mathbb{Z}$ is the kernel of the map $\mathbb{Z} \hookrightarrow T \to T/(1 - \bar{x}) \cong \mathbb{Z}/2$, which is the ideal $2\mathbb{Z}$. Since $2\mathbb{Z}$ is not minimal, we have contradicted "Going Down". ■

Exercise III.14. *Let I be a 0-dimensional ideal in an affine k-algebra S, where k is a field. Show that S is integral over its subring $R = k + I$.*

[Manuel Reyes; mreyes@math] The hypotheses imply that $\overline{S} := S/I$ is a 0-dimensional noetherian ring, hence artinian (see the comments under (2.11)). Then by (II.4.20), $\dim_k \overline{S} < \infty$. So $\overline{S}$ is algebraic over k, hence integral over k. Taking any $s \in S$, this means that there is some monic polynomial $f \in k\,[x]$ such that $f\,(s) \in I$. This means that $g\,(x) := f\,(x) - f\,(s) \in R\,[x]$ is a monic polynomial such that $g\,(s) = 0$. So s is integral over R, and hence the extension $S \supseteq R$ is integral. (Note that in fact the only coefficient of g that might possibly lie in $R \setminus k$ is its constant coefficient!) ■

Exercise III.15. *Supply a proof for Prop. 3.8, and for the last conclusion in (1.4).*

[Soroosh] Recall proposition 3.8 claims that if $s_i \in S$ are almost integral over R, then $R[s_1, ..., s_n]$ is contained in a f.g. R-submodule of S. In particular, all elements of S that are almost integral over R form a subring of S. We prove this by induction. When $n = 1$, then $R[s_1]$ is contained in a f.g. R submodule of S by definition of almost integrality of s_1. Now assume that $R[s_1, ..., s_m]$ is contained in a f.g. submodule of S, say T_1, for some m. We want to show that $R[s_1, ..., s_m, s_{m+1}] = R[s_1, ..., s_m][s_{m+1}]$ is also contained in a f.g. submodule of S. Note that $R[s_{m+1}]$ is contained in a f.g. submodule, say T_2, since s_{m+1} is almost integral. Choose a set of generators for T_1 and T_2, say

$$\begin{aligned} T_1 &= a_1R + \cdots + a_kR, \\ T_2 &= b_1R + \cdots + b_lR. \end{aligned}$$

Let T be the R module generated by all a_ib_j's. We want to show $R[s_1, \ldots, s_{m+1}]$ is contained in T. It is enough to show that $s_1^{\alpha_1} \ldots s_{m+1}^{\alpha_{m+1}}$ is contained in T for all such $(\alpha_1, \ldots, \alpha_{m+1})$, since they are generators for $R[s_1, \ldots, s_{m+1}$. However by assumption

$$\begin{aligned} s_1^{\alpha_1} \ldots s_m^{\alpha_m} &= u_1a_1 + \cdots + u_ka_k, \\ s_{m+1}^{\alpha_{m+1}} &= v_1b_1 + \cdots + v_lb_l, \\ \Rightarrow s_1^{\alpha_1} \ldots s_{m+1}^{\alpha_{m+1}} &= \sum u_iv_jba_ib_j, \end{aligned}$$

which implies $s_1^{\alpha_1} \ldots s_{m+1}^{\alpha_{m+1}} \in T$ which is finitely generated.

As for the last conclusion in (1.4), recall that we want to prove that if C is the integral closure of S in R, then for any multiplicative set M, $M^{-1}C$ is the integral closure of $M^{-1}S$ in $M^{-1}R$. To see this, let $s \in M^{-1}S$. We want to show that s is integral over $M^{-1}R$ if and only if $s \in M^{-1}C$. Assume s is integral. Since $s \in M^{-1}S$, we can find $n \in M$ such that $ns \in S$. We have $ns \in M^{-1}C$ if and only if $s \in M^{-1}C$. Furthermore, since n is a unit in $M^{-1}R$, we have ns is still integral over R. Therefore we may as well assume that $s \in S$. We can find a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ with $a_i \in M^{-1}R$ such that $f(s) = 0$. Letting $a_i = r_i/m_i$ we can clear the denominators to get a polynomial $g(x) = mx^n + b_{n-1}x^{n-1} + \cdots + a_0$ such that $g(s) = 0$. Now

$$\begin{aligned} m^{n-1}g(x) &= (mx)^n + b_{n-1}(mx)^{n-1} + \cdots + m^{n-1}a_0 \\ &= G(mx). \end{aligned}$$

Therefore ms is integral over R, which implies $ms \in C$. That means $s \in M^{-1}C$.

To prove the converse, assume that $s \in M^{-1}C$. Then for some $m \in M$ we have $ms \in C$, which means we can find monic polynomial $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$, with $b_i \in R$, such that $g(ms) = 0$. Let

$$\begin{aligned} f(x) &= \frac{g(mx)}{m^n} \\ &= x^n + \frac{b_{n-1}}{m}x^{n-1} + \cdots + \frac{b_0}{m^n}. \end{aligned}$$

Note that the coefficients of f are all in $M^{-1}R$, and hence s is a root of a monic polynomial over $M^{-1}R$, which means s is integral over $M^{-1}R$. ■

Exercise III.16. *Show that a domain R with quotient field K is normal iff, for every nonzero finitely generated ideal I in R, $\{s \in K : sI \subseteq I\}$ equals R.*

[ecarter@math] First suppose the latter condition is satisfied, and let $q = a/b$ be integral over R, where $a, b \in R$ and $b \neq 0$. Then for some n and some $f_0, f_1, \ldots, f_{n-1} \in R$,

$$q^n = f_0 + f_1 q + \cdots + f_{n-1} q^{n-1}.$$

Let $I = (a^{n-1}b, a^{n-2}b^2, \ldots, b^n)$. For each $k \geq 2$, $qa^{n-k}b^k = a^{n-k+1}b^{k-1} \in I$. Then since

$$qa^{n-1}b = q^n b^n = b^n(f_0 + f_1 q + \cdots + f_{n-1} q^{n-1}) \in I,$$

$qI \subseteq I$, which implies that $q \in R$ by hypothesis. Therefore R is normal.

Now suppose R is normal. Let I be a nonzero finitely generated ideal in R and let $s \in K$ be such that $sI \subseteq I$. Let $a_1, a_2, \ldots, a_n$ be nonzero elements of I which generate it. For each i, $sa_i \in I$, so there exist $b_{1i}, b_{2i}, \ldots, b_{ni}$ such that

$$sa_i = b_{1i}a_1 + b_{2i}a_2 + \cdots + b_{ni}a_n.$$

Then for a given element $r_1a_1 + \cdots + r_na_n$ of I, where each $r_i \in R$, multiplication by s corresponds to the matrix multiplication

$$\begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \\ \vdots \\ r_n \end{pmatrix}$$

Call the matrix on the left A. Then by Cayley-Hamilton, A satisfies the polynomial $\chi_A(\lambda) = \det(\lambda I - A)$, which is monic with coefficients in R. Therefore $\chi_A(s)a_1 = 0$. Since $a_1 \neq 0$ and R is a domain, $\chi_A(s) = 0$. Then since s is integral over R, $s \in R$. ■

Exercise III.17. *Let R be a UFD with $2 \in U(R)$. For any non-zero $r \in R$ not divisible by the square of any prime element, show that $S = R[x]/(x^2 - r)$ is a normal domain.*

[anton@math] Note: If $r = u^2$ for some $u \in U(R)$, then it is not divisible by the square of any prime element, but S is obviously not a domain. The result may hold when r is a unit but not the square of a unit, but I will assume $r \notin U(R)$.

First observe that $S = R \oplus xR$, with the multiplication rule $(a+bx)(c+dx) = ac + bdr + (ad + bc)x$. To see that S is a domain, assume $(a + bx)(c + dx) = ac+bdr+(ad+bc)x = 0+0x$. We can factor out $gcd(a, b)$ and $gcd(c, d)$, so we can assume $gcd(a, b) = gcd(c, d) = 1$ (note that here we are using the assumption that $a+bx$ and $c+dx$ are non-zero). If a prime p divides a, then since $ad+bc = 0$, we have that $p|c$. Since $ac+bdr = 0$, we get $p^2|r$, contradicting that r is square free. Thus, a must be a unit in R, and c must be a unit by symmetry. If $p|b$, then since $ac + bdr = 0$, we get $p | ac$, contradicting that $a, c \in U(R)$. Thus, b must also be a unit, and d must be a unit by symmetry. Since $ac + bdr = 0$, we get that r is a unit, a contradiction.

Clearing denominators in the usual way, we can write any element of $Q(S)$ as $\frac{a}{b} + \frac{c}{d}x$, with $a, b, c, d \in R$; we may assume a and b are relatively prime and c and d are relatively prime. Assume such an element is integral. If $c = 0$, then $\frac{a}{b}$ is integral over R, so $\frac{a}{b} \in R$ since R is normal. If $c \neq 0$, then the minimal polynomial over $Q(R)$ is

$$\left(y - \left(\frac{a}{b} + \frac{c}{d}x\right)\right)\left(y + \left(\frac{a}{b} - \frac{c}{d}x\right)\right) = y^2 - \frac{2a}{b}y + \frac{a^2}{b^2} - \frac{c^2}{d^2}r.$$

By the observation in the solution of problem III.1, we must have $\frac{2a}{b} \in R$ and $\frac{a^2}{b^2} - \frac{c^2}{d^2}r \in R$. Since $2 \in U(R)$, we have that $a/b \in R$, so we must have $\frac{c^2}{d^2}r \in R$, so $d^2 | c^2 r$ in R. Since r is square-free, any prime dividing d must divide c (with at least as much multiplicity), so $d | c$. Thus, $\frac{a}{b} + \frac{c}{d}x \in S$, so S is normal. ■

Exercise III.18. *If T/S is integral and S/R is almost integral, show that T/R is almost integral. Using this, show that, for any ring extension S/R, the complete integral closure of R in S is integrally closed in S.*

[annejls@math] Take $t \in T$. We must find a f. g. R-submodule $N \subset T$ that contains $R[t]$. Now, T/S is integral, so there exist $s_1, s_2, \ldots, s_n \in S$ such that $t^n + s_1 t^{n-1} + \cdots + s_n = 0$. Next, S/R is almost integral, so by Prop. 3.8, there exists a f.g. R-module M with $R[s_1, s_2, \ldots, s_n] \subset M \subset S$. Let $N = M + Mt + \cdots + Mt^{n-1}$, which is f. g. over R because M is. This yields $R[t] \subset R[s_1, s_2, \ldots, s_n, t] \subset N \subset S$, as desired.

Now, consider any ring extension S/R. Let C be the complete integral closure of R in S. For $s \in S$, we have $R \subset C$ an almost integral extension and $C \subset C[s]$ an integral extension, so from the first part of this exercise, $R \subset C[s]$ is almost integral. In particular, s is almost integral over R. However, C is the complete integral closure of R in S, so $s \in C$. ■

Exercise III.19. *In the case where $D \neq K$ in (3.6), name an ideal in the non-noetherian domain R in (3.7) that is not f.g. Do the same for the normal domain $R = \bigcup_{i \geq 0} R_i$ constructed after the proof of (3.19).*

[mreyes@math] The ring from example (3.6) is $R = D + xK[x] \subseteq K[x]$. Let

$$I = xK[x] = \{f(x) \in R : f(0) = 0\} \lhd R.$$

We claim that I is not finitely generated. Indeed, assume for contradiction that I is finitely generated. For $f(x) = a_1 x + \cdots + a_n x^n \in I$, it is straightforward to verify that the function $\varphi : I \to K$ given by $f \mapsto a_1$ is a D-module homomorphism. For any $s \in K$, $sx \in I$ implies that φ is surjective. This means that K is also a finitely generated D-module. But a module-finite ring extension is integral, and because D is normal this means that $D = K$, a contradiction. So I cannot be finitely generated.

In (3.19), we set $R_i = \mathbb{Q}\left[x, \frac{y}{x^i}\right]$ for $i \geq 0$, and we have $R = \bigcup_{i\geq 0} R_i \subseteq \mathbb{Q}[x,y]_x$. We claim that the ideal $I = \bigcup_{i\geq 0}\left(\frac{y}{x^i}\right)$ is not finitely generated; assume for contradiction that it is f.g. It is easy to see that this is finitely generated iff the ascending chain of ideals

$$(y) \subseteq \left(\frac{y}{x}\right) \subseteq \left(\frac{y}{x^2}\right) \subseteq \cdots$$

stabilizes, say $\left(\frac{y}{x^n}\right) = \left(\frac{y}{x^{n+1}}\right)$. In particular, $\frac{y}{x^{n+1}} \in \left(\frac{y}{x^n}\right)$. So there exists $f \in R$ such that $\frac{y}{x^{n+1}} = f\frac{y}{x^n}$. Then the equation $\frac{y}{x^n} = xf\frac{y}{x^n}$ and the fact that R is a domain imply that $1 = xf$. Consider that the map $\mathbb{Q}[x,y] \to \mathbb{Q}(x)$ given by evaluating y at 0 sends x to a unit. So it extends to a map $\mathbb{Q}[x,y]_x \to \mathbb{Q}(x)$ given by evaluating y at 0. This then restricts to a map $\varepsilon : R \to \mathbb{Q}(x)$. Writing $f = g\left(x, \frac{y}{x^m}\right)$ for some $g \in \mathbb{Q}[t_1, t_2]$, applying ε to the equation $1 = xf$ gives $1 = xg(x,0)$ in $\mathbb{Q}(x)$, where $g(x,0)$ is a polynomial in x, a contradiction. So I must not have been finitely generated. ■

Exercise III.20. *Referring to the notations and assumptions in (3.21), we have shown that the domain R there has complete integral closure $R^\dagger = K[x]$. If D is completely normal, show that R is completely integrally closed in $K[x]$ (that is, if $\alpha \in K[x]$ is almost integral over R (*as an element of $K[x]$*), then $\alpha \in R$).*

[los@math, anton@math] Recall that K is the field of fractions of D, and $R = xK[x] + D$. Assume $\alpha \in K[x]$ is almost integral over R, so $R[\alpha] \subseteq T \subseteq K[x]$, with T a finitely generated module over R. Since almost integral elements form a ring, we may add an element of R to α without changing whether it is almost integral. Since $xK[x] \subseteq R$, we may assume $\alpha \in K$.

It is easy to see that the constant terms of the generators of T generate the module T_0 of constant terms of elements of T (as a D-module). In particular, T_0 is a finitely generated D-module. Now we have that $D[\alpha]$ (the ring constant terms of $R[\alpha]$) is contained in T_0. Since D is completely normal, we get that $\alpha \in D \subseteq R$. Thus, R is completely integrally closed in $K[x]$. ■

Exercise III.21. *Show that the quotient field of $\mathbb{Z}[[x]]$ is not $\mathbb{Q}((x))$ by considering the power series $\sum_{n=0}^\infty 2^{-n^2}x^n$. How about the power series for e^x?*

[anton@math] If the power series $\sum_{n=0}^\infty a_n x^n \in \mathbb{Q}[[x]]$ is in the quotient field of $\mathbb{Z}[[x]]$, then there is some $\sum_{n=0}^\infty b_n x^n \in \mathbb{Z}[[x]]$ so that $\sum_{i=0}^n a_i b_{n-i}$,the coefficients of the product, are in $\mathbb{Z}$ for each n. In particular, $a_n b_0 \in \mathbb{Z} + \sum_{i=0}^{n-1} a_i\mathbb{Z}$. If $b_0 = 0$, we may divide the power series by the lowest power of x that appears to get a power series that satisfies the above condition and has a constant term. So we may assume $b_0 \neq 0$.

Assume that the first power series, with $a_i = 2^{-i^2}$, is in the quotient field of $\mathbb{Z}[[x]]$. Then $2^{-n^2}b_0 \in \mathbb{Z} + \sum_{i=0}^{n-1} 2^{-i^2}\mathbb{Z} = 2^{-(n-1)^2}\mathbb{Z}$. It follows that $2^{2n-1}|b_0$. But this must hold for all n, a contradiction.

Assume that the second power series, with $a_i = 1/i!$, is in the quotient field of $\mathbb{Z}[[x]]$. Then $b_0/n! \in \mathbb{Z} + \sum_{i=0}^{n-1}\mathbb{Z}\cdot 1/i! \subseteq \mathbb{Z}[1/(n-1)!]$. If n is prime, it follows that $n|b_0$. But this must hold for all primes n, a contradiction. ■

[lam@math] *Discussion.* I liked Anton's solution! The e^x example was cute; just don't assign it as homework to your Math 1B students. In the meantime, I have now found good references for this Exercise: see Hutchins's "Examples of Commutative Rings", pp. 102-103. Hutchins used the example $a_n = (n+1)^{-1}$. This does work but is a little surprising, since a_n goes to zero much more slowly than in the two examples above, and a_n fails the Ratio Test. But Hutchins's Example 96(b) is truly nice — except for the fact that he totally botched up his Taylor series! [I have come to find out that Hutchins's book is not error-free. For instance, in Example 93, he was confusing "completely normal" with "goodness" (that is, the $(*)$ property in our Lecture Notes). This makes Example 93 very confusing to follow. Fortunately, he realized this later, and acknowledged his mistake on the Errata sheet. In general, the (*) property *does not* imply "completely normal" — except for, say, valuation rings as we have seen.]

In Example 96(d), Hutchins wondered what is the integral closure of $\mathbb{Z}[[x]]$ in $\mathbb{Q}((x))$. I don't know the answer. [Gilmer: 1967] (referred to on p. 97) contains much information on $Q(R[[x]])$ for a general domain R. ■

Exercise III.22. *Let K be a field. If $\{R_i\}$ is a family of valuation rings of K forming a chain (w.r.t. inclusion), show that $R = \cap_i R_i \in Val(K)$. What about the case where $\{R_i\}$ does not form a chain?*

[David Brown, brownda@math] Suppose $0 \neq x \notin R$. Then there exists an i such that $x \notin R_i$. But then since the R_i form a chain, $x \notin R_j$ for all $j \geq i$. But then, since each R_j is a valuation ring, $x^{-1} \in R_j$ for all $j \geq i$. Since $\{R_i\}$ form a chain, $x^{-1} \in R_i$ for all i, so $x \in R$.

However, $2/3$ and $3/2 \notin \mathbb{Z}_{(2)} \cap \mathbb{Z}_{(3)}$ ■

Exercise III.23. *Let $R \subset S$ be rings, with $c_1, c_2 \in S$. If c_j is integral over $I_j \lhd R$ ($j = 1, 2$), show that c_1c_2 is integral over I_1I_2, and that $r_1c_1 + r_2c_2$ is integral over $I_1 + I_2$ for all $r_j \in R$.*

[annejls@math] Let C be the integral closure of R in S, and as usual let $C(I)$ denote the set of elements of S that are integral over I. Recall that by Prop. 1.6, if $I \lhd R$, then $C(I) = \sqrt{IC}$. So, to prove the first part, we need only show that $c_1c_2 \in \sqrt{(I_1I_2)C}$. We have from the proposition, $c_i \in \sqrt{I_iC}$, so $c_1^m \in I_1C$ and $c_2^n \in I_2C$ for some m, n. Thus, $(c_1c_2)^{\max(m,n)} \in I_1I_2C$, so $c_1c_2 \in \sqrt{I_1I_2C}$.

To prove the second part, we must show that $r_1c_1 + r_2c_2 \in \sqrt{(I_1 + I_2)C}$. However, C contains R, and $\sqrt{(I_1 + I_2)C}$ is an ideal of C, so we need only show that each $c_i \in \sqrt{(I_1 + I_2)C}$. This follows, because $c_i \in \sqrt{I_iC} \subset \sqrt{(I_1 + I_2)C}$. ■

Exercise III.24. *Let $K = k(x)$ where k is a field, and let $\pi(x) = x^n + a_1x^{n-1} + \cdots + a_n \in k[x]$ be irreducible and different from x. Let $R = k[x]_{(\pi)} \in Val_k(K)$, and write $y = 1/x$. By (4.23), there should exist a monic irreducible polynomial $\pi'(y) \in k[y]$ such that $R = k[y]_{(\pi')}$. Find $\pi'(y)$.*

[shenghao@math] $a_n \neq 0$, since if $a_n = 0$, then $x|\pi(x)$, and so $\pi(x)$ is irreducible only when $\pi(x) = x$, which has been excluded. Divide $\pi(x)$ by $a_n x^n$ we get $a_n^{-1} + a_1 a_n^{-1} y + \cdots + y^n$, and this is our $\pi'(y)$. ■

Exercise III.25. *Let $(R, \mathfrak{m})$ be a noetherian local domain with $m \neq 0$. If all nonzero ideals of R have the form $\mathfrak{m}^i$ $(i \geq 0)$, show that R is a DVR.*

[Manuel Reyes; mreyes@math] If $i \geq j$ we have $\mathfrak{m}^i \subseteq \mathfrak{m}^j$, so the ideals of R form a chain. So R is a valuation ring; in particular it is normal. Also, if $\mathfrak{p} = \mathfrak{m}^n \neq 0$ is a prime of R, then $\mathfrak{p} \supseteq \mathfrak{m}^n$ implies that $\mathfrak{p} \supseteq \mathfrak{m}$. So $\mathfrak{p} = \mathfrak{m}$ is maximal, and $\dim R = 1$. Now R is a noetherian normal domain of dimension 1, so R is a DVR by (4.4)(2). ■

[lam@math] Here's another way. By Nakayama, there exists $\pi \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then $(\pi) \neq \mathfrak{m}^i$ for $i \geq 2$ forces $(\pi) = \mathfrak{m}$. Now (4.4)(3) implies R is a DVR. ■

Exercise III.26. *Let $(R, \mathfrak{m})$ be a valuation ring of principal type. (1) Show that $\mathfrak{p} := \bigcap_{n=0}^{\infty} \mathfrak{m}^n \subsetneq \mathfrak{m}$, and that $\mathfrak{p}$ is a prime containing all nonmaximal primes of R. (2) If $\dim R = 2$, show that $\operatorname{Spec}(R) = \{(0), \mathfrak{p}, \mathfrak{m}\}$, and that $\mathfrak{p}$ is not f.g.*

[Manuel Reyes; mreyes@math] (1) Let $0 \neq \pi \in R$ be such that $\mathfrak{m} = (\pi)$. Assume for contradiction that $\mathfrak{m} = \mathfrak{m}^2$; then $\pi \in (\pi^2)$. So $\pi = r\pi^2$ for some $r \in R$, and because R is a domain this means that $1 = r\pi$. So $\pi \in U(R)$, contradicting that $\pi \in \mathfrak{m}$. Hence we must have $\mathfrak{p} \subseteq \mathfrak{m}^2 \subsetneq \mathfrak{m}$. By (4.8)(G), we know that $\mathfrak{p}$ is prime. Finally, let $\mathfrak{q}$ be a nonmaximal prime in R. Then because $\mathfrak{m} \nsubseteq \mathfrak{q}$, we must have $\mathfrak{q} \subseteq \mathfrak{p}$ by (4.8). So $\mathfrak{p}$ indeed contains all nonmaximal primes of R.

(2) Now suppose that $\dim(R) = 2$, and let $\mathfrak{q} \in \operatorname{Spec}(R) \setminus \{\mathfrak{p}, \mathfrak{m}\}$. Because $\mathfrak{q}$ is nonmaximal, $\mathfrak{q} \subseteq \mathfrak{p}$. But $\mathfrak{q} \neq \mathfrak{p}$ implies that

$$(0) \subseteq \mathfrak{q} \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}.$$

Then because $\dim(R) = 2$, we must have $\mathfrak{q} = (0)$. So $\operatorname{Spec}(R) = \{(0), \mathfrak{p}, \mathfrak{m}\}$. Now for any $a \in \mathfrak{p} \subsetneq \mathfrak{m} = (\pi)$, write $a = \pi b$. Then because $\pi \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, we must have $b \in \mathfrak{p}$. So $x = \pi b \in \mathfrak{m}\mathfrak{p}$ implies that $\mathfrak{p} = \mathfrak{m}\mathfrak{p}$. If $\mathfrak{p}$ were finitely generated, then Nakayama's lemma would imply that $\mathfrak{p} = (0)$, contradicting that $\dim R = 2$. So $\mathfrak{p}$ cannot be f.g. ■

Exercise III.27. *(This supersedes the earlier Exercise 27.) Let $\alpha \in K$, where K is the quotient field of a normal domain R. Let I be the kernel of the R-algebra homomorphism $\varphi : R[x] \to K$ defined by $\varphi(x) = \alpha$. Using (6.11), show that I is generated by a set of linear polynomials in $R[x]$. If R is a UFD, show that I is generated by a single linear polynomial.*

[los@math] Let J denote the subideal of I generated by the elements of I of degree 1. Let $f(x) = c_0 + c_1 x + \cdots + c_n x^n \in I$. We will show by induction on n that $f \in J$. For $n \leq 1$ there is nothing to show. Therefore assume $n > 1$. We show below that $c_n \alpha \in R$. Assume this is the case. Then the polynomial $g(x) = c_n x - c_n \alpha$ is either 0 or an element of I of degree 1. Therefore

$x^{n-1}g(x) \in J$. The polynomial $f_1(x) = f(x) - x^{n-1}g(x)$ has degree $< n$ and belongs to I, hence by the induction hypothesis actually belongs to J. This in turn shows that $f \in J$, which is what we wanted.

Next we show $c_n\alpha \in R$. For this, because R is normal it will be enough by (6.11) to show that $c_n\alpha \in V$ for every valuation ring V of K containing R. Let V be such a valuation ring, and v the associated valuation. If $\alpha \in V$, then it is clear that $c_n\alpha \in V$, because $c_n \in R \subseteq V$. Assume therefore that $\alpha \notin V$, or, equivalently, $v(\alpha) < 0$. From $f(\alpha) = 0$ we get the relation $-c_n\alpha^n = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$. Therefore we have

$$\begin{aligned} v(c_n\alpha) + (n-1)v(\alpha) = v(c_n\alpha^n) &\geq \min_{0 \leq i \leq n-1} v(c_i\alpha^i) \\ &= \min_{0 \leq i \leq n-1} (v(c_i) + iv(\alpha)) \\ &\geq (n-1)v(\alpha), \end{aligned}$$

the last inequality holding because $v(c_i) \geq 0$ and $v(\alpha) < 0$. Cancelling the term $(n-1)v(\alpha)$ on both sides, we obtain $v(c_n\alpha) \geq 0$. This means that $c_n\alpha \in V$, which was what we needed to show.

Now we prove the last statement. Assume that R is a unique factorization domain. Let $\{b_\lambda x - a_\lambda : \lambda \in \Lambda\}$ be the collection of nonzero linear polynomials in I. Thus for all λ we have $\alpha = a_\lambda/b_\lambda$. Let a/b be an expression for α in lowest form. This makes sense, because R is a unique factorization domain. It is then clear that the linear polynomial $bx - a$ belongs to I and divides every $b_\lambda x - a_\lambda$. Therefore I is generated by $bx - a$. ■

Exercise III.28. *Show that the valuation ring associated with the valuation v constructed in (5.18) indeed has residue field isomorphic to k as claimed.*

[los@math, anton@math] Recall that $(\Gamma, +, \leq)$ is an ordered abelian group, K is the field of fractions of the group algebra $k[\Gamma]$, and $v\left(\frac{f_\alpha t_\alpha + \cdots}{g_\beta t_\beta + \cdots}\right) = \alpha - \beta$, where $f_\alpha t_\alpha$ and $g_\beta t_\beta$ are the lowest order terms in the numerator and denominator, respectively.

The valuation ring R is the ring of quotients $\frac{f_\alpha t_\alpha + \cdots}{g_\beta t_\beta + \cdots}$ with $\beta \leq \alpha$, and the maximal ideal $\mathfrak{m}$ is the set of such terms with $\beta < \alpha$. It is clear that $R/\mathfrak{m}$ contains an isomorphic copy of k. Moreover, $\frac{f_\alpha t_\alpha + \cdots}{g_\alpha t_\alpha + \cdots} - \frac{f_\alpha}{g_\alpha} = \frac{g_\alpha(f_\alpha + \cdots) - f_\alpha(g_\alpha + \cdots)}{g_\alpha(g_\alpha t_\alpha + \cdots)} \in \mathfrak{m}$. That is, every element of $R \setminus \mathfrak{m}$ differs from an element of k by something in $\mathfrak{m}$. It follows that $R/\mathfrak{m} \cong k$. ■

Exercise III.29. *Prove the following criterion from Krull's Idealtheorie, S. 110:*

"Kriterium: $\mathfrak{V}$ ist dann und nur dann Bewertungsring, wenn in $\mathfrak{V}$ die Menge aller Nichteinheiten ein Ideal bildet und wenn jeder echte Zwischenring zwischen $\mathfrak{V}$ und dem Quotientenkörper $\mathfrak{K}$ ein Reziprokes einer Nichteinheit von $\mathfrak{V}$ enthält."

[Lars Kindler, lars_k@berkeley.edu] Upon request, here is a solution in German: Sei zunächst $\mathfrak{V}$ ein Bewertungsring. Dann ist $\mathfrak{V}$ lokaler Ring mit maximalem Ideal $\mathfrak{m} = \mathfrak{V} \setminus U(\mathfrak{V})$. Ist $\mathfrak{S}$ ein echter Zwischenring zwischen $\mathfrak{V}$ und $\mathfrak{K}$ und ist $a/b \in \mathfrak{S} \backslash \mathfrak{V}$, also $a, b \in \mathfrak{V}$, $b \in \mathfrak{m}$ und $b \not| a$, so ist $b = ab'$ für ein geeignetes $b' \in \mathfrak{V}$, da $\mathfrak{V}$ nach Vorraussetzung ein Bewertungsring ist, und $a/b = 1/b' \in \mathfrak{S} \setminus \mathfrak{V}$. Das wiederum bedeutet $b' \in \mathfrak{m}$, wie behauptet.

Umgekehrt sei nun $\mathfrak{V}$ ein Ring mit dem Ideal $\mathfrak{m} := \mathfrak{V} \backslash U(\mathfrak{V})$ und der Eigenschaft dass es zu jedem Zwischenring $\mathfrak{S} \supset \mathfrak{V}$ in $\mathfrak{K}$ ein $x \in \mathfrak{m}$ gibt, mit $1/x \in \mathfrak{S}$. Dann ist $\mathfrak{V}$ lokaler Ring mit maximalem Ideal $\mathfrak{m}$ und für ein Element $x \in U(\mathfrak{K})$ gilt nach Chevalleys Lemma $\mathfrak{m}\mathfrak{V}[x] \subsetneq \mathfrak{V}[x]$ oder $\mathfrak{m}\mathfrak{V}[x^{-1}] \subsetneq \mathfrak{V}[x^{-1}]$. Nach Vorraussetzung folgt nun $\mathfrak{V}[x] = \mathfrak{V}$ oder $\mathfrak{V}[x^{-1}] = \mathfrak{V}$, das heißt $\mathfrak{V}$ ist Bewertungsring. ■

Exercise III.30. *Let $v : k \twoheadrightarrow \Gamma_\infty$ be a valuation on a field k with valuation ring $(R, \mathfrak{m})$. For $f(x) = \sum_i a_i x^i \in k[x]$, define $v'(f) = \min\{v(a_i)\} \in \Gamma_\infty$. Show that v' is a valuation on $k[x]$, which extends uniquely to a valuation on $k(x)$ with valuation ring $R[x]_{\mathfrak{m}[x]}$ and the same value group Γ. (The residue field of this valuation ring is the rational function field $(R/\mathfrak{m})(x)$.)*

[Manuel Reyes; mreyes@math] First let $f(x) = \sum a_i x^i$ and $g(x) = \sum b_i x^i$ be any elements of $k[x]$. Choose a_m and b_n with minimal valuations among the coefficients of f and g, respectively, and such that m and n are minimal. We have $fg = \sum c_k x^k$, where $c_k = \sum_{i+j=k} a_i b_j$. First consider that because each $v(a_i b_j) = v(a_i) + v(b_j) \geq v(a_m) + v(b_n) = v(a_m b_n)$, we have $v(c_k) \geq \min\{v(a_i b_j) : i + j = k\} \geq v(a_m b_n)$ for all k. Now we claim that $v(c_{m+n}) = v(a_m b_n)$. Suppose that a pair of nonnegative integers $(i, j) \neq (m, n)$ is such that $i + j = m + n$. Then we must have $i < m$ or $j < n$, say $i < m$ without loss of generality. Then by minimality of m, this means that $v(a_i) > v(a_m)$. So $v(a_i b_j) > v(a_m b_j) \geq v(a_m b_n)$. Then Proposition (5.8) implies that $v(c_k) = v(a_m b_n)$. So

$$\begin{aligned} v'(fg) &= \min\{v(c_k)\} \\ &= v(c_{m+n}) \\ &= v(a_m b_n) \\ &= v(a_m) + v(b_n) \\ &= v'(f) + v'(g), \end{aligned}$$

showing that v' satisfies property (1) of valuations. Keeping the same notations as above, for all i we must have $v(a_i + b_i) \geq \min\{v(a_i), v(b_i)\} \geq \min\{v(a_m), v(b_n)\}$. So

$$\begin{aligned} v'(f+g) &= \min\{v(a_i + b_i)\} \\ &\geq \min\{v(a_m), v(b_n)\} \\ &= \min\{v'(f), v'(g)\}. \end{aligned}$$

Thus v' also satisfies property (2) for valuations, and v' is a valuation.

Proposition (5.9) now implies that v' extends uniquely to the quotient field $k(x)$ of $k[x]$. The fact that $(R, \mathfrak{m})$ is the valuation ring of v and the definition of v' together imply that

$$\begin{aligned} R[x] &= \{f \in k[x] : v'(f) \geq 0\}, \\ \mathfrak{m}[x] &= \{f \in k[x] : v'(f) > 0\}, \\ R[x] \smallsetminus \mathfrak{m}[x] &= \{f \in k[x] : v'(f) = 0\}. \end{aligned}$$

Let $S \subseteq k(x)$ be the valuation ring of v'; clearly $R[x]_{\mathfrak{m}[x]} \subseteq S$. So suppose that $\frac{f(x)}{g(x)} \in S$, with $g \neq 0$. This means that $v'\left(\frac{f}{g}\right) \geq 0$, or $v'(f) \geq v'(g)$ Let c be a (nonzero) coefficient of g with minimal valuation, so that $v'(g) = v(c)$. Then $v'\left(c^{-1}g\right) = 0$, implying that $c^{-1}g \in R[x] \smallsetminus \mathfrak{m}[x]$. It follows that $v'\left(c^{-1}f\right) \geq v'\left(c^{-1}g\right) = 0$, so that $c^{-1}f \in R[x]$. Hence $\frac{f}{g} = \frac{c^{-1}f}{c^{-1}g} \in R[x]_{\mathfrak{m}[x]}$, proving that $S = R[x]_{\mathfrak{m}[x]}$. ■

Exercise III.31. *Show that, in a valuation ring $(R, \mathfrak{m})$, $\mathfrak{m}$ is a principal ideal iff $\mathfrak{m}^n$ is a principal ideal for some $n \geq 1$.*

[Manuel Reyes; mreyes@math] The "only if" part being clear, let us prove the "if" direction. Suppose that $\mathfrak{m}^n$ is principal. If $\mathfrak{m}^n = 0$, then the fact that R is a domain implies that $\mathfrak{m} = 0$ is principal. Otherwise we have $\mathfrak{m}^n \neq 0$, which means that $\mathfrak{m} \neq 0$. In this case we want to show that R is of principal type. So assume for contradiction that this is not the case, namely $\mathfrak{m} = \mathfrak{m}^2$. Then $\mathfrak{m} = \mathfrak{m}^2 = \cdots = \mathfrak{m}^n$ is principal, contradicting that R was not of principal type. ■

Exercise III.32. *Show that a valuation ring R is a UFD iff R is a DVR or a field.*

[Manuel Reyes; mreyes@math] We will actually prove that for a valuation ring R, the following are equivalent:

(1) R is a UFD

(2) The principal ideals of R satisfy ACC

(3) R is a PID

(4) R is a DVR or a field.

The implication (4) $\Rightarrow$ (1) is clear,(1) $\Rightarrow$ (2) follows from (6.16), and (3) $\Rightarrow$ (4) is (4.4)(1). For (2) $\Rightarrow$ (3), let R be a valuation ring whose principal ideals satisfy the ACC. To see that R is a PID let $I \lhd R$, and let $\mathcal{F}$ be the family of principal ideals contained in I. Then $\mathcal{F}$ is nonempty since $(0) \subseteq I$. By the chain condition, $\mathcal{F}$ has a maximal element, say $(a) \subseteq I$. If $I \neq (a)$, there exists $b \in I \smallsetminus (a)$. Because R is a valuation ring (specifically, a Bezout ring), (a, b) is a principal ideal in I strictly containing (a), contradicting the maximality of (a). So $I = (a)$ is principal, and R is a PID. ■

[Lars Kindler, lars_k@berkeley.edu] First, let R be a UFD. By (4.9) it suffices to show that $\dim R \leq 1$ and that $\mathfrak{m}$ is principal. If $\dim R = 0$ then R is a field, so we may assume $\dim R > 0$. Let $\mathfrak{p} \neq (0)$ be a prime ideal in R. Then there is a prime element $p \in \mathfrak{p}$ and every element $x \in \mathfrak{m}$ is either in (p) or we have $x|p$. But $x|p$ also implies $x \in (p)$, since p is prime. Thus $\mathfrak{m} = (p) = \mathfrak{p}$, which shows that $\mathfrak{m}$ is principal and $\dim R = 1$, and hence R is a DVR. The converse is clear, since if R is a PID or a field then R is a UFD. ■

Exercise III.33. *For a normal domain R, show that every irreducible monic polynomial in $R[x]$ is prime.*

[Jonah (jblasiak@math)] Let K be the quotient field of R, and let $h(x)$ be an irreducible monic polynomial in $R[x]$. $K[x]$ is a UFD, so $h(x)$ factors (in $K[x]$) into a product of primes, and we may assume each of these primes is a monic polynomial. Let $f(x)$ be one such prime factor; then by normality of R and Monicity Lemma 3.2, $f(x) \in R[x]$. This holds for all prime factors, so by irreducibility of $h(x)$ in $R[x]$, there must only be one prime factor, i.e. h(x) is prime in $K[x]$. By Proposition 6.19, $h(x)$ is prime in $R[x]$. ■

Exercise III.34. *(Slight modification of (6.18).) If R is a UFD, show that, for any nonzero $a \in R$, every prime in Ass(R/aR) is principal. Show that the converse holds if R is a noetherian domain.*

[ecarter@math] Let R be a UFD, let a be a nonzero element of R, and let $\mathfrak{p}$ be the annihilator of some nonzero $b \in R/aR$. Write $a = p_1 \cdots p_n$, where each p_i is prime. Then since $a \in \mathfrak{p}$, we may suppose without loss of generality that $p_1 \in \mathfrak{p}$. Since a divides $p_1 b$ in R, we can write $p_1 b = a q_1 \cdots q_m$ where each q_i is prime. Since a does not divide b in R, none of the q_i's is an associate of p_1. Then $b = p_2 \cdots p_n q_1 \cdots q_m$. Then for any $c \in \mathfrak{p}$, a divides cb in R so that p_1 divides $c q_1 \cdots q_m$ in R. Therefore $c \in (p_1)$, which shows that $\mathfrak{p}$ is generated by p_1 as desired.

Conversely, suppose R is a noetherian domain and let $\mathfrak{P}$ be a nonzero prime ideal. Then there exists a nonzero $a \in \mathfrak{P}$, and $\mathfrak{P}$ contains a prime $\mathfrak{p}$ which is minimal over aR. Since $aR = \mathrm{ann}(R/aR)$, $\mathfrak{p} \in \mathrm{Ass}(R/aR)$ by propisition 6.4 of chapter I. Therefore $\mathfrak{p} = (p)$ for some $p \in \mathfrak{p}$, so $\mathfrak{P}$ contains a prime element. Therefore R is a UFD. ■

Exercise III.35. *(Slight modification of (6.20).) Let R be a domain whose principal ideals satisfy the ACC, and let S be a multiplicative set generated by a set of prime elements in R. Show that a prime $\mathfrak{P} \in$Spec(R) disjoint from S is principal iff its localization $\mathfrak{P}_S$ is principal.*

[annejls@math] The forward implication is clear: if $\mathfrak{P} = (a)$, then $\mathfrak{P}_S = (a)$. For the reverse, assume $\mathfrak{P}_S = (a/s)$, where $a \in R$, $s \in S$. We now repeat the argument in the proof of Nagata's theorem. Let S be generated by some prime elements π_i. If a is divisible by some π_i: $a = a'\pi_i$, then replace a by a'. Repeat as long as such a π_i exists; this process terminates in a finite number of steps by the ACC on principal ideals. Note that we have $\mathfrak{P}_S = (a)_S$. Now, we claim that $\mathfrak{P} = (a)_R$. Writing $\mathfrak{P} = \mathfrak{P}_S \cap R$, we see that $\mathfrak{P} \supset (a)_R$ follows. For the reverse containment, consider $c = a\frac{b}{t} \in \mathfrak{P}_S \cap R$, with $c, b \in R$, $t \in S$. Now, t is a product of π_i's, none of which divide a from our "trimming down," so t divides b. In other words, $b/t \in R$, so $c = a\frac{b}{t} \in (a)_R$, as desired. ■

Exercise III.36. *For any field k, use Nagata's theorem (6.20) to show that the noetherian ring R defined in (6.22) is a UFD. (**Hint.** Let $t = z^{-1}$, $u = t^3x$, and $v = t^2y$. Show that $z = u^2 + v^3$, and compute $R[z^{-1}]$.)*

[annejls@math] We have $R = k[x,y,z]/(x^2+y^3-z^7)$, where $k = \mathbb{F}_2$. R is Noetherian, so by Nagata's theorem, it suffices to show that R_z is a UFD. We have $t = z^{-1}$ a unit in R_z, so we can make the change of variables $u = t^3x$ and $v = t^2y$. That is, $R_z = k[x,y,z,t]/(x^2 + y^3 - z^7, tz - 1) = k[u,v,z,z^{-1}]/((u/t^3)^2 + (u/t^2)^3 - z^7, tz - 1) = k[u,v,z,z^{-1}]/(u^2 + v^3 - z) = k[u,v]_{u^2+v^3}$. This is the localization of a UFD, so it is a UFD. ■

Exercise III.37. *For any field k, show that the affine algebras $k[x,y,z]/(x^2 - yz)$ and $k[w,x,y,z]/(wx - yz)$ are not UFDs.*

[anton@math, los@math] We will use the following fact. *Lemma:* Let R be a domain, and let $a \in R$ be a nonzero element. Then the kernel of the map φ of $R[t]$-algebras from $R[s,t]$ to $R[t,t^{-1}]$ such that $\varphi(s) = a/t$ is generated by $st-a$. (In particular, this shows that the ideal generated by $st - a$ is prime.) *Proof:* Let $I = \ker(\varphi)$, and let $J = (st - a)$. It is clear that $J \subseteq I$. Any polynomial $f \in R[s,t]$ is congruent modulo J to one of the form $f_1(t)+sf_2(s)$. On the other hand, it is clear that any element of the kernel of φ that is of this form is zero. Therefore $I = J$. Set $A_1 = k[x,y,z]/(x^2-yz)$. By the lemma, A_1 is isomorphic to the subring $A_1' = k[x,y,x^2/y]$ of $B_1 = k[x,y,y^{-1}]$. (Here $R = k[x]$.) We will show that the element y of A_1' is irreducible. Suppose $y = fg$, with $f, g \in A_1'$. Since y is invertible in B_1, each of f and g must be invertible in B_1. The invertible elements of B_1 are precisely the monomials cy^n, with $n \in \mathbb{Z}$ and $c \in k$ a nonzero constant. However, it is clear that of these, only those with $n \geq 0$ belong to A_1'. One of f and g must actually therefore be a constant, hence invertible in A_1'. Thus y is irreducible in $A_1 \cong A_1'$. If A_1 is to be a UFD, y must also be prime. However, $A_1/(y) \cong k[z][x]/(x^2)$, which is not a domain. Therefore A_1 cannot be a UFD. Now let $A_2 = k[x,y,z,w]/(wx - yz)$. By the lemma, A_2 is isomorphic to the subring $A_2' = k[w,x,y,wx/y]$ of $B_2 = k[w,x,y,y^{-1}]$. Invoking identical arguments to those in the case of A_1, we see that y is irreducible in A_2. But $A_2/(y) \cong k[z][w,x]/(wx)$ is not a domain. Therefore y is not a prime element of A_2, and this ring is therefore not a UFD. ■

Exercise III.38. *Let $R \subseteq S$ be rings such that $S \setminus R$ is closed under multiplication. Show that R is integrally closed in S.*

[igusa@math] Assume that R is not integrally closed in S. Let $s \in S \setminus R$ be integral over R. Let $f(x) \in R[x]$ be a minimal (monic) polynomial satisfied by s over R. Write $f(x) = x^n + a_1x^{n-1} + ... + a_n$ with $a_i \in R$. Then in particular, $s^n + a_1s^{n-1} + ... + a_{n-1}s = \neg a_n \in R$. So, setting $t = s^{n-1}n + a_1s^{n-2} + ... + a_{n-1}$

we have that $st \in R$ and therefore $t \in R$ since $s \notin R$ and $S \setminus R$ is closed under multiplication. Letting $g(x) = x^{n-1}n + a_1 x^{n-2} + ... + a_{n-1} - t$ we have that $g \in R[x]$ and $g(s) = 0$ and $\deg(g) = \deg(f) - 1$ contradicting the minimality of f. ■

Exercise III.39. *Show that $S \supseteq R$ is an integral extension iff, for every $\mathfrak{P} \in \mathrm{Spec}(S)$, $S/\mathfrak{P}$ is an integral extension of $R/R \cap \mathfrak{P}$.*

[anton@math, los@math] The "only if" direction is clear. Assume therefore that S is an extension of R which is not integral. Let s be an element of S which is not integral over R, and let T be the multiplicative subset $\{f(s) : f \in R[T],\ f \text{ monic}\}$ of S. Since s, by hypothesis, is not integral over R, we have $0 \notin T$, hence $T^{-1}S \neq 0$. Let $\mathfrak{P}$ be the contraction to S of any prime ideal of $T^{-1}S$. Then $\mathfrak{P}$ is prime and $\mathfrak{P} \cap T = \emptyset$. This shows that for this choice of $\mathfrak{P}$, the quotient $S/\mathfrak{P}$ is not integral over $R/R \cap \mathfrak{P}$, completing the proof of the equivalence. ■