jdk carlson: Exercises to Atiyah and Macdonald's *Introduction to Commutative Algebra*, 2019 palingenesis

revision of November 8, 2021

FIX REFERENCES

LINK EXERCISES

DO CHAPTER 10 BODY OMISSION: COMPLETION

FIX TENSOR HEIGHT

CHECK SEQUENCE NOTATION THROUGHOUT

CHECK WHICH ASTERISK SOLUTIONS ARE STATED IN THE TEXT

Motivation

This note is intended to contain full solutions to all exercises in this venerable text,[1] as well as proofs of results omitted or left to the reader. It has none of the short text's pith or elegance, tending rather to the other extreme, citing chapter and verse from the good book and spelling out, step-by-step, things perhaps better left unsaid. It attempts to leave no "i" undotted, no "t" uncrossed, no detail unexplained. We are rather methodical in citing results when we use them, even if they've likely long been assimilated by the reader. Having found some solution sets online unclear at points (sometimes due to our own shortcomings, at other times due to theirs), we in this note strive to suffer from the opposite problem. Often we miss the forest for the trees. We prefer to see this not as "pedantic," but as "thorough." Sometimes we have included multiple proofs if we have found them, or failed attempts at proof if their failure seems instructive. The work is our own unless explicitly specified otherwise. It is hoped that the prolix and oftentimes plodding nature of these solutions will illuminate more than it conceals.

[1] [A–M]

Notation

Problems copied from the book and propositions are in italics, definitions emphasized (italic when surrounding text is Roman, and Roman when surrounding text is italic), and headings in bold or italics, following the book, and our solutions and occasional comments in Roman. Solutions that were later supplanted by better ones but still might potentially be worth seeing have usually been included, but as footnotes, decreasing both page count and legibility. Propositions, exercises, theorems, lemmas, and corollaries from the main body of the text will always be cited as "$(n.m)$" or $(n.m.$t)", where n is the chapter number, m the section number, and "t" an optional Roman numeral. For example, Proposition 1.10, part ii) is cited as "(1.10.ii)". Propositions or assertions proved in these solutions but not stated in the text are numbered with an asterisk, e.g. "Proposition 4.12*" and thereafter "(4.12*)". Exercises from the "EXERCISES" sections that follow each chapter, on the other hand, we cite with (square) brackets as e.g. "[3.1]" and "[1.2.i]". Displays in this document are referred back to as e.g. "Eq. 1.1" or "Seq. 2.2". Ends of proofs for exercises go unmarked, though we will sometimes mark proofs for discrete propositions we prove in the course of doing problems or expanding upon material.

Our mathematical notation follows that of the book, with a few exceptions as noted below. For strict set containment, "$\subset$" is supplanted by "$\subsetneq$", which is preferred for its lack of ambiguity; it is not to be confused with "$\not\subseteq$", which means "does not contain." "$\ni$" is a backward "$\in$", and means "contains the element" (rather than "such that"). The ideal generated by a set of elements is noted by listing them between parentheses: e.g., (x, y) is generated by $\{x, y\}$ and $(x_\alpha)_{\alpha \in \mathrm{A}}$ is generated by $\{x_\alpha : \alpha \in \mathrm{A}\}$. Contrastingly (and disagreeing with the book), we notate sequences and ordered lists with angle brackets: $\langle x, y\rangle$ is an ordered pair and $\langle x_\alpha\rangle_{\alpha \in \mathrm{A}}$ is a list of elements x_α indexed by a set A; in particular $\langle x_n\rangle_{n\in\mathbb{N}}$ is a sequence. Popular algebraic objects like $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ will be denoted in blackboard bold instead of bold, and 0 is included in $\mathbb{N}$. $\mathbb{F}_q$ denotes a ("the") finite field with q elements. "$\mathfrak{a} \lhd A$" means that $\mathfrak{a}$ is an ideal of the ring A. For set complement/exclusion, the symbol "\" replaces "—" on the off chance it might otherwise be confused with subtraction in cases (like topological groups) where both operations are feasible. The set of units of the ring A will be denoted by $A^\times$ rather than A^*, which is assigned a different meaning on p. 107. Bourbaki's word "quasi-compact" for the condition that every open cover has a finite subcover (not necessarily requiring the space be Hausdorff) we replace with "compact"; this usage seems to hold generally outside of algebraic geometry and most of the topologies we encounter here are not Hausdorff anyway. "ker", "im", and "coker" will go uncapitalized. $\mathfrak{N}(A)$ and $\mathfrak{R}(A)$ always denote, respectively, the nilradical and the Jacobson radical of the ring A; we just write $\mathfrak{N}$ and $\mathfrak{R}$ where no ambiguity is possible. The notation $\mathrm{id}_M \colon M \to M$ for the identity map replaces the book's "1" as slightly more unambiguous; 1 or 1_A is instead the unity of the ring A. "Multiplicative submonoid" is preferred to the book's "multiplicatively closed subset" as indicating that a subset of a ring contains 1 and is closed under the ring's multiplication. "Zorn's Lemma," capitalized, is the proper name of a result discovered by Kazimierz Kuratowski some thirteen years earlier than by Max Zorn. For a map $f\colon A \to B$, we can replace the arrow with "$\twoheadrightarrow$" when f is surjective, "$\rightarrowtail$" when it is injective, "$\hookrightarrow$" when it is an inclusion, and "$\xrightarrow{\sim}$" when it is an isomorphism. $A \cong B$ means that there exists some isomorphism between A and B, and $X \approx Y$ that X and Y are homeomorphic topological spaces. $[M]$ is the isomorphism class of M. For a map $f\colon A \to B$, if $U \subseteq A$ and $V \subseteq B$ are such that $f(U) \subseteq V$, then $f|_U^V$ is the restricted and corestricted map $U \to V$. Very occasionally, $\varkappa$, λ, μ may be cardinals (or homomorphisms), and indices α, β, γ may be ordinals. $\aleph_0$ is the cardinality of $\mathbb{N}$.

Rings and Ideals

Theorem 1.3. *Every ring $A \neq 0$ has at least one maximal ideal.*

In order to apply Zorn's Lemma, it is necessary to prove that if $\langle \mathfrak{a}_\alpha \rangle_{\alpha \in \mathrm{A}}$ is a chain of ideals (meaning, recall, that for all α, $\beta \in \mathrm{A}$ we have $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ or $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$) then the union $\mathfrak{a} = \bigcup_{\alpha \in \mathrm{A}} \mathfrak{a}_\alpha$ is an ideal. Indeed, if a, $b \in \mathfrak{a}$, then there are α, $\beta \in \mathrm{A}$ such that and $a \in \mathfrak{a}_\alpha$ and $b \in \mathfrak{a}_\beta$. Without loss of generality, suppose $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$. Then a, $b \in \mathfrak{a}_\beta$, so since $\mathfrak{a}_\beta$ is an ideal we have $a - b \in \mathfrak{a}_\beta \subseteq \mathfrak{a}$. If $x \in A$ and $a \in \mathfrak{a}$, then there is $\alpha \in \mathrm{A}$ such that $a \in \mathfrak{a}_\alpha$. As $\mathfrak{a}_\alpha$ is an ideal, $xa \in \mathfrak{a}_\alpha \subseteq \mathfrak{a}$. Therefore $\mathfrak{a}$ is an ideal.

Exercise 1.12.
i) $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

For each $a \in \mathfrak{a}$ we have $a\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}$, so $a \in (\mathfrak{a} : \mathfrak{b})$.

ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.

By definition, for $x \in (\mathfrak{a} : \mathfrak{b})$ we have $x\mathfrak{b} \subseteq \mathfrak{a}$.

iii) $\big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = \big((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}\big)$.

$$x \in \big((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}\big) \iff x\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b}) \iff x\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{a} \iff x \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c});$$
$$x \in \big((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b}\big) \iff x\mathfrak{b} \subseteq (\mathfrak{a} : \mathfrak{c}) \iff x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a} \iff x \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c}).$$

iv) $\big(\bigcap_i \mathfrak{a}_i : \mathfrak{b}\big) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$.

$$x \in \Big(\bigcap_i \mathfrak{a}_i : \mathfrak{b}\Big) \iff x\mathfrak{b} \subseteq \bigcap_i \mathfrak{a}_i \iff \forall i\ (x\mathfrak{b} \subseteq \mathfrak{a}_i) \iff x \in \bigcap_i (\mathfrak{a}_i : \mathfrak{b}).$$

v) $\big(\mathfrak{a} : \sum_i \mathfrak{b}_i\big) = \bigcap_i (\mathfrak{a} : \mathfrak{b}_i)$.

$$x \in \Big(\mathfrak{a} : \sum_i \mathfrak{b}_i\Big) \iff \mathfrak{a} \supseteq x\Big(\sum_i \mathfrak{b}_i\Big) = \sum_i x\mathfrak{b}_i \iff \forall i\ (x\mathfrak{b}_i \subseteq \mathfrak{a}) \iff x \in \bigcap_i (\mathfrak{a} : \mathfrak{b}_i).$$

For an A-module M and subsets $N \subseteq M$ and $E \subseteq A$, define $(N : E) := \{m \in M : Em \subseteq N\}$; for subsets N, $P \subseteq M$ and $E \subseteq A$, define $(N : P) := \{a \in A : aP \subseteq N\}$.

Note for future use that then ii) holds equally well for subsets $\mathfrak{a}$, $\mathfrak{b} \subseteq M$, or $\mathfrak{b} \subseteq A$ and $\mathfrak{a} \subseteq M$; iii) holds for $\mathfrak{a}$, $\mathfrak{b} \subseteq M$ and $\mathfrak{c} \subseteq A$; and iv) and v) hold for modules $\mathfrak{a}$, $\mathfrak{a}_i$ and modules *or ideals* $\mathfrak{b}$, $\mathfrak{b}_i$.

Exercise 1.13.
—i) $\mathfrak{a} \subseteq \mathfrak{b} \implies r(\mathfrak{a}) \subseteq r(\mathfrak{b})$.

If $x \in r(\mathfrak{a})$, for some $n > 0$ we have $x^n \in \mathfrak{a} \subseteq \mathfrak{b}$, so $x \in r(\mathfrak{b})$.

0) $r(\mathfrak{a}^n) = r(\mathfrak{a})$ *for all* $n > 0$.

$\mathfrak{a}^n \subseteq \mathfrak{a}$, so by part —i) we have $r(\mathfrak{a}^n) \subseteq r(\mathfrak{a})$. If $x \in r(\mathfrak{a})$, then for some $m > 0$, $x^m \in \mathfrak{a}$. But then $x^{mn} \in \mathfrak{a}^n$ and $x \in r(\mathfrak{a}^n)$.

i) $r(\mathfrak{a}) \supseteq \mathfrak{a}$.

For each $a \in \mathfrak{a}$ we have $a^1 \in \mathfrak{a}$, so $a \in r(\mathfrak{a})$.

ii) $r\big(r(\mathfrak{a})\big) = r(\mathfrak{a})$.

$$x \in r\big(r(\mathfrak{a})\big) \iff \exists n > 0\,\big(x^n \in r(\mathfrak{a})\big) \iff \exists n, m > 0\,\big((x^n)^m = x^{mn} \in \mathfrak{a}\big) \iff x \in r(\mathfrak{a}).$$

iii) $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$.

For the first equality, note $(\mathfrak{a}\cap\mathfrak{b})^2 \subseteq \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, so by parts 0) and —i), $r(\mathfrak{a}\cap\mathfrak{b}) = r\big((\mathfrak{a}\cap\mathfrak{b})^2\big) \subseteq r(\mathfrak{a}\mathfrak{b}) \subseteq r(\mathfrak{a}\cap\mathfrak{b})$. For the second, note that if $m, n > 0$ are such that $x^m \in \mathfrak{a}$ and $x^n \in \mathfrak{b}$, then $x^{\max\{m,n\}} \in \mathfrak{a}\cap\mathfrak{b}$, and conversely.

iv) $r(\mathfrak{a}) = (1) \iff \mathfrak{a} = (1)$.

If $r(\mathfrak{a}) = (1)$, then $1 \in r(\mathfrak{a})$, so for some n we have $1 = 1^n \in \mathfrak{a}$, and then $\mathfrak{a} = (1)$.

v) $r(\mathfrak{a}+\mathfrak{b}) = r\big(r(\mathfrak{a}) + r(\mathfrak{b})\big)$.

Since $\mathfrak{a}, \mathfrak{b} \subseteq \mathfrak{a}+\mathfrak{b}$, by part —i) we have $r(\mathfrak{a}), r(\mathfrak{b}) \subseteq r(\mathfrak{a}+\mathfrak{b})$, so $r(\mathfrak{a}) + r(\mathfrak{b}) \subseteq r(\mathfrak{a}+\mathfrak{b})$. By parts —i), and ii), we see $r\big(r(\mathfrak{a}) + r(\mathfrak{b})\big) \subseteq r\big(r(\mathfrak{a}+\mathfrak{b})\big) = r(\mathfrak{a}+\mathfrak{b})$. Conversely, by part i), we have $\mathfrak{a} \subseteq r(\mathfrak{a})$ and $\mathfrak{b} \subseteq r(\mathfrak{b})$, so adding, $\mathfrak{a}+\mathfrak{b} \subseteq r(\mathfrak{a}) + r(\mathfrak{b})$. By part —i), $r(\mathfrak{a}+\mathfrak{b}) \subseteq r\big(r(\mathfrak{a}) + r(\mathfrak{b})\big)$.

vi) If $\mathfrak{p}$ is prime, $r(\mathfrak{p}^n) = \mathfrak{p}$ for all $n > 0$.

By part 0), $r(\mathfrak{p}^n) = r(\mathfrak{p})$. By (1.14), $r(\mathfrak{p}) = \mathfrak{p}$.

Proposition 1.17. *iv*) Both extension and contraction are order-preserving with respect to containment; i.e. for ideals $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$ of A we have $\mathfrak{a}_1^e \subseteq \mathfrak{a}_2^e$ and for ideals $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ of B we have $\mathfrak{b}_1^c \subseteq \mathfrak{b}_2^c$.*[1]

If $\mathfrak{a}_1 \subseteq \mathfrak{a}_2$, then $f(\mathfrak{a}_1) \subseteq f(\mathfrak{a}_2)$, so $\mathfrak{a}_1^e = Bf(\mathfrak{a}_1) \subseteq Bf(\mathfrak{a}_2) = \mathfrak{a}_2^e$. If $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$, then $\mathfrak{b}_1^c = f^{-1}(\mathfrak{b}_1) \subseteq f^{-1}(\mathfrak{b}_2) = \mathfrak{b}_2^c$.

Exercise 1.18. *Let $f : A \to B$ be a ring homomorphism, and let $\mathfrak{a}$, $\mathfrak{a}_j$ be ideals of A and $\mathfrak{b}$, $\mathfrak{b}_j$ ideals of B.*
$\big(\sum \mathfrak{a}_j\big)^e = \sum \mathfrak{a}_j^e$.

Because the homomorphism f distributes over finite sums and multiplication of ideals distributes over addition,

$$\Big(\sum \mathfrak{a}_j\Big)^e = Bf\Big(\sum \mathfrak{a}_j\Big) = B \cdot \sum f(\mathfrak{a}_j) = \sum Bf(\mathfrak{a}_j) = \sum \mathfrak{a}_j^e.$$

$(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e$.

Because $1 \in B$, we have $B = BB$; as f is a homomorphism and ideal multiplication commutes,

$$(\mathfrak{a}_1\mathfrak{a}_2)^e = Bf(\mathfrak{a}_1\mathfrak{a}_2) = BBf(\mathfrak{a}_1)f(\mathfrak{a}_2) = Bf(\mathfrak{a}_1)Bf(\mathfrak{a}_2) = \mathfrak{a}_1^e\mathfrak{a}_2^e.$$

$\big(\sum \mathfrak{b}_j\big)^c \supseteq \sum \mathfrak{b}_j^c$.

Given any finitely many nonzero $a_j \in f^{-1}(\mathfrak{b}_j)$, we have $f\big(\sum_j a_j\big) = \sum_j f(a_j) \in \sum_j \mathfrak{b}_j$.

$(\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c$.

If $f(a_j) \in \mathfrak{b}_j$ for $j = 1, 2$, then $f(a_1a_2) = f(a_1)f(a_2) \in \mathfrak{b}_1\mathfrak{b}_2$.

$\big(\bigcap_j \mathfrak{a}_j\big)^e \subseteq \bigcap_j \mathfrak{a}_j^e$.

$$\Big(\bigcap \mathfrak{a}_j\Big)^e = Bf\Big(\bigcap \mathfrak{a}_j\Big) \subseteq B \cdot \bigcap f(\mathfrak{a}_j) = \bigcap Bf(\mathfrak{a}_j) = \bigcap \mathfrak{a}_j^e.$$

$\big(\bigcap \mathfrak{b}_j\big)^c = \bigcap \mathfrak{b}_j^c$.

$$\Big(\bigcap \mathfrak{b}_j\Big)^c = f^{-1}\Big(\bigcap \mathfrak{b}_j\Big) = \bigcap f^{-1}(\mathfrak{b}_j) = \bigcap \mathfrak{b}_j^c.$$

$(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e)$.

[1] This is trivial, but the book never seems to explicitly state that it is the case, so here is a place to cite when we use it.

By the result on multiplying extended ideals, and since $(\mathfrak{a}_1 : \mathfrak{a}_2)\mathfrak{a}_2 \subseteq \mathfrak{a}_1$ by (1.13.ii), we have

$$(\mathfrak{a}_1 : \mathfrak{a}_2)^e \mathfrak{a}_2^e = \big((\mathfrak{a}_1 : \mathfrak{a}_2)\mathfrak{a}_2\big)^e \overset{(1.17.\text{iv}^*)}{\subseteq} \mathfrak{a}_1^e.$$

$(\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c)$.

By the result on multiplying contracted ideals, and since $(\mathfrak{b}_1 : \mathfrak{b}_2)\mathfrak{b}_2 \subseteq \mathfrak{b}_1$ by (1.13.ii),

$$(\mathfrak{b}_1 : \mathfrak{b}_2)^c \mathfrak{b}_2^c \subseteq \big((\mathfrak{b}_1 : \mathfrak{b}_2)\mathfrak{b}_2\big)^c \overset{(1.17.\text{iv}^*)}{\subseteq} \mathfrak{b}_1^c.$$

$r(\mathfrak{a})^e \subseteq r(\mathfrak{a}^e)$.

Let $b = \sum_j b_j f(x_j)$ for $b_j \in B$ and $x_j^{n_j} \in \mathfrak{a}$. Some $f(x_j)^{n_j}$ divides each term of $b^{\sum_j (n_j - 1) + 1}$, so $b \in r(\mathfrak{a}^e)$.

$r(\mathfrak{b})^c = r(\mathfrak{b}^c)$.

$$a \in f^{-1}\big(r(\mathfrak{b})\big) \iff \exists n > 0 \,\big(f(a^n) = f(a)^n \in \mathfrak{b}\big) \iff \exists n > 0 \,\big(a^n \in f^{-1}(\mathfrak{b})\big) \iff a \in r\big(f^{-1}(\mathfrak{b})\big).$$

The set of extended ideals is closed under sum and product, and the set of contracted ideals is closed under intersection, quotient, and radical.

It now suffices to show $(\mathfrak{b}_1^c : \mathfrak{b}_2^c) = (\mathfrak{b}_1^{ce} : \mathfrak{b}_2^{ce})^c$. Indeed, using the preceding facts and (1.17.ii),

$$a \in (\mathfrak{b}_1^c : \mathfrak{b}_2^c) \iff a\mathfrak{b}_2^c \subseteq \mathfrak{b}_1^c \implies f(a)f(\mathfrak{b}_2^c) \subseteq f(\mathfrak{b}_1^c) \iff f(a)\mathfrak{b}_2^{ce} \subseteq \mathfrak{b}_1^{ce} \iff a \in (\mathfrak{b}_1^{ce} : \mathfrak{b}_2^{ce})^c;$$
$$a \in (\mathfrak{b}_1^{ce} : \mathfrak{b}_2^{ce})^c \iff f(a)\mathfrak{b}_2^{ce} \subseteq \mathfrak{b}_1^{ce} \implies a\mathfrak{b}_2^c \subseteq f^{-1}\big(f(a)\big)\mathfrak{b}_2^c = f^{-1}\big(f(a)\big)\mathfrak{b}_2^{cec} \subseteq \mathfrak{b}_1^{cec} = \mathfrak{b}_1^c \implies a \in (\mathfrak{b}_1^c : \mathfrak{b}_2^c).$$

EXERCISES

Let x be a nilpotent element of a ring A. Show that $1 + x$ is a unit of A. Deduce that the sum of a nilpotent element and a unit is a unit.

The nilradical is a subset of the Jacobson radical, and by (1.9), for any $x \in \mathfrak{N}$ we have $1 + x = 1 - (-x)$ a unit.[2] Now if x is nilpotent and u a unit, then $u^{-1}x$ is nilpotent as well and $u + x = u(1 + u^{-1}x)$ is invertible.

Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$. Prove that
i) f is a unit in $A[x] \iff a_0$ is a unit in A and $a_1, \ldots, a_n$ are nilpotent.

$\Longleftarrow$: If a_0 is a unit and the a_j are nilpotent for $j \geq 1$, then since $\mathfrak{N}$ is an ideal by (1.7), the $a_j x^j$ are nilpotent for $j \geq 1$ and $y = \sum_{j=1}^n a_j x^j$ is nilpotent, and by [1.1], $f = a_0 + y$ is invertible.

$\Longrightarrow$: We induct on $\deg f$. The degree zero case is trivial. Suppose we have proved the result for degrees $< n$, and let $\deg f = n$. Suppose that f is a unit, with inverse $g = \sum_{i=0}^m b_i x^i$; assume for uniformity of notation that $a_j = b_i = 0$ for integers i, j outside the ranges indicated. Write $c_k = \sum_{j=0}^k a_j b_{k-j}$ for $0 \leq k \leq m + n$, so that $1 = fg = \sum_k c_k x^k$. We have $1 = c_0 = a_0 b_0$, so a_0 and b_0 are units, and the other c_k are all 0. Note in particular $0 = c_{m+n} = a_n b_m$: a power of a_n annihilates b_m. This is the $r = 1$ case of a general claim that $a_n^r b_{m+1-r} = 0$ for $1 \leq r \leq m + 1$. Indeed, fix such an r and inductively assume $a_n^s b_{m+1-s} = 0$ for $1 \leq s \leq r$. We have

$$0 = c_{m+n-r} = b_{m-r} a_n + b_{m-r+1} a_{n-1} + \cdots + b_m a_{n-r}.$$

Multiplying by a_n^r, we get

$$0 = a_n^{r+1} b_{m-r} + \underbrace{a_n^r b_{m-r+1}}_{0}(a_{n-1} a_n) + \cdots + \underbrace{a_n b_m}_{0}(a_{n-r} a_n^{r-1}),$$

[2] Alternatively, let $n > 0$ be minimal such that $x^n = 0$, and let $y = \sum_{j=0}^{n-1} (-x)^j$; then

$$(1 + x)y = \sum_{j=0}^{n-1} (-x)^j - \sum_{j=1}^{n} (-x)^j = 1 \pm x^n = 1.$$

so $0 = a_n^{r+1} b_{m-r}$, completing the induction. When we get to $r = m$ we see $b_0 a_n^{m+1} = 0$, so since b_0 is a unit, a_n is nilpotent. Hence $a_n x^n$ is nilpotent, and by [1.1], $f - a_n x^n$ is a unit. This has degree $< n$, so by induction, $a_1, \ldots, a_{n-1}$ are nilpotent.

ii) f is nilpotent $\Longleftrightarrow$ $a_0, a_1, \ldots, a_n$ are nilpotent.

$\Longleftarrow$: Since $\mathfrak{N}(A[x])$ is an ideal by (1.7), if all $a_j \in \mathfrak{N}$, then all $a_j x^j \in \mathfrak{N}$, so $f = \sum a_j x^j \in \mathfrak{N}$.

$\Longrightarrow$: On the other hand, for each prime $\mathfrak{p} \lhd A$, we have $\mathfrak{p}[x] \lhd A[x]$ prime since it is the kernel of the surjection $A[x] \twoheadrightarrow (A/\mathfrak{p})[x]$, whose image is an integral domain by [1.2.iii]: if $a_j x^j \in A[x]$ is a zero-divisor, there exists a nonzero $c \in A$ with $c \cdot \sum a_j x^j = 0$, so each $c \cdot a_j = 0$, and hence $a_j = 0$ as $A/\mathfrak{p}$ is an integral domain. Thus

$$\mathfrak{N}(A[x]) \overset{(1.8)}{\subseteq} \bigcap (\mathfrak{p}[x]) = \left(\bigcap \mathfrak{p}\right)[x] = \mathfrak{N}(A)[x].^{3}$$

iii) f is a zero-divisor $\Longleftrightarrow$ there exists $a \neq 0$ in A such that $af = 0$.

The "if" direction is trivial; the "only if" we prove by induction. We prove something slightly more specific: if a nonzero $g = b_0 + b_1 x + \cdots + b_m x^m \in (0 : f)$ is of least possible degree m, then $b_m f = 0$.

For the base case, if $f = a_0$ has degree zero, then of course $b_m a_0 = b_m f = 0$. Suppose inductively that for all zero-divisors f' of degree $n - 1$ we know there is some $b \in A$ such that $bf' = 0$. Let $\deg f = n$ and g and m be as before. Since $fg = 0$, also $a_n b_m = 0$, so $\deg(a_n g) < m$. As $a_n g f = 0$ as well, by minimality of m, we know $a_n g = 0$. Now $0 = fg - a_n x^n g = (f - a_n x^n) g$. Since $f' = f - a_n x^n$ is of degree $< n$, by the inductive assumption $b_m f' = 0$, so $b_m f = b_m a_n x^n + b_m f' = 0$, completing the induction.

iv) f is said to be primitive *if $(a_0, a_1, \ldots, a_n) = (1)$. Prove that if $f, g \in A[x]$, then fg is primitive $\Longleftrightarrow$ f and g are primitive.*

We can actually let $A[x] := A[x_1, \ldots, x_r]$ be a polynomial ring in several indeterminates, writing x for the sequence $x_1, \ldots, x_r$, in the proof below.

Note that a polynomial is primitive just if no maximal ideal contains all its coefficients. Let $\mathfrak{m} \lhd A$ be maximal. Since $A/\mathfrak{m}$ is a field, $A[x]/\mathfrak{m}[x] \cong (A/\mathfrak{m})[x]$ is an integral domain. Thus

$$f, g \notin \mathfrak{m}[x] \Longleftrightarrow \bar{f}, \bar{g} \neq 0 \text{ in } (A/\mathfrak{m})[x] \Longleftrightarrow \overline{fg} \neq 0 \text{ in } (A/\mathfrak{m})[x] \Longleftrightarrow fg \notin \mathfrak{m}[x].$$

Therefore no maximal ideal contains all the coefficients of fg just if the same holds for f and g.[4]

This result is called *Gauß's Lemma* and was originally proven in his *Disquisitiones Arithmeticae* for $A = \mathbb{Z}$. Cf. also [9.2].

Generalize the results of Exercise 2 to a polynomial ring $A[x_1, \ldots, x_r]$ in several indeterminates.

We start with an assumption about the ring $B = A[x_1, \ldots, x_r]$ and prove the corresponding statement about the ring $B[y] = A[x_1, \ldots, x_r, y]$ in one more indeterminate. For a multi-index $\alpha = \langle j_1, \ldots, j_r \rangle$ we write $a_{\alpha,k} := a_{j_1,\ldots,j_r,k}$ and $x^\alpha := x_1^{j_1} \cdots x_r^{j_r}$. If $f \in B[y]$, we can write it as $f = \sum_{\alpha,k} a_{\alpha,k} x^\alpha y^k = \sum_k h_k y^k$, where $h_k = \sum_\alpha a_{\alpha,k} x^\alpha \in B$.

i) f is a unit in $B[y]$ $\Longleftrightarrow$ $a_{0,0}$ is a unit in A and all other $a_{\alpha,k}$ are nilpotent.

$$f \in B[y]^\times \underset{B[y]/B}{\overset{[1.2.\text{i}]}{\Longleftrightarrow}} h_0 \in B^\times \text{ and other } h_k \in \mathfrak{N}(B) \underset{B/A}{\overset{[1.3.\text{i}],[1.3.\text{ii}]}{\Longleftrightarrow}} a_{0,0} \in A^\times \text{ and other } a_{\alpha,k} \in \mathfrak{N}(A).$$

[3] Alternate proof: suppose $f^m = 0$ and j is minimal with $a_j \neq 0$. Then the lowest term $a_j^m x^{jm}$ of f is 0, so a_j is nilpotent and $f - a_j x^j$ is nilpotent. Repeatedly lopping off lowest terms, we see each $a_j \in \mathfrak{N}(A)$.

[4] We also have the following generalization of the classical proof. Suppose f is not primitive, so that for some maximal $\mathfrak{m} \lhd A$ we have $f \in \mathfrak{m}[x]$. Then $fg \in \mathfrak{m}[x]$, so fg is not primitive. The same holds if g is not primitive.

Now suppose fg is not primitive; we show one of f and g is also not. There is a maximal ideal $\mathfrak{m}$ containing all of the coefficients $c_r = \sum_j a_j b_{r-j}$ of fg; we suppose that neither all of the a_j nor all of the b_k lie in $\mathfrak{m}$ and obtain a contradiction. There are a least J and a least K such that $a_J, b_K \notin \mathfrak{m}$. Now $\mathfrak{m}$ contains the coefficient $c_{J+K} = \sum_{j<J} a_j b_{J+K-j} + a_J b_K + \sum_{k<K} a_{J+K-k} b_k$, and each of the sums is in $\mathfrak{m}$ by assumption, so $a_J b_K \in \mathfrak{m}$ as well. Since $\mathfrak{m}$ is prime, we have a_J or b_K in $\mathfrak{m}$, a contradiction.

Use of [1.3.ii] is permissible because it is independent, but we could also perform the induction in both exercises at the same time.

ii) f is nilpotent $\iff$ all $a_{\alpha,k}$ are nilpotent.

$$f \in \mathfrak{N}\big(B[y]\big) \underset{B[y]/B}{\overset{[1.2.ii]}{\iff}} \text{all } h_k \in \mathfrak{N}(B) \underset{B/A}{\overset{[1.3.ii]}{\iff}} \text{all } a_{\alpha,k} \in \mathfrak{N}(A).$$

iii) f is a zero-divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$.

The inductive assumption will be that if $g \in B$ is a zero-divisor, and $b \in B$ is of minimal multidegree α (in the reverse lexicographic order) such that $bg = 0$, then if a is the coefficient of the leading term of b, we have $ag = 0$.

The "if" is again trivial. For the "only if," suppose f is a zero-divisor in $B[y]$. By [1.2], there exists a nonzero $b \in B$ such that $bf = 0$. Thus $bh_k = 0$ for each k. By the inductive assumption the highest coefficient $a \in A$ of b is such that $ah_k = 0$ for each k. Then $af = 0$.

iv) Prove for $f, g \in A[x_1, \ldots, x_r]$ that fg is primitive over $A \iff f$ and g are primitive over A.

The proof in [1.2.iv] goes through equally well in this case.

In the ring $A[x]$, the Jacobson radical is equal to the nilradical.

We know $\mathfrak{N} \subseteq \mathfrak{R}$ by (1.8), since maximal ideals are prime, so it remains to show all elements of $\mathfrak{R}$ are nilpotent. Let $f = \sum a_j x^j \in \mathfrak{R}$, where $a_j \in A$. By (1.9), $1 - xf$ is a unit. By [1.2.i], then, all $a_j \in \mathfrak{N}$, so by [1.2.ii], $f \in \mathfrak{N}$.

Let A be a ring and let $A[[x]]$ be the ring of formal power series $f = \sum_{n=0}^{\infty} a_n x^n$ with coefficients in A. Show that

i) f is a unit in $A[[x]] \iff a_0$ is a unit in A.

$\Longleftarrow$: Supposing a_0 is a unit, we construct an inverse $g = \sum_m b_m x^m$ to f. Let $b_0 = a_0^{-1}$. We want $fg = \sum_j c_j x^j = 1$, so for $j \geq 1$ we want $c_j = \sum_{n=0}^{j} a_n b_{j-n} = 0$. Now suppose we have found satisfactory coefficients b_j for $j \leq k$. We need $c_{k+1} = a_0 b_{k+1} + \sum_{n=1}^{k+1} a_n b_{k+1-n} = 0$; but we can solve this to find the solution $b_{k+1} = -a_0^{-1}\big(\sum_{n=1}^{k+1} a_n b_{k+1-n}\big)$. Since we can do this for all k, we have constructed an inverse to f.

$\Longrightarrow$: If $g = \sum_m b_m x^m$ is an inverse of f, then $fg = 0$ implies $a_0 b_0 = 1$ so that a_0 is a unit.

ii) If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. Is the converse true?

The two proofs of "$\Longrightarrow$" in [1.2.ii] both hold, *mutatis mutandis*, here.

The converse is untrue. Let $B = C[y_1, y_2, \ldots]$ be a polynomial ring in countably many indeterminates over an integral domain C, and let $\mathfrak{b} = (y_1, y_2^2, y_3^3, \ldots)$ be the smallest ideal containing each y_n^n for $n \geq 1$. Then writing z_n for the image of y_n in $A = B/\mathfrak{b}$, we have $z_n^n = 0$ and $z_n^{n-1} \neq 0$. Thus an element of A is equal to zero just if, written as a polynomial in the z_n over C, each term is divisible by some z_n^n. Now let $f = \sum_{n=0}^{\infty} z_n x^n \in A[[x]]$. By construction, each coefficient is nilpotent. However, for each n, one term of the coefficient in A of $x^{n(n+1)}$ in f^n is z_{n+1}^n, which is nonzero and cannot be cancelled, so $f^n \neq 0$.

iii) f belongs to the Jacobson radical of $A[[x]] \iff a_0$ belongs to the Jacobson radical of A.

If the constant coefficient of $g \in A[[x]]$ is $b_0 \in A$, then the constant coefficient of $1 - fg$ is $1 - a_0 b_0$. Now

$$f \in \mathfrak{R}\big(A[[x]]\big) \overset{(1.9)}{\iff} \forall g \in A[[x]]\ \big(1 - fg \in A[[x]]^{\times}\big) \overset{[1.5.i]}{\iff} \forall b_0 \in A\ \big(1 - a_0 b_0 \in A^{\times}\big) \overset{(1.9)}{\iff} a_0 \in \mathfrak{R}(A).$$

iv) The contraction of a maximal ideal $\mathfrak{m}$ of $A[[x]]$ is a maximal ideal of A, and $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x.

Since $x \in A[[x]]$ has constant term $0 \in \mathfrak{R}(A)$, by iii) above, $x \in \mathfrak{R}\big(A[[x]]\big)$, and hence $(x) \subseteq \mathfrak{m}$. As $\mathfrak{m} \backslash (x) = \mathfrak{m}^c$, we get $\mathfrak{m} = \mathfrak{m}^c + (x)$. Now $A/\mathfrak{m}^c \cong A[[x]]/\mathfrak{m}$ is a field, so $\mathfrak{m}^c \lhd A$ is maximal.[5]

[5] I was tempted to use here that $\mathfrak{a}^e = \mathfrak{a}A[[x]] = \mathfrak{a}[[x]]$ for any $\mathfrak{a} \lhd A$, but it turns out this is wrong in general. It does hold for finitely generated $\mathfrak{a}$ (see [Eisenbud, Ex. 7.13]), and it is true ([4.7.i]) that $\mathfrak{a}A[x] = \mathfrak{a}[x]$ in $A[x]$, but there are counterexamples if $\mathfrak{a}$ is not finitely generated. For example, as in part ii) let C be a ring and $\mathfrak{b} = (y_1, y_2, y_3, \ldots)$ in $B = C[y_1, y_2, y_3, \ldots]$. Then $\sum y_n x^n$ is in $\mathfrak{b}[[x]]$ but not in $\mathfrak{b}B[[x]]$. To see this, suppose not; then there is a finite collection of $b_j \in \mathfrak{b}$ and there are $b'_{j,n} \in B$ such that $\sum y_n x^n = \sum_j \big(b_j \sum_n b'_{j,n} x^n\big)$, so that for all n we have$\sum_j b_j b'_{j,n} = y_n$ in B. But then $\mathfrak{b}$ would be finitely generated by these finitely many b_j, which is impossible because each b_j is in a subring of C generated over B by finitely many y_n.

v) Every prime ideal of A is the contraction of a prime ideal of $A[[x]]$.

Let $\mathfrak{p} \lhd A$ be prime, and let $\mathfrak{q} = \mathfrak{p}A[[x]] + (x)$ be the ideal of $A[[x]]$ generated by $\mathfrak{p}$ and x. Evidently $\mathfrak{q}^c = \mathfrak{p}$, and $A[[x]]/\mathfrak{q} \cong A/\mathfrak{p}$ is an integral domain, so $\mathfrak{q}$ is prime.

A ring A is such that every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element e such that $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of A are equal.

$\mathfrak{N} \subseteq \mathfrak{R}$ in any ring. Now suppose $a \notin \mathfrak{N}$. Then $(a) \nsubseteq \mathfrak{N}$, so there is a nonzero idempotent $e = ax \in (a)$. Since $(1-e)e = 0$, we see $1-e$ is a zero-divisor, and hence not a unit; by (1.9), $ax = e \notin \mathfrak{R}$, so $a \notin \mathfrak{R}$. Thus $\mathfrak{R} \subseteq \mathfrak{N}$.

Let A be a ring in which every element satisfies $x^n = x$ for some $n > 1$ (depending on x). Show that every prime ideal in A is maximal.

Let $\mathfrak{p} \lhd A$ be prime and $x \in A \backslash \mathfrak{p}$, with $x^n = x$ for some $n \geq 2$. In the domain $A/\mathfrak{p}$ we can cancel $\bar{x} \neq 0$, and so $\bar{x}\bar{x}^{n-2} = \bar{x}^{n-1} = 1$, showing an inverse $\bar{x}^{-1} = \bar{x}^{n-2}$ exists. Thus $A/\mathfrak{p}$ is a field and $\mathfrak{p}$ was maximal.[6]

Let A be a ring $\neq 0$. Show that the set of prime ideals of A has minimal elements with respect to inclusion.

Partially order the set Spec(A) of prime ideals of A by $\mathfrak{p} \leq \mathfrak{q} :\iff \mathfrak{p} \supseteq \mathfrak{q}$. We find minimal elements by Zorn's Lemma. Let $\langle \mathfrak{p}_\alpha \rangle_{\alpha \in \mathrm{A}}$ be a totally ordered chain in Spec(A), and let $\mathfrak{p} = \bigcap_{\alpha \in \mathrm{A}} \mathfrak{p}_\alpha$ be the intersection. It is an ideal. Now suppose $xy \in \mathfrak{p}$ and $x \notin \mathfrak{p}$. Then $xy \in \mathfrak{p}_\alpha$ for each $\mathfrak{a}$; as $\mathfrak{p}_\alpha$ is prime, this means each $\mathfrak{p}_\alpha$ contains either x or y. Since $x \notin \mathfrak{p}$, there is some β such that $x \notin \mathfrak{p}_\beta$; since $\alpha \geq \beta \iff \mathfrak{p}_\alpha \subseteq \mathfrak{p}_\beta$, we have for all $\alpha \geq \beta$ that $x \notin \mathfrak{p}_\alpha$, so $y \in \mathfrak{p}_\alpha$. As for $\gamma \leq \beta$ we have $y \in \mathfrak{p}_\beta \subseteq \mathfrak{p}_\gamma$, we know $y \in \mathfrak{p}_\alpha$ for all $\alpha \in \mathrm{A}$. Thus $y \in \mathfrak{p}$. Therefore $\mathfrak{p} \in$ Spec(A), and Spec(A) has minimal elements.

Let $\mathfrak{a}$ be an ideal $\neq (1)$ in a ring A. Show that $\mathfrak{a} = r(\mathfrak{a}) \iff \mathfrak{a}$ is an intersection of prime ideals.

By (1.14), $r(\mathfrak{a}) = \bigcap\{\mathfrak{p} \in \mathrm{Spec}(A) : \mathfrak{a} \subseteq \mathfrak{p}\}$. If $\mathfrak{a}$ is an intersection of prime ideals, it is the intersection $r(\mathfrak{a})$ of all primes that contain it, and if not, it then cannot be $r(\mathfrak{a})$, so it must be a proper subset.

Let A be a ring, $\mathfrak{N}$ its nilradical. Show the following are equivalent:
i) A has exactly one prime ideal;
ii) every element of A is either a unit or nilpotent;
iii) $A/\mathfrak{N}$ is a field.

i) $\implies$ ii): If $\mathfrak{p}$ is the only prime, $\mathfrak{N} \overset{(1.8)}{=} \mathfrak{p}$ and $\mathfrak{p}$ is also the only maximal ideal. Then $x \notin A^\times \overset{(1.5)}{\iff} x \in \mathfrak{p} = \mathfrak{N}$.

ii) $\implies$ iii): If $\bar{x} \in A/\mathfrak{N}$ is nonzero, any lift $x \notin \mathfrak{N}$, and so has an inverse y. Then $\bar{x}^{-1} = \bar{y}$ in $A/\mathfrak{N}$.

iii) $\implies$ i): If $A/\mathfrak{N}$ is a field, then $\mathfrak{N}$ is a maximal ideal. Since every prime $\mathfrak{p} \supseteq \mathfrak{N}$, we have $\mathfrak{p} = \mathfrak{N}$ the only prime.

A ring A is Boolean *if $x^2 = x$ for all $x \in A$. In a Boolean ring A, show that*
i) $2x = 0$ for all $x \in A$;

$x + 1 = (x+1)^2 = x^2 + 1^2 + 2x = (x+1) + 2x$, so subtracting $x+1$ from both sides, $0 = 2x$.

ii) every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements;

By [1.7], every prime ideal is maximal. $x^2 - x = x(x-1) = 0$ holds for each $x \in A$, so $\bar{x}(\bar{x}-1) = 0$ holds for each $\bar{x} \in A/\mathfrak{p}$; as $A/\mathfrak{p}$ is an integral domain, this means each element is either 0 or 1, so $A/\mathfrak{p} \cong \mathbb{F}_2$.

iii) every finitely generated ideal in A is principal.

We induct on the number of generators. The one-generator case is trivial. Suppose every ideal generated by n elements is principal, and $\mathfrak{a} = (x_1, \ldots, x_n, y)$. Let x generate $(x_1, \ldots, x_n)$, and let $z = x + y - xy$. Then $xz = x^2 + xy - x^2y = x$ and $yz = y$, so $\mathfrak{a} = (x, y) = (z)$.

[6] Here is a more baroque proof. Since $x^n = x$, if for any $m > 0$ we have $x^m = 0$, then taking p such that $n^p > m$, we see $0 = x^m x^{n^p - m} = x^{n^p} = x$, so $\mathfrak{N} = (0)$. If 0 and 1 (possibly equal) are the only elements of A, we are done. If not, let $x \notin \{0, 1\}$. We have $x(1 - x^{n-1}) = 0$, and by assumption x and x^{n-1} are nonzero, so $1 - x^{n-1}$ is a zero-divisor, hence not a unit, and so x^{n-1} is not in the Jacobson radical by (1.9), meaning x is not in the Jacobson radical either. Thus $\mathfrak{R} = (0)$.

A local ring contains no idempotent $\neq 0$, 1.

Let A be a ring. For any idempotent unit e, we have $e = e^{-1}e^2 = e^{-1}e = 1$. Suppose $e^2 = e \neq 0, 1$ in A. Then e is not a unit, and by (1.5) is contained in some maximal ideal $\mathfrak{m}$. Similarly $(1-e)^2 = 1 - 2e + e^2 = 1 - e$ is another idempotent $\neq 0$, 1, hence not a unit. But were A local, e would be in $\mathfrak{m} = \mathfrak{N}$, so $1 - e$ would be a unit by (1.9).[7]

Let K be a field and let Σ be the set of all irreducible monic polynomials f in one indeterminate with coefficients in K. Let A be the polynomial ring over K generated by indeterminates x_f, one for each $f \in \Sigma$. Let $\mathfrak{a}$ be the ideal of A generated by the polynomials $f(x_f)$ for all $f \in \Sigma$. Show that $\mathfrak{a} \neq (1)$.

If $\mathfrak{a} = (1)$, there exist finitely many $a_f \in A$ such that $1 = \sum a_f f(x_f)$. The set I of x_g occurring in this expression (not only those in the $f(x_f)$, but also those occurring in the a_f) is finite. We may enumerate I as $x_1, \ldots, x_i, \ldots, x_n$, corresponding to irreducible polynomials f_i, and suppose n is minimal such that such an equation holds. Write $B = K[x_1, \ldots, x_{n-1}]$, $C = B[x_n]$, and $\mathfrak{b} := \big(f_1(x_1), \ldots, f_{n-1}(x_{n-1})\big) \lhd B$. By minimality of n, the ideal $\mathfrak{b}$ is proper, so $\mathfrak{b}^e = \mathfrak{b}[x_n] \lhd C$ is as well, while by the equation above, $\mathfrak{b}^e + \big(f_n(x_n)\big) = C$. Since $\mathfrak{b} \neq B$, we know $B/\mathfrak{b} \neq 0$. Let g be the image of $f_n(x_n)$ in $(B/\mathfrak{b})[x_n]$. Since f_n is irreducible in $K[x_n]$, its degree $\deg_{x_n} f_n \geq 1$ and also $\deg_{x_n} g \geq 1$. Then

$$0 = \frac{C}{\mathfrak{b}^e + \big(f_n(x_n)\big)} \cong \frac{C/\big(\mathfrak{b}[x_n]\big)}{(g)} = \frac{B[x_n]/\big(\mathfrak{b}[x_n]\big)}{(g)} \cong \frac{(B/\mathfrak{b})[x_n]}{(g)} \neq 0,$$

which is a contradiction.[8]

Let $\mathfrak{m}$ be a maximal ideal of A containing $\mathfrak{a}$ and let $K_1 = A/\mathfrak{m}$. Then K_1 is an extension field of K in which each $f \in \Sigma$ has a root. Repeat the construction with K_1 in place of K, obtaining a field K_2, and so on. Let $L = \bigcup_{n=1}^{\infty} K_n$. Then L is a field in which each $f \in \Sigma$ splits completely into linear factors. Let $\overline{K}$ be the set of all elements of L which are algebraic over K. Then $\overline{K}$ is an algebraic closure of K.

We should probably show that $\overline{K}$ is closed under subtraction and multiplication. Let $a, b \in \overline{K}$ have conjugates a_i, b_j over K. Then $\prod_{i,j}(x - a_i + b_j)$ is symmetric in the a_i and the b_j, and so has coefficients in K, so $a - b \in \overline{K}$. Similarly $\prod_{i,j}(x - a_i b_j)$ is symmetric, so $ab \in \overline{K}$.

In a ring A, let Σ be the set of all ideals in which every element is a zero-divisor. Show that the set Σ has maximal elements and that every maximal element of Σ is a prime ideal. Hence the set of zero-divisors in A is a union of prime ideals.

Order Σ by inclusion; to show it has maximal elements, it suffices by Zorn's Lemma to show every chain $\langle \mathfrak{a}_\alpha \rangle_{\alpha \in \mathrm{A}}$ has an upper bound in Σ. Let $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. It contains only zero-divisors, since if $x \in \mathfrak{a}$, then there is α such that $x \in \mathfrak{a}_\alpha$, and then by definition x is a zero-divisor.

Let $\mathfrak{p}$ be a maximal element of Σ; we must show it to be prime. Suppose $x, y \notin \mathfrak{p}$. Then there are non-zero-divisors in $(x) + \mathfrak{p}$ and $(y) + \mathfrak{p}$, and their product is an element of $(xy) + \mathfrak{p}$ that is again a non-zero-divisor. Thus $xy \notin \mathfrak{p}$, lest there be something in $\mathfrak{p}$ other than a zero-divisor. This shows $\mathfrak{p}$ is prime.

Thus Σ has maximal elements and every element of Σ is contained in one; considering principal ideals, this shows every zero-divisor is in a maximal element of Σ. The last statement follows.

The prime spectrum of a ring

Let A be a ring and let X be the set of all prime ideals of A. For each subset E of A, let $V(E)$ denote the set of all prime ideals of A which contain E. Prove that

i) if $\mathfrak{a}$ is the ideal generated by E, then $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

Let $\mathfrak{p} \in X$. We have $E \subseteq \mathfrak{a}$, so if $\mathfrak{a} \subseteq \mathfrak{p}$, then $E \subseteq \mathfrak{p}$. On the other hand, if $E \subseteq \mathfrak{p}$, then $\mathfrak{a} = AE \subseteq A\mathfrak{p} = \mathfrak{p}$. Thus $V(E) = V(\mathfrak{a})$. By (1.14), $r(\mathfrak{a}) = \bigcap V(\mathfrak{a})$, so $\mathfrak{p} \supseteq r(\mathfrak{a}) \iff \mathfrak{p} \supseteq \mathfrak{a}$ and $V(\mathfrak{a}) = V\big(r(\mathfrak{a})\big)$.

ii) $V(0) = X$, $V(1) = \varnothing$.

For every prime ideal $\mathfrak{p}$ we have $0 \in \mathfrak{p}$ and $1 \notin \mathfrak{p}$.

[7] Cf. the implication iii) $\Longrightarrow$ ii) in [1.22] for another proof: by (1.4), each of (e) and $(1-e)$ is contained in a maximal ideal, and we can show the two are coprime, so no maximal ideal can contain both. Actually, there is even an isomorphism $A \xrightarrow{\sim} A/(e) \times A/(1-e)$, so A obviously has more than one maximal ideal.

[8] This proof is taken from [Morandi].

iii) if $\langle E_i \rangle_{i\in I}$ is any family of subsets of A, then $V\Big(\bigcup_{i\in I} E_i\Big) = \bigcap_{i\in I} V(E_i)$.

$$\mathfrak{p} \in V\Big(\bigcup_i E_i\Big) \iff \bigcup_i E_i \subseteq \mathfrak{p} \iff \forall i \in I\ (E_i \subseteq \mathfrak{p}) \iff \forall i \in I\ (\mathfrak{p} \in V(E_i)) \iff \mathfrak{p} \in \bigcap_i V(E_i).$$

Note also for future use that $\bigcup E_i \subseteq \mathfrak{p} \iff \bigcup AE_i \subseteq A\mathfrak{p} = \mathfrak{p} \iff \sum AE_i \subseteq \mathfrak{p}$, so in particular for ideals $\mathfrak{a}_i$ we have $V\big(\bigcup \mathfrak{a}_i\big) = V\big(\sum \mathfrak{a}_i\big)$

iv) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$ for any ideals $\mathfrak{a}$, $\mathfrak{b}$ of A.

Suppose $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$ and $\mathfrak{b} \not\subseteq \mathfrak{p}$. Then there is $b \in \mathfrak{b} \backslash \mathfrak{p}$, and $ab \in \mathfrak{p}$ for all $a \in \mathfrak{a}$, so the primality of $\mathfrak{p}$ gives $a \in \mathfrak{p}$ and thus $\mathfrak{a} \subseteq \mathfrak{p}$. Thus if $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$, we have shown $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$, so $\mathfrak{p} \in V(\mathfrak{a}) \cup V(\mathfrak{b})$. On the other hand, if $\mathfrak{p}$ contains $\mathfrak{a}$ or contains $\mathfrak{b}$, then it must contain the subset $\mathfrak{a}\mathfrak{b}$. Thus $V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a}) \cup V(\mathfrak{b})$.

Now $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, so if $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$, then $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. On the other hand, if $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, then we have shown either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$, so since $\mathfrak{a} \cap \mathfrak{b}$ is a subset of both of these we have $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{p}$. Thus $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$.

These results show that the sets $V(E)$ satisfy the axioms for closed sets in a topological space. The resulting topology is called the Zariski topology. *The topological space X is called the* prime spectrum *of A, and is written* Spec(A).

Draw pictures of Spec($\mathbb{Z}$), Spec($\mathbb{R}$), Spec($\mathbb{C}[x]$), Spec($\mathbb{R}[x]$), Spec($\mathbb{Z}[x]$).

There is only one point, (0), in Spec($\mathbb{R}$).

In Spec($\mathbb{Z}$), the elements are (0) and (p) for each positive prime $p \in \mathbb{N}$, and the closed sets are X, $\varnothing$, and all finite sets containing (0).

In $\mathbb{C}[x]$, all polynomials split into linear factors, so the irreducible polynomials are $x - \alpha$ for $\alpha \in \mathbb{C}$. Since $\mathbb{C}$ is a field, this means the only primes are (0) and $(x - \alpha)$ for $\alpha \in \mathbb{C}$. The closed sets are again X, $\varnothing$, and all finite sets containing (0). As a point set, it makes sense to think of X as the complex plane plus one additional dense point.

In $\mathbb{R}[x]$, all polynomials split into linear factors and polynomials of the form $(x - \alpha)(x + \alpha)$ for $\alpha \in \mathbb{C}$ with $\operatorname{Im}(\alpha) > 0$. Thus the primes of $\mathbb{R}[x]$ correspond to points of $\mathbb{R}$, points of the upper half plane, and the dense point (0) again.

In $\mathbb{Z}[x]$, there are irreducible polynomials f of all degrees ≥ 1, giving rise to prime ideals (f), there are ideals (p) for all positive primes $p \in \mathbb{N}$, and there are ideals $(p, f) = (p) + (f)$, which are maximal. There is also (0). The closed sets are X, $\varnothing$, and all finite sets C containing (0) and such that if $(p, f) \in C$ then $(p), (f) \in C$.[9]

*For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = $* Spec($A$). *The sets X_f are open. These are called the* basic open sets *of* Spec(A). *Show that they form a basis of open sets for the Zariski topology.*

To see the collection $\{X_f\}$ is a basis for the topology of X we can show it i) contains, for each $\mathfrak{p} \in X_f \cap X_g$, an X_h with $\mathfrak{p} \in X_h \subseteq X_f \cap X_g$, ii) includes $\varnothing$, and iii) covers X. These follow, respectively, from i), ii), and iii) below.

i) $X_f \cap X_g = X_{fg}$;

Taking complements, this is the same as saying $V(f) \cup V(g) = V(fg)$, or that a prime contains fg if and only if it contains one of f and g. But this is in the definition of a prime ideal.

ii) $X_f = \varnothing \iff f$ is nilpotent;

$$X_f = \varnothing \iff V(f) = X \iff \forall \mathfrak{p} \in X\ (f \in \mathfrak{p}) \overset{(1.8)}{\iff} f \in \mathfrak{N}.$$

iii) $X_f = X \iff f$ is a unit;

$$X_f = X \iff V(f) = \varnothing \iff \forall \mathfrak{p} \in X\ (f \notin \mathfrak{p}) \overset{(1.5)}{\iff} f \in A^\times.$$

iv) $X_f = X_g \iff r\big((f)\big) = r\big((g)\big)$;

[9] Mumford's famous picture of this space can be seen at [LeBruyn].

We can prove something slightly better: $X_f \subseteq X_g \iff V(g) \subseteq V(f) \iff r\big((f)\big) \subseteq r\big((g)\big)$. The first step is obvious because complementation is containment-reversing. Recall from [1.15.i] that $V(f) = V\big((f)\big)$. For the second step, we generalize again, from $(f), (g) \lhd A$ to arbitrary ideals $\mathfrak{a}$, $\mathfrak{b}$.[10] Note the antitone Galois correspondence[11]

$$\mathfrak{a} \subseteq \bigcap Y \iff \forall \mathfrak{p} \in Y\ (\mathfrak{a} \subseteq \mathfrak{p}) \iff Y \subseteq V(\mathfrak{a})$$

between ideals $\mathfrak{a} \lhd A$ and subsets $Y \subseteq \operatorname{Spec}(A)$. Applying it to $Y = V(\mathfrak{b})$ yields

$$V(\mathfrak{b}) \subseteq V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \bigcap V(\mathfrak{b}) \overset{(1.14)}{=} r(\mathfrak{b}) \overset{(1.13)}{\iff} r(\mathfrak{a}) \subseteq r(\mathfrak{b}).$$

v) X is compact (that is, every open covering of X has a finite sub-covering).

This follows from the more general vi), taking $f = 1$.

vi) More generally, each X_f is compact.

Recall that the closed sets of X are all of the form $V(\mathfrak{a})$ for $\mathfrak{a} \lhd A$. Let a collection $\big\{X \setminus V(\mathfrak{a}_\alpha)\big\}_\alpha$ of open sets be given. This collection covers X_f if and only if the following equivalent conditions hold:

$$\bigcap_\alpha V(\mathfrak{a}_\alpha) \subseteq V(f) \overset{[1.15]}{\iff} V\Big(\sum_\alpha \mathfrak{a}_\alpha\Big) \subseteq V\big((f)\big) \underset{\text{of iv)}}{\overset{\text{proof}}{\iff}} r\big((f)\big) \subseteq r\Big(\sum_\alpha \mathfrak{a}_\alpha\Big) \overset{(1.13)}{\iff} \exists m \geq 1 \Big[f^m \in \sum_\alpha \mathfrak{a}_\alpha\Big];$$

and then our task is to find a finite set of $\mathfrak{a}_\alpha$ for which the last still holds. But each element of $\sum \mathfrak{a}_\alpha$ is a finite sum of elements from the individual $\mathfrak{a}_\alpha$, so $f^m \in \sum \mathfrak{a}_\alpha$ just if for some finite subset $\{\mathfrak{a}_j\}_{j=1}^n$ we have $f^m \in \sum_{j=1}^n \mathfrak{a}_j$.

vii) An open subset of X is compact if and only if it is a finite union of sets X_f.

Each X_f is compact, and a union of a finite collection of compact sets is compact[12], so a finite union of basic open sets X_f is compact.

On the other hand, suppose a set is open and compact. Since it is open, we can write it as a union of some basic open sets X_{f_α}; since it is compact, we can take a finite subcover, showing it is a union of finitely many basic open sets.

For psychological reasons it is sometimes convenient to denote a prime ideal of A by a letter such as x or y when thinking of it as a point of $X = \operatorname{Spec}(A)$. When thinking of x as a prime ideal of A, we denote it by $\mathfrak{p}_x$ (logically, of course, it is the same thing). Show that

i) The set $\{x\}$ is closed (we say that x is a "closed point") in $\operatorname{Spec}(A) \iff \mathfrak{p}_x$ is maximal;

Let $Y \subseteq X$, and let $V(\mathfrak{a}) \subseteq X$ be a closed set. Recall our Galois correspondence: $Y \subseteq V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \bigcap_{y \in Y} \mathfrak{p}_y$.

$$\overline{Y} = \bigcap \big\{V(\mathfrak{a}) : Y \subseteq V(\mathfrak{a})\big\} = \bigcap \Big\{V(\mathfrak{a}) : \mathfrak{a} \subseteq \bigcap_{y \in Y} \mathfrak{p}_y\Big\} \overset{[1.15]}{=} V\Big(\sum \Big\{\mathfrak{a} : \mathfrak{a} \subseteq \bigcap_{y \in Y} \mathfrak{p}_y\Big\}\Big) = V\Big(\bigcap_{y \in Y} \mathfrak{p}_y\Big), \tag{1.1}$$

so $\{x\}$ is closed just if $\{x\} = V(\mathfrak{p}_x)$, or in other words iff no other prime contains $\mathfrak{p}_x$.

ii) $\overline{\{x\}} = V(\mathfrak{p}_x)$;

$$\overline{\{x\}} \underset{1.1}{\overset{\text{Eq.}}{=}} V\Big(\bigcap \{\mathfrak{p}_x\}\Big) = V(\mathfrak{p}_x).$$

[10] The proof branches here; if you like, you can apply what follows in this footnote instead of the final two sentences in the body text. Recall also from (1.14) that for all ideals $\mathfrak{a} \lhd A$ we have $r(\mathfrak{a}) = \bigcap V(\mathfrak{a})$, from [1.15.i] that $V(\mathfrak{a}) = V\big(r(\mathfrak{a})\big)$, and from [1.15.iii] that $V(—)$ is containment-reversing. Finally note taking intersections of collections is a containment-reversing operation. Then

$$r(\mathfrak{a}) \subseteq r(\mathfrak{b}) \implies V(\mathfrak{b}) = V\big(r(\mathfrak{b})\big) \subseteq V\big(r(\mathfrak{a})\big) = V(\mathfrak{a});$$
$$V(\mathfrak{b}) \subseteq V(\mathfrak{a}) \implies r(\mathfrak{a}) = \bigcap V(\mathfrak{a}) \subseteq \bigcap V(\mathfrak{b}) = r(\mathfrak{b}).$$

[11] [WPGalois]

[12] To see this, let a cover $\mathscr{V}$ of the finite union $K = \bigcup_{j=1}^n$ of compact sets K_j be given. For each K_j take a finite subcollection $\mathscr{U}_j \subseteq \mathscr{V}$ covering K_j; then $\bigcup_j \mathscr{U}_j \subseteq \mathscr{V}$ is a finite collection covering K.

iii) $y \in \overline{\{x\}} \iff \mathfrak{p}_x \subseteq \mathfrak{p}_y$*;*

$$y \in \overline{\{x\}} \overset{\text{ii)}}{=} V(\mathfrak{p}_x) \iff \mathfrak{p}_x \subseteq \mathfrak{p}_y.$$

iv) X is a T_0-space (this means that if x, y are distinct points of X, then either there is a neighborhood of x which does not contain y, or else there is a neighborhood of y which does not contain x).

If every neighborhood of x contains y and vice versa, then $y \in \overline{\{x\}}$ and $x \in \overline{\{y\}}$, so by part iii); $\mathfrak{p}_x \subseteq \mathfrak{p}_y \subseteq \mathfrak{p}_x$ and $x = y$.

A topological space X is said to be irreducible *if $X \neq \varnothing$ and if every pair of non-empty open sets in X intersect, or equivalently if every non-empty open set is dense in X. Show that* $\operatorname{Spec}(A)$ *is irreducible if and only if the nilradical of A is a prime ideal.*

$\varnothing$ is not an intersection of two nonempty open sets just if X is not a union of two proper closed sets $V(\mathfrak{a})$, $V(\mathfrak{b})$. By the proof of [1.17.iv],

$$X = V(0) \neq V(\mathfrak{a}) \iff r(\mathfrak{a}) \nsubseteq r(0) \overset{(1.8)}{=} \mathfrak{N} \overset{(1.13)}{\iff} \mathfrak{a} \nsubseteq \mathfrak{N},$$

and by [1.15.iv], $V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{ab})$, so X is irreducible just if for all ideals $\mathfrak{a}$, $\mathfrak{b} \nsubseteq \mathfrak{N}$ we also have $\mathfrak{ab} \nsubseteq \mathfrak{N}$; by contraposition, this is that $\mathfrak{ab} \subseteq \mathfrak{N} \implies \mathfrak{a} \subseteq \mathfrak{N}$ or $\mathfrak{b} \subseteq \mathfrak{N}$.

But this condition is just a rephrasing of primality: if $\mathfrak{N}$ is prime, then as in [1.15.iv], $\mathfrak{ab} \subseteq \mathfrak{N} \implies \mathfrak{a} \subseteq \mathfrak{N}$ or $\mathfrak{b} \subseteq \mathfrak{N}$; conversely, if the condition holds, then $ab \in \mathfrak{N} \implies (a)(b) \subseteq \mathfrak{N} \implies (a)$ or $(b) \subseteq \mathfrak{N} \implies a$ or $b \in \mathfrak{N}$, so $\mathfrak{N}$ is prime.

Let X be a topological space.

i) If Y is an irreducible (Exercise 19) subspace of X, then the closure $\overline{Y}$ of Y in X is irreducible.

Let open U, $V \subseteq \overline{Y}$ be non-empty. Then $U \cap Y$ and $V \cap Y$ are non-empty by the definition of closure. Since Y is irreducible, $U \cap V \cap Y \neq \varnothing$, and *a fortiori* $U \cap V \neq \varnothing$.

ii) Every irreducible subspace of X is contained in a maximal irreducible subspace.

We apply Zorn's Lemma. Order the irreducible subspaces Σ of X by inclusion, and let $\langle Y_\alpha \rangle$ be a linearly ordered chain. Set $Z = \bigcup_\alpha Y_\alpha$; we will be done if we can show $Z \in \Sigma$. Let U, $V \subseteq Z$ be open and non-empty. By definition, U meets some Y_α and V meets some Y_β. Without loss of generality, suppose $\alpha \leq \beta$. Then as $Y_\alpha \subseteq Y_\beta$, we have both $U \cap Y_\beta$ and $V \cap Y_\beta$ non-empty and open in Y_β, so by irreducibility of Y_β we have $U \cap V \cap Y_\beta \neq \varnothing$ and $U \cap V \neq \varnothing$, showing Z is irreducible.

iii) The maximal irreducible subspaces of X are closed and cover X. They are called the irreducible components *of X. What are the irreducible components of a Hausdorff space?*

To see that a maximal irreducible subspace is closed, note that its closure is irreducible by part i) and contains it, and so equals it by maximality. To see the maximal irreducible subspaces cover X, note that each singleton is irreducible and contained in some maximal irreducible subspace.

Every subspace of a Hausdorff space is Hausdorff. If a Hausdorff space has two distinct points, they have two disjoint neighborhoods by definition, so the space is not irreducible. Thus the irreducible components of a Hausdorff space are the singletons.

iv) If A is a ring and $X = \operatorname{Spec}(A)$, then the irreducible components of X are the closed sets $V(\mathfrak{p})$, where $\mathfrak{p}$ is a minimal prime ideal of A (Exercise 8).

Any closed subset of X is of the form $V(\mathfrak{a})$ for some ideal $\mathfrak{a} \lhd A$, and is homeomorphic to $\operatorname{Spec}(A/\mathfrak{a})$ by [1.21.iv]. By [1.19], $V(\mathfrak{a}) = V\big(r(\mathfrak{a})\big)$ is irreducible if and only if $\mathfrak{N}(A/\mathfrak{a})$ is prime, or equivalently if $r(\mathfrak{a})$ is prime in A; so the irreducible closed subspaces of X are $V(\mathfrak{p})$ for $\mathfrak{p} \in X$. Such a $V(\mathfrak{p})$ is maximal just if there is no $\mathfrak{q} \in X$ with $V(\mathfrak{p}) \subsetneq V(\mathfrak{q})$, or equivalently, by the proof of [1.17.iv], there is no prime $\mathfrak{q} \subsetneq \mathfrak{p}$.

Let $\phi\colon A\to B$ be a ring homomorphism. Let $X=\operatorname{Spec}(A)$ and $Y=\operatorname{Spec}(B)$. If $\mathfrak{q}\in Y$, then $\phi^{-1}(\mathfrak{q})$ is a prime ideal of A, i.e., a point of X. Hence ϕ induces a mapping $\phi^*\colon Y\to X$. Show that

i) If $f\in A$ then $\phi^{*-1}(X_f)=Y_{\phi(f)}$, and hence that ϕ^* is continuous.

$$\mathfrak{q}\in Y_{\phi(f)} \iff \phi(f)\notin\mathfrak{q} \iff f\notin\phi^{-1}(\mathfrak{q}) \iff \phi^*(\mathfrak{q})=\phi^{-1}(\mathfrak{q})\in X_f \iff \mathfrak{q}\in(\phi^*)^{-1}(X_f).$$

ii) If $\mathfrak{a}$ is an ideal of A, then $\phi^{*-1}\big(V(\mathfrak{a})\big)=V(\mathfrak{a}^e)$.

First, note that (1.17.i) implies extension and contraction of ideals form an isotone Galois correspondence:[13]

$$\mathfrak{a}\subseteq\mathfrak{b}^c \iff \mathfrak{a}^e\subseteq\mathfrak{b}.$$

Indeed, if $\mathfrak{a}\subseteq\mathfrak{b}^c$, then extending, $\mathfrak{a}^e\subseteq\mathfrak{b}^{ce}\subseteq\mathfrak{b}$, and if $\mathfrak{a}^e\subseteq\mathfrak{b}$, then contracting, $\mathfrak{a}\subseteq\mathfrak{a}^{ec}\subseteq\mathfrak{b}^c$. Now for $\mathfrak{q}\in\operatorname{Spec}(B)$,

$$\mathfrak{q}\in(\phi^*)^{-1}\big(V(\mathfrak{a})\big) \iff \phi^*(\mathfrak{q})\in V(\mathfrak{a}) \iff \mathfrak{a}\subseteq\mathfrak{q}^c \iff \mathfrak{a}^e\subseteq\mathfrak{q} \iff \mathfrak{q}\in V(\mathfrak{a}^e).$$

iii) If $\mathfrak{b}$ is an ideal of B, then $\overline{\phi^*(V(\mathfrak{b}))}=V(\mathfrak{b}^c)$.

By Eq. 1.1 from [1.18.i], $\overline{\phi^*(V(\mathfrak{b}))}$ is the set of prime ideals containing $\bigcap\phi^*\big(V(\mathfrak{b})\big)$, which ideal equals

$$\bigcap\{\mathfrak{q}^c:\mathfrak{b}\subseteq\mathfrak{q}\in Y\}\overset{(1.18)}{=}\Big(\bigcap_{\mathfrak{b}\subseteq\mathfrak{q}\in Y}\mathfrak{q}\Big)^c\underset{(1.14)}{=}r(\mathfrak{b})^c\overset{(1.18)}{=}r(\mathfrak{b}^c).$$

But $V\big(r(\mathfrak{b}^c)\big)=V(\mathfrak{b}^c)$.

iv) If ϕ is surjective, then ϕ^* is a homeomorphism of Y onto the closed subset $V\big(\ker(\phi)\big)$ of X. (In particular, $\operatorname{Spec}(A)$ *and* $\operatorname{Spec}(A/\mathfrak{N})$ *(where $\mathfrak{N}$ is the nilradical of A) are naturally homeomorphic.)*

If $\phi\colon A\to A/\mathfrak{a}$ is surjective, (1.1) gives an containment-preserving and -reflecting bijection between the set of ideals $\mathfrak{b}\lhd A$ containing $\mathfrak{a}$ and the ideals $\mathfrak{b}/\mathfrak{a}\lhd A/\mathfrak{a}$. Since this relation preserves and reflects primes (p. 9), for any ideal $\mathfrak{b}/\mathfrak{a}$ of $A/\mathfrak{a}$,

$$\phi^*\big(V\big(\mathfrak{b}/\mathfrak{a}\big)\big)=\big\{\mathfrak{p}\in\operatorname{Spec}(A):\mathfrak{b}/\mathfrak{a}\subseteq\mathfrak{p}/\mathfrak{a}\in\operatorname{Spec}(A/\mathfrak{a})\big\}=V(\mathfrak{b}),$$

so $\phi^*|^{V(\mathfrak{a})}$ is a bijection taking closed sets to closed sets, continuous by part i), and hence a homeomorphism. For the parenthetical remark, note that $\operatorname{Spec}(A)=V\big(\mathfrak{N}(A)\big)$ by (1.8).

v) If ϕ is injective, then $\phi^*(Y)$ is dense in X. More precisely, $\phi^*(Y)$ is dense in X $\iff$ $\ker(\phi)\subseteq\mathfrak{N}$.

The second statement does imply the first, because if ϕ is injective, then indeed $\ker(\phi)=0\subseteq\mathfrak{N}$. Now $\phi^*(Y)$ is dense just if

$$X=\overline{\phi^*(Y)}=\overline{\phi^*\big(V(0)\big)}\overset{[1.12.iii]}{=}V(0^c)=V\big(\ker(\phi)\big).$$

But $\ker(\phi)$ is contained in every prime of A if and only if it is contained in their intersection, which by (1.8) is $\mathfrak{N}(A)$.

vi) Let $\psi\colon B\to C$ be another ring homomorphism. Then $(\psi\circ\phi)^*=\phi^*\circ\psi^*$.

By definition, $a\in(\psi\circ\phi)^*(\mathfrak{p}_x)\iff\psi\big(\phi(a)\big)\in\mathfrak{p}_x\iff\phi(a)\in\psi^*(\mathfrak{p}_x)\iff a\in\phi^*\big(\psi^*(\mathfrak{p}_x)\big)$.

vii) Let A be an integral domain with just one nonzero prime ideal $\mathfrak{p}$, and let K be the field of fractions of A. Let $B=(A/\mathfrak{p})\times K$. Define $\phi\colon A\to B$ by $\phi(x)=(\bar{x},x)$, where $\bar{x}$ is the image of x in $A/\mathfrak{p}$. Show that ϕ^* is bijective but not a homeomorphism.

A has two prime ideals, $\mathfrak{p}$ and (0), and B, a product of two fields, has prime ideals $\mathfrak{q}_1=\{\bar{0}\}\times K$ and $\mathfrak{q}_2=(A/\mathfrak{p})\times\{0\}$; the zero ideal of B is not prime. Now $\phi^*(\mathfrak{q}_1)=\{x\in A:\bar{x}=0\}=\mathfrak{p}$, and $\phi^*(\mathfrak{q}_2)=\{x\in A:x=0\}=(0)$, so ϕ^* is bijective. However, by [1.18.iii] $\mathfrak{p}\in\overline{\{(0)\}}$ in $\operatorname{Spec}(A)$, while in $\operatorname{Spec}(B)$ we have $\mathfrak{q}_2\notin\{\mathfrak{q}_1\}=\overline{\{\mathfrak{q}_1\}}$ (both primes being maximal), so ϕ^* cannot be a homeomorphism.

[13] [WPGalois]

Let $A = \prod_{i=1}^{n} A_i$ be a direct product of rings A_i. Show that $\operatorname{Spec}(A)$ *is the disjoint union of open (and closed) subspaces X_i, where X_i is canonically homeomorphic with* $\operatorname{Spec}(A_i)$.

Let $\mathrm{pr}_i : A \to A_i$ be the canonical projection, and $\mathfrak{b}_i = \prod_{j \neq i} A_j$ its kernel; then by [1.21.iv], pr_i^* is a homeomorphism $\operatorname{Spec}(A_i) \xrightarrow{\approx} V(\mathfrak{b}_i)$. Since $\bigcap_{i=1}^{n} \mathfrak{b}_i = 0$, it follows by [1.15.iv] that $\bigcup V(\mathfrak{b}_i) = V\big(\bigcap \mathfrak{b}_i\big) = V(0) = \operatorname{Spec}(A)$, so the $V(\mathfrak{b}_i)$ cover $\operatorname{Spec}(A)$.[14] Since $\mathfrak{b}_i + \mathfrak{b}_j = A$ for $i \neq j$ and by [1.15], $V(\mathfrak{b}_i) \cap V(\mathfrak{b}_j) = V(\mathfrak{b}_i + \mathfrak{b}_j) = V(1) = \varnothing$, it follows the $V(\mathfrak{b}_j)$ are disjoint. Since the complement $\bigcup_{j \neq i} V(\mathfrak{b}_j)$ of each $V(\mathfrak{b}_i)$ is a finite union of closed sets, the $V(\mathfrak{b}_i)$ are also open.

Conversely, let A be any ring. Show that the following statements are equivalent:
i) $X = \operatorname{Spec}(A)$ is disconnected.
ii) $A \cong A_1 \times A_2$ where neither of the rings A_1, A_2 is the zero ring.
iii) A contains an idempotent $\neq 0, 1$
In particular, the spectrum of a local ring is always connected (Exercise 12).

We showed ii) $\implies$ i) above; in this case $X = X_1 \amalg X_2$ is a disjoint union two non-empty open sets.

i) $\implies$ iii): Suppose $X = \operatorname{Spec}(A)$ is disconnected; then by definition it is a disjoint union of two non-empty closed sets $V(\mathfrak{a})$, $V(\mathfrak{b})$. By [1.15.iii] we have $\varnothing = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b})$, so no prime contains $\mathfrak{a} + \mathfrak{b}$, which must then equal (1). Let $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ be such that $a + b = 1$. By [1.15.iv], $X = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$, so by (1.8), $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{N}$ and there is some $n \geq 1$ with $(ab)^n = 0$. We have $(1) = (a^n) + (b^n)$ by (1.16), so we can find $e \in (a^n)$ such that $1 - e \in (b^n)$. We then have $e - e^2 = e(1-e) \in (ab)^n = 0$, so $e = e^2$. If $e = 1$ we would have $1 \in \mathfrak{a}$ and if $e = 0$ we would have $1 \in \mathfrak{b}$, contrary to assumption, so e is a nontrivial idempotent.

iii) $\implies$ ii): Suppose $e \neq 0, 1$ is an idempotent. Then as in the proof of [1.12], $1 - e$ is also an idempotent $\neq 0, 1$, and neither is a unit. This means (e) and $(1-e)$ are proper, nonzero ideals, and they are coprime since $e + [1-e] = 1$. Since $(e)(1-e) = (e - e^2) = (0)$, then, (1.10.i) shows $(e) \cap (1-e) = (0)$. Let $\phi : A \to A/(e) \times A/(1-e)$ be the natural homomorphism. (1.10.ii,iii) show ϕ is an isomorphism.[15]

Let A be a Boolean ring (Exercise 11), and let $X = \operatorname{Spec}(A)$.
i) For each $f \in A$, the set X_f (Exercise 17) is both open and closed in X.

X_f is open because it is the complement of $V(f)$. It is open because $V(f) = X_{1-f}$. Indeed, $X = X_f \cup X_{1-f}$, since any ideal containing both f and $1-f$ contains 1; and $X_f \cap X_{1-f} = X_{f(1-f)} = X_0 = \varnothing$ by [1.17.i] and [1.17.ii].

ii) Let $f_1, \ldots, f_n \in A$. Show that $X_{f_1} \cup \cdots \cup X_{f_n} = X_f$ for some $f \in A$.

$\bigcup X_{f_i} = \bigcup \big(X \setminus V(f_i)\big) = X \setminus \bigcap V(f_i) = X \setminus V\big(\sum (f_i)\big)$ by [1.15]. By [1.11.iii], $\sum (f_i) = (f)$ for some $f \in A$, so $\bigcup X_{f_i} = X \setminus V(f) = X_f$.

iii) The sets X_f are the only open subsets of X which are both open and closed.

Let U be both open and closed. Since it is closed and X is compact, U is compact. By [1.17.vii], U is a union of finitely many X_{f_j}. By part ii), it is an X_f for some $f \in A$.

iv) X is a compact Hausdorff space.

The compactness of X is [1.17.v]. To show X is Hausdorff, let $x, y \in X$; we will show that if they do not have disjoint neighborhoods X_f and X_{1-f}, then $x = y$. Now $X_f \ni x$ and $X_{1-f} \ni y$ just if $f \notin \mathfrak{p}_x$ and $1 - f \notin \mathfrak{p}_y$. By part i), this is the same as saying $f \notin \mathfrak{p}_x$ and $f \in \mathfrak{p}_y$. If no such f exists, we have $\mathfrak{p}_y \subseteq \mathfrak{p}_x$, and since [1.11.ii] showed $\mathfrak{p}_y$ is maximal, $\mathfrak{p}_x = \mathfrak{p}_y$.

[14] In unnecessary detail, for each j there is an element $e_j \in A$ with a 1 in the j coordinate and 0 at each other coordinate. Let $\mathfrak{a} \lhd A$ be an ideal, and $a = \langle a_1, \ldots, a_n \rangle \in \mathfrak{a}$. Then $ae_j = a_j e_j \in \mathfrak{a}$, and $a = \sum a_j e_j = \sum a e_j$, so $\mathfrak{a} = \sum \mathfrak{a} e_j$. We have $\mathfrak{b}_j = \sum_{i \neq j} (e_i)$. To see $\operatorname{Spec}(A) = \bigcup X_j$, note that if $\mathfrak{a} \lhd A$ contains neither e_i nor e_j for some $i \neq j$, then since $e_i e_j = 0 \in \mathfrak{a}$, we know $\mathfrak{a}$ is not prime. Therefore all the prime ideals of A contain some $\mathfrak{b}_j$, and thus are of the form $\mathfrak{p} = \mathrm{pr}_j^*(\mathfrak{p}_j) = \mathfrak{p}_j e_j + \mathfrak{b}_j$ for some $\mathfrak{p}_j \in \operatorname{Spec}(A_j)$, and hence are in some X_j.

[15] We can also show ii) $\implies$ iii): $\langle 1, 0 \rangle \in A_1 \times A_2$ is an idempotent $\neq 0, 1$.

Let L be a lattice, in which the sup and inf of two elements a, b are denoted by $a \vee b$ and $a \wedge b$ respectively. L is a Boolean lattice *(or* Boolean algebra*) if*

i) L has a least element and a greatest element (denoted by 0, 1 respectively);

ii) each of $\vee$, $\wedge$ is distributive over the other;

iii) Each $a \in L$ has a unique "complement" $a' \in L$ such that $a \vee a' = 1$ and $a \wedge a' = 0$.

For example, the set of all subsets of a set, ordered by inclusion, is a Boolean lattice.

Let L be a Boolean lattice. Define addition and multiplication in L by the rules

$$a + b = (a \wedge b') \vee (a' \wedge b), \qquad ab = a \wedge b.$$

Verify that in this way L becomes a Boolean ring, say $A(L)$.

To verify the ring axioms, we first require some lemmas about Boolean algebra.

- Commutativity: The supremum $x \vee y$, by definition, is the unique $z \geq x, y$ such that for all other $w \geq x, y$ we have $w \geq z$, and this definition is symmetric in x and y; thus $x \vee y = y \vee x$. Dually, $x \wedge y = y \wedge x$ is the unique $z \leq x, y$ such that for all other $w \leq x, y$ we have $w \leq z$, and this definition is symmetric in x and y.

- Associativity: $(x \vee y) \vee z$ is the unique least element $t \geq x \vee y,\ z$. Then we have $t \geq x, y, z$, so $(x \vee y) \vee z \geq x \vee y \vee z$, the joint supremum of x, y, z. On the other hand, $x \vee y \vee z \geq x, y, z$ as well, so $x \vee y \vee z \geq x \vee y,\ z$, and by definition $x \vee y \vee z \geq (x \vee y) \vee z$. Since we have both inequalities and $\langle L, \leq \rangle$ is a partial order, $(x \vee y) \vee z = x \vee y \vee z$. Symmetrically, $x \vee y \vee z = x \vee (y \vee z)$. The proof $(x \wedge y) \wedge z = x \wedge y \wedge z = x \wedge (y \wedge z)$ is dual, exchanging $\wedge$ for $\vee$ and $\geq$ for $\leq$.

- Idempotence: $x \vee x = x = x \wedge x$, for x is the least element greater than both x and x, and also the greatest element less than both of them.

- Absorption: $x \vee (x \wedge y) = x = x \wedge (x \vee y)$, because x is the least element $\geq x,\ x \wedge y$ and the greatest $\leq x,\ x \vee y$.

- Identity: for all $x \in L$ we have $0 \leq x \leq 1$, so $0 \wedge x = 0$ and $0 \vee x = x = x \wedge 1$ and $x \vee 1 = 1$.

- De Morgan's laws: $(x \vee y)' = x' \wedge y'$ and $(x \wedge y)' = x' \vee y'$. For the first, note that

$$\begin{aligned}(x' \wedge y') \wedge (x \vee y) &= (x' \wedge y' \wedge x) \vee (x' \wedge y' \wedge y) = (0 \wedge y') \vee (x' \wedge 0) = 0 \vee 0 = 0,\\ (x' \wedge y') \vee (x \vee y) &= (x' \vee x \vee y) \wedge (y' \vee x \vee y) = (1 \vee y) \wedge (x \vee 1) = 1 \wedge 1 = 1;\end{aligned}$$

  since $(x \vee y)'$ is postulated to be unique with these properties, we have $(x \vee y)' = x' \wedge y'$. The other law $(x \wedge y)' = x' \vee y'$ is dual; the proof is the same, exchanging $\wedge$ for $\vee$ and vice versa everywhere.

From now on write $\cdot$ for $\wedge$. We prove a few more miscellaneous facts.

- $a + b = (ab') \vee (a'b) = (a \vee a')(a \vee b)(b' \vee a')(b' \vee b) = 1(a \vee b)(a' \vee b')1 = (a \vee b)(a' \vee b')$.

- $(a + b)' = \big[(a \vee b)(a' \vee b')\big]' = (a \vee b)' \vee (a' \vee b')' = a'b' \vee ab$.

- $1' = 0$: for $1 \wedge 0 = 1$ and $1 \wedge 0 = 0$.

- $1 + a = (a \vee 1)(a' \vee 0) = 1a' = 1 \wedge a' = a'$.

Now we can prove the ring axioms for $A(L)$.

- Commutativity of $+$: $a + b = (a \vee b)(a' \vee b') = (b \vee a)(b' \vee a') = b + a$.

- Associativity of $\cdot$: $\cdot$ is $\wedge$.

- Commutativity of $\cdot$: $\cdot$ is $\wedge$.

- Associativity of $+$: $(a+b)+c$ is

$$\begin{aligned}\big([a+b]\vee c\big)\big([a+b]'\vee c'\big) &= (ab'\vee a'b\vee c)(a'b'\vee ab\vee c')\\ &= ab'a'b'\vee ab'ab\vee ab'c'\vee\\ &\quad a'ba'b'\vee a'bab\vee a'bc'\vee\\ &\quad ca'b'\vee cab\vee cc' \qquad (1.2)\\ &= 0\vee 0\vee ab'c'\vee 0\vee 0\vee a'bc'\vee ca'b'\vee cab\vee 0.\\ &= ab'c'\vee a'bc'\vee a'b'c\vee abc.\end{aligned}$$

  Write $x^+ = x$ and $x^- = x'$. Then $(a+b)+c$ is the supremum of the four possible terms $a^\pm b^\pm c^\pm$ with an odd number of $+$'s. This is invariant under permutations of a, b, c, so by commutativity, $a+(b+c) = (b+c)+a = (a+b)+c$.

- $1a = a$: for $1a = 1\wedge a = a$.

- $a+0 = a$: for $a+0 = (a\vee 0)(a'\vee 1) = a1 = a$.

- $a = -a$: for $a+a = (a\vee a)(a'\vee a') = aa' = 0$.

- Distributivity of $\cdot$ over $+$: $a(b+c) = a\big([bc']\vee[b'c]\big) = abc'\vee ab'c$, while

$$\begin{aligned}ab+ac = (ab\vee ac)\big([ab]'\vee[ac]'\big) &= ab[ab]'\vee ac[ab]'\vee ab[ac]'\vee ac[ac]'\\ &= 0\vee ac[a'\vee b']\vee ab[a'\vee c']\vee 0\\ &= aca'\vee acb'\vee aba'\vee abc'\\ &= 0\vee abc'\vee 0\vee ab'c = abc'\vee ab'c.\end{aligned}$$

- Boolean ring: $a^2 = a\wedge a = a$ by idempotence of $\wedge$.

Conversely, starting from a Boolean ring A, define an ordering on A as follows: $a \le b$ means that $a = ab$. Show that, with respect to this ordering, A is a Boolean lattice. In this way we obtain a one-to-one-correspondence between (isomorphism classes of) Boolean rings and (isomorphism classes of) Boolean lattices.

Write $L = L(A)$ for ordered set. We verify the partial order axioms, the lattice axioms, and the Boolean algebra axioms.

- $\le$ is reflexive: $a = aa$, so $a \le a$.

- $\le$ is antisymmetric: Suppose $a \le b \le a$. Then $a = ab$ and $b = ab$, so $a = b$.

- $\le$ is transitive: Let $a \le b \le c$. Then $a = ab$ and $b = bc$, so $a = ab = a(bc) = (ab)c = ac$ and $a \le c$.

- Binary suprema exist in $\langle L, \le\rangle$: Let $a\vee b = a+b+ab$. We have $a(a\vee b) = a(a+b+ab) = a^2+ab+a^2b = a$ by [1.11.i], so $a \le a\vee b$, and symmetrically $b \le a\vee b$. Now suppose a, $b \le c$. Then $a = ac$ and $b = bc$, so $(a\vee b)c = (a+b+ab)c = ac+bc+a(bc) = a+b+ab = a\vee b$, and $a\vee b \le c$. This shows $a\vee b$ is the least upper bound of a, b in the partial order $\langle L, \le\rangle$.

- Binary infima exist in $\langle L, \le\rangle$: Let $a\wedge b = ab$. Then $(a\wedge b)a = aba = ab = a\wedge b$, so $a\wedge b \le a$, and symmetrically $a\wedge b \le b$. Now suppose $c \le a$, b. Then $c = ca = cb$, so $c(a\wedge b) = c(ab) = (ca)b = cb = c$, and so $c \le a\wedge b$. This shows $a\wedge b$ is the greatest lower bound of a, b in the partial order $\langle L, \le\rangle$.

- A least element exists in $\langle L, \le\rangle$: For any $a\in A$ we have $0 = 0a$, so $0 \le a$.

- A greatest element exists in $\langle L, \le\rangle$: For any $a\in A$ we have $a = a1$, so $a \le 1$.

- $\wedge$ distributes over $\vee$: $(a\vee b)\wedge c = (a+b+ab)c = ac+bc+abc = ac+bc+(ac)(bc) = ac\vee bc = (a\wedge c)\vee(b\wedge c)$.

- $\vee$ distributes over $\wedge$: $(a \wedge b) \vee c = ab \vee c = ab + c + abc$, while also

$$\begin{aligned}(a \vee c) \wedge (b \vee c) &= (a + c + ac)(b + c + bc)\\ &= ab + ac + abc + cb + cc + cbc + acb + acc + acbc\\ &= ab + 2ac + 3abc + 2bc + c\\ &= ab + c + abc.\end{aligned}$$

- Each $a \in A$ has a unique complement: Suppose a' is such that $a \vee a' = 1$ and $a \wedge a' = 0$. Then $aa' = 0$, while $1 = a + a' + aa' = a + a'$. Then $a' = 1 - a = 1 + a$. Thus the complement, if it exists, is unique. And $a' = 1 + a$ is indeed a complement: $a \wedge a' = a(1 + a) = a + a^2 = 0$, while $a \vee a' = a + a' + aa' = a + (1 + a) + 0 = 1$.

We finally should verify that these correspondences are inverse. Let A be a Boolean ring, and $A' = A\big(L(A)\big)$. Then $\cdot_{A'} = \wedge_{L(A)} = \cdot_A$, and addition in A' is

$$a +_{A'} b = ab' \vee a'b = ab' +_A a'b +_A ab'a'b = ab' +_A a'b = a(1 +_A b) +_A (1 +_A a)b = a +_A ab +_A b +_A ab = a +_A b,$$

so $A\big(L(A)\big) = A$. On the other hand let L be a Boolean algebra and $L' = L\big(A(L)\big)$. Then $\wedge_{L'} = \cdot_{A(L)} = \wedge_L$. Finally the join in L' is given by

$$\begin{aligned}x \vee_{L'} y = x + y + xy &\underset{1.2}{\overset{\text{Eq.}}{=}} xyxy \vee_L x'y'xy \vee_L x'y(xy)' \vee_L xy'(xy)'\\ &= xy \vee_L 0 \vee_L x'y(x' \vee_L y') \vee_L xy'(x' \vee_L y')\\ &= xy \vee_L x'yx' \vee_L x'yy' \vee_L xy'x' \vee_L xy'y'\\ &= xy \vee_L x'y \vee_L xy'\\ &= xy \vee_L xy' \vee_L yx \vee_L yx'\\ &= x(y \vee_L y') \vee_L y(x \vee_L x')\\ &= x \vee_L y\end{aligned}$$

From the last two exercises deduce Stone's theorem, that every Boolean lattice is isomorphic to the lattice of open-and-closed subsets of some compact Hausdorff topological space.

Let a Boolean algebra L be given, and let A be the associated Boolean ring. By [1.23.iv], $X = \operatorname{Spec}(A)$ is a compact Hausdorff space. Let B be the algebra of simultaneously open and closed sets in X. By the definition of open and closed, it is closed under binary union and intersection, so it is a sublattice of the power set $\langle \mathscr{P}(X), \subseteq \rangle$ under inclusion. By the definition of a topology, $\varnothing, X \in B$. By set algebra, $\cup$ and $\cap$ each distribute over the other. The complement V of an open and closed set U is open and closed, and is the unique $V \subseteq \mathscr{P}(X)$ with $U \cup V = X$ and $U \cap V = \varnothing$. Thus B is a Boolean algebra.

By [1.23.i] and [1.23.iii], B is the set of X_f for $f \in A$, so the correspondence $\phi\colon L \to B$ taking $f \mapsto X_f$ is surjective. Since no nonzero element of A is nilpotent, by [1.17.ii], ϕ is also injective.

To show ϕ is an order isomorphism (hence a Boolean algebra isomorphism), it remains to show that $f \leq g \iff X_f \subseteq X_g$. Now $f \leq g \iff f = fg \implies f \in (g)$, and conversely if $f = ag \in (g)$, then $fg = (ag)g = ag = f$. Thus $f \leq g \iff f \in (g)$. Now

$$f \in (g) \iff \exists n \geq 1 \,\big(f = f^n \in (g)\big) \iff f \in r\big((g)\big) \overset{(1.13)}{\iff} r\big((f)\big) \subseteq r\big((g)\big),$$

and from the proof of [1.17.iv], $r\big((f)\big) \subseteq r\big((g)\big) \iff X_f \subseteq X_g$. Therefore $f \leq g \iff X_f \subseteq X_g$, so ϕ is an order isomorphism.

Let A be a ring. The subspace of Spec(A) *consisting of the* maximal *ideals of A, with the induced topology, is called the* maximal spectrum *of A and is denoted by* Max(A). *For arbitrary commutative rings it does not have the nice functorial properties of* Spec(A) *(see Exercise 21), because the inverse image of a maximal ideal under a ring homomorphism need not be maximal.*

Let X be a compact Hausdorff space and let $C(X)$ denote the ring of all real-valued continuous functions on X (add and multiply functions by adding and multiplying their values). For each $x \in X$, let $\mathfrak{m}_x$ be the set of all $f \in C(X)$ such that $f(x) = 0$. The ideal $\mathfrak{m}_x$ is maximal, because it is the kernel of the (surjective) homomorphism $C(X) \to \mathbb{R}$ which takes f to $f(x)$. If $\widetilde{X}$ denotes Max$\big(C(X)\big)$, *we have therefore defined a mapping $\mu\colon X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$.*

We shall show that μ is a homeomorphism of X onto $\widetilde{X}$.

i) Let $\mathfrak{m}$ be any maximal ideal of $C(X)$, and let $V = V(\mathfrak{m})$ be the set of common zeros of the functions in $\mathfrak{m}$: that is,

$$V = \{x \in X : f(x) = 0 \text{ for all } f \in \mathfrak{m}\}.$$

Suppose that V is empty. Then for each $x \in X$ there exists $f_x \in \mathfrak{m}$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is an open neighborhood U_x of x in X on which f_x does not vanish. By compactness a finite number of the neighborhoods, say $U_{x_1}, \ldots, U_{x_n}$, cover X. Let

$$f = f_{x_1}^2 + \cdots + f_{x_n}^2.$$

Then f does not vanish at any point of X, hence is a unit in $C(X)$. But this contradicts $f \in \mathfrak{m}$, hence V is not empty. Let x be a point of V. Then $\mathfrak{m} \subseteq \mathfrak{m}_x$, hence $\mathfrak{m} = \mathfrak{m}_x$ because $\mathfrak{m}$ is maximal. Hence μ is surjective.

ii) By Urysohn's lemma (this is the only non-trivial fact required in the argument) the continuous functions separate the points of X. Hence $x \neq y \implies \mathfrak{m}_x \neq \mathfrak{m}_y$, and therefore μ is injective.

iii) Let $f \in C(X)$; let

$$U_f = \{x \in X : f(x) \neq 0\}$$

and let

$$\widetilde{U}_f = \{\mathfrak{m} \in \widetilde{X} : f \notin \mathfrak{m}\}.$$

Show that $\mu(U_f) = \widetilde{U}_f$. The open sets U_f (resp. $\widetilde{U}_f$) form a basis of the topology of X (resp. $\widetilde{X}$) and therefore μ is a homeomorphism.
Thus X can be reconstructed from the ring of functions $C(X)$.

For each $f \in C(X)$, we have

$$x \in U_f \iff f(x) \neq 0 \iff f \notin \mathfrak{m}_x \iff \mathfrak{m}_x \in \widetilde{U}_f,$$

so μ restricts to a bijection $U_f \leftrightarrow \widetilde{U}_f$. It remains to show these sets form bases.

The U_f will form a basis for X if whenever $x \in W \subseteq X$ with W open, there is an $f \in C(X)$ such that $x \in U_f \subseteq W$. But as X is compact Hausdorff, it is normal, and so the Urysohn lemma applies to show closed sets can be separated by continuous functions. Thus there is $f \in C(X)$ such that $f(X \setminus W) = \{0\}$ and $f(x) = 1$, and then evidently $x \in U_f \subseteq W$.

Each $\widetilde{U}_f$ is open the subspace topology inherited from $\operatorname{Spec}(C(X))$, being the intersection of $\widetilde{X}$ with the open set $\operatorname{Spec}(C(X))_f$ of [1.17]. As these sets form a basis for $\operatorname{Spec}(C(X))$ (see [1.17]), the $\widetilde{U}_f$ form a basis for $\widetilde{X}$.

Affine algebraic varieties

Let k be an algebraically closed field and let

$$f_\alpha(t_1, \ldots, t_n) = 0$$

be a set of polynomial equations in n variables with coefficients in k. The set X of all points $x = \langle x_1, \ldots, x_n \rangle \in k^n$ which satisfy these equations is an affine algebraic variety.

Consider the set of all polynomials $g \in k[t_1, \ldots, t_n]$ with the property that $g(x) = 0$ for all $x \in X$. This set is an ideal $I(X)$ in the polynomial ring, and is called the ideal of the variety X. *The quotient ring*

$$P(X) = k[t_1, \ldots, t_n]/I(X)$$

is the ring of polynomial functions on X, because two polynomials g, h define the same polynomial function on X if and only if $g - h$ vanishes at every point of X, that is, if and only if $g - h \in I(X)$.

Let ξ_i be the image of t_i in $P(X)$. The ξ_i $(1 \leq i \leq n)$ are the coordinate functions *on X: if $x \in X$, then $\xi_i(x)$ is the ith coordinate of x. $P(X)$ is generated as a k-algebra by the coordinate functions, and is called the* coordinate ring *(or affine algebra) of X.*

As in Exercise 26, for each $x \in X$ let $\mathfrak{m}_x$ be the ideal of all $f \in P(X)$ such that $f(x) = 0$; it is a maximal ideal of $P(X)$. Hence, if $\widetilde{X} = \operatorname{Max}(P(X))$, we have defined a mapping $\mu : X \to \widetilde{X}$, namely $x \mapsto \mathfrak{m}_x$. It is easy to show that μ is injective: if $x \neq y$, we must have $x_i \neq y_i$ for some i $(1 \leq i \leq n)$, and hence $\xi_i - x_i$ is in $\mathfrak{m}_x$ but not in $\mathfrak{m}_y$, so that $\mathfrak{m}_x \neq \mathfrak{m}_y$. What is less obvious (but still true) is that μ is surjective. *This is one form of Hilbert's Nullstellensatz (see Chapter 7).*

Abbreviate $k[t] := k[t_1, \ldots, t_n]$. As in [1.26], $\mathfrak{m}_x$ is maximal because it is the kernel of the surjective homomorphism $f \mapsto f(x) \colon P(X) \to k$. To be more explicit about what $\mathfrak{m}_x$ looks like, note that if $x = \langle x_1, \ldots, x_n \rangle$, then the polynomial function $\xi_i - x_i \in P(X)$ vanishes at x, so that $\xi_i - x_i \in \mathfrak{m}_x$. On the other hand, since $(t_1 - x_1, \ldots, t_n - x_n)$ is the kernel of the surjective homomorphism $k[t] \twoheadrightarrow k$ taking $1 \mapsto 1$ and $t_i \mapsto x_i$, it is a maximal ideal of $k[t]$, so by the correspondence (1.1) we have $(\xi_1 - x_1, \ldots, \xi_n - x_n) \subseteq \mathfrak{m}_x$ maximal, which shows the the containment must in fact be an equality.

We then want to show the images of these $\mathfrak{m}_x$ are the only maximal ideals of $P(X)$. By (1.1), it will suffice to do this for $X = k^n$ and $P(X) = k[t]$ and then prove that $x \in X \iff I(X) \subseteq \mathfrak{m}_x$, which will be item 8 in a list of remarks that follows.

First we show all maximal ideals of $P(X)$ come from points. One way is to use an equivalent result traditionally called the *weak Nullstellensatz*; see [5.17] for a statement and proof. Another is to use *Zariski's Lemma* ((5.24), [5.18], (7.9)) that any field L finitely generated as an algebra over a field K is a finite algebraic extension of K, which implies both. This is done in [5.19]. Here is a more elementary proof[16] avoiding the technology of Chapter 5, but it too runs through Zariski's Lemma.

Lemma 1.27.1*. *If an integral domain A is algebraic over a field k, then A is a field.*

Proof. Let $0 \neq a \in A$. Since A is a domain and a is algebraic over k, the kernel of the projection $k[x] \twoheadrightarrow k[a]$ is a nonzero prime ideal. But $k[x]$ is a PID, so this kernel is maximal, $k[a]$ is a field, and a is a unit. □

Proposition 1.27.2*. *If $k \subseteq L$ are fields in some integral domain B finitely generated as a k-algebra, L is algebraic over k.*

Proof. Imagine there were a transcendental element $a \in L$, and include a in a finite set T of generators for B as a k-algebra. Select a maximal k-algebraically independent set $S \subseteq T$ containing a, so that the field of fractions L' of B is a finite extension of $k(S)$.[17] Picking an $k(S)$-basis of L' gives us a representation ϕ of multiplication on L' by square matrices over $k(S)$. Writing the entries of the matrices $\phi(t)$ for $t \in T$ as fractions in $k[S]$, let g be the product of all the denominators, so that $\phi(B)$ has entries in $k[S, g^{-1}]$. If $p \in k[a]$ is any irreducible element, then $p^{-1} \in L$ since L is a field, so $\phi(p^{-1})$ is a diagonal matrix with entries p^{-1}. Then this entry lies in $k[S, g^{-1}]$, so there is some positive power g^m such that $g^m p^{-1} \in k[S]$, meaning $p | g^m$. Since p is irreducible and $k[a]$ and $k[S]$, being isomorphic to polynomial rings, are UFDs, it follows p is a scalar multiple of one of those finitely many irreducible factors $q_i \in k[S]$ of g which also lie in $k[a]$. By unique factorization, it follows each element of $k[a]$ is divisible by a q_i; but this obviously doesn't hold of $1 + \prod q_i$, so we have a contradiction. □

Taking $B = L$ in (1.27.2*) yields Zariski's Lemma. One could at this point use the proof of [5.19], but we will follow an alternate route, proving another lemma we will encounter again later.

Lemma 1.27.3*. *If k is a field, B a finitely generated k-algebra, and $A \to B$ a k-algebra homomorphism, then contractions in A of maximals ideal of B are maximal.*

Proof. Since B is a finitely generated k-algebra, it is *a fortiori* finitely generated over A, so $B/\mathfrak{m}$ is a field finitely generated over the integral domain $A/\mathfrak{m}^c$. By (1.27.2*), $B/\mathfrak{m}$ is algebraic over k. Since $A/\mathfrak{m}^c$ is contained in $B/\mathfrak{m}$, it is also algebraic over k too. But then $A/\mathfrak{m}^c$ is a field by (1.27.1*), so $\mathfrak{m}^c$ is maximal. □

Proposition 1.27.4*. *If k is an algebraically closed field, all maximal ideals of the polynomial ring $k[t]$ are of the form $\mathfrak{m}_x$.*

Proof. Let $\mathfrak{m} \lhd k[t]$ be maximal. Then each contraction $\mathfrak{m} \cap k[t_i]$ is maximal in the PID $k[t_i]$ by (1.27.3*), and hence generated by an irreducible polynomial.[18] As k is algebraically closed, this polynomial is linear, so we may rescale it to be $t_i - x_i$ for some $x_i \in k$. But then $t_i - x_i \in \mathfrak{m}$, so $\mathfrak{m}_x \subseteq \mathfrak{m}$ and $\mathfrak{m} = \mathfrak{m}_x$. □

We take this opportunity to collect some remarks, culminating in the desired item 8. If $S \subseteq k[t]$ is a set of polynomials, generating the ideal $\mathfrak{a} = (S)$, we define the *zero set* $Z(S)$ of S to be

$$Z(S) = Z(\mathfrak{a}) := \Big\{ \langle a_1, \ldots, a_n \rangle \in k^n : \forall f \in \mathfrak{a} \, \big[f(a_1, \ldots, a_n) = 0 \big] \Big\};$$

[16] [Kemper, Prop. 1.5]

[17] This proof can be modified to use concepts from later on: pick a finite basis for L' over $k(S)$; each basis element satisfies a monic polynomial with coefficients in $k(S)$. Let $g \in k[S]$ be a common multiple of the denominators of these coefficients. Then L' is integral over $k[S]_g$ by (5.3), so $k[S]_g$ is a field by (5.7) or [5.5.i]. But this is a contradiction, for the polynomial ring $k[S]$ cannot be a Goldman domain by (5.18.1*).

[18] Note that the only reason we need the lemmas is to show this polynomial is not zero.

with this definition,[19] it is clear that an affine algebraic variety X is just a set $Z(S)$ for some dimension n and some $S \subseteq k[t]$; and the maximal ideals of $P(k^n) = k[t]$ referred to above are $\mathfrak{m}_x = I(\{x\})$.

We have the following inclusion relations[20] involving Z and I, for $x \in k^n$, $X, X_1, X_2 \subseteq k^n$, and $S, S_1, S_2 \subseteq k[t]$.

0. $X \subseteq Z(S) \iff S \subseteq I(X)$: for both mean $f(x) = 0$ for all $f \in S$ and all $x \in X$.
1. $X_1 \subseteq X_2 \implies I(X_2) \subseteq I(X_1)$: for if $f \in k[t]$ vanishes on X_2, it also does on the subset X_1.
2. $S_1 \subseteq S_2 \implies Z(S_2) \subseteq Z(S_1)$: for if S_2 annihilates $x \in k^n$, so does the subset S_1.
3. $X \subseteq ZI(X)$: "X is annihilated by everything annihilating X"; apply item 0 to $I(X) \subseteq I(X)$.
4. $S \subseteq IZ(S)$: "S vanishes on everything S vanishes on"; apply item 0 to $Z(S) \subseteq Z(S)$.
5. $I(X) = IZI(X)$: for $X \overset{3.}{\subseteq} ZI(X)$, so $IZI(X) \overset{1.}{\subseteq} I(X)$; but $I(X) \overset{4.}{\subseteq} IZI(X)$.
6. $Z(S) = ZIZ(S)$: for $S \overset{4.}{\subseteq} IZ(S)$, so $ZIZ(S) \overset{2.}{\subseteq} Z(S)$; but $Z(S) \overset{3.}{\subseteq} ZIZ(S)$.
7. $Z(\mathfrak{m}_x) = \{x\}$: if $I(\{x\}) = \mathfrak{m}_x$ annihilates $y \in k^n$, then $\forall i\ (y_i - x_i = 0)$, so $y = x$; and $\{x\} \overset{3.}{\subseteq} Z(\mathfrak{m}_x)$.
8. $X = Z(S) \implies \big[I(X) \subseteq \mathfrak{m}_x \iff x \in X\big]$: if $I(X) \subseteq \mathfrak{m}_x$, then $\{x\} \overset{7.}{=} Z(\mathfrak{m}_x) \overset{2.}{\subseteq} ZI(X) = ZIZ(S) \overset{6.}{=} Z(S) = X$; and if $x \in X$, then $I(X) \overset{1.}{\subseteq} \mathfrak{m}_x$.
9. $r\big(I(X)\big) = I(X)$: Since $\mathfrak{N}(k) = 0$, if $f(x)^m = 0$ for $m \geq 1$, then $f(x) = 0$.

Note as a consequence of item 8 that a variety is non-empty just if its ideal is contained in some $\mathfrak{m}_x$. In particular, if there were some maximal ideal $\mathfrak{m}$ that were not one of the $\mathfrak{m}_x$, we would have $Z(\mathfrak{m}) = \varnothing$.

Let $f_1, \ldots, f_m$ be elements of $k[t_1, \ldots, t_n]$. They determine a polynomial mapping *$\phi\colon k^n \to k^m$: if $x \in k^n$, the coordinates of $\phi(x)$ are $f_1(x), \ldots, f_m(x)$.*

Let X, Y be affine algebraic varieties in k^n, k^m respectively. A mapping $\phi\colon X \to Y$ is said to be regular *if ϕ is the restriction to X of a polynomial mapping from k^n to k^m.*

If η is a polynomial function on Y, then $\eta \circ \phi$ is a polynomial function on X. Hence ϕ induces a k-algebra homomorphism $P(Y) \to P(X)$, namely $\eta \mapsto \eta \circ \phi$. Show that in this way we obtain a one-to-one correspondence between the regular mappings $X \to Y$ and the k-algebra homomorphisms $P(Y) \to P(X)$.

The map $\phi^\#$ induced by ϕ is a ring homomorphism: for all $x \in X$, $\eta, \zeta \in P(Y)$, and $* \in \{+, -, \cdot\}$, we have

$$\big[(\eta * \zeta) \circ \phi\big](x) = (\eta * \zeta)\big(\phi(x)\big) = \eta\big(\phi(x)\big) * \zeta\big(\phi(x)\big) = \big[(\eta \circ \phi) * (\zeta \circ \phi)\big](x).$$

Preservation of k is trivial: for $a \in k$ we have $a \circ \phi = a$ because a takes no arguments.

To see that the correspondence $\phi \mapsto \phi^\#$ is injective, suppose $\phi^\# = \psi^\#$ for ϕ, ψ regular mappings $X \to Y$ induced, respectively, by coordinates $\phi_j, \psi_j\colon k^n \to k$ for $1 \leq j \leq m$. Letting υ_i $(1 \leq i \leq m)$ be the coordinate functions on Y, we then have

$$\phi_i = \upsilon_i \circ \phi = \phi^\#(\upsilon_i) = \psi^\#(\upsilon_i) = \upsilon_i \circ \psi = \psi_i$$

on X, so $\phi_i = \psi_i$ on X; thus $\phi_i - \psi_i \in I(X)$ for each i, and $\phi = \psi$ as regular maps from X.

To see the correspondence is surjective, let λ be a k-algebra homomorphism $P(Y) \to P(X)$. Precomposing with a quotient projection $\pi\colon k[u] := k[u_1, \ldots, u_m] \to P(Y)$ from the polynomial ring, we have a homomorphism $\varkappa\colon k[u] \to P(X)$. By the universal property of polynomial rings, this function is uniquely determined by its values on indeterminates, say $\phi_i = \varkappa(u_i) \in P(X)$, which each define a regular function $X \to k$. Let $\phi\colon X \to k^m$ be the regular function with coordinates ϕ_i. Then if $\eta \in k[u]$, we have

$$\varkappa(\eta) = \eta\big(\varkappa(u_1), \ldots, \varkappa(u_m)\big) = \eta(\phi_1, \ldots, \phi_m) = \eta \circ \phi.$$

[19] This is closely related indeed to the sets $V(E)$ of [1.15], to the extent that the same letter V is often used, and the topology on k^n gotten by taking the $Z(S)$ as closed sets is also called the Zariski topology. The correspondence is gotten by taking $A = k[t]$; then under the bijection $k^n \leftrightarrow \operatorname{Max}(A)$ (to be proved), we have $Z(S) \leftrightarrow V(S) \cap \operatorname{Max}(A)$.

[20] The first three show among other things show Z and I form an antitone *Galois connection* between the powersets $\mathscr{P}\big(k[t]\big)$ and $\mathscr{P}(k^n)$, as partially ordered by inclusion—see e.g. [WPGalois]—and the next four are formal consequences of this Galois connection.

To show $\lambda = \phi^{\#}$ is as hoped, it remains to show that $\operatorname{im}\phi \subseteq Y$. This is the case just if for all $\eta \in I(Y) \subseteq k[u]$ and $x \in X$ we have $\eta\big(\phi(x)\big) = 0$, or in other words if $\eta \circ \phi = 0$; but this is true because $\eta \circ \phi = x(\eta) = \lambda\big(\pi(\eta)\big) = \lambda(0) = 0$.

For later use, note that given $X \xrightarrow{\phi} Y \xrightarrow{\psi} Z$ we have $(\psi \circ \phi)^{\#} = (\phi^{\#} \circ \psi^{\#})$. Indeed, if $\zeta \in P(Z)$, then

$$(\psi \circ \phi)^{\#}(\zeta) = \zeta \circ \psi \circ \phi = \phi^{\#}(\zeta \circ \psi) = \phi^{\#}\big(\psi^{\#}(\zeta)\big). \tag{1.2}$$

This shows the coordinate ring is a *contravariant functor* from the category of affine algebraic varieties and regular maps to the category of finitely generated k-algebras and k-algebra homomorphisms. This functor is actually an equivalence of categories.

Note in particular that in this framework, point inclusions $\{0\} \to \{x\} \hookrightarrow X$ correspond bijectively to k-algebra homomorphisms $P(X) \to k$.

Modules

Exercise 2.2. *i)* $\operatorname{Ann}(M+N)=\operatorname{Ann}(M)\cap\operatorname{Ann}(N)$.

$$a\in\operatorname{Ann}(M+N)\iff 0=a(M+N)=aM+aN\iff aM=aN=0\iff a\in\operatorname{Ann}(M)\cap\operatorname{Ann}(N).$$

ii) $(N:P)=\operatorname{Ann}\big((N+P)/N\big)$.

$$xP\subseteq N\iff x(N+P)=xN+xP\subseteq N\iff x\big((N+P)/N\big)=0\text{ in }(N+P)/N.$$

Proposition 2.9. *i) Let*

$$M'\xrightarrow{u}M\xrightarrow{v}M''\to 0 \tag{2.1}$$

be a sequence of A-modules and homomorphisms. Then Seq. 2.1 is exact $\iff$ for all A-modules N, the sequence

$$0\to\operatorname{Hom}(M'',N)\xrightarrow{\bar v}\operatorname{Hom}(M,N)\xrightarrow{\bar u}\operatorname{Hom}(M',N) \tag{2.2}$$

is exact.

The book proves that if Seq. 2.2 is exact for all N, then Seq. 2.1 is exact. So suppose Seq. 2.1 is exact, let N be any A-module, and consider Seq. 2.2. Let $\phi\in\operatorname{Hom}(M'',N)$. If $0=\phi\circ v=\bar v(\phi)$, then $\phi=0$ since v is surjective; thus $\bar v$ is injective. We have $\bar u\big(\bar v(\phi)\big)=\bar v(\phi)\circ u=\phi\circ v\circ u=\phi\circ 0=0$, so $\bar u\circ\bar v=0$. Now let $\psi\in\operatorname{Hom}(M,N)$ and suppose $\psi\in\ker\bar u$. Then $\psi\circ u=0$, so $\ker v=\operatorname{im}u\subseteq\ker\psi$, and ψ factors through the quotient module $M''=\operatorname{im}v\cong M/u(M')$ (see p. 19): there is $\bar\psi\in\operatorname{Hom}(M'',N)$ with $\psi=\bar\psi\circ v=\bar v(\psi)$. Thus $\psi\in\operatorname{im}\bar v$.

ii) Let

$$0\to N'\xrightarrow{u}N\xrightarrow{v}N'' \tag{2.3}$$

be a sequence of A-modules and homomorphisms. Then Seq. 2.3 is exact $\iff$ for all A-modules M, the sequence

$$0\to\operatorname{Hom}(M,N')\xrightarrow{\bar u}\operatorname{Hom}(M,N)\xrightarrow{\bar v}\operatorname{Hom}(M,N'') \tag{2.4}$$

is exact.

Suppose Seq. 2.3 is exact, let M be an A-module, and consider Seq. 2.4. Let $\phi\in\operatorname{Hom}(M,N')$. If $\phi\in\ker\bar u$, then $u\circ\phi=0$; since u is injective, $\phi=0$. Also $\bar v\big(\bar u(\phi)\big)=v\circ u\circ\phi=0\circ\phi=0$, so $\bar v\circ\bar u=0$. Finally, let $\psi\in\ker\bar v\subseteq\operatorname{Hom}(M,N)$. Then $v\circ\psi=0$, so $\operatorname{im}\psi\subseteq\ker v=\operatorname{im}u$. Since u is injective, $\bar\phi=u^{-1}\circ\phi$ is a well-defined map such that $\bar u(\bar\phi)=u\circ\bar\phi=\phi$.

For the other direction, suppose that for all A-modules M, Seq. 2.4 is exact, and consider Seq. 2.3. First, let $M=\mathbb{Z}$. Suppose $n'\in N'$ is such that $u(n')=0$. Let $\phi\colon\mathbb{Z}\to N'$ be given by $\phi(1)=n'$. Then $(u\circ\phi)(1)=u(n')=0$, so $\phi\in\ker\bar u$; since $\bar u$ is injective, $\phi=0$, so $n'=0$. This shows u is injective. Also, letting $M=N'$, and considering the map $\operatorname{id}_{N'}$, we get $0=\bar v\big(\bar u(\operatorname{id}_{N'})\big)=v\circ u\circ\operatorname{id}_{N'}=v\circ u$. Finally, let $n\in\ker v\subseteq N$, and let $\psi\colon\mathbb{Z}\to N$ be given by $\psi(1)=n$. Then $\operatorname{im}\big(\bar v(\psi)\big)=\operatorname{im}(v\circ\psi)=v(n\mathbb{Z})=0$. By exactness of Seq. 2.4, there is $\bar\psi\colon\mathbb{Z}\to N'$ such that $\bar u(\bar\psi)=u\circ\bar\psi=\psi$; in particular, $n=\psi(1)=u\big(\bar\psi(1)\big)$, so $n\in\operatorname{im}u$, and $\ker v\subseteq\operatorname{im}u$.

Proposition 2.10. *The Snake Lemma.*

Starting with the two middle rows exact and maps α, β, γ making the two middle squares commute, we derive the rest of the commutative diagram. For convenience, we have renamed objects and maps and will tend to omit parentheses. Except where otherwise noted, all deductions are by commutativity or exactness.

$$\begin{tikzcd}
 & \ker\alpha \arrow[r, "x'"] \arrow[d, hook, "i_\alpha"] & \ker\beta \arrow[r, "\lambda'"] \arrow[d, hook, "i_\beta"] & \ker\gamma \arrow[dddll, rounded corners, "\delta"] \arrow[d, hook, "i_\gamma"] & \\
 & A \arrow[r, "x"] \arrow[d, "\alpha"] & B \arrow[r, "\lambda"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & D \arrow[r, "\phi"] \arrow[d, "q_\alpha"] & E \arrow[r, "\psi"] \arrow[d, "q_\beta"] & F \arrow[d, "q_\gamma"] & \\
 & \operatorname{coker}\alpha \arrow[r, "\overline{\phi}"] & \operatorname{coker}\beta \arrow[r, "\overline{\psi}"] & \operatorname{coker}\gamma &
\end{tikzcd}$$

- Note that if $a \in \ker\alpha$, then $\alpha a = 0$, so $\beta x a = \phi\alpha a = 0$, and $xa \in \ker\beta$; thus we can define a restriction $x' \colon \ker\alpha \to \ker\beta$.
- In the same way, we can define a restriction $\lambda' \colon \ker\beta \to \ker\gamma$.
- Since $\phi(\operatorname{im}\alpha) = \operatorname{im}(\beta x)$, ϕ induces a map $\overline{\phi} \colon \operatorname{coker}\alpha \to \operatorname{coker}\beta$ taking $\overline{d} = d + \operatorname{im}\alpha \mapsto \phi d + \operatorname{im}\beta = \overline{\phi d}$.
- $\overline{\psi} \colon \operatorname{coker}\beta \to \operatorname{coker}\gamma$ is defined similarly.

  The new squares all commute by definition.

- We check that the connecting map $\delta \coloneqq q_\alpha \phi^{-1}\beta\lambda^{-1}i_\gamma$ is well defined. Let $c \in \ker\gamma$ and $b \in \lambda^{-1}\{c\}$. Since $\psi\beta b = \gamma\lambda b = \gamma c = 0$, there is a unique $d \in D$ such that $\phi d = \beta b$, so δ can assign the value $\overline{d} = d + \operatorname{im}\alpha$ to c. We made a choice of b in this definition. Suppose $b' \in \lambda^{-1}\{c\}$ as well, and d' is the unique element of $\phi^{-1}\{\beta b'\}$. Since $\lambda(b - b') = c - c = 0$, there is $a \in A$ with $xa = b - b'$. As

  $$\phi d = \beta b = \beta(b' + xa) = \beta b' + \phi\alpha a = \phi(d' + \alpha a),$$

  from the injectivity of ϕ we see $d = d' + \alpha a$, so that $\overline{d} = \overline{d'}$ and δc is well defined.

Now we show exactness of $\ker\alpha \to \ker\beta \to \ker\gamma \to \operatorname{coker}\alpha \to \operatorname{coker}\beta \to \operatorname{coker}\gamma$. First come the easier parts:

- $i_\gamma \lambda' x' = \lambda x i_\alpha = 0 i_\alpha = 0$. As i_γ is a monomorphism, $\lambda' x' = 0$.
- $\overline{\psi}\,\overline{\phi} q_\alpha = q_\gamma \psi\phi = q_\gamma 0 = 0$. As q_α is an epimorphism, $\overline{\psi}\,\overline{\phi} = 0$.
- $\delta\lambda' = q_\alpha\phi^{-1}\beta(\lambda^{-1}i_\gamma\lambda') = q_\alpha\phi^{-1}(\beta i_\beta) = q_\alpha\phi^{-1}0 = 0$.
- $\overline{\phi}\delta = (\overline{\phi} q_\alpha)\phi^{-1}\beta\lambda^{-1}i_\gamma = (q_\beta\phi)\phi^{-1}\beta\lambda^{-1}i_\gamma = (q_\beta\beta)\lambda^{-1}i_\gamma = 0\lambda^{-1}i_\gamma = 0$.

The other containments aren't much worse:

- $\ker\lambda' \subseteq \operatorname{im} x'$: Suppose $b \in \ker\beta \cap \ker\lambda$. Then there is $a \in A$ such that $xa = b$. Now $\phi\alpha a = \beta x a = \beta b = 0$, and since ϕ is injective, $a \in \ker\alpha$; thus $b \in \operatorname{im} x'$.
- $\ker\overline{\psi} \subseteq \operatorname{im}\overline{\phi}$: Suppose $\overline{\psi}\,\overline{e} = \overline{0}$; then there is $c \in C$ such that $\psi e = \gamma c$. As λ is surjective, there is $b \in B$ such that $\lambda b = c$, and then $\psi\beta b = \gamma\lambda b = \gamma c = \psi e$, so $e - \beta b \in \ker\psi = \operatorname{im}\phi$. Letting $a \in A$ be such that $\phi a = e - \beta b$, we see $\overline{\phi}\,\overline{a} = \overline{e} - \overline{\beta b} = \overline{e}$, so $\overline{e} \in \operatorname{im}\overline{\phi}$.
- $\ker\delta \subseteq \operatorname{im}\lambda'$: Suppose $\overline{0} = \delta c$ and pick $b \in \lambda^{-1}\{c\}$. Then $\overline{d} = \overline{0}$ for the unique $d \in \phi^{-1}\{\beta b\}$, so $d \in \operatorname{im}\alpha$. If $\alpha a = d$, then $\beta x a = \phi\alpha a = \phi d = \beta b$, so $b - xa \in \ker\beta$. We have $\lambda(b - xa) = c - 0$, so $c \in \operatorname{im}\lambda'$.
- $\ker\overline{\phi} \subseteq \operatorname{im}\delta$: Suppose $\overline{\phi}(\overline{d}) = \overline{\phi d} = \overline{0}$, so that there exists $b \in \beta^{-1}\{\phi d\}$. Setting $\lambda b = c$, we see $\gamma c = \gamma\lambda b = \psi\beta b = (\psi\phi)d = 0$, so $c \in \ker\gamma$. Now $\delta c = q_\alpha\phi^{-1}\beta\lambda^{-1}c = q_\alpha\phi^{-1}\beta b = q_\alpha\phi^{-1}\phi d = \overline{d}$, so $d \in \operatorname{im}\delta$.

Further, if the first sequence given is short exact (i.e., x is injective), then x', as a restriction of x, is injective; and if the second sequence given is short exact (i.e., ψ is surjective), then $\overline{\psi}$ is surjective, for if $\overline{f} \in \operatorname{coker}\gamma$, there is some $e \in E$ such that $\psi e = f$, and then $\overline{\psi}\,\overline{e} = \overline{f}$.

Proposition 2.12. *Let $M_1, \ldots, M_r$ be A-modules. Then there exists a pair $\langle T, g\rangle$ consisting of an A-module T and an A-multilinear mapping $g\colon M_1 \times \cdots \times M_r \to T$ with the following property:*

Given any A-module P and any A-multilinear mapping $f\colon M_1 \times \cdots \times M_r \to P$, there exists a unique A-homomorphism $f'\colon T \to P$ such that $f' \circ g = f$.

Moreover, if $\langle T, g\rangle$ and $\langle T', g'\rangle$ are two such pairs with this property, then there exists a unique isomorphism $j\colon T \to T'$ such that $j \circ g = g'$.

"The details may safely be left to the reader." First we prove existence. Let C be the free A-module on $M = \prod_{j=1}^{r} M_j$, and let D be the submodule generated by the following elements, for all $x_j, x'_j \in M_j$ ($j = 1, \ldots, r$), and $a \in A$:

$$\langle x_1, \ldots, x_j + x'_j, \ldots, x_r\rangle - \langle x_1, \ldots, x_j, \ldots, x_r\rangle - \langle x_1, \ldots, x'_j, \ldots, x_r\rangle,$$
$$\langle x_1, \ldots, ax_j, \ldots, x_r\rangle - a\langle x_1, \ldots, x_j, \ldots, x_r\rangle.$$

Let $T = C/D$, and write the image of $(x_1, \ldots, x_r) \in C$ as $x_1 \otimes \cdots \otimes x_r \in T$; these elements evidently generate T, and we have, for all $x_j, x'_j \in M_j$ ($j = 1, \ldots, r$), and $a \in A$,

$$x_1 \otimes \cdots \otimes (x_j + x'_j) \otimes \cdots \otimes x_r = (x_1 \otimes \cdots \otimes x_j \otimes \cdots \otimes x_r) + (x_1 \otimes \cdots \otimes x'_j \otimes \cdots \otimes x_r,)$$
$$x_1 \otimes \cdots \otimes ax_j \otimes \cdots \otimes x_r = a(x_1 \otimes \cdots \otimes x_j \otimes \cdots \otimes x_r),$$

so the map $g\colon M \to T$ given by $\langle x_1, \ldots, x_r\rangle \mapsto x_1 \otimes \cdots \otimes x_r$ is A-multilinear.

Let P be an A-module; any map $f\colon M \to P$ extends uniquely to a linear map $\bar{f}\colon C \to P$ since C is freely generated over A by the elements of M. f is A-multilinear just if $\bar{f}$ vanishes on the elements we specified to generate D and thus induces on the quotient a unique A-linear map $f'\colon T \to P$ taking $x_1 \otimes \cdots \otimes x_r \mapsto f(x_1, \ldots, x_r)$; in this case, $f = f' \circ g$.

Now suppose $\langle T', g'\rangle$ has the same universal property as $\langle T, g\rangle$. Then the A-multilinear map $g\colon M \to T$ factors through g' as $g = j \circ g'$ for a unique A-linear map $j\colon T' \to T$. Similarly, $g'\colon M \to T'$ factors through g as $g' = j' \circ g$ for a unique $j'\colon T \to T'$, and we have

$$g = j \circ g' = j \circ j' \circ g.$$

Because $g\colon M \to T$ is itself multilinear, by the definition of a tensor product, there is a unique linear map $i\colon T \to T$ such that $g = i \circ g$; but clearly the identity map id_T has this property, so $j \circ j' = \mathrm{id}_T$. Symmetrically,

$$g' = j' \circ g = j' \circ j \circ g',$$

so $j' \circ j = \mathrm{id}_{T'}$ and j and $j' = j^{-1}$ are isomorphisms.

Proposition 2.14. *Let M, N, P be A-modules. Then there exist the following unique isomorphisms:*
i) $M \otimes N \to N \otimes M$, $\quad x \otimes y \mapsto y \otimes x$;

The map $\langle x, y\rangle \mapsto \langle y, x\rangle \mapsto y \otimes x$ from $M \times N \to N \times M \to N \otimes M$ is bilinear, so it corresponds to a unique linear map $M \otimes N \to N \otimes M$ taking $x \otimes y \mapsto y \otimes x$. The same argument provides a map $N \otimes M \to M \otimes N$ taking $y \otimes x \mapsto x \otimes y$. These maps are clearly inverse on the decomposable elements $x \otimes y \in M \otimes N$ and $y \otimes x \in N \otimes M$, and since these elements generate the modules, the maps are inverse.

ii) $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$, $\quad (x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$;

The book demonstrates the isomorphism $(M \otimes N) \otimes P \to M \otimes N \otimes P$. A symmetric argument provides an isomorphism $M \otimes (N \otimes P) \to M \otimes N \otimes P$.

iii) $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$, $\quad \langle x, y\rangle \otimes z \mapsto \langle x \otimes z, y \otimes z\rangle$;

Let $f\colon (M \oplus N) \times P \to (M \otimes P) \oplus (N \otimes P)$ be given by $f\big(\langle x, y\rangle, z\big) := \langle x \otimes z, y \otimes z\rangle$. We claim it is A-bilinear. Let

$x, x' \in M$, $y, y' \in N$, $z, z' \in P$, and $a \in A$: then indeed

$$\begin{aligned}
f\big(a\langle x, y\rangle, z\big) &= f\big(\langle ax, ay\rangle, z\big) = \langle ax \otimes z, ay \otimes z\rangle = \big\langle a(x \otimes z), a(y \otimes z)\big\rangle = a\langle x \otimes z, y \otimes z\rangle = af\big(\langle x, y\rangle, z\big),\\
f\big(\langle x, y\rangle, az\big) &= \langle x \otimes az, y \otimes az\rangle = \big\langle a(x \otimes z), a(y \otimes z)\big\rangle = a\langle x \otimes z, y \otimes z\rangle = af\big(\langle x, y\rangle, z\big),\\
f\big(\langle x, y\rangle + \langle x', y'\rangle, z\big) &= f\big(\langle x + x', y + y'\rangle, z\big) = \big\langle (x + x') \otimes z, (y + y') \otimes z\big\rangle\\
&= \langle x \otimes z, y \otimes z\rangle + \langle x' \otimes z, y' \otimes z\rangle = f\big(\langle x, y\rangle, z\big) + f\big(\langle x', y'\rangle, z\big),\\
f\big(\langle x, y\rangle, z + z'\big) &= \big\langle x \otimes (z + z'), y \otimes (z + z')\big\rangle = \langle x \otimes z + x \otimes z', y \otimes z + y \otimes z'\rangle\\
&= \langle x \otimes z, y \otimes z\rangle + \langle x \otimes z', y \otimes z'\rangle = f\big(\langle x, y\rangle, z\big) + f\big(\langle x, y\rangle, z'\big).
\end{aligned}$$

Thus f factors through the canonical map $g\colon (M \oplus N) \times P \to (M \oplus N) \otimes P$ as $f = f' \otimes g$, where

$$\begin{aligned}
f'\colon (M \oplus N) \otimes P &\to (M \otimes P) \oplus (N \otimes P),\\
\langle x, y\rangle \otimes z &\mapsto \langle x \otimes z, y \otimes z\rangle
\end{aligned}$$

is A-linear.

On the other hand, we also have bilinear maps

$$\begin{aligned}
j_1\colon M \times P &\to (M \oplus N) \otimes P,\\
\langle x, z\rangle &\mapsto \langle x, 0\rangle \otimes z
\end{aligned}
\qquad \text{and} \qquad
\begin{aligned}
j_2\colon N \times P &\to (M \oplus N) \otimes P,\\
\langle y, z\rangle &\mapsto \langle 0, y\rangle \otimes z,
\end{aligned}$$

which give rise to linear maps

$$\begin{aligned}
\bar{j}_1\colon M \otimes P &\to (M \oplus N) \otimes P,\\
x \otimes z &\mapsto \langle x, 0\rangle \otimes z
\end{aligned}
\qquad \text{and} \qquad
\begin{aligned}
\bar{j}_2\colon N \otimes P &\to (M \oplus N) \otimes P,\\
y \otimes z &\mapsto \langle 0, y\rangle \otimes z.
\end{aligned}$$

By the universal property of the direct sum, we get a unique A-linear map

$$\begin{aligned}
j\colon (M \otimes P) \oplus (N \otimes P) &\to (M \oplus N) \otimes P,\\
\langle x \otimes z, 0\rangle &\mapsto \langle x, 0\rangle \otimes z,\\
\langle 0, y \otimes z\rangle &\mapsto \langle 0, y\rangle \otimes z.
\end{aligned}$$

Now the image of $\langle x, y\rangle \otimes z \in (M \oplus N) \otimes P$ under $j \circ f$ is

$$j(x \otimes z, y \otimes z) = \langle x, 0\rangle \otimes z + \langle 0, y\rangle \otimes z = \langle x, y\rangle \otimes z,$$

and since these elements generate $(M \oplus N) \otimes P$, we see $j \circ f$ is the identity. Similarly, the images of the elements $\langle x \otimes z, 0\rangle$ and $\langle 0, y \otimes z\rangle$ of $(M \otimes P) \oplus (N \otimes P)$ under $f \circ j$ are respectively

$$f\big(\langle x, 0\rangle \otimes z\big) = \langle x \otimes z, 0\rangle \quad \text{and} \quad f\big(\langle 0, y\rangle \otimes z\big) = \langle 0, y \otimes z\rangle,$$

and these elements generate $(M \otimes P) \oplus (N \otimes P)$, so $f \circ j$ is the identity, and f and j are inverse isomorphisms.

iii) For any A-modules M_i $(i \in I)$ and N,*

$$N \otimes \bigoplus_{i \in I} M_i \cong \bigoplus_{i \in I} (N \otimes M_i).$$[1]

Proof. For each finite subset $J \subseteq I$, write $M_J := \bigoplus_{j \in J} M_j$. Then $M_J + M_{J'} = M_{J \cup J'}$, for all finite $J, J' \subseteq I$. Taking all maps to be the natural insertions, [2.17] shows $M \cong \varinjlim M_J$. Similarly, for $J \subseteq J'$, the natural injection $\bigoplus_{j \in J}(N \otimes M_j) \to \bigoplus_{j \in J'}(N \otimes M_j)$, can be viewed as an inclusion, and [2.17] again says $\varinjlim_J \Big(\bigoplus_{j \in J}(N \otimes M_j)\Big) \cong \bigoplus_{i \in I}(N \otimes M_i)$. Thus

$$N \otimes \bigoplus_{i \in I} M_i \overset{[2.17]}{\cong} N \otimes \varinjlim_J M_J \overset{[2.20]}{\cong} \varinjlim_J (N \otimes M_J) \overset{(2.14.\text{iii})}{\cong} \varinjlim_J \Big(\bigoplus_{j \in J}(N \otimes M_j)\Big) \overset{[2.17]}{\cong} \bigoplus_{i \in I}(N \otimes M_i). \qquad \square$$

[1] This generalizes (2.14.iii) and uses independent later exercises regarding direct limits.

iv) $A \otimes M \to M, \qquad a \otimes x \mapsto ax.$

By the definition of an A-module M there is a bi-additive map $\mu\colon A \times M \to M$, A-linear in the first variable. The required identity $\mu\big(a, \mu(b, m)\big) = \mu(ab, m)$ shows that μ is A-linear in the second variable if we consider M to have the A-module structure induced by μ. Thus, with $g\colon A \times M \to A \otimes M$ the canonical map, we get a unique factorization $\mu = \mu' \circ g$, where $\mu'\colon A \otimes M \to M$ is A-linear and $\mu'(a \otimes x) = ax$. On the other hand there is also an obviously A-linear map $\iota\colon M \to A \otimes M$ given by $x \mapsto 1 \otimes x$. We check that these maps are inverse:

$$\iota\big(\mu'(a \otimes x)\big) = \iota(ax) = 1 \otimes ax = a \otimes x \quad \text{and} \quad \mu'\big(\iota(x)\big) = \mu'(1 \otimes x) = x.$$

Exercise 2.15. *Let A, B be rings, let M be an A-module, P a B-module, and N an (A, B)-bimodule (that is, N is simultaneously an A-module and a B-module and the two structures are compatible in the sense that $a(xb) = (ax)b$ for all $a \in A$, $b \in B$, $x \in N$). Then $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ an A-module, and we have*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

As in the proof of (2.14.iii), for each $z \in P$ we have a map $f_z\colon M \times N \to M \otimes_A (N \otimes_B P)$ given by $\langle x, y\rangle \mapsto x \otimes (y \otimes z)$, which we claim is A-bilinear in the first two variables. Bi-additivity is clear, and for $a \in A$ we have

$$\begin{aligned} f_z(ax, y) &= ax \otimes (y \otimes z) = a\big(x \otimes (y \otimes z)\big) = af_z(x, y),\\ f_z(x, ay) &= x \otimes (ay \otimes z) = x \otimes a(y \otimes z) = a\big(x \otimes (y \otimes z)\big) = af_z(x, y). \end{aligned}$$

Thus each f_z induces an A-linear map $\bar{f}_z\colon M \otimes_A N \to M \otimes_A (N \otimes_B P)$ taking $x \otimes y \mapsto x \otimes (y \otimes z)$. Allowing z to vary, we have a bi-additive map $g\colon (M \otimes_A N) \times P \to M \otimes_A (N \otimes_B P)$ taking $\langle x \otimes y, z\rangle \mapsto \bar{f}_z(x \otimes y)$. This g is obviously A-linear in the first variable, and is B-bilinear since for $b \in B$ we have

$$\begin{aligned} g\big((x \otimes y)b, z\big) &= g(x \otimes yb, z) = x \otimes (yb \otimes z) = x \otimes (y \otimes z)b = \big(x \otimes (y \otimes z)\big)b = g(x \otimes y, z)b,\\ g(x \otimes y, zb) &= x \otimes (y \otimes zb) = x \otimes (y \otimes z)b = \big(x \otimes (y \otimes z)\big)b = g(x \otimes y, z)b. \end{aligned}$$

Thus, by the universal property, g gives rise to an (A, B)-linear map $\bar{g}\colon (M \otimes_A N) \otimes_B P \to M \otimes_A (N \otimes_B P)$ taking $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z)$. A symmetric argument gives the inverse map $x \otimes (y \otimes z) \mapsto (x \otimes y) \otimes z$.

Exercise 2.20. *If $f\colon A \to B$ is a ring homomorphism and M is a flat A-module, then $M_B = B \otimes_A M$ is a flat B-module.*

Let $j\colon N_1 \rightarrowtail N_2$ be any injective B-module homomorphism. By (2.19), to show M_B is a flat B-module it suffices to show $j \otimes \mathrm{id}_{M_B}\colon N_1 \otimes_B M_B \to N_2 \otimes_B M_B$ is injective. By restricting scalars along f, we can consider all modules as A-modules, and find canonical A-module isomorphisms

$$N_i \otimes_B M_B = N_i \otimes_B (B \otimes_A M) \overset{(2.15)}{\cong} (N_i \otimes_B B) \otimes_A M \underset{(2.14.\mathrm{iv})}{\overset{(2.14.\mathrm{i})}{\cong}} N_i \otimes_A M.$$

Since j is still injective considered as an A-module homomorphism and M is flat, $j \otimes \mathrm{id}_M\colon N_1 \otimes_A M \to N_2 \otimes_A M$ is injective. Composing on both sides with the canonical isomorphisms yields

$$x \otimes y \mapsto (x \otimes 1) \otimes y \mapsto x \otimes (1 \otimes y) \mapsto j(x) \otimes (1 \otimes y) \mapsto \big(j(x) \otimes 1\big) \otimes y \mapsto j(x) \otimes y$$

which then must also be injective; but this is $j \otimes \mathrm{id}_{M_B}$.

Proposition 2.21*. *The direct sum M of a family of A-modules M_i $(i \in I)$ is characterized up to isomorphism by the following universal property: there exists a family of homomorphisms $j_i\colon M_i \to M$ such that for any A-module N and family of homomorphisms $f_i\colon M_i \to N$, there exists a unique homomorphism $f\colon M \to N$ such that $f_i = f \circ j_i$ for all $i \in I$.*

For each $x = \langle x_i\rangle \in M$, write $p_i(x) = x_i \in M_i$; then the *projections* $p_i\colon M \to M_i$ are surjective homomorphisms. For each $x_i \in M_i$, write $j_i(x_i)$ for the unique element $y \in M$ such that $p_i(y) = x_i$ and $p_t(y) = 0$ for all $t \neq i$. These *insertions* $j_i\colon M_i \to M$ are injective homomorphisms. Note that $p_i \circ j_i = \mathrm{id}_{M_i}$, while $p_i \circ j_t = 0$ for $t \neq i$.

Since for any $x \in M$ we have only finitely many $p_i(x) \neq 0$, it follows $x = \sum_{i \in I} j_i\big(p_i(x)\big)$, or $\mathrm{id}_M = \sum(j_i \circ p_i)$. Thus for any homomorphism $f\colon M \to N$ we have

$$f = f \circ \mathrm{id}_M = f \circ \Big(\sum(j_i \circ p_i)\Big) = \sum(f \circ j_i \circ p_i).$$[2]

[2] So $f\colon \langle x_i\rangle \mapsto \sum f_i(x_i)$.

Thus f is uniquely determined by the maps $f \circ j_i \circ p_i$, and since each $p_i \colon M \to M_i$ is surjective, by the maps $f \circ j_i$. On the other hand, given an arbitrary family of maps $f_i \colon M_i \to N$, we can define $f \colon M \to N$ by $f = \sum_t (f_t \circ p_t)$, and precomposing with j_i, we get $f \circ j_i = \sum_t (f_t \circ p_t \circ j_i) = f_i \circ p_i \circ j_i = f_i$. Thus M satisfies the universal property.

Now suppose another module M' and family of homomorphisms $j'_i \colon M_i \rightarrowtail M'$ also have this property. Then associated to the maps $j_i \colon M_i \to M$, there is a unique $u \colon M' \to M$ such that each $j_i = u \circ j'_i$, and associated to the maps $j'_i \colon M_i \to M'$, there is a unique $u' \colon M \to M'$ such that each $j'_i = u' \circ j_i$. It follows each $(u \circ u') \circ j_i = u \circ j'_i = j_i$. By assumption, associated to the $j_i \colon M_i \to M$ there is a unique map $j \colon M \to M$ such that $j_i = j \circ j_i$; since both id_M and $u \circ u'$ meet this criterion, it follows that the two are equal. Symmetrically, $u' \circ u = \mathrm{id}_{M'}$, so $M \cong M'$.

Proposition 2.22*. *Let $f_i \colon M_i \to N_i$ $(i \in I)$ be a family A-module homomorphisms, and M and N the respective direct sums of the M_i and the N_i. Write j_i for the insertions $M_i \rightarrowtail M$, k_i for the insertions $N_i \rightarrowtail N$, p_i for the projections $M \twoheadrightarrow M_i$, and q_i for the projections $N \twoheadrightarrow N_i$. Then there is a unique* direct sum *map $f = \bigoplus_{i \in I} f_i \colon M \to N$ such that*

$$f_i = q_i \circ f \circ j_i \quad \text{and} \quad q_i \circ f \circ j_t = 0 \text{ for } i \neq t.$$

Moreover,
i) f is injective if and only if each f_i is injective;
ii) f is surjective if and only if each f_i is surjective.

The map $\langle x_i \rangle \mapsto \big\langle f_i(x_i) \big\rangle$ satisfies the conditions on f.[3] Since any other g satisfying the equations takes $j_i(x_i)$ to $k_i\big(f_i(x_i)\big)$, it follows by additivity that $g \colon \langle x_i \rangle \mapsto \big\langle f_i(x_i) \big\rangle$ for all $\langle x_i \rangle \in M$, so $g = f$.[4]

i): Suppose all f_i are injective. If $f\big(\langle x_i \rangle\big) = \big\langle f_i(x_i) \big\rangle = 0$, then each $f_i(x_i) = 0$, so each $x_i = 0$, and $\langle x_i \rangle = 0$.[5]
If some f_i takes a nonzero x_i to 0, then f takes its image $j(x_i)$ to 0, and so is also not injective.[6]

ii): Let $y = \langle y_i \rangle \in N$ be given. By assumption, there is for each i an $x_i \in M_i$ with $f_i(x_i) = y_i$; if $y_i = 0$, we may take $x_i = 0$. Then $x = \langle x_i \rangle \in M$ and $f(x) = y$, so f is surjective.[7]
If $y_i \in N_i$ is not in $\operatorname{im} f_i$, then $k_i(y_i)$ cannot be in the image of $f \colon \langle x_i \rangle \mapsto \big\langle f_i(x_i) \big\rangle$, so f is not surjective.[8]

EXERCISES

Show that $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$ if m, n are coprime.

Since m, n are coprime, by Bézout's lemma there are a, $b \in \mathbb{Z}$ such that $am + bn = 1$.[9] Let $x \otimes y \in (\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$. Then $x \otimes y = (am + bn)(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = 0$.

Let A be a ring, $\mathfrak{a}$ an ideal, M an A-module. Show that $(A/\mathfrak{a}) \otimes_A M$ is isomorphic to $M/\mathfrak{a}M$.

Applying the right exact functor $- \otimes_A M$ to the short exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$, we see the sequence

$$\mathfrak{a} \otimes M \xrightarrow{j} A \otimes M \to (A/\mathfrak{a}) \otimes M \to 0$$

is exact, so

$$(A/\mathfrak{a}) \otimes M \cong (A \otimes M)/\operatorname{im} j.$$

But the absorption isomorphism $A \otimes M \to M$ of (2.14.iv) sends $\operatorname{im} j \to \mathfrak{a}M$, so $(A \otimes M)/\operatorname{im} j \cong M/\mathfrak{a}M$.

[3] More formally, by (2.21), there is a unique $f \colon M \to N$ with $f \circ j_i = k_i \circ f_i \colon M_i \to N$. Now each $q_i \circ f \circ j_i = q_i \circ k_i \circ f_i = f_i$, and $q_i \circ f \circ j_t = (q_i \circ k_t) \circ f_t = 0$ for $t \neq i$.

[4] Suppose that g also satisfies the first equation. Then each $k_i \circ f_i = k_i \circ q_i \circ g \circ j_i = g \circ j_i$, so by uniqueness in (2.21), $f = g$.

[5] Alternately, $f = \sum_{i,t} k_i \circ q_i \circ f \circ j_t \circ p_t = \sum k_i \circ q_i \circ f \circ j_i \circ p_i = \sum k_i \circ f_i \circ p_i$. Since $(\operatorname{im} q_i) \cap (\sum_{t \neq i} \operatorname{im} q_t) = 0$, we know $\ker f = \bigcap \ker(k_i \circ f_i \circ p_i)$. Since each $k_i \circ f_i$ is injective, this is $\bigcap \ker p_i = 0$.

[6] If $f = \sum k_t \circ f_t \circ p_t$ is injective, so is $f \circ j_i = \sum_t k_t \circ f_t \circ p_t \circ j_i = k_i \circ f_i$. Since k_i is injective, so is f_i.

[7] Proceeding formally, since each $f_i = q_i \circ f \circ j_i$ is surjective, so is each $q_i \circ f$. Since $\mathrm{id}_N = \sum k_i \circ q_i$, we have $f = \mathrm{id}_N \circ f = \sum k_i \circ q_i \circ f$, so $\operatorname{im} f = \sum \operatorname{im}(k_i \circ q_i \circ f) = \sum k_i(N_i) = N$.

[8] Since $f_i \circ p_i = q_i \circ f \circ j_i \circ p_i = q_i \circ f \circ \sum (j_t \circ p_t) = q_i \circ f$, if some $y_i \in N_i$ is not in $\operatorname{im} f_i$, it is not in the image of $f_i \circ p_i = q_i \circ f$, and so $k_i(y_i) \in N_i$ is not in the image of $k_i \circ q_i \circ f = f$.

[9] [MWBezout]; Another way of putting this is that m and n being coprime in the arithmetic sense of having no common irreducible factors implies that (m) and (n) are coprime in the algebraic sense (p. 7) that $(m) + (n) = (1)$.

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

Let $\mathfrak{m}$ be the maximal ideal and $k = A/\mathfrak{m}$ the residue field. The scalar extensions $M_k \coloneqq k \otimes_A M$ and N_k are k-vector spaces. That $M \otimes N = 0$ implies

$$M_k \otimes N_k = (k \otimes M) \otimes (k \otimes N) \underset{(2.14.\mathrm{iv})}{\overset{(2.14.\mathrm{iii})}{\cong}} k \otimes (M \otimes N) = (M \otimes N)_k = 0.$$

But dimension of vector spaces is multiplicative under tensor, so M_k or $N_k = 0$. Without loss of generality, assume $M_k = 0$. By [2.2], $M_k \cong M/\mathfrak{m}M$, so $\mathfrak{m}M = M$. By Nakayama's Lemma (2.6), since M is finitely generated and $\mathfrak{m}$ is the Jacobson radical, we have $M = 0$.

Let M_i $(i \in I)$ be any family of A-modules, and let M be their direct sum. Prove that M is flat $\iff$ each M_i is flat.

Let an A-linear map $j \colon N' \to N$ be given. Using the isomorphisms of (2.14.iii*) identifies $j \otimes \mathrm{id}_M$ with a map $h \colon \bigoplus_{i\in I}(N' \otimes M_i) \to \bigoplus_{i \in I}(N' \otimes M_i)$, and the compositions

$$N' \otimes M_i \rightarrowtail \bigoplus_{i\in I}(N' \otimes M_i) \xrightarrow{\sim} N' \otimes M \xrightarrow{j \otimes \mathrm{id}_M} N \otimes M \xrightarrow{\sim} \bigoplus_{i\in I}(N \otimes M_i) \twoheadrightarrow N \otimes M_i$$

are $j \otimes \mathrm{id}_{M_i}$, the associated maps $N' \otimes M_i \to N \otimes M_t$ for $t \neq i$ being zero. Thus h is the direct sum of the $j \otimes \mathrm{id}_{M_i}$, and by (2.22.i*), $j \otimes \mathrm{id}_M$ is injective just if they are.

If the M_i are flat and j is injective, then by (2.19) each of the $j \otimes \mathrm{id}_{M_i}$ are as well, and so $j \otimes \mathrm{id}_M$ is. Hence M is flat. If M_i is not flat, there exists a j such that $j \otimes \mathrm{id}_{M_i}$ is not injective, and so $j \otimes \mathrm{id}_M$ is not. Hence M is not flat.

Let $A[x]$ be the ring of polynomials in one indeterminate over a ring A. Prove that $A[x]$ is a flat A-algebra.

A is a flat A-module, for by (2.14.iv) the functor $- \otimes_A A$ is naturally isomorphic to the identity functor. Let $M_i = Ax^i \subseteq A[x]$ for $i \in \mathbb{N}$. Each $M_i \cong A$ as an A-module, and so is flat. Then as a module, $A[x] = \bigoplus_{i \in \mathbb{N}} M_i$ is flat by [2.4].

For any A-module M, let $M[x]$ denote the set of all polynomials in x with coefficients in M, that is to say expressions of the form

$$m_0 + m_1 x + \cdots + m_r x^r \quad (m_i \in M).$$

Defining the product of an element of $A[x]$ and an element of $M[x]$ in the obvious way, show that $M[x]$ is an $A[x]$-module.

As an A-module, we have $M[x] \cong \bigoplus_{n \in \mathbb{N}} Mx^n$. We define the action of $A[x]$ on $M[x]$ by $(\sum a_i x^i)(\sum m_j x^j) = \sum c_k x^k$, where $c_k = \sum_{i+j=k} a_i m_j$. We check the distributivity and associativity. Let $f(x) = \sum_i a_i x^i$ and $g(x) = \sum_j b_j x^j \in A[x]$ and $m(x) = \sum_k m_k x^k$ and $n(x) = \sum_k n_k x^k \in M[x]$. Associativity is given by

$$\big[f(x)g(x)\big]m(x) = \left[\sum_l \Big(\sum_{i+j=k} a_i b_j\Big) x^k\right]\Big(\sum_l m_l x^l\Big) = \sum_p \left(\sum_{k+l=p} \Big(\sum_{i+j=k} a_i b_j\Big) m_k\right) x^p = \sum_p \Big(\sum_{i+j+k=p} a_i b_j m_k\Big) x^p;$$

$$f(x)\big[g(x)m(x)\big] = \Big(\sum_i a_i x^i\Big)\left[\sum_l \Big(\sum_{j+k=l} b_j m_k\Big) x^l\right] = \sum_p \left(\sum_{i+l=p} a_i \Big(\sum_{j+k=l} b_j m_k\Big)\right) x^p = \sum_p \Big(\sum_{i+j+k=p} a_i b_j m_k\Big) x^p.$$

Distributivity is given by

$$\begin{aligned}\big[f(x) + g(x)\big]m(x) &= \Big(\sum_i (a_i + b_i) x^i\Big)\Big(\sum_k m_k x^k\Big) = \sum_l \Big(\sum_{i+k=l} (a_i m_k + b_i m_k)\Big) x^l \\ &= \Big(\sum_i a_i x^i\Big)\Big(\sum_k m_k x^k\Big) + \Big(\sum_i b_i x^i\Big)\Big(\sum_k m_k x^k\Big) = f(x)m(x) + g(x)m(x);\end{aligned}$$

$$\begin{aligned}f(x)\big[m(x) + n(x)\big] &= \Big(\sum_i a_i x^i\Big)\Big(\sum_k (m_k + n_k) x^k\Big) = \sum_l \Big(\sum_{i+k=l} (a_i m_k + a_i n_k)\Big) x^l \\ &= \Big(\sum_i a_i x^i\Big)\Big(\sum_k m_k x^k\Big) + \Big(\sum_i a_i x^i\Big)\Big(\sum_k n_k x^k\Big) = f(x)m(x) + f(x)n(x).\end{aligned}$$

Show $M[x] \cong A[x] \otimes_A M$.

Define $\phi\colon M[x] \to A[x] \otimes_A M$ by $m(x) = \sum m_j x^j \mapsto \sum (x^j \otimes m_j)$. It is obviously additive, and is $A[x]$-linear, for if $f(x) = \sum a_i x^i \in A[x]$, then

$$\begin{aligned}\phi\big(f(x)m(x)\big) &= \sum_k \sum_{i+j=k} \phi(a_i m_j x^k) = \sum_k \sum_{i+j=k} (x^k \otimes a_i m_j) = \sum_i \sum_j (x^i x^j \otimes a_i m_j) \\ &= \sum_j \bigg(\Big(\sum_i a_i x^i\Big) x^j \otimes m_j\bigg) = \Big(\sum_i a_i x^i\Big)\Big(\sum_j x^j \otimes m_j\Big) = f(x)\phi\big(m(x)\big).\end{aligned}$$

Define $\bar{\psi}\colon A[x] \times M \to M[x]$ by $\bar{\psi}\big(\sum a_i x^i,\, m\big) = \sum (a_i m) x^i$. It is clearly bi-additive and A-bilinear, and so induces a linear map $\psi\colon A[x] \otimes_A M \to M[x]$ sending $\big(\sum a_i x^i\big) \otimes m \mapsto \sum (a_i m) x^i$. Now ϕ and ψ are inverse, for

$$\psi\big(\phi(m_i x^i)\big) = \psi(x^i \otimes m_i) = m_i x^i$$

and

$$\phi\big(\psi(a_i x^i \otimes m)\big) = \phi\big((a_i m) x^i\big) = x^i \otimes a_i m = a_i x^i \otimes m.$$

Let $\mathfrak{p}$ *be a prime ideal in* A*. Show that* $\mathfrak{p}[x]$ *is a prime ideal in* $A[x]$*. If* $\mathfrak{m}$ *is a maximal ideal in* A*, is* $\mathfrak{m}[x]$ *a maximal ideal in* $A[x]$*?*

$\mathfrak{p}[x]$ is the kernel of the "reduction of coefficients" homomorphism $A[x] \twoheadrightarrow (A/\mathfrak{p})[x]$, and $(A/\mathfrak{p})[x]$ is an integral domain (see the proof of [1.2.ii]).

On the other hand, the ideal $(2) \lhd \mathbb{Z}$ is maximal, but the ideal $2\mathbb{Z}[x] \lhd \mathbb{Z}[x]$ is not maximal, as the quotient $(\mathbb{Z}/2\mathbb{Z})[x]$ is not a field. $2\mathbb{Z}[x]$ is properly contained in the maximal ideal $(2, x)$.

i) If M *and* N *are flat* A*-modules, then so is* $M \otimes_A N$*.*

Let $j\colon P' \rightarrowtail P$ be an injective A-linear map. Since N is flat, the map $\mathrm{id}_N \otimes j\colon N \otimes P' \to N \otimes P$ is injective. Since M is flat, the map $\mathrm{id}_M \otimes (\mathrm{id}_N \otimes j)\colon M \otimes (N \otimes P') \to M \otimes (N \otimes P)$ is injective. But by the associativity (2.14.ii) of $\otimes_A$, this is up to a canonical isomorphism the map $\mathrm{id}_{M \otimes N} \otimes j$ induced from j by tensoring with $M \otimes N$, so $M \otimes N$ is flat.

ii) If B *is a flat* A*-algebra and* N *is a flat* B*-module, then* N *is flat as an* A*-module.*

Let $j\colon M' \rightarrowtail M$ be an injective A-module homomorphism, and let $f\colon A \to B$ be the map making B an A-algebra. Since B is a flat A-module, the map $\mathrm{id}_B \otimes_A j\colon B \otimes_A M' \to B \otimes_A M$ is injective, and since N is flat as a B-module, the map

$$\mathrm{id}_N \otimes_B (\mathrm{id}_B \otimes_A j)\colon N \otimes_B (B \otimes_A M') \to N \otimes_B (B \otimes_A M)$$

is injective as well. Composing the associativity isomorphisms of (2.15), we see

$$(\mathrm{id}_N \otimes_B \mathrm{id}_B) \otimes_A j\colon (N \otimes_B B) \otimes_A M' \to (N \otimes_B B) \otimes_A M$$

is injective, so by the isomorphism $N \cong N \otimes_B B$ of (2.14.iv), so is $\mathrm{id}_N \otimes_A j\colon N \otimes_A M' \to N \otimes_A M$.

Let $0 \to M' \to M \to M'' \to 0$ *be an exact sequence of* A*-modules. If* M' *and* M'' *are finitely generated, then so is* M*.*

Without loss of generality view $M' \to M$ as an inclusion and $M \to M''$ as a quotient mapping. Let the finite sets $\{x_i\}_i$ and $\{\bar{y}_j\}_j$ respectively generate M' and M''. Lift the $\bar{y}_j$ to elements y_j of M. The submodule of M generated by the finite set $\{x_i\}_i \cup \{y_j\}_j$ contains M' and has image M'', so by the bijection (p. 18) between submodules of M'' and submodules of M containing M', it is M.

Let A *be a ring,* $\mathfrak{a}$ *an ideal contained in the Jacobson radical of* A*; let* M *be an* A*-module and* N *a finitely generated* A*-module, and let* $u\colon M \to N$ *be a homomorphism. If the induced homomorphism* $M/\mathfrak{a}M \to N/\mathfrak{a}N$ *is surjective, then* u *is surjective.*

As the induced homomorphism sends $M \twoheadrightarrow M/\mathfrak{a}M \twoheadrightarrow N/\mathfrak{a}N$, we must have $u(M) + \mathfrak{a}N = N$. Since N is finitely generated and $\mathfrak{a} \subseteq \mathfrak{R}$, by the corollary (2.7) of Nakayama's Lemma, $u(M) = N$.

Let A be a ring $\neq 0$. Show that $A^m \cong A^n \implies m = n$.

Let $\phi\colon A^m \to A^n$ be an isomorphism and $\mathfrak{m} \lhd A$ a maximal ideal. If $k = A/\mathfrak{m}$ is the quotient field, then $\mathrm{id}_k \otimes \phi\colon k \otimes_A A^m \to k \otimes_A A^n$ is an isomorphism by (2.18), taking $N = k$, $M' = 0$, $M = A^m$, and $M'' = A^n$. But by (2.8), we have $k \otimes_A A^n \cong k^n$ an n-dimensional k-vector space. Since dimension of vector spaces is an isomorphism invariant, $m = n$.

If $\phi\colon A^m \to A^n$ is surjective, then $m \geq n$.

As above, tensoring with $k = A/\mathfrak{m}$ shows that the k-linear map $\mathrm{id}_k \otimes \phi\colon k^m \to k^n$ is surjective. But if $m < n$, the m elements $\phi(e_i)$ cannot span k^n, so $m \geq n$.

If $\phi\colon A^m \to A^n$ is injective, is it always the case that $m \leq n$?

It is indeed the case. Some poached solutions follow.[10]

i)[11] This solution is simplest and uses results already proven in the book by Ch. 2. Let $\phi\colon A^m \to A^n$ be an A-linear map with $m > n$; we prove it is not injective. Compose with the inclusion $i\colon A^n = A^n \times \{0\}^{m-n} \hookrightarrow A^n \times A^{m-n} = A^m$ on the first n coordinates to get an A-module endomorphism $\psi = i \circ \phi\colon A^m \to A^m$. If $\pi\colon A^m \to A$ is the projection on the last coordinate, we have $\pi \circ \psi = 0$. Now by (2.4), ψ satisfies an equation

$$\psi^n + a_1 \psi^{n-1} + \cdots + a_n \,\mathrm{id}_{A^m} = 0$$

for some $a_j \in A$. Assume n is minimal such this happens. Taking π of both sides, we see $a_n = 0$. Now as ψ is A-linear, we have $\psi \circ (\psi^{n-1} + a_1\psi^{n-2} + \cdots + a_{n-1}\,\mathrm{id}_{A^m}) = 0$. Since n was minimal, the map $\psi^{n-1} + a_1\psi^{n-2} + \cdots + a_{n-1}\,\mathrm{id}_{A^m} \neq 0$, so its image M is not 0, yet $\psi(M) = 0$, so ψ (and hence ϕ) is not injective.

ii)[12] The other proof feasibly accessible using knowledge available so far uses some linear algebra, generalized to the context of free modules over a commutative ring A. Given a square matrix N of rank n with entries $a_{ij} \in A$, the *determinant* $\det A$ is the element of A given by $\sum_\sigma (\operatorname{sgn}\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$ where σ ranges over all $n!$ permutations of $\{1, \ldots, n\}$ and $\operatorname{sgn}\sigma$ is the parity of the permutation, which is ± 1 depending as σ is even or odd. From this formula it follows that if two rows of N are identical, the determinant is 0. Note that there are n^2 square matrices N_{ij} of rank $n-1$ given by deleting the entries in the i^{th} row and j^{th} column. The (i,j)-*cofactor* of N is given by $c_{ij} = (-1)^{i+j} \det N_{ij} \in A$. The determinant of N can be calculated recursively by the *cofactor expansion* $\det N = \sum_{i=1}^n a_{ij} c_{ij}$ for fixed j or $\sum_{j=1}^n a_{ij} c_{ij}$ for fixed i. The *adjugate* $\mathrm{Adj}(N) = (b_{ij})$ of N is the $n \times n$ matrix with entries $b_{ij} = c_{ji}$ the cofactors of N. The (i,j) entry of $N \cdot \mathrm{Adj}(N)$ is $\sum_{k=1}^n a_{ik} c_{kj} = \sum_k a_{ik} b_{jk}$. For $i = j$, the cofactor expansion of the determinant shows this number is $\det N$. For $i \neq j$ this expression for the entry is, up to a sign, the cofactor expansion, along the i^{th} row, of the determinant of the matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{jn} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix},$$

whose $i^{\text{th}}$and j^{th} rows are equal; and so the entry is 0. Thus $N \cdot \mathrm{Adj}(N) = \det(N) \cdot I_n$ is the scalar product of $\det N$ and the $n \times n$ identity matrix.

Note that it suffices to prove an A-module homomorphism $\phi\colon A^m \to A^n$ cannot be injective for $m = n+1$, since if $n \leq m-1$ we could compose with the inclusion $A^n \hookrightarrow A^{m-1}$ to transform an injection $A^m \rightarrowtail A^n$ to an injection $A^m \rightarrowtail A^{m-1}$. If e_i $(i = 1, \ldots, n+1)$ is the standard basis for A^{n+1} and f_j $(j = 1, \ldots, n)$ is the standard basis for A^n,

[10] Several solutions are up at http://mathoverflow.net/questions/136/atiyah-macdonald-exercise-2-11/2622. I was unable to find a solution myself, at least before giving up and searching online.

[11] Balazs Strenner

[12] Robin Chapman

then $\phi(e_i) = \sum_{j=1}^{n} a_{ji} f_j$ for some $a_{ji} \in A$, and ϕ is represented by the matrix

$$M = \begin{pmatrix} a_{11} & \cdots & a_{1,n+1} \\ \vdots & \ddots & \vdots \\ a_{n,1} & \cdots & a_{n,n+1} \end{pmatrix},$$

so ϕ is injective just if there is no nonzero vector $v = (b_1, \ldots, b_{n+1})^\top \in A^{n+1}$ such that $Mv = 0$. Now let M_i be the $n \times n$ matrix obtained from M by deleting the i^{th} column and let v have components $b_i = (-1)^i \det M_i$. Then the j^{th} component of Mv is $\sum_{i=1}^{n+1} (-1)^i a_{ji} \det M_i$. But this is $(-1)^j$ times the cofactor expansion along the j^{th} row of the determinant of the $(n+1) \times (n+1)$ matrix

$$\begin{pmatrix} a_{11} & \cdots & a_{1,n+1} \\ \vdots & \ddots & \vdots \\ a_{j1} & \cdots & a_{j,n+1} \\ a_{j1} & \cdots & a_{j,n+1} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{n,n+1} \end{pmatrix},$$

which is zero because the j^{th} row is repeated, so $Mv = 0$.

Now if some $\det M_i$ is nonzero, we have achieved our goal of finding a nonzero $v \in \ker \phi$. Otherwise, $\det M_{n+1} = 0$. If M_{n+1} has a nonzero vector $v' = (b_1, \ldots, b_n)^\top$ in its kernel, then $v = (b_1, \ldots, b_n, 0)^\top$ is a nonzero vector in the kernel of M. It then falls to us to show that if a square matrix N of rank n has determinant 0, it has nontrivial kernel. Let $r < n$ be the rank of the largest square submatrix (obtained from N by deleting rows and columns) with nonzero determinant; by shuffling rows, we may assume that $r \times r$ occurs in the upper left of N. Let R be the $(r+1) \times (r+1)$ matrix on the upper left of N containing it; since $\det R \neq 0$ by the maximality of r, taking the cofactor expansion along the first column of R shows that the first column v'' of $\operatorname{Adj}(R)$ has some nonzero entry. Now $Rv'' = 0$, since $R \cdot \operatorname{Adj}(R) = \det(R) \cdot I_{r+1} = 0$. If we let v' be v'' with $n - r$ zeros added at the end, then as the determinant of N is zero, the rest of the rows of N are linear combinations of rows of R, so $Nv' = 0$.

iii)[13] Abstracting from the last proof at a rather high level is the following. It requires the notion of exterior product: $\bigwedge_A^n M = \big(\bigotimes_A^n M\big)/N$, where $\bigotimes_A^n M$ is the n-fold tensor product $M \otimes_A \cdots \otimes_A M$ and N is the submodule generated by all elements $(\cdots \otimes x \otimes y \otimes \cdots) + (\cdots \otimes y \otimes x \otimes \cdots)$. The image of $x \otimes \cdots \otimes y$ is denoted by $x \wedge \cdots \wedge y$, and we have (by fiat) the equalities $x_1 \wedge \cdots \wedge x_n = (\operatorname{sgn} \sigma) x_{\sigma(1)} \wedge \cdots \wedge x_{\sigma(n)}$, where σ is a permutation of $\{1, \ldots, n\}$ and $\operatorname{sgn} \sigma$ its parity. We then have a theorem:[14]

$$\text{a subset } \{u_1, \ldots, u_m\} \text{ of } M = A^n \text{ is linearly independent} \iff \forall a \in A\ [a \cdot (u_1 \wedge \cdots \wedge u_m) = 0 \implies a = 0],$$

where $u_1 \wedge \cdots \wedge u_m \in \bigwedge_A^n M$. This proves the result because for $m > n$ we have $\bigwedge_A^m (A^n) = 0$.

The remaining proofs use material developed later in the book.

iv)[15] Let $\phi \colon A^m \rightarrowtail A^n$ be an injective A-module homomorphism represented by the matrix M. Let $B = \mathbb{Z}[\ldots, a_{ij}, \ldots]$ be the subring of A generated by all the entries of the matrix M; since $\mathbb{Z}$ is Noetherian, by (7.5) (the Hilbert Basis Theorem) and (7.1) (quotient preserves a.c.c.), B is a Noetherian ring; and ϕ restricts to an injective linear map $\psi \colon B^m \rightarrowtail B^n$. Note that B^n, by (6.4), is Noetherian. If we assume $m > n$ we can derive a contradiction. Write $B^m = M \oplus N$ with $M \cong B^n$ and $N \cong B^{m-n}$. Then we have isomorphic images M_1 and N_1 of M, N in M, and isomorphic images M_2, N_2 in M_1, and isomorphic images M_3, N_3 in M_2, etc. This yields an infinite ascending chain

$$N_1 \subsetneq N_1 \oplus N_2 \subsetneq N_1 \oplus N_2 \oplus N_3 \subsetneq \cdots,$$

contradicting the ascending chain condition.

v)[16] Continue with the Noetherian ring B of iv). By [1.8], B has a minimal prime ideal $\mathfrak{p}$. By p. 38 the localization $C = B_{\mathfrak{p}}$ has only one prime ideal $\mathfrak{q} = \mathfrak{p}C$. By (3.3) (localization is exact), the induced map $\psi_{\mathfrak{p}} \colon C^m \to C^n$ is injective

[13] Pete L. Clark, via Tsit Yuen Lam's *Lectures on Rings and Modules*, pp. 15–16, via Nicolas Bourbaki's *Algebra*

[14] Nicolas Bourbaki, *Algebra*, Chapter III, §7.9, Prop. 12, page 519

[15] from Tsit Yuen Lam's *Lectures on Rings and Modules*, p. 14, and referred by Pete L. Clark

[16] Georges Elencwajg

as well. By (7.3) (localization preserves a.c.c.), C is Noetherian, and since it has just one prime ideal, it has (Krull) dimension (p. 90) zero. By (8.5), C is Artinian as well, so by (6.8) it has a finite composition series as a C-module. By (6.7), the length of this composition series is independent of the series chosen, so C has a well defined finite length $l(C) \geq 1$. Now let us consider the lengths of C^m and C^n. (6.9) says the length of a module is an additive function, so using the natural exact sequences $0 \to C \to C^{n+1} \to C^n \to 0$, we have $l(C^n) = n \cdot l(C)$ by induction. We also have, by assumption, an exact sequence

$$0 \to C^m \xrightarrow{\psi_{\mathfrak{p}}} C^n \to \operatorname{coker}(\psi_{\mathfrak{p}}) \to 0,$$

so $n \cdot l(C) = m \cdot l(C) + l\big(\operatorname{coker}(\psi_{\mathfrak{p}})\big)$, and thus $m \leq n$.

vi)[17] Finally, there is another matrix-theoretic proof, involving localization. $\phi \colon A^{n+1} \to A^n$ is injective just if each of its localizations is injective, by (3.9). By [1.8], A has a minimal prime ideal $\mathfrak{p}$, and by [1.10], $\mathfrak{q} = \mathfrak{p}A_{\mathfrak{p}}$ is the nilradical in the localization $B = A_{\mathfrak{p}}$, and all other elements of B are units. We claim any finite set of elements in $\mathfrak{q}$ is jointly annihilated by some nonzero element of $\mathfrak{q}$. For the base case, if $0 \neq x \in \mathfrak{q}$ and $r > 0$ is minimal such that $x^r = 0$, then $x^{r-1} \in \mathfrak{q}$ is a nonzero element annihilating x. Let $0 \neq y \in \operatorname{Ann}(S)$ for a finite set $S \subseteq \mathfrak{q}$, and let $z \in \mathfrak{q} \backslash \{0\}$. There is $r > 0$ such that $z^r = 0$, and so there is a minimal $s \in [1, r]$ such that $yz^s = 0$. Then $0 \neq yz^{s-1} \in \operatorname{Ann}\big(S \cup \{z\}\big)$. This lemma essentially allows us to use Gaussian elimination.

Let $M = [a_{ji}]$ be the matrix of the B-module homomorphism $\psi = \phi_{\mathfrak{p}} \colon B^{n+1} \to B^n$. The columns represent the images $\psi(e_i)$, which we are linearly independent just if ψ is injective. Now if there is some linear dependency among the columns, then adding a multiple of one column to another preserves the existence of the dependency. Since the operation of adding a multiple of one column to another is invertible (subtract a multiple of the column), this column operation also reflects dependence, so the columns of the altered matrix are independent just if the columns of the original are. Clearly the same holds for the operations of multiplying all the entries of a column by a unit, swapping rows, and swapping columns.

If any column contains no unit, then by the claim above, there is a nonzero a annihilating that column, and the vector $(0 \cdots a \cdots 0)^\top$ is killed by M, contradicting injectivity of ψ. Thus if ψ is injective all columns contain some unit. If the first column contains a unit, we may shuffle rows so that a_{11} is a unit, and multiplying the first column by a_{11}^{-1} we may assume $a_{11} = 1$. Subtracting multiples of this first column from the others we may clear the rest of the first row. If the second column contains a unit, by swapping rows we may assume it is a_{22}. Multiplying by a unit, we can assume $a_{22} = 1$, and subtracting multiples of the second column from the other columns, we may clear the rest of the second row.

Carrying on in this fashion, we either come upon a column containing no unit or transform the matrix to the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

contradicting injectivity.

Note there exist abelian groups G isomorphic to G^n for $n = 1, 2, \ldots, \aleph_0$. Let $G = \prod_{j \in \mathbb{N}} H_j$ be the direct product of infinitely many copies H_j of some abelian group H. Since $\mathbb{N}$ is infinite, there are for each $n \in \mathbb{N}$ bijections $\phi_n \colon \{1, \ldots, n\} \times \mathbb{N} \leftrightarrow \mathbb{N}$, and there is a bijection $\phi_\omega \colon \mathbb{N} \times \mathbb{N} \leftrightarrow \mathbb{N}$. These yield, for $n \in \mathbb{N} \cup \{\aleph_0\}$, group isomorphisms $\psi_n \colon G^n \xrightarrow{\sim} G$ by letting $\psi(x)_{\phi_n(i,j)} = (x_i)_j$, where $x_i \in G = \prod_{\mathbb{N}} H$, so $(x_i)_j \in H$. This shows that if we weaken the definition of a ring to that of a "rng" ("ring without identity": $\langle A, \cdot \rangle$ is only required to be a semigroup, not a monoid), the proposition doesn't hold. For it is possible to have a nonzero rng whose product is identically zero: any additive abelian group G gives rise to a rng with trivial multiplication. It is then legitimate to define a G-module structure on another abelian group M by $g \cdot m = 0$.

Let M be a finitely generated A-module and $\phi \colon M \to A^n$ a surjective homomorphism. Show that $\ker(\phi)$ *is finitely generated.*

Lemma.* *Let A be a ring and M and N be A-modules. If there exist homomorphisms $s \colon N \to M$ and $r \colon M \to N$ such that $r \circ s = \mathrm{id}_N$, then $M \cong N \oplus (\operatorname{coker} s) \cong N \oplus (\ker r)$.*

Define the map $\varkappa \colon M \to N \oplus (\operatorname{coker} s)$ by $x \mapsto \big\langle r(x), \bar{x} \big\rangle$. For injectivity, suppose $x \in \ker \varkappa$. Then $\bar{x} = 0$, so there is $y \in N$ such that $x = s(y)$, and $0 = r(x) = rs(y) = y$, so $x = 0$. For surjectivity, let $y \in N$ and $\bar{x} \in \operatorname{coker} s$ be

[17] Karl Dahlke, http://mathreference.com/mod-pit,basec.html#embed

arbitrary, and let $x \in M$ be some lift of $\bar{x}$. If $z = x + s\big(y - r(x)\big)$, then $\bar{z} = \bar{x}$, while $r(z) = r(x) + rs(y) - rsr(x) = r(x) + y - r(x) = y$.

An isomorphism $M \to N \oplus \ker r$ is given by $\lambda = \langle r, \mathrm{id}_M - sr\rangle$. Indeed, $r(\mathrm{id}_M - sr) = r - rsr = 0$; and $x \in \ker\lambda$ implies $r(x) = 0$ and $x = x - sr(x) = 0$; and for any $y \in N$ and $z \in \ker r$, if we let $w = s(y) + z$, then $\lambda(w) = \big\langle rs(y) + r(z), s(y) + z - srs(y) - sr(z)\big\rangle = \langle y, s(y) + z - s(y)\rangle = \langle y, z\rangle$.

Now we will show $\ker\phi$ is a quotient (actually a summand) of M; hence the images of a finite set of generators for M will generate $\ker\phi$. Let $e_1, \ldots, e_n$ be a basis for A^n and pick any elements $\chi(e_i) \in \phi^{-1}(e_i)$; this extends to a homomorphism $\chi\colon A^n \to M$ such that $\phi\chi = \mathrm{id}_{A^n}$. Define $\psi = \mathrm{id}_M - \chi\phi$: it takes $M \to \ker\phi$ since $\phi\chi\phi = \phi$. For $x \in \ker\phi$ we have $\psi(x) = x$, so ψ is surjective. In fact, writing $\iota\colon \ker\phi \hookrightarrow M$ for the inclusion, $\phi \circ \iota = \mathrm{id}_{\ker\phi}$, so $\ker\phi$ is a summand, with $\operatorname{coker}\iota = M/\ker\phi \cong \operatorname{im}\phi = A^n$ as the other summand.

Let $f\colon A \to B$ be a ring homomorphism, and let N be a B-module. Regarding N as an A-module by restriction of scalars, form the B-module $N_B = B \otimes_A N$. Show that the homomorphism $g\colon N \to N_B$ which maps y to $1 \otimes y$ is injective and that $g(N)$ is a direct summand of N_B.

The quotient map $N_B = B \otimes_A N \twoheadrightarrow B \otimes_B N$ is also a B-module homomorphism, since $b(b' \otimes y) = bb' \otimes y \mapsto bb' \otimes y = b(b' \otimes y)$, and composing with the isomorphism (2.14.iv*) gives a B-module homomorphism $h\colon N_B \to N$ taking $b \otimes y \mapsto by$. Now $hg = \mathrm{id}_N$, so by the lemma in (2.12*), g injects N as a summand of N_B.

Direct limits

A partially ordered set I is said to be a directed *set if for each pair i, j in I there exists $k \in I$ such that $i \leq k$ and $j \leq k$.*

Let A be a ring, let I be a directed set and let $(M_i)_{i\in I}$ be a family of A-modules indexed by I. For each pair i, j in I such that $i \leq j$, let $\mu_{ij}\colon M_i \to M_j$ be an A-homomorphism, and suppose that the following axioms are satisfied:

(1) μ_{ii} is the identity mapping of M_i, for all $i \in I$;

(2) $\mu_{ik} = \mu_{jk} \circ \mu_{ij}$ whenever $i \leq j \leq k$.

Then the modules M_i and homomorphisms μ_{ij} are said to form a direct system $\mathbf{M} = (M_i, \mu_{ij})$ *over the directed set I.*

We shall construct an A-module M called the direct limit *of the direct system* $\mathbf{M}$. *Let C be the direct sum of the M_i, and identify each module M_i with its canonical image in C. Let D be the submodule of C generated by all elements of the form $x_i - \mu_{ij}(x_i)$ where $i \leq j$ and $x_i \in M_i$. Let $M = C/D$, let $\mu\colon C \to M$ be the projection, and let μ_i be the restriction of μ to M_i.*

The module M, or more correctly the pair consisting of M and the family of homomorphisms $\mu_i\colon M_i \to M$, is called the direct limit *of the direct system* $\mathbf{M}$, *and is written $\varinjlim M_i$. From the construction it is clear that $\mu_i = \mu_j \circ \mu_{ij}$ whenever $i \leq j$.*

In case it wasn't clear, let $i \leq j$ and $x_i \in M_i$: then $x_i - \mu_{ij}(x_i) \in D = \ker(\mu)$, so $\mu_i(x_i) = \mu(x_i) = \mu\big(\mu_{ij}(x_i)\big) = \mu_j(\mu_{ij}(x_i))$.

In the situation of Exercise 14, show that every element of M can be written in the form $\mu_i(x_i)$ for some $i \in I$ and some $x_i \in M_i$.

[FIX]

If $(I, \leq)$ is directed and $S \subseteq I$ is finite, then by induction there is a $j \in I$ such that for each $i \in S$ we have $i \leq j$. Surely this is the case if $j = i \in \{i\} = S$, and if it is the case for a given S and we add a new element i_{n+1} to S, then there is an element $k \geq i_{n+1}, j$, and so $k \geq$ every element of $S \cup \{i_{n+1}\}$.

Let $x \in M$; then it is the image under the quotient map $C \to C/D = M$ of some sum $\sum_{i\in S} x_i \in C = \bigoplus_{i\in I} M_i$, where $S \subseteq I$ is finite by definition. Pick a $j \in I$ such that for all $i \in S$ we have $j \geq i$. The elements $\mu_{ij}(x_i) - x_i \in D$, so $\tilde{x}_j = \sum_{i\in S} \mu_{ij}(x_i) \equiv \sum_{i\in S} x_i \pmod D$ and $\mu_j(\tilde{x}_j) = \mu(\tilde{x}_j) = x$.

Show also that if $\mu_i(x_i) = 0$ then there exists $j \geq i$ such that $\mu_{ij}(x_i) = 0$ in M_j.

We first assemble some auxiliary information about the module D. First, given any generator $(\mathrm{id} - \mu_{ij})(x_i)$ of D, multiplying by $a \in A$ we get $(\mathrm{id} - \mu_{ij})(ax_i)$, since the μ_{ij} are A-module homomorphisms. Similarly, given generators $(\mathrm{id} - \mu_{ij})(x_i)$ and $(\mathrm{id} - \mu_{ij})(y_i)$, their sum is a generator $(\mathrm{id} - \mu_{ij})(x_i + y_i)$. Thus, in considering expressions $\sum_{k=1}^{n} a_k\big(x_{i_k} - \mu_{i_k j_k}(x_{i_k})\big)$ it suffices to assume each $a_k = 1$ and each pair (i_k, j_k) only occurs once.

Now suppose that $x_i \in M_i$ is such that $\mu_i(x_i) = \mu(x_i) = 0$. Then $x_i \in M_i \cap D$, so x_i can be written as a finite sum

$$x_i = \sum_{(j,k)\in T} \Big[y_j - \mu_{jk}(y_k)\Big] = \sum_{j\in S} z_j \tag{2.5}$$

for some finite set $S \subseteq I$, some set $T \subseteq S^2$ of pairs (j, k) with $j \leq k$, and some elements $y_j, z_j \in M_j$. Here the middle sum expresses $x_i \in D$ in terms of generators for D, and the right sum breaks the middle sum into components in M_j. Since Eq. 2.5 takes place in the direct sum, we must have cancellation in all components but the i^{th}, so $z_i = x_i$, and for $j \neq i$ we have $z_j = 0$. Let $\ell \in I$ be an element such that $\ell \geq k$ for each $k \in S$. Then using the equations $\mu_{j\ell} = \mu_{k\ell} \circ \mu_{jk}$,

$$\mu_{i\ell}(x_i) = \sum_{j \in S} \mu_{j\ell}(z_j) = \sum_{(j,k) \in T} \Big[\mu_{j\ell}(y_j) - \mu_{k\ell}\big(\mu_{jk}(y_j)\big) \Big] = 0.$$

Show that the direct limit is characterized (up to isomorphism) by the following property. Let N be an A-module and for each $i \in I$ let $\alpha_i \colon M_i \to N$ be an A-module homomorphism such that $\alpha_i = \alpha_j \circ \mu_{ij}$ whenever $i \leq j$. Then there exists a unique homomorphism $\alpha \colon M \to N$ such that $\alpha_i = \alpha \circ \mu_i$ for all $i \in I$.

I think we should add the requirement on (M, μ_i, μ_{ij}) that we have $\mu_i = \mu_j \circ \mu_{ij}$ for all $i \leq j \in I$.

First we show that $M = \varinjlim M_i$ satisfies this property. We showed $\mu_i = \mu_j \circ \mu_{ij}$ in [2.14]. Given arbitrary A-module homomorphisms $\alpha_i \colon M_i \to N$, we have by the universal property of direct sums a unique induced homomorphism $\widetilde{\alpha} \colon C = \bigoplus_{i \in I} M_i \to N$. For any $x_i \in M_i$ and $j \geq i$, consider the generator $x_i - \mu_{ij}(x_i)$ of D. By the definition of $\widetilde{\alpha}$ and the compatibility condition on the α_i we have

$$\widetilde{\alpha}\big(x_i - \mu_{ij}(x_i)\big) = \alpha_i(x_i) - \alpha_j\big(\mu_{ij}(x_i)\big) = \alpha_i(x_i) - \alpha_i(x_i) = 0,$$

so $D \subseteq \ker(\widetilde{\alpha})$ and $\widetilde{\alpha}$ induces an A-module homomorphism $\alpha \colon M = C/D \to N$. Moreover, by definition $\alpha\big(\mu_i(x_i)\big) = \widetilde{\alpha}(x_i) = \alpha_i(x_i)$.

$$\begin{tikzcd}
M_i \arrow[dd, "\mu_{ij}"'] \arrow[dr, "\mu_i=\beta_i"'] \arrow[drr, bend left, "\mu'_i=\alpha_i"] & & \\
& M \arrow[loop above, "\gamma"] \arrow[r, shift left, "\alpha"] & M' \arrow[l, shift left, "\beta"] \\
M_j \arrow[ur, "\mu_j=\beta_j"] \arrow[urr, bend right, "\mu'_j=\alpha_j"'] & &
\end{tikzcd}$$

Now suppose that $(M, \mu_i \colon M_i \to M)$ and $(M', \mu'_i \colon M_i \to M')$ both satisfy the universal mapping property. Since (M', μ'_i) is a direct limit of (M_i, μ_{ij}) we have by definition that $\mu'_i = \mu'_j \circ \mu_{ij}$. But then setting $\alpha_i = \mu'_i$ in the universal property of (M, μ_i) as a direct limit, we get a unique homomorphism $\alpha \colon M \to M'$ such that $\mu'_i = \alpha_i = \alpha \circ \mu_i$. Symmetrically, we get a unique homomorphism $\beta \colon M' \to M$ such that $\mu_i = \beta \circ \mu'_i$. Now $\mu_i = \beta \circ \mu'_i = \beta \circ \alpha \circ \mu_i \colon M_i \to M$ for each i. Since $\mu_i = \mu_j \circ \mu_{ij}$, there exists a unique homomorphism $\gamma \colon M \to M$ such that $\mu_i = \gamma \circ \mu_i$; as both id_M and $\beta \circ \alpha$ meet the requirements for γ, by uniqueness, $\beta \circ \alpha = \mathrm{id}_M$. Symmetrically, $\alpha \circ \beta = \mathrm{id}_{M'}$, so $\alpha \colon M \longleftrightarrow M' \colon \beta$ are inverse isomorphisms.

Let $(M_i)_{i \in I}$ be a family of submodules of an A-module, such that for each pair of indices i, j in I there exists $k \in I$ such that $M_i + M_j \subseteq M_k$. Define $i \leq j$ to mean $M_i \subseteq M_j$ and let $\mu_{ij} \colon M_i \to M_j$ be the embedding of M_i in M_j. Show that

$$\varinjlim M_i = \sum M_i = \bigcup M_i.$$

In particular, any A-module is the direct limit of its finitely generated submodules.

For each i we have $M_i \subseteq \sum M_i$, so $\bigcup M_i \subseteq \sum M_i$. On the other hand, if $y = \sum_{i \in I} x_i \in \sum M_i$ is any finite sum, let $S = \{i \in I : x_i \neq 0\}$, and let $j \in I$ be $\geq$ each element of S; then $\sum_{i \in S} M_i \subseteq M_j$, so $y \in M_j \subseteq \bigcup_{i \in I} M_i$. Thus $\sum M_i = \bigcup M_i$.

We show $\varinjlim M_i \cong \bigcup M_i$ by showing $\bigcup M_i$ has the expected universal property ([2.16]). Let $\mu_i \colon M_i \hookrightarrow \bigcup M_i$ be the inclusion, and suppose we have $\alpha_i \colon M_i \to N$ such that $\alpha_i = \alpha_j \circ \mu_{ij}$ for $i \leq j$. This is just the same as saying that if $M_i \subseteq M_j$ we have $\alpha_j|_{M_i} = \alpha_i$, so that the α_i are consistent on all intersections and thus their union defines a unique function $\alpha = \bigcup \alpha_i \colon \bigcup M_i \to N$ restricting to α_i on each M_i; that is $\alpha_i = \alpha \circ \mu_i$. Now α is A-linear because its restriction to each M_i is, so $\bigcup M_i$ satisfies the universal mapping property required of $\varinjlim M_i$.

It follows that an A-module M is the direct limit of its finitely generated submodules, for any $x \in M$ is in the finitely generated submodule Ax (so M is the union of its finitely generated submodules) and if $N_1, N_2 \subseteq M$ are finitely generated submodules, then both are contained in the finitely generated module $N_1 + N_2 \subseteq M$ (so the finitely generated submodules and inclusions form a direct system).

Let $\mathbf{M} = (M_i, \mu_{ij})$, $\mathbf{N} = (N_i, \nu_{ij})$ be direct systems of A-modules over the same directed set. Let M, N be the direct limits and $\mu_i : M_i \to M$, $\nu_i : N_i \to N$ the associated homomorphisms.

$$\begin{tikzcd}
 & & M \arrow[ddd, dotted, "\phi"] \\
M_i \arrow[urr, "\mu_i"] \arrow[r, "\mu_{ij}"'] \arrow[d, "\phi_i"] \arrow[ddrr, bend right=60, "\alpha_i"'] & M_j \arrow[ur, "\mu_j"'] \arrow[d, "\phi_j"'] \arrow[ddr, "\alpha_j"] & \\
N_i \arrow[r, "\nu_{ij}"] \arrow[drr, "\nu_i"'] & N_j \arrow[dr, "\nu_j"] & \\
 & & N
\end{tikzcd}$$

A homomorphism *$\Phi : \mathbf{M} \to \mathbf{N}$ is by definition a family of A-module homomorphisms $\phi_i : M_i \to N_i$ such that $\phi_j \circ \mu_{ij} = \nu_{ij} \circ \phi_i$ whenever $i \le j$. Show that Φ defines a unique homomorphism $\phi = \varinjlim \phi_i : M \to N$ such that $\phi \circ \mu_i = \nu_i \circ \phi_i$ for all $i \in I$.*

Define $\alpha_i : M_i \to N$ by $\alpha_i = \nu_i \circ \phi_i$. Then if $i \le j$ we have

$$\alpha_j \circ \mu_{ij} = \nu_j \circ \phi_j \circ \mu_{ij} = \nu_j \circ \nu_{ij} \circ \phi_i = \nu_i \circ \phi_i = \alpha_i,$$

so by the universal property of [2.16] there is a unique map $\phi : M \to N$ such that $\phi \circ \mu_i = \alpha_i = \nu_i \circ \phi_i$ for all $i \in I$.

A sequence of direct systems and homomorphisms

$$\mathbf{M} \to \mathbf{N} \to \mathbf{P}$$

is exact *if the corresponding sequence of modules and module homomorphisms is exact for each $i \in I$. Show that the sequence $M \to N \to P$ of direct limits is then exact.*

Let the components of $\Phi : \mathbf{M} \to \mathbf{N}$ and $\Psi : \mathbf{N} \to \mathbf{P}$ be $\phi_i : M_i \to N_i$ and $\psi_i : N_i \to P_i$, inducing $\phi : M \to N$ and $\psi : N \to P$, and let the maps in the direct systems $\mathbf{M}, \mathbf{N}, \mathbf{P}$ be respectively $\mu_{ij}, \nu_{ij}, \pi_{ij}$. To show $\psi \circ \phi = 0$, recall ([2.15]) that any element $x \in M$ is of the form $\mu_i(x_i)$ for some $x_i \in M_i$ and some $i \in I$. By the assumed exactness, $(\psi_i \circ \phi_i)(x_i) = 0$. Then using the defining properties of x_j and of ϕ and ψ ([2.18]),

$$(\psi \circ \phi)(x) = (\psi \circ \phi \circ \mu_i)(x_i) = (\psi \circ \nu_i \circ \phi_i)(x_i) = (\pi_i \circ \psi_i \circ \phi_i)(x_i) = \pi_i(0) = 0.$$

$$\begin{tikzcd}
x_i \arrow[r, mapsto, "\phi_i"] \arrow[d, mapsto, "\mu_i"'] & {} \arrow[r, mapsto, "\psi_i"] \arrow[d, mapsto, "\nu_i"] & 0 \arrow[d, mapsto, "\pi_i"] \\
x \arrow[r, mapsto, "\phi"] & {} \arrow[r, mapsto, "\psi"] & \phi(\psi(x))
\end{tikzcd}$$

$$\begin{tikzcd}
M_i \arrow[r, "\phi_i"] \arrow[d, "\mu_i"'] & N_i \arrow[r, "\psi_i"] \arrow[d, "\nu_i"] & P_i \arrow[d, "\pi_i"] \\
M \arrow[r, "\phi"] & N \arrow[r, mapsto, "\psi"] & P
\end{tikzcd}$$

$$\begin{tikzcd}
 & y_i \arrow[r, mapsto, "\psi_i"] \arrow[d, mapsto, "\nu_{ij}"] & {} \arrow[d, mapsto, "\pi_{ij}"] \\
x_j \arrow[r, mapsto, "\phi_j"] \arrow[d, mapsto, "\mu_j"] & \nu_{ij}(y_i) \arrow[r, mapsto, "\psi_j"] \arrow[d, mapsto, "\nu_j"] & 0 \arrow[d, mapsto, "\pi_j"] \\
x \arrow[r, mapsto, "\phi"] & y \arrow[r, mapsto, "\psi"] & 0
\end{tikzcd}$$

$$\begin{tikzcd}
 & N_i \arrow[r, "\psi_i"] \arrow[d, "\nu_{ij}"] & P_i \arrow[d, "\pi_{ij}"] \\
M_j \arrow[r, "\phi_j"] \arrow[d, "\mu_j"] & N_j \arrow[r, "\psi_j"] \arrow[d, "\nu_j"] & P_j \arrow[d, "\pi_j"] \\
M \arrow[r, "\phi"] & N \arrow[r, "\psi"] & P
\end{tikzcd}$$

On the other hand, suppose $y \in \ker(\psi)$. By [2.15], there are $i \in I$ and $y_i \in N_i$ such that $y = \nu_i(y_i)$, and by the defining property ([2.18]) of ψ we have $0 = \psi(y) = \psi\big(\nu_i(y_i)\big) = \pi_i\big(\psi_i(y_i)\big)$. By [2.15] there is $j \ge i$ such that $0 = \pi_{ij}\big(\psi_i(y_i)\big) = \psi_j\big(\nu_{ij}(y_i)\big)$, where we use the definition of Ψ being a homomorphism. Since we assumed the sequence of direct systems is exact, it follows that there is $x_j \in M_j$ such that $\phi_j(x_j) = \nu_{ij}(y_i)$. But then if $x = \mu_j(x_j)$ we have

$$\phi(x) = \phi\big(\mu_j(x_j)\big) = \nu_j\big(\phi_j(x_j)\big) = \nu_j\big(\nu_{ij}(y_i)\big) = \nu_i(y_i) = y,$$

using the definitions of x and ϕ, the assumed property of x_j, the result of [2.14] for the direct system $\mathbf{N}$, and the assumed property of y_i. Thus $\ker(\psi) \subseteq \operatorname{im}\phi$ and the sequence $M \to N \to P$ is exact.

Tensor products commute with direct limits

Keeping the same notation as in Exercise 14 let N be any A-module. Then $(M_i \otimes N, \mu_{ij} \otimes 1)$ is a direct system; let $P = \varinjlim (M_i \otimes N)$ be its direct limit. For each $i \in I$ we have a homomorphism $\mu_i \otimes 1 : M_i \otimes N \to M \otimes N$, hence by Exercise 16 homomorphism $\psi : P \to M \otimes N$. Show that ψ is an isomorphism so that

$$\varinjlim (M_i \otimes N) \cong \big(\varinjlim M_i\big) \otimes N.$$

First we show the direct limit of $(M_i \times N, \mu_{ij} \times \mathrm{id}_N)$ is $M \times N$. Indeed, let $\alpha_i : M_i \times N \to Q$ be a collection of A-linear maps such that for all $i \le j$ we have $\alpha_i = \alpha_j \circ (\mu_{ij} \times \mathrm{id}_N)$. For $M \times N$ to satisfy the universal property characterizing $\varinjlim (M_i \times N)$ ([2.16]), we want to define a unique $\alpha : M \times N \to Q$ such that $\alpha_i = \alpha \circ (\mu_i \times \mathrm{id}_N)$. This forces us to attempt the definition $\alpha(\mu_i(x_i), y) := \alpha_i(x_i, y)$. Now α is defined on all of $M \times N$ since by [2.15] each element $x \in M$ is $\mu_i(x_i)$ for some $i \in I$ and $x_i \in M_i$. To show it is well defined, suppose $x = \mu_i(x_i) = \mu_j(x_j)$. Then there is some $k \geq i, j$, and $x = \mu_k(\mu_{ik}(x_i)) = \mu_k(\mu_{jk}(x_j))$ since $\mu_i = \mu_k \circ \mu_{ik}$. Now as $\alpha_i = \alpha_j \circ (\mu_{ij} \times \mathrm{id}_N)$ we have

$$\alpha(\mu_i(x_i), y) = \alpha_i(x_i, y) = \alpha_k(\mu_{ik}(x_i), y) = \alpha_k(\mu_{jk}(x_j), y) = \alpha_j(x_j, y) = \alpha(\mu_j(x_j), y),$$

so α is well defined. The existence of a unique such α shows that $\left(\varinjlim M_i\right) \times N \cong \varinjlim \left(M_i \times N\right)$.

Let $\pi_i : M_i \otimes N \to P$ be the canonical map making P the direct limit, and for each $i \in I$ let $g_i : M_i \times N \to M_i \otimes N$ be the canonical bilinear mapping. These g_i form a homomorphism between the direct systems $(M_i \times N)$ and $(M_i \otimes N)$, so by [2.18] they induce a unique homomorphism

$$g : M \times N \cong \varinjlim \left(M_i \times N\right) \to \varinjlim \left(M_i \otimes N\right) = P$$

such that $g \circ (\mu_i \times \mathrm{id}_N) = \pi_i \circ g_i$. We have $g(x, y) = g_i(x_i, y)$, and each g_i is A-bilinear, so since any element of $M \times N$ has a representative in some $M_i \times N$, g is A-bilinear as well. Thus g induces an A-module homomorphism $\phi : M \otimes N \to P$ such that

$$\phi \circ (\mu_i \otimes \mathrm{id}_N) = \pi_i \tag{2.6}$$

for each i. Note on the other hand that

$$\psi \circ \pi_i = \mu_i \otimes \mathrm{id}_N \tag{2.7}$$

by the definition of ψ.

Now by [2.15], each element $p \in P$ can be written as $\pi_i(p_i)$ for some $p_i \in M_i \otimes N$. Since this module is generated by elements $x_i \otimes y$, for $x_i \in M_i$ and $y \in N$, by linearity of ψ and ϕ we may assume $p_i = x_i \otimes y$. We then have, by [2.16], that

$$\phi(\psi(p)) = \phi(\psi(\pi_i(p_i))) \overset{\text{Eq. 2.7}}{=} (\phi \circ (\mu_i \otimes \mathrm{id}_N))(p_i) \overset{\text{Eq. 2.6}}{=} \pi_i(p_i) = p.$$

Similarly, let $x \otimes y$ be a generator of $M \otimes N$. Then by [2.15] there are $i \in I$ and $x_i \in M_i$ such that $x \otimes y = \mu_i(x_i) \otimes y$, and

$$\psi(\phi(x \otimes y)) = \psi(\phi[(\mu_i \otimes \mathrm{id}_N)(x_i \otimes y)]) \overset{\text{Eq. 2.6}}{=} \psi(\pi_i(x_i \otimes y)) \overset{\text{Eq. 2.7}}{=} (\mu_i \otimes \mathrm{id}_N)(x_i \otimes y) = x \otimes y.$$

Thus ψ and ϕ are inverse isomorphisms.

Let $(A_i)_{i \in I}$ be a family of rings indexed by a directed set I, and for each pair $i \leq j$ in I let $\alpha_{ij} : A_i \to A_j$ be a ring homomorphism, satisfying conditions (1) and (2) of Exercise 14 Regarding each A_i as a $\mathbb{Z}$-module we can then form the direct limit $A = \varinjlim A_i$. Show that A inherits a ring structure from the A_i so that the mappings $A_i \to A$ are ring homomorphisms. The ring A is the direct limit *of the system (A_i, α_{ij}).*

If $A = 0$ prove that $A_i = 0$ for some $i \in I$.

Let $a, b \in A$. By [2.15] there are $i, j \in I$ and $a_i \in A_i$, $b_j \in B_j$ such that $\alpha_i(a_i) = a$ and $\alpha_j(b_j) = b$. Now there is $k \in I$ such that $k \geq i, j$, and $\alpha_k(\alpha_{ik}(a_i)) = \alpha_i(a_i) = a$ and $\alpha_k(\alpha_{jk}(b_j)) = \alpha_j(b_j) = b$. Define $ab = \alpha_k(\alpha_{ik}(a_i) \cdot \alpha_{jk}(b_j))$. We have made three choices in this definition, i, j, and k. Fixing i, j, suppose we picked k' instead of k. There is some $l \in I$ with $l \geq k, k'$, and we have $\alpha_k(\alpha_{ik}(a_i) \cdot \alpha_{jk}(b_j)) = (\alpha_l \circ \alpha_{kl})(\alpha_{ik}(a_i) \cdot \alpha_{jk}(b_j)) = \alpha_l(\alpha_{il}(a_i) \cdot \alpha_{jl}(b_j))$, and symmetrically for k', so the definition is independent of the choice of k. Now suppose instead we choose a representative $b = \alpha_{j'}(b_{j'})$ with $b_{j'} \in A_{j'}$. Let $k \geq i, j, j'$. Consider $c = \alpha_{jk}(b_j) - \alpha_{j'k}(b_{j'})$. We chose these elements so that $\alpha_k(c) = 0$, so by [2.15] there is $l \geq k$ such that $\alpha_{kl}(c) = \alpha_{jl}(b_j) - \alpha_{j'l}(b_{j'}) = 0$, or $\alpha_{jl}(b_j) = \alpha_{j'l}(b_{j'})$. Taking $k = l$ in the definition of ab, we see that the definition is independent of j. Symmetrically, it is independent of i. Thus we have a well defined multiplication on A.

Now by definition, if $a_i, b_i \in A_i$ we have $\alpha_i(a_i)\alpha_i(b_i) = \alpha_i(\alpha_{ii}(a_i)\alpha_{ii}(b_i)) = \alpha_i(a_i b_i)$, so the α_i preserve multiplication. To show they are ring homomorphisms, we just need to show $\alpha_i(1) = 1$ in A. But for any $b \in A$, we can write it as $\alpha_j(b_j)$ for some $b_j \in A_j$, and pick $k \geq i, j$, and then

$$\alpha_i(1)b = \alpha_k(\alpha_{ik}(1)\alpha_{jk}(b_j)) = \alpha_k(\alpha_{jk}(b_j)) = \alpha_j(b_j) = b$$

since $\alpha_{ik}(1) = 1$, each α_{ik} being a ring homomorphism. Thus each α_i is a ring homomorphism.

To verify the ring axioms for A, we just need to note that for any three elements $a, b, c \in A$ the elements ab, ba, $a(bc)$, $(ab)c$, $ab + ac$, $a(b + c)$ are calculated via representatives in some ring A_k, then sent into A via α_k; since they hold in each A_k, they hold in A.

We can in fact prove $A = 0 \iff \exists i \in I\ (A_i = 0)$. Assume $A = 0$; then $1 = 0$ in A. Now since $\alpha_i : A_i \to A$ is a ring homomorphism, $\alpha_i(1) = 1$. By [2.15], there is $j \geq i$ such that $\alpha_{ij}(1) = 0$. But the α_{ij} are defined to be ring homomorphisms, in particular sending 1 to 1. Thus $1 = 0$ in A_j, so $A_j = 0$.

On the other hand, if some $A_i = 0$, then for all $j \geq i$ we have $1 = \alpha_{ij}(1) = \alpha_{ij}(0) = 0$, so $A_j = 0$ for $j \geq i$. Now any element $a \in A$ can be written as $\alpha_k(a_k)$ for some k and $a_k \in A_k$, by [2.15]. Find $j \geq i, k$; then $a = \alpha_k(a_k) = \alpha_j(\alpha_{kj}(a_k)) = \alpha_j(0) = 0$, so $A = 0$.

Let (A_i, α_{ij}) be a direct system of rings and let $\mathfrak{N}_i$ be the nilradical of A_i. Show that $\varinjlim \mathfrak{N}_i$ is the nilradical of $\varinjlim A_i$.

If each A_i is an integral domain, then $\varinjlim A_i$ is an integral domain.

Let $A = \varinjlim A_i$ and suppose a is in its nilradical. Then there is $n > 0$ such that $a^n = 0$. Let $i \in I$ and $a_i \in A_i$ be such that $\alpha_i(a_i) = a$. Then $0 = a^n = \alpha_i(a_i)^n = \alpha_i(a_i^n)$, so by [2.15] there is $j \geq i$ such that $\alpha_{ij}(a_i^n) = \alpha_{ij}(a_i)^n = 0$. Write $a' = \alpha_{ij}(a_i) \in A_j$. Then $a' \in \mathfrak{N}_j$ and $\alpha_j(a') = \alpha_j(\alpha_{ij}(a_i)) = \alpha_i(a_i) = a$, so $a \in \varinjlim \mathfrak{N}_i$. On the other hand, if $a_j^n = 0$, then surely $\alpha_j(a_j)^n = 0$, so $\varinjlim \mathfrak{N}_j$ is contained in the nilradical of A.

Similarly, suppose A is not an integral domain. Then there exist nonzero $a, b \in A$ such that $ab = 0$. Since $a, b \neq 0$, by [2.15], no representative of a or b can be zero. Let $\alpha_i(a_i) = a$ and $\alpha_j(b_j) = b$, and find $k \geq i, j$. Then $ab = \mu_k(\alpha_{ik}(a_i)\alpha_{jk}(b_j)) = 0$, so by [2.15] there is $l \geq k$ such that $\alpha_{lk}(\alpha_{ik}(a_i)\alpha_{jk}(b_j)) = \alpha_{il}(a_i)\alpha_{jl}(b_j) = 0$. But $a = \alpha_l(\alpha_{il}(a_i))$ and $b = \alpha_l(\alpha_{jl}(b_j))$ are nonzero, so $\alpha_{il}(a_i)$ and $\alpha_{jl}(b_j)$ are nonzero, hence zero-divisors in A_l.

Let $(B_\lambda)_{\lambda \in \Lambda}$ be a family of A-algebras. For each finite subset of Λ let B_J denote the tensor product (over A) of the B_λ for $\lambda \in J$. If J' is another finite subset of Λ and $J \subseteq J'$, there is a canonical A-algebra homomorphism $B_J \to B_{J'}$. Let B denote the direct limit of the rings B_J as J runs through all finite subsets of Λ. The ring B has a natural A-algebra structure for which the homomorphisms $B_J \to B$ are A-algebra homomorphisms. The A-algebra B is the tensor product *of the family $(B_\lambda)_{\lambda \in \Lambda}$.*

We should first note that the map given on p. 31 making the tensor product of A-algebras an A-algebra is a misprint. If we have ring homomorphisms $f : A \to B$ and $g : A \to C$, and define $h' : A \to B \otimes_A C$ by $h'(a) = f(a) \otimes g(a)$, then $h'(1) = 1 \otimes 1$ but

$$h'(a) = f(a) \otimes g(a) = a^2(1 \otimes 1) \neq a(1 \otimes 1) = ah'(1)$$

in general. The proper definition is instead $h : a \mapsto f(a) \otimes 1 = 1 \otimes g(a) = a(1 \otimes 1)$.

If $J = \{\lambda_1, \ldots, \lambda_m\}$ and $J' = J \cup \{\lambda_{m+1}, \ldots, \lambda_n\}$, the canonical homomorphism $B_J \to B_{J'}$ is given by $b_{\lambda_1} \otimes \cdots \otimes b_{\lambda_m} \mapsto b_{\lambda_1} \otimes \cdots \otimes b_{\lambda_m} \otimes 1 \otimes \cdots \otimes 1$. It is obviously an A-algebra homomorphism. Let $\beta_J : B_J \to B$ denote the canonical map associated to the direct limit. The A-algebra structure on B can be given as follows: let $b \in B$ and $a \in A$. There are a finite $J \subseteq \Lambda$ and an element $b_J \in B_J$ such that $b = \beta_J(b_J)$; define $ab = \beta_J(ab_J)$. Since the maps $B_J \to B_{J'}$ are A-algebra homomorphisms, this definition is independent of the choice of J. We saw in [2.21] that β_J is a ring homomorphism, and by the definition of scalar multiplication in B it is also an A-algebra homomorphism.

Flatness and Tor

In these Exercises it will be assumed that the reader is familiar with the definition and basic properties of the Tor functor.

If M is an A-module, the following are equivalent:

i) M is flat;

ii) $\operatorname{Tor}_n^A(M, N) = 0$ for all $n > 0$ and all A-modules N;

iii) $\operatorname{Tor}_1^A(M, N) = 0$ for all A-modules N.

i) $\implies$ ii): Recall that $\operatorname{Tor}_n^A(M, -)$ are the derived functors of $- \otimes_A M$. This means that if we let

$$P : \cdots \to P_2 \to P_1 \to P_0 \to N \to 0$$

be a projective resolution of N, and tensor with M to get

$$P \otimes_A M : \cdots \to P_2 \otimes_A M \to P_1 \otimes_A M \to P_0 \otimes_A M \to 0$$

(lopping off the $M \otimes N$ term so that we get $H_0 = M \otimes N$), then the homology groups $H_n(P \otimes_A M) = \ker(P_n \otimes M \to P_{n-1} \otimes M) / \operatorname{im}(P_{n+1} \otimes M \to P_n \otimes M)$ are by definition the groups $\operatorname{Tor}_n^A(M, N)$. Since M is flat, the sequence $P \otimes_A M$ is exact except at $P_0 \otimes_A M$, so the homology groups $\operatorname{Tor}_n^A(M, N) = 0$ for $n > 0$.

ii) $\implies$ iii): $1 > 0$.

iii) $\implies$ i): Let $0 \to N' \to N \to N'' \to 0$ be a short exact sequence of A-module homomorphisms. Since the $\operatorname{Tor}_n^A(M, -)$ are derived functors, they fit into a Tor exact sequence including $\operatorname{Tor}_1^A(M, N'') \to M \otimes_A N' \to M \otimes_A N$. As by assumption $\operatorname{Tor}_1^A(M, -) = 0$, we get a short exact sequence $0 \to M \otimes_A N' \to M \otimes_A N$; as the injection $N' \rightarrowtail N$ was arbitrary, M is flat by (2.19).

Let $0 \to N' \to N \to N'' \to 0$ be an exact sequence, with N'' flat. Then N' is flat $\iff$ N is flat.

The book suggests we use the Tor exact sequence. It seems that this requires us to use the additional fact (not a priori obvious) that $\operatorname{Tor}_n^A(M, N) \cong \operatorname{Tor}_n^A(N, M)$ for all $n \geq 0$ and A-modules M, N. Making this assumption, let M be an arbitrary A-module; we have an exact sequence

$$\begin{tikzcd}
& 0 \arrow[d, equal] & & & 0 \arrow[d, equal] & & \\
\cdots \arrow[r] & \operatorname{Tor}_2^A(M,N'') \arrow[r] & \operatorname{Tor}_1^A(M,N') \arrow[r] & \operatorname{Tor}_1^A(M,N) \arrow[r] & \operatorname{Tor}_1^A(M,N'') \arrow[r] & M \otimes_A N' \arrow[r] & \cdots .
\end{tikzcd}$$

The criterion [2.24.iii] and the isomorphism $\operatorname{Tor}_1^A(N', M) \cong \operatorname{Tor}_1^A(N, M)$ mean N is flat just if N' is.

We now prove that $\operatorname{Tor}_n^A(M, N) \cong \operatorname{Tor}_n^A(N, M)$.[18]

First, a lemma: if F is a free A-module, then $\operatorname{Tor}_1^A(F, -) = 0$ and $\operatorname{Tor}_1^A(-, F) = 0$. Since F is flat by [2.4], by [2.24] we have $\operatorname{Tor}_1^A(F, -) = 0$. As for $\operatorname{Tor}_1^A(-, F)$,[19] consider the free resolution $P_2 = 0 \to P_1 = 0 \to P_0 = F \to F \to 0$ of F; tensoring with any A-module M we get a sequence $0 \to P_1 \otimes M = 0 \to F \otimes M \to 0$, whose homology $\operatorname{Tor}_1^A(M, F)$ at $P_1 \otimes M = 0$ is 0.

Now let M and N be arbitrary A-modules. We can write them as quotients of free A-modules F, G, so that we have exact sequences $D\colon 0 \to M' \to F \to M \to 0$ and $E\colon 0 \to N' \to G \to N \to 0$. By [2.4], F and G are flat, so the sequences $0 \to M' \otimes G \to F \otimes G \to M \otimes G \to 0$ and $0 \to F \otimes N' \to F \otimes G \to F \otimes N \to 0$ are exact. The Tor exact sequence for $M \otimes E$ is $0 = \operatorname{Tor}_1^A(M, G) \to \operatorname{Tor}_1^A(M, N) \to M \otimes N' \to M \otimes G \to M \otimes N \to 0$. Tensoring E with D, adding in the Tor exact sequence, and using (2.18), we have the commutative diagram on the right with exact rows and columns. The Snake Lemma, applied to the middle two rows, gives an exact sequence $0 \to \operatorname{Tor}_1^A(M, N) \to M' \otimes N \to F \otimes N$. On the other hand, the Tor exact sequence for $N \otimes D$ and commutativity of the tensor product (2.14.i) give an exact sequence

$$\begin{tikzcd}
& & & \operatorname{Tor}_1^A(M, G) \arrow[r, equal] \arrow[d] & 0 \\
& & 0 \arrow[r] \arrow[d] & \operatorname{Tor}_1^A(M, N) \arrow[d] \arrow[dddll, rounded corners] & \\
& M' \otimes N' \arrow[r] \arrow[d] & F \otimes N' \arrow[r] \arrow[d] & M \otimes N' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M' \otimes G \arrow[r] \arrow[d] & F \otimes G \arrow[r] \arrow[d] & M \otimes G \arrow[r] \arrow[d] & 0 \\
& M' \otimes N \arrow[r] \arrow[d] & F \otimes N \arrow[r] \arrow[d] & M \otimes N \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd}$$

$$0 = \operatorname{Tor}_1^A(N, F) \to \operatorname{Tor}_1^A(N, M) \rightarrowtail M' \otimes N \to F \otimes N.$$

Since $\operatorname{Tor}_1^A(M, N)$ and $\operatorname{Tor}_1^A(N, M)$ both embed as the kernel of $M' \otimes N \to F \otimes N$, we see $\operatorname{Tor}_1^A(M, N) \cong \operatorname{Tor}_1^A(N, M)$.

Let N be an A-module. Then N is flat $\iff$ $\operatorname{Tor}_1(A/\mathfrak{a}, N) = 0$ for all finitely generated ideals $\mathfrak{a}$ in A.

The implication $\implies$ follows from [2.24].

For $\impliedby$, assume $\operatorname{Tor}_1(A/\mathfrak{a}, N) = 0$ for all finitely generated ideals $\mathfrak{a}$ in A. Then given $E\colon 0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$, the Tor sequence of $E \otimes N$ shows that $\mathfrak{a} \otimes N \to A \otimes N$ is injective. Now let $\mathfrak{b}$ be an arbitrary ideal of A; we want to show $\mathfrak{b} \otimes N \to A \otimes N$ injective. Inclusions $\mathfrak{a}_i \hookrightarrow \mathfrak{a}_j$ of finitely generated A-submodules (ideals) in $\mathfrak{b}$ induce maps of exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{a}_i \otimes N \arrow[r, hook] \arrow[d, hook] & A \otimes N \arrow[r, two heads] \arrow[d, equal] & A/\mathfrak{a}_i \otimes N \arrow[r] \arrow[d, two heads] & 0 \\
0 \arrow[r] & \mathfrak{a}_j \otimes N \arrow[r, hook] & A \otimes N \arrow[r, two heads] & A/\mathfrak{a}_j \otimes N \arrow[r] & 0,
\end{tikzcd}$$

which piece together to give homomorphisms between the exact systems $(\mathfrak{a}_i \otimes N)$, $(A \otimes N)$, and $(A/\mathfrak{a}_i \otimes N)$ for finitely generated ideals $\mathfrak{a}_i \subseteq \mathfrak{b}$ of A. By [2.17], the direct limit $\varinjlim \mathfrak{a}_i = \mathfrak{b}$. Obviously $\varinjlim A = A$, and similarly, $\varinjlim A/\mathfrak{a}_i \cong A/\mathfrak{b}$.[20] By [2.20] we have $\varinjlim(\mathfrak{a}_i \otimes N) \cong \mathfrak{b} \otimes N$ and $\varinjlim(A \otimes N) = A \otimes N \cong N$, and $\varinjlim(A/\mathfrak{a}_i \otimes N) \cong A/\mathfrak{b} \otimes N \cong N/\mathfrak{b}N$

[18] http://uni.edu/ajur/v3n3/Banerjee%20pp%207-14.pdf

[19] http://math.uchicago.edu/~may/MISC/TorExt.pdf

[20] To see this we show that $A/\mathfrak{b}$ has the universal property ([2.16]) of the direct system $(A/\mathfrak{a}_i, \pi_{ij})$, writing $\pi_{ij}\colon A/\mathfrak{a}_i \twoheadrightarrow A/\mathfrak{a}_j$ and $\pi_i\colon A/\mathfrak{a}_i \twoheadrightarrow A/\mathfrak{b}$. Set $\pi_{0i}\colon A \twoheadrightarrow A/\mathfrak{a}_i$. Evidently $\pi_j \circ \pi_{ij} = \pi_i\colon A/\mathfrak{a}_i \twoheadrightarrow A/\mathfrak{a}_j \twoheadrightarrow A/\mathfrak{b}$. Let $\alpha_i\colon A/\mathfrak{a}_i \to P$ be such that $\alpha_j \circ \pi_{ij} = \alpha_i$. If we want to define

by [2.2]. Then [2.19] states that direct limit is an exact functor, so the direct limit $0 \to \mathfrak{b} \otimes N \to A \otimes N \to N/\mathfrak{b}N \to 0$ is also exact, and thus $\mathfrak{b} \otimes N \to A \otimes N$ is injective. Writing $E' \colon 0 \to \mathfrak{b} \to A \to A/\mathfrak{b} \to 0$ and looking at the Tor sequence of $E' \otimes N$, the injectivity of this map shows $\operatorname{Tor}_1(A/\mathfrak{b}, N) = 0$.

Now let M be a finitely generated module, generated by say $x_1, \ldots, x_n$, and for $i = 0, \ldots, n$ let $M_i = \sum_{j=0}^{i} Ax_j$. Then each M_i/M_{i-1}, $i = 1, \ldots n$ is generated by one element $\bar{x}_i$, so the map $f_i \colon A \to M_i/M_{i+1}$ given by $a \mapsto a\bar{x}_i$ is a surjective A-module homomorphism, and by the second display of p. 19 (the first isomorphism theorem), if we write $\mathfrak{a}_i = \ker(f_i)$ we have $A/\mathfrak{a}_i \cong M_i/M_{i-1}$. Consider the short exact sequences $E_i \colon 0 \to M_{i-1} \to M_i \to A/\mathfrak{a}_i \to 0$ given by these isomorphisms. Suppose inductively that $\operatorname{Tor}_1(M_{i-1}, N) = 0$; this is trivial for $i = 1$ and $M_0 = 0 = A/(1)$. The Tor sequence of $E_i \otimes N$ gives, in part, $0 = \operatorname{Tor}_1(M_{i-1}, N) \to \operatorname{Tor}_1(M_i, N) \to \operatorname{Tor}_1(A/\mathfrak{a}_i, N) = 0$, so by exactness $\operatorname{Tor}_1(M_i, N) = 0$. By induction, $\operatorname{Tor}_1(M, N) = 0$ for all finitely generated modules.

Now let $0 \to K \to P$ be any injection of finitely generated A-modules. Complete this to a short exact sequence $E'' \colon 0 \to K \to P \to K/P \to 0$, where K/P is finitely generated as well. The Tor sequence of $E'' \otimes N$ gives $0 = \operatorname{Tor}(K/P, N) \to K \otimes N \to P \otimes N$, so $K \otimes N \to P \otimes N$ is injective. Since $K \rightarrowtail P$ was an arbitrary injection of finitely generated A-modules, by criterion iv) of (2.19), N is flat.

A ring A is absolutely flat *if every A-module is flat. Prove that the following are equivalent:*

i) A is absolutely flat;

ii) every principal ideal is idempotent;

iii) every finitely generated ideal is a direct summand of A.

i) $\Longrightarrow$ ii): Let $\mathfrak{a} \lhd A$. The inclusion $\mathfrak{a} \hookrightarrow A$ is of course injective; by assumption, the module $A/\mathfrak{a}$ is flat, so the induced map $\mathfrak{a} \otimes_A A/\mathfrak{a} \to A \otimes_A A/\mathfrak{a} \xrightarrow{\sim} A/\mathfrak{a}$ is injective, where the isomorphism is by the absorption law (2.14.iv). But this composition is the zero map, for it takes $a \otimes \bar{1} \mapsto a \otimes \bar{1} \mapsto \bar{a} = \bar{0}$, and thus the module $\mathfrak{a} \otimes_A A/\mathfrak{a} = 0$. Since we have a short exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$, tensoring with $\mathfrak{a}$, assumed flat, gives by (2.19), an exact sequence $0 = \mathfrak{a} \otimes_A \mathfrak{a} \to A \otimes_A \mathfrak{a} \to 0 = \mathfrak{a} \otimes_A A/\mathfrak{a}$, showing the composition $\mathfrak{a} \otimes_A \mathfrak{a} \to A \otimes_A \mathfrak{a} \to \mathfrak{a}$, using (2.14.iv), is an isomorphism. But this sends $a \otimes a' \mapsto a \otimes a' \mapsto aa'$, so since this map is surjective, every element of $\mathfrak{a}$ is a finite sum of elements aa' with $a, a' \in \mathfrak{a}$ and thus $\mathfrak{a} = \mathfrak{a}^2$. In particular, for any $x \in A$ we have $(x) = (x)^2$ idempotent.

ii) $\Longrightarrow$ iii): If every finitely generated ideal $\mathfrak{a}$ is generated by some idempotent e, then by the proof of iii) $\Longrightarrow$ ii) in [1.22], we have a decomposition $A \cong (e) \oplus (1-e)$. Obviously this decomposition is only interesting if $e \neq 0, 1$.

It remains to show each finitely generated ideal is generated by a single idempotent. For a principal ideal (x), by assumption $x \in (x^2)$, so we may write $x = ax^2$ for some $a \in A$. Multiplying both sides by a, we have $ax = a^2x^2 = (ax)^2$, so $e = ax$ is idempotent. Since $e = ax \in (x)$ and $x = ax^2 = (ax)x = ex \in (e)$, we have $(x) = (e)$. Now any finitely generated ideal $\mathfrak{a} = (x_1, \ldots, x_n) = (e_1, \ldots, e_n)$ is generated by idempotents, where e_i is an idempotent generating (x_i). As in [1.11.iii], we show every ideal finitely generated by idempotents is generated by a single element. This is trivial for $n = 1$, so inductively suppose it holds for all ideals with n generators, and let $\mathfrak{a} = (x_1, \ldots, x_n, y)$ be an ideal generated by $n+1$ elements. Let e be an idempotent generating $(x_1, \ldots, x_n)$ and f an idempotent generating (y), so that $\mathfrak{a} = (e, f)$. If we let $z = e + f - ef$, then we have $ez = e^2 + ef - e^2f = e$ and $fz = fe + f^2 - fef = f$, so $\mathfrak{a} = (e, f) = (z)$ is principal, and there is thus an associated idempotent g such that $(g) = (z) = \mathfrak{a}$.

iii) $\Longrightarrow$ i): Let N be an arbitrary A-module. To show it is flat, by [2.26] it suffices to show that $\operatorname{Tor}_1^A(A/\mathfrak{a}, N) = 0$ for all finitely generated ideals $\mathfrak{a} \in A$. By assumption, each of these is a direct summand, so $A \cong \mathfrak{a} \oplus A/\mathfrak{a}$, and by (2.14.iv,iii) we have isomorphisms $N \cong A \otimes N \cong (\mathfrak{a} \otimes N) \oplus (A/\mathfrak{a} \otimes N)$, so the inclusion $\mathfrak{a} \hookrightarrow A$ induces an injection $\mathfrak{a} \otimes N \rightarrowtail A \otimes N$. Now the Tor exact sequence for $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ includes the fragment $0 = \operatorname{Tor}_1^A(A, N) \to \operatorname{Tor}_1^A(A/\mathfrak{a}, N) \to \mathfrak{a} \otimes N \to A \otimes N$, so $\operatorname{Tor}_1^A(A/\mathfrak{a}, N)$ is isomorphic to the kernel of $\mathfrak{a} \otimes N \rightarrowtail A \otimes N$, which is zero.

A Boolean ring is absolutely flat.

In a Boolean ring each element is idempotent, so each principal ideal is idempotent, so by [2.27] the ring is absolutely flat.

The ring of Chapter 1, Exercise 7 is absolutely flat.

Recall that this is a ring A in which for every element a there is a number $n = n(a) > 1$ such that $a^n = a$. Then $a = a^2a^{n-2} \in (a^2)$ so every principal ideal is idempotent, and by [2.27] A is absolutely flat.

$\alpha \colon A/\mathfrak{b} \to P$ such that $\alpha \circ \pi_i = \alpha_i$, taking $i = 0$, we are forced to try $\alpha(\pi_0(a)) = \alpha(a + \mathfrak{b}) = \alpha_0(a)$ for $a \in A$. Indeed, for any i and any $a + \mathfrak{a}_i \in A/\mathfrak{a}_i$ we have

$$\alpha_i(a + \mathfrak{a}_i) = \alpha_i(\pi_{0i}(a)) = \alpha_0(a) = \alpha(\pi_0(a)) = \alpha(\pi_i(a + \mathfrak{a}_i))$$

so this homomorphism meets the requirement and $A/\mathfrak{b}$ has the universal property.

CITE [1.12]?

Every homomorphic image of an absolutely flat ring is absolutely flat.

Let A be absolutely flat and let $(\bar{x})$ be a principal ideal in $A/\mathfrak{a}$. Then for the lift $x \in A$ we have, by [2.27], that $(x)^2 = (x)$, so there is $a \in A$ such that $ax^2 = x$. Downstairs in $A/\mathfrak{a}$ we have $\bar{a}\bar{x}^2 = \bar{x}$, so $(\bar{x})^2 = (\bar{x})$ and $A/\mathfrak{a}$ is absolutely flat by [2.27] again.

If a local ring is absolutely flat, then it is a field.

Let $\mathfrak{m}$ be the maximal ideal of a local, absolutely flat ring A. We want to show $\mathfrak{m} = 0$. Suppose $x \in \mathfrak{m}$. Then by [2.27] we have an idempotent $e \in (x)$ with $(e) = (x)$, and $e = 0 \iff x = 0$. Then $f = 1 - e$ is an idempotent as well, but also f is a unit by (1.9) since e is in the Jacobson radical $\mathfrak{R} = \mathfrak{m}$. Then we have $1 = f^{-1}f = f^{-1}f^2 = (f^{-1}f)f = f$, so $e = 0$. Thus $\mathfrak{m} = 0$, so $A \cong A/(0) = A/\mathfrak{m}$ is a field.

If A is absolutely flat, every non-unit in A is a zero-divisor.

Let $x \in A$ be a non-unit; then $(x) \neq (1)$ is a finitely generated ideal, and so by [2.27] there is another ideal $\mathfrak{b} \neq (0)$ such that $A \cong (x) \oplus \mathfrak{b}$. Then $\mathfrak{b}x \in (x) \cap \mathfrak{b} = (0)$, so x is a zero-divisor.

Rings and Modules of Fractions

Exercise. *Verify that these definitions [repeated below] are independent of the choices of representatives (a, s) and (b, t), and that $S^{-1}A$ satisfies the axioms of a commutative ring with identity.*

We recall that S is a multiplicative submonoid of A, meaning a subset closed under multiplication and containing 1. An element of $S^{-1}A$ is defined to be an equivalence class a/s of pairs $(a, s) \in A \times S$ under the relation $\equiv$ given by

$$(a, s) \equiv (b, t) \iff \exists u \in S\,[(at - bs)u = 0].$$

The book shows that $\equiv$ indeed is an equivalence relation, and then defines

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}, \qquad \frac{a}{s} \cdot \frac{b}{t} := \frac{as}{bs}.$$

It falls to us to verify these operations are well defined. To show $\frac{a}{s} + \frac{b}{t}$ is independent of the representatives of a/s and b/t chosen, suppose we calculated with two pairs of representatives $(a, s) \equiv (a', s')$ and $(b, t) \equiv (b', t')$. Then by definition there are $u, v \in S$ such that $(as' - a's)u = 0 = (bt' - b't)v$ in A. We need to verify that $(at + bs, st) \equiv (a't' + b's', s't')$, meaning that there exists $w \in S$ such that $([at + bs]s't' - [a't' + b's']st)w = 0$ in A. But $w = uv$ works, for

$$w([at+bs]s't'-[a't'+b's']st) = uv(as'tt'+bss't'-a'stt'-b'ss't) = u(as'-a's)tt'v+v(bt'-b't)ss'u = 0+0 = 0.$$

Similarly, $\cdot$ is well defined: $(ab, st) \equiv (a'b', s't')$, for setting $w = uv$ we have

$$w(abs't' - a'b'st) = uv(abs't' - a'bst' + a'bst' - a'b'st) = u(as' - a's)bt'v + v(bt' - b't)a'su = 0 + 0 = 0.$$

Note as a preliminary that for any $a/s \in A$ and $t \in S$ we have $at/st = a/s$, for $(at)s - a(st) = 0$ by commutativity and associativity of $\cdot$ in A.

Now we verify that $(S^{-1}A, +, 0/1)$ is an abelian group. $+$ is associative, since given $a/s, b/t, c/u \in S^{-1}A$ we have

$$\left(\frac{a}{s} + \frac{b}{t}\right) + \frac{c}{u} = \frac{at + bs}{st} + \frac{c}{u} = \frac{atu + bsu + cst}{stu} = \frac{a}{s} + \frac{bu + ct}{tu} = \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u}\right),$$

using distributivity and commutativity of $\cdot$ in A. We see $+$ is commutative, for

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st} = \frac{bs + at}{ts} = \frac{b}{t} + \frac{a}{s},$$

using commutativity of $+$ and $\cdot$ in A. For any element $v \in S$, we have $0/v = 0v/1v = 0/1$ a neutral element for $+$, since

$$\frac{0}{1} + \frac{a}{s} = \frac{0s + a1}{1s} = \frac{a}{s},$$

using the properties of 0 and 1 in A. The additive inverse of a/s is $(-a)/s$, because

$$\frac{a}{s} + \frac{-a}{s} = \frac{as + (-a)s}{s^2} = \frac{0}{s^2} = \frac{0}{1}.$$

Now we want to prove that $(S^{-1}A, +, \cdot, 0/1, 1/1)$ is a commutative ring. The new $\cdot$ is associative since

$$\left(\frac{a}{s}\frac{b}{t}\right)\frac{c}{u} = \frac{ab}{st}\frac{c}{u} = \frac{abc}{stu} = \frac{a}{s}\frac{bc}{tu} = \frac{a}{s}\left(\frac{b}{t}\frac{c}{u}\right),$$

implicitly using associativity of $\cdot$ in A. The new $\cdot$ is commutative because

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st} = \frac{ba}{ts} = \frac{b}{t}\frac{a}{s},$$

using commutativity of $\cdot$ in A. The element $1/1$ is neutral for $\cdot$ because

$$\frac{1}{1}\frac{a}{s} = \frac{1a}{1s} = \frac{a}{s},$$

1 being neutral for $\cdot$ in A. Finally, $\cdot$ distributes over $+$ because

$$\frac{a}{s}\left(\frac{b}{t}+\frac{c}{u}\right) = \frac{a}{s}\frac{bu+ct}{tu} = \frac{abu+act}{stu} = \frac{absu+acst}{stsu} = \frac{absu}{stsu} + \frac{acst}{stsu} = \frac{ab}{st} + \frac{ac}{su} = \frac{a}{s}\frac{b}{t} + \frac{a}{s}\frac{c}{u}.$$

Let M be an A-module. If we redefine a, b, c to be elements of an M, then (but for our tendency to write as rather than sa, which strictly speaking doesn't matter for modules over commutative rings) the proofs of well-definedness, associativity, commutativity, $0/1$, and $-a/s = -(a/s)$ for $(S^{-1}A, +, 0/1)$ go through to define an abelian group structure on $(S^{-1}M, +, 0/1)$. Now we show $S^{-1}M$ carries a natural $S^{-1}A$-module structure. If we let $b = m \in M$, the well-definedness proof for $\cdot$ in $S^{-1}A$ shows that $\frac{a}{s}\frac{m}{t} = \frac{am}{st}$ gives a well-defined scalar product $S^{-1}A \times S^{-1}M \to S^{-1}M$. We have the four axioms of p. 17 to verify. If we let $a \in M$, the proof $\frac{1}{1}\frac{a}{s} = \frac{a}{s}$ shows $1/1$ acts as the identity on $S^{-1}M$, the fourth axiom. Letting $b, c \in M$, the associativity of $\cdot$, and the distributivity of $\cdot$ over $+$ for $S^{-1}A$ provide the third and first axioms. Letting $a, b \in A$, $s, t, u \in S$ and $m \in M$, the second (and last) axiom is

$$\left(\frac{a}{s}+\frac{b}{t}\right)\frac{m}{u} = \frac{at+bs}{st}\frac{m}{u} = \frac{atm+bsm}{stu} = \frac{atm}{stu} + \frac{bsm}{stu} = \frac{am}{su} + \frac{bm}{tu}.$$

Proposition 3.11. *v) The operation S^{-1} commutes with formation of finite sums, products, intersections and radicals.*

(3.4.i,ii) show S^{-1} distributes over finite sums and intersections. (1.18) shows $S^{-1}(\mathfrak{ab}) = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$, and $S^{-1}r(\mathfrak{a}) \subseteq r(S^{-1}\mathfrak{a})$. It remains to show $r(S^{-1}\mathfrak{a}) \subseteq S^{-1}r(\mathfrak{a})$, so suppose $x/s \in S^{-1}A$ is in $r(S^{-1}\mathfrak{a})$. Then for some $n > 0$ its n^{th} power is some $a/t \in S^{-1}\mathfrak{a}$, meaning $x^n/s^n = (x/s)^n = a/t$ in $S^{-1}A$. By the definition of equality in $S^{-1}A$, there is some $u \in S$ so that $utx^n = us^n a \in \mathfrak{a}$. Multiplying both sides by $(ut)^{n-1}$ we see $(utx)^n \in \mathfrak{a}$, and $utx \in r(\mathfrak{a})$. Thus $utx/uts = x/s \in S^{-1}r(\mathfrak{a})$ as claimed.

EXERCISES

Let S be a multiplicatively closed subset of a ring A, and let M be a finitely generated A-module. Prove that $S^{-1}M = 0$ if and only if there exists $s \in S$ such that $sM = 0$.

Assume $sM = 0$ for some $s \in S$, and let $m/t \in S^{-1}M$. Then $s(1m - t0) = 0$ in M, so $m/t = 0/1$ in $S^{-1}M$.

Conversely, let M be an A-module finitely generated by $m_1, \ldots, m_n$, and suppose that $S^{-1}M = 0$. Then in particular we have for each i that $m/1 = 0/1$ in $S^{-1}M$, so there is $s_i \in S$ such that $0 = s_i(1m_i - 1\cdot 0) = s_i m_i$ in M. Let $s = s_1 \cdots s_n$, which is in S since S is multiplicatively closed. Then for any element $m = \sum a_i m_i \in M$ we have $0 = sm = s(1m - 1\cdot 0)$, and $m/1 = 0/1$ in $S^{-1}M$.

Let $\mathfrak{a}$ be an ideal of a ring A, and let $S = 1 + \mathfrak{a}$. Show that $S^{-1}\mathfrak{a}$ is contained in the Jacobson radical of $S^{-1}A$.

Since $0 \in \mathfrak{a}$ we have $1 \in S = 1 + \mathfrak{a}$, and if $a, b \in \mathfrak{a}$, then $(1+a)(1+b) = 1 + a + b + ab \in S = 1 + \mathfrak{a}$, so S is multiplicatively closed. Now to show $S^{-1}\mathfrak{a} \subseteq \mathfrak{R}(S^{-1}A)$, it is enough, by (1.9), to show the set $1 - S^{-1}\mathfrak{a} = 1 - (S^{-1}A)(S^{-1}\mathfrak{a})$ is made up of units. But if $\frac{a}{1+b} \in S^{-1}\mathfrak{a}$, then $\frac{1}{1} - \frac{a}{1+b} = \frac{1+b-a}{1+b} \in S^{-1}S \subseteq (S^{-1}A)^{\times}$.

Use this result and Nakayama's lemma to give a proof of (2.5) which does not depend on determinants.

(2.5) states that for all finitely generated A-modules M and $\mathfrak{a} \lhd A$ such that $\mathfrak{a}M = M$ there is $x \in 1 + \mathfrak{a}$ such that $xM = 0$.

So suppose M is finitely generated by some $m_1, \ldots, m_n$ with $\mathfrak{a}M = M$. Then localizing by $S = 1 + \mathfrak{a}$, by (3.11.v) we have $(S^{-1}\mathfrak{a})(S^{-1}M) = S^{-1}M$. The last paragraph shows that $S^{-1}\mathfrak{a} \subseteq \mathfrak{R}(S^{-1}A)$, the Jacobson radical, and $S^{-1}M$ is finitely generated over $S^{-1}A$ by $m_1/1, \ldots, m_n/1$, so the conditions of Nakayama's Lemma are met, and we conclude $S^{-1}M = 0$. But then by [3.1] there is $x \in S = 1 + \mathfrak{a}$ such that $xM = 0$.

Let A be a ring, let S and T be two multiplicatively closed subsets of A, and let U be the image of T in $S^{-1}A$. Show that the rings $(ST)^{-1}A$ and $U^{-1}(S^{-1}A)$ are isomorphic.

As a preliminary, we prove the canonical map $\phi_S\colon A \to S^{-1}A$ is a epimorphism, meaning not that is surjective, but that it is right-cancellable. Suppose we have a ring homomorphisms $\mu\colon S^{-1}A \to B$, and let $\lambda = \mu \circ \phi_S$. Since for all $s \in S$ we have $\phi_S(s) \in S^{-1}A$ a unit, we then have $\lambda(s) = \mu(\phi_S(s))$ a unit of B. By (3.1) there is a *unique* ring homomorphism $\nu\colon S^{-1}A \to B$ such that $\nu \circ \phi_S = \lambda$. Thus

$$\mu \circ \phi_S = \nu \circ \phi_S \implies \mu = \nu. \tag{3.1}$$

Now U is a multiplicative submonoid of $S^{-1}A$ since it is the image of a multiplicative submonoid under a ring homomorphism, which preserves multiplication and unity. ST is also multiplicative submonoid of A, since $1 \in S$, T implies $1 = 1 \cdot 1 \in ST$, and if st, $s't' \in ST$, where s, $s' \in S$ and t, $t' \in T$, then $(st)(s't') = (ss')(tt') \in ST$ since S and T are multiplicatively closed. Note $S = S \cdot 1 \subseteq ST$ and $T = 1T \subseteq ST$.

Consider the canonical map $\phi_{ST}\colon A \to (ST)^{-1}A$. Each element of S is taken to a unit, since $S \subseteq ST$, so by (3.1) there is a unique homomorphism $\rho_S^{ST}\colon S^{-1}A \to (ST)^{-1}A$ such that

$$\rho_S^{ST} \circ \phi_S = \phi_{ST}. \tag{3.2}$$

$$\begin{tikzcd}
A \arrow[r, "\phi_S"] \arrow[rrd, "\phi_{ST}"'] & S^{-1}A \arrow[r, "\phi_U"] \arrow[rd, dotted, "\rho_S^{ST}"] & U^{-1}(S^{-1}A) \arrow[d, dotted, shift right, "\psi"'] \\
 & & (ST)^{-1}A \arrow[u, dotted, shift right, "\psi'"']
\end{tikzcd}$$

By the proof of that proposition we have $\rho_S^{ST}(a/s) = \phi_{ST}(a)\phi_{ST}(s)^{-1} = a/s \in (ST)^{-1}A$. Now each element $t/1 \in U \subseteq S^{-1}T \subseteq S^{-1}A$ is taken by ρ_S^{ST} to $t/1 \in (ST)^{-1}A$, which is a unit since $T \subseteq ST$. Then (3.1) again induces a unique homomorphism $\psi\colon U^{-1}(S^{-1}A) \to (ST)^{-1}A$ such that, if $\phi_U\colon S^{-1}A \to U^{-1}(S^{-1}A)$ is the canonical map, then

$$\psi \circ \phi_U = \rho_S^{ST}. \tag{3.3}$$

Composing with $\phi_S\colon A \to S^{-1}A$ on the right we get

$$\psi \circ \phi_U \circ \phi_S \overset{\text{Eq. 3.3}}{=} \rho_S^{ST} \circ \phi_S \overset{\text{Eq. 3.2}}{=} \phi_{ST}. \tag{3.4}$$

If ψ is a bijection, we are done. However it's more natural to use universal properties to construct an inverse. Now the composition $\phi_U \circ \phi_S\colon A \to S^{-1}A \to U^{-1}(S^{-1}A)$ taking $a \mapsto a/1 \mapsto \frac{a/1}{1/1}$ takes each element of S to a unit (inverse $\frac{1/s}{1/1}$) and each element of T to a unit (inverse $\frac{1/1}{t/1}$), and so takes each element of ST to a unit. By (3.1), there is a unique homomorphism $\psi'\colon (ST)^{-1}A \to U^{-1}(S^{-1}A)$ such that

$$\psi' \circ \phi_{ST} = \phi_U \circ \phi_S. \tag{3.5}$$

Composing with ψ on the left gives $\psi \circ \psi' \circ \phi_{ST} \overset{\text{Eq. 3.5}}{=} \psi \circ \phi_U \circ \phi_S \overset{\text{Eq. 3.4}}{=} \phi_{ST}$. Since ϕ_{ST} is an epimorphism (Eq. 3.1), $\psi \circ \psi' = \mathrm{id}_{(ST)^{-1}A}$. On the other hand, since $\psi \circ \phi_U \overset{\text{Eq. 3.3}}{=} \rho_S^{ST}$, composing with ψ' on the left and ϕ_S on the right gives $\psi' \circ \psi \circ \phi_U \circ \phi_S \overset{\text{Eq. 3.4}}{=} \psi' \circ \phi_{ST} \overset{\text{Eq. 3.5}}{=} \phi_U \circ \phi_S$. Since ϕ_U and ϕ_S are epimorphisms (Eq. 3.1), we have $\psi' \circ \psi = \mathrm{id}_{U^{-1}(S^{-1}A)}$.[1]

[1] A proof avoiding universal properties is as follows. Define a ring isomorphism $\psi\colon (ST)^{-1}A \to U^{-1}(S^{-1}A)$. Set $\psi(a/st) = \frac{a/s}{t/1}$. To see it is well-defined, suppose $a/st = a'/s't'$ in $(ST)^{-1}A$; we claim that $\frac{a/s}{t/1} = \frac{a'/s'}{t'/1}$. This will follow if there is $u = t_0/1 \in U$ such that $\frac{at't_0}{s} = u\frac{a}{s}\frac{t'}{1} = u\frac{a'}{s'}\frac{t}{1} = \frac{a'tt_0}{s'}$ in $S^{-1}A$. This will in turn be the case if there is $s_0 \in S$ such that $s_0at't_0s' = s_0a'tt_0s$ in A. But since we assumed $a/st = a'/s't'$, by definition there is $s''t'' \in ST$ such that $s''t''as't' = s''t''a'st$, and we may take $s_0 = s''$ and $t_0 = t''$.

Now we show it is a bijection. Any element of $U^{-1}(S^{-1}A)$ can be written as $\frac{a/s}{t/1}$ for some $a \in A$, $s \in S$, $t \in T$, and then is mapped onto by a/st, so ϕ is surjective. Now suppose $\frac{a/s}{t/1} = \phi(a/st) = 0 = \frac{0}{1} = \frac{0/1}{1/1}$. By the definition of equality in $U^{-1}(S^{-1}A)$, there is $u = t'/1 \in U$ such that $\frac{at'}{s} = \frac{t'}{1}\frac{a}{s}\frac{1}{1} = \frac{t'}{1}\frac{0}{1}\frac{t}{1} = \frac{0}{1}$ in $S^{-1}A$. But then by the definition of equality in $S^{-1}A$ there is $s' \in S$ such that $s't'a = s'0s = 0$. Then $a/1 = 0/1$ in $(ST)^{-1}A$, so $\frac{a}{st}$ is zero and ϕ is injective.

It remains to show ψ is a ring homomorphism. Now $\psi(1/(1 \cdot 1)) = \frac{1/1}{1/1}$ is the unity of $U^{-1}(S^{-1}A)$, and if we let a/st and $a'/s't' \in (ST)^{-1}A$, *Let $f : A \to B$ be a homomorphism of rings and let S be a multiplicatively closed subset of A. Let $T = f(S)$. Show that $S^{-1}B$ and $T^{-1}B$ are isomorphic as $S^{-1}A$-modules.*

As a homomorphic image of a multiplicative submonoid, T is a multiplicative submonoid of B. Now $g = \mathrm{id}_B \times f$ is a surjection $B \times S \twoheadrightarrow B \times T$, and we will show it induces a bijection of equivalence classes $S^{-1}B \longleftrightarrow T^{-1}B$. The action of $S \subseteq A$ on B, by definition is $s \cdot b = f(s)b$, so the equivalence relation $\equiv_S$ on $B \times S$ is defined by $(b, s) \equiv_S (b', s') :\iff \exists s'' \in S\ (f(s''s)'b = f(s''s)b')$ this is the same equation that holds just if $(b, f(s)) \equiv_T (b', f(s'))$ in $B \times T$. Thus two elements of $B \times S$ define the same element of $S^{-1}B$ just if their g-images define the same element of $T^{-1}B$, so g induces a bijection $\phi \colon S^{-1}B \to T^{-1}B$. Since f is a homomorphism, it follows easily that ϕ is also a homomorphism of rings. Finally, if $a/s \in S^{-1}A$ and $b/s' \in S^{-1}B$, we have $\phi\left(\frac{a}{s}\frac{b}{s'}\right) = \phi\left(\frac{f(a)b}{ss'}\right) = \frac{f(a)b}{f(s)f(s')} = \frac{a}{s}\frac{b}{f(s')} = \frac{a}{s}\phi\left(\frac{b}{s'}\right)$, so ϕ is a $S^{-1}A$-module isomorphism.

Let A be a ring. Suppose that, for each prime ideal $\mathfrak{p}$, the local ring $A_\mathfrak{p}$ has no nilpotent element $\neq 0$. Show that A has no nilpotent element $\neq 0$. If each $A_\mathfrak{p}$ is an integral domain, is A necessarily an integral domain?

By (3.12), we have $\mathfrak{N}(A_\mathfrak{p}) = \mathfrak{N}(A)_\mathfrak{p}$ for each prime $\mathfrak{p}$, where $\mathfrak{N}(A)$ is the nilradical of A. By (3.8), this means $\mathfrak{N}(A) = 0$.

It is possible for a ring with zero-divisors to have all localizations at primes integral domains, for suppose $A = \prod_{j=1}^n k_j$ is a product of $n \geq 2$ fields; it is not an integral domain, but we shall show its localizations at primes are. By [1.22], the only prime ideals of A are $\mathfrak{p}_j = 0k_j \times \prod_{i \neq j} k_i$; their complements are $S_j = k_j^\times \times \prod_{i \neq j} k_i$ Now each inserted k_j is naturally an A-module, and A is a direct sum of these modules. By (3.4.i), localization distributes over finite direct sums of A-modules. Now $S_j^{-1}k_j \cong k_j$, while for $i \neq j$ we have $0 \in S_j \cdot k_i$, so by [3.1], $S_j^{-1}k_i = 0$. Thus all localizations $A_{\mathfrak{p}_j} \cong k_j$ at primes are fields, and a fortiori integral domains.

Let A be a ring $\neq 0$ and let Σ be the set of all multiplicatively closed subsets S of A such that $0 \notin S$. Show that Σ has maximal elements and that $S \in \Sigma$ is maximal if and only if $A \backslash S$ is a minimal prime ideal of A.

Certainly $\{1\} \in \Sigma$, so Σ is non-empty. To find maximal elements of Σ, we apply Zorn's Lemma. Let $(S_\mathfrak{a})_{\mathfrak{a} \in I}$ be a totally ordered chain in Σ; we claim its union S is an upper bound. Surely $0 \notin S$ since 0 is in no $S_\mathfrak{a}$, and if two elements $s, t \in S$ are given, they belong to some S_α and S_β, respectively. If $\gamma = \max\{\alpha, \beta\}$, then we have both $s, t \in S_\gamma$, so $st \in S_\gamma \subseteq S$, and thus $S \in \Sigma$ is an upper bound for the chain.

Assume $\mathfrak{p}$ is a prime ideal, and let $S = A \backslash \mathfrak{p}$. Then by the definition of being prime, $a, b \in S = A \backslash \mathfrak{p}$ implies $ab \in S$, so S is multiplicatively closed. Conversely, if the complement of a multiplicative submonoid is an ideal, it is prime. Since $0 \in \mathfrak{p}$, we don't have 0 in S, so $S \in \Sigma$.

Let $S \in \Sigma$ be maximal, and $\mathfrak{p} = A \backslash S$. Note that the smallest multiplicative submonoid containing $a \in A$ and S is $\{sa^n : s \in S,\ n > 0\}$. If $a \in \mathfrak{p}$, this monoid is strictly larger than S, and so by maximality of $S \in \Sigma$, contains zero. Thus $a \in \mathfrak{p}$ just if there are $n > 0$ and $s \in S$ with $sa^n = 0$. Suppose $a, b \in \mathfrak{p}$, and let $m, n > 0$ and $s, t \in S$ such that $sa^m = tb^n = 0$. If $p = m + n - 1$, then a^m or b^n divides each term of $(a - b)^p$ so $st(a - b)^p = 0$, and $a - b \in \mathfrak{p}$. Thus $\mathfrak{p}$ is an additive subgroup of A. If $x \in A$ is any other element, then $s(ax)^m = (sa^m)x^m = 0x^m = 0$, so $ax \in \mathfrak{p}$ as well. Thus $\mathfrak{p}$ is an ideal. If $\mathfrak{q} \subsetneq \mathfrak{p}$ was a smaller prime ideal, then $A \backslash \mathfrak{q}$ would be an element of Σ strictly containing S, which we assumed is impossible, so $\mathfrak{p}$ is minimal.

If, on the other hand $\mathfrak{p}$ is a minimal prime ideal, then $S = A \backslash \mathfrak{p}$ is an element of Σ. If $T \supseteq S$ is maximal, then $A \backslash T \subset \mathfrak{p}$ is a minimal prime ideal, hence equal to $\mathfrak{p} = A \backslash S$, and so $S = T$ is maximal.

A multiplicatively closed subset S of a ring A is said to be saturated *if*

$$xy \in S \iff x \in S \text{ and } y \in S.$$

we have the equations

$$\phi\left(\frac{a}{st} + \frac{a'}{s't'}\right) = \phi\left(\frac{as't' + a'st}{sts't'}\right) = \frac{\frac{at's'+a'ts}{ss'}}{\frac{tt'}{1}} = \frac{\frac{at'}{s} + \frac{a't}{s'}}{\frac{tt'}{1}} = \frac{\frac{a}{}s\frac{t'}{1} + \frac{a'}{s'}\frac{t}{1}}{\frac{t}{1}\frac{t'}{1}} = \frac{\frac{a}{}s}{\frac{t}{1}} + \frac{\frac{a'}{s'}}{\frac{t'}{1}} = \phi\left(\frac{a}{st}\right) + \phi\left(\frac{a'}{s't'}\right),$$

$$\phi\left(\frac{a}{st} \cdot \frac{a'}{s't'}\right) = \phi\left(\frac{aa'}{sts't'}\right) = \frac{\frac{aa}{ss'}}{\frac{tt'}{1}} = \frac{\frac{a}{s} \cdot \frac{a'}{s'}}{\frac{t}{1} \cdot \frac{t'}{1}} = \frac{\frac{a}{s}}{\frac{t}{1}} \cdot \frac{\frac{a'}{s'}}{\frac{t'}{1}} = \phi\left(\frac{a}{st}\right)\phi\left(\frac{a'}{s't'}\right).$$

Prove that
i) S is saturated $\iff$ $A\backslash S$ is a union of prime ideals.

Suppose a subset $S \subseteq A$ is such that $A\backslash S = \bigcup \mathfrak{p}_\alpha$ is a union of prime ideals. Then $1 \notin \mathfrak{p}_\alpha$ for all α, so $1 \in S$. Suppose $x, y \in S = A\backslash \bigcup \mathfrak{p}_\alpha$. Then for all $\mathfrak{p}_\alpha$ we have $x, y \notin \mathfrak{p}_\alpha$, so $xy \notin \mathfrak{p}_\alpha$, and thus $xy \in \bigcap (A\backslash \mathfrak{p}_\alpha) = A\backslash \bigcup \mathfrak{p}_\alpha = S$. Thus S is a multiplicative submonoid. On the other hand, if we have $x \notin S$, then there is some $\mathfrak{p}_\alpha \ni x$, and that being an ideal we have $xy \in \mathfrak{p}_\alpha \subseteq A\backslash S$, and symmetrically for y. Thus S is saturated.

Now suppose $S \subseteq A$ is saturated. To show the complement is a union of prime ideals, it suffices to manufacture, for any element $a \in A\backslash S$, a prime ideal $\mathfrak{p} \ni a$ disjoint from S. Note that if $a \in A\backslash S$, by saturation for all $b \in A$ we have $ab \notin S$, so that (a) is an ideal disjoint from S. The set Υ of ideals of A containing a and disjoint from S is then non-empty, and it is closed under increasing unions, so by Zorn's Lemma it contains a maximal element $\mathfrak{p}$. We will be done if we can show $\mathfrak{p}$ is prime, so suppose $x, y \notin \mathfrak{p}$. Then $(x) + \mathfrak{p}$ and $(y) + \mathfrak{p}$ are not in Υ, and so intersect S. If $s, t \in S$ are such that $s \in (x) + \mathfrak{p}$ and $t \in (y) + \mathfrak{p}$, then $st \in \big((x)+\mathfrak{p}\big)\big((y)+\mathfrak{p}\big) \subseteq (xy) + \mathfrak{p}$, so $xy \notin \mathfrak{p}$. Thus $\mathfrak{p}$ is prime.

ii) If S is any multiplicatively closed subset of A, there is a unique smallest saturated multiplicatively closed subset $\overline{S}$ containing S, and that $\overline{S}$ is the complement in A of the union of the prime ideals which do not meet S. ($\overline{S}$ is called the saturation *of S.)*

Let $\overline{S}$ be the complement of the union of primes $\mathfrak{p}$ not meeting S: $\overline{S} := A\backslash \bigcup \{\mathfrak{p} \in \operatorname{Spec}(A) : S \cap \mathfrak{p} = \varnothing\}$. Then $\overline{S}$ is saturated, by i), and contains S, since $A\backslash \overline{S} \subseteq A\backslash S$. Moreover, any saturated set containing S is the complement of a union of primes not meeting S, and since $\overline{S}$ is the complement of the largest such union, it is the smallest saturated set containing S.

If $S = 1 + \mathfrak{a}$, find $\overline{S}$.

A prime $\mathfrak{p}$ meets S just if we have $a \in \mathfrak{a}$ and $x \in \mathfrak{p}$ such that $x = 1 + a$, or $1 = a - x$, so that $(1) = \mathfrak{a} + \mathfrak{p}$. Thus the union in $A\backslash \overline{S}$ is over all prime ideals *not* coprime to $\mathfrak{a}$. In particular, for every such $\mathfrak{p}$, there is a maximal ideal $\mathfrak{m} \supseteq \mathfrak{a} + \mathfrak{p}$. Since every maximal ideal is prime and every prime ideal is contained in a maximal ideal, it suffices to take the union of *maximal* ideals *containing* $\mathfrak{a}$. Thus $\overline{S} = A\backslash \bigcup \{\mathfrak{m} \in \operatorname{Max}(A) : \mathfrak{a} \subseteq \mathfrak{m}\}$.

Let S, T be multiplicatively closed subsets of A, such that $S \subseteq T$. Let $\phi \colon S^{-1}A \to T^{-1}A$ be the homomorphism which maps each $a/s \in S^{-1}A$ to a/s considered as an element of $T^{-1}A$. Show that the following statements are equivalent:
i) ϕ is bijective.
ii) For each $t \in T$, $t/1$ is a unit in $S^{-1}A$.
iii) For each $t \in T$ there exists $x \in A$ such that $xt \in S$.
iv) T is contained in the saturation of S (Exercise 7).
v) Every prime ideal which meets T also meets S.

Note that $S \subseteq T \implies ST = T$ since T is multiplicatively closed. Now use the unique homomorphism $\rho_S^T \colon S^{-1}A \to T^{-1}A$, defined in the proof of [3.3], such that $\rho_S^T \circ \phi_S = \phi_T$. (3.1) shows $\rho_S^T(a/s) = \phi_T(a)\phi_T(s)^{-1} = a/s \in T^{-1}A$.

i) $\implies$ ii): If ρ_S^T is bijective, it is an isomorphism, so since $\rho_S^T(t/1) = t/1 \in T^{-1}A$ is a unit (inverse $1/t$), $t/1 \in S^{-1}A$ is also a unit.

ii) $\implies$ iii): If $t/1$ is a unit in $S^{-1}A$, then there is $x/s \in S^{-1}A$ such that $tx/1s = 1/1$, which by definition means there is $s' \in S$ such that $s'tx1 = s's1$ in A. Then $(s'x)t \in S$.

iii) $\implies$ i): Suppose $\rho_S^T(a/s) = 0/1$ in $T^{-1}A$. Then there is $t \in T$ such that $ta = 0$. If $x \in A$ is such that $xt \in S$, then $(xt)a = 0$ shows that $a/s = 0/1$ in $S^{-1}A$. Now let $a/t \in T^{-1}A$ be arbitrary, and let $x \in A$ be such that $xt \in S$. Then $a/t = xa/xt = \rho_S^T(xa/xt)$ is the image of an element of $S^{-1}A$.

iii) $\implies$ iv): $\overline{S}$ is saturated, so if for each $t \in T$ there is $x \in A$ such that $xt \in S \subseteq \overline{S}$, then by definition we have $xt \in \overline{S}$, so in particular $T \subseteq \overline{S}$.

iv) $\implies$ iii): Write $S' = \{a \in A : \exists x \in A\ (ax \in S)\}$, so that by definition We claim $S' = \overline{S}$ is the saturation of S. Surely $S \subseteq S' \subseteq \overline{S}$, since if $s \in S$ then $s \cdot 1 \in S$, and since if $ax \in \overline{S}$ then $ax \in \overline{S}$. To show the other inclusion it suffices to show S' is also saturated. Clearly, if $ab \in S'$, then there exist $xy \in A$ such that $ax, by \in S$, and then $ab \cdot xy = ax \cdot by \in S$, so $ab \in S'$. Supposing on the other hand that $a \notin S'$, then there is no $x \in A$ such that $ax \in S$, and certainly for all $b, y \in A$ we have $aby \notin S$, so $ab \notin S'$; and symmetrically if $b \notin S'$. Thus $S' = \overline{S}$ is saturated.

By definition $t \in S' \iff \exists x \in A\ (xt \in S)$.

iv) $\iff$ v):

$$
\begin{aligned}
T \subseteq \overline{S} \iff \overline{T} \subseteq \overline{\overline{S}} = \overline{S} \iff \bigcup\{\text{primes not meeting } S\} = A \backslash \overline{S} \subseteq A \backslash \overline{T} = \bigcup\{\text{primes not meeting } T\} \\
\iff \{\text{primes not meeting } S\} \subseteq \{\text{primes not meeting } T\} \\
\iff \{\text{primes meeting } T\} \subseteq \{\text{primes meeting } S\}.
\end{aligned}
$$

The set S_0 of all non-zero-divisors in A is a saturated multiplicatively closed subset of A. Hence the set D of zero-divisors in A is a union of prime ideals (see Chapter 1, Exercise 14). Show that every minimal prime ideal of A is contained in D.

If $1 = 0$, then S_0 should probably be considered empty, so henceforward let's assume not. Then $1 \in S_0$. If $x, y \in S_0$, then $xy \neq 0$, and for all $a \in A$ we have $a(xy) = (ax)y \neq 0$, so $xy \in S_0$. Thus S_0 is a multiplicative submonoid. Now suppose $x \in D$, say with $ax = 0$. For any $y \in A$ we then have $axy = 0$, so $xy \in D$; thus S_0 is saturated.

Recall from [3.6] that Σ is the collection of multiplicative submonoids S of A not containing 0. We claim that S_0 is contained in every maximal element $S \in \Sigma$. Indeed, if we did not have $S_0 \subseteq S$, then the product $S_0 S$ would strictly contain S, and thus contain $s_0 s = 0$, for some $s_0 \in S_0$ and $s \in S$, contradicting the defining assumption $S_0 \cap D = \varnothing$. Now by [3.6] the maximal elements of Σ are of the form $A \backslash \mathfrak{p}$ for $\mathfrak{p}$ a minimal prime of A, so we have $A \backslash D \subseteq A \backslash \mathfrak{p}$, or $\mathfrak{p} \subseteq D$, for all minimal primes $\mathfrak{p}$.

The ring $S_0^{-1}A$ is called the total ring of fractions *of A. Prove that*

i) S_0 is the largest multiplicatively closed subset of A for which the homomorphism $A \to S_0^{-1}A$ is injective.

$a \mapsto a/1 = 0/1$ in $S^{-1}A$ implies there is some $s \in S$ such that $sa \cdot 1 = 0 \cdot 1 = 0$ in A. This cannot happen if $S \subseteq S_0$, but can happen for any S strictly larger than S, since such will contain a zero-divisor s.

ii) Every element in $S_0^{-1}A$ is either a zero-divisor or a unit.

Let $a/s \in S_0^{-1}A$. If a/s is a zero-divisor, there is $b/t \in S_0^{-1}A$ such that $ab/st = 0/1$, so there exists $u \in S_0$ such that $uab = 0st = 0$ in A, and $ab = 0$, then, since u is not a zero-divisor; thus a is a zero-divisor in A. Thus if $a/s \in S_0^{-1}A$ is not a zero-divisor, then $a \in S_0$, so $s/a \in S_0^{-1}A$ is an inverse to a/s, which is then a unit.

iii) Every ring in which every non-unit is a zero-divisor is equal to its total ring of fractions (i.e., $A \to S_0^{-1}A$ is bijective).

If $S = \{1\}$ we obviously have $A \cong S^{-1}A$, and the inclusion $\{1\} \hookrightarrow S_0$ induces the homomorphism $\phi\colon A \to S_0^{-1}A$ as in [3.8]. This map is bijective just if, by condition ii), for each $s \in S_0$, $s/1$ is a unit in $S_0^{-1}A$. But each $s \in S_0$ has an inverse s^{-1} in A by assumption, and then $s^{-1}/1$ is an inverse of $s/1$ in $S_0^{-1}A$.

Let A be a ring.

i) If A is absolutely flat (Chapter 2, Exercise 27) and S is any multiplicatively closed subset of A, then $S^{-1}A$ is absolutely flat.

Let M be an $S^{-1}A$-module, and write $M|_A$ for M viewed as an A-module by restriction of scalars along the canonical map $A \to S^{-1}A$. We can then take $S^{-1}(M|_A)$, allowing division by elements of S again, and we want to show the composition of natural maps $\psi\colon M \to M|_A \to S^{-1}(M|_A)$ taking $m \mapsto m \mapsto m/1$ gives an $S^{-1}A$-module isomorphism. For surjectivity, let m/s be any element of $S^{-1}(M|_A)$. In M, the scalar product $m' = \frac{1}{s}m$ is defined, and we have $sm' = m$ in the module M. Since $s \in A$, we also have $sm' = m$ in $M|_A$. But then, by definition $m'/1 = m/s$ in $S^{-1}M$, so ψ is surjective. For injectivity, suppose $\psi(m) = m/1 = 0/1$ in $S^{-1}(M|_A)$. Then there is $s \in S$ such that $sm = 0$ in $M|_A$. But then $sm = 0$ in M, so $0 = \frac{1}{s}sm = m$. Thus ψ is injective. That ψ preserves the $S^{-1}A$-module structure is seen as follows. All homomorphisms are A-linear. If we take $m \in M$ and apply $1/s$ to get $m' = \frac{1}{s}m$, then we have $sm' = m$ in $M|_A$, since $s \in A$, and thus $s(m'/1) = s\psi(m') = m$ in $S^{-1}(M|_A)$. But we also have $s\frac{m}{s} = m$ in $S^{-1}(M|_A)$, so $s\left(\frac{m'}{1} - \frac{m}{s}\right) = 0 \in S^{-1}(M|_A)$, and multiplying on the left by $1/s$ we see $m'/1 = m/s$. Thus $\psi\left(\frac{1}{s}m\right) = \frac{1}{s}\psi(m)$, so ψ is $S^{-1}A$-linear.

To show $S^{-1}A$ is absolutely flat, now, let M be an $S^{-1}A$ module and $\phi\colon N' \rightarrowtail N$ an injective $S^{-1}A$-module homomorphism. We want $\mathrm{id}_M \otimes \phi\colon M \otimes_{S^{-1}A} N' \rightarrowtail M \otimes_{S^{-1}A} N$ to be injective. Note that $M|_A \otimes_A N'|_A \to M|_A \otimes_A N|_A$ is injective since all A-modules are flat. Since localization is exact, we also have $S^{-1}(M|_A \otimes_A N'|_A) \to S^{-1}(M|_A \otimes_A N'|_A)$ injective. But by (3.7), this is equivalent to an injective $S^{-1}A$-module homomorphism $S^{-1}(M|_A) \otimes_{S^{-1}A} S^{-1}(N'|_A) \rightarrowtail S^{-1}(M|_A) \otimes_{S^{-1}A} S^{-1}(N|_A)$, and we have shown that this is the same as $\mathrm{id}_M \otimes \phi\colon M \otimes_{S^{-1}A} N' \rightarrowtail M \otimes_{S^{-1}A} N$.

ii) A is absolutely flat $\iff$ $A_\mathfrak{m}$ is a field for each maximal ideal $\mathfrak{m}$.

If A is absolutely flat, then by i) each $A_\mathfrak{m}$ is absolutely flat. But then by [2.28], $A_\mathfrak{m}$, being local, is a field.

Now assume each localization $A_\mathfrak{m}$ is a field, and let M be an A-module. The localization $M_\mathfrak{m}$ is an $A_\mathfrak{m}$-module, and since $A_\mathfrak{m}$ is a field, it is a *free* $A_\mathfrak{m}$-module. But free modules are flat, by [2.4] (sums of flat modules are flat, and vice versa), and the absorption law (2.14.iv). Thus $M_\mathfrak{m}$ is a flat $A_\mathfrak{m}$-module for each $\mathfrak{m}$. By (3.10), M is a flat A-module.

Let A be a ring. Prove that the following are equivalent:
i) $A/\mathfrak{N}$ is absolutely flat ($\mathfrak{N}$ being the nilradical of A).
ii) Every prime ideal of A is maximal.
iii) Spec(A) *is a T_1-space (i.e., every subset consisting of a single point is closed).*
iv) Spec(A) *is Hausdorff.*

i) $\Longrightarrow$ iv): Let $A/\mathfrak{N}$ be absolutely flat and $X = \operatorname{Spec}(A/\mathfrak{N})$. Let $x \neq y \in X$ be two distinct points. We find them disjoint basic open neighborhoods (defined in [1.17]) X_e, X_f. Since $\mathfrak{p}_x, \mathfrak{p}_y$ are distinct maximal ideals, we have $\mathfrak{p}_x + \mathfrak{p}_y = (1)$, so there are elements $a \in \mathfrak{p}_x$ and $b \in \mathfrak{p}_y$ with $(a)+(b) = (1)$. By [2.27.ii], there are idempotents e generating (a) and g generating (b), so that $(e, g) = (1)$. Let $f = g(1-e)$. Then $ef = 0$, while $g = eg + f \in (e, f)$, so $(e, f) = (1)$. Since $e \in \mathfrak{p}_x$ and $\mathfrak{p}_x \neq (1)$, we have $x \in X_f$, and similarly $y \in X_e$. But by [1.17.i,ii] we have $X_e \cap X_f = X_{ef} = X_0 = \varnothing$. Also $X_e \cup X_f = V(e) \cap V(f) = V\big((e)+(f)\big) = V(1) = \varnothing$. Now Spec$(A)$ is homeomorphic to X by [1.21.iv], and so also Hausdorff.

iv) $\Longrightarrow$ iii): Fix $x \in X$. For each $y \neq x$ we have a U_y containing y but not x. Then $\{x\} = X \setminus \bigcup_{y \neq x} U_y$ is closed.

iii) $\iff$ ii): By [1.18.i], $\{x\}$ is closed just if $\mathfrak{p}_x$ is maximal. Thus all singletons are closed just if all primes are maximal.

ii) $\iff$ i): All primes of A are maximal
$$\begin{aligned}
&\overset{(1.7)}{\iff} \forall \mathfrak{m} \in \operatorname{Max}(A), \text{ no prime ideal of } A \text{ is strictly between } \mathfrak{m} \text{ and } \mathfrak{N}\\
&\overset{(1.1)}{\iff} \forall \mathfrak{m} \in \operatorname{Max}(A), \text{ the only prime of } A/\mathfrak{N} \text{ contained in } \mathfrak{m}/\mathfrak{N} \text{ is } (0)\\
&\overset{(3.11.iv)}{\iff} \forall \mathfrak{m} \in \operatorname{Max}(A), \text{ the only prime ideal of } (A/\mathfrak{N})_\mathfrak{m} \text{ is } (0)\\
&\iff \forall \mathfrak{m} \in \operatorname{Max}(A), (A/\mathfrak{N})_\mathfrak{m} \text{ is a field}\\
&\overset{[3.10]}{\iff} A/\mathfrak{N} \text{ is absolutely flat.}
\end{aligned}$$

If these conditions are satisfied, show that Spec(A) *is compact and totally disconnected (i.e., the only connected subsets of* Spec(A) *are those consisting of a single point).*

We already showed Spec(A) was compact in [1.17]. In the proof that i) $\Longrightarrow$ iv) above, we found, for any two distinct points x, y, disjoint open neighborhoods X_f, X_e whose union is the entire space. Any subset $S \subseteq \operatorname{Spec}(A)$ containing x, y is then disconnected by $S \cap X_f$ and $S \cap X_e$, so Spec(A) is totally disconnected.

Let A be an integral domain and M an A-module. An element $x \in M$ is a torsion element *of M if* $\operatorname{Ann}(x) \neq 0$*, that is if x is killed by some non-zero element of A. Show that the torsion elements of M form a submodule of M. This submodule is called the* torsion submodule *and is denoted by $T(M)$.*

Let $x, y \in T(M)$ and $c \in A$. Then there are $a, b \neq 0$ in A such that $ax = by = 0$. Since A is an integral domain, $ab \neq 0$ and we have $ab(x+y) = b0 + a0 = 0$, so $x + y \in T(M)$. Also $a(cx) = c0 = 0$, so $cx \in T(M)$.

If $T(M) = 0$, the module M is said to be torsion-free. Show that
i) If M is any A-module, then $M/T(M)$ is torsion-free.

Let $\bar{x} \in M/T(M)$ and suppose $a \in A \setminus \{0\}$ is such that $a\bar{x} = \bar{0}$. Then any representative x of $\bar{x}$ in M is such that $ax \in T(M)$. But then there is $b \neq 0$ such that $bax = 0$ in M. Since $ba \neq 0$, we see $x \in T(M)$, so $\bar{x} = \bar{0}$.

ii) If $f\colon M \to N$ is a module homomorphism, then $f\big(T(M)\big) \subseteq T(N)$.

Let $x \in T(M)$ and $0 \neq a \in A$ such that $ax = 0$. Then $0 = f(ax) = af(x)$, so $f(x) \in T(N)$.

iii) If $0 \to M' \to M \to M''$ is an exact sequence, then the sequence $0 \to T(M') \to T(M) \to T(M'')$ is exact.

Write $M' \xrightarrow{f} M' \xrightarrow{g} M''$. $T(f)$ is injective because it is a restriction of the injective map f. $T(g) \circ T(f)$ is zero because it is a restriction of the zero map $g \circ f$. If $x \in T(M) \cap \ker(g)$, then it is in $\operatorname{im}(f)$, so there is $y \in M'$ such that $x = f(y)$. If $0 \neq a \in A$ is such that $ax = 0$, then $f(ay) = 0$; as f is injective, $ay = 0$, so $y \in T(M')$.

iv) If M is any A-module, then $T(M)$ is the kernel of the mapping $x \mapsto 1 \otimes x$ of M into $K \otimes_A M$, where K is the field of fractions of A.

Take $S = A\backslash\{0\}$ and use (3.5), which gives an isomorphism $K \otimes_A M \xrightarrow{\sim} S^{-1}M$ taking $(a/x) \otimes m \mapsto am/x$. We then have $1 \otimes m \mapsto m/1 = 0$ in $S^{-1}M$ just if ([3.1]) there is $x \in S$ such that $xm = 0$.[2]

Let S be a multiplicatively closed subset of an integral domain A. In the notation of Exercise 12, show that $T(S^{-1}M) = S^{-1}(TM)$.

Let $x \in T(M)$ and $0 \neq a \in \mathrm{Ann}(x)$. Then for all $s \in S$ we have $a(x/s) = ax/s = 0$ in $S^{-1}M$, so $S^{-1}(T(M)) \subseteq T(S^{-1}M)$. Conversely, suppose $x/s \in T(S^{-1}M)$. Then there is a nonzero $a/t \in S^{-1}A$ such that $ax/st = 0/1$, so there is $u \in S$ such that $uax = 0$. But $ua \neq 0$ since A is an integral domain, so $x \in T(M)$ and $x/s \in S^{-1}(T(M))$. Thus $T(S^{-1}M) = S^{-1}(T(M))$

Deduce that the following are equivalent:
i) M is torsion-free.
ii) $M_{\mathfrak{p}}$ is torsion-free for all prime ideals $\mathfrak{p}$.
iii) $M_{\mathfrak{m}}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

For each $a \in A$, the map $l_a \colon x \mapsto ax$ is an A-module homomorphism $M \to M$; it induces $x/s \mapsto ax/s$ in each $M_{\mathfrak{p}}$ for $\mathfrak{p}$ a prime. By (3.9), l_a is injective just if each localization $(l_a)_{\mathfrak{m}}$ for $\mathfrak{m}$ maximal (or just prime) is injective. By the above, this is the same as demanding $l_{a/s}$ is injective for all $s \in S$. But a module is torsion-free just if all l_a (and friends) are injective, for $a \neq 0$.

Let M be an A-module and $\mathfrak{a}$ an ideal of A. Suppose that $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m} \supseteq \mathfrak{a}$. Prove that $M = \mathfrak{a}M$.

By (1.1), there is a bijective correspondence between maximal ideals $\mathfrak{m} \supseteq \mathfrak{a}$ and maximal ideals $\mathfrak{m}'$ of $A/\mathfrak{a}$. Now if $M_{\mathfrak{m}} = 0$, then

$$0 = M_{\mathfrak{m}}/(\mathfrak{a}M)_{\mathfrak{m}} \overset{(3.4.\text{iii})}{\cong} (M/\mathfrak{a}M)_{\mathfrak{m}} \overset{(3.5)}{\cong} A_{\mathfrak{m}} \otimes_A M/\mathfrak{a}M$$

as $A_{\mathfrak{m}}$-modules. For any $x \in \mathfrak{a}$, any $s \in A\backslash\mathfrak{m}$, and any $\bar{m} \in M/\mathfrak{a}M$ we then have $(x/s) \otimes \bar{m} = (1/s) \otimes x\bar{m} = 0$ in $A_{\mathfrak{m}} \otimes_A M/\mathfrak{a}M$, so this $A/\mathfrak{a}$-module is naturally isomorphic to $(A/\mathfrak{a})_{\mathfrak{m}} \otimes_{A/\mathfrak{a}} M/\mathfrak{a}M = 0$. Now $(M/\mathfrak{a}M)_{\mathfrak{m}/\mathfrak{a}} \cong (A/\mathfrak{a})_{\mathfrak{m}/\mathfrak{a}} \otimes_{A/\mathfrak{a}} M/\mathfrak{a}M$ by (3.5), and [3.4] shows $(A/\mathfrak{a})_{\mathfrak{m}}$ and $(A/\mathfrak{a})_{\mathfrak{m}/\mathfrak{a}}$ are isomorphic, so we finally see each localization of $M/\mathfrak{a}M$ at a maximal ideal of $A/\mathfrak{a}$ is zero. Then (3.8) says that $M/\mathfrak{a}M = 0$. Thus $M = \mathfrak{a}M$.

Let A be a ring, and let F be the A-module A^n. Show that every set of n generators of F is a basis of F.

Let e_i be the standard basis of A^n and x_i our generators; $\phi\colon e_i \mapsto x_i$ is then a surjective homomorphism, and $\langle x_i \rangle$ will be a basis just if ϕ is also injective. By (3.9), ϕ is injective just if each $\phi_{\mathfrak{m}}$ is injective for $\mathfrak{m} \lhd A$ maximal. Thus without loss of generality we may assume A is local. Let $N = \ker(\phi)$, so we have an exact sequence $0 \to N \to F \to F \to 0$. Tensoring with the residue field $k = A/\mathfrak{m}$ gives an exact sequence $k \otimes N \to k \otimes F \to k \otimes F \to 0$. Now (2.14.iii,iv) give $k \otimes F = k \otimes A^{\oplus n} \cong (k \otimes A)^{\oplus n} \cong k^n$. The map $k^n \to k^n$ is a surjection of vector spaces of the same dimension, hence an isomorphism, and thus $k \otimes N = 0$. Now [2.12] shows that N is finitely generated, and [2.2] gives $k \otimes N = (A/\mathfrak{m}) \otimes N \cong N/\mathfrak{m}N = 0$. Thus $N = \mathfrak{m}N$, and Nakayama's Lemma (2.6) gives $N = 0$ ($\mathfrak{m}$ being the Jacobson radical of the local ring A). Thus ϕ is injective.

Deduce that every set of generators of F has at least n elements.

Supposing $m < n$ elements $x_1, \ldots, x_m$ generate F, then expanding this set at random by nonzero elements $y_1, \ldots, y_{n-m}$, we would have a set of n generators. By what we've proven above, this would be a basis. But since the x_i are generators, we could write $y_1 = \sum_{i=1}^{m} a_i x_i$ with not all $a_i = 0$, contradicting this set being a basis.

We also showed this in [2.11]. (Surjections $A^m \twoheadrightarrow A^n$ only occur for $m \geq n$.)

[2] Alternately, we may follow the book's hint. Suppose $x \in T(M)$, and $0 \neq a \in A$ is such that $ax = 0$. Then in $K \otimes_A M$ we have the equalities $1 \otimes x = \frac{a}{a} \otimes x = \frac{1}{a} \otimes ax = \frac{1}{a} \otimes 0 = 0$.

For the other inclusion, we write $K \otimes_A M$ as a direct limit. For each $x \in S = A\backslash\{0\}$, we have a cyclic A-module $A_x := Ax \subseteq K$, and given $x, y \in S$, we have natural inclusions $A_x \hookrightarrow A_{x,y}$ and $A_y \hookrightarrow A_{xy}$, given by $a/x \mapsto ay/xy$ and $a/y \mapsto ax/xy$, so these modules A_x form a direct system, with an inclusion $A_x \hookrightarrow A_y$ just when $x \mid y$. Since every element $\xi \in K$ can be written as a/x for some $a \in A$ and $x \in S$, by [2.17], $K = \varinjlim Ax$.

By [2.20], $K \otimes_A M \cong \varinjlim (Ax \otimes_A M)$. Now by [2.15], every element $1 \otimes m$ representing 0 is already equal to zero at some finite stage; that is, there is some $x \in S$ such that $1 \otimes m = 0$ in $Ax \otimes_A M$. But as an A-module Ax is isomorphic to A under $a/x \mapsto a$, so we have a composite isomorphism $Ax \otimes_A M \to A \otimes_A M \to M$ taking $(a/x) \otimes m \mapsto a \otimes m \mapsto am$. Since $0 = 1 \otimes m = (x/x) \otimes m \mapsto xm$ we then have $xm = 0$, so $x \in T(M)$.

Let B be a flat A-algebra. Then the following conditions are equivalent:
i) $\mathfrak{a}^{ec} = \mathfrak{a}$ for all ideals $\mathfrak{a}$ of A.
ii) $\mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is surjective.
iii) For every maximal ideal $\mathfrak{m}$ of A we have $\mathfrak{m}^e \neq (1)$.
iv) If M is any non-zero A-module, then $M_B \neq 0$.
v) For every A-module M, the mapping $x \mapsto 1 \otimes x$ of M into M_B is injective.
B is said to be faithfully flat *over A.*

Write $f \colon A \to B$ for the map making B a flat A-algebra.

i) $\Longrightarrow$ ii) : Recall that $f^* \colon \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is given by $\mathfrak{q} \mapsto \mathfrak{q}^c$. Thus $f^*(\mathfrak{p}^e) = \mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$, so f^* is surjective.

ii) $\Longrightarrow$ iii): Let $\mathfrak{m} \in \mathrm{Max}(A)$. If $f^*(\mathfrak{n}) = \mathfrak{m}$, then we have $f(\mathfrak{m}) \subseteq \mathfrak{n}$, so $\mathfrak{m}^e = Bf(\mathfrak{m}) \subseteq \mathfrak{n}$. If $\mathfrak{m}^e = (1)$, then $f^*(\mathfrak{n}) = f^*\big((1)\big) = (1) \neq \mathfrak{m}$, so $\mathfrak{m}^e \neq (1)$.

iii) $\Longrightarrow$ iv): We use contraposition. Supposing iv) false, let $M \neq 0$ be an A-module such that $M_B = B \otimes_A M = 0$. Since B is flat, inclusions $M' \hookrightarrow M$ induce injections $M'_B \rightarrowtail M_B$, so $M'_B = 0$ for all submodules $M' \subseteq M$. In particular this is the case for all cyclic submodules Ax. Ax is isomorphic, as an A-module, to a quotient of A, say $A/\mathfrak{a}$. Now $0 = (Ax)_B \cong B \otimes_A A/\mathfrak{a} \cong B/\mathfrak{a}B = B/f(\mathfrak{a})B$, using [2.2] and the definition $a \cdot b = f(a)b$ of the A-module structure on B, so $\mathfrak{a}^e = f(\mathfrak{a})B = B$. If $\mathfrak{m} \supseteq \mathfrak{a}$ is a maximal ideal of A, then also $B = \mathfrak{m}^e$, so iii) doesn't hold.

iv) $\Longrightarrow$ v): We again use contraposition. Suppose v) is false, and let M be an A-module such that the canonical map to M_B isn't injective. Then there is a non-zero element $x \in M$ such that $1 \otimes x = 0$ in M_B. By flatness, the inclusion $Ax \hookrightarrow M$ induces an injection $(Ax)_B \rightarrowtail M_B$, but the image of this map is $B \otimes x = 0$, so $(Ax)_B = 0$ and iv) does not hold.

v) $\Longrightarrow$ i): We once again use contraposition. We always have $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, by (1.17.i), so suppose $\mathfrak{a} \lhd A$ is such that $\mathfrak{a} \subsetneq \mathfrak{a}^{ec}$. Then the submodule $\mathfrak{a}^{ec}/\mathfrak{a}$ of $M := A/\mathfrak{a}$ is nonzero. By [2.2], $M_B = B \otimes_A (A/\mathfrak{a}) \cong B/\mathfrak{a}B = B/\mathfrak{a}^e$, so the natural map $M \to M_B$ is essentially the map $A/\mathfrak{a} \to B/\mathfrak{a}^e$ induced by f, whose kernel is $f^{-1}(\mathfrak{a}^e)/\mathfrak{a} = \mathfrak{a}^{ec}/\mathfrak{a}$, which we have noted is not zero.

Let $A \xrightarrow{f} B \xrightarrow{g} C$ be ring homomorphisms. If $g \circ f$ is flat and g is faithfully flat, then f is flat.

Let $j \colon N \hookrightarrow M$ be an inclusion of A-modules. $g \circ f$ is flat, so $j_C \colon N_C \rightarrowtail M_C$ is injective. Now $M_C = C \otimes_A M \cong C \otimes_B B \otimes_A M \cong (M_B)_C$ by (2.14.iv) and (2.15), and similarly for N. Since g is faithfully flat, the canonical maps $i_N \colon N_B \to (N_B)_C$ and $i_M \colon M_B \to (M_B)_C$ are injective, and we have the commutative diagram at right. f_C is injective since $g \circ f$ is flat. If f_B wasn't an injection, $i_M \circ f_B$ would not be injective. But $i_M \circ f_B = f_C \circ i_N$ is a composition of injections.

$$\begin{tikzcd}
N_B \arrow[r, "f_B"] \arrow[d, tail, "i_N"'] & M_B \arrow[d, tail, "i_M"] \\
(N_B)_C \arrow[r, tail, "f_C"'] & (M_B)_C
\end{tikzcd}$$

Let $f : A \to B$ be a flat homomorphism of rings, let $\mathfrak{q}$ be a prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then $f^* \colon \mathrm{Spec}(B_\mathfrak{q}) \to \mathrm{Spec}(A_\mathfrak{p})$ is surjective.

Since for all $s \in S := A \backslash \mathfrak{p}$ we have $f(s) \notin \mathfrak{q}$, f induces a map $\tilde{f} \colon A_\mathfrak{p} \to B_\mathfrak{q}$ taking $a/s \mapsto f(a)/f(s)$. We also have an A-algebra $B_\mathfrak{p} = f(S)^{-1}B$, and since $f(S) \subseteq B \backslash \mathfrak{q} =: T$, [3.3] gives an isomorphism $B_\mathfrak{q} = T^{-1}B = U^{-1}(f(S)^{-1}B) = U^{-1}B_\mathfrak{p}$, where $U = \{t/1 \in B_\mathfrak{p} : t \in T\}$. Now $\tilde{f}$ evidently factors through this ring: $A_\mathfrak{p} \to B_\mathfrak{p} \to B_\mathfrak{q}$. Since f is flat, (3.10) says the map $A_\mathfrak{p} \to B_\mathfrak{p}$ is flat. Since $B_\mathfrak{q}$ is a localization of $B_\mathfrak{p}$, by (3.6) the map $B_\mathfrak{p} \to B_\mathfrak{q}$ is flat. Then [2.8.ii] shows that $B_\mathfrak{q}$ is flat as an $A_\mathfrak{p}$-module. Now if p/s is an element of the maximal ideal $\mathfrak{p}A_\mathfrak{p}$ of $A_\mathfrak{p}$, we have $\tilde{f}(p/s) = f(p)/f(s) \in f(\mathfrak{p})B_\mathfrak{q} \subseteq \mathfrak{q}B_\mathfrak{q}$, so it is not the case that $(\mathfrak{p}A_\mathfrak{p})^e = (1)$. Then by [3.16.iii], $B_\mathfrak{q}$ is faithfully flat over $A_\mathfrak{p}$ and the map $f^* \colon \mathrm{Spec}(B_\mathfrak{q}) \to \mathrm{Spec}(A_\mathfrak{p})$ is surjective

Let A be a ring, M an A-module. The support *of M is defined to be the set $\mathrm{Supp}(M)$ of prime ideals $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$. Prove the following results:*
i) $M \neq 0 \iff \mathrm{Supp}(M) \neq \varnothing$.

This follows from (3.8): $M = 0 \iff \forall \mathfrak{p} \in \mathrm{Spec}(A)\ (M_\mathfrak{p} = 0)$.

ii) $V(\mathfrak{a}) = \mathrm{Supp}(A/\mathfrak{a})$.

Let $\mathfrak{p} \in \mathrm{Spec}(A)$ and $S = A \backslash \mathfrak{p}$. By [3.8] and (3.4.iii), we have $(A/\mathfrak{a})_\mathfrak{p} \cong S^{-1}A/S^{-1}\mathfrak{a}$. This is non-zero just if $(1/1) = S^{-1}A \neq S^{-1}\mathfrak{a}$, so that $1/1 \neq a/s$ for any $a \in \mathfrak{a}$ and $s \in S$. By definition, this means there is no $t \in S$ such that $st = at \in \mathfrak{a} \cap S$. Redefining $s' = st$ and $a' = at$, without loss of generality $t' = 1$, so $(A/\mathfrak{a})_\mathfrak{p} \neq 0 \iff \mathfrak{a} \cap S = \varnothing$ But since $S = A \backslash \mathfrak{p}$, we have $\mathfrak{a} \cap S \neq \varnothing \iff \mathfrak{a} \subseteq \mathfrak{p} \iff \mathfrak{p} \in V(\mathfrak{a})$.

iii) If $0 \to M' \to M \to M'' \to 0$ *is an exact sequence, then* $\operatorname{Supp}(M) = \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$.

Let $\mathfrak{p} \in \operatorname{Spec}(A)$. By (3.3), localization gives an exact sequence $0 \to M'_{\mathfrak{p}} \to M_{\mathfrak{p}} \to M''_{\mathfrak{p}} \to 0$. If $\mathfrak{p} \in \operatorname{Supp}(M')$, then $M'_{\mathfrak{p}} \neq 0$ injects into $M_{\mathfrak{p}}$, so $\mathfrak{p} \in \operatorname{Supp}(M)$. If $\mathfrak{p} \in \operatorname{Supp}(M'')$, then $M_{\mathfrak{p}}$ surjects onto $M''_{\mathfrak{p}} \neq 0$, so $\mathfrak{p} \in \operatorname{Supp}(M)$. If $\mathfrak{p} \notin \operatorname{Supp}(M') \cup \operatorname{Supp}(M'')$, then our exact sequence reduces to $0 \to 0 \to M_{\mathfrak{p}} \to 0 \to 0$, so $M_{\mathfrak{p}} = 0$ and $\mathfrak{p} \notin \operatorname{Supp}(M)$.

iv) If $M = \sum M_i$, *then* $\operatorname{Supp}(M) = \bigcup \operatorname{Supp}(M_i)$.

The inclusions $M_i \hookrightarrow M$ give rise to injections $(M_i)_{\mathfrak{p}} \rightarrowtail M_{\mathfrak{p}}$ by (3.3). Thus if any $(M_i)_{\mathfrak{p}} \neq 0$ we have $M_{\mathfrak{p}} \neq 0$, so $\bigcup \operatorname{Supp}(M_i) \subseteq \operatorname{Supp}(M)$. On the other hand, we have a natural surjection $\bigoplus M_i \twoheadrightarrow \sum M_i = M$, and (see next paragraph) localization distributes over direct sums, so by exactness again we have a surjection $\bigoplus (M_i)_{\mathfrak{p}} \twoheadrightarrow M_{\mathfrak{p}}$. Thus if all $(M_i)_{\mathfrak{p}} = 0$, then $M_{\mathfrak{p}} = 0$.

To see localization distributes over direct sums, note

$$S^{-1}\Big(\bigoplus M_i\Big) \overset{(3.5)}{\cong} S^{-1}A \otimes_A \Big(\bigoplus M_i\Big) \overset{[2.20]}{\cong} \bigoplus (S^{-1}A \otimes M_i) \overset{(3.5)}{\cong} \bigoplus S^{-1}M_i. \tag{3.6}$$

Note that if we forgot tensor isn't left exact (which I did, for a while), we would think we had counterexamples to this. Consider $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Q}$ as $\mathbb{Z}$-modules. Now $\mathbb{Q}$ is generated over $\mathbb{Z}$ by the elements $\frac{1}{n}$, so it is a sum of the submodules $\frac{1}{n}\mathbb{Z}$. Thus the elements $z_n = 1 \otimes \frac{1}{n}$ generate $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Q}$ over $\mathbb{F}_p$. In fact all are zero, since the generator $z_n = p \otimes \frac{1}{pn} = 0$. We can view $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Q}$ as the direct limit of $M_n = \mathbb{F}_p \otimes_{\mathbb{Z}} \frac{1}{n}\mathbb{Z}$ along the maps $M_n \to M_{mn}$ induced by $\frac{1}{mn}\mathbb{Z} \hookrightarrow \frac{1}{n}\mathbb{Z}$, and this shows that the map $M_n \to M_{pn}$ is zero. Thus $\mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Q} = 0$ has empty support. Now the cyclic $\mathbb{F}_p$-modules M_n are all isomorphic to $\mathbb{F}_p$, for we have isomorphisms $M_n \cong \frac{1}{n}\mathbb{Z}/\frac{p}{n}\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$, which has support $\{(0)\}$. If tensor were left exact, the inclusion $\frac{1}{n}\mathbb{Z} \hookrightarrow \mathbb{Q}$ would induce an injection $M_n \rightarrowtail \mathbb{F}_p \otimes_{\mathbb{Z}} \mathbb{Q} = 0$, and we would have $\{(0)\} \subseteq \varnothing$, which is obviously false. In fact the induced map is $1 \otimes \frac{1}{n} \mapsto z_n = 0$.

v) If M *is finitely generated, then* $\operatorname{Supp}(M) = V(\operatorname{Ann}(M))$ *(and is therefore a closed subset of* $\operatorname{Spec}(A)$*).*

Let $x_1, \ldots, x_n$ be generators for M. Then Ax_i are cyclic modules, so there are $\mathfrak{a}_i \lhd A$ such that the maps $a \mapsto ax_i$ induce isomorphisms $A/\mathfrak{a}_i \xrightarrow{\sim} Ax_i$. Since $M = \sum_i Ax_i$, by iv) and i) of this exercise, and [1.15.iv],

$$\operatorname{Supp}(M) = \bigcup \operatorname{Supp}(Ax_i) = \bigcup \operatorname{Supp}(A/\mathfrak{a}_i) = \bigcup V(\mathfrak{a}_i) = V\Big(\bigcap \mathfrak{a}_i\Big).$$

Now $a \in A$ annihilates M just if for each i we have $ax_i = 0$, and this happens exactly when $a \in \mathfrak{a}_i$, so $\bigcap \mathfrak{a}_i = \operatorname{Ann}(M)$ and $\operatorname{Supp}(M) = V(\operatorname{Ann}(M))$.

vi) If M, N *are finitely generated, then* $\operatorname{Supp}(M \otimes_A N) = \operatorname{Supp}(M) \cap \operatorname{Supp}(N)$.

For any $\mathfrak{p} \in \operatorname{Spec}(A)$, (3.7) gives $(M \otimes_A N)_{\mathfrak{p}} = M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$. Now the localizations $M_{\mathfrak{p}}$ and $N_{\mathfrak{p}}$ are again finitely generated modules over the local ring $A_{\mathfrak{p}}$, so [2.3] shows the tensor product is non-zero if and only if both factors are nonzero. So $\mathfrak{p} \in \operatorname{Supp}(M \otimes_A N)$ just if $\mathfrak{p}$ is in both $\operatorname{Supp}(M)$ and $\operatorname{Supp}(N)$.

vii) If M *is finitely generated and* $\mathfrak{a}$ *is an ideal of* A, *then* $\operatorname{Supp}(M/\mathfrak{a}M) = V(\mathfrak{a} + \operatorname{Ann}(M))$*;*

$M/\mathfrak{a}M \cong A/\mathfrak{a} \otimes_A M$ by (3.5), so by iv) we have $\operatorname{Supp}(M/\mathfrak{a}M) = \operatorname{Supp}(A/\mathfrak{a}) \cap \operatorname{Supp}(M)$. By ii) and v) above, and [1.15.iii], this is $V(\mathfrak{a}) \cap V(\operatorname{Ann}(M)) = V(\mathfrak{a} \cup \operatorname{Ann}(M)) = V(\mathfrak{a} + \operatorname{Ann}(M))$.

viii) If $f : A \to B$ *is a ring homomorphism and* M *is a finitely generated* A*-module, then* $\operatorname{Supp}(B \otimes_A M) = f^{*-1}(\operatorname{Supp}(M))$.

Let $\mathfrak{q} \in \operatorname{Spec}(B)$, and $\mathfrak{p} = \mathfrak{q}^c$. We show $\mathfrak{q} \in \operatorname{Supp}(M_B) \iff \mathfrak{p} \in \operatorname{Supp}(M)$.

$$(B \otimes_A M)_{\mathfrak{q}} \overset{(3.5)}{\cong} B_{\mathfrak{q}} \otimes_A M \overset{(2.14.iv)}{\cong} (B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} A_{\mathfrak{p}}) \otimes_A M \underset{(3.5)}{\overset{(2.15)}{\cong}} B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}.$$

Now if $M_{\mathfrak{p}} = 0$, clearly $(M_B)_{\mathfrak{q}} = 0$. Thus we have the containment $\operatorname{Supp}(B \otimes_A M) \subseteq (f^*)^{-1}1(\operatorname{Supp}(M))$.

On the other hand, suppose $0 = (M_B)_{\mathfrak{q}} \cong B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$, and let $x_1, \ldots, x_n$ be generators of M over A. Then the equations $(1/1) \otimes (x_i/1) = 0$ hold in $B_{\mathfrak{q}} \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ By (2.13) there is a finitely generated $A_{\mathfrak{p}}$-submodule $N_i \subseteq B$ where already $(1/1) \otimes (x_i/1) = 0$. Let $N = \sum_{i=1}^{n} N_i \subseteq B$; then N is finitely generated, and $(1/1) \otimes (x/1) = 0$ in $N \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}}$ for all $x \in M_{\mathfrak{p}}$, so $N \otimes_{A_{\mathfrak{p}}} M_{\mathfrak{p}} = 0$. But then by [2.3] we have either $N = 0$ or $M_{\mathfrak{p}} = 0$, and we have $1/1 \in N$, so $M_{\mathfrak{p}} = 0$.

The $\subseteq$ containment holds for any module M, but the $\supseteq$ doesn't necessarily hold for non-finitely generated modules. Here is an obvious counterexample, thanks to Angelo Vistoli[3]: Take $f\colon A=\mathbb{Z}\twoheadrightarrow\mathbb{Z}/p\mathbb{Z}=B$, for $p>0$ a prime number, and $M=\mathbb{Q}$. Then $B\otimes_A M=0$ since $\bar{1}\otimes 1/1=\bar{1}\otimes\bar{p}/p=\bar{p}\otimes\frac{1}{p}=\bar{0}\otimes\frac{1}{p}=0$, and so $\operatorname{Supp}(M_B)=\operatorname{Supp}(0)=\varnothing$ by i). On the other hand, $\operatorname{Supp}(M)=\operatorname{Spec}(\mathbb{Z})$ since no nonzero element of $\mathbb{Z}$ annihilates an element of $\mathbb{Q}$.[4] Now the only nontrivial ideal of $B=\mathbb{Z}/p\mathbb{Z}$ is (0), and $(0)^c=f^{-1}\big((0)\big)=(p)$, so $(f^*)^{-1}(\operatorname{Spec}(\mathbb{Z}))=\{(0)\}\neq\varnothing$.

To see the delicacy of the assumption of finite generation, it is illuminating to look at a failed proof and see what goes wrong. First, suppose $M=Ax\cong A/\mathfrak{a}$ is cyclic. Then $M_B=B\otimes_A M\cong B/\mathfrak{a}B=B/\mathfrak{a}^e$ by [2.2] and the definition of the A-module structure on B. Thus $\operatorname{Supp}(M_B)=V(\operatorname{Ann}(B/\mathfrak{a}^e))=V(\mathfrak{a}^e)$ by v), while $\operatorname{Supp}(M)=V(\operatorname{Ann}(A/\mathfrak{a}))=V(\mathfrak{a})$. By (1.17.i) $\mathfrak{a}^e\subseteq\mathfrak{q}\implies\mathfrak{a}\subseteq\mathfrak{a}^{ec}\subseteq\mathfrak{q}^c=\mathfrak{p}$, while $\mathfrak{a}\subseteq\mathfrak{p}=\mathfrak{q}^c\implies\mathfrak{a}^e\subseteq\mathfrak{q}^{ce}\subseteq\mathfrak{q}$, so $\operatorname{Supp}(M_B)=(f^*)^{-1}(\operatorname{Supp}(M))$ for M cyclic. Now suppose M is generated over A by some x_i, so M_B is generated over B by the $1\otimes x_i$. Write $\mathfrak{a}_i=\operatorname{Ann}_A(x_i)$. Now, using the cyclic case at the line break,

$$\begin{aligned}\operatorname{Supp}(M_B)=\operatorname{Supp}\Big(\sum B(1\otimes x_i)\Big)&\overset{\text{iv)}}{=}\bigcup\operatorname{Supp}(B(1\otimes x_i))\overset{?}{=}\bigcup\operatorname{Supp}(B\otimes_A Ax_i)\\&=\bigcup(f^*)^{-1}(\operatorname{Supp}(Ax_i))=(f^*)^{-1}\Big(\bigcup\operatorname{Supp}(Ax_i)\Big)\overset{\text{iv)}}{=}(f^*)^{-1}(\operatorname{Supp}(M)).\end{aligned}$$

What goes wrong is the step labeled with a question mark, for tensor is not left exact! The map $B\otimes_A Ax_i\to B\otimes_A M$ induced by the inclusion $Ax_i\hookrightarrow M$ need not be injective, so the support of the submodule of M_B generated by $1\otimes x_i$ can easily be smaller than $\operatorname{Supp}(B\otimes_A Ax_i)$. This happens, for example, in our "counterexample" in iv), where $M=\mathbb{Q}$, $A=\mathbb{Z}$, and $B=\mathbb{F}_p$, using that $0=\mathbb{F}_p\cdot(1\otimes\frac{1}{n}\mathbb{Z})$ is not $\mathbb{F}_p\otimes_{\mathbb{Z}}\frac{1}{n}\mathbb{Z}\cong\mathbb{F}_p\otimes_{\mathbb{Z}}\mathbb{Z}\cong\mathbb{F}_p$:

$$\begin{aligned}\varnothing=\operatorname{Supp}_{\mathbb{F}_p}\Big(\sum\mathbb{F}_p\cdot(1\otimes 1/n)\Big)&\overset{\text{iv)}}{=}\bigcup\operatorname{Supp}_{\mathbb{F}_p}(\mathbb{F}_p\cdot(1\otimes 1/n))\subseteq\bigcup\operatorname{Supp}_{\mathbb{F}_p}(\mathbb{F}_p\otimes_{\mathbb{Z}}(1/n)\mathbb{Z})=\bigcup\operatorname{Supp}_{\mathbb{F}_p}(\mathbb{F}_p\otimes_{\mathbb{Z}}\mathbb{Z})\\&=\bigcup(f^*)^{-1}(\operatorname{Supp}_{\mathbb{Z}}(\mathbb{Z}))=(f^*)^{-1}(\{\operatorname{Spec}(\mathbb{Z})\})=(f^*)^{-1}(\{(p)\})=\{(0)\}.\end{aligned}$$

This point may not be that subtle, but it eluded me for longer than I care to admit.

Let $f:A\to B$ be a ring homomorphism, $f^*\colon\operatorname{Spec}(B)\to\operatorname{Spec}(A)$ the associated mapping. Show that

i) Every prime ideal of A is a contracted ideal $\iff$ f^* is surjective.

By definition, f^* is surjective if and only if for every $\mathfrak{p}\in\operatorname{Spec}(A)$ there is $\mathfrak{q}\in\operatorname{Spec}(B)$ such that $\mathfrak{p}=f^*(\mathfrak{q})=\mathfrak{q}^c$, meaning every prime ideal of A is a contracted ideal.

ii) Every prime ideal of B is an extended ideal $\implies$ f^* is injective.

Suppose $\mathfrak{q}_1=\mathfrak{a}_1^e$ and $\mathfrak{q}_2=\mathfrak{a}_2^e$ are prime ideals of B whose images under f^* are equal. That means, by the definition of f^*, that $\mathfrak{a}_1^{ec}=\mathfrak{q}_1^c=\mathfrak{q}_2^c=\mathfrak{a}_2^{ec}$. But then extending again, and using (1.17.ii), we get $\mathfrak{q}_1=\mathfrak{a}_1^e=\mathfrak{a}_1^{ece}=\mathfrak{a}_2^{ece}=\mathfrak{a}_2^e=\mathfrak{q}_2$.

Is the converse of ii) true?

No. Note that we always have $\mathfrak{q}^{ce}\subseteq\mathfrak{q}$, so the trick will be to sabotage all extensions of primes so that they are not themselves prime, and the containment is proper. Let A be a ring and consider the ring[5] $A[\epsilon]\coloneqq A[x]/(x^2)$. Since there is a quotient map $\pi\colon A[\epsilon]\twoheadrightarrow A$ with kernel (ϵ), each prime $\mathfrak{p}\lhd A$ gives rise to a distinct prime $\pi^{-1}(\mathfrak{p})$ of $A[\epsilon]$ containing (ϵ). Since $\epsilon^2=0$, all primes of $A[\epsilon]$ contain (ϵ), so these are all the primes of $A[\epsilon]$. We can write them as $\mathfrak{p}^+=\pi^{-1}(\mathfrak{p})=\mathfrak{p}A+(\epsilon)$. Now consider the inclusion $j:A\to A[\epsilon]$. Then for a prime $\mathfrak{p}\lhd A$ we have $\mathfrak{p}^e=\mathfrak{p}A[\epsilon]=\mathfrak{p}A+\mathfrak{p}\epsilon$. This ideal is not prime, since $A[\epsilon]/\mathfrak{p}^e\cong(A/\mathfrak{p})[\epsilon]$ is not a domain. The prime ideals $\mathfrak{p}^+$ properly contain $\mathfrak{p}^e$. Thus *no extended ideal $\mathfrak{p}^e$ is prime, and no prime ideal $\mathfrak{p}^+$ is extended.* On the other hand $j^*\colon\mathfrak{p}^+\mapsto\mathfrak{p}$ is a bijective function $\operatorname{Spec}(A[\epsilon])\longleftrightarrow\operatorname{Spec}(A)$.

[3] http://mathoverflow.net/questions/50406/extension-of-scalars-and-support-of-a-non-finitely-generated-module

[4] In fact $S^{-1}\mathbb{Q}\cong\mathbb{Q}$ for any $S=\mathbb{Z}\backslash\mathfrak{q}$, by the map $\phi\colon S^{-1}\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}\cong S^{-1}\mathbb{Q}\to\mathbb{Q}$ taking $\frac{n}{s}\otimes\frac{a}{b}\mapsto\frac{na}{bs}$. To see injectivity, note that in $S^{-1}\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Q}$ we have $\frac{n}{s}\otimes\frac{a}{b}=\frac{1}{s}\otimes\frac{na}{b}=\frac{1}{s}\otimes\frac{sna}{sb}=\frac{1}{1}\otimes\frac{na}{sb}$, so any sum of decomposable elements $\frac{n_i}{s_i}\otimes\frac{a_i}{b_i}$ can be written as $1\otimes z$, where $z=\sum_i\frac{n_ia_i}{s_ib_i}$, and then $\phi(1\otimes z)=z=0\iff 1\otimes z=0$. ϕ is surjective since $1/1\in S^{-1}\mathbb{Z}$.

[5] of "dual numbers": cf. http://en.wikipedia.org/wiki/Dual_numbers

i) Let A be a ring, S a multiplicatively closed subset of A, and $\phi\colon A \to S^{-1}A$ the canonical homomorphism. Show that $\phi^*\colon \operatorname{Spec}(S^{-1}A) \to \operatorname{Spec}(A)$ is a homeomorphism of $\operatorname{Spec}(S^{-1}A)$ onto its image in $X = \operatorname{Spec}(A)$. Let this image be denoted by $S^{-1}X$. In particular, if $f \in A$, the image of $\operatorname{Spec}(A_f)$ in X is the basic open set X_f (Chapter 1, Exercise 17).

The one-to-one correspondence given by (3.11.iv) is a bijection between $Y = \operatorname{Spec}(S^{-1}A)$ and $S^{-1}X = \{\mathfrak{p} \in X : \mathfrak{p} \cap S = \varnothing\}$, given by contraction ϕ^* and extension of prime ideals. In particular, $\mathfrak{p}^{ec} = \mathfrak{p}$ for primes $\mathfrak{p} \subseteq A \backslash S$.[6] By [1.21.i], ϕ^* is continuous. Since all ideals of $S^{-1}A$ are extended ideals by (3.11.i), to prove $\phi^*|^{S^{-1}X}$ is a homeomorphism onto its image, it is enough to show ϕ^* sends a non-empty closed set $V(\mathfrak{a}^e) \subseteq Y$ to the closed subset $V(\mathfrak{a}) \cap S^{-1}X \subseteq X$. Indeed, if $\mathfrak{a} \subseteq \mathfrak{p} \subseteq A \backslash S$, then $\mathfrak{a}^e \subseteq \mathfrak{p}^e \neq (1)$, and if $\mathfrak{a}^e \subseteq \mathfrak{p}^e \neq (1)$, then $\mathfrak{a} \subseteq \mathfrak{a}^{ec} \subseteq \mathfrak{p}^{ec} = \mathfrak{p}$.

Now let $S = \{1, f, f^2, \ldots\}$ for some $f \in A$. Then $S^{-1}\mathfrak{p} \in \operatorname{Spec}(A_f)$ just if $\mathfrak{p} \cap S = \varnothing$, and since $\mathfrak{p}$ is prime, this happens just if $f \notin \mathfrak{p}$, so that $\mathfrak{p} \in X_f$.

ii) Let $f\colon A \to B$ be a ring homomorphism. Let $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$, and let $f^*\colon Y \to X$ be the mapping associated with f. Identifying $\operatorname{Spec}(S^{-1}A)$ with its canonical image $S^{-1}X$ in X, and $\operatorname{Spec}(S^{-1}B)$ ($= \operatorname{Spec}(f(S)^{-1}B)$) with its canonical image $S^{-1}Y$ in Y, show that $S^{-1}f^*\colon \operatorname{Spec}(S^{-1}B) \to \operatorname{Spec}(S^{-1}A)$ is the restriction of f^* to $S^{-1}Y$, and that $S^{-1}Y = f^{*-1}(S^{-1}X)$.

Let $\mathfrak{q} \in Y$. Then $f(S) \cap \mathfrak{q} \neq \varnothing \iff \exists s \in S\, \big(f(s) \in \mathfrak{q}\big) \iff \exists s \in S\, \big(s \in f^{-1}(q)\big) \iff S \cap f^{-1}(\mathfrak{q}) \neq \varnothing$, so $\mathfrak{q} \in S^{-1}Y \iff f^*(\mathfrak{q}) \in S^{-1}X \iff \mathfrak{q} \in (f^*)^{-1}(S^{-1}X)$, showing $S^{-1}Y = (f^*)^{-1}(S^{-1}X)$.

$$\begin{tikzcd}
S^{-1}\mathfrak{q} \arrow[r, mapsto] \arrow[d, mapsto, "(S^{-1}f)^*"] & \mathfrak{q} \arrow[d, mapsto, "f^*"] \\
S^{-1}\big(f^{-1}(\mathfrak{q})\big) \arrow[r, mapsto] & f^{-1}(\mathfrak{q})
\end{tikzcd}$$

$$\begin{tikzcd}
\operatorname{Spec}(S^{-1}B) \arrow[r, "(\phi^*_{f(S)})^{-1}", "\approx"'] \arrow[d, "(S^{-1}f)^*"] & S^{-1}Y \arrow[r, hook] \arrow[d, "f^*"] & \operatorname{Spec}(B) \arrow[d, "f^*"] \\
\operatorname{Spec}(S^{-1}A) \arrow[r, "(\phi^*_S)^{-1}", "\approx"'] & S^{-1}X \arrow[r, hook] & \operatorname{Spec}(A)
\end{tikzcd}$$

Now $S^{-1}f\colon S^{-1}A \to S^{-1}B$ is given by $\frac{a}{s} \mapsto \frac{f(a)}{f(s)}$. Let $\mathfrak{q} \in S^{-1}Y$ and $a/s \in S^{-1}A$. We have

$$\frac{a}{s} \in (S^{-1}f)^{-1}(S^{-1}\mathfrak{q}) \iff \exists q \in \mathfrak{q}\, \exists t \in S \left[\frac{f(a)}{f(s)} = \frac{q}{f(t)}\right]$$
$$\iff \exists u, t \in S\, \exists q \in \mathfrak{q}\, [f(uta) = f(us)q \in \mathfrak{q}].$$

This certainly is the case if $f(a) = q \in \mathfrak{q}$ (take $t = s$ and $u = 1$), and if $f(a) \notin \mathfrak{q}$, then since $f(S) \cap \mathfrak{q} = \varnothing$ we have $f(Sa) \cap \mathfrak{q} = \varnothing$ ($\mathfrak{q}$ being prime), so $a/s \notin (S^{-1}f)^{-1}(S^{-1}\mathfrak{q})$. Thus $(S^{-1}f)^{-1}(S^{-1}\mathfrak{q}) = S^{-1}\big(f^{-1}(\mathfrak{q})\big)$, giving the commutative diagrams at left.

iii) Let $\mathfrak{a}$ be an ideal of A and let $\mathfrak{b} = \mathfrak{a}^e$ be its extension in B. Let $\bar{f}\colon A/\mathfrak{a} \to B/\mathfrak{b}$ be the homomorphism induced by f. If $\operatorname{Spec}(A/\mathfrak{a})$ is identified with its canonical image $V(\mathfrak{a})$ in X, and $\operatorname{Spec}(B/\mathfrak{b})$ with its image $V(\mathfrak{b})$ in Y, show that $\bar{f}^*$ is the restriction of f^* to $V(\mathfrak{b})$.

$$\begin{tikzcd}
\operatorname{Spec}(B/\mathfrak{b}) \arrow[r, "\varpi^*", "\approx"'] \arrow[d, "\bar{f}^*"] & V(\mathfrak{b}) \arrow[r, hook] \arrow[d, "f^*"] & \operatorname{Spec}(B) \arrow[d, "f^*"] \\
\operatorname{Spec}(A/\mathfrak{a}) \arrow[r, "\pi^*", "\approx"'] & V(\mathfrak{a}) \arrow[r, hook] & \operatorname{Spec}(A)
\end{tikzcd}$$

Let $\mathfrak{q} \in V(\mathfrak{b})$. Then $\mathfrak{a} \subseteq \mathfrak{a}^{ec} = \mathfrak{b}^c \subseteq \mathfrak{q}^c = f^*(\mathfrak{q})$, so $f^*\big(V(\mathfrak{b})\big) \subseteq V(\mathfrak{a})$. Now write $\pi\colon A \twoheadrightarrow A/\mathfrak{a}$ and $\varpi\colon B \twoheadrightarrow B/\mathfrak{b}$. Then by definition, $\bar{f}\big(\pi(a)\big) = f(a) + \mathfrak{b} = \varpi\big(f(a)\big)$, so $\bar{f} \circ \pi = \varpi \circ f$. Taking *'s and using [1.21.vi], $\pi^* \circ \bar{f}^* = f^* \circ \varpi^*$, giving the commutative diagram at right.

iv) Let $\mathfrak{p}$ be a prime ideal of A. Take $S = A\backslash\mathfrak{p}$ in ii) and then reduce mod $S^{-1}\mathfrak{p}$ as in iii). Deduce that the subspace $f^{*-1}(\mathfrak{p})$ of Y is naturally homeomorphic to $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) = \operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$, where $k(\mathfrak{p})$ is the residue field of the local ring $A_\mathfrak{p}$. $\operatorname{Spec}(k(\mathfrak{p}) \otimes_A B)$ is called the fiber *of f^* over $\mathfrak{p}$.*

$$\begin{tikzcd}
\operatorname{Spec}(A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}) \arrow[d, hook] & \operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}) \arrow[l, "\overline{(f_\mathfrak{p})}^*"] \arrow[d, hook] \\
\operatorname{Spec}(A_\mathfrak{p}) \arrow[d, hook] & \operatorname{Spec}(B_\mathfrak{p}) \arrow[l, "(f_\mathfrak{p})^*"] \arrow[d, hook] \\
\operatorname{Spec}(A) & \operatorname{Spec}(B) \arrow[l, "f^*"]
\end{tikzcd}$$

Making the identifications of ii) and iii), we have the commutative diagram at right. Now $k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ is a field, so its prime spectrum is $\{(0)\}$. Following the definitions of the inclusions, we see $\operatorname{Spec}(k(\mathfrak{p}))$ corresponds to the set of primes in $\operatorname{Spec}(A_\mathfrak{p})$ that contain $\mathfrak{p}A_\mathfrak{p}$, which in turn corresponds to the set of primes in $\operatorname{Spec}(A)$ that are contained in $\mathfrak{p}$ and contain $\mathfrak{p}$, or in other words the singleton $\{\mathfrak{p}\}$. Thus $\operatorname{Spec}(B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p})$ is identified with the preimage $(f^*)^{-1}(\mathfrak{p})$ of $\mathfrak{p}$. Now writing $T = (A/\mathfrak{p})\backslash\{0\}$ for the image of $S = A\backslash\mathfrak{p}$ in $A/\mathfrak{p}$, we have

$$k(\mathfrak{p}) \otimes_A B = (A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}) \otimes_A B \overset{(3.4.\text{iii})}{\cong} (A/\mathfrak{p})_\mathfrak{p} \otimes_A B \overset{[3.4]}{\cong} T^{-1}(A/\mathfrak{p}) \otimes_A B \overset{(3.5)}{\cong} T^{-1}(A/\mathfrak{p}) \otimes_{A/\mathfrak{p}} A/\mathfrak{p} \otimes_A B$$
$$\overset{[2.2]}{\cong} T^{-1}(A/\mathfrak{p}) \otimes_{A/\mathfrak{p}} B/\mathfrak{p}B \overset{(3.5)}{\cong} T^{-1}(B/\mathfrak{p}B) \overset{[3.4]}{\cong} S^{-1}(B/\mathfrak{p}B) \overset{(3.4.\text{iii})}{\cong} B_\mathfrak{p}/\mathfrak{p}B_\mathfrak{p}.$$

[6] by (3.11.ii), $\mathfrak{p}^{ec} = \bigcup_{s \in S}(\mathfrak{p} : s)$, and since $S \cap \mathfrak{p} = \varnothing$, we have $sa \in \mathfrak{p} \iff a \in \mathfrak{p}$, and $\mathfrak{p}^{ec} = \mathfrak{p}$. This is closely related to (3.16).

Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Then the canonical image of $\operatorname{Spec}(A_{\mathfrak{p}})$ *in* $\operatorname{Spec}(A)$ *is equal to the intersection of all the open neighborhoods of* $\mathfrak{p}$ *in* $\operatorname{Spec}(A)$*.*

Write $S = A \backslash \mathfrak{p}$. The canonical image $S^{-1}X$ of $\operatorname{Spec}(A_{\mathfrak{p}})$ in $\operatorname{Spec}(A)$ is the set of primes $\mathfrak{q} \lhd A$ that don't meet $A \backslash \mathfrak{p}$, or in other words are contained in $\mathfrak{p}$. By [1.17], the basic open sets X_f form a basis of $\operatorname{Spec}(A)$, so every open neighborhood of $\mathfrak{p}$ contains some X_f, and the intersection of all open neighborhoods of $\mathfrak{p}$ is $Z := \bigcap\{X_f : \mathfrak{p} \in X_f\}$.

Now if $\mathfrak{p} \in X_f$, we have $f \notin \mathfrak{p}$, so for any prime $\mathfrak{q} \subseteq \mathfrak{p}$ we a fortiori have $f \notin \mathfrak{q}$; so every open set $X_f \ni \mathfrak{p}$ we have $S^{-1}X \subseteq X_f$. Thus $S^{-1}X \subseteq Z$. On the other hand, suppose $\mathfrak{q} \notin S^{-1}X$. Then $\mathfrak{q}$ meets $S = A \backslash \mathfrak{p}$, so there exists $f \in \mathfrak{q} \backslash \mathfrak{p}$. Then $\mathfrak{p} \in X_f$ but $\mathfrak{q} \notin X_f$, and therefore $\mathfrak{q} \notin Z$. Thus $Z \subseteq S^{-1}X$.

Let A be a ring, let $X = \operatorname{Spec}(A)$ and let U be a basic open set in X (i.e., $U = X_f$ for some $f \in A$: Chapter 1, Exercise 17).
i) If $U = X_f$, show that the ring $A(U) = A_f$ depends only on U and not on f.

Write $S_f = \{1, f, f^2, \ldots\}$, and note that $\mathfrak{p} \in X_f \iff f \notin \mathfrak{p} \iff S_f \cap \mathfrak{p} = \varnothing$, since $\mathfrak{p}$ is prime. Recall ([3.7.ii]) that the saturation $\overline{S_f}$ is defined to be the complement of the union of all prime ideals which do not meet S_f, so that $T := \overline{S_f} = \overline{S_g}$. Recall the natural homomorphisms $\rho_f^T : A_f \to T^{-1}A$ and $\rho_g^T : A_g \to T^{-1}A$ of [3.2], and that, by [3.8], since T is the saturation of S_f and of S_g, these maps are isomorphisms. Then $\rho_f^g := (\rho_g^T)^{-1} \circ \rho_f^T$ is an isomorphism $A_f \xrightarrow{\sim} A_g$, and we have the following commutative diagram:

$$\begin{tikzcd}
 & A \arrow[dl, "\phi_g"'] \arrow[d, "\phi_T"] \arrow[dr, "\phi_f"] & \\
A_f \arrow[r, "\sim", "\rho_f^T"'] & T^{-1}A & A_g . \arrow[l, "\sim"', "\rho_g^T"]
\end{tikzcd}$$

Since ϕ_f is an epimorphism (Eq. 3.1 in [3.3]) it follows from the commutativity of the two small triangles that $\rho_f^g : A_f \to A_g$ is the *unique* isomorphism of the two rings making the big triangle commute: $\phi_g = \rho_f^g \circ \phi_f$. Thus

$A(U)$ is unique up to a unique isomorphism.[7]

ii) Let $U' = X_g$ be another basic open set such that $U' \subseteq U$. Show that there is an equation of the form $g^n = uf$ for some integer $n > 0$ and some $u \in A$, and use this to define a homomorphism $\rho\colon A(U) \to A(U')$ (i.e., $A_f \to A_g$) by mapping a/f^m to au^m/g^{mn}. Show that ρ depends only on U and U'. This homomorphism is called the restriction *homomorphism.*

If $X_g \subseteq X_f$, then by definition every prime $\mathfrak{p}$ not containing g doesn't contain f.[8] By de Morgan's laws, every prime containing f contains g. Intersecting these sets of primes, by (1.14) we have $g \in r\big((g)\big) \subseteq r\big((f)\big)$. Thus there

[7] An alternate, more direct proof not using saturation is as follows.

If $X_f = X_g$, by [1.17.iv], $r\big((f)\big) = r\big((g)\big)$. In particular, $f \in r\big((g)\big)$ and $g \in r\big((f)\big)$, so there are $u, v \in A$ and $n, m > 0$ such that $g^n = uf$ and $f^m = vg$.

By (3.2), ϕ_g will induce a unique isomorphism $\rho\colon A_f \to A_g$ such that $\phi_g = \rho \circ \phi_f \colon A \to A_f \to A_g$ just if

- For all $n \geq 0$, we have $\dfrac{f^n}{1}$ a unit of A_g;
- $\phi_g(c) = \dfrac{c}{1} = 0 \implies \exists n \geq 0\,[f^n c = 0]$;
- Every element of A_g is of the form $\dfrac{c}{1}\left(\dfrac{f^k}{1}\right)$.

To prove the first item it will suffice to show $f/1$ is a unit in A_g. But $uf = g^n$ in A, so $(u/g^n)(f/1) = 1/1$ in A_g, so that $f/1$ has inverse u/g^n. Note that also $(u/1)(f/g^n)$, so $u/1$ is a unit of A_g as well.

For the second item, suppose $a/1 = 0$ in A_g. Then by definition there is $k \geq 0$ such that $g^k a = 0$ in A. Multiplying by $v^n g^{n-k}$ we get $f^{mn}c = v^n u f a = v^n g^n a = 0$.

For the third item, note that since $f^m = vg$ in A, we have $(f^m/1)(1/g) = v/1$ in A_g. Multiplying by $(f/1)^{-m}$, we see $1/g = (v/1)(f/1)^{-m}$ in A_g. Thus an arbitrary element a/g^l of A_g can be written as $(av^l/1)(f/1)^{-lm}$.

Yet another proof, this time not using universal properties or saturations, follows. I include it because I took the time to work it out, but the reader is advised to skip it.

Define $\rho_f^g\colon A_f \to A_g$ by $c/f^k \mapsto c(f')^k$ and $\rho_g^f\colon A_g \to A_f$ by $c/g^k \mapsto c(g')^k$, where $f' = u/g^n$ and $g' = v/f^m$ Then

$$(\rho_g^f \circ \rho_f^g)\left(\frac{c}{f^k}\right) = \rho_g^f\left(\frac{cu^k}{g^{kn}}\right) = \frac{cu^k v^{kn}}{f^{kmn}}.$$

But $cu^k v^{kn}/f^{kmn} = c/f^k$ in A_f, for

$$f^k cu^k b^{kn} = c(uf)^k v^{kn} = cg^{kn}v^{kn} = c(vg)^{kn} = cf^{kmn}$$

in A. Symmetrically $\rho_f^g \circ \rho_g^f = \mathrm{id}_{A_g}$. It remains to show these maps are well-defined homomorphisms. By symmetry, it will suffice to do so for ρ_f^g. Suppose $c/f^k = d/f^l$ in A_f. Then by definition there is $p \geq 0$ such that $f^p f^l c = f^p f^k d$. For ρ_f^g to be well-defined we require that

$$\frac{cu^k}{g^{kn}} = \rho_f^g\left(\frac{c}{f^k}\right) = \rho_f^g\left(\frac{d}{f^l}\right) = \frac{du^l}{g^{ln}}$$

in A_g. But this means, by definition, there is $q \geq 0$ such that

$$cf^l g^q u^{k+l} = g^q(uf)^l cu^k = g^q g^{ln} cu^k = g^q g^{kn} du^l = g^q (uf)^k du^l = df^k g^q u^{k+l}$$

in A. Take $q = pn$. Then, as hoped,

$$cf^l g^{pn} u^{k+l} = cf^l (uf)^p u^{k+l} = (cf^l f^p) u^{k+l+p} = (df^k f^p) u^{k+l+p} = df^k (uf)^p u^{k+l} = df^k g^{pn} u^{k+l}.$$

By definition, ρ_f^g is multiplicative, for we have

$$\rho_f^g\left(\frac{c}{f^k}\right)\rho_f^g\left(\frac{d}{f^l}\right) = c(f')^k d(f')^l = (cd)(f')^{k+l} = \rho_f^g\left(\frac{c}{f^k}\cdot\frac{d}{f^l}\right).$$

Finally, for additivity, note that

$$\rho_f^g\left(\frac{c}{f^k} + \frac{d}{f^l}\right) = \rho_f^g\left(\frac{cf^l + df^k}{f^{k+l}}\right) = (cf^l + df^k)(f')^{k+l} = \frac{(cf^l + df^k)u^{k+l}}{g^{n(k+l)}};$$
$$\rho_f^g\left(\frac{c}{f^k}\right) + \rho_f^g\left(\frac{d}{f^l}\right) = c(f')^k + d(f')^l = \frac{cu^k}{g^{nk}} + \frac{du^l}{g^{nl}} = \frac{cu^k g^{nl} + du^l g^{nk}}{g^{n(k+l)}} = \frac{cu^k (uf)^l + du^l (uf)^k}{g^{n(k+l)}}.$$

[8] From this, we see that the union of primes not meeting $S_g = \{1, g, g^2, \ldots\}$ is a subset of the union of primes not meeting S_f, so by the definition of saturation in [3.7.ii], we have $\overline{S_f} \subseteq \overline{S_g}$, so [3.3] and [3.8] give us a unique homomorphism $\overline{S_f}^{-1}A \to \overline{S_g}^{-1}A$ commuting with

is $n > 0$ so that $g^n \in (f)$. Then for some $u \in A$, $g^n = uf$. To define a unique homomorphism $\rho\colon A_f \to A_g$ such that $\phi_g = \rho \circ \phi_f\colon A \to A_f \to A_g$, by (3.1) it suffices to show that $\phi_g(f) = f/1$ (and hence $\phi_g(f^n)$) is a unit. But since $g^n = uf$ in A we have $(f/1)(u/g^n) = 1$ in A_g. Thus a unique $\rho^g_f\colon A_f \to A_g$ exists such that $\phi_g = \rho^g_f \circ \phi_f$ and it must take $1/f \mapsto u/g^n$ so that $(f/1)\rho(1/f) = 1/1$.

$$\begin{tikzcd}
A_f \arrow[rr, "\rho^g_f"] & & A_g \arrow[dd, "\rho^{g'}_g", "\sim"'] \\
& A \arrow[ul, "\phi_f"'] \arrow[ur, "\phi_g"] \arrow[dl, "\phi_{f'}"] \arrow[dr, "\phi_{g'}"'] & \\
A_{f'} \arrow[uu, "\rho^f_{f'}", "\sim"'] \arrow[rr, "\rho^{g'}_{f'}"'] & & A_{g'}
\end{tikzcd}$$

To show uniqueness, suppose $\rho^f_{f'}\colon A_{f'} \xrightarrow{\sim} A_f$ and $\rho^{g'}_g\colon A_g \xrightarrow{\sim} A_{g'}$ are canonical isomorphisms, commuting with the canonical maps ϕ from A, and let ρ^g_f and $\rho^{g'}_{f'}$ be the unique maps given in the preceding paragraph. Canonicity means that all the triangles in the diagram at right commute. That "ρ depends only on U and U'" can mean nothing stronger than that the outer square commutes. Now

$$\rho^{g'}_{f'} \circ \phi_{f'} = \phi_{g'} = \rho^{g'}_g \circ \phi_g = \rho^{g'}_g \circ \rho^g_f \circ \phi_f = \rho^{g'}_g \circ \rho^g_f \circ \rho^f_{f'} \circ \phi_{f'}.$$

As $\phi_{f'}$ is an epimorphism (Eq. 3.1 in [3.3] again), $\rho^{g'}_{f'} = \rho^{g'}_g \circ \rho^g_f \circ \rho^f_{f'}$.

iii) If $U = U'$, then ρ is the identity map.

$\rho^U_U = \mathrm{id}_{A(U)}$ satisfies the equation $\phi_U = \rho^U_U \circ \phi_U$, and is unique since ϕ_U is an epimorphism by Eq. 3.1 of [3.3].

iv) If $U \supseteq U' \supseteq U''$ are basic open sets in X, show that the diagram

$$\begin{tikzcd}
A(U) \arrow[rr] \arrow[dr] & & A(U'') \\
& A(U') \arrow[ur] &
\end{tikzcd}$$

(in which the arrows are restriction homomorphisms) is commutative.

$$\begin{tikzcd}
S^{-1}A \arrow[dr, "\rho^T_S"] \arrow[ddrr, bend left, "\rho^V_S"] & & \\
& T^{-1}A \arrow[dr, "\rho^V_T"] & \\
A \arrow[uu, "\phi_S"] \arrow[ur, "\phi_T"] \arrow[rr, "\phi_V"'] & & V^{-1}A
\end{tikzcd}$$

Recall that [3.3] and [3.8] give us, for multiplicatively submonoids $S \subseteq T \subseteq A$ *unique* homomorphisms $\rho^T_S\colon S^{-1}A \to T^{-1}A$ such that $\phi_T = \rho^T_S \circ \phi_S$, where $\phi_S\colon A \to S^{-1}A$ is the epimorphic (Eq. 3.1) canonical map. If $S \subseteq T \subseteq V \subseteq A$ are multiplicative submonoids, we have

$$\phi_V = \rho^V_T \circ \phi_T = \rho^V_T \circ \rho^T_S \circ \phi_S,$$

but $\rho^V_S \circ \phi_S = \phi_V$ as well, so since ϕ_S is epimorphic, $\rho^V_T \circ \rho^T_S = \rho^V_S$. Now let $U = X_f \supseteq U' = X_{f'} \supseteq U'' = X_{f''}$ and $S = \overline{S_f} \subseteq T = \overline{S_{f'}} \subseteq V = \overline{S_{f''}}$, and use ii).

v) Let x $(= \mathfrak{p})$ be a point of X. Show that

$$\varinjlim_{U \ni x} A(U) \cong A_{\mathfrak{p}}.$$

Let, again, $S = A \backslash \mathfrak{p}$. For $f, g \in S$, write $f \le g$ if $r\big((g)\big) \subseteq r\big((f)\big)$, or equivalently if $X_g \subseteq X_f$. This makes S into a directed pre-order, for

- $r\big((f)\big) \subseteq r\big((f)\big) \implies f \le f$,
- $f \le g \le h$ implies $r\big((h)\big) \subseteq r\big((g)\big) \subseteq r\big((f)\big)$, which implies $f \le h$, and
- if $f, g \in S$ we have $fg \in S$, and $r\big((fg)\big) \subseteq r\big((f)\big) \cap r\big((g)\big)$.

Now one can take direct limits over directed pre-orders, but the result is the same if we collapse the pre-order to its skeleton, or arbitrarily take one element in each equivalence class, where $f \equiv g \iff f \le g \le f$, and then take the direct limit. Since we defined direct limits over partial orders, let's do that. For each basic open set U, take just one representative f such that $U = X_f$. The uniqueness from part ii) makes our choice, up to a unique isomorphism, irrelevant. Then the restricted pre-order $(S', \le)$ is a directed set. Consider the system $\mathbf{B} = (A_f, \rho^g_f)_{f,g \in S'}$, where the restriction map ρ^g_f of ii) is defined if $f \le g$. Now S' is a directed set and parts iii) and iv) of this exercise give axioms

the maps ϕ from A. Recall that [3.8] gives us unique isomorphisms $A_f \xrightarrow{\sim} \overline{S_f}^{-1}A$ and $\overline{S_g}^{-1}A \xrightarrow{\sim} A_g$ commuting with the ϕ; letting ρ^g_f be the composition $A_f \xrightarrow{\sim} \overline{S_f}^{-1}A \to \overline{S_g}^{-1}A \xrightarrow{\sim} A_g$, we have a unique ring homomorphism $A_f \to A_g$ such that $\phi_g = \rho^g_f \circ \phi_f$. But this doesn't give us an explicit expression for the homomorphism.

(1) and (2) of [2.14] defining compatibility conditions for maps in a direct system. Thus $\mathbf{B}$ is a direct system. Write $B = \varinjlim \mathbf{B}$ for the limit, and $\rho_f : A_f \to B$ for the canonical map.

Now for each $f \in S'$ we have $S_f = \{1, f, f^2, \ldots\} \subseteq S$, so by [3.3] and [3.8] there is a unique map $\sigma_f := \rho_f^S : A_f = S_f^{-1}A \to S^{-1}A = A_\mathfrak{p}$ such that $\sigma_f \circ \phi_f = \phi_S$. If $f \leq g \in S'$, then

$$\sigma_g \circ \rho_f^g \circ \phi_f = \rho_g^S \circ \rho_f^g \circ \phi_f = \rho_f^S \circ \phi_f = \sigma_f \circ \phi_f,$$

where the middle equality comes from the slightly generalized version of part iv), and then since ϕ_f is an epimorphism (Eq. 3.1 of [3.3]), $\sigma_g \circ \rho_f^g = \sigma_f$. Since the σ_f meet this compatibility condition, by [2.16], there then exists a unique ring map $\sigma : B \to A_\mathfrak{p}$ such that $\sigma \circ \rho_f = \sigma_f$ for all $f \in S'$. It remains to show σ is a bijection.

Let $b \in B$ be such that $\sigma(b) = 0$ in $A_\mathfrak{p}$. By [2.15] there is some $f \in S'$ such that b has a representative in A_f, so let $a \in A$ and $n \geq 0$ be such that $\rho_f(a/f^n) = b$. Then we have $0 = \sigma(b) = \sigma(\rho_f(a/f^n)) = \sigma_f(a/f^n) = \rho_f^S(a/f^n)$. That means that considered as an element of $A_\mathfrak{p}$ we have $a/f^n = 0$, so by [3.1] there is $s \in A \backslash \mathfrak{p} = S$ such that $sa = 0$ in A. But then in A_{sf} we have $\rho_f^{sf}(a/f^n) = as^n/(sf)^n = 0$, so

$$b = \rho_f(a/f^n) = \rho_{sf}(\rho_f^{sf}(a/f^n)) = \rho_{sf}(0) = 0,$$

showing σ is injective.

Let any element $a/s \in S^{-1}A = A_\mathfrak{p}$ be given. Then $a/s \in A_s$ is of course such that $\rho_s^S(a/s) = a/s$, and if we let $b = \rho_s(a/s)$, then

$$\sigma(b) = \sigma(\rho_s(a/s)) = \sigma_s(a/s) = \rho_s^S(a/s) = a/s.$$

Therefore σ is surjective, completing the proof.

The assignment of the ring $A(U)$ to each basic open set U of X, and the restriction homomorphisms ρ, satisfying the conditions iii) and iv) above, constitutes a presheaf of rings *on the basis of open sets $(X_f)_{f \in A}$. v) and iv) says that the stalk of this presheaf at $x \in X$ is the corresponding local ring $A_\mathfrak{p}$.*

Complete the description of a presheaf structure on $X = \mathrm{Spec}(A)$, by defining $A(U)$ for all *open subsets $U \subseteq X$, not just basic ones.*

Let $V \subseteq X$ be an arbitrary open set, and let $\{X_{f_i}\}_{i \in I}$ be all the basic open sets contained in V. Let S_i be the saturation of $\{1, f_i, f_i^2, \ldots\}$, so that $S_i = A \setminus \bigcup U_i$ by [3.7.ii]. By [3.8] we have a canonical isomorphism $A(U_i) \cong S_i^{-1}A$. Then $S_V = \bigcap_{i \in I} S_j$ is a saturated set since it contains 1, and

$$xy \in S_V \iff \forall i \in I\ (xy \in S_i) \iff \forall i \in I\ (x \in S_i \ \&\ y \in S_i) \iff x \in S_V \ \&\ y \in S_V.$$

Now

$$S_V = \bigcap_{i \in I}\Big(A \setminus \bigcup_{\mathfrak{p} \in U_i} \mathfrak{p}\Big) = A \setminus \bigcup_{i \in I} \bigcup_{\mathfrak{p} \in U_i} \mathfrak{p} = A \setminus \bigcup \Big\{\mathfrak{p} : \mathfrak{p} \in \bigcup_{i \in I} U_i\Big\} = A \setminus \bigcup_{\mathfrak{p} \in V} \mathfrak{p}. \tag{3.7}$$

Define $A(V) := S_V^{-1}A$. If $W \subseteq V$ is a smaller open set, Eq. 3.7 shows that $S_V \subseteq S_W$, so [3.3] and [3.8] give us a natural restriction map $\rho_V^W : A(V) \to A(W)$. [23.iii,iv] show that these maps define a presheaf, and [3.8] shows this definition agrees with the other one if V is a basic open set. Since every open set contains a basic open set, the rings $A(U_f)$ are cofinal in the $A(V)$, so the direct limits $A_\mathfrak{p} \cong \varinjlim_{V \ni \mathfrak{p}} A(V) \cong \varinjlim_{U_f \ni \mathfrak{p}} A(U_f)$ are isomorphic and stalks are unchanged.

Show that the presheaf of Exercise 23 has the following property. Let $(U_i)_{i \in I}$ be a covering of X by basic open sets. For each $i \in I$ let $s_i \in A(U_i)$ be such that, for each pair of indices i, j, the images of s_i and s_j in $A(U_i \cap U_j)$ are equal. Then there exists a unique $s \in A$ (= $A(X)$) whose image in $A(U_i)$ is s_i, for all $i \in I$. (This essentially implies that the presheaf is a sheaf.)

Let $U_i = X_{f_i}$. By [1.17.v], X is compact , so there are finitely many $U_1, \ldots, U_n$ covering X. Thus

$$X \setminus \bigcap_{i=1}^n V(f_i) = \bigcup_{i=1}^n (X \setminus V(f_i)) = \bigcup_{i=1}^n X_{f_i} = X.$$

By [1.15.iii,i], $\varnothing = \bigcap_{i=1}^{n} V(f_i) = \left(\sum_{i=1}^{n}(f_i)\right)$, so no maximal ideal contains $\sum_{i=1}^{n}(f_i)$, which then must be (1). Fix $m \geq 1$. (1.16) shows that for any ideals $\mathfrak{a}, \mathfrak{b} \lhd A$, if $\mathfrak{a}+\mathfrak{b} = (1)$, then $\mathfrak{a}^m + \mathfrak{b} = (1)$, since $\mathfrak{a} \subseteq r(\mathfrak{a}^m)$. Applying this repeatedly to the sum $\sum_{i=1}^{n}(f_i) = (1)$, taking $\mathfrak{a} = (f_1)$, then (f_2), etc., we see $\sum_{i=1}^{n}(f_i^m) = 1$, so there are $a_i \in A$ such that

$$\sum_{i=1}^{n} a_i f_i^m = 1. \tag{3.8}$$

We first show uniqueness of $s \in A$, assuming it exists. If s and s' both meet the conditions, then $\rho_X^{U_i}(s) = \rho_X^{U_i}(s')$ for each canonical restriction map $\rho_X^{U_i} = \phi_i \colon A \to A(U_i)$, so $\rho_X^{U_i}(s-s') = 0$. We want to show $t = s - s'$ is zero. Now $t \in \ker(\rho_X^{U_i})$ if and only if, by [3.1], for some number $m_i \geq 0$ we have $f_i^{m_i} t = 0$. Let $m = \max_{i=1}^{n} m_i$, so for $i = 1, \ldots, n$ we have $f_i^m t = 0$. Multiplying t by the expression Eq. 3.8 for 1, we get

$$t = 1t = \sum_{i=1}^{n} a_i f^m t = \sum_{i=1}^{n} a_i \cdot 0 = 0.$$

Now we must show existence. We initially restrict attention to the open cover $\{U_1, \ldots, U_n\}$. Suppose $s_i \in A_{f_i}$ is given by $b_i'/f_i^{m_i}$. Let $m = \max_{i=1}^{n} m_i$. Then setting $b_i = b_i' f_i^{m-m_i}$, we have $s_i = (b_i'/f_i^{m_i})(f_i/f_i)^{m-m_i} = b_i/f_i^m$. Write $g_i = f_i^m$.[9] Now $X_{f_i} \cap X_{f_j} = X_{f_i f_j}$ by [1.17.i], and the images $b_i/g_i = b_j/g_j$ in $A_{f_i f_j}$ just if there is $m_{ij} \geq 0$ such that $(g_i g_j)^{m_{ij}} g_j b_i = (g_i g_j)^{m_{ij}} g_i^m b_j$. (If $X_{f_i f_j} = \varnothing$, then $f_i f_j$ is nilpotent, by [1.17.ii], and then $1/1 = (f_i f_j / f_i f_j)$ is nilpotent, so $1 = 0 \in A_{f_i g_i}$ and the restrictions agree trivially.) Take $p = \max_{i,j} m_{ij}$; then

$$g_i^p g_j^{p+1} b_i = g_i^{p+1} g_j^p b_j. \tag{3.9}$$

We want to find an s such that $s/1 = b_i/g_i$ in each A_{f_i}, meaning there exists k such that $g_i^{k+1} s = g_i^k (s g_i) = g_i^k b_i$ in A. In an attempt to make this work and find s, fix j, take Eq. 3.8, with m to be determined later, and multiply both sides by $g_j^k b_j$. Then

$$g_j^k b_j = \sum_{i=1}^{n} a_i b_j g_j^k g_i^m.$$

We want to use Eq. 3.9 to get one more g_j on the right-hand side, so we should require $m \geq p+1$ and $k \geq p$. Then

$$g_j^k b_j = \sum_{i=1}^{n} a_i (b_j g_j^p g_i^{p+1}) g_j^{k-p} g_i^{m-p-1} \overset{\text{Eq. 3.9}}{=} \sum_{i=1}^{n} a_i (b_i g_j^{p+1} g_i^p) g_j^{k-p} g_i^{m-p-1} = g_j^{k+1} \sum_{i=1}^{n} a_i b_i g_i^{m-1}.$$

In particular, $k = p$ and $m = p+1$ work. Then if we take $s = \sum_{i=1}^{n} a_i b_i g_i^p$, we have $g_j^p b_j = g_j^{p+1} s$ for all $j = 1, \ldots, n$, so this s satisfies $\rho_X^{U_j}(s) = s_j$, as hoped.

Now let $U_i = V = X_h$ be an arbitrary element of the initial cover (hence not necessarily one of $U_1, \ldots, U_n$). We must show $\rho_X^V = s_i =: t$. Now $W_j = U_j \cap V$, for $j = 1, \ldots, n$, are by [1.17.i] also basic open sets, and by assumption

$$\rho_V^{W_j}(t) = \rho_{U_j}^{W_j}(s_j) = \rho_X^{W_j}(s) \overset{[3.23.\text{iv}]}{=} (\rho_V^{W_j} \circ \rho_X^V)(s).$$

Thus $\rho_V^{W_j}(t - \rho_X^V(s)) = 0$ for $j = 1, \ldots, n$. But the W_j cover $X_h = \operatorname{Spec}(A_h)$. Now by the uniqueness clause above, applied to A_h instead of A and the open cover W_j instead of U_j, and implicitly using the isomorphisms $(A_h)_{f_j/1} \cong A_{hf_j}$, we have $t = \rho_X^V(s)$.

[9] Though a posteriori it seems natural, the substitution of g_i for f_i and the conditions on k, m later I learned from looking over Jinhyun Park's solution: `http://mathsci.kaist.ac.kr/~jinhyun/sol2/comm.html`.

Let $f: A \to B$, $g: A \to C$ be ring homomorphisms and let $h: A \to B \otimes_A C$ be defined by $h(x) = f(x) \otimes g(x)$. Let X, Y, Z, T be the prime spectra of A, B, C, $B \otimes_A C$ respectively. Then $h^*(T) = f^*(Y) \cap g^*(Z)$.

The first thing is to note that, as on p. 31, the suggested map h is not an A-algebra homomorphism. See [2.23]. Instead define $h: a \mapsto f(a) \otimes 1 = 1 \otimes g(a)$.

That out of the way, let $\mathfrak{p} \in X$ and write $k = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. We have

$$\mathfrak{p} \in h^*(T) \iff \varnothing \neq (h^*)^{-1}(\mathfrak{p}) \overset{[3.21.\mathrm{iv}]}{\approx} \operatorname{Spec}(k \otimes_A B \otimes_A C) \overset{(2.14.\mathrm{i,ii})}{\approx} \operatorname{Spec}(B \otimes_A k \otimes_A C)$$
$$\overset{(2.14.\mathrm{i})}{\approx} \operatorname{Spec}(B \otimes_A (k \otimes_k k) \otimes_A C) \overset{(2.15)}{\approx} \operatorname{Spec}\big((B \otimes_A k) \otimes_k (k \otimes_A C)\big)$$

Now the only ring with empty spectrum is the zero ring, and a tensor product of vector spaces is nonzero just if each factor is nonzero. Thus $\mathfrak{p} \in h^*(T)$ just if $k \otimes_A B$ and $k \otimes_A C$ are nonzero. By [3.21.iv] again, this happens just if $\mathfrak{p} \in f^*(Y)$ and $\mathfrak{p} \in g^*(Z)$.

Let $(B_\alpha, g_{\alpha\beta})$ be a direct system of rings and B the direct limit. For each α, let $f_\alpha: A \to B_\alpha$ be a ring homomorphism such that $g_{\alpha\beta} \circ f_\alpha = f_\beta$ whenever $\alpha \leq \beta$ (i.e. the B_α form a direct system of A-algebras). The f_α induce $f: A \to B$. Show that

$$f^*\big(\operatorname{Spec}(B)\big) = \bigcap_\alpha f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big).$$

To see the map f is well defined, choose any α and define $f(a) = g_\alpha(f_\alpha(a))$, where $g_\alpha: B_\alpha \to B$ is the canonical map in the definition of the direct limit. Suppose $\gamma \geq \alpha$. Then

$$g_\alpha \circ f_\alpha \overset{[2.14]}{=} g_\gamma \circ g_{\alpha\gamma} \circ f_\alpha = g_\gamma \circ f_\gamma$$

Thus, for any α, β, find $\gamma \geq \alpha, \beta$; then $g_\alpha \circ f_\alpha = g_\gamma \circ f_\gamma = g_\beta \circ f_\beta$, so the definition is independent of α.

Let $\mathfrak{p} \in \operatorname{Spec}(A)$ be given, and set $k = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$. Recall from [2.20] that $\varinjlim(B_\alpha \otimes_A k) \cong B \otimes_A k$, so the two have homeomorphic spectra. Now by [3.21.iv], $\mathfrak{p} \in f^*\big(\operatorname{Spec}(B)\big)$ just if $\operatorname{Spec}(B \otimes_A k) \neq \varnothing$ just if $k \otimes_A B \neq 0$. On the other hand $\mathfrak{p} \in f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big)$ just if $k \otimes_A B_\alpha \neq 0$. Now by [2.21], $k \otimes_A B = 0$ just if for some α, $k \otimes_A B_\alpha = 0$.

i) Let $f_\alpha: A \to B_\alpha$ be any family of A-algebras and let $f: A \to B$ be their tensor product over A (Chapter 2, Exercise 23). Then

$$f^*\big(\operatorname{Spec}(B)\big) = \bigcap_\alpha f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big).$$

Recall from [2.23] that $B = \varinjlim B_J$, where each J is a finite set of α's, $B_J = \bigotimes_{\alpha \in J}^A B_\alpha$, and if $J = \{\alpha_1, \ldots, \alpha_m\}$ and $I = J \cup \{\alpha_{m+1}, \ldots, \alpha_n\}$ we define $g_{JI}(b_1 \otimes \cdots \otimes b_n) = b_1 \otimes \cdots \otimes b_n \otimes 1 \otimes \cdots \otimes 1$. For each J, $f_J: a \mapsto f_{\alpha_1}(a) \otimes 1 \otimes \cdots \otimes 1 = a(1 \otimes \cdots \otimes 1)$ defines an A-algebra homomorphism $A \to B_J$ independent of the apparent choice of non-1 coordinate by the definition of the tensor product. Now we are in the situation of [3.26], and $f^*\big(\operatorname{Spec}(B)\big) = \bigcap_J f_J^*\big(\operatorname{Spec}(B_J)\big)$. But by iterated application of [3.25], we have $f_J^*\big(\operatorname{Spec}(B_J)\big) = \bigcap_{\alpha \in J} f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big)$, so $f^*\big(\operatorname{Spec}(B)\big) = \bigcap_J f_J^*\big(\operatorname{Spec}(B_J)\big)$. (To consider only singletons $J = \{\alpha\}$ is strictly speaking insufficient since without [3.25], we don't know for $I \ni \alpha$ what relation exists between $f_I^*\big(\operatorname{Spec}(B_I)\big)$ and $f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big)$.)

ii) Let $f_\alpha: A \to B_\alpha$ be any finite family of A-algebras and let $B = \prod_\alpha B_\alpha$. Define $f: A \to B$ by $f(x) = (f_\alpha(x))$. Then $f^*\big(\operatorname{Spec}(B)\big) = \bigcup_\alpha f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big)$.

Recall [1.22]: if e_α has α-coordinate 1 and other coordinates 0, and $\mathfrak{b} \lhd B$, then $\mathfrak{b} = \sum \mathfrak{b}e_\alpha$, and, writing $\pi_\alpha: B \twoheadrightarrow B_\alpha$ for the canonical projection, $B/\mathfrak{b} \cong \prod B_\alpha/\pi_\alpha(\mathfrak{b})$, so $\mathfrak{p} \lhd B$ is prime just if it is of the form $\mathfrak{p}_\alpha^+ = \mathfrak{p}_\alpha e_\alpha + \sum_{\beta \neq \alpha}(e_\beta)$ for some α and some prime $\mathfrak{p}_\alpha \lhd B_\alpha$. Recall that this gives a homeomorphism between $\operatorname{Spec}(B)$ and the disjoint union of the $\operatorname{Spec}(B_\alpha)$. Now

$$f^{-1}(\mathfrak{p}_\alpha^+) = f^{-1}\big(\{b = (b_\alpha) \in B : \exists a \in A \ \forall \beta \ (f_\beta(a) = b_\beta \ \& \ f_\alpha(a) = b_\alpha \in \mathfrak{p}_\alpha)\}\big) = \{a \in A : f_\alpha(a) \in \mathfrak{p}_\alpha\} = f_\alpha^{-1}(\mathfrak{p}_\alpha), \quad \text{so}$$

$$f^*\big(\operatorname{Spec}(B)\big) = \bigcup_\alpha \{f^{-1}(\mathfrak{p}_\alpha^+) : \mathfrak{p}_\alpha \in \operatorname{Spec}(B_\alpha)\} = \bigcup_\alpha \{f_\alpha^{-1}(\mathfrak{p}_\alpha) : \mathfrak{p}_\alpha \in \operatorname{Spec}(B_\alpha)\} = \bigcup_\alpha f_\alpha^*\big(\operatorname{Spec}(B_\alpha)\big).$$

iii) Hence the subsets of $X = \operatorname{Spec}(A)$ of the form $f^*\bigl(\operatorname{Spec}(B)\bigr)$, where $f\colon A \to B$ is a ring homomorphism, satisfy the axioms for closed sets in a topological space. The associated topology is the constructible *topology on X. It is finer than the Zariski topology (i.e., there are more open sets, or equivalently more closed sets).*

For a homomorphism $f\colon A \to B$, write $C_f = f^*\bigl(\operatorname{Spec}(B)\bigr)$ for the closed set of the constructible topology defined by f. To finish checking the C_f define a topology, we should ensure that $\varnothing$ and X are among them. But $X = C_{\mathrm{id}_A}$, and $\varnothing = C_z$ for $z\colon A \to 0$, which has no prime ideals. Every $V(\mathfrak{a})$ closed in the Zariski topology is C_f for the canonical map $f\colon A \twoheadrightarrow A/\mathfrak{a}$, so the constructible topology is at least as fine as the Zariski topology. It is not always strictly finer, as witness the zero ring or a ring with only one prime ideal.

iv) Let X_C denote the set X endowed with the constructible topology. Show that X_C is compact.

To show every finite open cover of X has a finite subcover is the same as showing that for every collection of closed sets of X with empty intersection, some finite subset has empty intersection.

So let $\{C_f : f\colon A \to B_f\}$ have empty intersection. Write $g\colon A \to B = \bigotimes_f B_f$ for the canonical map given by [2.23] making B an A-algebra. Then by [3.27.i],

$$\varnothing = \bigcap C_f = \bigcap f^*\bigl(\operatorname{Spec}(B_f)\bigr) = g^*\bigl(\operatorname{Spec}(B)\bigr),$$

so $\operatorname{Spec}(B)$ is empty. Since by (1.4) every ring where $0 \neq 1$ has a maximal ideal, $B = \varinjlim_J B_J = 0$. But then by [2.21], we have some $B_J = \bigotimes^A_{f\in J} B_f = 0$ for some finite subset J of the f. Write $h\colon A \to B_J$. Applying [3.27.i] again, we have

$$\varnothing = h^*\bigl(\operatorname{Spec}(B_J)\bigr) = \bigcap_{f\in J} f^*\bigl(\operatorname{Spec}(B_f)\bigr) = \bigcap_{f\in J} C_f.$$

(Continuation of Exercise 27.)

i) For each $g \in A$, the set X_g (Chapter 1, Exercise 17) is both open and closed in the constructible topology.

If $f\colon A \to A_g$ is the canonical map, then C_f is by (3.11.iv) the set of primes not meeting $\{1, g, g^2, \ldots\}$, so $C_f = X_g$ is closed in the constructible topology. On the other hand since the constructible topology is at least as fine as the Zariski topology, X_g is open. More explicitly, let $\mathfrak{a} = r\bigl((g)\bigr)$ be the intersection of all primes containing g. Then for all primes $\mathfrak{p} \in \operatorname{Spec}(A)$ we have $\mathfrak{p} \in V(\mathfrak{a}) \iff g \in \mathfrak{p} \iff \mathfrak{p} \notin X_g$, so $X_g = X \setminus V(\mathfrak{a})$. But $V(\mathfrak{a})$ is C_f for the canonical map $f\colon A \to A/\mathfrak{a}$.

ii) Let C' denote the smallest topology on X for which the sets X_g are both open and closed, and let $X_{C'}$ denote the set X endowed with this topology. Show that $X_{C'}$ is Hausdorff.

Let $x, y \in X_{C'}$ be distinct points. Then the corresponding primes $\mathfrak{p}_x, \mathfrak{p}_y \in \operatorname{Spec}(A)$ are not equal, so one is not strictly contained in the other. Suppose without loss of generality that $\mathfrak{p}_x \not\subseteq \mathfrak{p}_y$. Then there is $f \in \mathfrak{p}_x \setminus \mathfrak{p}_y$, meaning $y \in X_f$, but $x \in X_{C'} \setminus X_f$. But these are disjoint open sets by the definition of C'.

iii) Deduce that the identity mapping $X_C \to X_{C'}$ is a homeomorphism. Hence a subset E of X is of the form $f^*\bigl(\operatorname{Spec}(B)\bigr)$ for some $f\colon A \to B$ if and only if it is closed in the topology C'.

First, the identity mapping $X_C \to X_{C'}$ is of course a bijection.

Second, the topology C' is the topology generated by subbasic closed sets X_g and $X \setminus X_g$ for each $g \in A$. (Thus a closed set K of $X_{C'}$ is one that can be written as finite a union of arbitrary intersections of these.) But these subbasic sets are also closed in X_C, so every closed set of $X_{C'}$ is closed in X_C and the identity map is continuous.

Third, a continuous bijection $\psi\colon Y \longleftrightarrow Z$ between a compact space Y and a Hausdorff space Z is well known to be a homeomorphism.[10]

iv) The topological space X_C is compact, Hausdorff and totally disconnected.

Since X_C is compact, $X_{C'}$ is Hausdorff, and we have just shown $X_C \approx X_{C'}$, it remains to see X_C is totally disconnected. But this follows from our proof it is Hausdorff, for given any distinct $x, y \in S \subseteq X_C$ we have found disjoint closed open sets $U = X_f$ and $V = X_C \setminus X_f$ separating them, whose union is the whole space X_C, and so $S = (U \cap S) \amalg (V \cap S)$ is a disjoint union of closed open sets (in the relative topology) separating x from y.

[10] It suffices to prove it takes open sets to open sets. Let $U \subseteq Y$ be open; then its complement $K = Y \setminus U$ is closed. As a closed subset of a compact space, K is compact. Since ψ is continuous, $\psi(K)$ is compact. As a compact subset of a Hausdorff space, $\psi(K)$ is closed. Thus $Z \setminus \psi(K) = \psi(Y \setminus K) = \psi(U)$ is open.

Let $f: A \to B$ be a ring homomorphism. Show that $f^*: \mathrm{Spec}(B) \to \mathrm{Spec}(A)$ is a continuous closed *mapping (i.e., maps closed sets to closed sets) for the constructible topology.*

Let any constructible closed set $K \subseteq \mathrm{Spec}(B)$ be given, and let $g: B \to C$ be such that $K = g^*\big(\mathrm{Spec}(C)\big)$. Then

$$f^*(K) = f^*\Big(g^*\big(\mathrm{Spec}(C)\big)\Big) \overset{[1.21.vi]}{=} (g \circ f)^*\big(\mathrm{Spec}(C)\big)$$

is by definition a closed set of $\mathrm{Spec}(A)$ in the constructible topology.

Show that the Zariski topology and the constructible topology on $\mathrm{Spec}(A)$ *are the same if and only if $A/\mathfrak{N}$ is absolutely flat (where $\mathfrak{N}$ is the nilradical of A).*

First suppose $A/\mathfrak{N}$ is absolutely flat. Then by [3.11], $X = \mathrm{Spec}(A)$ in the Zariski topology is Hausdorff. Since the constructible topology is at least as fine as the Zariski topology, the identity map $X_C \to X$ is a continuous bijection from a compact space to a Hausdorff space, hence a homeomorphism; see the footnote to [3.28.iii].

Now suppose $X = X_C$. Then X is Hausdorff, so by [3.11], $A/\mathfrak{N}$ is absolutely flat.

Primary Decomposition

Proposition 4.8. *Let S be a multiplicatively closed subset of A, and let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal.*
ii) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary, and its contraction in A is $\mathfrak{q}$.

The book states that "The verification that $S^{-1}\mathfrak{q}$ is primary is straightforward." We complete the this verification. Suppose $x/s,\ y/t \in S^{-1}A$ are such that $xy/st \in S^{-1}\mathfrak{q}$. Then there are some $z \in \mathfrak{q}$ and $u \in S$ such that $xy/st = z/u$ in $S^{-1}A$. That means there is $v \in S$ such that $vuxy = vstz \in \mathfrak{q} \subseteq A$. Since $\mathfrak{q}$ is primary, either $vux \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n > 0$. If $vux \in \mathfrak{q}$, then $vux/svu = x/s \in S^{-1}\mathfrak{q}$. If $y^n \in \mathfrak{q}$, then $(y/t)^n = (1/t^n)(y^n/1) \in S^{-1}\mathfrak{q}$. Thus $x/s \in S^{-1}\mathfrak{q}$ or $(y/t)^n \in S^{-1}\mathfrak{q}$, showing $S^{-1}\mathfrak{q}$ is primary.

Proposition 4.12*.[1] *Let A be a ring, S a multiplicatively closed subset of A. Write $\phi_S : A \to S^{-1}A$ for the canonical map. For any ideal $\mathfrak{a}$, let $S(\mathfrak{a})$ denote the contraction along ϕ_S of $S^{-1}\mathfrak{a}$ in A (bottom of p. 53, [4.11]). The ideal $S(\mathfrak{a})$ is called the* saturation *of $\mathfrak{a}$ with respect to S.*
i) $\bigcup_{s\in S}(\mathfrak{a} : s) = \{x \in A : \exists s \in S\ (sx \in \mathfrak{a})\} = S(\mathfrak{a}) = \mathfrak{a}^{ec} \supseteq \mathfrak{a}$.
ii) $S(0) = \ker(\phi_S)$.
iii) Let $S_\mathfrak{p} = A \backslash \mathfrak{p}$ for $\mathfrak{p}$ a prime ideal of A. If $\mathfrak{q}$ is $\mathfrak{p}$-primary, then $S_\mathfrak{p}(\mathfrak{q}) = \mathfrak{q}$.
iv) $S_\mathfrak{p}(0)$ is contained in every $\mathfrak{p}$-primary ideal of A.
v) If $S_1 \subseteq S_2 \subseteq A$ are multiplicative submonoids, then $S_1(\mathfrak{a}) \subseteq S_2(\mathfrak{a})$.
vi) If $\mathfrak{b} \lhd A$ is an ideal containing $\mathfrak{a}$, then $S(\mathfrak{a}) \subseteq S(\mathfrak{b})$.

i): $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$ is part of (1.17.i). Since $S^{-1}\mathfrak{a} = S^{-1}A \cdot \mathfrak{a} = \mathfrak{a}^e$, by definition we have $S(\mathfrak{a}) = \left(S^{-1}\mathfrak{a}\right)^c = \mathfrak{a}^{ec}$. Now $x \in S(\mathfrak{a}) \iff x/1 \in S^{-1}\mathfrak{a} \iff \exists a \in A\ \exists s \in S\ (x/1 = a/s)$. By the definition of $S^{-1}A$, this happens if and only if there exist $t, s \in S$ and $a \in \mathfrak{a}$ such that $tsx = ta \in S \cdot \mathfrak{a} = \mathfrak{a}$. Thus $x \in S(\mathfrak{a}) \iff Sx \cap \mathfrak{a} \neq \varnothing \iff \exists s \in S\ (sx \in \mathfrak{a})$. This happens just if $x \in \bigcup_{s\in S}(\mathfrak{a} : s)$.

ii): $(0)^e = S^{-1}(0) = (0)$, so $S\big((0)\big) = (0)^{ec} = (0)^c = \phi_S^{-1}\big((0)\big) = \ker(\phi_S)$.

iii): $x \in S_\mathfrak{p}(\mathfrak{q}) \iff \exists s \in S_\mathfrak{p}\ (sx \in \mathfrak{q})$. Since $s \notin \mathfrak{p} = r(\mathfrak{q})$ and $\mathfrak{q}$ is primary, $x \in \mathfrak{q}$, so $\mathfrak{q} \subseteq \mathfrak{q}^{ec} = S_\mathfrak{p}(\mathfrak{q}) \subseteq \mathfrak{q}$.

iv): Let $\mathfrak{q}$ be $\mathfrak{p}$-primary. If $x \in S_\mathfrak{p}(0)$, there is $s \in S_\mathfrak{p}$ such that $sx = 0 \in \mathfrak{q}$. Since by definition $s \notin \mathfrak{p} = r(\mathfrak{q})$, no power of s is in $\mathfrak{q}$, so since $\mathfrak{q}$ is primary, $x \in \mathfrak{q}$.

v): If $\exists s \in S_1\ (sx \in \mathfrak{a})$, then $s \in S_2$, so $\exists s \in S_2\ (sx \in \mathfrak{a})$. By i), we have $S_1(\mathfrak{a}) \subseteq S_2(\mathfrak{a})$.

vi): Apply (1.17.iv*) twice: $\mathfrak{a} \subseteq \mathfrak{b} \implies \mathfrak{a}^e \subseteq \mathfrak{b}^e \implies S(\mathfrak{a}) = \mathfrak{a}^{ec} \subseteq \mathfrak{b}^{ec} = S(\mathfrak{b})$.

EXERCISES

If an ideal $\mathfrak{a}$ has a primary decomposition, then Spec$(A/\mathfrak{a})$ *has only finitely many irreducible components.*

Let $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ be the primary decomposition. Recall from [1.20.iv] that the irreducible components of $X =$ Spec$(A/\mathfrak{a})$ are the closed sets $V(\bar{\mathfrak{p}})$, where $\bar{\mathfrak{p}}$ is a minimal prime ideal of $A/\mathfrak{a}$. These are of the form $\bar{\mathfrak{p}} = \mathfrak{p}/\mathfrak{a}$ for primes $\mathfrak{p} \lhd A$ minimal over $\mathfrak{a}$, hence in bijection with the set of primes minimal over $\mathfrak{a}$. By (4.6), this is the set of minimal elements of the finite set of $r(\mathfrak{q}_i)$, hence finite.

If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ has no embedded prime ideals.

$\mathfrak{a} = r(\mathfrak{a}) = \bigcap\{\mathfrak{p} \in \text{Spec}(A) : \mathfrak{a} \subseteq \mathfrak{p}\}$ gives a "primary decomposition" of $\mathfrak{a}$ since prime ideals are primary (clearly, p. 50). The scare quotes are because there may be infinitely many primes. Now if we take the intersection over only the minimal primes over $\mathfrak{a}$, the intersection is clearly still $\mathfrak{a}$, and by construction there are no embedded primes. The intersection still needn't be finite however. Take for example an infinite direct product $A = \prod_{i\in I} k_i$ of fields, and for each $i \in I$ let $\mathfrak{p}_i = \{0\} \times \prod_{j\neq i} k_j$. Then $A/\mathfrak{p}_i \cong k_i$, is a field, so $\mathfrak{p}_i$ is prime, and the zero ideal (0) is the intersection of the $\mathfrak{p}_i$, but if any of these is omitted, the intersection contains non-zero elements.

[1] This is not a proposition from the book. It is original, and designed to be used in and generalize some parts of [4.10–13].

If A is absolutely flat, every primary ideal is maximal.

Let $\mathfrak{q} \lhd A$ be primary, and $\mathfrak{p} = r(\mathfrak{q})$. By [2.28], $A/\mathfrak{q}$ is absolutely flat, and every zero-divisor is nilpotent. But by [2.28] again, every non-unit is a zero-divisor, so every non-unit is nilpotent. By [1.10], it follows that $A/\mathfrak{q}$ has exactly one prime ideal; hence is a local, absolutely flat ring. But then by [2.28] yet again, $A/\mathfrak{q}$ is a field, and it follows that $\mathfrak{q}$ was maximal.

In the polynomial ring $\mathbb{Z}[t]$, the ideal $\mathfrak{m} = (2, t)$ is maximal and the ideal $\mathfrak{q} = (4, t)$ is $\mathfrak{m}$-primary, but is not a power of $\mathfrak{m}$.

$\mathbb{Z}[t]/\mathfrak{m} \cong \mathbb{Z}/(2)$ is a field, while $\mathbb{Z}[t]/\mathfrak{q} \cong \mathbb{Z}/(4)$ has all zero-divisors ($\bar{0}$ and $\bar{2}$) nilpotent, and so is primary. The radical $r(\mathfrak{q}) = r\big((4)+(t)\big) = r\big(r(4)+r(t)\big) = r(2, t) = \mathfrak{m}$ by (1.13.v,vi). The powers of $\mathfrak{m}$ are $(2, t)$, $\mathfrak{m}^2 = (4, 2t, t^2)$, etc. $\mathfrak{q}$ is contained in $\mathfrak{m}$, properly since $2 \notin \mathfrak{q}$, and contains $\mathfrak{m}^2$, again properly since $t \notin \mathfrak{m}^2$. For $n \geq 2$ we have $\mathfrak{m}^n \subseteq \mathfrak{m}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{m}$, so $\mathfrak{q}$ is not a power of $\mathfrak{m}$.

In the polynomial ring $K[x, y, z]$ where K is a field and x, y, z are independent indeterminates, let $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$, $\mathfrak{m} = (x, y, z)$; $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are prime, and $\mathfrak{m}$ is maximal. Let $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2$. Show that $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is a reduced primary decomposition of $\mathfrak{a}$. Which components are isolated and which are embedded?

Write $A = K[x, y, z]$. Now $A/\mathfrak{p}_1 \cong K[z]$ and $A/\mathfrak{p}_2 \cong K[y]$ are integral domains, and $A/\mathfrak{m} \cong K$ is a field. We have the following five equations:

$$\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 = (x, y)(x, z) = (x^2, xy, xz, yz);$$

$$\mathfrak{m}^2 = (x, y, z)(x, y, z) = (x^2, y^2, z^2, yz, xz, xy);$$

$$\mathfrak{p}_1 \cap \mathfrak{m}^2 = (x, y) \cap (x^2, y^2, z^2, yz, xz, xy) = (x^2, y^2, xz, yz, xy);$$

$$\mathfrak{p}_2 \cap \mathfrak{m}^2 = (x, z) \cap (x^2, y^2, z^2, yz, xz, xy) = (x^2, z^2, yz, xz, xy);$$

$$\mathfrak{p}_1 \cap \mathfrak{p}_2 = (x, y) \cap (x, z) = (x, yz);$$

so none of the last three pairwise intersections is $\mathfrak{a}$. On the other hand,

$$\mathfrak{p}_1 \cap (\mathfrak{p}_2 \cap \mathfrak{m}^2) = (x, y) \cap (x^2, z^2, yz, xz, xy) = (x^2, xy, yz, xz) = \mathfrak{a},$$

and $r(\mathfrak{p}_1) = \mathfrak{p}_1$, $r(\mathfrak{p}_2) = \mathfrak{p}_2$, and $r(\mathfrak{m}^2) = \mathfrak{m}$ (by (1.13.vi)) are distinct prime ideals, so this is an irredundant primary decomposition of $\mathfrak{a}$. We have $\mathfrak{p}_1 \subsetneq \mathfrak{m} \supsetneq \mathfrak{p}_2$, and $\mathfrak{p}_1 \not\subseteq \mathfrak{p}_2 \not\subseteq \mathfrak{p}_1$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are isolated and $\mathfrak{m}$ is embedded.

Let X be an infinite compact Hausdorff space, $C(X)$ the ring of real-valued continuous functions on X (Chapter 1, Exercise 26). Is the zero ideal decomposable in this ring?

No. First recall from [1.16.i] that every maximal ideal $\mathfrak{m}$ of $C(X)$ is of the form $\mathfrak{m}_x = \{f \in C(X) : f(x) = 0\}$ for some $x \in X$.

Next note that every primary ideal is contained in a unique maximal ideal. Indeed suppose $\mathfrak{a} \subseteq \mathfrak{m}_x \cap \mathfrak{m}_y$ with $x \neq y \in X$. Since X is Hausdorff, there are disjoint open neighborhoods $U \ni x$ and $V \ni y$. Since a compact Hausdorff space is normal, Urysohn's lemma can be applied. Thus there are an $f \in C(X)$ such that $f(x) = 1$ and $f(X\backslash U) = \{0\}$ and a $g \in C(X)$ such that $f(y) = 1$ while $f(X\backslash V) = \{0\}$. Since $U \cap V = \varnothing$, we see $(X\backslash U) \cup (X\backslash V) = X$, so $fg = 0 \in \mathfrak{a}$, while $f \in \mathfrak{m}_y\backslash\mathfrak{m}_x$ and $g^n \in \mathfrak{m}_x\backslash\mathfrak{m}_y$, so neither is in $\mathfrak{a}$, and thus $\mathfrak{a}$ is not primary.

Now let $\mathfrak{q}_i \subseteq \mathfrak{m}_{x_i}$ be a finite collection of primary ideals and their containing maximal ideals. What follows is due to Hao Guo [GuoEmail]; the earlier version made an unjustified assumption. Since X is infinite, there is a point x_0 not among the x_i, meaning particularly that $\mathfrak{q}_i$ is not contained in $\mathfrak{m}_{x_0}$. Each $\mathfrak{q}_i$, then, contains some f_i vanishing at x_i but not at x_0. It follows that the product of the f_i does not vanish at x_0, so this product is a nonzero element of $\prod \mathfrak{q}_i \subseteq \bigcap \mathfrak{q}_i$. As the finitely many primary ideals $\mathfrak{q}_i$ were arbitrary, there can be no primary decomposition of (0) in $C(X)$.

Let A be a ring and let $A[x]$ denote the ring of polynomials in one indeterminate over A. For each ideal $\mathfrak{a}$ of A, let $\mathfrak{a}[x]$ denote the set of all polynomials in $A[x]$ with coefficients in $\mathfrak{a}$.

i) $\mathfrak{a}[x]$ is the extension of $\mathfrak{a}$ to $A[x]$.

Identify $\mathfrak{a} \lhd A$ with its image in $A[x]$; then $\mathfrak{a}^e := \mathfrak{a}A[x] = \mathfrak{a}[x]$. Very explicitly, $\mathfrak{a} \cdot A[x] = \{\sum a_i \cdot p_i(x) : a_i \in \mathfrak{a},\ p_i(x) \in A[x]\}$, but each $a_i \cdot p_i(x)$ has all coefficients in $\mathfrak{a}$, and so is in $\mathfrak{a}[x]$; conversely, each element $\sum a_i x^i \in \mathfrak{a}[x]$ can be written as $\sum a_i \cdot p_i(x)$ for $a_i \in \mathfrak{a}$ and $p_i(x) = x^i \in A[x]$.

ii) If $\mathfrak{p}$ is a prime ideal in A, then $\mathfrak{p}[x]$ is a prime ideal in $A[x]$.

This is [2.7]. To reiterate, note that $\mathfrak{p}[x]$ is the kernel of the canonical surjection of $A[x]$ onto $(A/\mathfrak{p})[x]$, an integral domain.

iii) If $\mathfrak{q}$ is a $\mathfrak{p}$-primary ideal in A, then $\mathfrak{q}[x]$ is a $\mathfrak{p}[x]$-primary ideal in $A[x]$.

$\mathfrak{q}[x] = \mathfrak{q} + \mathfrak{q} \cdot (x)$, while $\mathfrak{p}[x] = \mathfrak{p} + \mathfrak{p} \cdot (x)$, and $r\big((x)\big) = (x)$. $\mathfrak{p}$ and $\mathfrak{q}$ can be identified with their images in $A[x]$, and in the bigger ring we still have $r(\mathfrak{q}) = \mathfrak{p} = r(\mathfrak{p})$. Then (1.13.v,iii) give

$$r\big(\mathfrak{q}[x]\big) = r\Big(r(\mathfrak{q}) + r\big(\mathfrak{q} \cdot (x)\big)\Big) = r\Big(\mathfrak{p} + r(\mathfrak{q}) \cap r\big((x)\big)\Big) = r\big(\mathfrak{p} + \mathfrak{p} \cap (x)\big) = r\big(\mathfrak{p} + \mathfrak{p} \cdot (x)\big) = r\big(\mathfrak{p}[x]\big) = \mathfrak{p}[x].$$

Now to see $\mathfrak{q}[x]$ is primary, note that the quotient $A[x]/\mathfrak{q}[x] \cong (A/\mathfrak{q})[x]$. Every zero-divisor in $A/\mathfrak{q}$ is nilpotent (p. 50). Suppose $\sum \bar{b}_i x^i = \bar{p}(x) \in (A/\mathfrak{q})[x]$ is a zero-divisor. Then by [1.2.iii], there is $\bar{a} \in A/\mathfrak{q}$ such that $\bar{a}\bar{p}(x) = 0$. This means $\bar{a} \cdot \bar{b}_i = 0$ for each i, so each $\bar{b}_i \in A/\mathfrak{q}$ is a zero-divisor, hence nilpotent. Then by [1.2.ii], $\bar{p}(x)$ is nilpotent. This shows (p. 50) that $\mathfrak{q}[x]$ is primary.

iv) If $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ is a minimal primary decomposition in A, then $\mathfrak{a}[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ is a minimal primary decomposition in $A[x]$.

$$\sum b_j x^j \in \mathfrak{a}[x] \iff \forall j\, \big(b_j \in \mathfrak{a} = \bigcap_i \mathfrak{q}_i\big) \iff \forall i\, \forall j\, (b_j \in \mathfrak{q}_i) \iff \forall i\, \big(\sum b_j x^j \in \mathfrak{q}_i[x]\big) \iff \sum b_j x^j \in \bigcap_i \mathfrak{q}_i[x],$$

so $\mathfrak{a}[x] = \bigcap_{i=1}^n \mathfrak{q}_i[x]$ as hoped. By iii), each $\mathfrak{q}_i$ is primary, so this is a primary decomposition. If we leave out some $\mathfrak{q}_j$, then the above shows $\bigcap_{i \neq j} \mathfrak{q}_i[x] = \big(\bigcap_{i \neq j} \mathfrak{q}_i\big)[x]$, which by assumption is not $\mathfrak{a}[x]$, using irredundancy of the given primary decomposition of $\mathfrak{a}$.

v) If $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$, then $\mathfrak{p}[x]$ is a minimal prime ideal of $\mathfrak{a}[x]$.

From ii), $\mathfrak{p}[x]$ is a prime ideal containing $\mathfrak{a}[x]$. If $\mathfrak{q} \in \operatorname{Spec}(A[x])$ is such that $\mathfrak{a}[x] \subseteq \mathfrak{q} \subseteq \mathfrak{p}[x]$, then taking contractions we have $\mathfrak{a} \subseteq A \cap \mathfrak{q} \subseteq \mathfrak{p}$, with $A \cap \mathfrak{q}$ prime. Since $\mathfrak{p}$ was minimal over $\mathfrak{a}$, we have $A \cap \mathfrak{q} = \mathfrak{p}$. Now $\mathfrak{p} \subseteq \mathfrak{q}$, so $\mathfrak{p}[x] = \mathfrak{p} + \mathfrak{p} \cdot (x) \subseteq \mathfrak{q}$, and thus $\mathfrak{q} = \mathfrak{p}[x]$. Thus $\mathfrak{p}[x]$ was minimal over $\mathfrak{a}[x]$.

Let k be a field. Show that in the polynomial ring $k[x_1, \ldots, x_n]$ the ideals $\mathfrak{p}_i = (x_1, \ldots, x_i)$ $(1 \leq i \leq n)$ are prime and all their powers are primary.

Write $A = k[x_1, \ldots, x_n]$. Then $A/\mathfrak{p}_i \cong k[x_{i+1}, \ldots, x_n]$ is an integral domain, so $\mathfrak{p}_i$ is prime. Now consider some power $\mathfrak{p}_i^m$. Write $\mathfrak{q}_i^m$ for its intersection with the subring $B_i = A[x_1, \ldots, x_i]$. Then $\mathfrak{p}_i^m = \mathfrak{q}_i^m[x_{i+1}, \ldots, x_n]$. By [4.7.iii], if $\mathfrak{q}_i^m$ is primary, then $\mathfrak{p}_i^m$ will also be.

So consider the quotient ring $C = B_i/\mathfrak{q}_i^m$. Write this as $C = k[y_1, \ldots, y_i]$, where the only relations $y_i = \bar{x}_i$ are (commutativity and) that any monomial in them of total degree greater than m is zero. Consider a product pq in C. If both p and q have nonzero constant term, then so does $pq \neq 0$. Any term divisible by some y_j is annihilated by $q = \prod_{j=1}^i y_j^{m-1}$, so $p \in C$ is zero-divisor if and only if its constant term is zero. If that is the case, then $p^m = 0$ since each term will have total degree $\geq m$. Thus every zero-divisor in C is nilpotent and $\mathfrak{q}_i^m$ is primary.

In a ring A, let $D(A)$ denote the set of prime ideals $\mathfrak{p}$ which satisfy the following condition: there exists $a \in A$ such that $\mathfrak{p}$ is minimal in the set of prime ideals containing $(0 : a)$. Show that $x \in A$ is a zero divisor $\iff$ $x \in \mathfrak{p}$ for some $\mathfrak{p} \in D(A)$.

If $a \neq 0$ but $xa = 0$, then $x \in (0 : a) \neq (1)$, so there exists a prime $\mathfrak{p} \supseteq (0 : a) \ni x$. By an application of Zorn's Lemma, or by [1.8] applied to $A/(0 : a)$ and (1.1), there is a minimal prime $\mathfrak{p}$ over $(0 : a)$, which then contains x.

Now suppose $x \in \mathfrak{p} \in D(A)$, with $a \in A$ such that $\mathfrak{p} \supseteq (0 : a)$ is minimal. Apparently $a \neq 0$, since otherwise $(1) = (0 : 0)$ is contained in no prime. By (1.1) and p. 9, $\bar{\mathfrak{p}} = \mathfrak{p}/(0 : a)$ is a minimal prime of $\bar{A} = A/(0 : a)$, and

$\bar{x} = x + (0 : a) \in \bar{\mathfrak{p}}$. Write $S = \bar{A}\backslash\bar{\mathfrak{p}}$. Since $\bar{\mathfrak{p}}$ is minimal, by [3.6], S is maximal in the collection Σ of multiplicative submonoids of $\bar{A}$ not containing $\bar{0}$. Let S' be the smallest submonoid of $\bar{A}$ containing $S \cup \{\bar{x}\}$; explicitly, $S' = \{s\bar{x}^n : s \in S,\ n \geq 0\}$. Since $\bar{x} \in \bar{\mathfrak{p}} = \bar{A}\backslash S$, by the maximality of S we have $S \subsetneq S' \notin \Sigma$, so $\bar{0} \in S'\backslash S$, and there are $s \in S$ and $n > 0$ with $0 = s\bar{x}^n = \bar{x}(s\bar{x}^{n-1})$, showing $\bar{x}$ is a zero-divisor in $\bar{A}$. Write $\bar{y} = s\bar{x}^{n-1} \neq 0$; then $xy \in (0 : a)$ in A. Now by assumption $\bar{y} \neq \bar{0}$, so $y \notin (0 : a)$, and thus $ay \neq 0$. But since $xy \in (0 : a)$ we have $0 = xya = x(ay)$, so x is a zero-divisor in A.

Let S be a multiplicatively closed subset of A, and identify $\operatorname{Spec}(S^{-1}A)$ *with its image in* $\operatorname{Spec}(A)$ *(Chapter 3, Exercise 21). Show that*

$$D(S^{-1}A) = D(A) \cap \operatorname{Spec}(S^{-1}A).$$

Write $\mathfrak{a}^e = S^{-1}\mathfrak{a}$ for the extension of $\mathfrak{a} \lhd A$ along the canonical $\phi_S \colon A \to S^{-1}A$ and $X = \operatorname{Spec}(A)$, $S^{-1}X = \{x \in \operatorname{Spec}(A) : \mathfrak{p}_x \cap S = \varnothing\}$. If $x \in X \setminus S^{-1}X$, then $\mathfrak{p}_x^e = (1)$, so not a prime and not in $D(S^{-1}A)$. So evidently $D(S^{-1}A) \subseteq S^{-1}X$. From now on suppose $\mathfrak{p} \in S^{-1}X$.

Let $x \in A$. Then (x) is finitely generated, so by (3.15) we have

$$\operatorname{Ann}(x)^e = S^{-1}\operatorname{Ann}(x) = S^{-1}\big((0) : (x)\big) = \big(S^{-1}(0) : S^{-1}(x)\big) = \operatorname{Ann}\big(S^{-1}(x)\big) = \operatorname{Ann}(x/1).$$

Now for any $x \in A$ and $s \in S$ we have $\operatorname{Ann}(x/s) = \operatorname{Ann}(x/1)$ since $ax/ts = 0 \iff \exists u \in S\ (uax = 0 \in A) \iff ax/s = 0$.

Now every ideal of $S^{-1}A$ is extended by (3.11.i), so $S^{-1}\mathfrak{p} \in D(S^{-1}A) \iff \exists x \in A$ such that $S^{-1}\mathfrak{p}$ is minimal over $\operatorname{Ann}(x/1) = S^{-1}\operatorname{Ann}(x) =$. Contracting both sides $\mathfrak{p} = \mathfrak{p}^{ec} \supseteq \operatorname{Ann}(x)^{ec} \supseteq \operatorname{Ann}(x)$. If there were an intermediate prime $\mathfrak{q}$ such that $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$, then extending, $\mathfrak{a}^e \subseteq \mathfrak{q}^e \subseteq \mathfrak{p}^e$, so $\mathfrak{q}^e = \mathfrak{p}^e$, and by (3.11.iv), $\mathfrak{q} = \mathfrak{p}$. Thus $\mathfrak{p} \in D(A)$.

On the other hand, suppose $\mathfrak{p} \in D(A) \cap S^{-1}X$ is minimal over $\mathfrak{a} = \operatorname{Ann}(x)$. Then $\operatorname{Ann}(x/1) = S^{-1}\mathfrak{a} \subseteq S^{-1}\mathfrak{p}$. If $S^{-1}\mathfrak{q}$ is such that $S^{-1}\mathfrak{a} \subseteq S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{p}$, then by (3.11.iv), $\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p}$, so by assumption $\mathfrak{q} = \mathfrak{p}$ and $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{p}$. Thus $S^{-1}\mathfrak{p}$ is minimal over $S^{-1}\mathfrak{a}$, so $S^{-1}\mathfrak{p} \in D(S^{-1}A)$.

If the zero ideal has a primary decomposition, show that $D(A)$ is the set of associated prime ideals of 0.

Let the primary decomposition be $(0) = \bigcap \mathfrak{q}_i$. Then (4.5) and (4.7) say that $\mathfrak{p}_i = r(\mathfrak{q}_i)$ are the ideals $r(0 : x)$ for $x \in A$, so the (finite) set of ideals $r(0 : x)$ are those primes associated to (0). But each $r(0 : x)$ is minimal over $(0 : x)$, so in $D(A)$.

For any prime ideal $\mathfrak{p}$ in a ring A, let $S_\mathfrak{p}(0)$ denote the kernel of the homomorphism $A \to A_\mathfrak{p}$. Prove that

i) $S_\mathfrak{p}(0) \subseteq \mathfrak{p}$.

Since $(0) \subseteq \mathfrak{p}$, (4.12*.i), (4.12*.vi) twice, and (3.13) give $S_\mathfrak{p}(0) = (0)^{ec} \subseteq \mathfrak{p}^{ec} = \mathfrak{p}$.[2]

ii) $r\big(S_\mathfrak{p}(0)\big) = \mathfrak{p} \iff \mathfrak{p}$ is a minimal prime ideal of A.

Taking r of i), we see $r\big(S_\mathfrak{p}(0)\big) \subseteq \mathfrak{p}$ regardless of minimality.

Now write $S = A\backslash\mathfrak{p}$. By (4.12*.i) or [3.1], $S_\mathfrak{p}(0) = \{x \in A : \exists s \in S\ (sx = 0)\} = \bigcup_{s\in S} \operatorname{Ann}(s)$. Thus

$$\begin{aligned}
\mathfrak{p} \subseteq r\big(S_\mathfrak{p}(0)\big) = r\big(\textstyle\bigcup_{s\in S}\operatorname{Ann}(s)\big) \overset{\text{p. 9}}{=} \textstyle\bigcup_{s\in S} r\big(\operatorname{Ann}(s)\big) &\iff \text{for each } x \in \mathfrak{p} \text{ there are } n > 0 \text{ and } s \in S \text{ such that } sx^n = 0\\
&\iff \forall x \in \mathfrak{p},\ 0 \in (\text{smallest submonoid containing } S \cup \{x\})\\
&\iff S \text{ is maximal among multiplicative submonoids } T \not\ni 0 \text{ of } A\\
&\underset{[3.6]}{\iff} \mathfrak{p} \text{ is minimal.}
\end{aligned}$$

iii) If $\mathfrak{p} \supseteq \mathfrak{p}'$, then $S_\mathfrak{p}(0) \subseteq S_{\mathfrak{p}'}(0)$.

Since $\mathfrak{p} \supseteq \mathfrak{p}' \iff S_\mathfrak{p} \subseteq S_{\mathfrak{p}'}$, this follows from (4.12*.v).

iv) $\bigcap_{\mathfrak{p}\in D(A)} S_\mathfrak{p}(0) = 0$, where $D(A)$ is defined in Exercise 9.

Obviously, 0 is in each $S_\mathfrak{p}(0)$. On the other hand, if $x \neq 0$, then $(0 : x) \neq (1)$, and there is a prime $\mathfrak{p}$ minimal over $(0 : x)$; by definition, $\mathfrak{p} \in D(A)$. Since $(0 : x) \subseteq \mathfrak{p}$, there is no $s \in A\backslash\mathfrak{p}$ such that $sx = 0$, and so [3.1] says $x \notin S_\mathfrak{p}(0)$.

[2] Alternately, suppose $x \in S_\mathfrak{p}(0)$; by (4.12*.i), there is $s \in S_\mathfrak{p}$ such that $sx = 0 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and doesn't contain s, we must have $x \in \mathfrak{p}$.

If $\mathfrak{p}$ is a minimal prime ideal of a ring A, show that $S_{\mathfrak{p}}(0)$ (Exercise 10) is the smallest $\mathfrak{p}$-primary ideal.

Write $\mathfrak{q} = S_{\mathfrak{p}}(0)$. Using minimality of $\mathfrak{p}$ and [4.10.ii], $r(\mathfrak{q}) = \mathfrak{p}$. To see $\mathfrak{q}$ is primary, suppose $xy \in \mathfrak{q}$. Then there is $n > 0$ such that $x^n y^n = (xy)^n \in \mathfrak{p}$. If $x \notin \mathfrak{q}$, then $x^n \notin \mathfrak{p}$ for all n, so $y^n \in \mathfrak{p} = r(\mathfrak{q})$, and there exists $m > 0$ such that $y^{mn} = (y^n)^m \in \mathfrak{q}$. Thus $\mathfrak{q}$ is primary.

Let $\mathfrak{a}$ be the intersection of the ideals $S_{\mathfrak{p}}(0)$ as $\mathfrak{p}$ runs through the minimal prime ideals of A. Show that $\mathfrak{a}$ is contained in the nilradical of A.

Let $P \subseteq \operatorname{Spec}(A)$ be the set of minimal prime ideals. Since all primes contains a member of P, we have, by (1.8), that $\mathfrak{N} = \bigcap P$. Now for each $\mathfrak{p} \in P$ we have $S_{\mathfrak{p}}(0) \subseteq \mathfrak{p}$ by [4.10.i], so $\mathfrak{a} := \bigcap_{\mathfrak{p} \in P} S_{\mathfrak{p}}(0) \subseteq \bigcap P = \mathfrak{N}$.

Suppose that the zero ideal is decomposable. Prove that $\mathfrak{a} = 0$ if and only if every prime ideal of 0 is isolated.

If (0) is decomposable, then (4.6) states each minimal prime ideal is a minimal ideal of (0) (and vice versa). Moreover, there are only finitely many prime ideals of (0). If every prime ideal of (0) is isolated, then all are minimal, and so $(0) = \bigcap\{\text{primes of } (0)\} = \bigcap P = \mathfrak{N}$, forcing $\mathfrak{a} = 0$.

On the other hand, suppose $\mathfrak{a} = 0$. Then $0 = \mathfrak{a} = \bigcap\{S_{\mathfrak{p}}(0) : \mathfrak{p} \in P\}$ gives a primary decomposition of (0). We may discard all but finitely many terms to obtain an irredundant decomposition. Now if (0) had an embedded prime $\mathfrak{P}$ containing an isolated prime $\mathfrak{p}$, we would have $S_{\mathfrak{P}}(0) \subseteq S_{\mathfrak{p}}(0)$ by [4.10.iii], contradicting irredundancy.

Let A be a ring, S a multiplicatively closed subset of A. For any ideal $\mathfrak{a}$, let $S(\mathfrak{a})$ denote the contraction of $S^{-1}\mathfrak{a}$ in A. The ideal $S(\mathfrak{a})$ is called the saturation *of $\mathfrak{a}$ with respect to S. Prove that*

i) $S(\mathfrak{a}) \cap S(\mathfrak{b}) = S(\mathfrak{a} \cap \mathfrak{b})$.

Note that $\mathfrak{a}^e \cap \mathfrak{b}^e = S^{-1}\mathfrak{a} \cap S^{-1}\mathfrak{b} = S^{-1}(\mathfrak{a} \cap \mathfrak{b}) = (\mathfrak{a} \cap \mathfrak{b})^e$ by (4.12*.i) and (3.11.v). Then recalling (1.18), $S(\mathfrak{a}) \cap S(\mathfrak{b}) = \mathfrak{a}^{ec} \cap \mathfrak{b}^{ec} = (\mathfrak{a}^e \cap \mathfrak{b}^e)^c = (\mathfrak{a} \cap \mathfrak{b})^{ec} = S(\mathfrak{a} \cap \mathfrak{b})$.[3][4]

ii) $S\big(r(\mathfrak{a})\big) = r\big(S(\mathfrak{a})\big)$. By (1.18), contraction commutes with r, and by (3.11.v), extension S^{-1} does.Therefore by (4.12*.i), $S\big(r(\mathfrak{a})\big) = r(\mathfrak{a})^{ec} = \big(r(\mathfrak{a}^e)\big)^c = r(\mathfrak{a}^{ec}) = r\big(S(\mathfrak{a})\big)$.[5]

iii) $S(\mathfrak{a}) = (1) \iff \mathfrak{a}$ meets S.

$S(\mathfrak{a}) = (1) \iff 1 \in S(\mathfrak{a}) \iff \exists s \in S\ (s = s \cdot 1 \in \mathfrak{a}) \iff \mathfrak{a} \cap S \neq \varnothing$.

iv) $S_1\big(S_2(\mathfrak{a})\big) = (S_1 S_2)(\mathfrak{a})$.

If $x \in (S_1 S_2)(\mathfrak{a})$, then there are $s_1 \in S_1$ and $s_2 \in S_2$ such that $s_1 s_2 x \in \mathfrak{a}$. Then $s_1 x \in S_2(\mathfrak{a})$, and $x \in S_1\big(S_2(\mathfrak{a})\big)$. On the other hand, if $x \in S_1\big(S_2(\mathfrak{a})\big)$, then there is $s_1 \in S_1$ such that $s_1 x \in S_2(\mathfrak{a})$, so there is $s_2 \in S_2$ such that $s_2 s_1 x \in \mathfrak{a}$, and then $x \in (S_1 S_2)(\mathfrak{a})$.

If $\mathfrak{a}$ has a primary decomposition, prove that the set of ideals $S(\mathfrak{a})$ (where S runs through all multiplicatively closed subsets of A) is finite.

Let the decomposition be $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$. By (4.9), $S(\mathfrak{a})$ is determined entirely by which of the $\mathfrak{p}_i = r(\mathfrak{q}_i)$ it meets. This yields at most 2^n different possibilities for $S(\mathfrak{a})$. (Make at most n possible choices of “empty” or “non-empty,” one for each intersection $S \cap \mathfrak{p}_i$.)

*Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Then n*th symbolic power of $\mathfrak{p}$ *is defined to be the ideal (in the notation of Exercise 12)*

$$\mathfrak{p}^{(n)} = S_{\mathfrak{p}}(\mathfrak{p}^n)$$

where $S_{\mathfrak{p}} = A \backslash \mathfrak{p}$. Show that

i) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal;

[3] Alternately, suppose that $x \in S(\mathfrak{a} \cap \mathfrak{b})$. Then there is $s \in S$ such that $sx \in \mathfrak{a} \cap \mathfrak{b}$, so $sx \in \mathfrak{a}$ and $sx \in \mathfrak{b}$, meaning $x \in S(\mathfrak{a})$ and $x \in S(\mathfrak{b})$; thus $x \in S(\mathfrak{a}) \cap S(\mathfrak{b})$. Now suppose $x \in S(\mathfrak{a}) \cap S(\mathfrak{b})$. Then there are $s,\, t \in S$ such that $sx \in \mathfrak{a}$ and $tx \in \mathfrak{b}$. Then $t(sx) \in t\mathfrak{a} \subseteq \mathfrak{a}$ and $s(tx) \in s\mathfrak{b} \subseteq \mathfrak{b}$, so $(st)x \in \mathfrak{a} \cap \mathfrak{b}$. Thus $x \in S(\mathfrak{a} \cap \mathfrak{b})$.

[4] Note that (4.12*.vi) follows: if $\mathfrak{a} \subseteq \mathfrak{b}$, then $S(\mathfrak{a}) \cap S(\mathfrak{b}) = S(\mathfrak{a} \cap \mathfrak{b}) = S(\mathfrak{a})$, so $S(\mathfrak{a}) \subseteq S(\mathfrak{b})$.

[5] Alternately, if $x \in S\big(r(\mathfrak{a})\big)$, then there is $s \in S$ such that $sx \in r(\mathfrak{a})$, so there is $n > 0$ such that $s^n x^n = (sx)^n \in \mathfrak{a}$. Then since $s^n \in S$ we have $x^n \in S(\mathfrak{a})$, so $x \in r(S(\mathfrak{a}))$. If $x \in r(S(\mathfrak{a}))$, then there is $n > 0$ such that $x^n \in S(\mathfrak{a})$, so there is $s \in S$ such that $sx^n \in \mathfrak{a}$. Then $(sx)^n = s^{n-1}(sx) \in \mathfrak{a}$ as well, so $sx \in r(\mathfrak{a})$ and $x \in S\big(r(\mathfrak{a})\big)$.

(3.13) shows $\mathfrak{p}^e$ is maximal, so by (4.2) $(\mathfrak{p}^e)^n$ is primary. By (3.11.v), $(\mathfrak{p}^e)^n = (\mathfrak{p}^n)^e$. Since contraction preserves being primary (p. 50) and $\mathfrak{p}^{(n)} = (\mathfrak{p}^n)^{ec}$ by (4.12*.i), it follows $\mathfrak{p}^{(n)}$ is primary.[6] As for the radical,

$$r(\mathfrak{p}^{(n)}) \overset{(4.12^*.\text{i})}{=} r\big((\mathfrak{p}^n)^{ec}\big) \overset{(1.18)}{=} \big(r(\mathfrak{p}^n)^e\big)^c \overset{(3.11.\text{v})}{=} r(\mathfrak{p}^n)^{ec} \overset{(1.13.\text{vi})}{=} \mathfrak{p}^{ec} \overset{(3.13)}{=} \mathfrak{p}.$$

ii) if $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component;

First, $\mathfrak{p}^{(n)}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$. If $\mathfrak{q} \supseteq \mathfrak{p}^n$ is $\mathfrak{p}$-primary and $x \in \mathfrak{p}^{(n)}$, then by (4.12*.i) there is $s \in S_\mathfrak{p}$ such that $xs \in \mathfrak{p}^n \subseteq \mathfrak{q}$. Since $s \notin r(\mathfrak{q}) = \mathfrak{p}$, we have $s^m \notin \mathfrak{q}$ for all m; as $\mathfrak{q}$ is primary, it follows that $x \in \mathfrak{q}$. Thus $\mathfrak{p}^{(n)} \subseteq \mathfrak{q}$.

Let $\bigcap \mathfrak{q}_i = \mathfrak{p}^n$ be a primary decomposition. Then by (1.13.vi,iii), $\mathfrak{p} = r(\mathfrak{p}^n) = r\big(\bigcap \mathfrak{q}_i\big) = \bigcap r(\mathfrak{q}_i)$. By (1.11.ii), $\mathfrak{p} = r(\mathfrak{q}_i)$ for some $\mathfrak{q} = \mathfrak{q}_i$. Thus $\mathfrak{p}$ definitely is a prime of $\mathfrak{p}^n$. If we had $r(\mathfrak{q}_j) \subsetneq \mathfrak{p}$ for some j, we would have $\mathfrak{p} = \bigcap r(\mathfrak{q}^l) \subseteq r(\mathfrak{q}_j) \subsetneq \mathfrak{p}$, a contradiction; thus $\mathfrak{p}$ is isolated. Since $\mathfrak{p}^{(n)}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$, $\mathfrak{p}^n = \mathfrak{p}^{(n)} \cap_{j \neq i} \mathfrak{q}_i$ is also a primary decomposition; but by the uniqueness (4.11) of isolated primary components, it follows $\mathfrak{q}_i = \mathfrak{p}^{(n)}$.

iii) If $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ has a primary decomposition, then $\mathfrak{p}^{(m+n)}$ is its $\mathfrak{p}$-primary component;

First show $\mathfrak{p}^{(m+n)}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$. Let $\mathfrak{q} \supseteq \mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ be $\mathfrak{p}$-primary, and $x \in \mathfrak{p}^{(m+n)}$. Then there is $s \in S_\mathfrak{p}$ such that $xs \in \mathfrak{p}^{m+n} = \mathfrak{p}^m\mathfrak{p}^n \subseteq \mathfrak{p}^{(m)}\mathfrak{p}^{(n)} \subseteq \mathfrak{q}$. Since $s \notin r(\mathfrak{q}) = \mathfrak{p}$ and $\mathfrak{q}$ is primary, it follows that $x \in \mathfrak{q}$. Thus $\mathfrak{p}^{(m+n)} \subseteq \mathfrak{q}$.

Now suppose $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)} = \bigcap \mathfrak{q}_i$ is a primary decomposition. Since $r(\mathfrak{p}^{(m)}) = r(\mathfrak{p}^{(n)}) = \mathfrak{p}$, it follows from (1.13.iii,vi) that $r(\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}) = r(\mathfrak{p}^{(m)}) \cap r(\mathfrak{p}^{(n)}) = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$. As in part ii), $\mathfrak{p} = r(\mathfrak{q}_i)$ for some i, so $\mathfrak{p}$ is a prime of $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$, and since the radical is not a proper subset of $\mathfrak{p}$, we know $\mathfrak{p}$ is isolated. Since $\mathfrak{p}^{(m+n)}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$, by (4.11) it follows $\mathfrak{p}^{(m+n)}$ is the uniquely determined $\mathfrak{p}$-primary component of $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$.

iv) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \iff \mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

N.B. The book has a misprint here: by part i), $\mathfrak{p}^{(n)}$ is *always* $\mathfrak{p}$-primary, so the condition should be that $\mathfrak{p}^n$ is $\mathfrak{p}$-primary.

Suppose $\mathfrak{p}^{(n)} = \mathfrak{p}^n$. Then since $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary by i), $\mathfrak{p}^n$ is $\mathfrak{p}$-primary. On the other hand suppose $\mathfrak{p}^n$ is $\mathfrak{p}$-primary. Then $\mathfrak{p}^n = \bigcap\{\mathfrak{p}^n\}$ gives a trivial primary decomposition, so by the first uniqueness theorem (4.5), $\mathfrak{p}$ is the only prime of $\mathfrak{p}^n$. By part ii), $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component of $\mathfrak{p}^n$, so we conclude $\mathfrak{p}^{(n)} = \mathfrak{p}^n$.

Let $\mathfrak{a}$ be a decomposable ideal in a ring A and let $\mathfrak{p}$ be a maximal element of the set of ideals $(\mathfrak{a} : x)$, where $x \in A$ and $x \notin \mathfrak{a}$. Show that $\mathfrak{p}$ is a prime ideal belonging to $\mathfrak{a}$.

First, let $\mathfrak{q}$ be $\mathfrak{p}'$-primary and $x \notin \mathfrak{q}$, so $(\mathfrak{q} : x)$ is a $\mathfrak{p}'$-primary ideal by (4.4.ii). Suppose x is such that $(\mathfrak{q} : x)$ is maximal among all ideals of this form. Let $y \in A \backslash (\mathfrak{q} : x) \subseteq A \backslash \mathfrak{q}$. Using (1.12.i,iii) we have $(\mathfrak{q} : x) \subseteq \big((\mathfrak{q} : x) : y\big) = (\mathfrak{q} : xy)$, and this last is $\mathfrak{p}'$-primary by (4.4.ii) since we assumed $xy \notin \mathfrak{q}$. As we are assuming $(\mathfrak{q} : x)$ maximal of this form, $(\mathfrak{q} : xy) = (\mathfrak{q} : x)$, so for every $z \in A$, $xyz \in \mathfrak{q} \implies xz \in \mathfrak{q}$. Taking $z = y^n$, $xy^{n+1} \in \mathfrak{q} \implies xy^n \in \mathfrak{q}$, and stringing these together, $xy^n \in \mathfrak{q} \implies x \in \mathfrak{q}$. But we assumed $x \notin \mathfrak{q}$, so that there is no power y^n of y such that $y^n \in (\mathfrak{q} : x)$, or in other words $y \notin r(\mathfrak{q} : x) = \mathfrak{p}'$. Summarizing, $y \in A \backslash (\mathfrak{q} : x) \implies y \in A \backslash \mathfrak{p}'$, or $\mathfrak{p}' \subseteq (\mathfrak{q} : x)$. But by assumption $(\mathfrak{q} : x) \subseteq \mathfrak{p}'$, so a maximal ideal of the form $(\mathfrak{q} : x)$, if such exists, is equal to $r(\mathfrak{q})$.

Now write $\mathfrak{a} = \bigcap_{i=1}^n \mathfrak{q}_i$ for an irredundant primary decomposition, and set $\mathfrak{p}_i = r(\mathfrak{q}_i)$.Suppose $x \in A$ is such that $(\mathfrak{a} : x)$ is maximal among such ideals. (1.12.iv) gives $(\mathfrak{a} : x) = \big(\bigcap \mathfrak{q}_i : x\big) = \bigcap (\mathfrak{q}_i : x)$, and (4.4) shows each $(\mathfrak{q}_i : x)$ is (1) or is $\mathfrak{p}_i$-primary. We can make any set of $(\mathfrak{q}_i : x) = (1)$, $i \in I$, by taking $x \in \bigcap_{i \in I} \mathfrak{q}_i$, so if $(\mathfrak{a} : x)$ is maximal, while still $(\mathfrak{a} : x) \neq (1)$ ($\iff x \notin \mathfrak{a}$), we have all but one $(\mathfrak{q}_i : x) = (1)$, and $(\mathfrak{q}_i : x)$ maximal among such proper ideals. The preceding paragraph shows this happens if and only if $(\mathfrak{a} : x) = (\mathfrak{q}_i : x) = \mathfrak{p}_i$, a prime ideal belonging to $\mathfrak{a}$.

Let $\mathfrak{a}$ be a decomposable ideal in a ring A, let Σ be an isolated set of prime ideals belonging to $\mathfrak{a}$, and let $\mathfrak{q}_\Sigma$ be the intersection of the corresponding primary components. Let f be an element of A such that, for each prime ideal $\mathfrak{p}$ belonging to $\mathfrak{a}$, we have $f \in \mathfrak{p} \iff \mathfrak{p} \notin \Sigma$, and let S_f be the set of all powers of f. Show that $\mathfrak{q}_\Sigma = S_f(\mathfrak{a}) = (\mathfrak{a} : f^n)$ for all large n.

Note that the solution itself doesn't explicitly use that Σ is composed of isolated primes of $\mathfrak{a}$. I think the assumption is only needed because if one has an isolated prime $\mathfrak{p}$ contained in an embedded prime $\mathfrak{P}$ with $\mathfrak{p} \notin \Sigma$ and $\mathfrak{P} \in \Sigma$, it's not possible to require $f \in \mathfrak{p} \notin \Sigma$ but $f \notin \mathfrak{P} \in \Sigma$.

[6] Alternately, suppose $xy \in \mathfrak{p}^{(n)}$; we will show $x \in \mathfrak{p}^{(n)}$ or $y \in r(\mathfrak{p}^{(n)})$. There is $s \in S_\mathfrak{p}$ such that $sxy \in \mathfrak{p}^n$. If $x \notin \mathfrak{p}^{(n)}$, then $sx \notin \mathfrak{p}^n$, so the highest possible power of $\mathfrak{p}$ containing sx is $\mathfrak{p}^{n-1}$. Then, using (1.13.vi), we must have $y \in \mathfrak{p} = r(\mathfrak{p}^n)$.

$(\mathfrak{a}:f^n)\subseteq S_f(\mathfrak{a})$: By definition, $S_f(\mathfrak{a})=\{x\in A:\exists f^n\in S_f\ (f^n x\in\mathfrak{a})\}=\bigcup_{n\geq 0}(\mathfrak{a}:f^n)$.

$S_f(\mathfrak{a})=\mathfrak{q}_\Sigma$: Fix a primary decomposition $\mathfrak{a}=\bigcap_{i=1}^m\mathfrak{q}_i$, with $\mathfrak{p}_i=r(\mathfrak{q}_i)$, such that $\Sigma=\{\mathfrak{p}_1,\ldots,\mathfrak{p}_p\}$.[7] [8] Since $\mathfrak{p}_i$ are prime, we have $S_f\cap\mathfrak{p}_i\neq\varnothing$ just if $f\in\mathfrak{p}_i$ just if $\mathfrak{p}_i\notin\Sigma$, so S_f meets $\mathfrak{p}_{p+1},\ldots,\mathfrak{p}_m$ but no others. Then (4.9) says $S_f(\mathfrak{a})=\bigcap_{i=1}^p\mathfrak{q}_i=\mathfrak{q}_\Sigma$.

$\exists n\geq 0\ \big(\mathfrak{q}_\Sigma\subseteq(\mathfrak{a}:f^n)\big)$: Since by (1.12.iv) we have $(\mathfrak{a}:f^n)=\bigcap(\mathfrak{q}_i:f^n)$, we are looking for n large enough that for each i and each $x\in\mathfrak{q}_\Sigma$ we have $f^n x\in\mathfrak{q}_i$. In case $\mathfrak{p}_i\in\Sigma$, we already have $f^0x=x\in\mathfrak{q}_\Sigma\subseteq\mathfrak{q}_i$. For $\mathfrak{p}_i\notin\Sigma$, we have by the definition of f that $f\in\mathfrak{p}_i=r(\mathfrak{q}_i)$. Thus there is $n_i\geq 1$ such that $f_i^{n_i}\in\mathfrak{q}_i$. Taking $n=\max_i n_i$ we then have $f^n x\in\mathfrak{q}_i$ for all i.

If A is a ring in which every ideal has a primary decomposition, show that every ring of fractions $S^{-1}A$ has the same property.

Recall from (3.11.i,ii) that every proper ideal of $S^{-1}A$ is an extended ideal $S^{-1}\mathfrak{a}$ for some $\mathfrak{a}\lhd A$ with $S\cap\mathfrak{a}=\varnothing$. So let a proper ideal $S^{-1}\mathfrak{a}\lhd S^{-1}A$ be given, and let $\mathfrak{a}=\bigcap\mathfrak{q}_i$ be a primary decomposition of $\mathfrak{a}$. By (3.11.v) we then have $S^{-1}\mathfrak{a}=S^{-1}\big(\bigcap\mathfrak{q}_i\big)=\bigcap S^{-1}\mathfrak{q}_i$. But by (4.8) that the proper primary ideals of $S^{-1}A$ are exactly those ideals of the form $S^{-1}\mathfrak{q}$ with $\mathfrak{q}$ primary in A such that $S\cap r(\mathfrak{q})=\varnothing$, so $\bigcap S^{-1}\mathfrak{q}_i$, perhaps omitting a few $\mathfrak{q}_i$ that meet S, is a primary decomposition of $S^{-1}\mathfrak{a}$.

Let A be a ring with the following property.

(L1) For every ideal $\mathfrak{a}\neq(1)$ in A and every prime ideal $\mathfrak{p}$, there exists $x\notin\mathfrak{p}$ such that $S_\mathfrak{p}(\mathfrak{a})=(\mathfrak{a}:x)$, where $S_\mathfrak{p}=A\backslash\mathfrak{p}$.

Then every ideal in A is an intersection of (possibly infinitely many) primary ideals.

For future overuse, we state and prove a slight generalization of a result of [4.11]: if $\mathfrak{a}\neq(1)$ is an ideal of A and $\mathfrak{p}$ is a prime ideal minimal over $\mathfrak{a}$, then $\mathfrak{q}=S_\mathfrak{p}(\mathfrak{a})$ is a $\mathfrak{p}$-primary ideal. To prove this, note that in the ring $A/\mathfrak{a}$, $\mathfrak{p}/\mathfrak{a}$ is a minimal prime, and [4.11] gives that $\bar{\mathfrak{q}}=S_{\mathfrak{p}/\mathfrak{a}}(\bar 0)$ is $\mathfrak{p}/\mathfrak{a}$-primary. We claim that $\bar{\mathfrak{q}}=\mathfrak{q}/\mathfrak{a}$, so that $\mathfrak{q}$, being the contraction of a primary ideal, is primary, by a remark on p. 50. Indeed, if $sx\in\mathfrak{a}$ for $s\in S_\mathfrak{p}$, then $\bar s\bar x=\bar 0$, where $\bar s\in S_{\mathfrak{p}/\mathfrak{a}}=(A/\mathfrak{a})\backslash(\mathfrak{p}/\mathfrak{a})$, the image of $A\backslash\mathfrak{p}$. On the other hand, if $\bar s\bar x=\bar 0$, with $\bar s\in S_{\mathfrak{p}/\mathfrak{a}}$, then $(s+\mathfrak{a})(x+\mathfrak{a})\subseteq\mathfrak{a}$, so $sx\in\mathfrak{a}$. Finally $r(\bar{\mathfrak{q}})=\mathfrak{p}/\mathfrak{a}$, so using the exercise (1.18) on contraction (along $A\to A/\mathfrak{a}$), $r(\mathfrak{q})=r(\bar{\mathfrak{q}}^c)=(r(\bar{\mathfrak{q}}))^c=(\mathfrak{p}/\mathfrak{a})^c=\mathfrak{p}$, so $\mathfrak{q}$ is $\mathfrak{p}$-primary as claimed.[9] [10]

Let $\mathfrak{p}_0$ be minimal over $\mathfrak{a}_0:=\mathfrak{a}$, and set $\mathfrak{q}_0:=S_{\mathfrak{p}_0}(\mathfrak{a}_0)$. By the above paragraph $\mathfrak{q}_0$ is $\mathfrak{p}_0$-primary and by (L1), there is $x_0\notin\mathfrak{p}_0$ such that $\mathfrak{q}_0=(\mathfrak{a}_0:x_0)$.

We claim $\mathfrak{a}_0=\mathfrak{q}_0\cap[\mathfrak{a}_0+(x_0)]$. Indeed, $\mathfrak{a}_0\subseteq\mathfrak{q}_0$ and $\mathfrak{a}_0\subseteq\mathfrak{a}_0+(x_0)$. On the other hand let $a_0+b_0x_0\in\mathfrak{a}_0+(x_0)$ be arbitrary. If it is also in $\mathfrak{q}_0=(\mathfrak{a}_0:x_0)$, then $x_0(a_0+b_0x_0)=a_0x_0+b_0x_0^2\in\mathfrak{a}_0$, implying $b_0x_0^2\in\mathfrak{a}_0\subseteq\mathfrak{q}_0$. Since $x_0^{2n}\notin\mathfrak{p}_0\supseteq\mathfrak{q}_0$, which is primary, we have $b_0\in\mathfrak{q}_0=(\mathfrak{a}_0:x_0)$, so $b_0x_0\in\mathfrak{a}_0$ and hence $a_0+b_0x_0\in\mathfrak{a}_0$.

Since this is so, there is an ideal $\mathfrak{a}_1\supseteq\mathfrak{a}_0+(x_0)$ maximal with respect to the requirement that $\mathfrak{q}_0\cap\mathfrak{a}_1=\mathfrak{a}_0$. Suppose $\mathfrak{a}_1\neq(1)$. Then there is a prime ideal $\mathfrak{p}_1$ minimal among those containing $\mathfrak{a}_1$, and $\mathfrak{q}_1:=S_{\mathfrak{p}_1}(\mathfrak{a}_1)$ is $\mathfrak{p}_1$-primary. By (L1), $\mathfrak{q}_1=(\mathfrak{a}_1:x_1)$ for some $x_1\notin\mathfrak{p}_1$. By the same argument as the previous paragraph, replacing every subscript 0 by a 1, we see $\mathfrak{a}_1=\mathfrak{q}_1\cap[\mathfrak{a}_1+(x_1)]$. Then $\mathfrak{a}_0=\mathfrak{q}_0\cap\mathfrak{a}_1=\mathfrak{q}_0\cap\mathfrak{q}_1\cap[\mathfrak{a}_1+(x_1)]$.

We continue this process of producing $\mathfrak{q}_\alpha$ by transfinite induction. For the "successor" step, suppose we have $\mathfrak{a}_0=[\mathfrak{a}_\alpha+(x_\alpha)]\cap\bigcap_{\beta\leq\alpha}\mathfrak{q}_\beta$ for some ordinal α and some primary ideals $\mathfrak{q}_\beta$ and $\mathfrak{a}_\alpha\nsubseteq r(\mathfrak{q}_\beta)$ for any $\beta<\alpha$. If $\mathfrak{a}_\alpha\neq(1)$, then as above there is $\mathfrak{a}_{\alpha+1}$ containing $\mathfrak{a}_\alpha+(x_\alpha)$, maximal subject to the constraint that $\mathfrak{a}_0=\mathfrak{a}_{\alpha+1}\cap\bigcap_{\beta\leq\alpha}\mathfrak{q}_\beta$. Take $\mathfrak{p}_{\alpha+1}$ a minimal prime over $\mathfrak{a}_{\alpha+1}$, so that $\mathfrak{q}_{\alpha+1}=S_{\mathfrak{p}_{\alpha+1}}(\mathfrak{a}_{\alpha+1})$ is $\mathfrak{p}_{\alpha+1}$-primary. By (L1) there is $x_{\alpha+1}\notin\mathfrak{p}_{\alpha+1}$ such that

[7] This paragraph adapted from Yimu Yin's solution: `http://pitt.edu/~yimuyin/research/AandM/exercises04.pdf`

[8] Here is a divergent, worse proof of $S_f(\mathfrak{a})\subseteq\mathfrak{q}_\Sigma$ that I came up with before looking up others' solutions. Assume $x\in S_f(\mathfrak{a})$. By [4.12.i], $S_f(\mathfrak{a})=\bigcap S_f(\mathfrak{q}_i)$, so there are $n_i\geq 0$ such that $f^{n_i}x\in S_f(\mathfrak{q}_i)$ for each i. Since $\mathfrak{q}_i$ is primary, we have $x\in\mathfrak{q}_i$ or $(f^{n_i})^{m_i}\in\mathfrak{q}_i$ for some $n_i\geq 0$, meaning $f\in r(\mathfrak{q}_i)=\mathfrak{p}_i$. By assumption $f\in\mathfrak{p}_i\iff\mathfrak{p}_i\notin\Sigma$, so for each $\mathfrak{q}_i$ with $\mathfrak{p}_i\in\Sigma$ we have $x\in\mathfrak{q}_i$. Thus $x\in\mathfrak{q}_\Sigma$.

[9] We can arguably simplify the situation of the problem slightly by replacing A with $A/\mathfrak{a}$ and $\mathfrak{a}$ with $(\bar 0)$. If we find a way to write $\bigcap_{\mathfrak{p}\in\Xi}S_{\mathfrak{p}/\mathfrak{a}}(\bar 0)=(\bar 0)$ for some set $\Xi\subseteq\mathrm{Spec}(A)$, and these $S_{\mathfrak{p}/\mathfrak{a}}(\bar 0)$ are primary, then contracting will show, by (1.18), that $\mathfrak{a}=\bigcap_{\mathfrak{p}\in\Xi}S_\mathfrak{p}(\mathfrak{a})$ is an intersection of primary ideals upstairs. Also, (L1) survives in $A/\mathfrak{a}$ since, by (1.18), $(\bar 0:\bar x_\mathfrak{p})^c=\big((\bar 0)^c:(\bar x_\mathfrak{p})^c\big)=\big(\mathfrak{a}:(x_\mathfrak{p})+\mathfrak{a}\big)=(\mathfrak{a}:x_\mathfrak{p})$, so $(\bar 0:\bar x_\mathfrak{p})=(\bar 0:\bar x_\mathfrak{p})^{ce}=(\mathfrak{a}:x_\mathfrak{p})^e=S_\mathfrak{p}(\mathfrak{a})/\mathfrak{a}$. (Finally looking over the book's "hint," I'm no longer sure this simplification really simplifies very much. In fact, it may make things a little harder.)

[10] What I now *want* to do is as follows. Recall from [4.9] the set $D(A)$ of prime ideals $\mathfrak{p}$ of A such that there exists $a\in A$ with $\mathfrak{p}$ minimal in the set of prime ideals containing $(0:a)$. By [4.10.iv], $\bigcap_{\mathfrak{p}\in D(A)}S_\mathfrak{p}(0)=0$. This would be what we wanted if we could be assured the $S_\mathfrak{p}(0)$ were all are primary. Let P be the set of minimal primes of A. If $\mathfrak{p}\in P$, then ([4.11]) $S_\mathfrak{p}(0)=(0:x_\mathfrak{p})$ is $\mathfrak{p}$-primary. But it's not clear we should have $D(A)=\mathrm{Spec}(A)$ or $D(A)=P$. We also have $\bigcap_{\mathfrak{p}\in P}S_\mathfrak{p}(0)=\bigcap_{\mathfrak{p}\in P}\big(0:(x_\mathfrak{p})\big)=\big(0:\sum_{\mathfrak{p}\in P}(x_\mathfrak{p})\big)$, which will equal zero if $\sum_{\mathfrak{p}\in P}(x_\mathfrak{p})$ contains a non-zero-divisor. But I am not sure why this would be the case.

$\mathfrak{q}_{\alpha+1} = (\mathfrak{a}_{\alpha+1} : x_{\alpha+1})$. The same argument showing $\mathfrak{a}_0 = \mathfrak{q}_0 \cap [\mathfrak{a}_0 + (x_0)]$ shows that $\mathfrak{a}_{\alpha+1} = \mathfrak{q}_{\alpha+1} \cap [\mathfrak{a}_{\alpha+1} + (x_{\alpha+1})]$, so

$$\mathfrak{a}_0 = \mathfrak{a}_{\alpha+1} \cap \bigcap_{\beta \leq \alpha} \mathfrak{q}_\beta = [\mathfrak{a}_{\alpha+1} + (x_{\alpha+1})] \cap \bigcap_{\beta \leq \alpha+1} \mathfrak{q}_\beta.$$

For the "limit" step, suppose that for all $\alpha < \beta$ we have $\mathfrak{a}_0 = \mathfrak{a}_{\alpha+1} \cap \bigcap_{\gamma \leq \alpha} \mathfrak{q}_\gamma$, with $\mathfrak{a}_\alpha \subsetneq \mathfrak{a}_\gamma$ for $\alpha < \gamma$. Set $\mathfrak{a}_\beta := \bigcup_{\alpha<\beta} \mathfrak{a}_\alpha$. Then $\mathfrak{a}_\alpha \subsetneq \mathfrak{a}_\beta$ for each $\alpha < \beta$, and

$$\mathfrak{a}_\beta \cap \bigcap_{\alpha<\beta} \mathfrak{q}_\alpha = \bigcup_{\alpha<\beta} \Big(\mathfrak{a}_\alpha \cap \bigcap_{\alpha<\beta} \mathfrak{q}_\alpha\Big) = \bigcup_{\alpha+1<\beta} \Big(\mathfrak{a}_{\alpha+1} \cap \bigcap_{\gamma\leq\alpha} \mathfrak{q}_\gamma \cap \bigcap_{\alpha<\gamma<\beta} \mathfrak{q}_\gamma\Big) = \bigcup_{\alpha+1<\beta} \Big(\mathfrak{a}_0 \cap \bigcap_{\gamma<\beta} \mathfrak{q}_\gamma\Big) = \bigcup_{\alpha+1<\beta} \mathfrak{a}_0 = \mathfrak{a}_0.$$

If at any stage we get $\mathfrak{a}_\alpha = (1)$ we are done. In particular, if for some $n < \omega$ we have $\mathfrak{a}_n = (1)$, then we have found a primary decomposition of $\mathfrak{a} = \mathfrak{a}_0$. Since for $\alpha < \beta$ we have strict containment $\mathfrak{a}_\alpha \subsetneq \mathfrak{a}_\beta$, the number of different $\mathfrak{a}_\alpha$ we encounter is bounded by the cardinality of A, so the process does eventually terminate, leaving us with a decomposition $\mathfrak{a} = \bigcap_{\alpha<\beta} \mathfrak{q}_\alpha$ for some primary ideals $\mathfrak{q}_\alpha$ and some β of cardinality less than that of A.

Consider the following condition on a ring A:
(L2) Given an ideal $\mathfrak{a}$ and a descending chain $S_1 \supseteq S_2 \supseteq \cdots \supseteq S_n \supseteq \cdots$ of multiplicatively closed subsets of A, there exists an integer n such that $S_n(\mathfrak{a}) = S_{n+1}(\mathfrak{a}) = \cdots$. Prove that the following are equivalent:
i) Every ideal in A has a primary decomposition;
ii) A satisfies (L1) and (L2).

i) $\Longrightarrow$ (L1): Let $\mathfrak{a} \lhd A$ have primary decomposition $\bigcap \mathfrak{q}_i$ and let $\mathfrak{p} \in \operatorname{Spec}(A)$ and $S_\mathfrak{p} = A \backslash \mathfrak{p}$. Also let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Let Σ be the set of indices i with $\mathfrak{q}_i \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}$ (hence $\mathfrak{q}_i \cap S_\mathfrak{p} = \varnothing$) and Ξ the set of those with $\mathfrak{q}_i \not\subseteq \mathfrak{p}$ (hence $\mathfrak{q}_i \cap S_\mathfrak{p} \neq \varnothing$). (4.9) says that $S_\mathfrak{p}(\mathfrak{a}) = \bigcap_{i\in\Sigma} \mathfrak{q}_i$. Now $(\mathfrak{a} : x) = \bigcap_{i=1}^m (\mathfrak{q}_i : x)$, and $(\mathfrak{q}_i : x) = (1)$ if $x \in \mathfrak{q}_i$ and $= \mathfrak{q}_i$ if $x \notin \mathfrak{p}_i$, so we are looking for $x \in \bigcap_{i\in\Xi}^m \mathfrak{q}_i \backslash \bigcup_{i\in\Sigma} \mathfrak{p}_i$. For each $i \in \Xi$, there is an element $x_i \in \mathfrak{q}_i \backslash \mathfrak{p}$, and then $x := \prod_{i\in\Xi} x_i \in \bigcap \mathfrak{q}_i \backslash \mathfrak{p}$ since $\mathfrak{p}$ is prime. But since $\bigcup_{i\in\Sigma} \mathfrak{p}_i \subseteq \mathfrak{p}$, we have $(\mathfrak{a} : x) = S_\mathfrak{p}(\mathfrak{a})$ as desired.

i) $\Longrightarrow$ (L2): Let $\mathfrak{a} \lhd A$ have primary decomposition $\bigcap_{i=1}^m \mathfrak{q}_i$. (4.9) states that $S_n(\mathfrak{a}) = \bigcap_{i\in\Xi_n} \mathfrak{q}_i$, where $\Xi_n \subseteq \{1, \ldots, m\}$ is the set of indices i such that $S_n \cap r(\mathfrak{q}_i) = \varnothing$. As n gets bigger, Ξ_n decreases; but it can decrease at most m times, so at some finite stage it is all done decreasing and $S_n(\mathfrak{a})$ has stabilized.

ii) $\Longrightarrow$ i): Let $\mathfrak{a} \lhd A$ be given. [4.17] shows there exist primary $\mathfrak{q}_\alpha$, $\alpha < \beta$, such that $\mathfrak{a} = \bigcap \mathfrak{q}_\alpha$. We will be done if we can show finitely many suffice. Write $\mathfrak{p}_\alpha = r(\mathfrak{q}_\alpha)$ and $S_\beta = A \backslash \bigcup_{\alpha<\beta} \mathfrak{p}_\alpha$. Then [3.7.i] shows that the S_α are saturated multiplicative submonoids of A and apparently $S_\alpha \supseteq S_\beta$ for $\alpha < \beta$. Recall from the proof of [4.17] that at each finite stage of the construction we have an ideal $\mathfrak{a}_{n+1}$ such that $\mathfrak{a} = \mathfrak{a}_{n+1} \cap \mathfrak{q}_n \cap \cdots \cap \mathfrak{q}_0$, and $\mathfrak{a}_{n+1} \not\subseteq \mathfrak{p}_m$ for $m < n+1$. Then $\mathfrak{a}_{n+1} \cap S_n \neq \varnothing$ and [4.12.iii] says that $S_n(\mathfrak{a}_{n+1}) = (1)$, so $S_n(\mathfrak{a}) = \mathfrak{q}_0 \cap \cdots \cap \mathfrak{q}_n$. (L2) says that the sequence $S_n(\mathfrak{a})$ stabilizes in finitely many steps, say at $S_n(\mathfrak{a}) = \mathfrak{q}_0 \cap \cdots \cap \mathfrak{q}_n$. Then for all $\alpha \geq n$ we have $S_\alpha(\mathfrak{a}) = \mathfrak{q}_0 \cap \cdots \cap \mathfrak{q}_n$.

Write $\mathfrak{a} = S_n(\mathfrak{a}) \cap \mathfrak{q}_\alpha \cap \bigcap_{\gamma \notin \{0, \ldots, n, \alpha\}} \mathfrak{q}_\gamma$. Then taking S_α and using the finitary distributive property [4.12.i], we should get a term $S_\alpha(\mathfrak{q}_\alpha)$. Note $\mathfrak{q}_\alpha \subseteq \mathfrak{p}_\alpha$ does not meet $A \backslash \mathfrak{p}_\alpha \supseteq S_\alpha$. Thus if $x \in S_\alpha(\mathfrak{q}_\alpha)$, so there is $s \in S_\alpha$ such that $sx \in \mathfrak{q}_\alpha$, that $\mathfrak{q}_\alpha$ is primary implies $\exists n$ ($s^n \in \mathfrak{q}_\alpha$) (which cannot happen) or $x \in \mathfrak{q}_\alpha$, so the contributed term is $S_\alpha(\mathfrak{q}_\alpha) = \mathfrak{q}_\alpha$. Thus $\bigcap_{i=0}^n \mathfrak{q}_i \cap \mathfrak{q}_\alpha \cap \cdots = \bigcap_{i=0}^n \mathfrak{q}_i$, so $\bigcap_{i=0}^n \mathfrak{q}_i \subseteq \mathfrak{q}_\alpha$. Since this holds for all $\alpha > n$, we see $\mathfrak{a} = \bigcap_{\alpha<\beta} \mathfrak{q}_\alpha = \bigcap_{i=0}^n \mathfrak{q}_i$ has a primary decomposition.

Let A be a ring and $\mathfrak{p}$ a prime ideal of A. Show that every $\mathfrak{p}$-primary ideal contains $S_\mathfrak{p}(0)$, the kernel of the canonical homomorphism $A \to A_\mathfrak{p}$.

This was proved for the first statement of [4.11].

Suppose that A satisfies the following condition: for every prime ideal $\mathfrak{p}$, the intersection of all $\mathfrak{p}$-primary ideals of A is equal to $S_\mathfrak{p}(0)$. (Noetherian rings satisfy this condition: see Chapter 10.) Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct prime ideals, none of which is a minimal prime ideal of A. Then there exists an ideal $\mathfrak{a}$ in A whose associated prime ideals are $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.

We attempt an induction proof. For $n = 1$, the ideal $\mathfrak{a} = \mathfrak{p}_1$ satisfies the condition. Suppose that the result has been proved for n, and let $\mathfrak{p}_{n+1}$ be one last prime. Then there is an ideal $\mathfrak{b}$ with a primary decomposition $\bigcap_{i=1}^n \mathfrak{q}_i$ where $r(\mathfrak{q}_i) = \mathfrak{p}_i$. What we'd like is to take any $\mathfrak{p}_{n+1}$-primary ideal $\mathfrak{q}_{n+1}$ and let $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{q}_{n+1}$. This will give us the decomposition we want unless it is redundant. If it is redundant, there is some term containing the intersection of the rest. Taking radicals and using the distributivity property (1.13.iii), the intersection of some n of the primes is contained in the remaining prime. By (1.11.ii), this implies that the big prime contains one of the first n. We can arrange then, by reordering the $\mathfrak{p}_i$ so that $\mathfrak{p}_{n+1}$ is maximal among them, that $\mathfrak{q}_{n+1}$ we don't have $\bigcap_{i\neq j}\mathfrak{q}_i \subseteq \mathfrak{q}_j$ for any $j \neq n+1$. Write $\mathfrak{p}' = \mathfrak{p}_{n+1}$

Now we only have to worry about the possibility that $\bigcap_{i=1}^{n}\mathfrak{q}_i \subseteq \mathfrak{q}'$. If there is a $\mathfrak{p}'$-primary $\mathfrak{q}'$ for which this doesn't happen, we are done. Otherwise, taking the intersection of both sides over all such, we see $\bigcap_{i=1}^{n}\mathfrak{q}_i \subseteq S_{\mathfrak{p}'}(0)$, using the first part of [4.11]. By [4.10.iii], for a smaller prime $\mathfrak{p} \subseteq \mathfrak{p}'$ we have $\bigcap_{i=1}^{n}\mathfrak{q}_i \subseteq S_{\mathfrak{p}'}(0) \subseteq S_{\mathfrak{p}}(0)$; in particular, we may take $\mathfrak{p}$ minimal. Now again taking radicals of both sides and using (1.13.iii), we get $\bigcap_{i=1}^{n}\mathfrak{p}_i \subseteq \mathfrak{p}$. By (1.11.ii) again, this means $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $i \in \{1, \dots, n\}$; but then by minimality of $\mathfrak{p}$, we have $\mathfrak{p}_i = \mathfrak{p}$. But the assumption of the problem was that none of the $\mathfrak{p}_i$ were minimal, so the possibility that worried us in this paragraph is forestalled, and we are done.

Primary decomposition of modules

Practically the whole of this chapter can be transposed to the context of modules over a ring A. The following exercises indicate how this is done.

Let M be a fixed A-module, N a submodule of M. The radical *of N in M is defined to be*

$$r_M(N) = \{x \in A : x^q M \subseteq N \text{ for some } q > 0\}.$$

Show that $r_M(N) = r(N : M) = r\big(\operatorname{Ann}(M/N)\big)$. *In particular,* $r_M(N)$ *is an* ideal.

$$x \in r_M(N) \iff \exists q > 0\ (x^q M \subseteq N) \iff \exists q > 0\ \big(x^q \in (N : M)\big) \iff x \in r(N : M).$$

By (2.2.ii), and since $N \subseteq M$, we have $(N : M) = \operatorname{Ann}\big((N + M)/N\big) = \operatorname{Ann}(M/N)$, so taking radicals, $r(N : M) = r\big(\operatorname{Ann}(M/N)\big)$.

State and prove the formulas for r_M *analogous to (1.13).*

—i) $P \subseteq N \implies r_M(P) \subseteq r_M(N)$: $x^q M \subseteq P$, implies $x^q M \subseteq N$.

0) $r_B(C^n) = r_B(C)$ *for B an A-algebra, C a subalgebra, and* $n > 0$: $C^n \subseteq C$, so $r_B(C^n) \subseteq r_B(C)$ by —i). If $x^q B \subseteq C$, then taking n^{th} powers, and remembering $1 \in B$, gives $x^{qn} B \subseteq C^n$.

i) $r_B(\mathfrak{b}) \supseteq f^{-1}(\mathfrak{b})$, *for* $f : A \to B$ *an A-algebra and* $\mathfrak{b} \lhd B$: If $b \in \mathfrak{b}$, then $bB = (b) \subseteq \mathfrak{b}$, and by definition if $f(a) = b$, then $aB = f(a)B \subseteq \mathfrak{b}$.

ii) $r\big(r_M(N)\big) = r_M(N)$: $x \in r\big(r_M(N)\big) \iff \exists p > 0\ \big(x^p \in r_M(N)\big)$ $\iff \exists p, q > 0\ \big(x^{pq} M \subseteq N\big) \iff x \in r_M(N)$.

iii) $r_M(N \cap P) = r_M(N) \cap r_M(P)$: If $x^n M \subseteq N \cap P$, then trivially $x^n M \subseteq N$ and $x^n M \subseteq P$. If $x^n M \subseteq N$ and $x^p M \subseteq P$, then for $q = \max\{n, p\}$ we have $x^q M \subseteq N \cap P$.

iv) $r_M(N) = (1) \iff M = N$: $1 \in r\big(\operatorname{Ann}(M/N)\big) \iff 1 \in \operatorname{Ann}(M/N) \iff M/N = 0 \iff M = N$.

v) $r_M(N + P) \supseteq r\big(r_M(N) + r_M(P)\big)$: By —i), $r_M(N)$, $r_M(P) \subseteq r_M(N + P)$, so $r_M(N) + r_M(P) \subseteq r_M(N + P)$. Taking radicals and applying ii), $r\big(r_M(N) + r_M(P)\big) \subseteq r\big(r_M(N + P)\big) = r_M(N + P)$. The converse is false. Let $A \neq 0$, $M = A \oplus A$ with action $a(b, c) = (ab, ac)$, $N = A \oplus (0)$, and $P = (0) \oplus A$, Then $M = N + P$, so $r_M(N + P) = (1)$, but $r_M(N) = r_M(P) = 0$.

vi) If $\mathfrak{p}$ *is prime,* $r(\mathfrak{p}^n) = \mathfrak{p}$ *for all* $n > 0$: I've no clue how to interpret a power of a module.

I seem to have failed this problem, in that I wasn't sure in all cases what the appropriately analogous formulas were. The ones involving algebras were stretches, brought about by the difficulty of comparing N and $r_M(N)$, one being a submodule of M and the other being an ideal of A.

An element $x \in A$ *defines an endomorphism* ϕ_x *of M, namely* $m \mapsto xm$. *The element x is said to be a* zero-divisor *(resp.* nilpotent*) in M if* ϕ_x *is not injective (resp. is nilpotent). A submodule Q of M is* primary in M *if* $Q \neq M$ *and every zero-divisor in* M/Q *is nilpotent.*

Show that if Q is primary in M, then $(Q : M)$ *is a primary ideal and hence* $r_M(Q)$ *is prime ideal* $\mathfrak{p}$. *We say that Q is* $\mathfrak{p}$-primary *(in M).*

Suppose $xy \in (Q : M)$ and $y \notin (Q : M)$ so that $xy(M/Q) = 0$ but $y(M/Q) \neq 0$. Then the endomorphism $\bar{\phi}_x \circ \bar{\phi}_y = \bar{\phi}_{xy}$ of M/Q is zero, though $\bar{\phi}_y$ is not. Then $\bar{\phi}_x$ has non-empty kernel, so x is a zero-divisor of Q. By the definition of “primary,” x is then nilpotent in M/Q, so for some $n>0$ we have $0=\bar{\phi}_x^{\circ n}=\bar{\phi}_{x^n}: M/Q\to M/Q$. Then the associated endomorphism $\phi_{x^n}: m\mapsto x^n m$ of M has image in Q, so $x^n\in(Q:M)$. Thus $(Q:M)$ is primary.

Prove the analogues of (4.3) and (4.4).

Lemma 4.3*. *If $Q_i\subseteq M$ $(1\leq i\leq n)$ are $\mathfrak{p}$-primary, then $Q=\bigcap_{i=1}^n Q_i$ is $\mathfrak{p}$-primary.*

Since the Q_i are primary, hence not equal to M, their intersection $Q\neq M$. Suppose $x\in A$ is a zero-divisor of M/Q. Then there is some nonzero $m\in M$ such that $xm\in Q=\bigcap Q_i$. Then x is a zero-divisor of each M/Q_i, so by assumption is nilpotent, meaning there is $n_i>0$ such that $x^{n_i}M\subseteq Q_i$. Taking $n=\max_i n_i$ we see $x^n M\subseteq Q$, so x is nilpotent in M/Q. Thus Q is primary. As for the radical,

$$r(Q:M)=r\Big(\bigcap Q_i:M\Big)\overset{(1.12.\text{iv})}{=}r\Big(\bigcap(Q_i:M)\Big)\overset{(1.13.\text{iii})}{=}\bigcap r(Q_i:M)=\bigcap_i\mathfrak{p}=\mathfrak{p}.$$

Lemma 4.4*. *i) Let $N\subseteq M$ be A-modules and $m\in N$. Then $(N:m)=(1)$;*
ii) Let $Q\subseteq M$ be a $\mathfrak{p}$-primary submodule, and $m\in M$. If $m\notin Q$ then $(Q:m)$ is $\mathfrak{p}$-primary;
iii) Let $Q\subseteq M$ be a $\mathfrak{p}$-primary submodule, and $x\in A$. If $x\notin\mathfrak{p}$ then $(Q:x):=\{m\in M: xm\in Q\}=Q$.

i): Since $m\in N$ and N is an A-module, $Am\subseteq N$, so $(N:m)=(1)$.

ii): Suppose $xy\in(Q:m)$, so $xym\in Q$. Suppose $y\notin(Q:m)$, so that $ym\notin Q$. Then x is a zero-divisor in M/Q, so by the assumption Q is primary, there is $n>0$ such that x^n acts as zero on M/Q. Then $x^n M\subseteq Q$, and in particular $x^n m\in Q$, so $x^n\in(Q:m)$. Thus $(Q:m)$ is primary.

Note that $m\in M$ implies $(Q:M)\subseteq(Q:m)$. Taking radicals, $\mathfrak{p}\subseteq r(Q:m)$. On the other hand assume $x\in r(Q:m)$. Then for some minimal $n>0$ we have $x^n m\in Q$. Then $x(x^{n-1}\bar{m})=\bar{0}$ in M/Q, so x is a zero-divisor of M/Q and hence there is $p>0$ such that $x^p M\subseteq Q$. Then $x\in r_M(Q)=\mathfrak{p}$. Thus $(Q:m)$ is $\mathfrak{p}$-primary.

iii): Obviously if $m\in Q$ then $xm\in Q$, so $Q\subseteq(Q:x)$. By contraposition, we will suppose $m\in(Q:x)\backslash Q$ and show $x\in\mathfrak{p}$. Well, $xm\in Q$, and $\bar{m}\neq\bar{0}$ in M/Q, so x is a zero-divisor, and for some power $n>0$ we have $x^n M\subseteq Q$. But then $x\in r_M(Q)=\mathfrak{p}$.

A primary decomposition of N in M *is a representation of N as an intersection*

$$N=Q_1\cap\cdots\cap Q_n$$

of primary submodules of M; it is a minimal primary decomposition *if the ideals $\mathfrak{p}_i=r_M(Q_i)$ are all distinct and if none of the components Q_i can be omitted from the intersection; that is $Q_i\not\supseteq\bigcap_{j\neq i}Q_j$ $(1\leq i\leq n)$.*

Prove the analogue of (4.5), that the prime ideals $\mathfrak{p}_i$ depend only on N (and M). They are called the prime ideals belonging to N in M.

Theorem 4.5*. *Let N be a decomposable submodule of M and let $N=\bigcap_{i=1}^n Q_i$ be a minimal primary decomposition of N. Let $\mathfrak{p}_i=r_M(Q_i)$ $(1\leq i\leq n)$. Then the $\mathfrak{p}_i$ are precisely the prime ideals which occur in the set of ideals $r(N:m)$ $(m\in M)$, and hence are independent of the particular decomposition of N.*

Set $P_i=\bigcap_{j\neq i}Q_j$. By the assumption of irredundancy, $Q_i\subsetneq P_i$. Let $m\in P_i\backslash Q_i$, and consider the ideal $(N:m)=(P_i\cap Q_i:m)\overset{(1.12.\text{iv})}{=}(P_i:m)\cap(Q_i:m)$. By (4.4*.i,ii) of [4.21] above $(P_i:m)=M$ and $(Q_i:m)$ is $\mathfrak{p}_i$-primary, so $(N:m)$ is $\mathfrak{p}_i$-primary. Thus each $\mathfrak{p}_i$ is $r(N:m)$ for some $m\in M$.[11]

Suppose on the other hand that $r(N:m)$ is a prime $\mathfrak{p}$ for some $m\in M$. Note $(N:m)=\Big(\bigcap Q_i:m\Big)\overset{(1.12.\text{iv})}{=}\bigcap(Q_i:m)$, so by (4.4*) above, $\mathfrak{p}=r(N:m)=\bigcap_{m\notin Q_i}\mathfrak{p}_i$. Since the prime $\mathfrak{p}$ is an intersection of some of the $\mathfrak{p}_i$, (1.11.ii) shows $\mathfrak{p}=\mathfrak{p}_i$ for some i.

Show that they are also the prime ideals belonging to 0 in M/N.

Note that for any module $P\subseteq M$ we have $(N:P)=(0+N:P+N)$. Indeed $xP\subseteq N\iff x(P+N)\subseteq 0+N=N$. Taking radicals, $r(N:P)=r(0+N:P+N)$. Specializing to cyclic submodules Am gives $r(N:m)=r(\bar{0}:\bar{m})$, so one is prime just if the other is, and by Theorem 4.5*, the same primes belong to $N\subseteq M$ and $0\subseteq M/N$.

[11] I owe this part of the argument to *Multiplicative Theory of Ideals* by Max D. Larsen and Paul Joseph McCarthy. I had initially started reasoning about ideals of the form $\big((Q:M):x\big)$, and was trying to prove that if $N=\bigcap Q_i$ is an irredundant decomposition, then $(N:M)=\bigcap(Q_i:M)$ was likewise.

State and prove the analogues of (4.6)–(4.11) inclusive. (There is no loss of generality in taking $N = 0$.)

We must convince ourselves we genuinely aren't losing any generality. What we should do is try to lift a primary decomposition, as we know (p. 50) primary ideals are preserved under contraction. So suppose we are given an irredundant primary decomposition $0 = \bigcap Q_i/N$ in M/N (recalling the correspondence (p. 18) between submodules of M/N and submodules of M containing N). Apparently $N = \bigcap Q_i$, and we should show that the Q_i are $r_{M/N}(Q_i/N)$-primary. Much as in the last part of [4.22], we have $(Q_i/N : M/N) = \{x \in A : xM \subseteq Q_i\} = (Q_i : M)$, and taking radicals gives $r_M(Q_i) = r_{M/N}(Q_i/N)$. Now we must show Q_i is primary. Suppose $x \in A$ is a zero-divisor of M/Q_i. The third isomorphism theorem (2.1.i) gives $M/Q_i \cong (M/N)/(Q_i/N)$, so x is a zero-divisor of the latter, hence nilpotent since Q_i/N is primary, hence nilpotent in M/Q_i since they are isomorphic. Thus Q_i is primary. It is clear that irredundancy is preserved under lifting, as $Q_i/N \supseteq \bigcap_{j \neq i} Q_j/N \iff Q_i \supseteq \bigcap_{j \neq i} Q_j$ by the order-preserving correspondence of p. 18.[12]

Proposition 4.6*. *Let $N \subseteq M$ be a decomposable module. Then any prime ideal $\mathfrak{p} \supseteq r_M(N)$ contains a minimal prime ideal belonging to N, and thus the minimal prime ideals of N are precisely the minimal elements in the set of all prime ideals containing $r_M(N)$.*

Write $N = \bigcap Q_i$, so that ([4.20.iii]) $r_M(N) = \bigcap r_M(Q_i) = \bigcap \mathfrak{p}_i$. If $\mathfrak{p} \supseteq \bigcap \mathfrak{p}_i$, then by (1.11.ii), there is i with $\mathfrak{p} \supseteq \mathfrak{p}_i$, and surely for any $\mathfrak{p}_j \subseteq \mathfrak{p}_i$ we have $\mathfrak{p}_j \subseteq \mathfrak{p}$, so $\mathfrak{p}$ contains an isolated prime ideal of N. In particular, if $\mathfrak{p}$ is minimal over $r_M(N)$, this shows it equals some isolated $\mathfrak{p}_j$.

Proposition 4.7*. *Let $N \subseteq M$ be a decomposable module, let $N = \bigcap_{i=1}^n Q_i$ be a minimal primary decomposition, and let $\mathfrak{p}_i = r_M(Q_i)$. Then*

$$\bigcup_{i=1}^{n} \mathfrak{p}_i = \{x \in A : (N : x) \neq N\}.$$

In particular, if $0 \subseteq M$ is decomposable, the set $D \subseteq A$ of zero-divisors of M is the union of the prime ideals belonging to 0.

Since by [4.22], the set of primes associated to $N \subseteq M$ is the same as that associated to $0 \subseteq M/N$, and for $x \in A$ we have $(N : x) \neq N \subseteq M$ just if $(0 : x) \neq 0 \subseteq M/N$, we can indeed assume $N = 0$.

Then the right-hand side D is the set of x such that there exists $m \neq 0 \in M$ such that $m \in (0 : x)$, or $xm = 0$; with is to say D is the set of zero-divisors of M. Now if $x \in r(D)$, then there is a nonzero $m \in M$ and a least $n > 0$ such that $x^n m = 0$. Then $m' = x^{n-1}m \neq 0$ and $xm = 0$, so $x \in D$. Thus $D = r(D) = r\Big(\bigcup_{m \neq 0}(0 : m)\Big) = \bigcup_{m \neq 0} r(0 : m)$. The proof of Theorem 4.5* ([4.22]) shows that each $r(0 : m)$ for $m \neq 0$ is the intersection of some of the $\mathfrak{p}_i$, and each $\mathfrak{p}_i = r(0 : m)$ for some m. Thus $D = \bigcup \mathfrak{p}_i$.

Proposition 4.8*. *Let S be a multiplicative submonoid of A, and let $Q \subseteq M$ be a $\mathfrak{p}$-primary module.*
i) If $S \cap \mathfrak{p} \neq \varnothing$, then $S^{-1}Q = S^{-1}M$.
*ii) If $S \cap \mathfrak{p} = \varnothing$, then $S^{-1}Q$ is a $S^{-1}\mathfrak{p}$-primary submodule of $S^{-1}M$, and its preimage (*contraction*) under the canonical map $M \to S^{-1}M$ is Q. Hence primary $S^{-1}A$-submodules of $S^{-1}M$ correspond to primary A-submodules of M.*

i): Let $s \in S \cap \mathfrak{p}$. Since $\mathfrak{p} = r_M(Q)$, there is $n > 0$ such that $s^n M \subseteq Q$. Then any element $m/t \in S^{-1}M$ can be written as $s^n m/s^n t \in S^{-1}Q$.

ii): Suppose $x/s \in S^{-1}A$ is a zero-divisor in $S^{-1}M/S^{-1}Q$. Then there is some non-zero $\overline{m/t} \in S^{-1}M/S^{-1}Q$ such that $(x/s)\overline{m/t} = \overline{xm/st} = 0$. Then $xm/st \in S^{-1}Q$, so there is $u \in S$ such that $uxm \in Q \subseteq M$. Then since $\overline{m/t}$ was non-zero, $m \notin Q$, so ux is a zero-divisor of M/Q, hence nilpotent since Q is primary. Then there is $n > 0$ such that $(ux)^n M \subseteq Q$. That means $x^n S^{-1}M = x^n u^n S^{-1}M \subseteq S^{-1}Q$, so x is nilpotent in $S^{-1}M/S^{-1}Q$, meaning $S^{-1}Q$ is primary.

If $x \in \mathfrak{p} = r_M(Q)$, let $n > 0$ be such that $x^n M \subseteq Q$. Then for arbitrary $s \in S$ we have $(x/s)^n S^{-1}M \subseteq S^{-1}Q$, so $x/s \in r(S^{-1}Q : S^{-1}M) = r_{S^{-1}M}(S^{-1}Q)$. On the other hand, if $x/s \in r_{S^{-1}M}(S^{-1}Q)$ then $(x^n/1)S^{-1}M = (x/s)^n S^{-1}M \subseteq S^{-1}Q$ for some $n > 0$. Thus for every $m/t \in S^{-1}M$ we have $x^n m/st \in S^{-1}Q$. This means there is $u \in S$ such that $ux^n m \in Q$. Then ux^n is a zero-divisor of M/Q, so nilpotent in M/Q, and so some power takes M into Q, and $ux^n \in r_M(Q) = \mathfrak{p}$. But then since $\mathfrak{p}$ is prime and $u \notin \mathfrak{p}$ we have $x^n \in \mathfrak{p}$, so $x \in r(\mathfrak{p}) = \mathfrak{p}$, and finally $x/s \in S^{-1}\mathfrak{p}$. Therefore $S^{-1}Q$ is $S^{-1}\mathfrak{p}$-primary.

[12] Note that, on the other hand primary decomposition does not generally survive the quotient process. Indeed, Example 3) on p. 51 shows that the primary ([4.8]) ideal $(x, z)^2$ of $k[x, y, z]$, where k is a field, has image no longer primary in the quotient ring $k[x, y, z]/(xy - z^2)$.

Now suppose $m \in M$ is such that $m/1 \in S^{-1}Q$. Then there is $s \in S$ such that $sm \in Q$. By (4.7*) above, $\mathfrak{p} = \{x \in A : Q \neq (Q : x)\}$, so $m \in (Q : s) = Q$ as $s \notin \mathfrak{p}$.

Finally, we show that every $S^{-1}A$-submodule N' of $S^{-1}M$ is an *extended module* of the form $S^{-1}N$ for some A-submodule $N \subseteq M$. Indeed, let N be the set of $n \in M$ such that $n/1 \in N'$, (which we can also think of as the contraction of N along the canonical map $f \colon M \to S^{-1}M$). If $n/s \in N'$, then $n/1 = s(n/s) \in N'$, so $n \in N$ and hence $n/s \in S^{-1}N$. On the other hand $f(N) = f\big(f^{-1}(N')\big) \subseteq N'$, so $S^{-1}N \subseteq N'$.

Proposition 4.9*. *Let S be a multiplicative submonoid of A and let $N \subseteq M$ be a decomposable ideal. Let $N = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of N. Let $\mathfrak{p}_i = r_M(Q_i)$ and suppose the Q_i numbered so that S meets $\mathfrak{p}_{p+1}, \ldots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_p$. Write $S(N) = \{m \in M : m/1 \in S^{-1}N\}$. Then*

$$S^{-1}N = \bigcap_{i=1}^{p} S^{-1}Q_i, \qquad S(N) = \bigcap_{i=1}^{p} Q_i,$$

and these are minimal primary decompositions.

By (3.4.ii) we have $S^{-1}N = \bigcap_{i=1}^{n} S^{-1}Q_i$. By (4.8*.i) above, we have $S^{-1}Q_i = S^{-1}M$ for $i > p$, so $S^{-1}N = \bigcap_{i=1}^{p} S^{-1}Q_i$, and by (4.8*.ii), $S^{-1}Q_i$ is $S^{-1}\mathfrak{p}_i$-primary for $i \leq p$. Since these $\mathfrak{p}_i$ don't meet S, by (3.11.iv), the $S^{-1}\mathfrak{p}_i$ are distinct primes of $S^{-1}A$. If we had, for some $j \leq p$, that $S^{-1}Q_j \supseteq \bigcap_{j \neq i=1}^{p} S^{-1}Q_i$, then taking preimages under $f \colon M \to S^{-1}M$ we see that $Q_j \supseteq \bigcap_{j \neq i} Q_i$, contradicting the assumed irredundancy of the Q_i. Thus $S^{-1}N = \bigcap_{i=1}^{p} S^{-1}Q_i$ is an irredundant primary decomposition of $S^{-1}N$. Taking preimages under $f \colon M \to S^{-1}M$,

$$S(N) = f^{-1}(S^{-1}N) = f^{-1}\Big(\bigcap_{i=1}^{p} S^{-1}Q_i\Big) = \bigcap_{i=1}^{p} f^{-1}(S^{-1}Q_i) = \bigcap_{i=1}^{p} Q_i$$

by (4.8*.ii) again. This is an irredundant primary decomposition since the decomposition of N is.

Theorem 4.10*. *Let $N \subseteq M$ be a decomposable ideal, let $N = \bigcap_{i=1}^{n} Q_i$ be a minimal primary decomposition of N, let $\mathfrak{p}_i = r_M(Q_i)$, and let $\Sigma = \{\mathfrak{p}_{i_1}, \ldots, \mathfrak{p}_{i_m}\}$ be an isolated set of prime ideals of N. Then $\bigcap_{\mathfrak{p}_i \in \Sigma} Q_i$ is independent of the decomposition.*

Let $S = A \backslash \bigcup \Sigma$. Then S is a multiplicative submonoid, and for $\mathfrak{p} \in \Sigma$ we have $\mathfrak{p} \cap S = \varnothing$, while if $\mathfrak{p} \notin \Sigma$, then since $\mathfrak{p}$ is not contained in an element of Σ by isolation, (1.11.i) shows $\mathfrak{p} \not\subseteq \bigcup \Sigma$, so $\mathfrak{p} \cap S \neq \varnothing$. Then $\bigcap_{\mathfrak{p}_i \in \Sigma} Q_i = S(N)$ by (4.9*), so this intersection is actually independent of the Q_i chosen.

Corollary 4.11*. *The isolated primary components (i.e., the primary components Q_i corresponding to minimal prime ideals $\mathfrak{p}_i$) are uniquely determined by N.*

Let $\mathfrak{p}_i$ be an isolated prime of N. Taking $\Sigma = \{\mathfrak{p}_i\}$ and $S_{\mathfrak{p}_i} = A \backslash \mathfrak{p}_i$ in (4.10*) above gives $S_{p_i}(N) = Q_i$ independent of the choice of decomposition.

Integral Dependence and Valuations

EXERCISES

Let $f\colon A \to B$ be an integral homomorphism of rings. Show that $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed *mapping, i.e. that it maps closed sets to closed sets. (This is a geometrical equivalent of (5.10).)*

Write $C = f(A)$. That f is integral means that B is integral over C. Write $f\colon A \overset{p}{\twoheadrightarrow} C \overset{i}{\hookrightarrow} B$. f will be closed if both p and i are closed.

But p^* is a homeomorphism between $\operatorname{Spec}(C)$ and $V\big(\ker(p)\big) \subseteq \operatorname{Spec}(A)$ by [1.21.v]. For any closed subset $K \subseteq \operatorname{Spec}(C)$, we have $p^*(K)$ closed in the subspace topology on $V\big(\ker(p)\big)$. Since this subset of $\operatorname{Spec}(A)$ is closed as well, $p^*(K)$ is closed in $\operatorname{Spec}(A)$. Thus all surjections induce closed maps on prime spectra.

For closedness of i^*, any closed subset of $\operatorname{Spec}(B)$ is ([1.15.i]) the set $V(\mathfrak{b})$ of all primes containing some radical ideal $\mathfrak{b} \lhd B$. Let $\mathfrak{c} = i^*(\mathfrak{b}) = \mathfrak{b} \cap C$, we claim $i^*\big(V(\mathfrak{b})\big) = V(\mathfrak{c})$. If $\mathfrak{b} \subseteq \mathfrak{q} \in \operatorname{Spec}(B)$, then intersecting both sides with C gives $\mathfrak{c} \subseteq i^*(\mathfrak{q}) \in \operatorname{Spec}(C)$, so $i^*\big(V(\mathfrak{b})\big) \subseteq V(\mathfrak{c})$. Surjectivity is a little less obvious. Every prime $\mathfrak{p} \supseteq \mathfrak{c}$ induces a quotient prime $\bar{\mathfrak{p}}$ of $C/\mathfrak{c}$. (5.6.i) says $j : C/\mathfrak{c} \rightarrowtail B/\mathfrak{b}$ is integral, so by (5.10), there is there is $\bar{\mathfrak{q}} \in \operatorname{Spec}(B/\mathfrak{b})$ (the image of $\mathfrak{q} \in \operatorname{Spec}(B)$) such that $j^*(\bar{\mathfrak{q}}) = \bar{\mathfrak{p}}$. Thus j^* surjectively maps $\operatorname{Spec}(B/\mathfrak{b}) \approx V(\mathfrak{b})$ to $\operatorname{Spec}(C/\mathfrak{c}) \approx V(\mathfrak{c})$, so using [3.21.iii], $i^*\big(V(\mathfrak{b})\big) = V(\mathfrak{c})$ and i^* is closed.[1]

Let A be a subring of a ring B such that B is integral over A, and let $f\colon A \to \Omega$ be a homomorphism of A into an algebraically closed field Ω. Show that f can be extended to a homomorphism of B into Ω.

Ω is an integral domain, so $f(A)$ is as well. Thus $\mathfrak{p} = \ker(f)$ is a prime ideal of A, and $f(A) \cong A/\mathfrak{p}$. By Theorem 5.10, there is a prime ideal $\mathfrak{q} \lhd B$ with $\mathfrak{q} \cap A = \mathfrak{p}$. Then $B/\mathfrak{q}$, by (5.6.i), is integral over $A/\mathfrak{p}$. Thus it suffices to prove the result in the case $A \subseteq B$ are integral domains with B integral over A and $f\colon A \rightarrowtail \Omega$ is an injection.

We use Zorn's Lemma to construct an embedding $B \rightarrowtail \Omega$. Let Σ be the set of pairs (C, σ), where $A \subseteq C \subseteq B/$ and $\sigma\colon C \to \Omega$ is an embedding, and such that $\sigma|_A = f$. Partially order Σ by $(C, \sigma) \leq (C', \sigma')$ just if $C \subseteq C'$ and $\sigma = \sigma'|_C$. $\Sigma \neq \emptyset$ since the inclusion (A, f) is a minimal element. If $\big\langle (C_\alpha, \sigma_\alpha)\big\rangle_\alpha$ is a chain in Σ, then $\bigcup C_\alpha \subseteq C$ and $\sigma = \bigcup \sigma_\alpha$ is a well defined homomorphism, injective since each σ_α is, so every chain has an upper bound. By Zorn's Lemma, there is a maximal element $(C, \sigma) \in \Sigma$. We will be done if $C = B$.

Suppose for a contradiction then there is $b \in B \backslash C$, and b is integral over A, hence *a fortiori* over C. Say b satisfies $p(x) = \sum c_i x^i \in C[x]$, and write $(\sigma p)(x) = \sum \sigma(c_i) x^i \in \Omega[x]$ Then the expected composition

$$C[x] \to \Omega[x] \to \Omega[x]/\big((\sigma p)(x)\big) \cong \Omega$$

has kernel $\big(p(x)\big)$, and so descends to an injection $C[x]/\big(p(x)\big) \rightarrowtail \Omega$ restricting to σ on C. But $C[x]/\big(p(x)\big) \cong C[b]$, and by assumption $C \subsetneq C[b] \subseteq B$ so the induced map $C[b] \rightarrowtail \Omega$ contradicts maximality of σ.

Let $f : B \to B'$ be a homomorphism of A-algebras, and let C be an A-algebra. If f is integral, prove that $f \otimes 1\colon B \otimes_A C \to B' \otimes_A C$ is integral. (This includes (5.6) ii) as a special case.)

Start with a decomposable element $x \otimes c \in B' \otimes_A C$. Since x is integral over B, it satisfies some polynomial equation $\sum_{i=0}^n f(b_i) x^i = 0$ for $b_i \in B$ (with leading coefficient $b_n = 1$). Then $\sum f(b_i) x^i \otimes c^n = 0$ in $B' \otimes_A C$. Rearranging, $0 = \sum \big(f(b_i) \otimes c^{n-i}\big)(x \otimes c)^i$. But each $f(b_i) \otimes c^{n-i} \in \operatorname{im}(f \otimes \mathrm{id}_C)$, so $x \otimes c$ is integral over $\operatorname{im}(f \otimes \mathrm{id}_C)$. But element of $B' \otimes_A C$ is a finite sum of elements of the form $x \otimes c$, so (5.3) shows that the whole ring $B' \otimes_A C$ is integral over $\operatorname{im}(f \otimes \mathrm{id}_C)$.

The parenthetical comment follows from setting $C = S^{-1}A$ and using (3.5), which states $S^{-1}A \otimes_A B \cong S^{-1}B$.

[1] I went this quotient route because first applying (5.10) for $\mathfrak{p} \in V(\mathfrak{c})$ gives a prime $\mathfrak{q} \in \operatorname{Spec}(B)$, but it wasn't completely obvious to me that $\mathfrak{q} \in V(\mathfrak{b})$.

Let A be a subring of B such that B is integral over A. Let $\mathfrak{n}$ be a maximal ideal of B and let $\mathfrak{m} = \mathfrak{n} \cap A$ be the corresponding maximal ideal of A (see (5.8)). Is $B_{\mathfrak{n}}$ necessarily integral over $A_{\mathfrak{m}}$?

Per the book's suggestion, no. Let k be a field, of characteristic $\neq 2$ so that $x+1 \neq x-1$, $B = k[x]$, and $A = k[x^2-1]$. Then $x \in B$ satisfies $y^2 - [1-(x^2-1)] = 0$ in $A[y]$, so is integral over A. Then by (5.3), B is integral over A. Now consider the ideal $\mathfrak{n} := (x-1)$ of B, and let $\mathfrak{m} := \mathfrak{n} \cap A = (x^2-1)$. Then $S_{\mathfrak{m}} := A \backslash \mathfrak{m}$. As $x+1 \notin \mathfrak{n}$ we have $1/(x+1) \in B_{\mathfrak{n}}$. If $1/(x+1)$ were integral over $A_{\mathfrak{m}}$, we would have $a_i/s_i \in S_{\mathfrak{m}}^{-1}A$ (in least terms) such that $\sum_{i=0}^{n}[a_i/s_i][1/(x+1)]^i = 0$ in $B_{\mathfrak{n}}$ and $a_n/s_n = 1$. We can rewrite that as $\sum a_i(x+1)^{n-i}/s_i(x+1)^n = 0$, and, B being an integral domain, we can multiply through by $(x+1)^n \prod_{i=0}^{n} s_i$ to get $\sum a_i t_i (x+1)^{n-i} = 0$ in B, where $t_i = \prod_{j \neq i} s_j \in A \backslash (x^2-1)$ and $a_n = 1$. Then $(x+1)$ divides each term but possibly $a_n t_n (x+1)^0 = t_n$. Since $0 \in (x+1)$, this forces $t_n \in (x+1) \cap A = (x^2-1)$, a contradiction.

Let $A \subseteq B$ be rings, B integral over A.

i) If $x \in A$ is a unit in B then it is a unit of A.

Let $x \in A \cap B^{\times}$. Then x is not in any $\mathfrak{n} \in \operatorname{Max}(B)$. Let $\mathfrak{m} \in \operatorname{Max}(A)$. By (4.10), there is $\mathfrak{n} \in \operatorname{Spec}(B)$ such that $\mathfrak{n} \cap A = \mathfrak{m}$, and by (5.8), $\mathfrak{n}$ is maximal. Thus $x \notin \mathfrak{n}$, hence $x \notin \mathfrak{m}$. As $\mathfrak{m}$ was arbitrary, x is in no maximal ideal of A, and hence $x \in A^{\times}$.[2]

ii) The Jacobson radical of A is the contraction of the Jacobson radical of B.

For a maximal ideal $\mathfrak{m}$ of A, (5.10) and (5.8) give a unique maximal ideal $\mathfrak{n}$ of B such that $\mathfrak{n} \cap A = \mathfrak{m}$. Write $N \subseteq \operatorname{Max}(B)$ for the set of these. Then

$$\mathfrak{R}(A) = \bigcap \operatorname{Max}(A) = \bigcap_{\mathfrak{n} \in N} (A \cap \mathfrak{n}) = A \cap \bigcap N \supseteq A \cap \bigcap \operatorname{Max}(B) = A \cap \mathfrak{R}(B).$$

On the other hand, by (5.8) again, the set $M = \{\mathfrak{n} \cap A : \mathfrak{n} \in \operatorname{Max}(B)\}$ is a subset of $\operatorname{Max}(A)$. Thus

$$A \cap \mathfrak{R}(B) = A \cap \bigcap \operatorname{Max}(B) = \bigcap_{\mathfrak{n} \in \operatorname{Max}(B)} (A \cap \mathfrak{n}) = \bigcap M \supseteq \mathfrak{R}(A).$$

Let $B_1, \ldots, B_n$ be integral A-algebras. Show that $\prod_{i=1}^{n} B_i$ is an integral A-algebra.

Use induction, and assume we have the $n = 2$ case. The base step $n = 1$ is trivial, so suppose we have proved the proposition up to n and have $B_1, \ldots, B_{n+1}$ integral A-algebras. The inductive assumption yields that $\prod_{i=1}^{n} B_i$ is an integral A-algebra, and the $n = 2$ case shows $\prod_{i=1}^{n+1} B_i \cong \prod_{i=1}^{n} B_i \times B_{n+1}$ is an integral A-algebra as well.

So it is now enough to prove the $n = 2$ case. Let B and C be integral A-algebras, and $(b, c) \in B \times C$. Then[3], [4]there are $p(x) \in A[x]$ such that $p(b) = 0$ in B and $q(x) \in A[x]$ such that $q(c) = 0$ in C. Therefore $p\big((b,c)\big) = \big(0, p(c)\big)$ and $q\big((b,c)\big) = \big(q(b), 0\big)$ in $B \times C$, so multiplying these, $(pq)\big((b,c)\big) = p\big((b,c)\big)q\big((b,c)\big) = \big(0, p(c)\big)\big(q(b), 0\big) = (0, 0)$, where $(pq)(x)$ has leading coefficient 1, showing (b, c) is integral over the image of A.

Let A be a subring of a ring B, such that the set $B \backslash A$ is closed under multiplication. Show that A is integrally closed in B.

Let $b \in B$ be integral over A, and let $n \geq 2$ be such that b satisfies an equation $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$ for $a_i \in A$. Since $0, a_0 \in A$, we have $b^n + \cdots + a_1 b \in A$. We can factor this as $b(b^{n-1} + \cdots + a_1) \in A$, and since $B \backslash A$ is multiplicatively closed, either $b \in A$ or $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 \in A$. Iterating this process, we eventually arrive at $b + a_{n-1} \in A$, so $b \in A$.

[2] The proof from (5.7) also works without modification. Suppose $x^{-1} \in B$. By uniqueness of inverses in B, the only possible inverse of x in A is x^{-1}, so we need to show $x^{-1} \in A$. Since x^{-1} is integral over A, there are $n > 0$ and $a_i \in A$ such that $x^{-n} = \sum_{i=0}^{n-1} a_i x^{-i}$ holds in B. Multiplying through by x^{n-1} yields $x^{-1} = \sum_{j=0}^{n-1} a_{n-1-j} x^j$, so $x^{-1} \in A$.

[3] This good solution taken from .

[4] Here is a terrible solution I came up with myself. First we show that $f(A) \times g(A)$ is integral over the subalgebra $A' = \operatorname{im}(f, g) = \{(f(a), g(a) : a \in A\} = A \cdot (1, 1)$. Now $f(A) \times g(A)$ is generated over A' by $(1, 0)$ and $(0, 1)$, so it is finitely generated, and $\phi \colon (x, y) \mapsto (bx, cy)$ is an A-module endomorphism of $f(A) \times g(A)$. (2.4) then gives us an equation of the form $\sum_{i \leq n} a_i \phi^i = 0$, where $a_n = 1$; applying both sides to $(1, 1)$ gives $\sum_{i \leq n} a_i (b, c)^i = (0, 0)$, showing (b, c) is integral over A'.

Since $A'' = f(A) \times g(A)$ is integral over $A' = \operatorname{im}(f, g)$, by (5.4) if $B \times C$ is integral over A'', it will also be integral over A'. It suffices by (5.3) to show each of $B \times \{0\}$ and $\{0\} \times C$ is integral over A''. We will prove it for $B \times \{0\}$, the argument for $\{0\} \times C$ being symmetric. So let $(b, 0) \in B \times C$. As b is integral over $\operatorname{im} A \subseteq B$, there are $a_i \in A$ such that $\sum_{0 \leq i \leq n} a_i b^i = 0$. Then $\sum a_i (b, 0)^i = \big(0, g(a_0)\big) \in A''$. Setting $a'_i = f(a_i)$ for $i \neq 0$ and $a'_0 = \big(f(a_0), 0\big)$ we have $\sum a_i (b, 0)^i = (0, 0)$, so $(b, 0)$ is integral over A''.

i) Let A be a subring of an integral domain B, and let C be the integral closure of A in B. Let f, g be monic polynomials in $B[x]$ such that $fg \in C[x]$. Then f, g are in $C[x]$.

(Note that A really plays no part: we could have started with $C \subseteq B$ integrally closed in B, and let $A = C$, with integral closure in B just C again, so without loss of generality we may take $A = C$.)

Let K be the field of fractions of B, let Ω be a splitting field of $fg \in K[x]$. Then in $\Omega[x]$ we have $fg = \prod_i(x - \xi_i)\prod_j(x - \eta_j)$, where the ξ_i are roots of f and the η_j are roots of g. Since each ξ_i and η_j is a root of $fg \in C[x]$, we have each ξ_i and η_j integral over C in Ω. Recall from (5.3) that the set D of elements of Ω integral over C is a ring. Since each coefficient of $f = \prod_i(x - \xi_i)$ (resp. $g = \prod_j(x - \eta_j)$) is a polynomial in the ξ_i (resp. η_j), we have $f, g \in D[x] \cap B[x] = (D \cap B)[x]$. But since $D \cap B$ consists of elements of B integral over C, and C is integrally closed in B, we have $D \cap B = C$, so $f, g \in C[x]$.

ii) Prove the same result without assuming that B (or A) is an integral domain.

Note in particular that considering linear polynomials $(x - b)$, $(x - c)$, this gives us a near-converse to [5.7]: $b + c \in C$ & $bc \in C \iff b, c \in C$

We need to see if we can alter our proof of part i) to avoid fields.[5] The revised version would go as follows: let B^+ be a ring containing B and such that f and g split into linear factors $x - \xi_i$ and $y - \eta_j$ in $B^+[x]$. These linear factors also divide fg, so ξ_i, η_j are roots of fg, and so are integral over C. The coefficients of f and g, being polynomials in the ξ_i and η_j, are then also integral over C by (3.8). But these coefficients are in B, so by assumption also in C.

To create the extension ring B^+ we need, let $\deg(f) = n$ and $\deg(g) = m$, and note that we can extend B to $B_1 = B[x]/\big(f(x)\big)$ to get a larger field in which f has a root $\alpha_1 = \bar{x}$. Then $f(y)$ is in the kernel of the canonical map $B_1[y] \twoheadrightarrow B_1[y]/(y - \alpha_1)$ since in the quotient $\bar{y} = \bar{\alpha}_1$, and $f(\bar{\alpha}_1) = 0$. Thus $f(y)$ is an element of the principal ideal $(y - \alpha_1)$, so there is a monic polynomial $f_1(y)$ in $B_1[y]$ such that $f(y) = f_1(y)(y - \alpha_1)$ in $B_1[y]$. Since degree of monic polynomials is multiplicative, we have $\deg(f_1) = n - 1$. Repeating this process, and because the degree of the non-linear factor decreases each time we make such an extension, we eventually get a ring $B' = B_n$ over which f splits. We can then perform a similar process for g over B' to get a ring $(B')_m = B^+$ in which both f and g split completely.

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

Write C' for the integral closure of $A[x]$ in $B[x]$. Then $x \in A[x] \subseteq C'$ and C is integral over A, hence over $A[x]$, so by (5.3), $A[x] \subseteq C[x] \subseteq C'$.

It is now enough to show $C[x]$ is integrally closed. Let $f \in B[x]$ be such that there exist $g_i \in C[x]$ with $g_n = 1$ and $f^n + \sum_{i=1}^{n-1} g_i f^i + g_0 = 0 \in C[x]$. Since $g_0 \in C[x]$, we have $C[x] \ni f^n + \sum_{i=1}^{n-1} g_i f^i = f(f^{n-1} + \sum_{i=1}^{n-1} g_i f^{i-1})$ a product of monic polynomials in $B[x]$. Then [5.8.ii] says that $f \in C[x]$.

A ring homomorphism $f : A \to B$ is said to have the going-up property *(resp. the* going-down property*) if the conclusion of the going-up theorem (5.11) (resp. the going-down theorem (5.16)) holds for B and its subring $f(A)$.*

Let $f^* : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be the mapping associated with f.

i) Consider the following three statements:

(a) f^* is a closed mapping.

(b) f has the going-up property.

(c) Let $\mathfrak{q}$ be any prime ideal of B and let $\mathfrak{p} = \mathfrak{q}^c$. Then $f^* : \operatorname{Spec}(B/\mathfrak{q}) \to \operatorname{Spec}(A/\mathfrak{p})$ is surjective.

Prove that (a) $\implies$ (b) $\iff$ (c) (See also Chapter 6, Exercise 11.)

Factorize the map canonically as $f = i \circ p$ for $p : A \twoheadrightarrow f(A)$ and $i : f(A) \hookrightarrow B$ the expected maps. p^* canonically homeomorphs $\operatorname{Spec}\big(f(A)\big)$ into the closed subset $V\big(\ker(f)\big) \subseteq \operatorname{Spec}(A)$ by [1.21.iv], and for each $\mathfrak{p} \supseteq \ker(f)$, the third isomorphism theorem (2.1.i) gives $p(A)/p(\mathfrak{p}) \cong A/\mathfrak{p}$, so f will satisfy any of the three properties if and only if i does. Thus we might as well assume $f : A \hookrightarrow B$ is an inclusion.

As far as the going-up property is concerned, by induction, it is enough to show that if $\mathfrak{p} \subseteq \mathfrak{p}' \in \operatorname{Spec}(A)$ and $\mathfrak{q} \in \operatorname{Spec}(B)$ is such that $\mathfrak{q} \cap A = \mathfrak{p}$, then there is $\mathfrak{q}' \supseteq \mathfrak{q}$ such that $\mathfrak{q}' \cap A = \mathfrak{p}'$. This is the same as showing each restriction $f^*\big|_{V(\mathfrak{q})}^{V(\mathfrak{p})} : V(\mathfrak{q}) \to V(\mathfrak{p})$ is surjective.

(a) $\implies$ (b): Since $V(\mathfrak{q})$ ([1.15]) is closed, by assumption $f^*\big(V(\mathfrak{q})\big)$ is a closed set containing $f^*(\mathfrak{q}) = \mathfrak{p}$, so $\overline{\{\mathfrak{p}\}} \subseteq f^*\big(V(\mathfrak{q})\big)$. (In fact, they are equal, for if $\mathfrak{p} \not\subseteq \mathfrak{q}' \cap A$, then $\mathfrak{q} \supseteq \mathfrak{p}$ is not contained in $\mathfrak{q}'$.) But by [1.18.ii], $V(\mathfrak{p}) = \overline{\{\mathfrak{p}\}}$, so $f^*\big|_{V(\mathfrak{q})}^{V(\mathfrak{p})}$ is surjective.

[5] Expanded from http://pitt.edu/~yimuyin/research/AandM/exercises05.pdf

(b) $\iff$ (c): The identifications of [3.21.iii] identify $f^*\big|_{V(\mathfrak{q})}^{V(\mathfrak{p})}$ with the map $\bar{f}^*\colon \operatorname{Spec}(B/\mathfrak{q}) \to \operatorname{Spec}(A/\mathfrak{p})$ induced by $\bar{f}\colon A/\mathfrak{p} \to B/\mathfrak{q}$. Then (b) holds if each $f^*\big|_{V(\mathfrak{q})}^{V(\mathfrak{p})}$ is surjective and (c) if each $\bar{f}^*$ is surjective, but these are essentially the same maps.

Consider the following three statements:

(a′) f^* is an open mapping.

(b′) f^* has the going-down property.

(c′) For any prime ideal $\mathfrak{q}$ of B, if $\mathfrak{p} = \mathfrak{q}^c$, then $f^*\colon \operatorname{Spec}(B_\mathfrak{q}) \to \operatorname{Spec}(A_\mathfrak{p})$ is surjective.

Prove that (a′)$\implies$(b′)$\iff$(c′). (See also Chapter 7, Exercise 23).

(b′) $\iff$ (c′): First we should show the map of (c′) exists. f composed with the canonical map $B \to B_\mathfrak{q}$ yields a map $f^\mathfrak{q}\colon A \to B_\mathfrak{q}$. Since each element of $S_\mathfrak{q} = B\backslash\mathfrak{q}$ by definition becomes a unit in $B_\mathfrak{q}$, and since $f^{-1}(S_\mathfrak{q}) = A\backslash f^{-1}(\mathfrak{q}) = A\backslash\mathfrak{p} = S_\mathfrak{p}$, each element of $S_\mathfrak{p}$ is sent to a unit in $B_\mathfrak{q}$, so by (3.1) there is a unique induced map $A_\mathfrak{p} \to B_\mathfrak{q}$, as hoped. Call this map $f_\mathfrak{p}^\mathfrak{q}$.

By induction, the going-down property requires only that if $\mathfrak{p}' \subseteq \mathfrak{p} \in \operatorname{Spec}(A)$ and $\mathfrak{q} \in \operatorname{Spec}(B)$ is such that $f^*(\mathfrak{q}) = \mathfrak{p}$, then there is $\mathfrak{q}' \subseteq \mathfrak{q}$ such that $f^*(\mathfrak{q}') = \mathfrak{p}'$. This is the same as showing each restriction $f^*\Big|_{S_\mathfrak{q}^{-1}\operatorname{Spec}(B)}^{S_\mathfrak{q}^{-1}\operatorname{Spec}(A)}$ is surjective, where $S^{-1}\operatorname{Spec}(A)$ is the set of primes in A not meeting S. But composing with the canonical inclusions $\operatorname{Spec}(A_\mathfrak{p}) \hookrightarrow S_\mathfrak{p}^{-1}\operatorname{Spec}(A)$ and $\operatorname{Spec}(B_\mathfrak{q}) \hookrightarrow S_\mathfrak{q}^{-1}\operatorname{Spec}(B)$ of [3.21.i], we can identify $(f_\mathfrak{p}^\mathfrak{q})^*$ with this restriction.

(a′) $\iff$ (b′): We claim that open sets in the Zariski topology are "downward closed," meaning $\mathfrak{p}' \subseteq \mathfrak{p} \in U \implies \mathfrak{p}' \in U$. Indeed, write $U = X\setminus C$, C closed. Then $\mathfrak{p}' \notin U$ would imply $\{\mathfrak{p}\} \subseteq C$, so $\overline{\{\mathfrak{p}\}} \subseteq \overline{C} = C$; but by [1.18.ii], $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}') \ni \mathfrak{p}$, so $\mathfrak{p} \in C$ and hence $\mathfrak{p} \notin U$. This may be obvious, but I don't recall having seen it proved.

Recall the notation $S^{-1}X = \{\mathfrak{p} \in X : S \cap \mathfrak{p} = \varnothing\}$ from [3.21.i] and let $X = \operatorname{Spec}(A)$ and $Y = \operatorname{Spec}(B)$. In the special cases $S_\mathfrak{p} = A\backslash\mathfrak{p}$ and $S_g = \{1, g, g^2, \ldots\}$, write $X_\mathfrak{p} = S_\mathfrak{p}^{-1}X$ and $X_g = S_g^{-1}X$. Recall from [3.22] that $Y_\mathfrak{q} \approx \operatorname{Spec}(B_\mathfrak{q})$ is the intersection of all its basic open neighborhoods Y_g ($g \notin \mathfrak{q}$). Write $f^\mathfrak{q}\colon A \to B_\mathfrak{q}$ again for the composition of f with the canonical map $\phi_\mathfrak{q}\colon B \to B_\mathfrak{q}$. Then

$$(f^\mathfrak{q})^*\big(\operatorname{Spec}(B_\mathfrak{q})\big) \overset{[1.21.\text{vi}]}{=} f^*\big(\phi_\mathfrak{q}^*\big(\operatorname{Spec}(B_\mathfrak{q})\big)\big) \overset{[3.21.\text{i}]}{=} f^*(Y_\mathfrak{q}) = \bigcap_{g \notin \mathfrak{q}} f^*(Y_g).$$

By [1.17], the Y_g are open, so the $U_g := f^*(Y_g)$ are open. Then since $\mathfrak{q} \in Y_g$ and $\mathfrak{p} = f^*(\mathfrak{q})$, $\mathfrak{p} \in U_g$, so all primes $\mathfrak{p}' \subseteq \mathfrak{p}$ are in U_g. Intersecting, $X_\mathfrak{p} \subseteq f_\mathfrak{q}^*\big(\operatorname{Spec}(B_\mathfrak{q})\big)$.

Now $f^\mathfrak{q}$ factors through $\phi_\mathfrak{p}\colon A \to A_\mathfrak{p}$ as $f^\mathfrak{q} = f_\mathfrak{p}^\mathfrak{q} \circ \phi_\mathfrak{p}$, so taking *'s, by [1.21.vi] we have $X_\mathfrak{p} \subseteq \operatorname{im}(\phi_\mathfrak{p}^* \circ (f_\mathfrak{p}^\mathfrak{q})^*)$. But $\phi_\mathfrak{p}^*$ is a homeomorphism between $\operatorname{Spec}(A_\mathfrak{p})$ and the open subset $X_\mathfrak{p} \subseteq X$ by [3.21.i], so $(f_\mathfrak{p}^\mathfrak{q})^*$ is surjective.

Let $f\colon A \to B$ be a flat homomorphism of rings. Then f has the going-down property.

[3.18] states that $f^*\colon \operatorname{Spec}(B_\mathfrak{q}) \twoheadrightarrow \operatorname{Spec}(A_\mathfrak{p})$ is surjective for each $\mathfrak{q} \in \operatorname{Spec}(B)$ and $\mathfrak{p} = \mathfrak{q}^c$. Then (c′) $\implies$ (b′) in [5.10] shows f has the going-down property.

Let G be a finite group of automorphisms of a ring A, and let A^G denote the subring of G-invariants, that is of all $x \in A$ such that $\sigma(x) = x$ for all $\sigma \in G$. Prove that A is integral over A^G.

The first (rather trivial) thing to do is to show A^G is a ring. But indeed, by the definition of a ring homomorphism we have $\sigma(1) = 1$ for all $\sigma \in G$, and if $a, b \in A^G$, then $\sigma(a - b) = \sigma(a) + \sigma(-b) = a - b$ and $\sigma(ab) = \sigma(a)\sigma(b) = ab$ for all $\sigma \in G$. Thus A^G, containing 1 and being closed under subtraction and multiplication, is a subring of A.

To see $A^G \hookrightarrow A$ is integral, let $x \in A$, and let t be an indeterminate. If $p := \prod_{\sigma \in G}\big(t - \sigma(x)\big) \in A[t]$, then each coefficient of p is a symmetric polynomial in the $\sigma(x)$, so $p \in A^G[t]$. As p is monic and $0 = x - x$ divides $p(x)$, we see x is a root of p, and so x is integral over A^G.

Let S be a multiplicatively closed subset of A such that $\sigma(S) \subseteq S$ for all $\sigma \in G$, and let $S^G = S \cap A^G$. Show that the action of G on A extends to an action on $S^{-1}A$, and that $(S^G)^{-1}A^G \cong (S^{-1}A)^G$.

Suppose $a/s = b/t \in S^{-1}A$. Then there is $u \in S$ such that $uta = usb$ in A. Applying $\sigma \in G$ yields $\sigma(u)\sigma(t)\sigma(a) = \sigma(u)\sigma(s)\sigma(b)$ in A, meaning $\sigma(a)/\sigma(s) = \sigma(b)/\sigma(t)$ in $S^{-1}A$. Thus if we define the action of G on $S^{-1}A$ by

$\sigma(a/s) \coloneqq \sigma(a)/\sigma(s)$, this definition is independent of the choice of representatives, hence well defined. It is obviously multiplicative, and only slightly less obviously additive:

$$\sigma\left(\frac{a}{s}+\frac{b}{t}\right)=\sigma\left(\frac{at+bs}{st}\right)=\frac{\sigma(at+bs)}{\sigma(st)}=\frac{\sigma(a)\sigma(t)+\sigma(b)\sigma(s)}{\sigma(s)\sigma(t)}=\frac{\sigma(a)}{\sigma(s)}+\frac{\sigma(b)}{\sigma(t)}=\sigma\left(\frac{a}{s}\right)+\sigma\left(\frac{b}{t}\right).$$

For each $a \in A^G$, we have $\sigma(a/1)=\sigma(a)/1=a/1$, so the natural map $A^G \hookrightarrow A \to S^{-1}A$ factors as $A^G \to (S^{-1}A)^G \hookrightarrow S^{-1}A$. Each element $s \in S^G$ becomes a unit in $S^{-1}A$, hence a unit in $(S^{-1}A)^G$ since $\sigma(1/s)=\sigma(1)/\sigma(s)=1/s$ for all $\sigma \in G$. Thus (3.1) gives a unique homomorphism $\chi : (S^G)^{-1}A^G \to (S^{-1}A)^G$ taking $a/s \mapsto a/s$.

χ is injective, for if $a/s=0$ in $(S^{-1}A)^G \subseteq S^{-1}A$, there is $t \in S$ such that $ta=0$. Then taking $t'=\prod_{\sigma\in G}\sigma(t)$, we also have $t'a=0$, meaning $a/s=0$ already in $(S^G)^{-1}A^G$.

On the other hand, let $a/s \in (S^{-1}A)^G$ Let $s'=\prod_{\sigma\neq \mathrm{id}_A}\sigma(s)\in S^G$. Then since a/s and $ss'/1$ are invariant, so is their product $as'/1$. Thus for every $\sigma \in G$ we have $\sigma(as')/1 = s(as'/1) = as'/1$, so there is $t_\sigma \in S$ such that $t_\sigma as' = t_\sigma \cdot \sigma(as')$. Set $t=\prod_{\tau\in G}\tau\bigl(\prod_{\sigma\in G}t_\sigma\bigr)\in S^G$. Then since t_σ divides t we have $\sigma(tas')=t\cdot\sigma(as')=tas'$, so $tas' \in A^G$. Then $a/s = ts'a/ts's$ with $ts'a \in A^G$ and $ts's \in S^G$, so χ is surjective.

In the situation of Exercise 12, let $\mathfrak{p}$ be a prime ideal of A^G, and let P be the set of prime ideals of A whose contraction is $\mathfrak{p}$. Show that G acts transitively on P. In particular, P is finite.

Let $\mathfrak{q}, \mathfrak{q}' \in P$. For any $x \in \mathfrak{q}$, we have $\prod_{\sigma\in G}\sigma^{-1}(x)\in A^G\cap\mathfrak{q}=\mathfrak{p}$. But also $\mathfrak{p}=A^G\cap\mathfrak{q}'$, so $\prod_{\sigma\in G}\sigma^{-1}(x)\in\mathfrak{q}'$. Thus, since $\mathfrak{q}$ is prime, for some $\sigma\in G$ we have $y=\sigma^{-1}(x)\in\mathfrak{q}'$. Then $x=\sigma(y)\in\sigma(\mathfrak{q}')$. Since $x\in\mathfrak{q}$ was arbitrary, we see $\mathfrak{q}\subseteq\bigcup_{\sigma\in G}\sigma(\mathfrak{q}')$. By (1.11.i), $\mathfrak{q}$ is contained in some $\sigma(\mathfrak{q}')$. Since both $\mathfrak{q}\cap A^G=\mathfrak{p}$ and $\sigma(\mathfrak{q}')\cap A^G=\sigma(\mathfrak{q}')\cap\sigma(A^G)=\sigma(\mathfrak{q}'\cap A^G)=\sigma(\mathfrak{p})=\mathfrak{p}$, (5.9) says we must have $\mathfrak{q}=\sigma(\mathfrak{q}')$. As $\mathfrak{q}$ and $\mathfrak{q}'\in P$ were arbitrary, it follows that G sends any element of P to any other element of P, so G acts transitively. Since G is finite, and sends $\mathfrak{q}$ to every element of P, we have $|P|=|G|/|\mathrm{Stab}_G(\mathfrak{q})|\leq|G|$ finite.

Let A be an integrally closed domain, K its field of fractions and L a finite normal separable extension of K. Let G be the Galois group of L over K and let B be the integral closure of A in L. Show that $\sigma(B)=B$ for all $\sigma\in G$, and that $A=B^G$.

If $b\in B$, then there it satisfies a polynomial equation $\sum a_i b^i=0$ for some $a_i\in A=A^G$. Applying a $\sigma\in G$ to this equation yields $0=\sigma(0)=\sigma\bigl(\sum a_i b^i\bigr)=\sum\sigma(a_i)\sigma(b)^i=\sum a_i\sigma(b)^i$. Thus $\sigma(b)$ satisfies a monic polynomial (the same as b does) over A, and hence is in B. Thus $\sigma(B)\subseteq B$. On the other hand, replacing σ by σ^{-1} in this reasoning yields $\sigma^{-1}(B)\subseteq B$, and applying σ to both sides gives $B=\sigma\bigl(\sigma^{-1}(B)\bigr)\subseteq\sigma(B)$. Since $\sigma\in G$ was arbitrary, $B=\sigma(B)$ for all $\sigma\in G$.

$B^G=B\cap L^G=B\cap K=A$, since K is the fixed field of G and A is integrally closed in K.

Let A, K be as in Exercise 14, let L be any finite extension field of K, and let B be the integral closure of A in L. Show that, if $\mathfrak{p}$ is any prime ideal of A, then the set of prime ideals $\mathfrak{q}$ of B which contract to $\mathfrak{p}$ is finite (in other words, that $\mathrm{Spec}(B)\to\mathrm{Spec}(A)$ *has finite fibers).*

Recall[6] that any extension factors as a separable extension followed by a purely inseparable extension. Since a product of two finite numbers is finite, it suffices to show the fibers are finite for either of these kinds of extensions.

In the case of a separable extension L/K, let $\Omega/L/K$ be the least normal extension of K containing L. Write C for the integral closure of A in Ω; it is clearly also integral over B. If B had infinitely many primes lying over $\mathfrak{p}$, then (5.10) would give us at least one prime of C lying over each of those, hence infinitely many primes of C lying over $\mathfrak{p}$. But $\Omega\supseteq K$ is a finite extension, so $H=\mathrm{Gal}(\Omega/K)$ is finite. By [5.14], $A=C^H$, so by [5.13] there are only finitely many primes of C lying over $\mathfrak{p}$.

In the case of a finite, purely inseparable extension L/K of fields of characteristic $p>0$, it is well known[7] that for each $x\in L$ there is $n\geq 0$ such that $x^{p^n}\in K$. If we let $x_1,\ldots,x_m$ generate L as a vector space over K, and let $n_i\geq 0$ be the least exponents such that ${x_i}^{p^{n_i}}\in K$, then if $n=\max_i n_i$, we have for all $c_i\in K$ that $\bigl(\sum_{i=1}^m c_i x_i\bigr)^{p^n}=\sum_{i=1}^m c_i^{p^n}x_i^{p^n}\in K$, (using the binomial theorem and the fact that p divides $\binom{p^n}{l}$ for $0<l<p^n$), so that $L^{p^n}\subseteq K$. Write B for the integral closure of A in L, and suppose $\mathfrak{P}\in\mathrm{Spec}(B)$ lies over $\mathfrak{p}\in\mathrm{Spec}(A)$. If $x\in B$ has $x^{p^n}\in\mathfrak{p}\subseteq\mathfrak{P}$, then as $\mathfrak{P}$ is prime we have $x\in\mathfrak{P}$; and if $x\in\mathfrak{P}$, then $x^{p^n}\in\mathfrak{P}\cap K=\mathfrak{p}$. Thus $\mathfrak{P}$ is determined uniquely by $\mathfrak{p}$, so the only possibility for a prime of B lying over $\mathfrak{p}$ is $\mathfrak{P}\coloneqq\{x\in B : x^{p^n}\in\mathfrak{p}\}$. To see $\mathfrak{P}$ really is an ideal, note that $b\in B$

[6] http://planetmath.org/encyclopedia/PurelyInseparable.html

[7] or sometimes the definition: http://planetmath.org/encyclopedia/PurelyInseparable.html

and $x, y \in \mathfrak{P}$ imply $(bx)^{p^n} = b^{p^n} x^{p^n} \in A\mathfrak{p} = \mathfrak{p}$ and $(x-y)^{p^n} = x^{p^n} + (-y)^{p^n} \in \mathfrak{p}$. To see $\mathfrak{P}$ is prime, suppose $xy \in \mathfrak{P}$ but $x \notin \mathfrak{P}$; then $x^{p^n} y^{p^n} \in \mathfrak{p}$ but $x^{p^n} \notin \mathfrak{p}$, so $y^{p^n} \in \mathfrak{p}$ and $y \in \mathfrak{P}$.

Noether's normalization lemma

Let k be a field and let $A \neq 0$ be a finitely generated k-algebra. Then there exist elements $y_1, \ldots, y_r \in A$ which are algebraically independent over k and such that A is integral over $k[y_1, \ldots, y_r]$.

We shall assume that k is infinite. *(The result is still true if k is finite, but a different proof is needed.) Let $x_1, \ldots, x_n$ generate A as a k-algebra. We can renumber the x_i so that $x_1, \ldots, x_r$ are algebraically independent over k and each of $x_{r+1}, \ldots, x_n$ is algebraic over $k[x_1, \ldots, x_r]$. Now proceed by induction on n. If $n = r$ there is nothing to do, so suppose $n > r$ and the result true for $n-1$ generators. The generator x_n is algebraic over $k[x_1, \ldots, x_{n-1}]$, hence there exists a polynomial $f \neq 0$ in n variables such that $f(x_1, \ldots, x_{n-1}, x_n) = 0$. Let F be the homogeneous part of highest degree in f. Since k is infinite, there exist $\lambda_1, \ldots, \lambda_{n-1} \in k$ such that $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Put $x_i' = x_i - \lambda_i x_n$ $(1 \leq i \leq n-1)$. Show that x_n is integral over the ring $A' = k[x_1', \ldots, x_{n-1}']$ and hence that A is integral over A'. Then apply the inductive hypothesis to A' to complete the proof.*

First, if the λ_i didn't exist, we would have $F(x_1, \ldots, x_{n-1}, x_n) = x_n^{\deg F} F(x_1, \ldots, x_{n-1}, 1) = 0$ by homogeneity. But k being infinite, F is zero as a function $k^n \to k$ if and only if $F = 0 \in k[x_1, \ldots, x_n]$.[8]

Let $F = \sum_I a_I \prod_{j=1}^n x_j^{i_j} = \sum_I a_I x_n^{i_n} \prod_{j=1}^{n-1} (x_j' + \lambda_j x_n)^{i_j}$. The coefficient of $x_n^{\deg F}$ in $F \in k[x_1', \ldots, x_{n-1}', x_n]$ is $c := \sum a_I \lambda_1^{i_1} \cdots \lambda_{n-1}^{i_{n-1}} = F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$, so that the equation $c^{-1} f(x_1, \ldots, x_{n-1}, x_n) = 0$ is monic when written in $A'[x_n]$. Thus x_n is integral over A', and so $A = k[x_1, \ldots, x_n]$ is integral over A' by (5.3). But by the induction hypothesis, A' is integral over some $k[y_1, \ldots, y_r]$, with $y_1, \ldots, y_r$ algebraically independent over k, and by the transitivity (5.4) of integral dependence, A is integral over $k[y_1, \ldots, y_r]$.[9]

From the proof [of [5.16]] it follows that $y_1, \ldots, y_r$ may be chosen to be linear combinations of $x_1, \ldots, x_n$. This has the following geometrical interpretation: if k is algebraically closed and X is an affine algebraic variety in k^n with coordinate ring $A \neq 0$, then there exists a linear subspace L of dimension r in k^n and a linear mapping of k^n onto L which maps X onto L.

$$\begin{tikzcd} X \arrow[r, hook, "\iota"] \arrow[dr, two heads, "\rho"'] & k^n \arrow[d, two heads, "\pi"] \\ & k^r \end{tikzcd}$$

$$\begin{tikzcd} A = k[x] & k[t] \arrow[l, two heads, "\iota^\#"'] \\ & k[y] \arrow[u, tail, "\pi^\#"'] \arrow[ul, tail, "\varpi"] \end{tikzcd}$$

We want the commutative diagram of regular maps on the right, with π linear. Letting the coordinate ring ([1.27]) of k^n be $k[t]$, that of the affine algebraic variety $X \subseteq k^n$ be $A = k[t]/I(X) = k[x]$, and that of k^r be $A_0 := k[y]$, [1.28] says that this is equivalent to demanding the diagram of k-algebra homomorphisms below it. Here $\iota^\#$ is the projection $t_j \mapsto x_j : k[t_1, \ldots, t_n] \twoheadrightarrow A$. The normalization proven above gives us a candidate map $\varpi : A_0 \rightarrowtail A$, namely the k-subalgebra inclusion gotten by mapping the y_i to algebraically independent elements x_i' of A such that A is integral over $A' = k[x_1', \ldots, x_r']$. In the course of the proof above, we found that when k is infinite (which is true if k is algebraically closed), we can take the x_i' to be k-linear combinations of the x_j. If $x_i' = \sum_{j=1}^n a_{ij} x_j$ in A for $a_{ij} \in k$, $1 \leq i \leq r$ and $1 \leq j \leq n$, and we want $\iota^\# \circ \pi^\# = \varpi$, we may take $\pi^\#(y_i) := \sum_{j=1}^n a_{ij} t_j$. Since $y_i : k^r \twoheadrightarrow k$ is the i^{th} projection and $\pi^\#(\eta) = \eta \circ \pi$ by definition, it follows that π should be given by $(v_1, \ldots, v_n) \mapsto \big(\sum_{j=1}^n a_{1j} v_j, \ldots, \sum_{j=1}^n a_{rj} v_j, \big)$. This is obviously linear, and by Eq. 1.2 of [1.28], $\varpi = \iota^\# \circ \pi^\# = (\pi \circ \iota)^\# = \rho^\#$ as hoped. (This map is not, as defined, to a linear *subspace* $L \subseteq k^n$, but we can if we like pick any r linearly independent vectors $w_i \in k^n$ and define a new map by $v \mapsto \sum (y_i \circ \pi)(v) w_i$.)

To see that ρ is surjective, let a point of k^r be given. Write it as an inclusion $p : \{0\} \to k^r$. It corresponds by [1.28] to a map $\psi_p : A_0 = k[y] \to k$ and hence to a map $A' = k[x'] \to k$.[10] Since A is integral over A', by [5.2] this

[8] Proved by induction, e.g. in Theorem 5.18 in *Fields and Galois Theory*, J.S. Milne, http://jmilne.org/math/CourseNotes/ft.html: if $n = 1$ and $F \neq 0$ then F has $\leq \deg(F)$ roots, so is not identically zero since k is infinite. Assume the result has been proved for n, let $F \in k[x_1, \ldots, x_{n+1}]$ be zero on k^{n+1}, and write $0 = F = \sum G_i x_{n+1}^i$ for $G_i \in k[x_1, \ldots, x_n]$. For any $(a_1, \ldots, a_n) \in k^n$ we have $F(a_1, \ldots, a_n, x_{n+1}) \in k[x_{n+1}]$ identically zero by assumption, so by the $n = 1$ case each $G_i(a_1, \ldots, a_n) = 0$. Then by the induction step each $G_i = 0$, so $F = 0$.

[9] We include as a bonus a proof (http://ericmalm.net/ac/projects/math210b-w08/math210b-transcendence.pdf) that works when k is finite. Again, assume that x_n is algebraic over $k[x_1, \ldots, x_{n-1}]$, and say that this is witnessed by $f(x_1, \ldots, x_n) = 0$. Let $d > \deg f$, and $x_i' = x_i - x_n^{d^i}$ for $i = 1, \ldots, n-1$. Write $x_i = x_i' + x_n^{d^i}$ in $f = 0$. Expanding out each monomial term $a_I x^I := a_I x_1^{i_1} \cdots x_n^{i_n}$ of f in terms of x_n and the x_i', the monomial term $a_I x_n^{e_I}$ divisible only by x_n will have have exponent $e_I = i_n + i_1 d + i_2 d^2 + \cdots + i_{n-1} d^{n-1}$. By our choice of d, the exponents e_I are all distinct as we range over different $a_I x^I$, so there is no cancellation among them. One such exponent e_M will be the greatest, and then we can divide through by the corresponding coefficient a_M to get $a_M f(x_1' + x_n^d, \ldots, x_{n-1}' + x_n^{d^{n-1}}, x_n) = 0$ monic in x_n. This shows A is integral over A', and we conclude as before. Note that we no longer have that the x_i are k-linear combinations of elements of A', however.

[10] http://math.stackexchange.com/questions/24794/atiyah-macdonald-exercises-5-16-5-19

extends to a map $\phi_b \colon A \to k$, corresponding to an inclusion $b \colon \{0\} \to X$. We have $\phi_b \circ \varpi = \psi_p$, so by Eq. 1.2 of [1.28] again, $\rho \circ b = p$.[11] We show in [8.5] that the fibers of ρ are finite of bounded cardinality.

Nullstellensatz (weak form).

Let X be an affine algebraic variety in k^n, where k is an algebraically closed field, and let $I(X)$ be the ideal of X in the polynomial ring $k[t_1, \ldots, t_n]$ Chapter 1, Exercise 27. If $I(X) \neq (1)$ then X is not empty.

Write $k[t] := k[t_1, \ldots, t_n]$. If $I(X) \neq (1)$, then $A = k[t]/I(X) \neq 0$, so by [5.16], X is carried by a linear projection onto a linear subspace $L \subseteq k^n$. Since L is non-empty, so must be X. Let's call this the *weaker Nullstellensatz*.

The name "*weak Nullstellensatz*" usually refers to the following related result:

Weak Nullstellensatz. *If k is an algebraically closed field and $\mathfrak{a} \lhd k[t_1, \ldots, t_n]$ is not (1), then $Z(\mathfrak{a}) \neq \varnothing$.*

This implies the weaker Nullstellensatz, for if $X = Z(\mathfrak{a})$ and $I(X) \neq (1)$, then since $\mathfrak{a} \subseteq IZ(\mathfrak{a}) \neq (1)$, we have $\mathfrak{a} \neq (1)$ and hence $X = Z(\mathfrak{a}) \neq \varnothing$. The weak Nullstellensatz would also *follow from* the weaker Nullstellensatz if we could prove $\mathfrak{a} \neq (1) \implies IZ(\mathfrak{a}) \neq (1)$. This is an easy consequence of the strong Nullstellensatz of [7.14], but one wants to prove strong from weak, not vice versa.

Deduce that every maximal ideal in the ring $k[t_1, \ldots, t_n]$ is of the form $(t_1 - a_1, \ldots, t_n - a_n)$ where $a_i \in k$.

This is also the result of [1.27], and there is a proof there. It does not seem to obviously follow from the weaker Nullstellensatz above, which we are supposed to use to prove it,[12] but does from the weak Nullstellensatz, which is in fact equivalent.

First assume the weak Nullstellensatz. If $\mathfrak{m} \lhd k[t]$ is a maximal ideal, then $Z(\mathfrak{m}) \neq \varnothing$, so there exists an $x \in Z(\mathfrak{m})$, meaning $\mathfrak{m} \subseteq IZ(\mathfrak{m}) \subseteq \mathfrak{m}_x$; as $\mathfrak{m}$ is maximal, it follows $\mathfrak{m} = \mathfrak{m}_x$. Now assume all maximal ideals of $k[t]$ come from points of k^n. Any $\mathfrak{a} \neq (1)$ is contained in some maximal ideal $\mathfrak{m}$ by (1.4), and by assumption $\mathfrak{m} = \mathfrak{m}_x$ for some $x \in k^n$, so since $\mathfrak{m}_x$ vanishes at x by definition, $x \in Z(\mathfrak{a})$.

Let k be a field and let B be a finitely generated k-algebra. Suppose that B is a field. Then B is a finite algebraic extension of k. (This is another version of Hilbert's Nullstellensatz. The following proof is due to Zariski. For other proofs, see (5.24), (7.9).)

This is called *Zariski's Lemma*, and there are other proofs at (1.27.2*), (5.24), (7.9).[13] Here is a simpler proof than that suggested.[14] Use Noether normalization ([5.16]) on the finitely generated k-algebra B: then there exist (possibly zero) elements $y_1, \ldots, y_r \in B$, algebraically independent over k, such that B is integral over $A = k[y_1, \ldots, y_r]$. By (5.7), B being a field implies A is a field, so there are zero y's and thus $A = k$. Then B is integral over k, hence a finite algebraic extension.

Now we proceed with the book's intended proof.

Let $x_1, \ldots, x_n$ generate B as a k-algebra. The proof is by induction on n. If $n = 1$ the result is clearly true, so assume $n > 1$.

If $B = k[x_1]$ is a field, it follows $x_1^{-1} \in B$, say $x_1^{-1} = \sum_{i=0}^n c_i x_1^i$ for $c_i \in k$. Multiplying both sides by x_1 and subtracting 1 gives $0 = \sum_{i=0}^n c_i x_1^{i+1} - 1$, showing x_1 is algebraic over k, so $B = k(x_1)$ is a finite algebraic extension.

Let $A = k[x_1]$ and let $K = k(x_1)$ be the field of fractions of A. By the inductive hypothesis, B is a finite algebraic extension of K, hence each of $x_2, \ldots, x_n$ satisfies a monic polynomial equation with coefficients in K, i.e. coefficients of the form a/b

[11] This can also be verified by evaluating both sides of $\phi_b \circ \varpi = \psi_p$ at each y_i:

$$y_i(p) = \phi_b\big(\sum a_{ij} x_j\big) = \sum a_{ij} b_j = \pi^\#(y_i)(b) = y_i\big(\pi(b)\big).$$

Note that kernels did not need to be mentioned here. One can also, however, prove ρ is surjective using the result of [1.27] that the maximal ideals of $P(X)$ are in bijection with the points of X. The regular map $\rho \colon X \to L$ induces by precomposition a homomorphism $\varpi = \rho^\# \colon P(Y) \to P(X)$, which in turn induces through contraction a map $\varpi^* \colon \operatorname{Spec}\big(P(X)\big) \to \operatorname{Spec}\big(P(Y)\big)$. Since A is integral over A_0, by (5.8) contractions of maximal ideals are maximal, so this restricts to a map $\widetilde{\rho} \colon \operatorname{Max}\big(P(X)\big) \to \operatorname{Max}\big(P(Y)\big)$. The identification $X \longleftrightarrow \operatorname{Max}\big(P(X)\big)$ conflates $\widetilde{\rho}$ with the original ρ by [1.28], so it is enough to show $\widetilde{\rho}$ is surjective. Since A is integral over A_0, this follows from (5.10) and (5.8).

[12] This has caused me some consternation; see the discussion at `http://math.stackexchange.com/questions/24794/atiyah-macdonald-exercises-5-16-5-19`.

[13] The original proof, from Oscar Zariski, "A new proof of Hilbert's Nullstellensatz", *Bull. Amer. Math. Soc.* Volume 53, Number 4 (1947), 362–368, can be found online at `http://projecteuclid.org/DPubS?verb=Display&version=1.0&service=UI&handle=euclid.bams/1183510605`.

[14] `http://www.math.lsa.umich.edu/~hochster/615W10/supNoeth.pdf`

where a and b are in A. If f is the product of the denominators of all these coefficients, then each of $x_2, \dots, x_n$ is integral over A_f.

Write a_i/b_i for the coefficients, with $a_i, b_i \in A$. If $f = \prod b_i$, then $a_i/b_i = a_i\big(\prod_{j\neq i} b_j\big)/f \in A_f$.

Hence B and therefore K is integral over A_f.

By (5.3), $B = A[x_2, \dots, x_n]$ is integral over A_f, so since $K \subseteq B$, we see K is also integral over A_f.

Suppose x_1 is transcendental over k. Then A is integrally closed, because it is a unique factorization domain.

First we show a UFD A is integrally closed. Suppose an element of its field of fractions is integral over A. We can write it in least terms as a/b, since A has unique factorization. Then $(a)+(b) = (1)$ in A, so $(a^n)+(b) = (1)$ for all n by (1.16). We have an equation $0 = (a/b)^n + \sum_{i=0}^{n-1} c_i(a/b)^i$, and multiplying by b^n gives $a^n = -\sum_{i=0}^{n-1} c_i a^i b^{n-i} \in (b)$. But then $(1) = (a^n) + (b) = (b)$, so b is a unit and $a/b \in A$.

Now, if x_1 is transcendental over k, then $A = k[x_1]$ has a division algorithm, so it is a PID and hence a UFD.

Hence A_f is integrally closed (5.12), and therefore $A_f = K$, which is clearly absurd.

(5.12) says A_f is the integral closure of A_f in $K_f \cong K$. But in the previous paragraph we showed K was integral over A_f, so $K = A_f$. To see this is impossible, see (5.18.1*) below.[15]

Hence x_1 is algebraic over k, hence K (and therefore B) is a finite extension of k.

We take this opportunity to prove a more general result, the Zariski–Goldman–Krull theorem.[16]

Definition. *A* Goldman domain *is a domain A containing some element a such that the localization A_a is a field.*

Note that then A_a is the field of fractions of A. Note also that an iterated localization $\big((A_a)_{\dots}\big)_z = A_{a\cdots z}$, so we can equivalently say a Goldman domain is a domain A whose field of fractions is a finitely generated A-algebra.

Lemma 5.18.1*. *No polynomial ring $A[x]$ is a Goldman domain.*

Proof. Assume A is a domain: if not, neither would $A[x]$ be Let K be the field of fractions of A. If $A[x]$ were a Goldman domain, then so would $K[x]$ be, since $K[x] = K \cdot A[x]$ and $K(x) = K \cdot A(x)$. Cribbing from Euclid, note that given any finite list of irreducible polynomials $p_i \in K[x]$, none divides $1 + \prod p_i$, so there are infinitely many irreducibles in $K[x]$. Since $K[x]$ is a UFD, there are then for any $f \in A[x]$ irreducible p not dividing any power f^n, so that $1/p \notin K[x]_f$.[17] □

Corollary 5.18.2*. *If a field L contains a subfield K and there exist elements $\beta \in L$ and $b \in K[\beta]$ such that $K[\beta]_b = L$, then β is integral over K; in this case, $K[\beta]$ is a field, so $b^{-1} \in K[\beta]$ as well and $L = K[\beta]$.*

Lemma 5.18.3*. *Suppose $A \subseteq A[\beta] = B \subseteq B_b = L$, where L is a field. Then there exists $a \in A$ such that A_a is a field and L is a finite extension of A_a.*

Proof. Write K for the field of fractions of A. Since $L = B_b = A[\beta]_b$, we see $L = K[\beta]_b$ as well, so by (5.18.2*), β is integral over K and $L = K[\beta]$. Thus $[L : K]$ is finite and $b \in L$ is integral over K. Multiplying denominators in the equations witnessing integrality of b and β over K, we obtain an $a \in A$ such that b and β are integral over A_a and hence the field $L = A_a[\beta]_b$ is integral over A_a. But then, by (5.7) or [5.5.i], A_a must be a field, and hence, being intermediate between A and its field of fractions, so must itself be K. □

Zariski–Goldman–Krull Theorem. *If a field L is a finitely generated algebra over a subring A, then there exists $a \in A$ such that A_a is a field and L is a finite extension field of A_a.*

[15] Alternately, find a non-zero proper ideal of A_f. By (3.11.iv), any ideal of A not meeting $S_f = \{1, f, f^2, \dots\}$ yields a proper ideal of A_f. But, for example, $(1-f)$ does not meet S_f, by unique factorization in $k[f]$, so $(1-f) \lhd A_f$ is a non-zero proper ideal.

[16] This sequence of results is a mild reformulation of the proof given by Daniel J. Bernstein at `http://cr.yp.to/zgk.html`.

[17] This proof is from Proposition 12.5 of Pete L. Clark's `http://math.uga.edu/~pete/integral.pdf`.

Here is an alternate proof taken from Richard G. Swan, "On Munshi's proof of the Nullstellensatz," at `http://www.math.uchicago.edu/~swan/nss.pdf`. Suppose for a contradiction there exists $f \in A[x]$ such that $A[x]_f$ is a field. Then $f \notin A$, for otherwise we would have $A[x]_f = A_f[x]$ a polynomial ring, so $\deg f \geq 1$, and in particular $1-f \neq 0$. Since $(1-f)^{-1} = g/f^n$ for some $g \in A[x]$, clearing denominators yields $f^n = (1-f)g$ in $A[x]$. Modulo $1-f$, we have $1 \equiv f$, so $1 \equiv f^n \equiv (1-f)g \equiv 0$, meaning $1-f$ is a unit of $A[x]$; but $\deg(1-f) \geq 1$ and A contains no nonzero nilpotents, so this is impossible by [1.2.i].

Proof. The proof proceeds by induction on the number n of generators for L over A. For $n = 0$, the result is trivial, since $L = A = A_1$. Assume the result proved for n generators and let $L' = A[\alpha_1, \ldots, \alpha_{n+1}]$ for some $\alpha_j \in L'$. Write $B = A[\alpha_1]$ and L for its field of fractions. The induction hypothesis, applied to the extension $B \subseteq L'$, yields $b \in B$ such that B_b $(= L)$ is a field and $[L' : L]$ is finite; and (5.18.3*), applied to $A \subseteq L$, yields $a \in A$ such that A_a is a field and $[L : A_a]$ is finite. Then $[L' : A_a] = [L' : L][L : A_a]$ is finite, concluding the induction. □

Zariski's Lemma is an immediate corollary. We will also meet Jacobson rings in [5.23], and show in (5.23.5*) that a ring is Jacobson if and only if its every quotient Goldman domain is a field.

Corollary 5.18.4*. *If a field L is a finitely generated algebra over a quotient domain B of a Jacobson ring A, then B is a field and L is a finite extension of B.*

Proof. By the Zariski–Goldman–Krull Theorem, B is a Goldman domain and L is a finite extension of its field of fractions. Since A is Jacobson, B is a field by (5.23.5*). □

Note that this is also the direction i) $\implies$ ii) of [5.25].

Generalized Nullstellensatz. *If A is a Jacobson ring and C a finitely generated A-algebra, then C is a Jacobson ring. If $\mathfrak{m} \lhd C$ is a maximal ideal of C, then $\mathfrak{m}^c$ is a maximal ideal of A and $C/\mathfrak{m}$ is a finite extension field of $A/\mathfrak{m}^c$.*[18]

Proof. The first statement is (ii) from [5.24]. For the second, write $A' = \operatorname{im} A \subseteq C$ and $\mathfrak{p} = \mathfrak{m} \cap A'$. Then $L = C/\mathfrak{m}$ is a field finitely generated over the domain $B = A'/\mathfrak{p}$, so by (5.18.4*), L is finite over B and B is a field. This means $\mathfrak{p}$ is maximal. By the correspondence (1.1) applied to $A \twoheadrightarrow A'$, it follows $\mathfrak{m}^c \lhd A$ is maximal and $A/\mathfrak{m}^c \cong A'/\mathfrak{p} = B$. □

Note how the second clause generalizes (1.27.3*): the codomain is now allowed to be any Jacobson ring finitely generated over the domain.

Deduce the result of Exercise 17 from Exercise 18.

Let k be an algebraically closed field. We prove (1.27.4*) from [1.27], namely that all maximal ideals $\mathfrak{m}$ of $k[t] := k[t_1, \ldots, t_n]$ come from points; the other results then follow as explained in [5.17]. $B = k[t]/\mathfrak{m}$ is a field finitely generated as a k-algebra, so by [5.18] it is a finite extension of k. Since k is algebraically closed, this gives a k-algebra isomorphism $\phi : B \xrightarrow{\sim} k$. If $t_i \mapsto x_i$ under the composition $k[t] \twoheadrightarrow B \xrightarrow{\sim} k$, then $t_i - x_i \in \mathfrak{m}$, so $\mathfrak{m}_x \subseteq \mathfrak{m}$. As $\mathfrak{m}_x$ is maximal, the two are equal.

Let A be a subring of an integral domain B such that B is finitely generated over A. Show that there exists $s \neq 0$ in A and elements $y_1, \ldots, y_n$ in B, algebraically independent over A and such that B_s is integral over B'_s, where $B' = A[y_1, \ldots, y_n]$.

Can we invoke ZGK?

Since B is an integral domain, so must A be. Let $S = A \backslash \{0\}$, so that $k = S^{-1}A$ is a field. Since B is finitely generated over A, $S^{-1}B$ is finitely generated over k. By Noether normalization ([5.16]), there exist elements $y_1/s_1, \ldots, y_n/s_n$ of $S^{-1}B$, with $y_i \in B$ and $s_i \in S$, which are algebraically independent over k and such that $S^{-1}B$ is integral over $C = k[y_1/s_1, \ldots, y_n/s_n]$. It follows that the y_j are also algebraically independent over A. Let $x_1, \ldots, x_r$ generate B over A; then the $x_i/1$ generate $S^{-1}B$ over k, and a fortiori over C. Since $S^{-1}B$ is integral over C, each $x_i/1$ satisfies a monic polynomial $p_i(x) = \sum c_{i,j}(x_i/1)^j$ in $C[x]$. Let $s \in S$ be so large that $sc_{i,j} \in B'$ for all i, j (multiply all the denominators). Then $p_i(x) \in B'_s[x]$ for each i, so each $x_i/1$ is integral over B'_s. Since $B_s = B'_s[x_1/1, \ldots, x_r/1]$, we see from (5.3) that B_s is integral over B'_s.

Let A, B be as in Exercise 20. Show that there exists $s \neq 0$ in A such that, if Ω is an algebraically closed field and $f : A \to \Omega$ is a homomorphism for which $f(s) \neq 0$, then f can be extended to a homomorphism $B \to \Omega$.

Recall $s \in A \backslash \{0\}$ from the previous proof, and suppose $f(s) \neq 0$. Then by (3.1) f extends uniquely to a map $f_s : A_s \to \Omega$. Next, $B'_s = A_s[y_1, \ldots, y_n]$ is a polynomial ring over A_s, so we may pick any $\omega_i \in \Omega$ and extend f_s to $f'_s : B'_s \to \Omega$ by $y_i \mapsto \omega_i$. As B_s is integral over B'_s, by [5.2] we may extend f'_s to $g_s : B_s \to \Omega$. Recalling the canonical map $\phi_s : B \to B_s$, define $g = g_s \circ \phi_s : B \to \Omega$. By our definitions, $g|_A = f$.

[18] This shows up for instance as Theorem 4.19 in Eisenbud.

Let A, B be as in Exercise 20. If the Jacobson radical of A is zero, then so is the Jacobson radical of B.

Let $0 \neq b \in B$. Since the Jacobson radical is defined as the intersection of the maximal ideals, we want to find a maximal ideal $\mathfrak{n}$ of B not containing b. This is the same as finding a map $g\colon B \twoheadrightarrow B/\mathfrak{n}$ to a field with $g(s) \neq 0$. As every field has an algebraic closure ([1.13]), it will suffice (WHY IS THIS ENOUGH? WHAT GUARANTEES THE KERNEL IS MAXIMAL?) to find an algebraically closed field Ω and a map $g\colon B \to \Omega$ such that $g(b) \neq 0$. If this map exists, by (3.1) it will have a unique extension $g_b\colon B_b \to \Omega$. Now $B_b = B[1/b]$ is finitely generated as a B-algebra, and B is finitely generated as an A-algebra, so B_b is finitely generated as an A-algebra. Let $s \in A\backslash\{0\}$, as in the previous problems, correspond to the extension $B_b \supseteq A$. Since the Jacobson radical of A is 0, there is a homomorphism $f\colon A \to \Omega$ with $f(s) \neq 0$, and by [5.21] it extends to a homomorphism $g_b\colon B_b \to \Omega$. Then the restriction $g = g_b|_B$ has $g(b) \neq 0$ and is the map we were after.

Let A be a ring. Show that the following are equivalent:
i) Every prime ideal in A is an intersection of maximal ideals.
ii) In every homomorphic image of A the nilradical is equal to the Jacobson radical.
iii) Every prime ideal in A which is not maximal is equal to the intersection of the prime ideals which contain it strictly.

i) $\implies$ ii): Let $\mathfrak{a} \lhd A$ and write $M(\mathfrak{a}) = V(\mathfrak{a}) \cap \operatorname{Max}(A)$ for the set of maximal ideals containing $\mathfrak{a}$. The radical $r(\mathfrak{a}) = \bigcap V(\mathfrak{a})$, and since each $\mathfrak{p} \in V(\mathfrak{a})$ is by assumption i) equal to $\bigcap M(\mathfrak{p})$, we also have $r(\mathfrak{a}) = \bigcap M(\mathfrak{a})$. In the quotient $A/\mathfrak{a}$ we then have $\mathfrak{N} = \mathfrak{R}$ by the correspondence (1.1).

ii) $\implies$ iii): Let $\mathfrak{p} \in \operatorname{Spec}(A)$ not be maximal. Then $(0) \lhd A/\mathfrak{p}$ is not maximal by the correspondence (1.1). Since $A/\mathfrak{p}$ is an integral domain, (0) is the nilradical, which by assumption ii) equals the Jacobson radical, the intersection of $\operatorname{Max}(A/\mathfrak{p})$. Then (0) is a fortiori the intersection of $\operatorname{Spec}(A/\mathfrak{p})\backslash\big\{(0)\big\}$. That means that upstairs in A, $\mathfrak{p}$ is the intersection of $V(\mathfrak{p})\backslash\{\mathfrak{p}\}$, the set of primes that strictly contain $\mathfrak{p}$.

iii) $\implies$ i): Two failed approaches are footnoted here.[19] These failing, we follow the book's hint. Assume $\mathfrak{p} \lhd A$ is a prime ideal that is not an intersection of maximal ideals, so that in $B = A/\mathfrak{p}$, the trivial ideal (0) is not an intersection of maximal ideals. In particular, the Jacobson radical $\mathfrak{R}(B) \neq (0)$, so there exists a non-zero $f \in \mathfrak{R}(B)$. Let Y_f be the set of primes of B not meeting $S_f = \{1, f, f^2, \ldots\}$. Y_f is not empty, as it contains (0). By (1.3), B_f contains a maximal ideal $B_f\mathfrak{q}$, and by the correspondence (3.11.iv) its contraction $\mathfrak{q}$ is a prime ideal maximal with respect to not meeting S_f, hence a maximal element of Y_f. But as assumption iii) continues to hold in B (whose prime and maximal ideals are by (1.1) images of those in A), it follows that $\mathfrak{q}$ is an intersection of prime ideals containing f. Then $\mathfrak{q}$ contains f as well, which is a contradiction.

A ring A with the three equivalent properties above is called a Jacobson ring.[20]

Lemma 5.23.1*. *A homomorphic image of a Jacobson ring is Jacobson.*

Proof. Let $\phi\colon A \twoheadrightarrow B$ be a ring surjection, and $\mathfrak{q} \in \operatorname{Spec}(B)$. If A is Jacobson, we can write $\mathfrak{q}^c = \bigcap \mathfrak{m}_\alpha$ for some $\mathfrak{m}_\alpha \in \operatorname{Max}(A)$, and then $\mathfrak{q} = \mathfrak{q}^{ce} = \bigcap \mathfrak{m}_\alpha^e$; but by (1.1), the $\mathfrak{m}_\alpha^e \lhd B$ are maximal, so by condition i), B is Jacobson. □

A rephrasing of condition i) is that A is a Jacobson ring just if for every quotient domain B we have $\mathfrak{R}(B) = 0$. We now relate Jacobson rings to the Goldman domains introduced in [5.18].

Definition. *A prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$ is a* Goldman ideal *if $A/\mathfrak{p}$ is a Goldman domain. For $\mathfrak{a} \lhd A$, let $G(\mathfrak{a})$ denote the set of Goldman ideals $\mathfrak{p}$ containing $\mathfrak{a}$.*

Lemma 5.23.2*. *For any ring A and ideal $\mathfrak{a} \lhd A$, we have $r(\mathfrak{a}) = \bigcap G(\mathfrak{a})$.*[21]

[19] One approach would use an induction argument on the length of chains of primes containing $\mathfrak{p} \in \operatorname{Spec}(A)$. Suppose that each chain $P \subseteq V(\mathfrak{p})\backslash\{\mathfrak{p}\}$ ([1.15]) of primes strictly containing $\mathfrak{p}$ is well-ordered by $\supseteq$. Then assign to each P an ordinal $\alpha(P)$ describing its order-type, and define $\alpha(\mathfrak{p}) = \sup \alpha(P)$ as P ranges over chains in $V(\mathfrak{p})\backslash\{\mathfrak{p}\}$. If $\alpha(\mathfrak{m}) = 0$, then $\mathfrak{m}$ is maximal and trivially an intersection of maximal ideals. Suppose $\alpha(\mathfrak{q}) = \beta$ and each $\mathfrak{p}$ with $\alpha(\mathfrak{p}) < \beta$ is an intersection of maximal ideals. Then by iii) $\mathfrak{q}$ is an intersection of primes $\mathfrak{p}$ with $\alpha(\mathfrak{p}) < \beta$ and so is itself an intersection of maximal ideals. This attempt fails because the relation $\supseteq$ (resp. $\subseteq$) on $\operatorname{Spec}(A)$ is not in general well-founded if A is not Noetherian (resp. Artinian). In the ring $A = k[x_1, x_n, \ldots]$ of example 6) on p. 75, if we take $\mathfrak{a}_n = (x_1, \ldots, x_n)$ and $\mathfrak{b}_n = (x_n, x_{n+1}, \ldots)$, then $\mathfrak{a}_n$ is an infinite ascending series of primes of A and $\mathfrak{b}_n$ an infinite decreasing series of primes.

The other approach was to let Σ be the set of prime ideals that are not intersections of maximal ideals and show $\Sigma = \varnothing$. If $\mathfrak{p}$ is maximal in Σ, then all primes containing it are intersections of maximal ideals, so by iii), $\mathfrak{p}$ is itself an intersection of maximal ideals; thus Σ cannot have any maximal elements. If the assumption that Σ is non-empty leads to a proof Σ has a maximal element, then we will have shown $\Sigma = \varnothing$. I wanted to assume Σ was nonempty and then use Zorn's Lemma to show Σ has maximal elements; it's not clear, however, that a chain in Σ has an upper bound in Σ.

[20] More on these rings can be found in Matthew Emerton's notes `http://www.math.uchicago.edu/~emerton/pdffiles/jacobson.pdf` and Pete L. Clark's notes `http://math.uga.edu/~pete/integral.pdf`.

[21] This statement and proof are from Proposition 12.9 in Pete L. Clark's notes `http://math.uga.edu/~pete/integral.pdf`.

Proof. Substituting $A/\mathfrak{a}$ for $\mathfrak{a}$ and using the correspondence (1.1), it is enough to show $\mathfrak{N} = \bigcap G(0)$. The containment $\mathfrak{N} \subseteq \bigcap G(0)$ follows by (1.8). For the other direction, suppose $a \in A \backslash \mathfrak{N}$. Then $A_a \neq 0$, and so by (3.11.iv), a maximal ideal of A_a contracts to a prime ideal $\mathfrak{p} \lhd A$ maximal with respect to the property of not containing a. Since every larger prime contains a, by (1.1), every nonzero prime of the domain $A/\mathfrak{p}$ contains $\bar{a}$. Therefore, by (3.11.iv) again, no nonzero prime survives in $(A/\mathfrak{p})_{\bar{a}}$, which then must be a field. It follows that $A/\mathfrak{p}$ is a Goldman domain, so that $\mathfrak{p}$ is a Goldman ideal not containing a. □

Lemma 5.23.3*. *If a ring A is such that every Goldman ideal is maximal, then A is Jacobson.*

Proof. Each prime $\mathfrak{p} = r(\mathfrak{p}) \overset{(5.23.2^*)}{=} \bigcap G(\mathfrak{p}) = \bigcap M(\mathfrak{p})$, by assumption, so satisfying condition i). □

Lemma 5.23.4*. *If a Goldman domain A has zero Jacobson radical, then it is a field.*

Proof. Suppose a domain A is not a field, but there exists an element $a \in A$ such that A_a is a field. Then for every element b of every maximal ideal $\mathfrak{m}$ of A, there exists an inverse c/a^n in A_a, so that $b \cdot (c/a^n) = 1$, or $bc = a^n$. Then $a^n \in \mathfrak{m}$, so $a \in \mathfrak{m}$, and hence $a \in \mathfrak{R}(A)$. □

Proposition 5.23.5*. *A ring A is Jacobson if and only if every quotient which is a Goldman domain is a field.*

Proof. $\Longrightarrow$: If $\mathfrak{p} \lhd A$ is a Goldman ideal, then $A/\mathfrak{p}$ is a domain, so $0 = \mathfrak{N}(A/\mathfrak{p}) = \mathfrak{R}(A/\mathfrak{p})$ by condition ii) for Jacobson rings. By (5.23.4*), $A/\mathfrak{p}$ is a field.

$\Longleftarrow$: This is (5.23.3*). □

Let A be a Jacobson ring (Exercise 23) and B an A-algebra. Show that if B is either (i) integral over A or (ii) finitely generated as an A-algebra, then B is Jacobson.

(ii): Let $\mathfrak{q} \in \operatorname{Spec}(B)$ and $\mathfrak{p} = \mathfrak{q}^c$. Then $B' = B/\mathfrak{q}$ is an integral domain finitely generated over $A' = A/\mathfrak{p}$. Since A was Jacobson, $\mathfrak{R}(A') = \mathfrak{N}(A') = (0)$, so by [5.22], the Jacobson radical $\mathfrak{R}(B') = (0)$. This shows that in $\mathfrak{q}$ is the intersection of the maximal ideals of B containing it.

(i): Let $\mathfrak{q} \in \operatorname{Spec}(B)$ and $b \in \mathfrak{b}$, the intersection of the maximal ideals containing $\mathfrak{q}$. Write $f: A \to B$ for the homomorphism making B an A-algebra. Then B is integral over the subring $f(A)[b]$. By (5.23.1*), $f(A)$ is Jacobson, and by (ii) above, so is $f(A)[b]$. Thus we may assume $A \subseteq B$ and $a := b \in A \cap \mathfrak{b}$. Now $B' = B/\mathfrak{q}$ is an integral domain, integral over $A' = A/\mathfrak{q}^c$ by (5.6.i), and $\mathfrak{b}/\mathfrak{q} = \mathfrak{R}(B')$. Since A was Jacobson, by (5.23.1*) again, A' is Jacobson, so $\mathfrak{R}(A') = 0$. But by [5.5.ii], $\mathfrak{R}(B') \cap A' = \mathfrak{R}(A')$, so $\bar{b} \in \mathfrak{R}(A') = 0$, meaning $b \in \mathfrak{q}$.

In particular, every finitely generated ring, and every finitely generated algebra over a field, is a Jacobson ring

A ring is finitely generated if it is finitely generated as a $\mathbb{Z}$-algebra, so by (ii) above it will suffice to show that $\mathbb{Z}$ and all fields are Jacobson. But the prime ideals of $\mathbb{Z}$ are all either maximal themselves or $(0) = \mathfrak{R}$, so $\mathbb{Z}$ is Jacobson by condition i) of [5.23], and similarly fields are Jacobson because their prime ideal is (0).

Let A be a ring. Show that the following are equivalent:
i) A is a Jacobson ring;
ii) Every finitely generated A-algebra B which is a field is finite over A.

i) $\Longrightarrow$ ii): Write A' for the image of the map $A \to B$; as a quotient of A, it is Jacobson, and as a subset of B, it is an integral domain; thus $\mathfrak{R}(A') = \mathfrak{N}(A') = 0$. Find an element $s \neq 0$ in A' as in [5.20], [5.21]. Then there is some maximal ideal $\mathfrak{m}$ of A' not containing s. If we let $k = A'/\mathfrak{m}$ and Ω be the algebraic closure of k, then the composition $f: A' \twoheadrightarrow k \hookrightarrow \Omega$ doesn't send s to 0, so by the assumption of [5.21], f extends to a homomorphism $g: B \to \Omega$. As a map of fields, g is injective, so $B \cong g(B)$. Since B is finitely generated over A', say $B = A'[y_1, \ldots, y_n]$, the image $g(B)$ is generated over k by the $g(y_i)$. But the $g(y_i)$ are algebraic over k, so $g(B)$ is a finitely generated k-module, thus a finitely generated A'-module, and finally a finitely generated A-module. (Question: unless A' is already a field, doesn't the fact that $g: B \to \Omega$ extends $A' \to A'/\mathfrak{m} = k$ contradict g's being an injection?)

ii) $\Longrightarrow$ i): Let $\mathfrak{p} \lhd A$ be a prime ideal, not maximal, and consider $A' = A/\mathfrak{p}$. We want to show the intersection of primes strictly containing $\mathfrak{p}$ in A is $\mathfrak{p}$; downstairs in A', we want to show the intersection of the non-zero primes is 0. Equivalently, for every nonzero $s \in A'$, $S_s = \{1, s, s^2, \ldots\}$ misses some non-zero prime ideal. Now A'_s is a finitely generated A'-algebra. If it is a field, then by assumption, it is finite over A, hence integral over A', and (5.7) says that A' is a field, so $\mathfrak{p}$ is maximal. So it is not a field, and it has a nonzero maximal ideal $\mathfrak{q}_s$, whose contraction to A' is a prime $\mathfrak{q}$ not meeting S_s by (3.11.iv).

Note that the direction i) $\implies$ ii) shows that Jacobson rings A are the furthest generalization of fields k for which Zariski's Lemma ((1.27.2*), (5.24), [5.18], (7.9)) still holds.

Let X be a topological space. A subset of X is locally closed *if it is the intersection of an open set and a closed set, or equivalently if it is open in its closure.*

We prove these conditions are equivalent. Supposing C is closed and U is open in X, we want to show $C\cap U$ is open in its closure. Let $\mathscr{C}$ be the collection of all closed sets of X containing U; then every closed set of X containing $C\cap U$ contains some member of $\mathscr{C}'=\{K\cap C : K\in\mathscr{C}\}$, so $\overline{C\cap U}=\bigcap\mathscr{C}'=C\cap\overline{U}$. Then $C\cap U=U\cap(C\cap\overline{U})$ is indeed open in $\overline{C\cap U}$.

On the other hand, if $S\subseteq X$ be given such that S is open in its closure $C=\overline{S}$, then there is by definition an open $U\subseteq X$ such that $S=U\cap C$.

The following conditions on a subset X_0 of X are equivalent:
(1) Every non-empty locally closed subset of X meets X_0;
(2) For every closed set E in X we have $\overline{E\cap X_0}=E$;
(3) The mapping $U\mapsto U\cap X_0$ of the collection of open sets of X onto the collection of open sets of X_0 is bijective.

(1) $\implies$ (2): If E is closed, $x\in E$, and U is any neighborhood of x, then $U\cap E$ is locally closed, so by (1), $U\cap E\cap X_0\neq\varnothing$. Thus every neighborhood of x meets $E\cap X_0$, so $x\in\overline{E\cap X_0}$. Thus $E\subseteq\overline{E\cap X_0}$. On the other hand, $\overline{E\cap X_0}\subseteq\overline{E}=E$.

(2) $\implies$ (3): By the definition of the subspace topology, the mapping $U\mapsto U\cap X_0$ is surjective from the topology of X to that of X_0. To see injectivity, suppose $U\cap X_0=V\cap X_0$; taking complements in X_0, we get $(X\setminus U)\cap X_0=(X\setminus V)\cap X_0$. Taking closures gives $\overline{(X\setminus U)\cap X_0}=\overline{(X\setminus V)\cap X_0}$. Since $X\setminus U$ and $X\setminus V$ are closed in X, (2) gives $X\setminus U=X\setminus V$; and taking complements finally shows $U=V$.

(3) $\implies$ (1): A locally closed subset of X is of the form $C\cap U=U\setminus V$ for $C=X\setminus V$ closed and U open. If $C\cap U$ doesn't meet X_0, then $X_0\cap U\cap C=\varnothing$, so $X_0\cap U\subseteq X\setminus C=V$. Intersecting both sides with $X_0\cap U$ gives $X_0\cap U\subseteq X_0\cap U\cap V$, but on the other hand since $U\cap V\subseteq U$, intersecting with X_0 gives $X_0\cap U\cap V\subseteq X_0\cap U$. Thus U and $U\cap V$ have the same image under the map of (3), so by assumption, $U=U\cap V$, or $U\subseteq V$. Then $C\cap U=U\setminus V=\varnothing$.

A subset X_0 satisfying these conditions is said to be very dense *in X.*
If A is a ring, show that the following are equivalent:
i) A is a Jacobson ring;
ii) The set of maximal ideals of A is very dense in $\mathrm{Spec}(A)$*;*
iii) Every locally closed subset of $\mathrm{Spec}(A)$ *consisting of a single point is closed.*

i) $\iff$ ii): Let $\mathfrak{a}\lhd A$ be an arbitrary ideal, so that $V(\mathfrak{a})\subseteq X=\mathrm{Spec}(A)$ ([1.15]) is an arbitrary closed subset, and let $\mathfrak{b}=\bigcap\big(V(\mathfrak{a})\cap\mathrm{Max}(A)\big)$ be the intersection of all maximal ideals containing $\mathfrak{a}$. Then by Eq. 1.1 from [1.18.i], the closure of $V(\mathfrak{a})\cap\mathrm{Max}(A)$ is $V(\mathfrak{b})$. Since $\mathfrak{a}$ is a subset of each prime in the set $V(\mathfrak{a})\cap\mathrm{Max}(A)$, we have $\mathfrak{a}\subseteq\mathfrak{b}$, so $V(\mathfrak{b})\subseteq V(\mathfrak{a})$. By (2) above, $\mathrm{Max}(A)$ is very dense in X just if $V(\mathfrak{a})\subseteq V(\mathfrak{b})$ for all $\mathfrak{a}$, so every prime containing $\mathfrak{a}$ contains $\mathfrak{b}$. This happens just if in in every quotient $A/\mathfrak{a}$, every prime contains the Jacobson radical, so the Jacobson radical and the nilradical are equal. By [5.23.ii], this happens if and only if A is a Jacobson ring.

i) $\iff$ iii): A locally closed subset $S\subseteq X$ can be written as $S=V(\mathfrak{a})\cap U$ with U open. If we write $U=X\setminus V(\mathfrak{b})$, then $S=V(\mathfrak{a})\setminus V(\mathfrak{b})$. If S is a singleton, there is exactly one prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ that does not contain $\mathfrak{b}$. Write $\mathfrak{c}=r(\mathfrak{p}+\mathfrak{b})$. By [1.15.i,iii], $V(\mathfrak{c})=V(\mathfrak{p}\cup\mathfrak{b})=V(\mathfrak{p})\cap V(\mathfrak{b})\subseteq V(\mathfrak{p})$. Then $S=\{\mathfrak{p}\}=V(\mathfrak{a})\setminus V(\mathfrak{b})=V(\mathfrak{p})\setminus V(\mathfrak{c})$, so all primes strictly containing $\mathfrak{p}$ contain $\mathfrak{c}$, and $\mathfrak{c}=\bigcap\big(V(\mathfrak{p})\setminus\{\mathfrak{p}\}\big)$ is strictly bigger than $\mathfrak{p}$. Now [1.18.i] says that each locally closed singleton $S=\{\mathfrak{p}\}$ is closed if and only if each such $\mathfrak{p}$ is maximal (and $\mathfrak{c}=(1)$, $V(\mathfrak{c})=\varnothing$) if and only if the only primes $\mathfrak{p}$ that are not intersections of larger primes are maximal; but this last condition says A is Jacobson, by [5.23.iii].

Valuation rings and valuations

Let A, B be two local rings. B is said to dominate *A if A is a subring of B and the maximal ideal $\mathfrak{m}$ of A is contained in the maximal ideal $\mathfrak{n}$ of B (or, equivalently, if $\mathfrak{m}=\mathfrak{n}\cap A$). Let K be a field and let Σ be the set of all local subrings of K. If Σ is ordered by the relation of domination, show that Σ has maximal elements and that $A\in\Sigma$ is maximal if and only if A is a valuation ring of K.*

Given a chain $(A_\alpha,\mathfrak{m}_\alpha)$ in this ordering, the union $A=\bigcup A_\alpha$ is a subring of K and $\mathfrak{m}=\bigcup\mathfrak{m}_\alpha$ is an ideal of A. If $k_\alpha=A_\alpha/\mathfrak{m}_\alpha$ are the residue fields, then we have a natural embedding $k_\alpha\hookrightarrow k_\beta$ for $\alpha\leq\beta$, and if $\alpha\leq\beta\leq\gamma$, then the canonical embedding $k_\alpha \hookrightarrow k_\gamma$ is the composition $k_\alpha \hookrightarrow k_\beta \hookrightarrow k_\gamma$. Thus the chain defines a direct system of field homomorphisms with direct limit k. Since the diagrams of short exact sequences

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{m}_\alpha \arrow[r, hook] \arrow[d, hook] & A_\alpha \arrow[r, two heads] \arrow[d, hook] & k_\alpha \arrow[r] \arrow[d, tail] & 0 \\
0 \arrow[r] & \mathfrak{m}_\beta \arrow[r, hook] & A_\beta \arrow[r, two heads] & k_\beta \arrow[r] & 0
\end{tikzcd}$$

are commutative, they give rise ([2.18,19]) to a short exact sequence $0 \to \mathfrak{m} \hookrightarrow A \twoheadrightarrow k \to 0$ of direct limits, showing $\mathfrak{m}$ is a maximal ideal of A. Thus each chain has an upper bound, so Zorn's Lemma gives maximal elements.[22]

Let $(A, \mathfrak{m})$ be a maximal element and Ω the algebraic closure of $A/\mathfrak{m}$. Then if $f : A \twoheadrightarrow A/\mathfrak{m} \hookrightarrow \Omega$ is the expected map, (A, f) is an element of the set called Σ on p. 65. If we have $(A, f) \leq (A, f')$ in this order, then $A \subseteq A'$ and $f'|_A = f$, so $\ker(f') \cap A = \ker(f) = \mathfrak{m}$. By maximality of $(A, \mathfrak{m})$, this means $A' = A$ and $f' = f$, so (A, f) is a maximal element in its ordering, and (5.21) says that $(A, \mathfrak{m})$ is a valuation ring of K.

If on the other hand $(A, \mathfrak{m})$ is a valuation ring dominated by $(B, \mathfrak{n})$, we show they are equal. By (5.18.ii), B is a valuation ring as well. Write $\mathfrak{m}_- = \mathfrak{m}\backslash\{0\} = \big(K\backslash A\big)^{-1}$ and $\mathfrak{n}_- = \mathfrak{n}\backslash\{0\} = \big(K\backslash B\big)^{-1}$. As $(B, \mathfrak{n})$ dominates $(A, \mathfrak{m})$, we have $\mathfrak{m}_- \subseteq \mathfrak{n}_-$ and $\mathfrak{m}_-^{-1} \subseteq \mathfrak{n}_-^{-1}$. By definition, $B\backslash A \subseteq B$, but by what we've shown, $B\backslash A \subseteq K\backslash A = \mathfrak{m}_-^{-1} \subseteq \mathfrak{n}_-^{-1} = K\backslash B$, so we conclude $B\backslash A = \varnothing$ and $B = A$.

Let A be an integral domain, K its field of fractions. Show that the following are equivalent:

(1) A is a valuation ring of K;

(2) If $\mathfrak{a}$, $\mathfrak{b}$ *are any two ideals of A, then either* $\mathfrak{a} \subseteq \mathfrak{b}$ *or* $\mathfrak{b} \subseteq \mathfrak{a}$.

(1) $\implies$ (2): Suppose $\mathfrak{a} \not\subseteq \mathfrak{b}$, so there is $a \in \mathfrak{a}\backslash\mathfrak{b}$. Obviously $a \neq 0$. If $\mathfrak{b} = 0$, then $\mathfrak{b} \subseteq \mathfrak{a}$; otherwise there is a nonzero $b \in \mathfrak{b}$. Then $a/b \neq 0$, so either $a/b \in A$ or $b/a \in A$. It it were the former, we would have $a = (a/b)b \in A\mathfrak{b} = \mathfrak{b}$, contrary to assumption, so $b/a \in A$. Thus $b = (b/a)a \in A\mathfrak{a} = \mathfrak{a}$. Since $b \in \mathfrak{b}\backslash\{0\}$ was arbitrary, $\mathfrak{b} \subseteq \mathfrak{a}$.

(2) $\implies$ (1): Let $a/b \in K^\times$ for $a, b \in A$ and $b \neq 0$. Then $a \in (a) \subseteq (b)$ or $b \in (b) \subseteq (a)$ in A. In the former case, write $a = xb$ with $x \in A$; then $a/b = xb/b = x \in A$. In the latter case, write $b = ya$ with $y \in A$; then $a/b = a/ya = 1/y$, so $(a/b)^{-1} = y \in A$.

Deduce that if A is a valuation ring and $\mathfrak{p}$ *is a prime ideal of A, then* $A_\mathfrak{p}$ *and* $A/\mathfrak{p}$ *are valuation rings of their fields of fractions.*

Since the containment relation on ideals of $A_\mathfrak{p}$ or $A/\mathfrak{p}$ is inherited from A, and both rings are still integral domains, they are also valuation rings.

Let A be a valuation ring of a field K. Show that every subring of K which contains A is a local ring of A.

Let $A \subseteq B \subseteq K$ be rings. By (5.18.ii), B is a valuation ring, so by (5.18.i) it is local with maximal ideal $\mathfrak{p}$. If $\mathfrak{m}$ is the maximal ideal of A, we have $\mathfrak{p} \subseteq \mathfrak{m}$, for if $0 \neq x \in B$ with $x^{-1} \notin B$, since $A \subseteq B$ we have $x^{-1} \notin A$, and as A is a valuation ring, $x \in A$. Then $\mathfrak{p} = \mathfrak{p} \cap A$ is a prime ideal of A. We claim $B = A_\mathfrak{p}$.

Slightly contrary to our usual notation, write $S^{-1} = \{x \in K : x^{-1} \in S\}$ for $S \subseteq K$. Since for each $x \in K^\times$ we have that $x \in A$ or $x^{-1} \in A$, or both, and similarly for B, we get decompositions $K = \mathfrak{m} \amalg A^\times \amalg \mathfrak{m}^{-1}$ and $K = \mathfrak{p} \amalg B^\times \amalg \mathfrak{p}^{-1}$, as in the figure below.

$\mathfrak{m}$	$A^\times$	$\mathfrak{m}^{-1}$
$\mathfrak{p}$	$B^\times$	$\mathfrak{p}^{-1}$

Since obviously $A \subseteq A_\mathfrak{p}$, it remains to show $B\backslash A \subseteq A_\mathfrak{p}$, but it is evident from the figure that $B\backslash A \subseteq (\mathfrak{m}\backslash\mathfrak{p})^{-1}$ (actually, they are equal). To prove it without reference to the figure, note that since $A = A^\times \cup \mathfrak{m} \subseteq B$, the first decomposition implies $B\backslash A \subseteq \mathfrak{m}^{-1}$, and since $B \cap \mathfrak{p}^{-1} = \varnothing$, we have $B\backslash A \subseteq \mathfrak{m}^{-1}\backslash\mathfrak{p}^{-1} = (\mathfrak{m}\backslash\mathfrak{p})^{-1} \subseteq (A\backslash\mathfrak{p})^{-1} \subseteq A_\mathfrak{p}$.

Note that this result does not contradict [5.27], since $\mathfrak{p} \subseteq \mathfrak{m}$ and therefore B does not dominate A.

Let A be a valuation ring of a field K. The group U of units of A is a subgroup of the multiplicative group $K^\times$ *of K.*

Let $\Gamma = K^\times/U$. *If* $\xi, \eta \in \Gamma$ *are represented by* $x, y \in K$, *define* $\xi \geq \eta$ *to mean* $xy^{-1} \in A$. *Show that this defines a total ordering on* Γ *which is compatible with the group structure (i.e.,* $\xi \geq \eta \implies \xi\omega \geq \eta\omega$ *for all* $\omega \in \Gamma$*). In other words,* Γ *is a totally ordered abelian group. It is called the* value group *of A.*

[22] My first inclination was to try to use the theorem as suggested, but the set Σ on p. 65 depends on choosing an algebraically closed field Ω and it's not immediate apparent what field to choose to be codomain for an entire chain. Moreover, depending what valuation ring one chooses, the target field changes. For example, for each nonzero $(p) \in \operatorname{Spec}(\mathbb{Z})$, the residue field of $\mathbb{Z}_{(p)} \subsetneq \mathbb{Q}$ is $\mathbb{F}_p$.

Well-definedness: Let x, $x' \in K^\times$ represent $\xi \in \Gamma$ and y, $y' \in K^\times$ represent $\eta \in \Gamma$. We show that the relation $\xi \geq \eta$ is independent of the representatives chosen. $\xi = Ux = Ux'$, so $Ux'x^{-1} = U$, meaning $x'x^{-1} \in U$, and similarly $y(y')^{-1} \in U$. The x, y version of $\xi \geq \eta$ gives $xy^{-1} \in A$. Then $x'(y')^{-1} = [x'x^{-1}][xy^{-1}][y(y')^{-1}] \in U^{-1}AU = A$, giving the x', y' version of $\xi \geq \eta$.

Reflexivity: If $x \in K^\times$ represents $\xi \in \Gamma$, then $xx^{-1} = 1 \in A$, showing $\xi \geq \xi$.

Antisymmetry: Let $x, y \in K^\times$ respectively represent $\xi, \eta \in \Gamma$. If $\xi \geq \eta$ and $\eta \geq \xi$, then $xy^{-1} \in A$ and $yx^{-1} \in A$. Since $(xy^{-1})(yx^{-1}) = 1$, this shows $xy^{-1} \in U$, so $\xi = Ux = Uy = \eta$.

Transitivity: Let x, y, $z \in K^\times$ respectively represent ξ, η, $\zeta \in \Gamma$. If $\xi \geq \eta$ and $\eta \geq \zeta$, then $xy^{-1} \in A$ and $yz^{-1} \in A$, so multiplying them, $xz^{-1} = (xy^{-1})(yz^{-1}) \in A$, and $\xi \geq \zeta$.

Compatibility: Let $x, y, w \in K^\times$ respectively represent $\xi, \eta, \omega \in \Gamma$. If $\xi \geq \eta$, then $xy^{-1} \in A$. But $xy^{-1} = x(ww^{-1})y^{-1} = (xw)(yw)^{-1}$, showing $\xi\omega \geq \eta\omega$.

Let $v \colon K^\times \to \Gamma$ be the canonical homomorphism. Show that $v(x+y) \geq \min\big(v(x), v(y)\big)$ for all $x, y \in K^\times$.

Without loss of generality, let $v(x) \geq v(y)$, so that $xy^{-1} \in A$. Then $A \ni xy^{-1} + 1 = (x+y)y^{-1}$, so $v(x+y) \geq v(y)$. Note also that $v(xy) = xyU = xU \cdot yU = v(x)v(y)$, so v is a *valuation* with values in Γ , in the terminology of the following exercise.

Conversely, let Γ be a totally ordered abelian group (written additively*), and K a field. A* valuation of K with values in Γ *is a mapping $v \colon K^\times \to \Gamma$ such that*
(1) $v(xy) = v(x) + v(y)$,
(2) $v(x+y) \geq \min\big(v(x), v(y)\big)$,
for all $x, y \in K^\times$. Show that the set of elements $x \in K^\times$ such that $v(x) \geq 0$ is a valuation ring of K. This ring is called the valuation ring *of v, and the subgroup $v(K^\times)$ of Γ is the* value group *of v.*

The book's statement needs to be corrected mildly: the ring surely needs $0 \in K$ as well. The traditional way to fix this is to add a new element ∞ to Γ, and let $\Delta = \Gamma \cup \{\infty\}$ be a monoid with subgroup Γ such that $\xi + \infty = \infty$ for all $\xi \in \Delta$.[23] One extends the order on Γ by $\infty \geq \xi$ for all $\xi \in \Delta$ and defines $v(0) := \infty$. This extended valuation v satisfies (1) since $v(0 \cdot x) = v(0) = \infty = \infty + v(x) = v(0) + v(x)$ and (2) since $v(0+x) = v(x) = \min\big(\infty, v(x)\big) = \min\big(v(0), v(x)\big)$.

Now let $A := \{x \in K : v(x) \geq 0\}$; we verify A is a valuation ring. We also verify $\mathfrak{m} = \{x \in K : v(x) > 0\}$ is the unique maximal ideal of A. Since associativity, commutativity, distributivity, and identities are inherited from K, we have only to check closure properties of A.

- $0 \in A$: Note $v(0) = \infty \geq 0$.
- $1 \in A$: Note $v(1) = v(1 \cdot 1) = v(1) + v(1)$, so subtracting off $v(1)$ gives $v(1) = 0$.
- $-1 \in A$: Note $0 = v(1) = v(-1 \cdot -1) = v(-1) + v(-1) = 2v(-1)$. If $v(-1) > 0$, then $0 = 2v(-1) > 0$, which is false; similarly, $v(-1) < 0$ would imply $0 = 2v(-1) < 0$, which is false; so $v(-1) = 0$.
- $x \in A \implies -x \in A$: If $x \in A$, then $v(-x) = v(-1 \cdot x) = v(-1) + v(x) = 0 + v(x) = v(x) \geq 0$.
- $x, y \in A \implies x + y \in A$: If $v(x), v(y) \geq 0$, then $v(x+y) \geq \min\big(v(x), v(y)\big) \geq 0$.
- $x, y \in A \implies xy \in A$: If $v(x), v(y) \geq 0$, then $v(xy) = v(x) + v(y) \geq 0$.
- $v(x^{-1}) = -v(x)$: $0 = v(1) = v(xx^{-1}) = v(x) + v(x^{-1})$; subtract $v(x)$ from both sides.
- $x \notin A \implies x^{-1} \in A$: If $x \notin A$, then $v(x) < 0$, so $v(x^{-1}) \geq 0$ and $x^{-1} \in A$.
- $x \in A \backslash \mathfrak{m} \implies x \in A^\times$: If $v(x) = 0$, then $v(x^{-1}) = 0$, so $x^{-1} \in A$ and $x \in A^\times$.

Thus the concepts of valuation ring and valuation are essentially equivalent.

To prove this statement, we should verify that these correspondences are inverse. Let A be a valuation ring of a field K, and let $v \colon K^\times \twoheadrightarrow K^\times/A^\times =: \Gamma$ be the canonical map. [5.30] shows it is a valuation. Its valuation ring is $A' := \{0\} \cup \{x \in K^\times : v(x) \geq 0\}$. Now by the definition of $\geq$ on Γ, we have $v(x) \geq 0 = v(1)$ just if $x = x1^{-1} \in A$, so $A' = A$.

[23] In multiplicative notation, this would be called a "group with zero," with the absorbing element ∞ playing the role of "zero."

Suppose on the other hand $v\colon K^\times \twoheadrightarrow \Gamma$ is a valuation, with valuation ring $A = \{0\} \cup \{x \in K^\times : v(x) \geq 0\}$ and value group Γ. Writing $U = \ker(v)$, and $\pi\colon K^\times \twoheadrightarrow K^\times/U$ for the natural map, there is a canonical isomorphism $\phi\colon K^\times/U \xrightarrow{\sim} \Gamma$ such that $v = \phi \circ \pi$. The field of fractions of A is K, so [5.30] gives a valuation $v'\colon K^\times \twoheadrightarrow K^\times/A^\times$. Now $A^\times = \big\{x \in A\backslash\{0\} : x^{-1} \in A\big\} = \{x \in K^\times : v(x) \geq 0 \;\&\; -v(x) = v(x^{-1}) \geq 0\} = \{x \in K^\times : v(x) = 0\} = U$, so $v' = \pi$. Thus $v = \phi \circ \pi = \phi \circ v'$, so v' is canonically equivalent to v. Finally, $v(x) \leq v(y) \iff 0 = v(1) = v(xx^{-1}) = v(x) - v(x) \leq v(y) - v(x) = v(yx^{-1}) \iff yx^{-1} \in A\backslash\{0\} \iff v'(x) \leq v'(y)$ by the definition of v' in [5.30], so the order is preserved.

Let Γ be a totally ordered abelian group. A subgroup Δ of Γ is isolated *in Γ if, whenever $0 \leq \beta \leq \alpha$ and $\alpha \in \Delta$, we have $\beta \in \Delta$. Let A be a valuation ring of a field K, with value group Γ (Exercise 31). If $\mathfrak{p}$ is a prime ideal of A, show that $v(A\backslash\mathfrak{p})$ is the set of elements ≥ 0 of an isolated subgroup Δ of Γ, and that the mapping so defined of* Spec(A) *into the set of isolated subgroups of Γ is bijective.*

Write $\Delta^+ = v(A\backslash\mathfrak{p})$. Obviously $1 \notin \mathfrak{p}$, so $v(1) = 0 \in \Delta^+$. If $\alpha = v(a)$ and $\beta = v(b)$ are in Δ^+, with a, $b \notin \mathfrak{p}$, then since $\mathfrak{p}$ is prime $ab \notin \mathfrak{p}$, and so $\alpha + \beta = v(a) + v(b) = v(ab) \in \Delta^+$. Thus Δ^+ is a submonoid of Γ and $\Delta = \Delta^+ \cup -\Delta^+$ is a subgroup whose elements ≥ 0 are Δ^+

Suppose $0 \leq \beta \leq \alpha$ in Γ with $\alpha \in \Delta^+$. If $\beta = 0$ or α, then $\beta \in \Delta^+$, so assume not. Let $\alpha = v(a)$ for $a \in A\backslash\mathfrak{p}$ and $\alpha - \beta = v(c)$ for $c \in A$. If $c \notin \mathfrak{p}$, then $\alpha - \beta \in \Delta^+$, so $\beta - \alpha \in \Delta$ and $\beta \in \Delta^+$, since Δ is a subgroup. If $c \in \mathfrak{p}$, consider $b = ac^{-1}$. Now $v(b) = \alpha - (\alpha - \beta) = \beta > 0$, so $b \in A$, but $b \notin \mathfrak{p}$, since otherwise $bc = a \in \mathfrak{p}$, contrary to assumption. Thus $\beta \in \Delta^+$.

The correspondence is injective, for assume $\mathfrak{p}$, $\mathfrak{q}$ in Spec(A) are such that $\Delta(\mathfrak{p}) = \Delta(\mathfrak{q})$. Then for every $x \in A\backslash\mathfrak{p}$ there is $y \in A\backslash\mathfrak{q}$ with $v(x) = v(y)$. Then $0 = v(x) - v(y) = v(xy^{-1})$, so $xy^{-1} \in A^\times$ and $x = (xy^{-1})y \in A^\times(A\backslash\mathfrak{q}) = A\backslash\mathfrak{q}$, so $A\backslash\mathfrak{p} \subseteq A\backslash\mathfrak{q}$. Symmetrically, $A\backslash\mathfrak{q} \subseteq A\backslash\mathfrak{p}$, so $\mathfrak{p} = \mathfrak{q}$.

For surjectivity, let an isolated subgroup Δ be given. The natural candidate for $\Delta = v(A\backslash\mathfrak{p})$ is $\mathfrak{p} = A\backslash v^{-1}(\Delta)$. Certainly it has the right image. Since $\infty \notin \Delta$ we get $0 \in \mathfrak{p}$. If $x \in \mathfrak{p}$, then $v(-x) = v(x) \notin \Delta$, so $-x \in \mathfrak{p}$. If x, $y \in \mathfrak{p}$, then $v(x+y) \geq \min\big(v(x), v(y)\big) > \Delta$, so $x + y \in \mathfrak{p}$. Finally, if x, $y \notin \mathfrak{p}$, then $v(x)$, $v(y) \in \Delta$, so $v(xy) = v(x) + v(y) \in \Delta$, and $xy \notin \mathfrak{p}$.

If $\mathfrak{p}$ is a prime ideal of A, what are the value groups of the valuation rings $A/\mathfrak{p}$, $A_\mathfrak{p}$?

For $A/\mathfrak{p}$, define $\bar{v}\colon A/\mathfrak{p} \to \Gamma \cup \{\infty\}$ by $\bar{v}(\bar{x}) = \begin{cases} v(x), & x \notin \mathfrak{p}, \\ \infty, & x \in \mathfrak{p}. \end{cases}$ Assuming it is well defined, it inherits axioms (1) and (2) of [5.31] from v. To see it is well defined, assume $x - y \in \mathfrak{p}$. Then

$$\bar{v}(\bar{x}) = \min\big(\bar{v}(\bar{x}), \infty\big) = \min\big(\bar{v}(\bar{x}), \bar{v}(\bar{y} - \bar{x})\big) \leq \bar{v}\big(\bar{x} + (\bar{y} - \bar{x})\big) = \bar{v}(\bar{y}),$$

and similarly $\bar{v}(\bar{y}) \leq \bar{v}(\bar{x})$. Then we can extend $\bar{v}$ to the fraction field k of $A/\mathfrak{p}$, and it gives a valuation $\bar{v}\colon k^\times \to \Delta$. Since units of $A/\mathfrak{p}$ are images of units of A (since in the quotient $\mathfrak{m} \mapsto \mathfrak{m}/\mathfrak{p}$ are the maximal ideals) and only these are taken to 0 by $\bar{v}$, we see $A/\mathfrak{p}$ is the valuation ring of $\bar{v}$, and Δ is the valuation group of $A/\mathfrak{p}$.

For $A_\mathfrak{p}$, the group $K^\times$ is unchanged. Since A is local, $\mathfrak{p} \subseteq \mathfrak{m}$, meaning $U = A\backslash\mathfrak{m} \subseteq A\backslash\mathfrak{p} \subseteq A_\mathfrak{p}\backslash\mathfrak{p}A_\mathfrak{p} =: U_\mathfrak{p}$, the units of $A_\mathfrak{p}$. Thus the value group is a further quotient of $\Gamma = K^\times/U$. We can write an element of $U_\mathfrak{p}$ as a/b for a, $b \in A\backslash\mathfrak{p}$, so $\Delta = v(A\backslash\mathfrak{p}) = v(U_\mathfrak{p})$. By the third isomorphism theorem (2.1.i), $K^\times/U_\mathfrak{p} \cong (K^\times/U)/(U_\mathfrak{p}/U) = \Gamma/v(U_\mathfrak{p}) = \Gamma/\Delta$.

Let Γ be a totally ordered abelian group. We shall show how to construct a field K and a valuation v of K with Γ as value group. Let k be any field and let $A = k[\Gamma]$ be the group algebra of Γ over k. By definition, A is freely generated as a k-vector space by elements x_α ($\alpha \in \Gamma$) such that $x_\alpha x_\beta = x_{\alpha+\beta}$. Show that A is an integral domain.

This will follow from our proof of (1) in the next paragraph.

If $u = \lambda_1 x_{\alpha_1} + \cdots + \lambda_n x_{\alpha_n}$ is any non-zero element of A, where the λ_i are all $\neq 0$ and $\alpha_1 < \cdots < \alpha_n$, define $v_0(u)$ to be α_1. Show that the mapping $v_0\colon A\backslash\{0\} \to \Gamma$ satisfies conditions (1) and (2) of Exercise 31.

(1) Let $f = \sum a_\alpha x_\alpha$ and $g = \sum b_\beta x_\beta$ be non-zero elements of A, with $v_0(f) = \alpha_0$ and $v_0(g) = \beta_0$. Then in fg, the non-zero coefficient of lowest index is that of $x_{\alpha_0+\beta_0}$, which is $a_{\alpha_0} b_{\beta_0}$, since for all other pairs α, β of indices we have $\alpha + \beta > \alpha_0 + \beta_0$. As k is a field, $a_{\alpha_0} b_{\beta_0} \neq 0$, so $fg \neq 0$ and $v(fg) = \alpha_0 + \beta_0$.

(2) Let $f = \sum a_\alpha x_\alpha$ and $g = \sum b_\beta x_\beta$ be nonzero elements of A, with $v_0(f) = \alpha_0$ and $v_0(g) = \beta_0$; then the lowest potentially nonzero coefficient index of $f + g$ is $\alpha_0 + \beta_0$. (Of course, there could be cancellation.) Thus $v_0(f + g) \geq \min\big(v_0(f), v_0(g)\big)$.

Let K be the field of fractions of A. Show that v_0 can be uniquely extended to a valuation v of K, and that the value group of v is precisely Γ.

Axiom (1) requires that $0 = v(f/f) = v_0(f) + v(1/f)$, so that $v(f^{-1}) = -v_0(f)$ for all nonzero $f \in A$. Then for $f/g \in K$ with $f, g \in A$ we must have $v(f/g) = v_0(f) - v_0(g)$, so the extension v is unique, if the definition defines a valuation. Suppose $f/g = f'/g'$ in K, for $f, f', g, g' \in A$. Then by the definition of localization, $fg' = f'g$, so $v_0(f) + v_0(g') = v_0(f') + v_0(g)$, and $v(f/g) = v_0(f) - v_0(g) = v_0(f') - v_0(g') = v(f'/g')$, so v is well defined. Evidently $v(K) = v(A) - v(A) = \Gamma - \Gamma = \Gamma$. It remains to verify axiom (2). Again let $f/g, f'/g' \in K$ be given, for some $f, f', g, g' \in A$. Then $h := \frac{f}{g} + \frac{f'}{g'} = \frac{fg'+f'g}{gg'}$, and

$$\begin{aligned} v(h) = v(fg'+f'g) - v(gg') &\geq \min\big(v(f)+v(g'), v(f')+v(g)\big) - \big(v(g)+v(g')\big) \\ &= \min\big(v(f)-v(g), v(f')-v(g')\big) = \min\big(v(f/g), v(f'/g')\big). \end{aligned}$$

It should be pointed out that $v(A) = v\big(k(\Gamma)\big) = \Gamma$ already, so A is *not* the valuation ring of K. Rather, $B = \{0\} \cup \{x \in K : v(x) \geq 0\}$ is, by [5.31].

Let A be a valuation ring and K its field of fractions. Let $f\colon A \to B$ be a ring homomorphism such that $f^*\colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is a closed *mapping. Then if $g\colon B \to K$ is any A-algebra homomorphism (i.e., if $g \circ f$ is the embedding of A in K) we have $g(B) = A$.*

Since $A = g\big(f(A)\big) \subseteq K$ we have $A \subseteq g(B) =: C$. Then C is a valuation ring, by (5.18.ii). Let $\mathfrak{o}$ be a maximal ideal of C; since $g|^C\colon B \twoheadrightarrow C$ is surjective, $g^*(\mathfrak{o}) = \mathfrak{n}$ is a maximal ideal of B. By [1.18.i], $\{\mathfrak{n}\} \subseteq \operatorname{Spec}(B)$ is closed; as f^* is a closed mapping, $f^*(\{\mathfrak{n}\})$ is closed, so by [1.18.i] again it must be a singleton containing a maximal ideal. As A is local, that ideal is the unique maximal ideal $\mathfrak{m} \lhd A$. Since $g \circ f\colon A \hookrightarrow K$ is the inclusion, this means that $\mathfrak{m} = f^*(\mathfrak{n}) = f^*\big(g^*(\mathfrak{o})\big) = (g \circ f)^*(\mathfrak{o}) = \mathfrak{o} \cap A$, so $\mathfrak{o}$ dominates $\mathfrak{m}$. By [5.27] (valuation rings are domination-maximal), this shows $A = C$ and $\mathfrak{m} = \mathfrak{o}$.

From Exercises 1 and 3 it follows that, if $f\colon A \to B$ is integral and C is any A-algebra, then the mapping $(f \otimes 1)^*\colon \operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec}(C)$ is a closed map.

Conversely, suppose that $f\colon A \to B$ has this property and that B is an integral domain. Then f is integral.

Write $A' = f(A) \subseteq B$, and K for the field of fractions of B. To show B is integral over A', it is enough to show B is in the integral closure of A' in K. By (5.22) it is enough to show B is in each valuation ring of K containing A'. Let C be one such. Then $A' \subseteq B$, $C \subseteq K$. Multiplication $B \times C \to K$ is A-bilinear (equivalently, A'-bilinear), so induces a map $g\colon B \otimes_A C \to K$. Now $f \otimes \mathrm{id}_C\colon A \otimes_A C \to B \otimes_A C$, and (2.14) gives an isomorphism $\phi\colon C \xrightarrow{\sim} A \otimes_A C$. Write $F = (f \otimes \mathrm{id}_C) \circ \phi$, so that $F^*\colon \operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec}(C)$ is closed, by assumption. The composition $g \circ F$ takes $c \mapsto 1_A \otimes c \mapsto 1_B \otimes c \mapsto c$, and so is the inclusion $C \hookrightarrow K$. The preceding [5.34] then says that $g(B \otimes_A C) = C$. In particular, for each $b \in B$ we have $b = g(b \otimes 1_C) \in C$, so $B \subseteq C$.

Show that the result just proved remains valid if B is a ring with only finitely many minimal prime ideals (e.g., if B is Noetherian).

First, if B is Noetherian, (7.13) says the (0) ideal has a primary decomposition, and (4.6) says the finitely many isolated primes of this decomposition are precisely the minimal ideals of B.

Second, the statement needs some clarification. The hypothesis being replaced (by B only having finitely many minimal prime ideals) is that B is integral, not the closed mapping assumption.

Now suppose $f\colon A \to B$ satisfies the assumption. and B has only finitely many minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. The surjections $\pi_i\colon B \twoheadrightarrow B/\mathfrak{p}_i$ give rise to compositions $\pi_i \circ f\colon A \to B \twoheadrightarrow B/\mathfrak{p}_i$. Let an A-algebra C be given. Since tensor is left exact and $B \twoheadrightarrow B/\mathfrak{p}_i$ is a surjection, $g_i\colon B \otimes_A C \to (B/\mathfrak{p}_i) \otimes_A C$ is a surjection. By [1.21.iv], $g_i^*\colon \operatorname{Spec}\big((B/\mathfrak{p}_i) \otimes_A C\big) \to \operatorname{Spec}(B \otimes_A C)$ is a closed map, and by assumption, $\operatorname{Spec}(B \otimes_A C) \to \operatorname{Spec}(C)$ is a closed map, so composing, $\operatorname{Spec}\big((B/\mathfrak{p}_i) \otimes_A C\big) \to \operatorname{Spec}(C)$ is closed. As C was arbitrary, $\pi_i \circ f$ has the property above, and since $B/\mathfrak{p}_i$ is an integral domain, $\pi_i \circ f$ is integral. By [5.6], the map $(\pi_1 \circ f, \ldots, \pi_n \circ f)\colon A \to \prod B/\mathfrak{p}_i$ is integral; this map factors as $(\pi_1, \ldots, \pi_n) \circ f\colon A \to B \to \prod B/\mathfrak{p}_i$. The kernel of the homomorphism $(\pi_1, \ldots, \pi_n)\colon B \to \prod B/\mathfrak{p}_i$ is the nilradical $\mathfrak{N} = \bigcap \mathfrak{p}_i$ of B, so we have a factorization $A \to B \twoheadrightarrow B/\mathfrak{N} \rightarrowtail \prod B/\mathfrak{p}_i$. Since $\prod B/\mathfrak{p}_i$ is integral over the image of A, so is the embedded subring $B/\mathfrak{N}$. Now let $x \in B$; then its image $\bar{x} \in B/\mathfrak{N}$ satisfies a monic polynomial equation $\bar{x}^m + \sum_{j<m} \bar{b}_j \bar{x}^j = \bar{0}$ for some $b_j \in f(A)$; lifting, this means $p(x) = x^m + \sum_{j<m} b_j x^j \in \mathfrak{N}$. Then there is an integer l large enough that $p(x)^l = 0$ in B; but $p(x)^l$ is a monic polynomial in $f(A)[x]$, so x is integral over $f(A)$.

Jordan–Hölder Theorem. Consider an A-module M of finite length. (6.7) says that every composition series of M has the same length, and the book claims (p. 77) that the multiset of isomorphism classes of quotients of successive terms is the same for any choice of composition series. The proof, it goes on, is the same as for finite groups. We recall it here.[1]

The proof proceeds by induction on the length $l(M)$ of M. If $l(M) = 0$ or 1, we are done. Assume inductively that the result holds for all modules of length n, and let $l(M) = n + 1$. Assume M has the two composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_{n+1} = 0, \qquad M = N_0 \supsetneq N_1 \supsetneq \cdots \supsetneq N_{n+1} = 0.$$

If $M_1 = N_1$, then by the inductive hypotheses the multisets $S = \{M_i/M_{i+1}\}_{i=1}^n$ and $T = \{N_i/N_{i+1}\}_{i=1}^n$ of quotients are equal so since $M/M_1 = M/N_1$, the quotient multisets of the two composition series for M are equal.

If $M_1 \neq N_1$, let $P_1 = M_1 \cap N_1$. Note that $M_1 \subsetneq M_1 + N_1 \subseteq M$, so since M/M_1 was assumed simple, $M_1 + N_1 = M$. Now $M_1/P_1 = M_1/(M_1 \cap N_1) \cong (M_1 + N_1)/N_1 = M/N_1$ by the second isomorphism theorem (2.1.ii), and this quotient is simple. Symmetrically, $N_1/P_1 \cong M/M_1$. By the proof of (6.7), $l(P_1) \leq l(M_1) = n$ is finite, so P_1 has a composition series $P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_p = 0$. Write U for the quotient multiset. $M_1 \supsetneq P_1 \supsetneq \cdots \supsetneq P_p = 0$ is a composition series for M_1. Since $l(M_1) = n$, we have $p = n$, and by the induction hypothesis, the multiset $\{M_1/P_1\} \cup U = \{M/N_1\} \cup U$ is the same as the multiset $S = \{M_i/M_{i+1}\}_{i=1}^n$. Then the quotient multiset for the M_i composition series of M is $\{M/M_1\} \cup S = \{M/M_1, M/N_1\} \cup U$. Similarly $N_1 \supsetneq P_i$ is a composition series for N_1 with quotient multiset $\{N_1/P_1\} \cup U = \{M/M_1\} \cup U$, by inductive assumption equal to the multiset $T = \{N_i/N_{i+1}\}_{i=1}^n$. Then the N_i composition series for M yields the quotient multiset $\{M/N_1\} \cup T = \{M/N_1, M/M_1\} \cup U$ as well.

EXERCISES

i) Let M be a Noetherian A-module and $u : M \to M$ a module homomorphism. If u is surjective, then u is an isomorphism.

For all $n \geq 0$, we have $\ker(u^n)$ a submodule of M and $\ker(u^n) \subseteq \ker(u^{n+1})$; as M is Noetherian, we eventually have $\ker(u^n) = \ker(u^{n+1})$. Any element $y \in \operatorname{im}(u^n)$ is $u^n(x)$ for some $x \in M$, and if $0 = u(y) = u\big(u^n(x)\big) = u^{n+1}(x)$, then $x \in \ker(u^{n+1}) = \ker(u^n)$, so $y = u^n(x) = 0$ already. Thus u is injective on $\operatorname{im}(u^n)$. But since u is surjective, $\operatorname{im}(u^n) = M$, so u is injective, hence an isomorphism.

ii) If M is Artinian and u is injective, then again u is an isomorphism.

For all $n \geq 0$, we have $\operatorname{im}(u^n)$ a submodule of M and $\operatorname{im}(u^n) \supseteq \operatorname{im}(u^{n+1})$; as M is Artinian, we eventually have $\operatorname{im}(u^n) = \operatorname{im}(u^{n+1})$. For each element $x \in M$ we have $u^n(x) \in \operatorname{im}(u^n) = \operatorname{im}(u^{n+1})$, so there is $y \in M$ with $u^n(x) = u^{n+1}(y) = u^n\big(u(y)\big)$. As u is injective, u^n is also injective, so $x = u(y)$. As x was arbitrary, u is surjective, hence an isomorphism.

Let M be an A-module. If every non-empty set of finitely generated submodules of M has a maximal element, then M is Noetherian.

By (6.2), it will suffice to show any submodule N of M is finitely generated. Let Σ be the set of finitely generated submodules of N. By assumption, Σ has a maximal element N_0. If $N_0 \subsetneq N$, there is $x \in N \backslash N_0$, and then $N_0 + Ax \supsetneq N_0$ is a finitely generated submodule of N, contradicting maximality of N_0. Thus $N_0 = N$ is finitely generated.

Let M be an A-module and let N_1, N_2 be submodules of M. If M/N_1 and M/N_2 are Noetherian, so is $M/(N_1 \cap N_2)$. Similarly with Artinian in place of Noetherian.

By the second isomorphism theorem (2.1.ii), $N_1/(N_1 \cap N_2) \cong (N_1 + N_2)/N_2$. Since $(N_1 + N_2)/N_2$ is a submodule of the Noetherian (resp. Artinian) M/N_2, (6.3.i) (resp. (6.3.ii)) shows $N_1/(N_1 \cap N_2)$ is Noetherian (resp. Artinian). Now the third isomorphism theorem (2.1.i) gives an exact sequence $0 \to N_1/(N_1 \cap N_2) \to M/(N_1 \cap N_2) \to M/N_1 \to 0$.

[1] http://planetmath.org/encyclopedia/ProofOfTheJordanHolderDecompositionTheorem.html

The outside terms are Noetherian (resp. Artinian), so another use of (6.3.i) (resp. (6.3.ii)) shows that $M/(N_1 \cap N_2)$ is Noetherian (resp. Artinian).

Let M be a Noetherian A-module and let $\mathfrak{a}$ be the annihilator of M in A. Prove that $A/\mathfrak{a}$ is a Noetherian ring.

M is finitely generated by (6.2), say by $x_1, \ldots, x_n$. Then if $\mathfrak{a}_i = \operatorname{Ann}(x_i)$, we have $A/\mathfrak{a}_i \cong Ax_i$; as a submodule of a Noetherian module, it is, by (6.3.i), also Noetherian. Since $\mathfrak{a} = \bigcap \mathfrak{a}_i$, by [6.3] and induction, $A/\mathfrak{a}$ is a Noetherian A-module, hence a Noetherian $A/\mathfrak{a}$-module.

If we replace "Noetherian" by "Artinian" in this result, is it still true?

No. Let $p \in \mathbb{N}$ be a non-zero prime and consider Example 3) of p. 74, the p-quasicyclic group $G = \mathbb{Z}/p^\infty\mathbb{Z}$.[2] It is an abelian group, so a $\mathbb{Z}$-module, and the book states that it is Artinian.[3] It is generated by the elements $x_n = \mathbb{Z}+1/p^n$, and $\operatorname{Ann}_{\mathbb{Z}}(x_n) = (p^n)$, so $\operatorname{Ann}_{\mathbb{Z}}(G) = (0)$. Now $\mathbb{Z} \cong \mathbb{Z}/(0)$ is not an Artinian ring by Example 2) of p. 74.

Our proof for the Noetherian case above fails precisely because there are infinitely many x_n; we do have each $\mathbb{Z}/(p^n) = \mathbb{Z}/\operatorname{Ann}_{\mathbb{Z}}(x_n)$ Artinian, being isomorphic to the submodule G_n of G, but the result of [6.3] does not extend to infinite intersections.

A topological space X is said to be Noetherian *if the open subsets of X satisfy the ascending chain condition (or, equivalently, the maximal condition). Since closed subsets are complements of open subsets, it comes to the same thing to say that the closed subsets of X satisfy the descending chain condition (or, equivalently, the minimal condition). Show that, if X is Noetherian, then every subspace of X is Noetherian, and that X is compact.*

Let $Y \subseteq X$ be a subspace; in the subspace topology, the open sets of Y are precisely the intersections with Y of open sets of X. If $\langle V_n \rangle$ is an ascending chain of open subsets of Y, let $U_n \subseteq X$ be open and such that $V_n = U_n \cap Y$. Then there is some n such that $U_n = U_{n+1} = \cdots$, so intersecting with Y, we get $V_n = V_{n+1} = \cdots$. This shows Y is Noetherian.

Let $\mathscr{U}$ be an open cover of X, and let Σ be the collection of all finite unions of elements of $\mathscr{U}$. By the maximal condition on opens, Σ has a maximal element V. If there is $x \in X \setminus V$, there is some $U \in \mathscr{U}$ containing x since $\mathscr{U}$ is an open cover, and then $U \cup V \in \Sigma$ strictly contains V, contradicting maximality. Thus $X = V$ is a finite union of elements of $\mathscr{U}$. This shows X is compact.

Prove that the following are equivalent:
i) X is Noetherian.
ii) Every open subspace of X is compact.
iii) Every subspace of X is compact.

i) $\Longrightarrow$ iii): This follows from [6.5]: each $Y \subseteq X$ is itself Noetherian, and each Noetherian space is compact.

iii) $\Longrightarrow$ ii): This is trivial: each open subspace is a subspace.

ii) $\Longrightarrow$ i): Let $U_1 \subseteq U_2 \subseteq \cdots$ be an ascending chain of open subsets of X, and $U = \bigcup_{n\in\mathbb{N}} U_n$. Since U is compact, U is a union of a finite set $\{U_{n_1}, \ldots, U_{n_m}\}$. But then if $n = \max_j n_j$, we see $U = U_n$.

A Noetherian space is a finite union of irreducible closed subspaces. Hence the set of irreducible components of a Noetherian space is finite.

Recall from [1.19] that a topological space C is irreducible if for every pair of nonempty open subsets U_1, U_2, we have $U_1 \cap U_2 \neq \varnothing$. Taking complements $F_i = C \setminus U_i$, this means for every pair of closed subsets $F_1, F_2 \subsetneq C$, we have $C \neq C\setminus(U_1 \cap U_2) = (C\setminus U_1) \cup (C \setminus U_2) = F_1 \cup F_2$. That is, C is not a union of proper closed subspaces.

Suppose, for a contradiction, that the result is false. Then there is a Noetherian space X such that X is an element of the set Σ of closed subsets of X that are not unions of finitely many irreducible closed subspaces. Since Σ is nonempty and X is Noetherian, Σ has a minimal element C. Since C is not a finite union of irreducible sets, it is not

[2] See http://planetmath.org/encyclopedia/QuasicyclicGroup.html. G is the group of elements of $\mathbb{Q}/\mathbb{Z}$ with denominator a p-power, or equivalently $\mathbb{Z}[1/p]/\mathbb{Z}$. Taking its image under $\bar{x} \mapsto e^{2\pi i x}$ gives an isomorphism to the subgroup $\{z : \exists n \geq 0\, (z^{p^n} = 1)\}$ of $\mathbb{C}^\times$. Thus it is an increasing union of the groups of $(p^n)^{\text{th}}$ roots of unity, or equivalently the direct limit of the system $(\mathbb{Z}/p^n\mathbb{Z}, \pi_{mn})$, where for $m \leq n$ we have $\pi_{mn} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ taking $1 \mapsto p^{n-m}$.

[3] are its only proper subgroups. First, we claim that if $x \in G_n \setminus G_{n-1}$, then $\langle x \rangle = G_n$. Since $x = \mathbb{Z} + a/p^n$ for some $a \in \mathbb{Z}\setminus(p)$, we have $(a)+(p) = (1)$ in $\mathbb{Z}$. By (1.16), $(a)+(p^n) = 1$, so there are $b, m \in \mathbb{Z}$ such that $ba + mp^n = 1$. Thus $(ba/p^n) = m + (1/p^n)$ in $\mathbb{Z}[1/p]$, so $bx = x_n$ and $\langle x \rangle = G_n$. Now suppose H is a proper subgroup of G. Since $G = \bigcup G_n$, we see H fails to contain some G_{n+1}. Let $n+1$ be minimal such that this happens. Then H contains no element of $G_{n+1} \setminus G_n$ by the work above, but by assumption contains all of G_n, so $H = G_n$. Now G is Artinian, for given a strictly descending chain of submodules starting with G, the second module is some G_n, and G_n properly contains only $n-1$ submodules.

itself an irreducible set. Thus it is reducible, and so a union of two proper closed subspaces F_1 and F_2. But F_1 and F_2 are both finite unions of irreducible closed sets, so C is as well, a contradiction.

Recall from [1.20.iii] that the irreducible components of a space X are the maximal irreducible subsets of X, and that they are closed and cover X. Since a Noetherian space X is a union of finitely many irreducible closed subspaces, it is a fortiori a union of finitely many *maximal* such, so it is a union of finitely many irreducible components. Let n be the minimal possible number needed to cover X, and let $C_1, \dots, C_n$ be irreducible components covering X. If F is any other irreducible closed set, then $F = \bigcup_{j=1}^n (F \cap C_j)$ expresses F as a union of closed subsets; as F is irreducible, $F \subseteq C_j$ for some j. Thus $C_1, \dots, C_n$ are the only irreducible components of X.

If A is a Noetherian ring, then Spec(A) *is a Noetherian topological space. Is the converse true?*

Every closed subset of Spec(A) is ([1.15]) of the form $V(\mathfrak{a})$ for some radical ideal $\mathfrak{a} \lhd A$. Let $\big(V(\mathfrak{a}_j)\big)_{j\in\mathbb{N}}$ be an infinite descending chain collection of closed subsets of Spec(A). Since $V(\mathfrak{a}_{j+1}) \subseteq V(\mathfrak{a}_j)$, taking intersections of these sets of primes (recalling the $\mathfrak{a}_j$ are radical; see (1.14)) gives $\mathfrak{a}_j \subseteq \mathfrak{a}_{j+1}$. Since A is Noetherian, eventually $\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots$, and so $V(\mathfrak{a}_n) = V(\mathfrak{a}_{n+1}) = \cdots$; thus Spec$(A)$ is Noetherian.

The converse is not true. Let k be a field, and $A = k[x_1, x_2, \dots]$ a polynomial ring over k in countably many indeterminates. Let any sequence $(m_n)_{n=1}^{\infty}$ of integers > 1 be given. Let $\mathfrak{b}$ be the ideal generated by $x_1^{m_1}$ and $x_n - x_{n+1}^{m_{n+1}}$ for all $n \geq 1$. Write $y_n = \bar{x}_n$ in $B = A/\mathfrak{b}$. Then $y_1^{m_1} = 0$ and $y_n = y_{n+1}^{m_{n+1}}$ for all $n \geq 1$. If $\mathfrak{p} = (y_1, y_2, \dots)$, we have $B/\mathfrak{p} \cong k$, so $\mathfrak{p}$ is maximal. Now $y_{n+1} \in r(y_n)$ and $y_1 \in r(0)$, so $\mathfrak{p} \subseteq \mathfrak{N}(B) \subseteq \mathfrak{p}$, showing $\mathfrak{p}$ is the unique minimal prime as well. Since all primes then contain $\mathfrak{p}$, which is maximal, $\mathfrak{p}$ is the only prime of B. Thus Spec$(B) = \{\mathfrak{p}\}$ is obviously Noetherian. But $(y_1) \subsetneq (y_2) \subsetneq (y_3) \subsetneq \cdots$ is an infinite ascending chain of ideals, so B is not Noetherian.

Relatedly[4], but using material from earlier in the book, let k be a field and Γ a non-zero totally ordered group with only finitely many isolated subgroups and such that $\Gamma_{>0} := \{\gamma \in \Gamma : \gamma > 0\}$ has no least element (for example take $\mathbb{Z}[1/p] \subseteq \Gamma \subseteq \mathbb{R}$ for $p \geq 2$). Let K be the field of fractions of the group algebra $k[\Gamma]$. Then [5.33] gives a surjective valuation $v \colon K^\times \to \Gamma$, and $A = \{0\} \cup \{x \in K : v(x) \geq 0\}$ is the associated valuation ring. [5.32] shows that A has only finitely many prime ideals. For any $\gamma \in \Gamma^+$, there exists $x \in k[\Gamma]$ with $v(x) = \gamma$. Elements $y \in (x)$ have value $v(y) \geq v(x)$ by axiom (1) of [5.31], so if $x, y \in A$ have $v(x) < v(y)$, it is impossible that $x \in (y)$, and by [5.28] we have $(y) \subsetneq (x)$. Now any infinite decreasing sequence $\gamma_1 > \gamma_2 > \cdots > 0$ in Γ gives rise to an infinite increasing sequence of ideals of A.

Simpler[5], let k be a field, $A = k[x_1, x_2, \dots]$ a polynomial ring over k in countably many indeterminates, $\mathfrak{c} = (x_1^2, x_2^2, \cdots)$, and $C = A/\mathfrak{c}$. Write $z_j = \bar{x}_j$ and $\mathfrak{q} = (z_1, z_2, \dots)$. Then $C/\mathfrak{q} \cong k$, so $\mathfrak{q}$ is maximal, and $\mathfrak{q} \subseteq \mathfrak{N}(C) \subseteq \mathfrak{q}$, so $\mathfrak{q}$ is minimal, and thus Spec$(C) = \{\mathfrak{q}\}$. But $(z_1) \subsetneq (z_1, z_2) \subsetneq (z_1, z_2, z_3) \subsetneq \cdots$ is an infinite ascending chain of ideals.

Deduce from Exercise 8 that the set of minimal prime ideals in a Noetherian ring is finite.

Let A be a Noetherian ring. By [6.8], X is a Noetherian space. By [6.7], X has only finitely many irreducible components. By [1.20.iv], the irreducible components of $X =$ Spec(A) are the closed sets $V(\mathfrak{p})$ for $\mathfrak{p}$ a minimal prime; thus there are only finitely many minimal primes of A.

If M is a Noetherian module (over an arbitrary ring A) then Supp(M) *is a closed Noetherian subspace of* Spec(A).

Recall ([3.19]) that Supp(M) is the set of prime ideals $\mathfrak{p} \lhd A$ such that $M_{\mathfrak{p}} \neq 0$. Write $\mathfrak{a} =$ Ann(M). By [3.19.v], Supp$(M) = V(\mathfrak{a})$ is closed. [1.21.iv] gives a homeomorphism $V(\mathfrak{a}) \approx$ Spec$(A/\mathfrak{a})$. But by [6.4], $A/\mathfrak{a}$ is a Noetherian ring, so [6.8] shows Spec$(A/\mathfrak{a}) \approx V(\mathfrak{a})$ is a Noetherian space.

Let $f \colon A \to B$ be a ring homomorphism and suppose that Spec(B) *is a Noetherian space (Exercise 5). Prove that $f^* \colon$* Spec$(B) \to$ Spec(A) *is a closed mapping if and only if f has the going-up property (Chapter 5, Exercise 10).*

In [5.10.i] we showed that f^* being closed implies f has the going-up property. Now suppose Spec(B) is Noetherian and f has the going-up property. Let $V(\mathfrak{b})$, for $\mathfrak{b} \lhd B$ radical, be an arbitrary closed set of Spec(B). Then by [6.5], $V(\mathfrak{b})$ is itself Noetherian, By [1.21.iv], $V(\mathfrak{b}) \approx$ Spec$(B/\mathfrak{b})$, so by [6.7], Spec$(B/\mathfrak{b})$ has only finitely many irreducible components. By [1.20.iv], these correspond to minimal primes of $B/\mathfrak{b}$, and hence minimal elements $\mathfrak{q}_j$ of $V(\mathfrak{b})$. Let $\mathfrak{p}_j = \mathfrak{q}_j^c$. Now (1.18) shows $\mathfrak{a} := \mathfrak{b}^c = \big(\bigcap \mathfrak{q}_j\big)^c = \bigcap \mathfrak{q}_j^c = \bigcap \mathfrak{p}_j$. Now if $\mathfrak{p} \in V(\mathfrak{a})$ we have $\bigcap \mathfrak{p}_j \subseteq \mathfrak{p}$, so by (1.10.ii),

[4] http://pitt.edu/~yimuyin/research/AandM/exercises06.pdf

[5] [KarpukSol]

$\mathfrak{p}_j \subseteq \mathfrak{p}$ for some j. Thus $V(\mathfrak{a}) = \bigcup V(\mathfrak{p}_j)$. [5.10.i] shows that $f^*\big(V(\mathfrak{q}_j)\big) = V(\mathfrak{p}_j)$, so $f^*\big(V(\mathfrak{b})\big) = f^*\big(\bigcup V(\mathfrak{q}_j)\big) = \bigcup f^*\big(V(\mathfrak{q}_j)\big) = \bigcup V(\mathfrak{p}_j) = V(\mathfrak{a})$ is closed.

Let A be a ring such that Spec(A) *is a Noetherian space. Show that the set of prime ideals of A satisfies the ascending chain condition. Is the converse true?*

Let $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \subseteq \cdots$ be an ascending chain of prime ideals of A. Then $V(\mathfrak{p}_1) \supseteq V(\mathfrak{p}_2) \supseteq \cdots$ is a descending chain of closed subsets of Spec(A). Since Spec(A) is Noetherian, the descending chain terminates in some $V(\mathfrak{p}_n) = V(\mathfrak{p}_{n+1})$. Then $\mathfrak{p}_n \in V(\mathfrak{p}_n) = V(\mathfrak{p}_{n+1})$, so $\mathfrak{p}_{n+1} \subseteq \mathfrak{p}_n \subseteq \mathfrak{p}_{n+1}$ and the chain stabilizes.

The converse is untrue. Let X be an infinite set; its power set $\mathscr{P}(X)$ with the partial order given by $\subseteq$ is a Boolean algebra by the proof of [1.25]. Let A be the associated Boolean ring ([1.24]). (Note that in fact $A \cong \prod_X \mathbb{F}_2$.) If $a \in A$, then the principal ideal $(a) \lhd A$ is the set of $ba = b \cap a$ for $b \in \mathscr{P}(X)$, which is the set of subsets $b \subseteq a$. Let $x_1, x_2, \ldots$ be an infinite sequence of distinct elements of X, and for each n let $\mathfrak{p}_n$ be the principal ideal generated by the element $X \backslash \{x_n\}$ of A. Each $\mathfrak{p}_n$ is prime, for if $a, b \in A \backslash \mathfrak{p}_n$, then $x_n \in a$ and $x_n \in b$, so $x_n \in a \cap b = ab$, meaning $ab \notin \mathfrak{p}_n$. If we let $S_n = \{s_1, \ldots, s_n\}$ for each $n \geq 1$, then $S_n \subsetneq S_{n+1}$ for each n, so if $\mathfrak{a}_n$ is the principal ideal (S_n), then $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$ for each n, so any prime containing the latter contains the former, and $V(\mathfrak{a}_n) \supseteq V(\mathfrak{a}_{n+1})$ in Spec(A). But $x_{n+1} \in S_{n+1} \in \mathfrak{a}_{n+1}$, so $\mathfrak{a}_{n+1} \nsubseteq \mathfrak{p}_{n+1}$, while for $a \in \mathfrak{a}_n$ we have $x_{n+1} \notin S_n \supseteq a$, so that $\mathfrak{a}_n \subseteq \mathfrak{p}_{n+1}$. Thus we have a strict containment $V(\mathfrak{a}_n) \supsetneq V(\mathfrak{a}_{n+1})$ for each n, so the $V(\mathfrak{a}_n)$ are an infinite descending sequence of closed subsets of Spec(A), which is then not Noetherian. But by [1.11.ii], every prime of A is maximal, so each chain of prime ideals of A has length zero, and the set of prime ideals of A satisfies the ascending chain condition.

For another demonstration the converse is untrue,[6] let k be a field, $B = \prod_{j=1}^{\infty} k$ the product of countably many copies of k, and $A = k \cdot 1 + \bigoplus k$ the subring of B consisting of all eventually constant sequences of elements of k. Write $e_j \in A$ for the element with a 1 at the j^{th} place and 0 elsewhere, and $f_n = 1 - \sum_{j \leq n} e_j$. For each $n \geq 0$ the subring $A_n = \sum_{j<n} ke_j + kf_n \subsetneq A$ is the set of sequences of elements of k constant from the $(n+1)^{\text{th}}$ element on, and we have a natural isomorphism $B_n \xrightarrow{\sim} k^{n+1}$ taking $e_j \mapsto e_j$ for $j \leq n$ and $f_n \mapsto e_{n+1}$. If $\mathfrak{b}_j = \sum_{i \neq j}(e_i)$, the proof of [1.22], shows that Spec(k^{n+1}) is a disjoint union of sets of ideals $\mathfrak{b}_j + \mathfrak{p}e_j$ for $\mathfrak{p}$ a prime of k; since k is a field, Spec$(k^{n+1}) = \{\mathfrak{b}_1, \ldots, \mathfrak{b}_{n+1}\}$. For the corresponding primes of B_n write $\mathfrak{p}_{n,j} = \sum_{i \neq j}(e_i) + (f_n)$ for $j = 1, \ldots, n$ and $\mathfrak{q}_n = \sum_{j \leq n}(e_j)$. Let $\mathfrak{p} \in$ Spec(B). Then $\mathfrak{p} \cap A_n$ is a prime. One possibility is that this prime is $\mathfrak{q}_n$ for each n. Since $B = \bigcup B_n$, then $\mathfrak{p}_0 := \mathfrak{p} = \bigcup \mathfrak{q}_n = \bigoplus k$, and $B/\mathfrak{p}_0 = B/\bigoplus k \cong k$, so $\mathfrak{p}_0$ is maximal.[7] Otherwise there is some A_n with $\mathfrak{p} \cap A_n = \mathfrak{p}_{n,m}$, and it follows $\mathfrak{p} \cap A_j = \mathfrak{p}_{j,m}$ for all $j \geq n$. Thus $e_j \in \mathfrak{p}$ for $j > m$ and $f_m \in \mathfrak{p}$, so $\mathfrak{p}$ contains $\mathfrak{p}_j = \sum_{n \neq j}(e_j) + (f_j)$. As $\mathfrak{p}_j$ is the kernel of the projection of A onto the j^{th} coordinate, it follows again $\mathfrak{p}_j$ is maximal, so $\mathfrak{p} = \mathfrak{p}_j$. All primes of A being maximal, It follows any ascending sequence of prime ideals of A is constant. On the other hand $\mathfrak{q}_n = \sum_{j \leq n}(e_j)$ gives an infinite ascending sequence of ideals of A. Evidently $V(\mathfrak{q}_n) \supseteq V(\mathfrak{q}_{n+1})$, and since $\mathfrak{q}_n \subseteq \mathfrak{p}_{n+1}$ but $\mathfrak{q}_{n+1} \nsubseteq \mathfrak{p}_{n+1}$, the inclusion is strict. Thus Spec(A) is not Noetherian.

[6] http://pitt.edu/~yimuyin/research/AandM/exercises06.pdf

[7] In case this wasn't clear, since the diagram

$$\begin{tikzcd}
0 \arrow[r] & \mathfrak{q}_n \arrow[r, hook] \arrow[d, hook] & A_n \arrow[r, two heads] \arrow[d, hook] & k \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & \mathfrak{q}_{n+1} \arrow[r, hook] & A_{n+1} \arrow[r, two heads] & k \arrow[r] & 0
\end{tikzcd}$$

is commutative, [2.18] and [2.19] give a short exact sequence $0 \to \mathfrak{p}_0 \hookrightarrow A \twoheadrightarrow k \to 0$ of direct limits.

Noetherian Rings

Theorem 7.5*. *If A is Noetherian, then the formal power series ring $A[[x]]$ is Noetherian.*

If $f = ax^m + (\deg > m)$ is an element of $A[[x]]$, define $\operatorname{ord}(f) = m$. Let $\mathfrak{a}$ be an ideal of $A[[x]]$, and let $\mathfrak{l}$ be the set of trailing coefficients of series in $\mathfrak{a}$. This is an ideal of A, for if $a, b \in \mathfrak{l}$ and $c \in A$, there are elements $f = ax^m + (\deg > m)$ and $g = bx^p + (\deg > p)$ of $\mathfrak{a}$; without loss of generality, assume $p \geq m$; then the trailing coefficient of $x^{p-m}f - g \in \mathfrak{a}$ is $a - b$, and the trailing coefficient of $cf \in \mathfrak{a}$ is ca. Since A is Noetherian, $\mathfrak{l}$ is finitely generated, say by $a_1, \dots, a_n$. By the definition of $\mathfrak{l}$, for $i = 1, \dots, n$ there is a series $f_i \in A[[x]]$ of the form $f_i = a_i x^{r_i} + (\deg > r_i)$. Let $r = \max_{i=1}^{n} r_i$. The f_i generate an ideal $\mathfrak{a}' \subseteq \mathfrak{a}$ in $A[[x]]$.

Let f be an arbitrary element of $\mathfrak{a}$, with $m = \operatorname{ord}(f) \geq r$. If $g_{i,0} = 0$ for all i, we have $f = f - \sum g_{i,0} f_i$ of order m. Let $p \geq m$, and assume inductively that there are polynomials $g_{i,p} \in A[x]$ with $\deg(g_{i,p}) \leq m - r_i$ such that $f' = f - \sum g_i f_i$ has $\operatorname{ord}(f') = p$. If $f' = ax^p + (\deg > p)$ write $a = \sum_{i=1}^{n} u_i a_i$, where $u_i \in A$; then $f' - \sum(u_i x^{p-r_i}) f_i = f - \sum(g_{i,p} + u_i x^{p-r_i}) f_i$ is in $\mathfrak{a}$ and has degree $> p$. Then $g_{i,p+1} = g_{i,p} + u_i x^{p-r_i}$ has degree $\leq p - r_i$. Since any terms we might add in transforming $g_{i,p}$ to $g_{i,p+1}$ are of strictly higher degree, as $p \to \infty$, the polynomials $g_{i,p} \in A[x]$ converge to some $g_i \in A[[x]]$, and $f - \sum g_i f_i = 0$, so $f \in \mathfrak{a}'$.

If we write $M = A + Ax + \cdots + Ax^{r-1}$, then this shows that for any $f \in \mathfrak{a}$, there is $g \in \mathfrak{a}'$ such that $f - g \in \mathfrak{a} \cap M$. Now M is a finitely generated A-module, so it is Noetherian by (6.5), and thus $\mathfrak{a} \cap M$ is a finitely generated A-module by (6.2). Therefore $\mathfrak{a} = (\mathfrak{a} \cap M) + \mathfrak{a}'$ is finitely generated.

EXERCISES

Let A be a non-Noetherian ring and let Σ be the set of ideals in A which are not finitely generated. Show that Σ has maximal elements and that the maximal elements of Σ are prime ideals.

Hence a ring in which every prime ideal is finitely generated is Noetherian (I. S. Cohen).

This result has actually be vastly generalized: there is a metatheorem giving results of the form "any ideal maximal with respect to not having property P is prime" for large natural classes of properties P of ideals.[1] For example, for any infinite cardinal $\varkappa$, any ideal maximal with respect to not being generated by $< \varkappa$ elements is prime (it is not however guaranteed that such ideals exist); the result we prove here is the $\varkappa = \aleph_0$ case.

Since A is not Noetherian, Σ is not empty. Let $\langle \mathfrak{a}_\alpha \rangle_\alpha$ be a chain in Σ, and $\mathfrak{a}$ its union. If $\mathfrak{a}$ was finitely generated, say by $x_i \in \mathfrak{a}_{\alpha_i}$ $(1 \leq i \leq n)$ with $\alpha_1 \leq \cdots \leq \alpha_n$, then we would have $\mathfrak{a} = (x_1, \dots, x_n) \subseteq \mathfrak{a}_{\alpha_n} \subseteq \mathfrak{a}$, showing $\mathfrak{a}_{\alpha_n} \notin \Sigma$, a contradiction. Then Zorn's Lemma furnishes maximal elements of Σ.

It is not harder to prove the next part for ideals generated by $< \varkappa$ elements than $< \aleph_0$ elements, so redefine Σ to be the set of ideals not generated by $< \varkappa$ elements. Let $\mathfrak{p}$ be a maximal element of Σ; by the last paragraph, Σ has maximal elements if $\varkappa = \aleph_0$. Suppose $a \notin \mathfrak{p}$ and $b \in A$ are such that $ab \in \mathfrak{p}$; we show $b \in \mathfrak{p}$. Now $(a) + \mathfrak{p} \in \Sigma$. If it is generated by the elements $(b_\alpha + x_\alpha)$ for $b_\alpha \in A$ and $x_\alpha \in \mathfrak{p}$ $(\alpha < \varkappa)$, then $(a) + \mathfrak{p} = (a) + (x_\alpha)$. Write $\mathfrak{a} = (x_\alpha)$. Now if $y \in \mathfrak{p} \backslash \mathfrak{a}$, then $y \in \mathfrak{p} \cap (a)$, so there is $z \in A$, such that $az = y \in \mathfrak{p}$. It follows that $z \in (\mathfrak{p} : a)$, so $y \in a(\mathfrak{p} : a)$. Thus $\mathfrak{a} + a(\mathfrak{p} : a) = \mathfrak{p})$. If $(\mathfrak{p} : a) \notin \Sigma$, we would have $a(\mathfrak{p} : a) \notin \Sigma$ and hence $\mathfrak{p} \notin \Sigma$, so it follows that $(\mathfrak{p} : a) \in \Sigma$. Now $\mathfrak{p} \subseteq (\mathfrak{p} : a)$, and if the containment were strict, we would have $(\mathfrak{p} : a) \notin \Sigma$, so $b \in (\mathfrak{p} : a) = \mathfrak{p}$.

Let A be a Noetherian ring and let $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$. Prove that f is nilpotent if and only if each a_n is nilpotent.

By [1.5.ii], if f is nilpotent, then all a_n are nilpotent. On the other hand, suppose all a_n are nilpotent. By (7.15), the nilradical $\mathfrak{N}$ of A is nilpotent, meaning there is $m \geq 1$ such that $\mathfrak{N}^m = 0$. That means any product $a_I = \prod_{i=1}^{m} a_{n_i} = 0$. In f^m, each term is divisible by some a_I, so $f^m = 0$.

[1] Tsit Yuen Lam and Manuel L. Reyes: http://bowdoin.edu/~reyes/oka1.pdf

Let $\mathfrak{a}$ be an irreducible ideal in a ring A. Then the following are equivalent:
i) $\mathfrak{a}$ is primary;
ii) for every multiplicatively closed subset S of A we have $(S^{-1}\mathfrak{a})^c = (\mathfrak{a} : x)$ for some $x \in S$;
iii) the sequence $(\mathfrak{a} : x^n)$ is stationary, for every $x \in A$.

i) $\implies$ ii): Let $\mathfrak{a}$ be primary and $a \in \mathfrak{a}$. (4.8) says that either $(S^{-1}\mathfrak{a})^c = \mathfrak{a} = (\mathfrak{a} : 1)$ or $(S^{-1}A)^c = A = (\mathfrak{a} : a)$.

ii) $\implies$ iii): Let $x \in A$, and $S_x = \{1, x, x^2, \ldots\}$. Recall from [4.12] that $S_x(\mathfrak{a}) := (S_x^{-1}\mathfrak{a})^c = \{y \in A : S_x y \cap \mathfrak{a} \neq \varnothing\}$. But this is $\bigcup_{s \in S_x} (\mathfrak{a} : s) = \bigcup_{n \geq 0} (\mathfrak{a} : x^n)$. By assumption, this is also equal to $(\mathfrak{a} : s)$ for some $s = x^n \in S$. Then $(\mathfrak{a} : x^n) \subseteq (\mathfrak{a} : x^{n+m}) \subseteq S_x(\mathfrak{a}) = (\mathfrak{a} : x^n)$ for all $m \geq 0$, so the chain of ideals $(\mathfrak{a} : x^n)$ is stationary.

iii) $\implies$ i): Since $\mathfrak{a}$ is irreducible in A, we have (0) irreducible in $A' = A/\mathfrak{a}$. Suppose $\widetilde{x}\widetilde{y} \in \mathfrak{a}$ with $\widetilde{x}, \widetilde{y} \in A$ and $y \notin \mathfrak{a}$. Let x, y be their images in A'. The increasing chain $(\mathfrak{a} : \widetilde{x}^n)$ in A is stationary, and its image in A' is $(0 : x^n) = \operatorname{Ann}(x^n)$, so for some n we have $\operatorname{Ann}(x^n) = \operatorname{Ann}(x^{n+1})$. If $a \in (y) \cap (x^n)$, write $a = by = cx^n$. Then $0 = bxy = cx^{n+1}$, so $c \in \operatorname{Ann}(x^{n+1}) = \operatorname{Ann}(x^n)$, meaning $a = cx^n = 0$. Thus $(0) = (y) \cap (x^n)$. Since (0) is irreducible, it follows that $(x^n) = (0)$, so $\widetilde{x}^n \in \mathfrak{a}$. Thus $\mathfrak{a}$ is primary.

Which of the following rings are Noetherian? In all cases the coefficients are complex numbers.
i) The ring of rational functions of z having no pole on the circle $|z| = 1$.

This ring A is Noetherian. Any element of A can be written in least terms as $p(z)/q(z) \in \mathbb{C}(z)$, for $p(z), q(z) \in \mathbb{C}[z]$ such that $q(z)$ has no root on the circle $|z| = 1$. Put another way, $q(z)$ can be any polynomial in the multiplicatively closed set $S = \mathbb{C}[z] \backslash \bigcup_{|a|=1} (z - a)$. Thus $A = S^{-1}\mathbb{C}[z]$. Since $\mathbb{C}[z]$ is Noetherian (for example by (7.5)), its localization A is Noetherian by (7.3).

ii) The ring of power series in z with a positive radius of convergence.

This ring A is Noetherian. Let B be an arbitrary ring, and z an indeterminate. Recall ([1.5]) that $f \in B[[z]]$ is a unit just if $f \in B^\times + (z)$, that is, the constant term of f is a unit. If $B = k$ is a field, this just means the constant term is nonzero. Each nonzero element $f \in k[[z]]$ has some order $\operatorname{ord}(f)$ (the least m such that the coefficient of z^m in f is non-zero), and thus $f = z^{\operatorname{ord}(f)} g$ for some $g \in k^\times + (z)$. Since g is a unit, it follows $fg^{-1} = z^{\operatorname{ord}(f)} \in (f)$, and so $(f) = (z^{\operatorname{ord}(f)})$. Thus the ideals of $k[[z]]$ are (0) and (z^n) for $n \geq 0$. But the non-trivial ideals of $k[[z]]$ are well-ordered by $\supseteq$, so we see (as in (7.5*)) that $k[[z]]$ is Noetherian.

We show that each ideal of A is the contraction of an ideal of $\mathbb{C}[[z]]$, so A is Noetherian. Let $f \in A \subsetneq \mathbb{C}[[z]]$ be nonzero, and write $f = z^m g$ for g a unit of $\mathbb{C}[[z]]$. The radius of convergence of g is the same as that of f, so $g \in A$.[2] The inverse g^{-1} of g in $\mathbb{C}[[z]]$ is also in A,[3] so $g^{-1}f = z^m$ in A, showing $(f) = (z^m)$ again.

iii) The ring of power series in z with an infinite radius of convergence.

This ring A is not Noetherian. Let $f_n = \prod_{j=n}^{\infty} \left(1 - \frac{z^2}{n^2}\right)$ for each $n \geq 1$. It can be shown that $f_n \in A$; in fact $\pi z f_1 = \sin \pi z$. (If you like, replace the factors by $1 - \frac{z^2}{2^{2n}}$, whose product more obviously converges.) Note that the roots of $1 - \frac{z^2}{n^2}$ are $z = \pm n$. Now each element of (f_n) vanishes at $\pm n$, for $\lim_{z \to n} |f_n(z)| = 0$, and if we have $g f_n(n) \neq 0$ for some $g \in \mathbb{C}[[z]]$, it follows $\lim_{z \to n} |g(z)| = \infty$, and hence g has radius of convergence $\leq n$ and is not in A. Now since $f_{n+1} | f_n$ for each n, we have $(f_n) \subseteq (f_{n+1})$, but $f_{n+1} \notin (f_n)$ since f_{n+1} does not vanish at $\pm n$. Thus (f_n) is an infinite ascending series of ideals in A.

iv) The ring of polynomials in z whose first n derivatives vanish at the origin (n being a fixed integer).

This ring A is Noetherian. We claim it is actually the subring $A = \mathbb{C} + (z^{n+1}) \subsetneq \mathbb{C}[z]$.[4] Now $\mathbb{C}[z^{n+1}] \cong \mathbb{C}[z]$ is Noetherian by (7.5), and the inclusion $\mathbb{C}[z^{n+1}] \hookrightarrow A$ makes A a $\mathbb{C}[z^{n+1}]$-module, finitely generated by $\{1, z, \ldots, z^n\}$. Then (7.2) says A is Noetherian as well.

[2] Write $f(z) = \sum a_n z^{n+m}$ and set $c = \limsup_{n \to \infty} \sqrt[n+m]{|a_n|}$ and $R = 1/c$. If $|z| < R$, then for some $\epsilon > 0$, we have $|z| < 1/(c + \epsilon)$, which implies that for all sufficiently large n we have $|a_n z^{n+m}| < |a_n|(c+\epsilon)^{-(n+m)} \leq \frac{c}{c+\epsilon}^{n+m}$. It follows that $|a_n z^n| \leq \frac{1}{|z|^m} \frac{c}{c+\epsilon}^{n+m}$ for n large enough, so by comparison with the geometric series, $g(z)$ converges.

[3] See the footnote to [10.8].

[4] Note first that the definition must be interpreted to involve the derivatives $\frac{d}{dz}, \ldots, \frac{d^n}{dz^n}$; the requirement specifically *can't* include that $f = (d/dz)^0(f)|_{z=0} = 0$, because we want 1 in our ring. A really is a ring (actually a $\mathbb{C}$-algebra), because derivatives are linear, and because by the generalized Leibniz formula (see http://planetmath.org/encyclopedia/GeneralizedLeibnizRule.html) $\frac{d^n}{dz^n}(fg) = \sum_{j=0}^{n} \binom{n}{j} \frac{d^{n-j}}{dz^{n-j}} f \cdot \frac{d^j}{dz^j} g$, so if the first n derivatives of f and g vanish at $z = 0$, then so do those of fg. Now $\frac{d^n}{dz^n}(z^m) = m \cdots (m - n + 1) z^{m-n}$, which is zero for $m \leq n$. If $f = \sum_{j=0}^{m} a_m z^m$, then $\frac{d^n}{dz^n}\Big|_{z=0}(f) = \sum_{j=n}^{m} a_j j \cdots (j - n + 1) 0^{j-n} = n! a_n$, which is zero just when $a_n = 0$. Thus the first n derivatives of f vanish at 0 just if the coefficients $a_1, \ldots, a_n$ are zero.

v) The ring of polynomials in z, w all of whose partial derivatives with respect to w vanish for $z=0$.

This ring A is not Noetherian. As in iv), the requirement must be on $\frac{\partial^n}{\partial w^n}\Big|_{z=0}$ for n *strictly greater* than 0 in order that $1 \in A$. The linearity of partial derivatives and the generalized Leibniz formula again show A really is a ring. Let $f \in A$, and write $f = \sum_{j=0}^m p_j(z)w^j$ for $p_j \in \mathbb{C}[z]$. If $a_j = p_j(0)$ is the constant term, then $\frac{\partial^n}{\partial w^n} f\Big|_{z=0} = \sum_{j=n}^m a_j j \cdots (j-n+1)w^{j-n}$, which vanishes identically in w just if all coefficients are zero. Then $a_j j \cdots (j-n+1) = 0$ for all $n > 0$ and $j \geq n$, so $a_j = 0$ for all $j > 0$. Thus $A = \mathbb{C}[z] + (z)\mathbb{C}[w]$. In particular, $w^n \notin A$, so we do *not* have $zw^n | zw^m$ for $m > n$. Now let $\mathfrak{a}_n = (zw, zw^2, \ldots, zw^n) \lhd A$. Then $\mathfrak{a}_n \subsetneq \mathfrak{a}_{n+1}$ since $zw^{n+1} \notin \mathfrak{a}_n$, so $(\mathfrak{a}_n)$ is an infinite ascending chain of ideals of A.

Let A be a Noetherian ring, B a finitely generated A-algebra, G a finite group of automorphisms of B, and B^G the set of all elements of B which are left fixed by every element of G. Show that B^G is a finitely generated A-algebra.

Recall from [5.12] that B is integral over B^G. Then (7.8) applied to the chain $A \subseteq B^G \subseteq B$ says that B^G is finitely generated as an A-algebra.

If a finitely generated ring is a field, then it is a finite field.

[CAN THIS BE IMPROVED BY USING DGK, etc.?]

Let k be our finitely generated field. We can without loss of generality assume 1 is part of the finite generating set; then k is finitely generated over the subring $A = \mathbb{Z} \cdot 1$. Since k is a field, A must be $\mathbb{Z}$ or $\mathbb{F}_p$. If $A \cong \mathbb{F}_p$, then A is a field, and Zariski's Lemma ((1.27.2*), (5.24), [5.18], (7.9)) shows k is a finite extension of $\mathbb{F}_p$, so a finite field.

Otherwise $A \cong \mathbb{Z}$, and we will derive a contradiction. k being a field, there is a subfield of k isomorphic to $\mathbb{Q}$. As k is finitely generated over this subfield, Zariski's Lemma shows k is a finite (hence integral) extension of $\mathbb{Q}$. Then (5.8) applied to the chain $\mathbb{Z} \subsetneq \mathbb{Q} \subseteq k$ gives $\mathbb{Q}$ finitely generated over $\mathbb{Z}$. But $\mathbb{Q}$ is not finitely generated over $\mathbb{Z}$.[5]

Let X be an affine algebraic variety given by a family of equations $f_\alpha(t_1, \ldots, t_n) = 0$ ($\mathfrak{a} \in I$) (Chapter 1, Exercise 27). Show that there exists a finite subset I_0 of I such that X is given by the equations $f_\alpha(t_1, \ldots, t_n) = 0$ for $\mathfrak{a} \in I_0$.

By (7.6) $A = k[t_1, \ldots, t_n]$ is Noetherian, so by (6.2) the ideal $\mathfrak{a} \lhd k[t_1, \ldots, t_n]$ generated by $\{f_\alpha : \alpha \in I\}$ is finitely generated. Say its generators are $g_1, \ldots, g_n \in \mathfrak{a}$. Then each g_i is an A-linear combination of finitely many $f_{\alpha_{i,j}}$. Now $I_0 = \{\alpha_{i,j} : i = 1, \ldots, n,\ \ j = 1, \ldots, m_i\} \subseteq I$ is a finite set, and $\{f_\alpha : \alpha \in I_0\}$ generates $\mathfrak{a}$. A point $x \in k^n$ satisfies $f_\alpha(x) = 0$ for all $\alpha \in I_0$ just if $f(x) = 0$ for all $f \in \mathfrak{a}$ just if $f_\alpha(x) = 0$ for all $\alpha \in I$, so X is given by the vanishing of the finite subset $\{f_\alpha : \alpha \in I_0\}$.

If $A[x]$ is Noetherian, is A necessarily Noetherian?

Yes. There is a canonical surjection $A[x] \twoheadrightarrow A$, so by (7.1), the quotient A is Noetherian if $A[x]$ is.

Let A be a ring such that

(1) for each maximal ideal $\mathfrak{m}$ of A, the local ring $A_\mathfrak{m}$ is Noetherian;

(2) for each $x \neq 0$ in A, the set of maximal ideals of A which contain x is finite.

Show that A is Noetherian.

Let $\mathfrak{a} \lhd A$ be a non-zero ideal. By (2), for each $x \in A$ the set M_x of maximal ideals $\mathfrak{m} \ni x$ is finite, so the set $M = \bigcap_{x \in \mathfrak{a}} M_x$ of maximal ideals containing $\mathfrak{a}$ is finite. For each $\mathfrak{m} \in M$, the extension $S_\mathfrak{m}^{-1}\mathfrak{a}$ of $\mathfrak{a}$ in $A_\mathfrak{m}$ is finitely generated by (6.2) since (1) says $A_\mathfrak{m}$ is Noetherian. We may without loss of generality take these generators to be of the form $x/1$ for $x \in \mathfrak{a}$. Let $\mathfrak{a}_\mathfrak{m} \subseteq \mathfrak{a}$ be the ideal of A finitely generated by these x. Now let z be an arbitrary non-zero element of $\mathfrak{a}$, and let N_z be the finite set $M_z \setminus M$. No $\mathfrak{n} \in N_z$ contains $\mathfrak{a}$, so there is $y_\mathfrak{n} \in \mathfrak{a} \setminus \mathfrak{n}$. Now let $\mathfrak{b} = \sum_{\mathfrak{m} \in M} \mathfrak{a}_\mathfrak{m} + (z) + \sum_{\mathfrak{n} \in N_z} (y_\mathfrak{n}) \subseteq \mathfrak{a}$. This ideal is finitely generated. For $\mathfrak{m} \in M$, we have $S_\mathfrak{m}^{-1}\mathfrak{a} \subseteq S_\mathfrak{m}^{-1}\mathfrak{b}$ by construction, so the two are equal. For maximal ideals $\mathfrak{m} \notin M_z$, we have $z \in S_\mathfrak{m}$, so $S_\mathfrak{m}^{-1}\mathfrak{b} = (1)$, and for $\mathfrak{n} \in N_z$ we have $y_\mathfrak{n} \in S_\mathfrak{n}$, so $S_\mathfrak{n}^{-1}\mathfrak{b} = (1)$. But if $\mathfrak{m} \notin M$, then $S_\mathfrak{m}^{-1}\mathfrak{a} = (1)$, and $\mathrm{Max}(A) \setminus M = (\mathrm{Max}(A) \setminus M_z) \cup N_z$, so the localizations of $\mathfrak{a}$ and $\mathfrak{b}$ are equal at all maximal ideals. This means the canonical injections (see (3.3)) $S_\mathfrak{m}\mathfrak{b} \to S_\mathfrak{m}\mathfrak{a}$ induced by $\mathfrak{b} \hookrightarrow \mathfrak{a}$ are all surjective. (3.9) then says that the inclusion $\mathfrak{b} \hookrightarrow \mathfrak{a}$ is surjective, so that $\mathfrak{b} = \mathfrak{a}$ is finitely generated.

[5] Suppose it were, say by $a_1/b_1, \ldots, a_n/b_n$ for $a_j, b_j \in \mathbb{Z}$, or without loss of generality by $1/b_j$. Then if $b = \prod_{j=1}^n b_j$, then $\mathbb{Q} = \mathbb{Z}[1/b]$. But then if $p \in \mathbb{N}$ is a prime not dividing b, we would have $1/p \notin \mathbb{Q}$, a contradiction.

Let M be a Noetherian A-module. Show that $M[x]$ (Chapter 2, Exercise 6) is a Noetherian $A[x]$-module.

This should be possible to prove in a way that specializes into the proof of Hilbert Basis Theorem (7.5) in the case $M = A$. Let N be a submodule of $M[x]$; by (6.2), it will be enough to show N is finitely generated over $A[x]$. Let $P \subseteq M$ be the A-module consisting of its leading coefficients. As M is a Noetherian A-module, P is finitely generated, say by $m_1, \ldots, m_n$. Let $p_1(x), \ldots, p_n(x)$ be elements of $M[x]$ with leading coefficients m_i, and let $N' \subseteq N$ be the $A[x]$-submodule finitely generated by the $p_i(x)$. Say $r_i = \deg(p_i)$ and $r = \max_{i=1}^{n} r_i$.

Suppose $f(x) \in N$ has $\deg(f) = p \geq r$ and leading coefficient $m \in P$. Then there are a_i in A such that $m = \sum a_i m_i$, so $\sum a_i p_i(x) x^{p-r_i} \in N'$ is such that $f'(x) = f(x) - \sum a_i g_i(x) x^{p-r_i}$ has $\deg(f') < m$. By induction, there is $g \in N'$ such that $\deg(f-g) < r$.

Write $N'' = M + Mx + \cdots + Mx^{r-1}$; then we have just shown $N = (N \cap N'') + N'$. Now N'' is a finitely generated A-module, so it is a Noetherian A-module by (6.5). Thus its submodule $N \cap N''$ is finitely generated over A by (6.2), and hence a fortiori finitely generated over $A[x]$. This shows N is finitely generated.

Let A be a ring such that each local ring $A_\mathfrak{p}$ is Noetherian. Is A necessarily Noetherian?

No. Let X be an infinite set and $A = \mathscr{P}(X)$ the power set, viewed as a Boolean ring. We showed in [6.12] that A is not Noetherian. Let $\mathfrak{p} \in \operatorname{Spec}(A)$, and $a/s \in A_\mathfrak{p}$, for $a \in A$ and $s \in A \backslash \mathfrak{p}$. By the definition of a Boolean ring, $a^2 = a$ and $s^2 = s$, so $(a/s)^2 = a^2/s^2 = a/s$ is idempotent. But $A_\mathfrak{p}$ is a local ring, so by [1.12], $a/s = 0$ or 1. Thus $A_\mathfrak{p} \cong \mathbb{F}_2$ is a field, hence surely Noetherian.

The other counterexample in [6.12] also works here. Recall that it is the subring $A = k \cdot 1 + \bigoplus k$ of the countable direct product $\prod_{j=1}^{\infty} k$, and it is not Noetherian. We claim that each localization at a prime is k, and hence Noetherian (cf. [3.5]). Write k_n for the n^{th} direct summand of $\mathfrak{p}_0 := \bigoplus k_n \subsetneq A$, and $k_0 := k \cdot 1 \subseteq A$. Recall that we defined $e_n \in k_n \subsetneq B$ be the image of the 1 of k_n and $f_n = 1 - \sum_{j \leq n} e_n$, and the prime ideals of A are just $\mathfrak{p}_0$ and $\mathfrak{p}_n := (f_n) + \bigoplus_{j \neq n} k_j$ for $n > 0$. Their complements are $S_n := A \backslash \mathfrak{p}_n = \mathfrak{p}_n + k_n^\times$. To find $S_n^{-1}A$, recall that for each $n \geq 0$, A is generated as an A-module by $\{f_n\} \cup \{e_j : j \geq 1\}$; thus there is an A-module surjection $M_n = Af_n \times \bigoplus_{j \geq 1} ke_j \to A$. Since localization is exact (3.3), $S_n^{-1}A$ is the image of the localization of the left-hand side under the induced map. For $n \geq 0$, write $D_n = Af_n \times \bigoplus_{j \neq n} ke_j$ for the submodule of M mapping onto $\mathfrak{p}_n$. It was shown in the course of proving [3.19.iv] that localization distributes over arbitrary exact sums, so to compute $S_n^{-1}M_n$, it will suffice to compute $S_n^{-1}ke_j$ for $j \neq n$, $S_n^{-1}ke_n$, and $S_n^{-1}Af_n$. Since S_0 contains each f_n, and $f_n e_j = 0$ for $j \leq n$, by [3.1] each $S_0^{-1}e_j = 0$; on the other hand, $S_0^{-1}Af_0 = (k_0^\times)^{-1}k_0 \cong k_0$. Thus $S_0^{-1}M \cong k_0 \cong k$. For $n > 0$, since S_n contains each e_j for $j \neq n$ and $e_j e_l = 0$ for $j \neq l$, we have $S_n^{-1}ke_j = 0$, by [3.1], for $j \neq n$; since S_n contains e_n and $e_n f_n = 0$, $S_n^{-1}Af_n = 0$; but $S_n^{-1}k_n = (k_n^\times)^{-1}k_n \cong k_n$; so $S_n^{-1}M \cong k_n \cong k$. Now for all $n \geq 0$, $S_n^{-1}A$ is a quotient of $S_n^{-1}A$, so it is also isomorphic to k.

Let A be a ring and B a faithfully flat A-algebra (Chapter 3, Exercise 16). If B is Noetherian, show that A is Noetherian.

Since B is faithfully flat over A we have $\mathfrak{a}^{ec} = \mathfrak{a}$ for all $\mathfrak{a} \lhd A$, so $\mathfrak{a} \mapsto \mathfrak{a}^e$ is injective. Thus any infinite ascending chain $\langle \mathfrak{a}_n \rangle_{n \in \mathbb{N}}$ of ideals of A would give rise to an infinite ascending chain $\langle \mathfrak{a}_n^e \rangle_{n \in \mathbb{N}}$ of ideals of B.

Let $f \colon A \to B$ be a ring homomorphism of finite type and let $f^* \colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ be the mapping associated with f. Show that the fibers of f^* are Noetherian subspaces of B [$\operatorname{Spec}(B)$, rather].

Recall (p. 30) that the homomorphism being of *finite type* means that B is finitely generated as an A-algebra (or equivalently, $f(A)$-algebra). Then B is a quotient of some polynomial ring $C = A[t_1, \ldots, t_m]$ (in particular, a C-algebra). Now recall from [3.21.iv] that the fiber $(f^*)^{-1}(\{\mathfrak{p}\}) \approx \operatorname{Spec}\big(k(\mathfrak{p}) \otimes_A B\big)$, where $k(\mathfrak{p})$ is the field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. By (2.14.iv) and (2.15), $k(\mathfrak{p}) \otimes_A B \cong k(\mathfrak{p}) \otimes_A C \otimes_C B$. But by [2.6] and induction,[6] $k(\mathfrak{p}) \otimes_A C = k(\mathfrak{p}) \otimes_A A[t_1, \ldots, t_m] \cong k(\mathfrak{p})[t_1, \ldots, t_m]$, so the fiber is $\operatorname{Spec}\big(k(\mathfrak{p})[t_1, \ldots, t_m] \otimes_C B\big)$. But $C \twoheadrightarrow B$ is surjective, and (2.18) says tensor is right exact, so $k(\mathfrak{p})[t_1, \ldots, t_m] \cong k(\mathfrak{p}) \otimes_A C \to k(\mathfrak{p}) \otimes_A B$ is surjective. (7.6) says $k(\mathfrak{p})[t_1, \ldots, t_m]$ is Noetherian, so by (7.1), its quotient $k(\mathfrak{p}) \otimes_A B$ is Noetherian, and by [6.8], this then has Noetherian spectrum.

Nullstellensatz, strong form

[6] Assume M is an A-module, and inductively, $M[x_1, \ldots, x_n] \cong A[x_1, \ldots, x_n] \otimes_A M$. Pretty clearly $A[x_1, \ldots, x_n][y] \cong A[x_1, \ldots, x_n, y]$. Then

$$M[x_1, \ldots, x_n, y] \overset{[2.6]}{\cong} A[y] \otimes_A M[x_1, \ldots, x_n] \overset{(2.14)}{\cong} A[y] \otimes_A A[x_1, \ldots, x_n] \otimes_A M \overset{[2.6]}{\cong} A[x_1, \ldots, x_n, y] \otimes_A M.$$

Let k be an algebraically closed field, let A denote the polynomial ring $k[t_1, \ldots, t_n]$ and let $\mathfrak{a}$ be an ideal in A. Let V be the variety in k^n defined by the ideal $\mathfrak{a}$, so that V is the set of all $x = \langle x_1, \ldots, x_n \rangle \in k^n$ such that $f(x) = 0$ for all $f \in \mathfrak{a}$. Let $I(V)$ be the ideal of V, i.e. the ideal of all polynomials $g \in A$ such that $g(x) = 0$ for all $x \in V$. Then $I(V) = r(\mathfrak{a})$.

Note that if we write $V = Z(\mathfrak{a})$, our goal is to show $IZ(\mathfrak{a}) = r(\mathfrak{a})$.

By item 4 of [1.29], $\mathfrak{a} \subseteq IZ(\mathfrak{a})$, and by item 9, $IZ(\mathfrak{a}) = r\big(IZ(\mathfrak{a})\big)$, so $r(\mathfrak{a}) \subseteq IZ(\mathfrak{a})$.

On the other hand, suppose $f \notin r(\mathfrak{a})$; we show $f \notin IZ(\mathfrak{a})$. As $f \notin r(\mathfrak{a})$, there is a prime $\mathfrak{p}$ containing $\mathfrak{a}$ but not f, so $g := \bar{f} \neq 0$ in the integral domain $B = A/\mathfrak{p}$. If $C = B_g = B[1/g]$, then by (1.3) C contains a maximal ideal $\mathfrak{n}$, and $C/\mathfrak{n}$ is a field. Now $C/\mathfrak{n}$ is a k-algebra, finitely generated over k by $1/g$ and the images of the t_i. By Zariski's Lemma ((1.27.2*), (5.24), [5.18], (7.9)) $C/\mathfrak{n}$ is a finite algebraic extension of k, and thus, since k is algebraically closed, isomorphic to k. Then the surjective k-algebra homomorphism

$$\phi\colon A \twoheadrightarrow A/\mathfrak{a} \twoheadrightarrow A/\mathfrak{p} = B \rightarrowtail B_g = C \twoheadrightarrow C/\mathfrak{n} \xrightarrow{\sim} k$$

has kernel $\mathfrak{m}$ a maximal ideal of A containing $\mathfrak{a}$. By [1.27], $\mathfrak{m}$ is of the form $\mathfrak{m}_x = (t_1 - x_1, \ldots, t_n - x_n)$ for some $x = \langle x_1, \ldots, x_n \rangle \in k^n$, so $\phi(t_j) = x_j$ and $\phi\colon A \to k$ is the "evaluate at x" map $h \mapsto h(x)$. Since $\phi(\mathfrak{a}) = 0$, we have $x \in Z(\mathfrak{a})$. Since $g = \bar{f}$ is a unit in C, its image remains a unit in k, so $g(x) = \phi(g) \neq 0$. It follows that $g \notin IZ(\mathfrak{a})$.

Here is the classic proof of the Strong Nullstellensatz from the Weak ([5.17], cf. [5.18], [1.27], (5.24), (7.9)) by what is called the "Rabinowitsch trick."[7]

Let k, A, and $\mathfrak{a} \lhd A$ be as above, and suppose $g \in IZ(\mathfrak{a})$. If y now is a new indeterminate, consider the polynomial ring $A[y]$. The polynomial $1 - yg$ is 1 on the set $Z(\mathfrak{a}^e) \subseteq k^{n+1}$, so that $\mathfrak{a}^e + (1 - yg)$ vanishes nowhere and hence by the Weak Nullstellensatz is the ideal (1) of $A[y]$. Then there are finitely many $f_i \in \mathfrak{a}$ and $h_i(y)$, $h'(y) \in A[y]$ such that

$$1 = \sum f_i h_i(y) + (1 - yg)h'(y).$$

Under the A-algebra homomorphism $A[y] \to A_g \subsetneq k(t)$ taking $y \mapsto 1/g$, this equation is mapped to

$$1 = \sum f_i h_i(1/g) + \Big(1 - \frac{g}{g}\Big)h'(1/g) = \sum f_i \frac{H_i}{g^m},$$

for some $H_i \in A$ and $m = \max_i\{\deg_y h_i\}$. Multiplying through by g^m shows $g \in r(\mathfrak{a})$.

To use the theory of Jacobson rings instead to prove the Strong Nullstellensatz, detouring past the Weak Nullstellensatz but not Zariski's Lemma, proceed as follows.

Recall from [5.24] that $A = k[t]$ is a Jacobson ring and from [5.23] that a prime of A is an intersection of maximal ideals. Since by [1.9] a radical ideal is an intersection of the primes containing it, it follows that a radical ideal in A is the intersection of the maximal ideals containing it. Since $IZ(\mathfrak{a})$ is radical by item 9 of [1.29], it follows it is the intersection of the maximal ideals containing it, so it only remains to show each maximal ideal containing $\mathfrak{a}$ also contains $IZ(\mathfrak{a})$. Taking $X = \{x\}$ in item 0 of [1.27], we have $x \in Z(\mathfrak{a}) \iff \mathfrak{a} \subseteq \mathfrak{m}_x$, and taking $X = Z(\mathfrak{a})$ in item 8, we have $x \in Z(\mathfrak{a}) \iff IZ(\mathfrak{a}) \subseteq \mathfrak{m}_x$. But by the result of [1.27], these are the only maximal ideals of A, so $r(\mathfrak{a}) = IZ(\mathfrak{a})$.

For further proofs of the Nullstellensatz, see this discussion: `http://mathoverflow.net/questions/15226/elementary-interesting-proofs-of-the-nullstellensatz`. For numerous relatives, see Chapter 11 of Pete L. Clark's notes `http://math.uga.edu/~pete/integral.pdf`.

Let A be a Noetherian local ring, $\mathfrak{m}$ its maximal ideal and k its residue field, and let M be a finitely generated A-module. Then the following are equivalent:

i) M is free;

ii) M is flat;

iii) the mapping of $\mathfrak{m} \otimes M$ into $A \otimes M$ is injective;

iv) $\mathrm{Tor}_1^A(k, M) = 0$.

i) $\implies$ ii): By (2.14.iv), A is a flat A-module. By [2.4], a direct sum of flat modules is flat, so a free A-module is flat.

[7] This originated in the influential one-page paper [Rabinowitsch]. Just who Rabinowitsch was is an interesting question; it appears that he later moved to the United States and became the influential mathematical physicist George Yuri Rainich. See also [MOPseud], [Mollin, p. 154], [Nark, p. 38].

ii) $\implies$ iii): This follows from (2.19) defining flatness.

iii) $\implies$ iv): We have a short exact sequence $0 \to \mathfrak{m} \otimes M \to A \otimes M \to k \otimes M \to 0$, implying $\operatorname{Tor}_1(k, M) = 0$ by the Tor exact sequence.

iv) $\implies$ i): Let $x_1, \ldots, x_n$ be such that their images form a basis of the finite-dimensional k-vector space $k \otimes_A M \cong M/\mathfrak{m}M$; by (2.8), they generate M. Then there is an A-linear surjection $A^n \twoheadrightarrow M$ taking $e_j \mapsto x_j$, say with kernel N, yielding a short exact sequence $0 \to N \to A^n \to M \to 0$ of A-modules. Tensoring with k we have a Tor sequence (using "ii) $\iff$ iv)") $\operatorname{Tor}_1(k, M) = 0 \to k \otimes N \to k^n \to k \otimes M \to 0$. Since $\dim_k k^n = n = \dim_k(k \otimes M)$, linear algebra (or (6.9)) gives $\dim_k(k \otimes N) = 0$, so $k \otimes N = 0$. As A is Noetherian, A^n is a Noetherian A-module by (6.5), and since $N \subseteq A^n$, by (6.2) N is finitely generated. k being finitely generated as well, [2.3] shows either $k = 0$ or $N = 0$. By assumption, $A \neq \mathfrak{m}$, so $k \neq 0$. Therefore $N = 0$, and the map $A^n \to M$ is an isomorphism.[8]

Let A be a Noetherian ring, M a finitely generated A-module. Then the following are equivalent:

i) M is a flat A-module;

ii) $M_\mathfrak{p}$ is a free $A_\mathfrak{p}$-module, for all prime ideals $\mathfrak{p}$;

iii) $M_\mathfrak{m}$ is a free $A_\mathfrak{m}$-module, for all maximal ideals $\mathfrak{m}$.

In other words, flat = locally free.

Since each $A_\mathfrak{p}$ is local and each $M_\mathfrak{p}$ finitely generated over $A_\mathfrak{p}$, [7.15] says $M_\mathfrak{p}$ is free if and only if it is flat. The equivalence then follows from (3.10).

Let A be a ring and M a Noetherian A-module. Show (by imitating the proofs of (7.11) and (7.12)) that every submodule N of M has a primary decomposition.

Call a submodule $M \subseteq N$ *irreducible* if it is not an intersection of two proper supermodules; that is, for $P_1, P_2 \subseteq M$ submodules, we have $N = P_1 \cap P_2 \implies P_1 = N$ or $P_2 = N$.

If a submodule $N \subseteq M$ can be written as a finite intersection $\bigcap_{j=1}^n P_j$ of irreducible modules $P_j \subseteq M$, we call this expression an *irreducible decomposition* of N.

Lemma 7.11*. *In a Noetherian A-module M, every submodule has an irreducible decomposition.*

Suppose Σ is the set of submodules of M not admitting an irreducible decomposition, and suppose for a contradiction that $\Sigma \neq \varnothing$. Then as M is Noetherian, Σ contains a maximal element N. Then $N = \bigcap\{N\}$ is not an irreducible decomposition, by assumption, so N is not irreducible, and we can write it as $N = P \cap P'$, where $P, P' \subsetneq M$ are submodules strictly containing N. Then P and P' do admit irreducible decompositions $P = \bigcap Q_j$ and $P' = \bigcap Q'_j$, so $N = \bigcap Q_j \cap \bigcap Q'_j$ is an irreducible decomposition, contradicting $N \in \Sigma$. Thus $\Sigma = \varnothing$.

Lemma 7.12*. *In a Noetherian A-module M, every irreducible submodule is primary.*

If $Q \subseteq M$ is a submodule, then $N = M/Q$ is also Noetherian by Prop. 6.3. If Q were irreducible, then by the correspondence of p. 18, the zero submodule of $N = M/Q$ would be irreducible. We will show that if Q is not primary, then $0 \subseteq M/Q$ is reducible, so Q is reducible.

Let $x \in A$ be a zero-divisor of N that is not nilpotent on N. The submodules $0 \subseteq (0 : x) \subseteq (0 : x^2) \subseteq \cdots \subseteq N$ form an increasing chain; since N is Noetherian, the chain stabilizes at some $P = (0 : x^p) = (0 : x^{p+1})$. Since x is not nilpotent on N, we have $P \neq N$, so there is some $n \in N \backslash P$. Then $x^p n \neq 0$, so $(x^p)n \neq 0$. If $n' \in (x^p)n \cap P$, we have an expression $n' = ax^p n \in P$, and multiplying by x gives $0 = ax^{p+1}n$. Then $an \in (0 : x^{p+1}) = (0 : x^p)$, so $n' = ax^p n = 0$. Thus $(x^p)n \cap P = 0$. Since x is a zero-divisor of N, we have $P \neq 0$, showing $0 \subseteq N$ is reducible.

Thus in an Noetherian A-module M, every submodule has an irreducible decomposition, and this is a primary decomposition.

[8] Here are two extra implications we don't need.

iv) $\implies$ iii): We have a short exact sequence $0 \to \mathfrak{m} \to A \to k \to 0$, giving a Tor exact sequence containing the fragment $0 = \operatorname{Tor}_1(k, M) \to \mathfrak{m} \otimes M \to A \otimes M$. This shows $\mathfrak{m} \otimes M \to A \otimes M$ is injective.

iii) $\implies$ ii): Let $\mathfrak{a}$ be a finitely generated ideal of A. We have a short exact sequence $0 \to \mathfrak{a} \to \mathfrak{m} \to \mathfrak{m}/\mathfrak{a} \to 0$ of A-modules, whose Tor exact sequence includes $\operatorname{Tor}_1(k, M) \to \mathfrak{a} \otimes M \to \mathfrak{m} \otimes M$. Since iii) $\iff$ iv), the first term is zero; it follows that $\mathfrak{a} \otimes M \rightarrowtail \mathfrak{m} \otimes M \rightarrowtail A \otimes M$ is injective. Now the short exact sequence $0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$ gives rise to a Tor exact sequence containing $\operatorname{Tor}_1(A/\mathfrak{a}, M) \to \mathfrak{a} \otimes M \to A \otimes M$; but we've just seen the kernel of the second map is zero, so $\operatorname{Tor}_1(A/\mathfrak{a}, M) = 0$. By [2.26], then, M is flat.

Let A be a Noetherian ring, $\mathfrak{p}$ a prime ideal of A, and M a finitely generated A-module. Show that the following are equivalent:
i) $\mathfrak{p}$ belongs to 0 in M;
ii) there exists $x \in M$ such that $\operatorname{Ann}(x) = \mathfrak{p}$;
iii) there exists a submodule of M isomorphic to $A/\mathfrak{p}$.

ii) $\iff$ iii): Let $x \in M$. Then the map $A \twoheadrightarrow Ax\colon a \mapsto ax$ has kernel $\operatorname{Ann}(x)$, so induces an A-module isomorphism $A/\operatorname{Ann}(x) \xrightarrow{\sim} Ax \subseteq M$. Then for any ideal $\mathfrak{a} \lhd A$, there is a (cyclic) submodule isomorphic to $A/\mathfrak{a}$ if and only if $\mathfrak{a} = \operatorname{Ann}(x)$ for some $x \in M$.

ii) $\implies$ i): By [7.17], $0 \subseteq M$ is decomposable. The primes belonging to 0 are those among the $r(0 : y) = r\big(\operatorname{Ann}(y)\big)$ for $y \in M$ by (4.5*) in [4.22]. Thus $\mathfrak{p} = \operatorname{Ann}(x)$ belongs to 0.

i) $\implies$ ii):[9] By [7.17], $0 \subseteq M$ is decomposable, so let $N_1 \cap \cdots \cap N_n$ be an irredundant primary decomposition. Let N be one of the N_j, and N' the intersection of all the others. We will show will suffice to show $\mathfrak{p} = r_M(N) = \operatorname{Ann}(x)$ for some $x \in M$. Since the decomposition is irredundant, $N' \not\subseteq N$, so we may find (and fix) a $y \in N' \backslash N$. If $a_1, \ldots, a_m$ generate $\mathfrak{p}_j$ (possible by (6.2) since A is Noetherian) then there is for each a_j some minimal $p_j \geq 1$ such that $a_p^{p_j} y \in N$. If $p = \max_j p_j$, then we see $\mathfrak{p}^p y \subseteq N$ and $\mathfrak{p}^{p-1} y \not\subseteq N$. Let $x \in \mathfrak{p}^{p-1} y \backslash N$ then. Since $y \in N'$, we then have $\mathfrak{p}x \subseteq \mathfrak{p}^p y \subseteq N \cap N' = 0$, so $\mathfrak{p} \subseteq \operatorname{Ann}(x)$. On the other hand, if $a \in A$ is such that $ax \in N$ (hence $= 0$), then a is a zero-divisor of M/N; as N is primary, this means a is nilpotent on M/N. But this says exactly that $a \in r_M(N) = \mathfrak{p}$. Thus $\mathfrak{p} = \operatorname{Ann}(x)$.[10]

Deduce that there exists a chain of submodules

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

such that each quotient M_i/M_{i-1} is of the form $A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is a prime ideal of A.

Since M is Noetherian, 0 is decomposable by [7.17], so some $\mathfrak{p}_1 \in \operatorname{Spec}(A)$ belongs to 0, and the above gives a submodule $M_1 \cong A/\mathfrak{p}_1$ of M. Assume inductively that we've found a chain $0 = M_0 \subsetneq \cdots \subsetneq M_n \subseteq M$. If $M_n = M$, we are done; otherwise, M/M_n is Noetherian, so its submodule 0 is decomposable by [7.17]. Let $\mathfrak{p}_{n+1}$ belong to it; then there is a submodule $N_{n+1} \subseteq M/M_n$ such that $N_{n+1} \cong A/\mathfrak{p}_{n+1}$. If $M_{n+1} \subseteq M$ is its pre-image under $M \twoheadrightarrow M/M_n$, we have $M_{n+1}/M_n \cong N_{n+1} \cong A/\mathfrak{p}_{n+1}$. Since M is Noetherian, this process cannot create an infinite ascending chain, so there is some M_r such that we cannot find an M_{r+1}. But we have shown that this only happens if $M_r = M$.

Let $\mathfrak{a}$ be an ideal in a Noetherian ring A. Let

$$\mathfrak{a} = \bigcap_{i=1}^{r} \mathfrak{b}_i = \bigcap_{j=1}^{s} \mathfrak{c}_j$$

be two minimal decompositions of $\mathfrak{a}$ as intersections of irreducible *ideals. Prove that $r = s$ and that (possibly after re-indexing the $\mathfrak{c}_j$) $r(\mathfrak{b}_i) = r(\mathfrak{c}_i)$ for all i.*

State and prove an analogous result for modules.

Since an ideal of A is just an A-submodule of A, a primary ideal of A is exactly a primary submodule of A (p. 50), an irreducible ideal of A is an irreducible submodule of A, $r_A(\mathfrak{a}) = r(\mathfrak{a})$, and A is a Noetherian ring just if it is Noetherian as an A-module, it will be enough to prove the result in the more general case of a submodule N of a Noetherian A-module M.

We first prove the book's hint: if $\bigcap_{i=1}^{r} P_i = \bigcap_{j=1}^{s} Q_j$ are minimal irreducible decompositions of $N \subseteq M$, and $P'_k := \bigcap_{i \neq k} P_i$ for each $k \in \{1, \ldots, r\}$, then N equals one of the $N_j := P'_k \cap Q_j$. Note that all these modules contain N, so it will be enough to show some $N_j \subseteq N$.[11] Surely since $\bigcap_{j=1}^{s} Q_j = N$ in M, we also have $\bigcap_j N_j = N$. Write $\pi_i\colon M \twoheadrightarrow M/P_i$ for the natural map, and $\phi = (\pi_1, \ldots, \pi_r)\colon M \to \bigoplus_i M/P_i$ for the induced map to the product. Now $\ker(\phi) = \bigcap_i P_i = N$. For each j and each $i \neq k$, we have $N_j \subseteq P'_k \subseteq P_i$, so $\pi_i(N_j) = 0$. Thus the only potentially non-zero coordinate of an element of the module $\phi(N_j)$ is the j^{th}, and it follows that these j^{th} coordinates make up

[9] Stolen from http://math.uiuc.edu/~r-ash/ComAlg/ComAlg1.pdf

[10] I worked for a while on another approach to this problem before turning to the experts, and this aborted effort went like this. By (4.5*) from [4.22], $\mathfrak{p} \in \operatorname{Spec}(A)$ belongs to 0 just if $\{(0 : x) : x \in A \;\&\; r(0 : x) = \mathfrak{p}\}$ is nonempty. A being Noetherian, this set contains some maximal element $\mathfrak{q} = (0 : x) = \operatorname{Ann}(x)$. We suppose $\mathfrak{q} \neq \mathfrak{p}$ and contradict maximality. If there is $a \in \mathfrak{p} \backslash \mathfrak{q}$, then there is some minimal $n \geq 2$ such that $a^n x = 0$, but $ax \neq 0$. Consider $(\mathfrak{q} : a) = \big((0 : x) : a\big) \overset{(1.12.\text{iii})}{=} (0 : ax)$. It contains $(0 : x)$, properly since $a^{n-1} \in (0 : ax) \backslash (0 : x)$. The proof will be concluded if we can show $r(0 : ax) = \mathfrak{p}$. Unfortunately, I seem unable to do this. I wanted to say "Since $a \notin \mathfrak{q}$, (4.4) says $r(\mathfrak{q} : a) = r(\mathfrak{q}) = \mathfrak{p}$, contradicting maximality of $\mathfrak{q}$"; however, (4.4) requires as a hypothesis that $\mathfrak{q}$ is primary, and it's not clear to me this must be the case.

[11] http://mathoverflow.net/questions/12322/atiyah-macdonald-exercise-7-19-decomposition-using-irreducible-ideals

a submodule $O_j = \pi_k(N_j)$ of M/P_k. Then $0 = \phi\big(\bigcap N_j\big) = \bigcap O_j \times \prod_{i \neq k}\{0\}$, so $\bigcap O_j = 0 \subseteq M/P_k$. As $P_k \subseteq M$ is irreducible, $0 \subseteq M/P_k$ is irreducible, meaning for some $j = j(k)$ we have $O_j = 0$. Then $\pi_i(N_{j(k)}) = 0$ for all i, including k, so $N_{j(k)} \subseteq N$.[12]

If we define ${}_1P_i = P_i$ for $i \neq k$ and ${}_1P_k = Q_{j(k)}$, we have another irreducible decomposition of N. Applying the previous result to the ${}_1P_i$ and the Q_j, we can then replace another of the P_i by another Q_j. Repeating this process for $k = 1, \ldots, r$, we eventually get an expression $Q_{j(1)} \cap \cdots \cap Q_{j(r)} = 0$. Since we postulated irredundancy for the Q_j decomposition, it follows $i \mapsto j(i)$ is surjective and $s \leq r$. A symmetric argument switching the roles of P_i and Q_j will then show $r \leq s$, so we see r and s are equal.

Fact 7.A*. *Any two minimal irreducible decompositions of a submodule have the same number of components.*

It remains to show we may reorder the Q_i so that $r_M(Q_i) = r_M(P_i)$ for all $i \in \{1, \ldots, s\}$. Recall from Lemma 7.12* of [7.17] that, since M is Noetherian, each irreducible module is primary, and from (4.3*) of [4.21], that an intersection of $\mathfrak{p}$-primary modules is $\mathfrak{p}$-primary; thus by collecting terms with the same radical, we obtain irredundant primary decompositions $M_1 \cap \cdots \cap M_m = N_1 \cap \cdots \cap N_n$ of $N \subseteq M$. By (4.5*) of [4.22], the sets $\{r_M(M_1), \ldots, r(M_m)\}$ and $\{r_M(N_1), \ldots, r(N_m)\} \subseteq \operatorname{Spec}(A)$ are equal, and so we may renumber them so that $\mathfrak{p}_i = r(M_i) = r(N_i)$. We may further reorder them, since there are only finitely many, so that each set $S_j := \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_j\} \subseteq \operatorname{Spec}(A)$ is isolated. Suppose that M_i is the intersection of m_i different P_j, and N_i is the intersection of n_i different Q_j. It will then suffice to show that $m_i = n_i$ for each i. By Thm. 4.10* of [4.23], applied to the isolated set S_1, we see $M_1 = N_1$. Irredundancy of the irreducible decompositions of N show the relevant P_j and Q_j each give a minimal irreducible decomposition of M_1, and then Fact 7.A above shows that $m_1 = n_1$. Assume inductively that we have shown $m_j = n_j$ for all $j < i$. Thm. 4.10* of [4.23], applied to the isolated set S_i, shows that $N_i' := \bigcap_{j=1}^{i} M_j = \bigcap_{j=1}^{i} N_j$. Irredundancy of the irreducible decompositions of N again show the relevant P_j and Q_j give a minimal irreducible decomposition of N_i', and Fact 7.A shows that $\sum_{j=1}^{i} m_j = \sum_{j=1}^{i} n_j$. By inductive assumption $m_j = n_j$ for all $j < i$, so subtracting these off, $m_i = n_i$, and we are done.

Let X be a topological space and let $\mathscr{F}$ be the smallest collection of subsets of X which contains all open subsets of X and is closed with respect to the formation of finite intersections and complements.

i) Show that a subset E of X belongs to $\mathscr{F}$ if and only if E is a finite union of sets of the form $U \cap C$, where U is open and C is closed.

Let $\mathscr{G}$ be the collection of finite unions of sets $U \cap C$, for U open and C closed.

First we show $\mathscr{G} \subseteq \mathscr{F}$. Each open set is in $\mathscr{F}$, and taking complements, each closed set is in $\mathscr{F}$. Taking intersections, each $U \cap C \in \mathscr{G}$ for U open and C closed. But $\mathscr{F}$ is closed under finite unions, for by De Morgan's laws, $\bigcup S_i = X \setminus \bigcap (X \setminus S_i)$, and $\mathscr{F}$ is assumed to be closed under complement and finite intersection.

Now we show $\mathscr{F} \subseteq \mathscr{G}$ by showing $\mathscr{G}$ satisfies the properties (except "smallest") postulated of $\mathscr{F}$.

- Taking $C = X$, each open $U \subseteq X$ is in $\mathscr{G}$.
- Finite intersections: It suffices to prove this for binary intersections. Let $S = \bigcup (U_i \cap C_i)$ and $S' = \bigcup (U_j' \cap C_j')$ be in $\mathscr{G}$. Then $S \cap S' = \bigcup_i (U_i \cap C_i) \cap \bigcup_j (U_j' \cap C_j') = \bigcup_{i,j} U_i \cap U_j' \cap C_i \cap C_j'$ by distributivity; since each $U_i \cap U_j'$ is open and each $C_i \cap C_j'$ is closed, $S \cap S' \in \mathscr{G}$.
- Complements: If $S = \bigcup_{i=1}^{n} (U_i \cap C_i) \in \mathscr{G}$, then De Morgan's laws give $X \setminus S = X \setminus \bigcup (U_i \cap C_i) = \bigcap X \setminus (U_i \cap C_i) = \bigcap [(X \setminus U_i) \cup (X \setminus C_i)]$. Now $S_{i1} = X \setminus C_i$ is open and $S_{i2} = X \setminus U_i$ is closed. Let F be the set of all functions $\{1, \ldots, n\} \to \{1, 2\}$, and for $f \in F$ write $S_f = \bigcap_{i=1}^{n} S_{i, f(i)}$. Then each S_f is a finite intersection of open and closed sets, hence an intersection of one closed set and one open set. Distributivity then gives $X \setminus S = \bigcap [(X \setminus U_i) \cup (X \setminus C_i)] = \bigcup_{f \in F} S_f \in \mathscr{G}$.

ii) Suppose that X is irreducible and let $E \in \mathscr{F}$. Show that E is dense in X (i.e., that $\overline{E} = X$) if and only if E contains a non-empty open set in X.

[12] I initially attempted a simpler argument as follows. Consider the projection $\pi \colon M \to M/P_k$. Since $\bigcap Q_j = N$, we have $\pi\big(\bigcap Q_j\big) = 0$. Since $P_k \subseteq M$ is irreducible, $0 \subseteq M/P_k$ is irreducible, and one of the $\pi(Q_j) = Q_j/P_k = 0$. This doesn't seem to work as stated, because there's no guarantee that $Q_j \supseteq P_k$, so that $\pi(Q_j)$ is a submodule.

If E contains a non-empty open set $U \subseteq X$, then $X = \overline{U} \subseteq \overline{E}$ by [1.19]. Now suppose $E = \bigcup (U_i \cap C_i) \in \mathscr{F}$ is dense in X. Recalling that closure distributes over finite unions,[13] we see $X = \overline{E} = \bigcup \overline{U_i \cap C_i}$. Recalling from [6.7] that an irreducible space is not a union of finitely many proper closed subspaces, for some i we have $\overline{U_i \cap C_i} = X$. Now $\overline{U_i \cap C_i} \subseteq \overline{U_i} \cap \overline{C_i}$ so $\overline{U_i} = X = \overline{C_i} = C_i$. Then E contains the open set $U_i = U_i \cap C_i$, which is non-empty since it is dense.

Let X be a Noetherian topological space (Chapter 6, Exercise 5) and let $E \subseteq X$. Show that $E \in \mathscr{F}$ if and only if, for each irreducible closed set $X_0 \subseteq X$, either $\overline{E \cap X_0} \neq X_0$ or else $E \cap X_0$ contains a non-empty open subset of X_0. The sets belonging to $\mathscr{F}$ are called the constructible *subsets of X.*

If $E \in \mathscr{F}$, then the previous [7.20] says that either $E \cap X_0$ contains a non-empty open set of X_0 or is not dense. But it is not dense precisely if its closure in X_0 is not all of X_0.

We prove the other direction by contraposition. Suppose $E \notin \mathscr{F}$. Then trivially $X \cap E \notin \mathscr{F}$, so the set of closed $C \subseteq X$ with $C \cap E \notin \mathscr{F}$ is non-empty. Since X is Noetherian, there are minimal such sets; let X_0 be one. If C, $C' \subsetneq X_0$ are closed, then by minimality, $C \cap E$ and $C' \cap E$ are in $\mathscr{F}$, so $\mathscr{F}$ also contains their union $(C \cup C') \cap E$. Apparently, then, we cannot have $C \cup C' = X_0$, showing X_0 is irreducible. We will show that $E \cap X_0$ is dense in X_0, yet contains no nonempty open subset of X_0.

Write F for the closure of $E \cap X_0$ in X_0. If F is a proper subset of X_0, then by minimality, $E \cap F \in \mathscr{F}$. Now $F = \overline{E} \cap X_0$,[14] so $E \cap X_0 = E \cap \overline{E} \cap X_0 = E \cap F \in \mathscr{F}$, contrary to assumption. Therefore $F = X_0$.

If $E \cap X_0$ contained a nonempty open subset U of X_0, then either $X_0 = U = E \cap X_0$, contradicting $E \cap X_0 \notin \mathscr{F}$, or $\varnothing \neq C \coloneqq X_0 \backslash U \subsetneq X_0$. By the definition of the subspace topology, C is closed in X and $U = V \cap X_0$ for some open $V \subseteq X$. Then $E \cap U = U = V \cap X_0 \in \mathscr{F}$, and by minimality of X_0 we have $C \cap E \in \mathscr{F}$. Since $U \cup C = X_0$, we then have $E \cap X_0 = (E \cap C) \cup (E \cap U)$ a union of elements of $\mathscr{F}$, hence in $\mathscr{F}$ itself, contrary to assumption. It follows that $E \cap X_0$ contains no nonempty open subset of X_0.

Let X be a Noetherian topological space and let E be a subset of X. Show that E is open in X if and only if, for each irreducible closed subset X_0 in X, either $E \cap X_0 = \varnothing$ or else $E \cap X_0$ contains a non-empty open subset of X_0.

Suppose first $E \subseteq X$ is open. Then for any subspace $X_0 \subseteq X$, by definition $E \cap X_0$ is an open subset of X_0; either it is empty, or it is not.

We prove the other direction by contraposition. Now suppose $E \subseteq X$ is not open; then $E \cap X$ is trivially not open, so the collection of closed subsets $C \subseteq X$ with $C \cap E$ not open in C is non-empty. As X is Noetherian, there are minimal elements of this collection; let X_0 be one. If C, $C' \subsetneq X_0$, then by minimality $C \cap E$ and $C' \cap E$ are open in X_0, so their union $(C \cup C') \cap E$ is open in X_0. It follows that $C \cup C' \neq X_0$, so X_0 is irreducible. We will show $E \cap X_0$ is non-empty, yet contains no non-empty open subset of X_0.

If $E \cap X_0$ were $\varnothing$, this intersection would be open, contrary to assumption, so the two sets do meet. Suppose for a contradiction that we can find a non-empty open subset $U \subseteq X_0 \cap E$ of X_0. Write $C = X_0 \backslash U$; since U is nonempty, $C \subsetneq X_0$, so by minimality of X_0 we have $C \cap E$ open in C. By the definition of the subspace topology, then, there is an open $V \subseteq X$ with $C \cap E = V \cap X_0$. Then $X_0 \cap E = (U \cap E) \cup (C \cap E) = U \cup (V \cap X_0)$ is a union of open subsets of X_0, hence open in X_0, contrary to assumption.

Let A be a Noetherian ring, $f \colon A \to B$ a ring homomorphism of finite type (so that B is Noetherian). Let $X = \operatorname{Spec}(A)$, $Y = \operatorname{Spec}(B)$ and let $f^* \colon Y \to X$ be the mapping associated with f. Then the image under f^* of a constructible subset E of Y is a constructible subset of X.

To see B is Noetherian, recall from p. 30 that being of finite type means that B is finitely generated as an A-algebra, hence a quotient of a polynomial ring over A. Then (7.5) and (7.1) show B is Noetherian.

Since $f^*\big(\bigcup S_i\big) = \bigcup f^*(S_i)$, it will suffice to consider E of the form $U \cap C$ for $U \subseteq Y$ open and $C \subseteq Y$ closed. An open subset $U \subseteq Y$ is a union of basic open sets Y_g for $g \in B$ ([1.17]). By [6.6], U is compact, so it is a union of finitely many Y_{g_i}. Then $U \cap C = \bigcup (Y_{g_i} \cap C)$, so it will suffice to verify the statement for $E = Y_g \cap C$. Since a closed subset $C \subseteq Y$ is $V(\mathfrak{b})$ for some ideal $\mathfrak{b} \lhd B$ ([1.15]), we may assume $E = Y_g \cap V(\mathfrak{b})$.

Now by [1.21.iv], $V(\mathfrak{b}) \approx \operatorname{Spec}(B/\mathfrak{b})$. Writing $\pi \colon B \twoheadrightarrow B/\mathfrak{b}$ and $\operatorname{Spec}(B/\mathfrak{b}) = \mathrm{Z}$, [1.21.i] says for $\mathfrak{q} \in V(\mathfrak{b})$ we have $\mathfrak{q} = \pi^*(\mathfrak{q}/\mathfrak{b}) \in Y_g \iff \pi(\mathfrak{q}) = \mathfrak{q}/\mathfrak{b} \in (\pi^*)^{-1}(Y_g) = \mathrm{Z}_{\pi(g)}$, so $E = V(\mathfrak{b}) \cap Y_g = \pi^*(\mathrm{Z}_{\pi(g)})$. Replacing $f \colon A \to B$

[13] $A \subseteq A \cup B$, so $\overline{A} \subseteq \overline{A \cup B}$, and similarly $\overline{B} \subseteq \overline{A \cup B}$, so $\overline{A} \cup \overline{B} \subseteq \overline{A \cup B}$. On the other hand, $A \cup B \subseteq \overline{A} \cup \overline{B}$, and the latter is closed, so $\overline{A \cup B} \subseteq \overline{A} \cup \overline{B}$.

[14] In general, if $A \subseteq Y \subseteq X$, the closure B of A in Y is equal to $\overline{A} \cap Y$. On the one hand, the latter is closed in Y and contains A, so $B \subseteq \overline{A} \cap Y$. On the other hand, if $x \in \overline{A} \cap Y$, then $x \in Y$ and every neighborhood $U \ni x$ contains some point of $A \subseteq Y$, so every neighborhood $U \cap Y \subseteq Y$ of x meets A, and thus $x \in B$.

by $A \to B \twoheadrightarrow B/\mathfrak{b}$, B by $B/\mathfrak{b}$, and Y_g by $Z_{\pi(g)}$, and noting $B/\mathfrak{b}$ is also of finite type over A, we may assume that $E \subseteq B$ is a basic open set.

If $\phi_g \colon B \to B_g$ is the canonical map, then $E = Y_g = \phi_g^*\big(\operatorname{Spec}(B_g)\big)$. Since we have a B-algebra surjection $B[t] \twoheadrightarrow B_g$ taking $t \mapsto 1/g$, it follows B_g is of finite type over A, and we may replace B by B_g, f by $\phi_g \circ f$, and E by $\operatorname{Spec}(B_g)$. Now we have only to show that given a map $f \colon A \to B$ of finite type, with A Noetherian, $f^*(Y)$ is constructible.[15]

We will attempt to use [7.21]. Let an irreducible closed set $X_0 \subseteq X$ be given. By the proof of [1.20.iv], X_0 is of the form $V(\mathfrak{p})$ for some prime $\mathfrak{p} \in X$.[16] Write $F = f^*(Y) \cap X_0$ for the set we want to prove constructible. We have $\mathfrak{p}' \in f^*(Y) \cap X_0$ if and only if there is $\mathfrak{q}' \in Y \cap (f^*)^{-1}(X_0) = (f^*)^{-1}(X_0)$ such that $\mathfrak{p}' = f^*(\mathfrak{q}')$; then $\mathfrak{p}' \in f^*\big((f^*)^{-1}(X_0)\big)$. Thus $F = f^*\big((f^*)^{-1}(X_0)\big)$. By [1.21.ii], $(f^*)^{-1}\big(V(\mathfrak{p})\big) = V(\mathfrak{p}B)$ is the pre-image of F and by [3.21.iii], f^* "restricts" to a map (which we call f^* again) $\operatorname{Spec}(B/\mathfrak{p}B) \to \operatorname{Spec}(A/\mathfrak{p})$, whose image we want to show is constructible; the rings are still Noetherian, with the map still of finite type. So we may assume A is a Noetherian integral domain and $f \colon A \to B$ is of finite type, and we want to show $f^*(Y)$ is constructible. Since B is then Noetherian, Y is a Noetherian space, so by [6.7], it is a union of finitely many irreducible components $Y_1, \ldots, Y_n$. Now by [7.21], it is enough to show either $f^*(Y)$ is not dense or contains a non-empty open set. If $f^*(Y)$ is dense, then $X = \overline{f^*(Y)} = \bigcup \overline{f^*(Y_j)}$, so by irreducibility of X, we have some $f^*(Y_j)$ dense[17]; we want to show this $f^*(Y_j)$ contains a non-empty open set. Write $Y_j = V(\mathfrak{q})$ for a prime ideal $\mathfrak{q} \lhd B$ ([1.20.iv]); then $f^*(Y_j)$ is the image of the map on spectra induced by the composition $A \to B \twoheadrightarrow B/\mathfrak{q}$. Replacing B with $B/\mathfrak{q}$ and f with this composition, we may assume A and B are Noetherian integral domains. Since $f^*(Y)$ is dense in X, by [1.21.v], we must have $\ker(f) \subseteq \mathfrak{N}(A) = 0$, so f is injective. Now we are in the situation of [5.21]. There exists a nonzero $s \in A$ such that given an algebraically closed field Ω and homomorphism $\phi \colon A \to \Omega$ such that $\phi(s) \neq 0$, we can extend ϕ to a homomorphism $B \to \Omega$. Since the images of these maps are subrings of a field, hence integral domains, it follows that their kernels $\mathfrak{p}$, $\mathfrak{q}$ are prime, with $\mathfrak{p} = A \cap \mathfrak{q} = f^*(\mathfrak{q})$. We have $\phi(s) \neq 0 \iff s \notin \ker(\phi) = \mathfrak{p}$, so for all $\mathfrak{p} \in X_s$ we have $\mathfrak{p} \in f^*(Y)$, so that $X_s \subseteq f^*(Y)$ is an open subset. But since A is an integral domain, s is not nilpotent, and thus by [1.17.ii], $X_s \neq \varnothing$.

The previous solution followed the book's breadcrumb trail; the following one is adapted from another solution set online.[18] We want to prove $f^*(Y)$ is constructible, assuming only that f is of finite type and A Noetherian. Given

[15] This following paragraph is an approach I once thought would work, but does not. I include it because I spent a good deal of time on it and its failure, at least to me, seemed somewhat subtle.

Since f is of finite type, it can be factored as $\pi \circ \iota$, where $\iota \colon A \hookrightarrow A[x_1, \ldots, x_n]$ is the canonical inclusion into a polynomial ring and $\pi \colon A[x_1, \ldots, x_n] \twoheadrightarrow B$ is a quotient map. Now $f^*(Y) = \iota^*\big(\pi^*(Y)\big)$, where $\pi^*(Y) = V\big(\ker(\pi)\big)$ by [1.21.iv]. If we vary B and f, this set varies over all closed subsets of $\operatorname{Spec}(A[x_1, \ldots, x_n])$; thus we may assume $f \colon A \hookrightarrow B = A[x_1, \ldots, x_n]$ and $E = V(\mathfrak{b})$ for some $\mathfrak{b} \lhd B$.

By [1.21.iii], we have $\overline{f^*(E)} = V(\mathfrak{b}^c)$, so certainly $f^*(E) \subseteq V(\mathfrak{b}^c)$. It would be nice if we could prove the reverse inclusion. (If that were so, however, it would follow that $\operatorname{Spec}(A[x_1, \ldots, x_n]) \to \operatorname{Spec}(A)$ is always a closed map, which we show below is not the case. By [6.11], this is equivalent to f having the going-up property, which we also show is not so in general.) To attempt this, let $\mathfrak{p} \in V(\mathfrak{b}^c)$ be given; we wish to find a prime $\mathfrak{q} \in V(\mathfrak{b})$ such that $A \cap \mathfrak{q} = \mathfrak{p}$. By [3.21.iii], f^* "restricts" to a map $\operatorname{Spec}(B/\mathfrak{p}^e) \to \operatorname{Spec}(A/\mathfrak{p})$ that we will also call f^*. Since $\mathfrak{p}^e = \mathfrak{p}[x_1, \ldots, x_n]$, the domain of the new f^* is the integral domain $(A/\mathfrak{p})[x_1, \ldots, x_n]$; what we now need is a prime $\mathfrak{q}$ of $(A/\mathfrak{p})[x_1, \ldots, x_n]$ containing the extension

$$\mathfrak{c} := \mathfrak{b}^e \lhd (A/\mathfrak{p})[x_1, \ldots, x_n]. \tag{7.1}$$

Replacing A with $A/\mathfrak{p}$ and $\mathfrak{b}$ with $\mathfrak{c}$, we may assume A is a Noetherian integral domain, $\mathfrak{b}$ is an ideal of $B = A[x_1, \ldots, x_n]$ such that $A \cap \mathfrak{b} = 0$, and we need a prime $\mathfrak{q} \in V(\mathfrak{b})$ such that $A \cap \mathfrak{q} = 0$. Write $S = A \backslash \{0\}$ and $K = S^{-1}A$ for the field of fractions of A. Then $S^{-1}B = K[x_1, \ldots, x_n]$, and [3.21.ii] gives a commutative diagram

$$\begin{tikzcd}
\{(0)\} = \operatorname{Spec}(K) \arrow[d, tail] & \operatorname{Spec}\big(K[x_1, \ldots, x_n]\big) \arrow[l, two heads] \arrow[d, tail] \\
\operatorname{Spec}(A) & \operatorname{Spec}\big(A[x_1, \ldots, x_n]\big). \arrow[l, two heads]
\end{tikzcd}$$

In $K[x_1, \ldots, x_n]$ there is certainly a maximal ideal $\mathfrak{n}$ containing the extension $S^{-1}\mathfrak{b} = \mathfrak{b}^e$, since $\mathfrak{b} \cap S = \varnothing$ implies, by (3.11.ii), that $S^{-1}\mathfrak{b} \neq (1)$. Then using (1.17.i), $\mathfrak{b} \subseteq \mathfrak{b}^{ec} \subseteq \mathfrak{n}^c =: \mathfrak{q}$, and following $\mathfrak{n}$ both ways around the diagram, we see $\mathfrak{q} \cap A = \mathfrak{n} \cap A = (0)$.

Now we have a "proof" that never requires the Noetherian hypothesis on A (or the finite type, either, seemingly). The argument breaks down at Eq. 7.1; it can easily happen that $\mathfrak{b}^e = \mathfrak{p}$, so there is no prime containing it. For an example, consider $A = \mathbb{Z}_{(p)}$ and the ideal $\mathfrak{q} = (px - 1)$ in $\mathbb{Z}_{(p)}[x]$ (http://bit.ly/S9wGoP). Then $\mathbb{Z}_{(p)}[x]/\mathfrak{q} \cong \mathbb{Z}_{(p)}[1/p] \cong \mathbb{Q}$, so $\mathfrak{q}$ is maximal, and hence $\{\mathfrak{q}\} \subsetneq \operatorname{Spec}\big(\mathbb{Z}_{(p)}[x]\big)$ is closed by [1.18.i]. But $\mathfrak{q} \cap \mathbb{Z}_{(p)} = (0)$, and $\{(0)\}$ is not closed in $\operatorname{Spec}\big(\mathbb{Z}_{(p)}\big)$, since its closure is $V\big((0)\big) = \{(0), (p)\}$ ([1.8.ii]). Also, the extension ($\mathfrak{c}$ above) of $\mathfrak{q}$ in $\mathbb{Z}_{(p)}/(p)\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$ is $(-1) = (1)$, so no prime contains it.

[16] The next thing I wanted to do is as follows. I leave it to posterity to rescue it, if possible. Eq. 1.1, (1.18), and (1.8) give $\overline{f^*(Y)} = V\big(\bigcap f^*(Y)\big) = V\Big(f\big(\bigcap Y\big)\Big) = V\big(\mathfrak{N}(B)^c\big)$. Then the closure of $f^*(Y) \cap V(\mathfrak{p})$ in $V(\mathfrak{p})$ is $\overline{f^*(Y)} \cap V(\mathfrak{p}) = V\big(\mathfrak{N}(B)^c\big) \cap V(\mathfrak{p})$ by the footnote to [7.21]. If it equals $V(\mathfrak{p})$; then each prime $\mathfrak{p}' \lhd A$ containing $\mathfrak{p}$ also contains $\mathfrak{N}(B)^c$; in particular, $\mathfrak{p}$ contains $\mathfrak{N}(B)^c$. This should hypothetically help us find a basic open subset X_h contained in $f^*(Y) \cap V(\mathfrak{p})$, but I do not know how.

[17] This line from Yimu Yin's solution: http://pitt.edu/~yimuyin/research/AandM/exercises07.pdf

[18] http://pitt.edu/~yimuyin/research/AandM/exercises07.pdf

that Y is Noetherian, and by [6.7] a union of finitely many irreducible components Y_1, it will be enough to show each $f^*(Y_1)$ is constructible. Let $\mathfrak{q}_1$ be a minimal prime of B such that $V(\mathfrak{q}_1) = Y_1$ ([1.20.iv]); then the image $F = f^*(Y_1)$ is contained in $V(\mathfrak{q}^c)$ by [1.21.iii], so f^* restricts to a map ([3.21.iii]) $B_1 = \operatorname{Spec}(B/\mathfrak{q}_1) \to \operatorname{Spec}(A/\mathfrak{q}_1^c) = A_1$. If $f^*(Y_1)$ is constructible in $X_1 = \operatorname{Spec}(A/\mathfrak{q}_1^c)$, it will also be in X: if $f^*(Y)$ is a union of sets $U' \cap C'$ for U' open and C' closed in X_1, then there are U open and C closed in X such that $U' = X_1 \cap U$ and $C' = X_1 \cap C$, and then $U' \cap C' = U \cap (C \cap X_1)$. Note that A_1 and B_1 are integral domains and $f_1 \colon A_1 \to B_1$ is injective. As in the previous proof, by [5.21] there is $s_1 \in A_1$ such that $s_1 \notin \mathfrak{p}_1 \in X_1$ implies $\mathfrak{p}_1 \in f_1^*(Y_1)$; thus $X_{s_1} \subseteq f_1^*(Y_1) = F$. Now s_1 is in each prime in $V(s_1) = X_1 \backslash X_{s_1}$, so we may consider ([3.21.iii] again) the restriction of f_1^* to the map $(f_1^*)^{-1}\big(V(s_1B)\big) \to V(s_1)$ as induced by the homomorphism $A_1' = A_1/(s_1) \to B_1/(s_1)B_1 = B_1'$. By [6.5], Y_1 is Noetherian, so by [6.7], it has finitely many irreducible components. Let Y_2 be one, and $\mathfrak{q}_2$ such that ([1.20.iv]) $V(\mathfrak{q}_2) = Y_2$. The image $(f_1')^*(Y_2)$ induced by $f_1' \colon A_1' \to B_1'$ is the same as (making identifications) the image $f_2^*(Y_2)$ induced by $f_2 \colon A_1'/\mathfrak{q}_2^c \to B_1'/\mathfrak{q}$. Again this is an injection of integral domains, so we can find an open subset $X_{s_2} \subseteq X_2$ contained in $f_2^*(Y_2)$. Iterating, we get a sequence of sets $X_{s_j} \subseteq F$, where each $X_{s_{j+1}}$ is open in the closed set $X_j \backslash X_{s_j}$. That means that there is an open $U_{j+1} \subseteq X_j$ such that $U_{j+1} \cap (X_j \backslash X_{s_j}) = X_{s_{j+1}}$. Thus $X_{s_{j+1}} \cup X_{s_j} = U_j \cup X_{s_j}$ is open in X_j. Therefore $W_n = \bigcup_{j=1}^n X_{s_j}$ is an increasing chain of open sets in F; since X is Noetherian, so is F by [2.5], so this chain terminates in some W_n.

At each point where we chose an irreducible component in the above process, we could have instead chosen a different irreducible component, and obtained a different open subset $W \subseteq F$. If we do this for each possible chain of irreducible components, and take the union, we have obtained F as an open set, which is certainly constructible.

With the notation and hypotheses of Exercise 23, f^* is an open mapping $\iff$ f has the going-down-property (Chapter 5, Exercise 10).

By [5.10.ii], if $f \colon A \to B$ is any ring homomorphism such that f^* is open, then f has the going-down property.

Conversely, suppose f has the going-down property, and let Y_s be a basic open set ([1.17]) in $Y = \operatorname{Spec}(B)$; it is enough to show $f^*(Y_s)$ is open. By (3.11.iv), the canonical map $B \to B_s$ has the going-down property, and $A \to B \to B_s$ is still of finite type, so replacing B with B_s and f with the composition, it is enough to show $f^*(Y)$ is open. Let X_0 be an arbitrary irreducible closed subset of X. By [7.22], to show $f^*(Y)$ is open it will suffice to show that either it does not meet X_0 or $F = f^*(Y) \cap X_0$ contains a non-empty open subset of X_0. Assume that $\mathfrak{q} \in F$. Then if $\mathfrak{p}' \subseteq \mathfrak{q}$ is another prime, we also have $\mathfrak{p}' \in f^*(Y)$, by going-down. But [1.20.iv] tells us there is a prime $\mathfrak{p}$ such that $X_0 = V(\mathfrak{p})$, and thus $\mathfrak{p} \in F$. Since $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}) = X_0$ ([1.18.ii]), we then have F dense in X_0. By the previous problem, $f^*(Y)$ is constructible, and so F is as well. [7.20.ii] then says that F contains a non-empty open set in X_0.

Let A be Noetherian, $f \colon A \to B$ of finite type and flat *(i.e., B is flat as an A-module). Then $f^* \colon \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ is an open mapping.*

By [5.11], since f is flat, it has the going-down property. By [7.24], then, f^* is an open mapping.

Grothendieck groups

Let A be a Noetherian ring and let $F(A)$ denote the set of all isomorphism classes of finitely generated A-modules. Let C be the free abelian group generated by $F(A)$. With each short exact sequence $0 \to M' \to M \to M'' \to 0$ of finitely generated A-modules we associate the element $[M'] - [M] + [M'']$ of C, where $[M]$ is the isomorphism class of M, etc. Let D be the subgroup of C generated by these elements, for all short exact sequences. The quotient group C/D is called the Grothendieck group *of A, and is denoted by $K(A)$. If M is a finitely generated A-module, let $\gamma(M)$, or $\gamma_A(M)$, denote the image of $[M]$ in $K(A)$.*

Before proceeding, we establish some additional notation. Let $\mathscr{F}(A)$ be the class of all finitely generated A-modules, $[-]_A \colon \mathscr{F}(A) \twoheadrightarrow F(A)$ the function taking a module to its isomorphism class, $i_A \colon F(A) \hookrightarrow C(A)$ the canonical inclusion of generators, and $\pi_A \colon C(A) \twoheadrightarrow K(A) = C(A)/D(A)$ the quotient map. Note that $\gamma_A = \pi_A \circ i_A \circ [-]_A$.

Since only one ring occurs in the discussion up to part iv), we will until then mostly suppress mention of A.[19]

[19] As an aside, note, although it's not strictly necessary for us to do so, that if $0 \to N \to M \to P \to 0$ is a short exact sequence of A-modules and N and P are finitely generated, then so is M, by [2.9]. It's also true that if M is finitely generated, then it is Noetherian by (6.5), so N and P are finitely generated. Again, generators of D are defined to be linear combinations of *finitely generated* classes, but these closure properties are somehow reassuring.

Show that $K(A)$ has the following universal property: for each additive function λ on the (proper) class of finitely generated A-modules, with values in an abelian group G, there exists a unique homomorphism $\lambda_0\colon K(A) \to G$ such that $\lambda(M) = \lambda_0\big(\gamma(M)\big)$ for all M.

Since for any short exact sequence $0 \to N \to M \to P \to 0$ of finitely generated A-modules we have $[N]-[M]+[P] \in D = \ker(\pi)$, its image under π is $0 = \pi\big([N]\big) - \pi\big([M]\big) + \pi\big([P]\big) = \gamma(N) - \gamma(M) + \gamma(P)$, so $\gamma\colon \mathscr{F} \to K$ is itself an additive function (p. 23). We will show a little more than the claim: not only is it the case that for each additive function $\lambda\colon \mathscr{F} \to G$ is there a unique homomorphism $\lambda_0\colon K \to G$ such that $\lambda = \lambda_0 \circ \gamma$, but to each homomorphism $\lambda_0\colon K \to G$ corresponds a unique additive function $\lambda = \lambda_0 \circ \gamma\colon \mathscr{F} \to G$, so the correspondence $\lambda \longleftrightarrow \lambda_0$ is bijective. In other words, γ is a *universal* additive function on $\mathscr{F}$.

For the correspondence $\lambda_0 \mapsto \lambda$, recall that γ is additive, so for any short exact sequence $0 \to N \to M \to P \to 0$ of finitely generated A-modules we have $\gamma(N) - \gamma(M) + \gamma(P) = 0$. It follows that for any homomorphism $\lambda_0\colon K \to G$, if we define $\lambda = \lambda_0 \circ \gamma$, then $\lambda(N) - \lambda(M) + \lambda(P) = \lambda_0\big(\gamma(N) - \gamma(M) + \gamma(P)\big) = \lambda_0(0) = 0$, so that λ is additive.

For the correspondence $\lambda \mapsto \lambda_0$, given an additive map $\mathscr{F} \to G$, we find a homomorphism $\lambda_0\colon K \to G$ such that $\lambda_0 \circ \gamma = \lambda$, then show it is unique. First, to see λ descends (uniquely) to a well defined function on F, consider the very boring short exact sequence $0 \to 0 \to 0 \to 0 \to 0$. By additivity, $\lambda(0) = \lambda(0) - \lambda(0) + \lambda(0) = 0$. If $M \cong N \in \mathscr{F}$, then there exists a short exact sequence $0 \to M \to N \to 0 \to 0$, so by additivity, $\lambda(M) - \lambda(N) = \lambda(M) - \lambda(N) + \lambda(0) = 0$, and $\lambda(M) = \lambda(N)$. Thus $\lambda(M)$ depends only on the isomorphism class of M and λ descends to a well defined function $\lambda_F\colon F \to G$ with $\lambda_F \circ [-] = \lambda$. Second, as C is the free abelian group on F, we have a unique homomorphism $\lambda_C\colon C \to G$ such that $\lambda_C \circ i = \lambda_F$. Third, given any short exact sequence $0 \to N \to M \to P \to 0$, we have $\lambda_C\big([N]-[M]+[P]\big) = \lambda_C\big([N]\big) - \lambda_C\big([M]\big) + \lambda_C\big([P]\big) = \lambda(N) - \lambda(M) + \lambda(P) = 0$, so $D \subseteq \ker(\lambda_C)$ and λ_C descends to a homomorphism $\lambda_0\colon K = C/D \to G$, with $\lambda_0 \circ \pi = \lambda_C$. As requested, $\lambda_0 \circ \gamma = \lambda_0 \circ \pi \circ i \circ [-] = \lambda_C \circ i \circ [-] = \lambda_F \circ [-] = \lambda$.

$$\begin{tikzcd}
\mathscr{F}(A) \arrow[d, "{[-]}"] \arrow[ddd, bend right, "\gamma"'] \arrow[dddr, bend left, "\lambda"] & \\
F(A) \arrow[d, hook, "i"] \arrow[ddr, dotted, "\lambda_F"] & \\
C(A) \arrow[d, "\pi"] \arrow[dr, dotted, "\lambda_C"] & \\
K(A) \arrow[r, dotted, "\lambda_0"'] & G
\end{tikzcd}$$

To see uniqueness, note that the $[M] \in C$ for $M \in \mathscr{F}$ are generators for C, so their images $\gamma(M) = \pi\big([M]\big)$ generate $K = C/D$. Thus if a partially defined function $l_0\colon K \to G$ satisfies $l_0\big(\gamma(M)\big) = \lambda(M)$, there is at most one way to extend l_0 to a totally defined homomorphism $\lambda_0\colon K \to G$.

Show that $K(A)$ is generated by the elements $\gamma(A/\mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal of A.

Let $M \in \mathscr{F}$, and recall from [7.18] (this is the first time we use that A is Noetherian) that there exists a chain $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$ of submodules with successive quotients of the form $A/\mathfrak{p}_j$ for $\mathfrak{p}_j \in \operatorname{Spec}(A)$. Thus we have for $1 \leq j \leq r$ short exact sequences $0 \to M_{j-1} \to M_j \to A/\mathfrak{p}_j \to 0$, showing that $[M_{j-1}] - [M_j] + [A/\mathfrak{p}_j] \in D$, and so $\gamma(M_j) = \gamma(M_{j-1}) + \gamma(A/\mathfrak{p}_j)$. Since $\gamma(M_0) = \gamma(0) = 0$, it follows by induction that $\gamma(M_n) = \sum_{j \leq n} \gamma(A/\mathfrak{p}_j)$; in particular, $\gamma(M) = \sum_{j=1}^{r} \gamma(A/\mathfrak{p}_j)$.

If A is a field, or more generally if A is a principal ideal domain, then $K(A) \cong \mathbb{Z}$.

First note that a field is a principal ideal domain (henceforth "PID"), with only the two ideals (0) and (1). Second, note that a principal ideal domain A is Noetherian by (6.2), since every ideal is by definition principal, so a fortiori finitely generated. By ii) above K is then generated by the elements $\gamma(A/\mathfrak{p})$ with $\mathfrak{p} \in \operatorname{Spec}(A)$. Let $(a) \neq (0)$ be any ideal of A; since A is an integral domain, $x \mapsto ax$ is injective, so we have a short exact sequence $0 \to A \to A \to A/(a) \to 0$ of A-modules, meaning $\gamma\big(A/(a)\big) = \gamma(A) - \gamma(A) + \gamma\big(A/(a)\big) = 0$ in K. Since A is an integral domain, (0) is prime, and so $\gamma\big(A/(0)\big) = \gamma(A)$ generates K. Thus K is a quotient of $\mathbb{Z}$, and it remains to show it isn't a proper quotient. To do this, it suffices to define a surjective homomorphism $K \twoheadrightarrow \mathbb{Z}$, and by i), it is enough to produce an additive function $\mathscr{F} \to \mathbb{Z}$ with image $\mathbb{N}$.[20]

Recall[21] that any finitely generated module M over a PID A can be written as a finite direct sum $A^r \oplus T(M)$ for some uniquely determined *rank* $r = \operatorname{rk}_A M \in \mathbb{N}$, where $T(M)$ is the torsion submodule of M ([2.12]). $\lambda := \operatorname{rk}_A$ has image $\mathbb{N}$ since $\lambda(A^n) = n$ for all $n \in \mathbb{N}$. Write L for the field of fractions of A. For any nonzero $m \in T(M)$, say with $a \in \operatorname{Ann}(m) \backslash \{0\}$, we have $1 \otimes m = (a/a) \otimes m = (1/a) \otimes am = (1/a) \otimes 0 = 0$ in $L \otimes M$, so $L \otimes M \cong L \otimes A^{\lambda(M)} \cong L^{\lambda(M)}$ by (2.14.iii,iv). Since by (3.6) L is a flat A-module, tensoring a short exact sequence $0 \to N \to M \to P \to 0$ of finitely generated A-modules with L gives rise to a short exact sequence $0 \to L^{\lambda(N)} \to L^{\lambda(M)} \to L^{\lambda(P)} \to 0$ of L-vector spaces. We know from linear algebra that $\lambda(N) - \lambda(M) + \lambda(P) = 0$, so λ is additive.

[20] I am not pleased with this proof; it seems intuitively obvious $\gamma(A)$ is not torsion, so I think there should be a quicker argument.

[21] http://planetmath.org/encyclopedia/FinitelyGeneratedModulesOverAPrincipalIdealDomain.html

Let $f\colon A \to B$ be a finite *ring homomorphism. Show that restriction of scalars gives rise to a homomorphism $f_!\colon K(B) \to K(A)$ such that $f_!\big(\gamma_B(N)\big) = \gamma_A(N)$ for a B-module N. If $g\colon B \to C$ is another finite ring homomorphism, show that $(g \circ f)_! = f_! \circ g_!$.*

If N is a finitely generated B-module, write $N|_f$ for the A-module obtained therefrom by restriction of scalars. (2.16) says that then $N|_f$ is a finitely generated A-module, so we have a function $|_f\colon \mathscr{F}(B) \to \mathscr{F}(A)$. An short exact sequence $0 \to N \to M \to P \to 0$ of B-modules remains exact viewed as a sequence of A-modules, so $\gamma_A \circ |_f$ is an additive map $\mathscr{F}(B) \to K(A)$. By the universal property of i), there is then a unique homomorphism $f_!\colon K(B) \to K(A)$ such that $f_! \circ \gamma_B = \gamma_A \circ |_f$.

Let M be a C-module, $a \in A$, and $x \in M$. Note that $M|_g$, $\big(M|_g\big)\big|_f$, and $M|_{g\circ f}$ have the same underlying abelian group, so the last two will be equal A-modules if they have the same A-action. The element $a \cdot x$ of $\big(M|_g\big)\big|_f$, by definition, is the element $f(a)\cdot x$ in $M|_g$, which in turn is $g\big(f(a)\big)\cdot x = (g \circ f)(a)\cdot x$ in M, which is $a \cdot x$ in $M|_{g\circ f}$. Thus $\big(M|_g\big)\big|_f = M|_{g\circ f}$. Abstracting, we can write $|_{g\circ f} = |_g \circ |_f \colon \mathscr{F}(C) \to \mathscr{F}(A)$. Now consider the diagram

$$\begin{tikzcd}
\mathscr{F}(A) \arrow[d, "\gamma_A"] & \mathscr{F}(B) \arrow[l, "|_f"'] \arrow[d, "\gamma_B"] & \mathscr{F}(C) \arrow[l, "|_g"'] \arrow[d, "\gamma_C"] \\
K(A) & K(B) \arrow[l, "f_!"'] & K(C). \arrow[l, "g_!"']
\end{tikzcd}$$

Commutativity of the two squares implies commutativity of the outer rectangle: $f_! \circ g_! \circ \gamma_C = f_! \circ \gamma_B \circ |_g = \gamma_A \circ |_f \circ |_g = \gamma_A \circ |_{g\circ f}$. Then $f_! \circ g_!$ is a homomorphism $\phi\colon K(C) \to K(A)$ satisfying $\phi \circ \gamma_C = \gamma_A \circ |_{g\circ f}$. As $(g \circ f)_!$ was defined to be the unique homomorphism with this property, it follows that $(g \circ f)_! = f_! \circ g_!$.

Let A be a Noetherian ring and let $F_1(A)$ be the set of all isomorphism classes of finitely generated flat *A-modules. Repeating the construction of Exercise 26 we obtain a group $K_1(A)$. Let $\gamma_1(M)$ denote the image of $[M]$ in $K_1(A)$.*

Two asides follow.[22][23]

Show that tensor product of modules over A induces a commutative ring structure on $K_1(A)$, such that $\gamma_1(M)\cdot\gamma_1(N) = \gamma_1(M \otimes N)$. The identity element of this ring is $\gamma_1(A)$.

First recall the notation we introduced in the proof of [7.26]. Let $\mathscr{F}_1 \subseteq \mathscr{F}$ be the class of all finitely generated flat A-modules. Note $F_1 \subseteq F$, so the map $[-]\colon \mathscr{F} \twoheadrightarrow F$ restricts to a map $\mathscr{F}_1 \twoheadrightarrow F_1$. Let C_1 be the free group on F_1. Since $F_1 \subseteq F$, there is a natural embedding $C_1 \rightarrowtail C$, which we view as an inclusion. Write $D_1 \subseteq C_1$ for the subgroup generated by $[N]-[M]+[P]$ for short exact sequences $0 \to N \to M \to P \to 0$ of objects in $\mathscr{F}_1$, and $\pi_1\colon C_1 \twoheadrightarrow K_1 = C_1/D_1$ for the quotient map.

A tensor product of finitely generated modules is finitely generated for if M, N are generated by some finitely many $x_i \in M$ and $y_j \in N$, then $M \otimes_A N$ is generated by the finitely many $x_i \otimes y_j$. Thus $-\otimes-$ is a map $\mathscr{F} \times \mathscr{F} \to \mathscr{F}$. By [2.8.i], a tensor product of flat modules is flat, so $-\otimes-$ restricts to a map $\mathscr{F}_1 \times \mathscr{F}_1 \to \mathscr{F}_1$. Given isomorphisms $\phi\colon M \xrightarrow{\sim} M'$ and $\psi\colon N \xrightarrow{\sim} N'$, we have an isomorphism $\phi \otimes \psi\colon M \otimes N \xrightarrow{\sim} M' \otimes N'$ (see p. 27), so tensor descends to a function $t\colon F \times F \to F$ taking $\big([M],[N]\big) \mapsto [M \otimes N]$, which in turn restricts to a function $t_1\colon F_1 \times F_1 \to F_1$. By (2.14.i,ii,iv), t and t_1 are commutative, associative binary operations on F, F_1 with identity element $[A]$, and so make F a monoid with submonoid F_1. Writing $\mathbb{Z}[F]$ and $\mathbb{Z}[F_1]$ for the monoid rings ([5.33]), the bijections $C \longleftrightarrow \mathbb{Z}[F]$ and $C_1 \longleftrightarrow \mathbb{Z}[F_1]$ (hereafter taken as identifications) define ring structures on these groups; write τ and τ_1 for the multiplications.

If $M \in \mathscr{F}_1$ and $0 \to N' \to N \to N'' \to 0$ is a a short exact sequence of A-modules, then by flatness of M this induces a short exact sequence $0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$, so $\tau_1\big([M], [N']-[N]+[N'']\big) = [M \otimes N'] - [M \otimes N] + [N \otimes N''] \in D_1$ for any generator $[N']-[N]+[N'']$ of D_1, showing D_1 is an ideal, and thus giving a ring structure on $K_1 = C_1/D_1$.[24] Now $\gamma_1(M)\cdot\gamma_1(N) = (\pi_1 \circ \tau_1)(M, N) = \pi_1\big([M \otimes N]\big) = \gamma_1(M \otimes N)$. Since

[22] If $0 \to N \to M \to P \to 0$ is an exact sequence of finitely generated A-modules and N and P are flat, so is M by [2.25]. This isn't strictly necessary for the definition, which only requires those sequences *such that* all terms are flat, but it's somehow comforting anyway.

[23] It is tempting, in order to do i) and ii), to consider K_1 as a subset of K and argue the desired multiplication on K_1 is a restriction of the map $\mu\colon K_1 \times K \to K$ making K a K_1-module. In general, it is not; the map $\epsilon\colon K_1 \to K$ defined in the remark by $\epsilon\big(\gamma_1(M)\big) = \gamma(M)$ is not in general injective. The problem is that, while $C_1 \subseteq C$ naturally, we don't necessarily have $D_1 = C_1 \cap D$. Indeed, D_1 is generated by $[N]-[M]+[P]$ for short exact sequences $0 \to N \to M \to P \to 0$ of objects in $\mathscr{F}_1$, but it is entirely possible that there are elements of $C_1 \cap D$ not generated by these sequences.

[24] It's worth noting that K generally fails to be a ring precisely because D is not generally an ideal, which is in turn the case because modules are not flat in general.

$[A]$ is the neutral element of F_1 (which shows A is flat, hence in $\mathscr{F}_1$), it becomes a unity in the monoid ring C_1, and its image $\gamma_1(A) \in K_1$ is the unity of K_1.

Show that tensor product induces a $K_1(A)$-module structure on the group $K(A)$, such that $\gamma_1(M) \cdot \gamma(N) = \gamma(M \otimes N)$.

Note that the (restricted) multiplication $\tau\colon C_1 \times C \to C$ makes the group C a C_1-module. A slight modification of the proof in the preceding paragraph that $D_1 \lhd C_1$ is an ideal, assuming $N', N, N'' \in \mathscr{F}$ and not necessarily in $\mathscr{F}_1$, shows that $\tau(C_1 \times D) \subseteq D$, so $K = C/D$ is naturally a C_1-module. If $D_1 \subseteq \operatorname{Ann}_{C_1}(K)$, then (p. 19) we may naturally regard K as a K_1-module. Indeed, for any $N \in \mathscr{F}$ and short exact sequence $0 \to M' \to M \to M'' \to 0$ in $\mathscr{F}_1$ we have a Tor exact sequence ([2.24]) $\operatorname{Tor}_1(M'', N) \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$, and $\operatorname{Tor}_1(M'', N) = 0$ by flatness of M'' ([2.24]), so $\tau\big([M'] - [M] + [M''], [N]\big) \in D$; since these $[M'] - [M] + [M'']$ are generators for D_1, it follows $D_1 \cdot K = 0$. Now $\gamma_1(M) \cdot \gamma(N) = (\pi \circ \tau)(M, N) = \pi\big([M \otimes N]\big) = \gamma(M \otimes N)$.

If A is a (Noetherian) local ring, then $K_1(A) \cong \mathbb{Z}$.

Note that the proof of [7.26.i] transfers verbatim to show that K_1 satisfies an analogous universal property: namely for any abelian group G, there is a bijective correspondence between additive functions $\lambda\colon \mathscr{F}_1 \to G$ and group homomorphisms $\lambda_0\colon K_1 \to G$ given by $\lambda = \lambda_0 \circ \gamma_1$. Then as in [7.26.iii], the additive function $\operatorname{rk}_A\colon \mathscr{F}_1 \to \mathbb{Z}$, with range $\mathbb{N}$, induces a surjective homomorphism $K_1 \to \mathbb{Z}$, and so K_1 contains an infinite cyclic additive subgroup. Recall from [7.15] that if A is Noetherian and local, then $M \in \mathscr{F}_1$ if and only if $M \cong A^n$ for some $n \in \mathbb{N}$. Since the $\gamma_1(M)$ generate K_1, it follows the additive group of K_1 is cyclic; hence $K_1 \cong \mathbb{Z}$.

Let $f\colon A \to B$ be a ring homomorphism, B being Noetherian. Show that extension of scalars gives rise to a ring homomorphism $f^!\colon K_1(A) \to K_1(B)$ such that $f^!\big(\gamma_1(M)\big) = \gamma_1(B \otimes_A M)$. If $g\colon B \to C$ is another ring homomorphism (with C Noetherian), then $(g \circ f)^! = g^! \circ f^!$.

(2.20) states that for M a flat A-module, $M|^f := B \otimes_A M$ is a flat B-module, and (2.17) that if M is finitely generated, so is $M|^f$. Thus we have a map $|^f\colon \mathscr{F}_1(A) \to \mathscr{F}_1(B)$. Set $\lambda = \gamma_{1,B} \circ |^f\colon \mathscr{F}_1(A) \to \mathscr{F}_1(B) \to K_1(B)$. If $0 \to N \to M \to P \to 0$ is a short exact sequence in $\mathscr{F}_1(A)$, then the proof of parts i,ii) shows that $0 \to N|^f \to M|^f \to P|^f \to 0$ is exact, so $\big[N|^f\big] - \big[M|^f\big] + \big[P|^f\big] \in D_1(B)$, showing λ is additive. By the universal property in the proof of part iii), it follows there is a unique group homomorphism $f_!\colon K_1(A) \to K_1(B)$ such that $f_! \circ \gamma_{1,A} = \gamma_{1,B} \circ |^f$. Further, this is a ring homomorphism, for $B \otimes_A A \cong B$ by (2.14.iv), and $(B \otimes_A M) \otimes_B (B \otimes_A N) \cong M \otimes_A B \otimes_B B \otimes_A N \cong M \otimes_A (B \otimes_B B) \otimes_A N \cong M \otimes_A B \otimes_A N \cong B \otimes_A (M \otimes_A N)$ by (2.14.i,ii,iv) and (2.15) (viewing B as a (B, A)-bimodule).

For $M \in \mathscr{F}_1(A)$ we have $\big(M|^f\big)|^g = C \otimes_B M|^f = C \otimes_B (B \otimes_A M) \cong (C \otimes_B B) \otimes_A M \cong C \otimes_A M = M|^{g \circ f}$ by (2.15) (viewing B as a (B, A)-bimodule) and (2.14.iv). If we write α_f for the map $F_1(A) \to F_1(B)$ induced by $|^f$, and so on, then we've shown $\alpha_{g \circ f} = \alpha_g \circ \alpha_f\colon F_1(A) \to F_1(C)$. Now $(g \circ f)^!$ is the unique homomorphism $\nu\colon K_1(A) \to K_1(C)$ such that $\nu \circ \gamma_{1,A} = \gamma_{1,C} \circ |^{g \circ f}$, and so is unique such that $\nu \circ \pi_{1,A} = \pi_{1,C} \circ \alpha_{g \circ f}$. On the other hand, the diagram at right shows $\nu = g^! \circ f^!$ also satisfies this equality, so $(g \circ f)^! = g^! \circ f^!$

$$\begin{tikzcd}
\mathscr{F}_1(A) \arrow[r, "|^f"'] \arrow[d, two heads] & \mathscr{F}_1(B) \arrow[r, "|^g"'] \arrow[d, two heads] & \mathscr{F}_1(C) \arrow[d, two heads] \\
F_1(A) \arrow[r, "\alpha_f"'] \arrow[d, "\pi_{1,A}"] & F_1(B) \arrow[r, "\alpha_g"'] \arrow[d, "\pi_{1,B}"] & F_1(C) \arrow[d, "\pi_{1,C}"] \\
K_1(A) \arrow[r, "f^!"'] & K_1(B) \arrow[r, "g^!"'] & K_1(C).
\end{tikzcd}$$

If $f\colon A \to B$ is a finite ring homomorphism then

$$f_!\big(f^!(x)y\big) = x f_!(y)$$

for $x \in K_1(A)$, $y \in K(B)$. In other words, regarding $K(B)$ as a $K_1(A)$-module by restriction of scalars, the homomorphism $f^!$ is a $K_1(A)$-module homomorphism

By bi-additivity of the module multiplication, since $f^!$ and $f_!$ are homomorphisms, and since elements $x = \gamma_{1,A}(M)$ and $y = \gamma_B(N)$ generate $K_1(A)$ and $K(B)$, it will suffice to check the equality for these elements:

$$\begin{aligned}
f_!\Big(f^!\big(\gamma_{1,A}(M)\big) \cdot \gamma_B(N)\Big) &\overset{\text{iv)}}{=} f_!\big(\gamma_{1,B}(B \otimes_A M) \cdot \gamma_B(N)\big) \overset{\text{ii)}}{=} f_!\Big(\gamma_B\big((M \otimes_A B) \otimes_B N\big)\Big) \\
&\underset{(2.14.\text{iv})}{\overset{(2.15)}{=}} f_!\big(\gamma_B(M \otimes_A N)\big) \overset{[7.26.\text{iv}]}{=} \gamma_A\big((M \otimes_A N)|_f\big) \\
&= \gamma_A(M \otimes_A N|_f) \overset{\text{ii)}}{=} \gamma_{1,A}(M) \cdot \gamma_A(N|_f) \overset{[7.26]}{=} \gamma_{1,A}(M) \cdot f_!\big(\gamma_B(N)\big).
\end{aligned}$$

It doesn't make sense to consider $f^!$ to be a $K_1(A)$-module homomorphism $K(A) \to K(B)$; we defined $f^!$ as a map $K_1(A) \to K_1(B)$ because a short exact sequence in $\mathscr{F}(A)$ has no reason to remain exact under $B \otimes_A$— for arbitrary finite A-algebras B. So assume instead that the book actually meant to ask about the homomorphism $f_!\colon K(B) \to K(A)$.[25] One can define a map $t'\colon \mathscr{F}_1(A) \times \mathscr{F}(B) \to F(B)$ by $t'(M,N) = M \otimes_A N|_f$, first restricting scalars along f and then regarding the result as a B-module by $b(m \otimes n) = m \otimes bn$. This then induces a bilinear map $\tau'\colon C_1(A) \times C(B) \to C(B)$ making $C(B)$ a $C_1(A)$-module. Thinking of B-modules as A-modules by restriction of scalars, our proof of part ii) above gives an induced map $\mu'\colon K_1(A) \times K(B) \to K(B)$ making $K(B)$ a $K_1(A)$-module. We claim $\mu'(x,y) = \mu_B\big(f^!(x), y\big)$; it again suffices to check for generators $x = \gamma_{1,A}(M)$ and $y = \gamma_B(N)$. Now

$$\mu_B\big(f^!(x), y\big) = \mu_B\big(\gamma_{1,B}(B \otimes_A M), \gamma_B(N)\big) = \gamma_B\big((B \otimes_A M) \otimes_B N\big) = \gamma_B(M \otimes_A N) = \mu'(x,y).$$

Remark. Since $F_1(A)$ is a subset of $F(A)$ we have a group homomorphism $\epsilon\colon K_1(A) \to K(A)$ given by $\epsilon\big(\gamma_1(M)\big) = \gamma(M)$. If the ring A is finite-dimensional and *regular*, i.e., if all its local rings $A_\mathfrak{p}$ are regular (Chapter 11) it can be shown that ϵ is an isomorphism.

[25] To regard $K(B)$ as a $K_1(A)$-module by restriction of scalars, one's first inclination is to set $x \cdot y = x \cdot f_!(y)$, but the former is supposed to be in $K(B)$ and the latter is in $K(A)$; apparently this is not what the book means by "restriction of scalars."

Artin Rings

Example. (p. 91, top) If $A = k[x_1, x_2, \ldots]$ is a polynomial ring in countably many indeterminates over a field k, the ideal $\mathfrak{a}$ is $(x_1, x_2^2, x_3^3, \ldots)$, and $B = A/\mathfrak{a}$, then writing $y_n = \bar{x}_n$, the book claims that $\mathfrak{m} = (y_1, y_2, \ldots)$ is the only prime ideal of B. Evidently $\mathfrak{m}$ is maximal, since $k[y_1, y_2, \ldots]/(y_1, y_2, \ldots) \cong k$. Since each $y_n \in \mathfrak{N}(B)$ is nilpotent, we have $\mathfrak{m} \subseteq \mathfrak{N}(B)$, so by (1.8) every prime of B contains $\mathfrak{m}$, which is then minimal, hence the only prime. But $(y_1) \subsetneq (y_1, y_2) \subsetneq \cdots$ is an infinite ascending sequence of ideals, so B is not Noetherian. Three other examples can be found in the solution to [7.8].

EXERCISES

Let $\mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = 0$ be a minimal primary decomposition of the zero ideal in a Noetherian ring [A], and let $\mathfrak{q}_i$ be $\mathfrak{p}_i$-primary. Let $\mathfrak{p}_i^{(m)}$ be the m^{th} symbolic power *of $\mathfrak{p}_i$ (Chapter 4, Exercise 13). Show that for each $i = 1, \ldots, n$ there exists an integer m_i such that $\mathfrak{p}_i^{(m_i)} \subseteq \mathfrak{q}_i$.*

Set $\mathfrak{q} = \mathfrak{q}_i$, $\mathfrak{p} = \mathfrak{p}_i$, and $S_\mathfrak{p} = A \backslash \mathfrak{p}$. From (7.14), since the radical $r(\mathfrak{q}) = \mathfrak{p}$, it follows from (7.14) that there is $m \in \mathbb{N}$ such that $\mathfrak{p}^m \subseteq \mathfrak{q}$. Then $\mathfrak{p}^{(m)} = S_\mathfrak{p}(\mathfrak{p}^m) \subseteq S_\mathfrak{p}(\mathfrak{q}) = \mathfrak{q}$ by (4.12*.iv,iii).

Suppose $\mathfrak{q}_i$ is an isolated primary component. Then $A_{\mathfrak{p}_i}$ is an Artin local ring, hence if $\mathfrak{m}_i$ is its maximal ideal we will have $\mathfrak{m}_i^r = 0$ for all sufficiently large r, hence $\mathfrak{q}_i = \mathfrak{p}_i^{(r)}$

Since $\mathfrak{p}^{(r)} \subseteq \mathfrak{q}$ for sufficiently large r, and $\mathfrak{p}^{(r)}$ is $\mathfrak{p}$-primary by [7.13.i], we have another primary decomposition $\mathfrak{p}^{(r)} \cap \bigcap_{j \neq i} \mathfrak{q}_j = 0$. By the uniqueness (4.11) of isolated primary components, it follows $\mathfrak{q} = \mathfrak{p}^{(r)}$.[1]

Now we claim $A_\mathfrak{p}$ is a local Artinian ring with nilpotent maximal ideal $\mathfrak{m} := \mathfrak{p}^e$. By (3.13), $A_\mathfrak{p}$ is local with maximal ideal $\mathfrak{m}$, and by (7.3) it is Noetherian. By (4.6), $\mathfrak{p}$ is minimal in $V(0) = \operatorname{Spec}(A)$; it follows from (3.13) that $\mathfrak{m}$ is also minimal in $A_\mathfrak{p}$, hence the only prime, so $\dim(A_\mathfrak{p}) = 0$ and $A_\mathfrak{p}$ is Artinian by (8.5). Further, $\mathfrak{m} = \mathfrak{N}(A_\mathfrak{p})$ by (1.8), so by (7.15) or (8.4) there is $r \in \mathbb{N}$ such that $\mathfrak{m}^r = 0$.[2]

If $\mathfrak{q}_i$ is an embedded primary component, then $A_{\mathfrak{p}_i}$ is not *Artinian, hence the powers $\mathfrak{m}_i^r$ are all distinct, and so the $\mathfrak{p}_i^{(r)}$ are all distinct. Hence in the given primary decomposition we can replace $\mathfrak{q}_i$ by any of the infinite set of $\mathfrak{p}_i$-primary ideals $\mathfrak{p}_i^{(r)}$ where $r \geq r_i$, and so there are infinitely many minimal primary decompositions of 0 which differ only in the $\mathfrak{p}_i$ component.*

If we have $\mathfrak{p}_j \subsetneq \mathfrak{p}$ with $\mathfrak{q}_j$ another primary component, then $\mathfrak{p}_j^e \subsetneq \mathfrak{p}^e$ in A_i, so $\dim(A_i) \geq 1$ and A_i is not Artinian by (8.5). It follows from (8.6) (using contraposition to exclude case ii)) that all the powers $\mathfrak{m}^r$ are distinct. If $\mathfrak{p}^r = \mathfrak{p}^{r+1}$ for some r, then taking extensions and using (3.11.v) we have $\mathfrak{m}^r = (\mathfrak{p}^e)^r = (\mathfrak{p}^r)^e = (\mathfrak{p}^{r+1})^e = (\mathfrak{p}^e)^{r+1} = \mathfrak{m}^{r+1}$, so it follows the $\mathfrak{p}^r$ are all distinct. Since A is Noetherian, $\mathfrak{p}^r$ has a primary decomposition by (7.13); by our proof of [4.13.ii], $\mathfrak{p}^{(r)}$ is the smallest primary ideal containing $\mathfrak{p}^r$. It follows that since the $\mathfrak{p}^r$ are distinct, so are the $\mathfrak{p}^{(r)}$. Now if $r \geq r_i$, we have $0 \neq \mathfrak{p}^{(r)} \subsetneq \mathfrak{p}^{(r_i)}$, so any of these $\mathfrak{p}^{(r)}$ can be substituted in the primary decomposition of (0).

[1] Despite the utter triviality of this two-line argument, I had to poach it from http://scribd.com/doc/47338424/atiyah-macdonald-solutions.

[2] I was unable to prove the "hence" of the problem; while I've proven the nilpotence of $\mathfrak{m}$ and that $\mathfrak{q} = \mathfrak{p}^{(r)}$ separately, I still don't know why the latter follows from the former.

Let A be a Noetherian ring. Prove that the following are equivalent:

A is Artinian;

Spec(A) *is discrete and finite;*

Spec(A) *is discrete.*

ii) $\Longrightarrow$ iii): Trivial.

iii) $\Longrightarrow$ i): If Spec(A) is discrete, then in particular each point is closed. By [1.18.i], the closed points correspond to maximal ideals, so every prime in A is maximal. Then $\dim(A) = 0$, so by (8.5), A is Artinian.

i) $\Longrightarrow$ ii): If A is Artinian, every prime ideal of A is maximal by (8.1), so by [1.18.i] or [3.11], each point of $X = \operatorname{Spec}(A)$ is closed. By (8.3) it only has a finite number of maximal (hence prime ideals), so it is finite. But then every subset of X is a finite union of closed sets, hence closed, and X is discrete.

Let k be a field and A a finitely generated k-algebra. Prove that the following are equivalent:

A is Artinian;

A is a finite k-algebra.

i) $\Longrightarrow$ ii): By (8.7), A is a finite direct product of local Artinian rings A_j, which are quotients of A under the projection, and hence again finitely generated (by the images of the generators of A, for instance). Thus if we can prove each of the finitely many A_j is a finite k-algebra, so will A be.

So without loss of generality assume A is local Artinian ring finitely generated over k, with lone prime $\mathfrak{m}$. Then $B = A/\mathfrak{m}$ is a field, again finitely generated over k, so by Zariski's Lemma ((1.27.2*), (5.24), [5.18], (7.9)), B is a finite algebraic extension of k, and hence a finite k-vector space. Since primary decompositions exist in the Noetherian ring A and $\operatorname{Spec}(A) = \{\mathfrak{m}\}$, we see $\mathfrak{m}$ belongs to (0). Then as A is finitely generated as an A-module, [7.18] gives us a chain $0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = A$ of A-submodules whose successive quotients are of the form $A/\mathfrak{p}_i$ for $\mathfrak{p}_i \in \operatorname{Spec}(A) = \{\mathfrak{m}\}$ — that is to say, all isomorphic to B. Thus we have a finite collection of short exact sequences $0 \to M_i \to M_{i+1} \to B \to 0$ of A-modules, which we may view as k-modules. Since $\dim_k$ is an additive function, this gives us $\dim_k M_{i+1} = \dim_k M_i + \dim_k B$, and taking $i = 0$ shows $\dim_k M_1 = \dim_k B$ is finite. By induction, $\dim_k A = n \dim_k B$ is finite.

ii) $\Longrightarrow$ i): A finite k-algebra (p. 30) is finitely generated as a k-module. By (6.10), it follows A satisfies the d.c.c. on k-submodules. Since each A-module is naturally also a k-module, it follows A satisfies the d.c.c. on ideals as well, and so is an Artinian ring.

Let $f\colon A \to B$ be a ring homomorphism of finite type. Consider the following statements:

f is finite;

the fibres of f^* are discrete subspaces of Spec(B)*;*

for each prime ideal $\mathfrak{p}$ of A, the ring $B \otimes_A k(\mathfrak{p})$ is a finite $k(\mathfrak{p})$-algebra ($k(\mathfrak{p})$ is the residue field of $A_\mathfrak{p}$);

the fibres of f^* are finite.

Prove that i) $\Longrightarrow$ ii) $\Longleftrightarrow$ iii) $\Longrightarrow$ iv).

If f is integral and the fibres of f^* are finite, is f necessarily finite?

For the last question, it is important to realize we are not assuming finite type; otherwise, (5.2) and the Remark on p. 60 show the answer is yes. Consider the algebraic closure $\overline{K}$ of a field K, constructed for example in [1.13].[3] The fibers of the inclusion $K \hookrightarrow \overline{K}$ will be finite, for both spectra are one-point spaces. However, this extension will not be finite unless $\dim_K \overline{K}$ is finite, which is not the case, for example, if K is a finite algebraic extension of any member of $\{\mathbb{F}_p, \mathbb{Q}, \mathbb{Q}_p, k(S)\}$, where k is any field and $S \neq \varnothing$ any set of indeterminates.

For the implications, fix $\mathfrak{p} \in \operatorname{Spec}(A)$ and let $k = k(\mathfrak{p}) = A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ be the residue field of the localization $A_\mathfrak{p}$. Recall from (2.14.i) that $C := B \otimes_A k \cong k \otimes_A B$ and from [3.21.iv] that $\operatorname{Spec}(C) \approx (f^*)^{-1}(\mathfrak{p})$. Note further, using (2.14.iv) and (2.15), that

$$C := B \otimes_A k \cong B \otimes_A (A_\mathfrak{p} \otimes_{A_\mathfrak{p}} k) \cong (B \otimes_A A_\mathfrak{p}) \otimes_{A_\mathfrak{p}} k. \tag{8.1}$$

i) $\Longrightarrow$ iii): Assume B is generated as an A-module by n elements. It follows from the proof of (2.17) that $B \otimes_A A_\mathfrak{p}$ is generated by n elements as an $A_\mathfrak{p}$-module and by (2.17) again and Eq. 8.1 that C is a $\leq n$-dimensional k-vector space. Since C is a k-algebra, it is then a finite k-algebra.

iii) $\Longrightarrow$ ii): By the assumption and [8.3], C is an Artinian ring. Then by [8.2], its spectrum $(f^*)^{-1}(\mathfrak{p})$ is discrete.

[3] We defined $\overline{K}$ as the subset of elements of $L = \bigcup_{n=0}^{\infty} K_n$ algebraic over $K = K_0$, where each K_{n+1} is the smallest algebraic extension of K_n in which each irreducible monic polynomial $p(x) \in K_n[x]$ has a root. But it turns out $K_1 = \overline{K} = L$. By (5.4) and induction, each K_n is integral over K, and each $\alpha \in \overline{K} \subseteq L$ is in some K_n, so $\overline{K}$ is integral over K. Since, each K_n is integral over K, each member thereof satisfies a polynomial equation $p(x) \in K[x]$; but that shows that $p(x)$ already has a root in K_1, which then must be itself algebraically closed.

ii) $\Longrightarrow$ iii): We first show C is a finitely generated k-algebra (and hence, by (7.7), Noetherian).[4] Since f is of finite type, there is a surjective ring homomorphism $A[x_1, \ldots, x_n] \to B$. Recalling from (2.18) that tensor is right exact, we apply $A_\mathfrak{p} \otimes_A -$ to both sides and use [2.6] (see the footnote to [7.13]) to get a surjective ring homomorphism $A_\mathfrak{p}[x_1, \ldots, x_n] \to A_\mathfrak{p} \otimes_A B$. Applying $k \otimes_{A_\mathfrak{p}} -$ to both sides, the same argument, followed by (2.15), (2.14.i), and Eq. 8.1, yields a surjective ring homomorphism $k[x_1, \ldots, x_n] \to k \otimes_{A_\mathfrak{p}} \big(A_\mathfrak{p} \otimes_A B\big) \cong C$, so C is a finitely generated k-algebra. By (7.7), C is a Noetherian ring, and by assumption, $(f^*)^{-1}(\mathfrak{p}) \approx \operatorname{Spec}(C)$ is discrete, so [8.2] shows C is Artinian. Because of this and because C is a finitely generated k-algebra, [8.3] shows C is a finite k-algebra.

ii) & iii) $\Longrightarrow$ iv): By iii), C is a finite k-algebra, hence *a fortiori* finitely generated, and hence by (7.7) a Noetherian ring; and by ii), $(f^*)^{-1}(\mathfrak{p}) \approx \operatorname{Spec}(C)$ is discrete; so from [7.2] it follows $\operatorname{Spec}(C) = (f^*)^{-1}(\mathfrak{p})$ is also finite.

In Chapter 5, Exercise 16, show that X is a finite covering of L (i.e., the number of points of X lying over a given point of L is finite and bounded.)

Refer back to our solution to [5.16] for notation. In summary, we were given an affine subvariety $X \subseteq k^n$ and from it constructed a linear surjection $\pi\colon k^n \twoheadrightarrow k^r = L$ such that $\pi|_X$ is already surjective. The coordinate rings ([1.27]) of X and L were written, respectively, as A and A', and r and π were chosen in such a way that the injection $\varpi = (\pi|_X)^\#\colon A' \rightarrowtail A$ was integral of finite type. View it as an inclusion. Recalling from [1.27] and [5.16] that we may identify X with $\operatorname{Max}(A)$ and the map $X \to L$ with its induced map $\operatorname{Max}(A) \to \operatorname{Max}(A')$, we now want to show only finitely many maximal ideals of A lie over any maximal ideal of A'. Using (5.2) again, ϖ is finite, so by [8.4] it follows the fibers of ϖ^* are finite.

However, we still want to uniformly bound the size of these fibers. Since ϖ is integral of finite type, by the Remark on p. 60, ϖ is finite; say A is generated as an A'-module by n elements. Then n is a uniform bound on the k-dimension of $B = A \otimes_{A'} k(\mathfrak{p})$ for $\mathfrak{p} \in \operatorname{Spec}(A')$, and by [3.21.iv] it is enough to show $\operatorname{Spec}(B)$ has $\leq n$ points. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ be distinct primes of B. Since they are coprime, the canonical map $B \to \prod B/\mathfrak{p}_i$ is surjective. Since B is a $k(\mathfrak{p})$-algebra, the $\mathfrak{p}_i$ and hence the $B/\mathfrak{p}_i$ are $k(\mathfrak{p})$-vector spaces as well. We have $n \geq \dim_k B \geq \sum_{i=1}^m \dim_k(B/\mathfrak{p}_i) \geq m$, so $\operatorname{Spec}(B)$ is finite.[5]

Let A be a Noetherian ring and $\mathfrak{q}$ a $\mathfrak{p}$-primary ideal in A. Consider chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$. Show that all such chains are of finite bounded length, and that all maximal chains have the same length.

We have a bijection, by (1.1) and (3.9), between the set $\Sigma = \{\mathfrak{a} \lhd A : \mathfrak{q} \subseteq \mathfrak{a} \subseteq \mathfrak{p}\}$ and the ideals $(\mathfrak{a}/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$ of $B = (A/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$, which we claim preserves and reflects being ($\mathfrak{p}$-)primary. By (4.8), extension along $A/\mathfrak{q} \to B$ preserves being primary (for $\bar{\mathfrak{a}} \subseteq \mathfrak{p}/\mathfrak{q}$), and by p. 50, contraction along $A \to B$ preserves being primary, so it remains to see extension $\mathfrak{a} \mapsto \mathfrak{a}/\mathfrak{q}$ along $A \twoheadrightarrow A/\mathfrak{q}$ does, for $\mathfrak{a} \supseteq \mathfrak{q}$. But for $x, y \in A$, $\bar{x}\bar{y} \in \mathfrak{a}/\mathfrak{q}$ implies $xy \in \mathfrak{a}$, so that $x \in \mathfrak{a}$ or some $y^n \in \mathfrak{q}$, meaning $\bar{x} \in \mathfrak{a}/\mathfrak{q}$ or $\overline{y^n} = \bar{y}^n \in \mathfrak{a}/\mathfrak{q}$.

Note that as a localization of a quotient of a Noetherian ring, B is also Noetherian, by (7.1) and (7.4). Since A is Noetherian and $r(\mathfrak{q}) = \mathfrak{p}$, (7.14) gives an $n \geq 1$ such that $p^n \subseteq \mathfrak{q}$, so the maximal ideal $\mathfrak{m}$ of the local ring B satisfies $\mathfrak{m}^n = 0$. By (8.6), B is Artinian. Also, for any $\mathfrak{b} \lhd B$ we have $\mathfrak{m}^n \subseteq \mathfrak{b} \subseteq \mathfrak{m}$, so by (7.16), $\mathfrak{b}$ is $\mathfrak{m}$-primary.[6]

Thus our question boils down to arbitrary chains of ideals in an Artinian ring B. By the definition of the word, these must all have finite length. A maximal chain is a composition series (p. 76), and by (6.7), these all have the same length.

[4] It feels like this should have been proven in the book somewhere already, but I don't see where, so I'm doing it here.

[5] A slightly different proof, from [Milne, Prop. 8.5], is as follows. Let $\mathfrak{m}' \in \operatorname{Max}(A')$ and $K = A'/\mathfrak{m}'$; then by (1.17.i), each $\mathfrak{m} \in \operatorname{Max}(A)$ with $\mathfrak{m}^c = \mathfrak{m}'$ has $(\mathfrak{m}')^e = \mathfrak{m}^{ce} \subseteq \mathfrak{m}$, so $\mathfrak{m}$ descends to a maximal ideal of $A/(\mathfrak{m}')^e$. Since A is a finite A'-module, with n generators for some n, by (2.8) $C = A/(\mathfrak{m}')^e$ is a $\leq n$-dimensional K-algebra. If $\operatorname{Spec}(C)$ contains m primes, then the same proof as above, with C replacing B, shows $n \geq m$, and this limits the number of maximal $\mathfrak{m}$ lying over $\mathfrak{m}'$.

[6] Amusingly, this seems to show the ideals of Σ were all $\mathfrak{p}$-primary. Can that be right?

Discrete Valuation Rings and Dedekind Domains

EXERCISES

Let A be a Dedekind domain, S a multiplicatively closed subset of A. Show that $S^{-1}A$ is either a Dedekind domain or the field of fractions of A.

By (9.3), A is an integrally closed Noetherian domain of dimension one. (5.12) implies that $S^{-1}A$ is also integrally closed and (7.3) that it is Noetherian. $S^{-1}A$ is a domain since it is contained in the field of fractions K of A. By (3.11.iv), the longest possible chain of prime ideals in $S^{-1}A$ is $(0) = S^{-1}(0) \subseteq S^{-1}\mathfrak{p}$ for a prime $\mathfrak{p} \lhd A$ not meeting S. Since $\mathfrak{p} \neq 0$ and S^{-1} are contained in a field, $S^{-1}\mathfrak{p} \neq (0)$. It follows from the definition (9.3) that $S^{-1}A$ is a Dedekind domain if there is some prime $\mathfrak{p}$ disjoint from S. If there is none, then (0) is maximal in $S^{-1}A$, which is then a field. Since it contains A, it then is K.

Suppose that $S \neq A \backslash \{0\}$, and let H, H' be the ideal class groups of A and $S^{-1}A$ respectively. Show that extension of ideals induces a surjective homomorphism $H \to H'$.

First we show $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ is a homomorphism of fractional ideal groups $I(A) \to I(S^{-1}A)$. Since A is Noetherian, each fractional ideal $\mathfrak{a}$ of A is finitely generated; it follows from (3.15) then that $S^{-1}(A : \mathfrak{a}) = (S^{-1}A : S^{-1}\mathfrak{a})$, so $S^{-1}\mathfrak{a}^{-1} = (S^{-1}\mathfrak{a})^{-1}$. For multiplication, $S^{-1}S^{-1} = S^{-1}$ since $1 \in S$, so $S^{-1}(\mathfrak{a}\mathfrak{b}) = S^{-1}S^{-1}\mathfrak{a}\mathfrak{b} = (S^{-1}\mathfrak{a})(S^{-1}\mathfrak{b})$.

This map is surjective because $\mathfrak{a} \mapsto S^{-1}\mathfrak{a}$ is surjective on integral ideals (3.11.i) and fractional ideals of a Noetherian ring are of the form $x^{-1}\mathfrak{a}$ for $x \in A$ and $\mathfrak{a} \lhd A$ (p. 96). For $x \in K$, we have $xA \mapsto S^{-1}(xA) = x(S^{-1}A)$, so principal fractional ideals are mapped to principal fractional ideals, and the surjective homomorphism $I(A) \to I(S^{-1}A)$ descends to a surjective homomorphism $H \to H'$.

Let A be a Dedekind domain. If $f = a_0 + a_1x + \cdots + a_nx^n$ is a polynomial with coefficients in A, the content *of f is the ideal $c(f) = (a_0, \ldots, a_n)$ in A.*

Prove *Gauss's lemma* that $c(fg) = c(f)c(g)$.

Let $f = \sum a_ix^i$, $g = \sum b_jx^j$, and $fg = \sum c_kx^k$, where $c_k = \sum_{i+j=k} a_ib_j$. We will have $c(fg) \subseteq c(f)c(g)$ just if for each prime $\mathfrak{p} \lhd A$, $c(fg)_\mathfrak{p} = \big(c(f)c(g)\big)_\mathfrak{p}$.[1] But $\big(c(f)c(g)\big)_\mathfrak{p} = c(f)_\mathfrak{p}c(g)_\mathfrak{p}$ by (3.11.v), and $c(f)_\mathfrak{p}$ is the content of the image of f in $A_\mathfrak{p}$. Thus, by the definition (9.3), we may assume A is a discrete valuation ring (henceforth "DVR").

Finitely generated ideals of A are principal[2], so we can write $c(f) = (a')$ and $c(g) = (b')$ and we know $a'b'$ divides fg in $A[x]$. Note that if d is a divisor of each coefficient of $h \in A[x]$, so that $h/d \in A[x]$, we have $c(h) = d \cdot c(h/d)$. Thus $(a') = c(f) = a' \cdot c(f/a')$, so $c(f/a') = (1)$, and similarly $c(g/b') = (1)$. In the terminology of [1.2.iv], f/a' and g/b' are primitive, by the result of that exercise, the same holds of $fg/a'b'$, which then has content (1). It follows that $c(f)c(g) = (a'b') = a'b' \cdot c(fg/a'b') = c(fg)$.

[1] Let $N, P \subseteq M$ be A- modules. To show $N = P$ it is enough to show that the inclusions $N \hookrightarrow N + P$ and $P \hookrightarrow N + P$ are surjective. By (3.9) and (3.4.i), this happens if and only if for all primes $\mathfrak{p} \lhd A$, $N_\mathfrak{p} \hookrightarrow (N+P)_\mathfrak{p} = N_\mathfrak{p} + P_\mathfrak{p}$ and $P_\mathfrak{p} \hookrightarrow N_\mathfrak{p} + P_\mathfrak{p}$ are surjective; but this happens just when $N_\mathfrak{p} = P_\mathfrak{p}$.

[2] Such a ring is called a *Bézout domain* because it satisfies *Bézout's lemma* that if d is a common divisor of a, $b \in A$, there exist y, $z \in A$ such that $d = ay + bz$; see http://en.wikipedia.org/wiki/Bézout_domain and http://planetmath.org/encyclopedia/BezoutDomain.html.

A ring satisfying Gauß's lemma is called a *Gaussian ring*, and the Gaussian rings that are domains turn out (see e.g. http://arxiv.org/abs/1107.0440) to be exactly the *Prüfer domains* (see http://en.wikipedia.org/wiki/Prüfer_domain). These rings have many characterizations, one of which is that all their localizations at primes are valuation rings, others being that the nonzero finitely generated ideals are all invertible and that all their ideals are flat. Cf. also http://planetmath.org/encyclopedia/PruferRing.html.

If one instead defines the content of a polynomial as the greatest common divisor of its coefficients (which will generate the ideal we called the content before, in the event this ideal is principal) one can extend the result to integral domains such that any two elements have greatest common divisors, and in particular to unique factorization domains. This is easily proved, e.g., at http://en.wikipedia.org/wiki/Gauss%27s_lemma_(polynomial)#A_proof_valid_over_any_GCD_domain. See also http://planetmath.org/GcdDomain.html and http://planetmath.org/encyclopedia/PropertiesOfAGcdDomain.html.

A valuation ring (other than a field) is Noetherian if and only if it is a discrete valuation ring.

The argument on p. 94 shows a DVR is a Noetherian valuation ring (and not a field).

For the other direction, by (5.18), a Noetherian valuation ring A is local. It is an integral domain by the definition on p. 65. It now will be enough, by (9.7), to show the non-zero fractional ideals of A are invertible, or by (9.2), to show the maximal ideal $\mathfrak{m}$ is principal and A has dimension one. First we show A is a PID. Any ideal $\mathfrak{a}$ of A is finitely generated as $(x_1, \ldots, x_n)$ for some $x_j \in A$ since A is Noetherian. By [5.28], the ideals (x_j) are totally ordered, so one contains all the others, and hence $\mathfrak{a}$ is principal.

To use (9.7), just note that since A is a Noetherian PID, any fractional ideal of A is of of the form $x^{-1}(y)$ for some $x, y \in A$ (p. 96) and so has an inverse $y^{-1}(x)$.

To use (9.2), set $\mathfrak{m} = (m)$. Any prime ideal (p) satisfies $(p) \subseteq (m)$, so for some $a \in A$ we have $am = p$ and hence, since (p) is prime, either $m \in (p)$ or $a \in (p)$. If the former holds, $\mathfrak{p} = \mathfrak{m}$. If the latter holds, we have $b \in A$ such that $p = am = bpm$, or $(1 - bm)p = 0$. As m is not a unit $1 - bm \neq 0$, so since A is an integral domain, $p = 0$. It follows that the only chain of prime ideals in A is $(0) \subsetneq \mathfrak{m}$, meaning A has dimension one.

Let A be a local domain which is not a field and in which the maximal ideal $\mathfrak{m}$ is principal and $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$. Prove that A is a discrete valuation ring.

Let p be a generator for $\mathfrak{m}$, so for each $n \geq 0$ we have $\mathfrak{m}^n = (p^n)$. Since $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$, it follows there is no n with $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, and every $x \in A \backslash \{0\}$ fails to be in some $\mathfrak{m}^n$, so there is a greatest number $v(x) \in \mathbb{N}$ such that $p^{v(x)}$ divides x (taking $p^0 = 1$). If $v(x) = n$, we can write $x = up^n$ for some $u \in A$; since $p^{n+1} \nmid x$, it follows that $u \in A \backslash \mathfrak{m} = A^\times$. Thus $A \backslash \{0\} \cong A^\times \times p^{\mathbb{N}}$ as a multiplicative monoid. It follows that for every pair $x, y \in A$ we have $v(x) \leq v(y) \iff x | y$. Therefore any ideal $\mathfrak{a}$ is generated by an element $x \in \mathfrak{a}$ with $v(x)$ minimal, so that the ideals of A are (0) and the (p^n). This shows A is Noetherian of dimension one. By any of the implications iii), v), vi) $\Longrightarrow$ i) of (9.2), A is a DVR.

Let M be a finitely-generated module over a Dedekind domain. Prove that M is flat $\iff$ M is torsion-free.

Let the Dedekind domain be A. Since A is an integral domain, by [3.13], M is torsion-free just if for each prime $\mathfrak{p} \lhd A$ we have $M_\mathfrak{p}$ torsion-free over the DVR $A_\mathfrak{p}$. Now each $M_\mathfrak{p}$ is finitely generated over a PID, and so[3] can be written as the direct sum of the torsion submodule and a free module. Thus each $M_\mathfrak{p}$ is torsion-free if and only if it is free. Since A is Noetherian and M is finitely generated, by [7.16], M is flat just if each of the $M_\mathfrak{p}$ is free. It follows that M is flat if and only if it is torsion-free.

Let M be a finitely generated torsion module ($T(M) = M$) over a Dedekind domain A. Prove that M is uniquely representable as a finite direct sum of modules $A/\mathfrak{p}_i^{n_i}$, where $\mathfrak{p}_i$ are nonzero prime ideals of A.

For each prime ideal $\mathfrak{p}$ of A we have $A_\mathfrak{p}$ a DVR. Since $M_\mathfrak{p}$ is finitely generated and torsion, and $A_\mathfrak{p}$ a PID (p. 94), the structure theorem for finitely generated modules shows[4] $M_\mathfrak{p}$ is isomorphic to a direct sum of modules $A_\mathfrak{p}/(d_j)$ for $d_j \in A_\mathfrak{p}$, where the (d_j) are primary and unique up to order. But since $A_\mathfrak{p}$ is a DVR, each $(d_j) = (\mathfrak{p}A_\mathfrak{p})^{n_j}$ for some $n_j \geq 1$. So $M_\mathfrak{p} \cong \bigoplus_j A_\mathfrak{p}/\mathfrak{p}^{n_j}A_\mathfrak{p}$. By exactness of localization (3.3) and [1.21.iv], since $\mathfrak{p}$ is the only prime ideal of A containing $\mathfrak{p}^{n_j}$ we have $A_\mathfrak{p}/\mathfrak{p}^{n_j}A_\mathfrak{p} \cong (A/\mathfrak{p}^{n_j})_\mathfrak{p} \cong A/\mathfrak{p}^{n_j}$, so each $M_\mathfrak{p}$ is of the form we desire for M. It will now suffice to show M is isomorphic to the direct sum of finitely many $M_\mathfrak{p}$.

Since M is finitely generated, [3.19.v] shows $\operatorname{Supp}(M) = V\big(\operatorname{Ann}(M)\big)$. As A is a Dedekind domain, the prime-power factorization of $\operatorname{Ann}(M)$ shows that $\operatorname{Supp}(M)$ is finite. Now the canonical maps $m \mapsto m/1 \colon M \to M_\mathfrak{p}$ for each $\mathfrak{p} \in \operatorname{Supp}(M)$ naturally compile into a map $\phi \colon M \to \bigoplus M_\mathfrak{p}$. Note that since each pair $\mathfrak{p} \neq \mathfrak{q}$ of primes is coprime, there are $x \in \mathfrak{p}^n \backslash \mathfrak{q}$ for arbitrarily high n, which then annihilate the (finitely generated) summands $A/\mathfrak{p}^n$ of $M_\mathfrak{p}$, so by [3.1], $(M_\mathfrak{p})_\mathfrak{q} = 0$ for distinct primes $\mathfrak{p}$ and $\mathfrak{q}$. On the other hand, $(M_\mathfrak{p})_\mathfrak{p} \cong M_\mathfrak{p}$.[5] Therefore, since localization distributes over direct sums (Eq. 3.6) localizing ϕ at $\mathfrak{q}$ shows $\phi_\mathfrak{q} \colon M_\mathfrak{q} \to \big(\bigoplus M_\mathfrak{p}\big)_\mathfrak{q} \cong (M_\mathfrak{q})_\mathfrak{q} \cong M_\mathfrak{q}$ is an isomorphism for $\mathfrak{q} \in \operatorname{Supp}(M)$; and similarly $\phi_\mathfrak{q} \colon M_\mathfrak{q} \to \big(\bigoplus M_\mathfrak{p}\big)_\mathfrak{q} \cong \bigoplus 0$ is an isomorphism $0 \to 0$ for $\mathfrak{q} \notin \operatorname{Supp}(M)$. By (3.9), ϕ is an isomorphism.

[3] http://planetmath.org/encyclopedia/FinitelyGeneratedModulesOverAPrincipalIdealDomain.html

[4] See http://en.wikipedia.org/wiki/Structure_theorem_for_finitely_generated_modules_over_a_principal_ideal_domain#Primary_decomposition.

[5] For a multiplicative submonoid S of A, the map $a \mapsto (a/1)/1 \colon A \to S^{-1}(S^{-1}A)$ satisfies the conditions (3.2), so that $S^{-1}A \cong S^{-1}(S^{-1}A)$, Using (3.5), we can rewrite this as $S^{-1}A \cong S^{-1}A \otimes_A S^{-1}A$, so for any A-module M, using (3.5) again and (2.14.ii), $S^{-1}M \cong S^{-1}A \otimes_A M \cong S^{-1}A \otimes_A S^{-1}A \otimes_A M \cong S^{-1}(S^{-1}M)$.

Let A be a Dedekind domain and $\mathfrak{a} \neq 0$ an ideal in A. Show that every ideal in $A/\mathfrak{a}$ is principal.

First, let $\mathfrak{p}$ be a prime and $n \geq 1$. As in the previous exercise, $A/\mathfrak{p}^n \cong A_\mathfrak{p}/\mathfrak{p}^n A_\mathfrak{p}$, and $A_\mathfrak{p}$ is a DVR, hence (p. 94) a PID, so each ideal of $A/\mathfrak{p}^n$ is principal.

Given any $\mathfrak{a} \lhd A$, use (9.1) to produce a prime factorization $\mathfrak{a} = \prod \mathfrak{p}_i^{n_i}$ and consider the standard map $A \to \prod A/\mathfrak{p}_i^{n_i}$. Since the $\mathfrak{p}_i^{n_i}$ are coprime, (1.10) says that $\mathfrak{a} = \bigcap \mathfrak{p}_i^{n_i}$ and the map is surjective with kernel $\mathfrak{a}$. Thus we can write $A/\mathfrak{a} \cong \prod A/\mathfrak{p}_i^{n_i}$ as a product of rings B_i each of whose ideals is principal. As in [1.22], each ideal $\mathfrak{b}$ of $A/\mathfrak{a}$ is a sum of ideals of the B_i. If e_i is the element of $A/\mathfrak{a}$ whose i-component is 1 and whose other components are zero, and $\mathfrak{b}$ has $\mathfrak{b}e_i = (b_i e_i)$ for $b_i \in B_i$, then $\mathfrak{b} = \sum \mathfrak{b}e_i$ is generated by the single element $b = \langle b_i \rangle \in A/\mathfrak{a}$ whose i-component is b_i, since $b \in \mathfrak{b}$ and each $b_i e_i = b e_i \in (b)$. Thus $A/\mathfrak{a}$ is principal.

Deduce that every ideal in A can be generated by at most 2 elements.

Suppose $\mathfrak{c} \lhd A$ is not principal, and let a nonzero $a \in \mathfrak{c}$ be given. Then the ideal $\mathfrak{c}/(a)$ of $A/(a)$ is principal, generated by $b + (a)$ for some $b \in \mathfrak{c}$. It follows that $\mathfrak{c} = (a, b)$ in A.[6]

Let $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ be three ideals in a Dedekind domain. Prove that

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c}),$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c}).$$

Writing I for the set of nonzero ideals of our Dedekind domain, the problem is asking us to prove the lattice $(I, +, \cap)$ is distributive. Since all the ideals in question are submodules of A, by the first footnote to [9.2], to prove an equation it suffices to show the localizations of the sides at each prime agree. By (3.4), localization distributes over sum and intersection, so we now only have to prove the equations for A a DVR. But $\mathfrak{p}^m + \mathfrak{p}^n = \mathfrak{p}^{\min\{m,n\}}$ and $\mathfrak{p}^m \cap \mathfrak{p}^n = \mathfrak{p}^{\max\{m,n\}}$, so $\mathfrak{p}^n \mapsto n$ is a lattice isomorphism $(I, +, \cap) \to (\mathbb{N}, \min, \max)$. Since the latter is distributive,[7] the equations hold, and we are done.[8]

[6] A converse also holds: if A is a domain such that for every $\mathfrak{a} \lhd A$ and nonzero $a \in \mathfrak{a}$ there exists b such that $(a, b) = \mathfrak{a}$, then A is a Dedekind domain.

To see this, note that A is Noetherian, and all its localizations $A_\mathfrak{p}$ at primes $\mathfrak{p}$ must also be Noetherian by (7.3) and satisfy the same two-generator property. Let $0 \neq \mathfrak{a} \lhd A_\mathfrak{p}$. Picking a nonzero element $a \in \mathfrak{m}\mathfrak{a} \subseteq \mathfrak{a}$ and applying the two-generator property to $\mathfrak{a}$, we see there must be $b \in \mathfrak{a}$ such that $\mathfrak{a} = (a, b) = \mathfrak{m}\mathfrak{a} + (b)$ in $A_\mathfrak{p}$. Now $\mathfrak{a}$ is finitely generated and $\mathfrak{m} = \mathfrak{R}(A_\mathfrak{p})$, so by the corollary (2.7) to Nakayama's Lemma, $\mathfrak{a} = (b)$. Thus $A_\mathfrak{p}$ is a local, Noetherian PID, and so by (9.2) is a DVR. Since this holds for all $\mathfrak{p}$, by (9.3) A is a Dedekind domain.

This result can apparently be attributed to a C.-H. Sah; see Theorem 20.11 of Pete L. Clark's notes `http://math.uga.edu/~pete/integral.pdf`.

[7] To be thorough about this, we show that the lattice given by a totally ordered set (like $\mathbb{N}$), when equipped with the operations $x \vee y = \max\{x, y\}$ and $x \wedge y = \min\{x, y\}$, satisfies the equations $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ and $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$ for all x, y, z. Since $\vee$ and $\wedge$ are symmetric in their arguments, we may assume without loss of generality that $y \leq z$. To prove the equations, using a bit more brute force than we would like, we tabulate the values of the relevant terms and check that the sides are equal given any of the three possible orderings of x, y, z.

	$x \vee (y \wedge z)$	$(x \vee y) \wedge (x \vee z)$	$x \wedge (y \vee z)$	$(x \wedge y) \vee (x \wedge z)$
	x y		x z	
$x \leq y \leq z$		y z		x x
	y	y	x	x
$y \leq x \leq z$		x z		y x
	x	x	x	x
$y \leq z \leq x$		x x		y z
	x	x	z	z

[8] It is not strictly necessary to localize. For A a Dedekind domain again, the prime factorization (9.1) shows that to prove an equation it will be enough to show $v_\mathfrak{p}$-values of the sides agree for all primes $\mathfrak{p}$, where $v_\mathfrak{p}$ is given by $\mathfrak{a} = \prod_{\mathfrak{p} \in P} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}$. To do this, we show $v_\mathfrak{p}$ is a lattice homomorphism $(I, +, \cap) \to (\mathbb{N}, \min, \max)$. Since A has dimension one, its primes are maximal and hence pairwise coprime. This allows us to conclude products of disjoint sets of prime ideals are coprime, as follows: if ideals $\mathfrak{a}_i$ and $\mathfrak{b}_j$ are such that $\mathfrak{a}_i + \mathfrak{b}_j = (1)$ for all i and j, then $\prod \mathfrak{a}_i + \prod \mathfrak{b}_j = (1)$, for $(1) = \prod_i (\mathfrak{a}_i + \mathfrak{b}_j) \subseteq \left(\prod \mathfrak{a}_i\right) + \mathfrak{b}_j$, so $(1) = \prod_j \left(\prod_i (\mathfrak{a}_i) + \mathfrak{b}_j\right) \subseteq \prod_i \mathfrak{a}_i + \prod_j \mathfrak{b}_j$. Thus by (1.10.i), each intersection of powers of distinct primes is actually a product, and vice versa. Products of ideals do distribute over sums (p. 6), and for $m \leq n$ we have $\mathfrak{a}^m + \mathfrak{a}^n = \mathfrak{a}^m$ and $\mathfrak{a}^m \cap \mathfrak{a}^n = \mathfrak{a}^n$. Write $n_\mathfrak{p} = \min\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\}$ and $N_\mathfrak{p} = \max\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\}$. Then

$$\mathfrak{a} + \mathfrak{b} = \prod \mathfrak{p}^{n_\mathfrak{p}} \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) - n_\mathfrak{p}} + \prod \mathfrak{p}^{n_\mathfrak{p}} \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b}) - n_\mathfrak{p}} = \prod \mathfrak{p}^{n_\mathfrak{p}} \cdot \left(\prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a}) - n_\mathfrak{p}} + \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b}) - n_\mathfrak{p}}\right) = \prod \mathfrak{p}^{n_\mathfrak{p}}$$

since the two terms in the parentheses share no prime factors in common. Similarly,

$$\mathfrak{a} \cap \mathfrak{b} = \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \cap \prod \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})} = \bigcap \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \cap \bigcap \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})} = \bigcap \left(\mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})} \cap \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{b})}\right) = \bigcap \mathfrak{p}^{N_\mathfrak{p}} = \prod \mathfrak{p}^{N_\mathfrak{p}}.$$

We now have $v_\mathfrak{p}(a + \mathfrak{b}) = \min\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\}$ and $v_\mathfrak{p}(a \cap \mathfrak{b}) = \max\{v_\mathfrak{p}(\mathfrak{a}), v_\mathfrak{p}(\mathfrak{b})\}$ as hoped.

(Chinese Remainder Theorem). Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ *be ideals and let* $x_1, \ldots, x_n$ *be elements in a Dedekind domain A. Then the system of congruences* $x \equiv x_i \pmod{\mathfrak{a}_i}$ $(1 \leq i \leq n)$ *has a solution* x *in* $A \iff x_i \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}$ *whenever* $i \neq j$.

Following the book's hint, define $\phi \colon A \to \bigoplus_{i=1}^{n} A/\mathfrak{a}_i$ by $\phi(x)_i = x + \mathfrak{a}_i$, and $\psi \colon \bigoplus_{i=1}^{n} A/\mathfrak{a}_i \to \bigoplus_{i<j} A/(\mathfrak{a}_i + \mathfrak{a}_j)$ by $\psi\big(\langle x_i + \mathfrak{a}_i \rangle\big)_{\langle i,j \rangle} = x_i - x_j + \mathfrak{a}_i + \mathfrak{a}_j$. The system of congruences $x \equiv x_i \pmod{\mathfrak{a}_i}$ has a solution x just if $\langle x_i + \mathfrak{a}_i \rangle \in \operatorname{im}(\phi)$, and the conditions $x_i \equiv x_j \pmod{\mathfrak{a}_i + \mathfrak{a}_j}$ are satisfied just if $\langle x_i + \mathfrak{a}_i \rangle \in \ker(\psi)$. Then the statement in question is true just if the sequence

$$A \xrightarrow{\phi} \bigoplus A/\mathfrak{a}_i \xrightarrow{\psi} \bigoplus A/(\mathfrak{a}_i + \mathfrak{a}_j)$$

is exact. But this means just to show $\operatorname{im}(\phi) = \ker(\psi)$, and thus by the first footnote to [9.3] it is enough to show it is true after localizing at each prime $\mathfrak{p}$. By (3.4), localization distributes over quotients and sums, so it is enough to prove the results for ideals $\mathfrak{a}_i = \mathfrak{p}^{k_i}$ of a DVR A. Without loss of generality, assume $k_i \leq k_j$ for $i < j$.

If $\langle x_i + \mathfrak{p}^{k_i} \rangle \in \ker(\psi)$, it follows that for $i < j$ we have $x_i - x_j \in \mathfrak{p}^{k_i} + \mathfrak{p}^{k_j} = \mathfrak{p}^{k_i}$. Then $\phi(x_n) = \langle x_i + \mathfrak{p}^{k_i} \rangle$, showing $\ker(\psi) \subseteq \operatorname{im}(\phi)$. That $\psi \circ \phi = 0$ holds in any ring: $\big((\psi \circ \phi)(x)\big)_{\langle i,j \rangle} = \psi\big(\langle x + \mathfrak{a}_i \rangle\big)_{\langle i,j \rangle} = x - x + \mathfrak{a}_i + \mathfrak{a}_j = \mathfrak{a}_i + \mathfrak{a}_j$.

Completions

More than any other chapter, this one leaves small, eminently believable statements unproved. Before tackling the exercises, we prove some of these assertions. Doing so takes a surprisingly long time.

Lemma 10.1. *Let H be the intersection of all neighborhoods of 0 in [a topological abelian group] G. Then*
i) H is a subgroup.

The book notes that "i) follows from the continuity of the group operations." This is true, as far as it goes, but is actually longer, in its details, than the rest of the proof.

Write $\mathscr{N}_G(0)$ for the set of neighborhoods of 0 ($\mathscr{N}(0)$ when G is understood). Note that since $x \mapsto -x$ is a homeomorphism, for each neighborhood $U \in \mathscr{N}(0)$ we also have $-U \in \mathscr{N}(0)$. Then $V = U \cap -U \in \mathscr{N}(0)$ and $V = -V$. If $x \in H$ and $U \in \mathscr{N}(0)$, find a subset $V \in \mathscr{N}(0)$ with $V = -V$. Then $x \in V = -V$, so $-x \in V \subseteq U$. Since U was arbitrary, $-x \in H$.

Since $+\colon G \times G \to G$ is continuous and sends $\langle 0, 0\rangle \mapsto 0$, for any $U \in \mathscr{N}(0)$ there is a neighborhood W of $\langle 0, 0\rangle$ in $G \times G$ that addition maps into U. By the definition of the product topology, then, there are $V_1, V_2 \in \mathscr{N}(0)$ such that $V_1 \times V_2 \subseteq W$. If we set $V = V_1 \cap V_2$, then $V + V \subseteq U$. Now suppose $x, y \in H$, and let $U \in \mathscr{N}(0)$. There is $V \in \mathscr{N}(0)$ such that $V + V \subseteq U$, and $x, y \in V$, so $x + y \in U$. As U was arbitrary, $x + y \in H$.

Finally, note $0 \in H$, so H is nonempty.

Equivalence of Cauchy sequences is an equivalence relation. * *(p. 102)*

$\langle x_\nu\rangle$ is equivalent to $\langle x_\nu\rangle$ since the differences $x_\nu - x_\nu$ are identically zero.

If $\langle x_\nu\rangle$ is equivalent to $\langle y_\nu\rangle$, then by definition $x_\nu - y_\nu \to 0$, which we take to mean that for every $U \in \mathscr{N}(0)$ there is $t(U) \in \mathbb{N}$ such that for all $\nu \geq t(U)$ we have $x_\nu - y_\nu \in U$. To show that $\langle y_\nu\rangle$ is also equivalent to $\langle x_\nu\rangle$, let $U \in \mathscr{N}(U)$ be given and find a subset $V \in \mathscr{N}(0)$ with $V = -V$. For $\nu \geq t(V)$ we have $x_\nu - y_\nu \in V = -V$, so $y_\nu - x_\nu \in V \subseteq U$.

Now suppose $\langle x_\nu\rangle$ is equivalent to $\langle y_\nu\rangle$ and $\langle y_\nu\rangle$ is equivalent to $\langle z_\nu\rangle$. To show $\langle x_\nu\rangle$ is equivalent to $\langle y_\nu\rangle$, let $U \in \mathscr{N}(0)$ be given, and let $V \in \mathscr{N}(0)$ be such that $V + V \subseteq U$. By assumption, there are numbers $t(V)$, $t'(V) \in \mathbb{N}$ such that for $\nu \geq t(V)$ we have $x_\nu - y_\nu \in V$ and for $\nu \geq t'(V)$ we have $y_\nu - z_\nu \in V$. For $\nu \geq \max\{t(V), t'(V)\}$ we have $x_\nu - z_\nu = (x_\nu - y_\nu) + (y_\nu - z_\nu) \in V + V \subseteq U$.

If $\langle x_\nu\rangle$, $\langle y_\nu\rangle$ are Cauchy sequences, so is $\langle x_\nu + y_\nu\rangle$, and its class in $\hat{G}$ depends only on the classes of $\langle x_\nu\rangle$ and $\langle y_\nu\rangle$.

Let $U \in \mathscr{N}(0)$, and let $V \in \mathscr{N}(0)$ be such that $V + V \subseteq U$. Since $\langle x_\nu\rangle$ and $\langle y_\nu\rangle$ are Cauchy, there are numbers $s(V)$ and $s'(V)$ such that $x_\mu - x_\nu \in V$ for all $\mu, \nu \geq s(V)$ and $y_\mu - y_\nu \in V$ for all $\mu, \nu \geq s'(V)$. Then for all $\mu, \nu \geq \max\{s(V), s'(V)\}$ we have $(x_\mu + y_\mu) - (x_\nu + y_\nu) = (x_\mu - x_\nu) + (y_\mu - y_\nu) \in V + V \subseteq U$. As U was arbitrary, $\langle x_\nu + y_\nu\rangle$ is Cauchy.

If $\langle x'_\nu\rangle$ represents the same class as $\langle x_\nu\rangle$, so that $x_\nu - x'_\nu \to 0$, then $\langle x_\nu + y_\nu\rangle$ and $\langle x'_\nu + y_\nu\rangle$ are equivalent, since $(x_\nu + y_\nu) - (x'_\nu + y_\nu) = (x_\nu - x'_\nu) + (y_\nu - y_\nu) = x_\nu - x'_\nu \to 0$. Similarly, if $\langle y'_\nu\rangle$ represents the same class as $\langle y_\nu\rangle$, then $\langle x'_\nu + y_\nu\rangle$ and $\langle x'_\nu + y'_\nu\rangle$ are equivalent, so by transitivity $\langle x_\nu + y_\nu\rangle$ and $\langle x'_\nu + y'_\nu\rangle$ are equivalent.

Similarly, if $\langle x_\nu\rangle$ is a Cauchy sequence, then $\langle -x_\nu\rangle$ is a Cauchy sequence whose class in $\hat{G}$ depends only on that of $\langle x_\nu\rangle$. *

This and the next are very easy, but necessary to show $\hat{G}$ is a group. Let $U \in \mathscr{N}(0)$ be given; since $\langle x_\nu\rangle$ is Cauchy, there is $s(U) \in \mathbb{N}$ such that $\mu, \nu \geq s(U)$ implies $x_\mu - x_\nu \in U$. But $(-x_\nu) - (-x_\mu) = -(x_\nu - x_\mu) = x_\mu - x_\nu \in U$ then, for all ν, $\mu \geq s(U)$. As U was arbitrary, $\langle -x_\nu\rangle$ is Cauchy.

If $\langle x'_\nu\rangle$ represents the same class as $\langle x_\nu\rangle$, so that $x_\nu - x'_\nu \to 0$, then $(-x_\nu) - (-x'_\nu) \to 0$ as well; for given any $U \in \mathscr{N}(0)$ we may find a smaller $V = -V \in \mathscr{N}(0)$ and some $t(V)$ such that for all $\nu \geq t(V)$ we have $x_\nu - x'_\nu \in V = -V$, so $(-x_\nu) - (-x'_\nu) = -(x_\nu - x'_\nu) \in V \subseteq U$ as well.

*$\langle 0\rangle$ is a Cauchy sequence.**

This is trivial, since all differences are zero.

Hence we have an addition in $\hat{G}$ with respect to which $\hat{G}$ is an abelian group.

By the last two facts on independence of representatives, it will be enough to show the set of Cauchy sequences in G forms an Abelian group. But this easily follows from the facts that this group is defined as a subgroup of the product group $G^{\mathbb{N}}$ and that the abelian group identities hold componentwise:

$$\big(\langle x_\nu\rangle + \langle y_\nu\rangle\big) + \langle z_\nu\rangle = \langle x_\nu + y_\nu\rangle + \langle z_\nu\rangle = \big\langle (x_\nu + y_\nu) + z_\nu\big\rangle = \big\langle x_\nu + (y_\nu + z_\nu)\big\rangle = \langle x_\nu\rangle + \langle y_\nu + z_\nu\rangle = \langle x_\nu\rangle + \big(\langle y_\nu\rangle + \langle z_\nu\rangle\big);$$
$$\langle x_\nu\rangle + \langle 0\rangle = \langle x_\nu + 0\rangle = \langle x_\nu\rangle;$$
$$\langle x_\nu\rangle + \langle -x_\nu\rangle = \big\langle x_\nu + (-x_\nu)\big\rangle = \langle 0\rangle;$$
$$\langle x_\nu\rangle + \langle y_\nu\rangle = \langle x_\nu + y_\nu\rangle = \langle y_\nu + x_\nu\rangle = \langle y_\nu\rangle + \langle x_\nu\rangle.$$

For each $x \in G$ the class of the constant sequence $\langle x\rangle$ is an element $\phi(x)$ of $\hat{G}$, and $\phi\colon G \to \hat{G}$ is a homomorphism of abelian groups. [The kernel of ϕ is the subgroup $\bigcap \mathscr{N}(0)$ of (10.1).]

This may be too obvious to bother with, but we do it anyway. Constant sequences are Cauchy because the differences $x - x = 0$ of $\langle x\rangle$ approach (are) 0. ϕ is obviously a homomorphism: $\phi(0)$ is the equivalence class of $\langle 0\rangle$, which is the zero of $\hat{G}$; $\langle -x\rangle = -\langle x\rangle$, so taking classes, $\phi(-x) = -\phi(x)$; and $\langle x+y\rangle = \langle x\rangle + \langle y\rangle$, so taking classes, $\phi(x+y) = \phi(x) + \phi(y)$. We have $x \in \ker(\phi)$ just if $\langle x\rangle$ is in the class of $\langle 0\rangle$, so that $x = x - 0 \to 0$ as the indices increase. But this means that for each $U \in \mathscr{N}(0)$ there is $t(U)$ such that for $\nu \geq t(U)$ we have $x \in U$. Since x is independent of ν, that just means $x \in U$, so $x \in \bigcap \mathscr{N}(0)$.

*There is a natural topology making $\hat{G}$ a topological group.**

For each $U \in \mathscr{N}_G(0)$, define $\hat{U} \subseteq \hat{G}$ to be the set of all elements $\hat{x} \in \hat{G}$ such that all representatives $\langle x_\nu\rangle$ of $\hat{x}$ are "eventually in" U:

$$\hat{U} := \Big\{ \hat{x} \in \hat{G} \;:\; \forall \langle x_\nu\rangle \in \hat{x}\ \exists \mathrm{N} \in \mathbb{N}\ \forall \nu \geq \mathrm{N}\ (x_\nu \in U) \Big\}.[1]$$

Note that for all $U, V \in \mathscr{N}_G(0)$ we have $\hat{0} \in \widehat{U \cap V} = \hat{U} \cap \hat{V}$. Then if we write let $\hat{\mathscr{N}} = \{\hat{U} : U \in \mathscr{N}_G(0)\}$ and take all translates in $\hat{G}$, these sets together generate a unique topology on $\hat{G}$ for which $\hat{\mathscr{N}}$ is a neighborhood basis of $\hat{0}$.DO THIS [2]

Suppose $\hat{x}, \hat{y} \in \hat{G}$ are such that their sum lies in an open set $W \subseteq \hat{G}$. By our definition of the topology, there is a $\hat{U} \in \hat{\mathscr{N}}$ such that $(\hat{x} + \hat{y}) + \hat{U} \subseteq W$. By our proof of (10.1.i), there is $V \in \mathscr{N}_G(0)$ such that $V + V \subseteq U$. If $\langle x_\nu\rangle\,\langle y_\nu\rangle$ are Cauchy sequences representing elements of $\hat{V}$, then there is $\mathrm{N} \in \mathbb{N}$ sufficiently large that for all $\nu \geq \mathrm{N}$ we have $x_\nu, y_\nu \in V$, and hence $x_\nu + y_\nu \in U$. Thus $\hat{V} + \hat{V} \subseteq \hat{U}$, so addition takes $\big(\hat{x} + \hat{V}\big) \times \big(\hat{y} + \hat{V}\big)$ into $(\hat{x} + \hat{y}) + \hat{U} \subseteq W$ and hence is continuous.

Similarly, any open set about $-\hat{x}$, contains a basic open set $-\hat{x} + \hat{U}$. By our proof of (10.1.i) again, there is a $V = -V \in \mathscr{N}_G(0)$ such that $V \subseteq U$. Then the opposite of any sequence eventually in V is also eventually in V, so $-\hat{V} = \hat{V}$, and $-\big(\hat{x} + \hat{V}\big) = -\hat{x} + \hat{V} \subseteq -\hat{x} + \hat{U}$, so inversion is also continuous.

*$\phi\colon G \to \hat{G}$ is continuous.**

Let $x \in G$ and consider a basic open neighborhood $\phi(x) + \hat{U}$. If $u \in U \in \mathscr{N}_G(0)$, there is some $V \in \mathscr{N}_G(0)$ such that $u + V \subseteq U$. Thus, if $\langle y_\nu\rangle$ is a Cauchy sequence equivalent to $\langle u\rangle$, we must eventually have $y_\nu - u \in V$, so that y_ν is eventually in $u + V \subseteq U$. This shows $\phi(u) \in \hat{U}$. It follows that $\phi(x + U) \subseteq \phi(x) + \hat{U}$, showing ϕ is continuous.

[1] We do have to stipulate eventual containment for *all* sequences in a class: in $\langle \mathbb{Q}, +\rangle$, for instance, the Cauchy sequences $\langle \frac{n-1}{n}\rangle$ and $\langle 1\rangle$ are equivalent, but the former is always in the open ball of radius 1 about 0, while the latter never is.

It took me a while to decide between this definition and several other less fruitful possibilities, and I eventually settled on this one as a result of Gerald A. Edgar's answer at http://math.stackexchange.com/questions/192808/topology-induced-by-the-completion-of-a-topological-group.

[2] Brian M. Scott's answer at http://math.stackexchange.com/questions/67259/inquiry-regarding-neighborhood-bases elaborates how this works. But there is a question as to how to prove that in the topology generated by the translates of $\hat{\mathscr{N}}$, these sets are actually neighborhoods: http://math.stackexchange.com/questions/234803/translating-a-neighborhood-basis-of-a-topological-group.

*If G is first countable or Hausdorff, then $\hat{G}$ is first countable or Hausdorff, respectively.**

If $\langle U_i\rangle_{i\in\mathbb{N}}$ is a countable neighborhood basis of 0 in G, we claim $\langle \hat{U}_i\rangle$ will be a countable neighborhood basis of $\hat{0}$ in $\hat{G}$. Indeed, for any $V\in\mathcal{N}_G(0)$ there is $U_i\subseteq V$, so for any $\hat{V}\in\hat{\mathcal{N}}$ there is $\hat{U}_i\subseteq\hat{V}$. By translation, we have countable neighborhood bases at every point of $\hat{G}$.

Given two distinct points of $\hat{G}$, finding disjoint neighborhoods of the two is equivalent, by translation, to finding disjoint neighborhoods of $\hat{0}$ and their difference $\hat{x}$. Let $\langle 0\rangle$ and $\langle x_\nu\rangle$ be representatives. Since they are assumed inequivalent, it follows there is some $U\in\mathcal{N}_G(0)$ such that the differences x_ν are not eventually in U, so that $\hat{x}\notin\hat{U}$. Using the proof of (10.1.i), find $V\in\mathcal{N}_G(0)$ such that $V+V\subseteq U$. Now we claim the basic neighborhoods $\hat{V}\ni\hat{0}$ and $\hat{x}+\hat{V}\ni\hat{x}$ are disjoint. If not, there would be $\hat{y}$ in their intersection, so that $\hat{y}\in\hat{V}$ and $\hat{y}\in\hat{x}+\hat{V}$, or equivalently $\hat{y}-\hat{x}\in\hat{V}$. But then from our proof $\hat{G}$ is a topological group we would have $\hat{x}=\hat{y}+(\hat{y}-\hat{x})\in\hat{V}+\hat{V}\subseteq\hat{U}$, after all.

*If G is first countable and Hausdorff, then $\hat{G}$ is complete in the sense that all Cauchy sequences in $\hat{G}$ converge to points of $\hat{G}$.**[3]

Let $\langle U_i\rangle_{i\in\mathbb{N}}$ be a countable neighborhood basis of 0 in G. By the proof of (10.1.i), we may assume $U_i=-U_i$ and $U_{i+1}+U_{i+1}\subseteq U_i$ for all n, so that the same will hold of $\langle\hat{U}_i\rangle$.

Let $\langle\hat{x}_n\rangle$ be a Cauchy sequence in $\hat{G}$, and select a representative $\langle x_{n,\nu}\rangle$ for each $\hat{x}_n$. For each n, since the sequence $\langle x_{n,\nu}\rangle$ is Cauchy, there is a number Λ_n such that when ν, $\mu\geq\Lambda_n$, we have $x_{n,\nu}-x_{n,\mu}\in U_{n+2}$. Since the sequence $\langle\hat{x}_n\rangle$ is Cauchy, there is for each $i\in\mathbb{N}$ an $N_i\in\mathbb{N}$ such that for all n, $m\geq N_i$ we have $\hat{x}_n-\hat{x}_m\in\hat{U}_{i+2}$. That in turn implies we have $x_{n,\nu}-x_{m,\nu}\in U_{i+2}$ for all sufficiently large ν.

Now for each $\nu\in\mathbb{N}$, let $y_\nu=x_{\nu,\Lambda_\nu}\in G$. We claim that $\langle y_\nu\rangle$ is a Cauchy sequence. Indeed, if n, $m\geq N_i$, there are arbitrarily large ν such that $x_{n,\nu}-x_{m,\nu}\in U_{i+2}$, in particular such that $\nu\geq\max\{\Lambda_n,\Lambda_m\}$, and then

$$y_n-y_m=x_{n,\Lambda_n}-x_{m,\Lambda_m}=\underbrace{(x_{n,\Lambda_n}-x_{n,\nu})}_{\nu\geq\Lambda_n}+(x_{n,\nu}-x_{m,\nu})+\underbrace{(x_{m,\nu}-x_{m,\Lambda_m})}_{\nu\geq\Lambda_m}\in U_{i+2}+U_{i+2}+U_{i+2}\subseteq U_i. \qquad (10.1)$$

Let $\hat{y}\in\hat{G}$ be the equivalence class of $\langle y_\nu\rangle$. Our goal is to show $\hat{x}_n\to\hat{y}$, or in other words that for each $\hat{U}_i$, we have $\hat{y}-\hat{x}_n\in\hat{U}_i$ for all sufficiently large n. In other words, we want to show that if n is big enough then each representative $\langle z_{n,\nu}\rangle$ of $\hat{y}-\hat{x}_n$ is in U_i for all high enough ν. It will actually be enough to find M_i such that for each $n\geq M_i$, the representative $\langle w_{n,\nu}\rangle=\langle y_\nu-x_{n,\nu}\rangle$ is eventually in U_{i+1}; for then, given $n\geq M_i$ and any other representative $\langle z_{n,\nu}\rangle$, we will have $z_{n,\nu}-w_{n,\nu}$ eventually in U_{i+1}, so that $z_{n,\nu}=(z_{n,\nu}-w_{n,\nu})+w_{n,\nu}$ is eventually in $U_{i+1}+U_{i+1}\subseteq U_i$.

$M_i=N_{i+2}$ from above will work, for if $m\geq N_{i+1}$ and $\nu\geq\Xi_m:=\max\{\Lambda_m,N_{i+1}\}$, then we indeed have

$$y_\nu-x_{m,\nu}=(y_\nu-y_m)+(y_m-x_{m,\nu})=\underbrace{(y_\nu-y_m)}_{\text{Eq. 10.1: } m,\nu\geq N_{i+1}}+\underbrace{(x_{m,\Lambda_m}-x_{m,\nu})}_{\nu\geq\Xi_m\geq\Lambda_m}\in U_{i+1}+U_{i+2}\subseteq U_i.$$

If H is another abelian group and $f\colon G\to H$ a continuous homomorphism, then the image under f of a Cauchy sequence in G is a Cauchy sequence in H, and therefore f induces a homomorphism $\hat{f}\colon\hat{G}\to\hat{H}$, which is continuous.

Let $\langle x_\nu\rangle$ be a Cauchy sequence in G and let $U\in\mathcal{N}_H(0)$ be given. Since $f(0)=0$, by continuity, there is $V\in\mathcal{N}_G(0)$ such that $f(V)\subseteq U$. By assumption there is $s(V)\in\mathbb{N}$ such that $x_\mu-x_\nu\in V$ for all $\mu,\nu\geq s(V)$. Then $f(x_\mu)-f(x_\nu)=f(x_\mu-x_\nu)\in f(V)\subseteq U$. Thus $\big\langle f(x_\nu)\big\rangle$ is Cauchy.

To show $\hat{f}$ is well defined, we must show it preserves equivalence. But if $\langle x_\nu\rangle$ and $\langle x'_\nu\rangle$ are equivalent, then there is $t(V)\in\mathbb{N}$ such that $x_\nu-x'_\nu\in V$ for $\nu\geq t(V)$, so $f(x_\nu)-f(x'_\nu)=f(x_\nu-x'_\nu)\in f(V)\subseteq U$, showing $\big\langle f(x_\nu)\big\rangle$ and $\big\langle f(x'_\nu)\big\rangle$ are equivalent.

It is obvious $\hat{f}$ is a homomorphism because operations on Cauchy sequence are defined componentwise and $\hat{f}$ is induced by applying f componentwise to Cauchy sequences.

[3] This is also a special case of a general result in Bourbaki's *General Topology* Part 1 (Chapter III, §3.5, Theorem I) regarding completions (in terms of Cauchy filters) with respect to the right uniformity, but I have not attempted to translate that proof into our language.

Our case could also be proved using the theorem that a first-countable, Hausdorff topological group is metrizable; see http://u.math.biu.ac.il/~megereli/mickey25.pdf.

To prove continuity we use the topology on the completion we defined above. Let a basic neighborhood $\hat{f}(\hat{x})+\hat{V}$ in $\hat{H}$ be given, where $V \in \mathcal{N}_H(0)$ Since f is continuous and $f(0)=0$, there is $U \in \mathcal{N}_G(0)$ such that $f(U) \subseteq V$. Then for each Cauchy sequence $\langle u_\nu \rangle$ eventually in U, the image sequence $\langle f(u_\nu)\rangle$ is eventually in V, so that $\hat{f}(\hat{U}) \subseteq \hat{V}$ and therefore $\hat{f}(\hat{x}+\hat{U}) \subseteq \hat{f}(\hat{x})+\hat{V}$, showing $\hat{f}$ is continuous.

Thus we have a sequence of subgroups

$$G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n \supseteq \cdots$$

and $U \subseteq G$ is a neighborhood of 0 if and only if it contains some G_n.

...

In fact if $g \in G_n$ then $g + G_n$ is a neighborhood of g; since $g + G_n \subseteq G_n$ this shows G_n is open. [Prove that taking the $x + G_n$ as a neighborhood basis of x defines a topology on G making G a topological group.] (pp. 102–3)*

The fact that the authors prove the G_n are open shows they are using the Bourbaki definition of neighborhoods:[4] to wit, given a topology on X, a set $N \subseteq X$ is defined to be a *neighborhood* of x just if there is an open set $U \subseteq X$ with $x \in U \subseteq N$. A *fundamental system of neighborhoods* (neighborhood basis) of a point $x \in X$ is then a collection $\mathscr{B}$ of subsets of X such that the neighborhoods of x are precisely the sets containing a member of $\mathscr{B}$. On the other hand, given collections $\mathscr{B}(x)$ of subsets of X, one for each $x \in X$, the following axioms guarantee that they define a unique topology under which each $\mathscr{B}(x)$ is a neighborhood basis for x:

1. if $N, N' \in \mathscr{B}(x)$, there there is $N'' \in \mathscr{B}(x)$ with $N'' \subseteq N \cap N'$;
2. x is in each member of $\mathscr{B}(x)$;
3. if $N \in \mathscr{B}(x)$, there is $N' \in \mathscr{B}(x)$ such that for all $y \in N'$ there exists $N'' \in \mathscr{B}(y)$ with $N'' \subseteq N$

   ("any neighborhood of x is also a neighborhood of all points sufficiently near x").

It is not hard to see that that the set of translates $x + G_n$ satisfies these axioms: 1. for $m \leq n$, evidently $x + G_n \subseteq (x + G_m) \cap (x + G_n)$; 2. obviously $x \in x + G_n$; 3. for all $y \in x + G_n$ we have $y + G_n = x + G_n + G_n = x + G_n$. Thus we have a well-defined topology on G. Inversion is continuous, since it sends $x + G_n \longleftrightarrow -x + G_n$, and addition is continuous since, given a basic neighborhood $x+y+G_n$, addition sends the neighborhood $(x+G_n)\times(y+G_n) \subseteq G \times G$ of $\langle x, y\rangle$ into it.

If $0 \to G' \overset{i}{\hookrightarrow} G \xrightarrow{p} G'' \to 0$ is an exact sequence of groups and $G_n \subseteq G$ is a subgroup, then

$$0 \to \frac{G'}{G' \cap G_n} \xrightarrow{\iota} \frac{G}{G_n} \xrightarrow{\pi} \frac{G''}{p(G_n)} \to 0$$

is an exact sequence. (pp. 104–5)*

The kernel of $G' \hookrightarrow G \twoheadrightarrow G/G_n$ is $G' \cap G_n$, so ι is defined and injective. The composition $G \overset{p}{\twoheadrightarrow} G'' \twoheadrightarrow G''/p(G_n)$ is surjective and takes the same value on any member of a class $g + G_n$, so π is defined and surjective. Since $p \circ i = 0$, so also $\pi \circ \iota = 0$. Now suppose $g + G_n \in \ker(\pi)$. Then $p(g) \in p(G_n)$, so there is $h \in G_n$ with $p(g-h) = 0$. By exactness of the original sequence, $g - h \in G'$. Now $\iota\big(g - h + (G' \cap G_n)\big) = g + G_n$, so the sequence is exact at G/G_n.

[W]e can apply (10.3) with $G' = G_n$[;] then $G'' = G/G_n$ has the discrete topology so that $\hat{G}'' = G''$.

From p. 103 recall that G_n is open, so its translates $g + G_n$ are open. Since these become points in G'', it follows G'' is discrete. Using the neighborhood $\{0\}$ of 0 in G'', it follows that for every Cauchy sequence $\langle \bar{x}_\nu \rangle$ in G'', there is some $s(\{0\})$ such that for all $\mu, \nu \geq s(\{0\})$ we have $\bar{x}_\mu - \bar{x}_\nu = 0$; that is, every Cauchy sequence is eventually constant. But a sequence that is eventually $\bar{x}$ is equivalent to the constant sequence $\langle \bar{x} \rangle$, so the canonical map $G'' \to \hat{G}''$ is an isomorphism.

Since the $\mathfrak{a}^n$ are ideals it is not hard to check that with [the $\mathfrak{a}$-topology] A is a topological ring, *i.e., that the ring operations are continuous.*

[4] Nicolas Bourbaki, *General Topology* Part 1, Definitions 4 and 5, pp. 18–21.

We have shown above that A is a topological group under addition; it remains to show multiplication is continuous. But multiplication maps the product neighborhood $(x+\mathfrak{a}^n)\times(y+\mathfrak{a}^n)$ of $\langle x, y\rangle$ into $xy+x\mathfrak{a}^n+y\mathfrak{a}^n+\mathfrak{a}^{2n}\subseteq xy+\mathfrak{a}^n$.

The completion $\hat{A}$ of A is again a topological ring[.]

In the light of (10.4), the unspecified topology in question should be given by letting the $x+\widehat{\mathfrak{a}^n}$ be a neighborhood basis for each $x\in\hat{A}$. Because $\langle\widehat{\mathfrak{a}^n}\rangle$ is a decreasing sequence of subgroups, $\hat{A}$ a topological group under addition. Each $\widehat{\mathfrak{a}^n}$ is an ideal, since it is the contraction of the ideal $\prod_{j=1}^{\infty}\mathfrak{a}^n/(\mathfrak{a}^j\cap\mathfrak{a}^n)$ in the product ring $\prod_{j=1}^{\infty}A/\mathfrak{a}^j$. Thus, as with A, multiplication $\hat{A}\times\hat{A}\to\hat{A}$ takes the neighborhood $(x+\widehat{\mathfrak{a}^n})\times(y+\widehat{\mathfrak{a}^n})$ of $\langle x, y\rangle$ into $xy+x\widehat{\mathfrak{a}^n}+y\widehat{\mathfrak{a}^n}+\widehat{\mathfrak{a}^{2n}}\subseteq xy+\widehat{\mathfrak{a}^n}$, so that $\hat{A}$ is a topological ring.

$\phi\colon A\to\hat{A}$ is a continuous ring homomorphism, whose kernel is $\bigcap\mathfrak{a}^n$.

By p. 102, ϕ is a group homomorphism with kernel as stated; multiplicativity follows because $\langle x\rangle\langle y\rangle=\langle xy\rangle$, and taking classes gives $\phi(x)\phi(y)=\phi(xy)$. As for continuity, for $x\in\mathfrak{a}^n$ we have $\phi(x)$ represented in $\prod_{j=1}^{\infty}A/\mathfrak{a}^j$ by $\langle x+\mathfrak{a}^j\rangle\in\prod_{j=1}^{\infty}\mathfrak{a}^n/(\mathfrak{a}^j\cap\mathfrak{a}^n)$, so that $\phi(\mathfrak{a}^n)\subseteq\widehat{\mathfrak{a}^n}$; thus for any $y\in A$ and any basic neighborhood $\phi(y)+\widehat{a^n}$ of $\phi(y)\in\hat{A}$ we have $\phi(y+\mathfrak{a}^n)\subseteq\phi(y)+\widehat{\mathfrak{a}^n}$.

Likewise for an A-module M: take $G=M$, $G_n=\mathfrak{a}^nM$. This defines the $\mathfrak{a}$-topology on M, [making M a continuous A-module.]

Because G_n is a decreasing sequence of additive subgroups, this does indeed define a topology on M. To see continuity, note that given a basic neighborhood $xm+\mathfrak{a}^nM$ of $xm\in M$, the map $A\times M\to M$ takes the open neighborhood $(x+\mathfrak{a}^n)\times(m+\mathfrak{a}^nM)$ of $\langle x, m\rangle$ into $(x+\mathfrak{a}^n)(m+\mathfrak{a}^nM)=xm+\mathfrak{a}^nm+x\mathfrak{a}^nM+\mathfrak{a}^{2n}M\subseteq xm+\mathfrak{a}^nM$.

[T]he completion $\hat{M}$ of M is a topological $\hat{A}$-module.

The topology on $\hat{M}$ is defined, as before by the basic neighborhoods $\widehat{\mathfrak{a}^nM}$ of 0. Here we note that the module multiplication $\hat{A}\times\hat{M}\to\hat{M}$ is left undefined. For elements $\langle x_j+\mathfrak{a}^j\rangle\in\hat{A}$ and $\langle m_j+\mathfrak{a}^jM\rangle\in\hat{M}$, define their product as $\langle x_j+\mathfrak{a}^j\rangle\cdot\langle m_j+\mathfrak{a}^jM\rangle=\langle x_jm_j+\mathfrak{a}^jM\rangle$. To see this works, first note that $x_{j+1}m_{j+1}-x_jm_j=x_{j+1}(m_{j+1}-m_j)+(x_{j+1}-x_j)m_j\in x_{j+1}\mathfrak{a}^jM+\mathfrak{a}^jm_j\subseteq\mathfrak{a}^jM$,[5] so the resulting sequence is in $\hat{M}$. Second, if we replaced x_j with $x_j'\in x_j+\mathfrak{a}^j$, then we would have $(x_j'-x_j)m_j\in\mathfrak{a}^jM$, and similarly if we replaced m_j with $m_j'\in m_j+\mathfrak{a}^jM$, so that this multiplication is well defined.

Now, observe $\widehat{\mathfrak{a}^k}\widehat{\mathfrak{a}^nM}\subseteq\widehat{\mathfrak{a}^{k+n}}M$. Indeed, if $x_j\in\mathfrak{a}^k$ and $m_j\in\mathfrak{a}^nM$ for all j, then $x_jm_j\in\mathfrak{a}^{k+n}M$ for all j, so that the sequence elements $x_jm_j+\mathfrak{a}^jM$ are in $\mathfrak{a}^{k+n}M/(\mathfrak{a}^jM+\mathfrak{a}^{k+n}M)$. For continuity, taking $x\in\hat{A}$ and $m\in\hat{M}$, and considering the basic neighborhood $xm+\widehat{\mathfrak{a}^nM}$ of their product, note that multiplication takes $(x+\widehat{\mathfrak{a}^n})\times(m+\widehat{\mathfrak{a}^nM})$ to $xm+\widehat{\mathfrak{a}^n}m+x\widehat{\mathfrak{a}^nM}+\widehat{\mathfrak{a}^n}\widehat{\mathfrak{a}^nM}\subseteq xm+\widehat{\mathfrak{a}^nM}$.

If $f\colon M\to N$ is any A-module homomorphism, [... f] defines $\hat{f}\colon\hat{M}\to\hat{N}$.

Let $\hat{f}\big(\langle m_j+\mathfrak{a}^jM\rangle\big)=\langle f(m_j)+\mathfrak{a}^jN\rangle$. This is an element of $\hat{N}$ since $f(m_{j+1})-f(m_j)=f(m_{j+1}-m_j)\in f(\mathfrak{a}^{j+1}M)\subseteq\mathfrak{a}^{j+1}N$. To see the map is well defined, note that if $m_j'-m_j\in\mathfrak{a}^jM$, then $f(m_j')\in f(m_j)+\mathfrak{a}^jN$.

$\hat{f}$ is a group homomorphism because it is defined in terms of the homomorphisms $\bar{f}\colon M/\mathfrak{a}^jM\to N/\mathfrak{a}^jN$ given by $\bar{f}(m+\mathfrak{a}^jM)=f(m)+\mathfrak{a}^jN$. It is a module homomorphism because $\hat{f}\Big(\langle x_jm_j+\mathfrak{a}^jM\rangle\Big)=\langle x_jf(m_j)+\mathfrak{a}^jN\rangle=\langle x_j+\mathfrak{a}^j\rangle\hat{f}\big(\langle m_j+\mathfrak{a}^jM\rangle\big)$ whenever $\langle x_j+\mathfrak{a}^j\rangle\in\hat{A}$ and $\langle m_j+\mathfrak{a}^jM\rangle\in\hat{M}$.

$\hat{f}$ is also continuous, because $\hat{f}\big(\widehat{\mathfrak{a}^nM}\big)\subseteq\widehat{A^nN}$, as $\hat{f}$ takes sequences of elements of $\mathfrak{a}^nM/(\mathfrak{a}^jM+\mathfrak{a}^nM)$ to sequences of elements of $\mathfrak{a}^nN/(\mathfrak{a}^jN+\mathfrak{a}^nN)$.

*If C is a ring, and $A=C[x_1,\ldots,x_n]$ a polynomial ring, and $\mathfrak{a}=(x_1,\ldots,x_n)$ the ideal of polynomials with no constant term, then $\hat{A}=C[[x_1,\ldots,x_n]]$, the ring of formal power series.**

This generalizes Example 1) on this page.

[5] Thanks to Jude Gaudot sp? for pointing out a misindexing in the earlier versions here.

$\mathfrak{a}^m \lhd A$ is the set of polynomials with no terms of degree $< m$. If we let $\mathfrak{b} = (x_1, \ldots, x_n)$ in $B := C[[x_1, \ldots, x_n]]$, then $\mathfrak{b}^m$ is the set of power series of order $\geq m$. Since every class modulo $\mathfrak{b}^m$ is represented by the (polynomial) class of its truncation below degree m, we have isomorphisms $B/\mathfrak{b}^m \cong A/\mathfrak{a}^m$ compatible with the maps $m+1 \mapsto m$, and so $\hat{B} \cong \hat{A}$. But the natural map $B \to \hat{B}$ is an isomorphism: it is injective since $\bigcap \mathfrak{b}^m = 0$, and surjective because if p_m is the sum of terms of b_{m+1} of total degree n and $\langle b_m + \mathfrak{b}^m \rangle \in \hat{B}$, then $\sum p_j + \mathfrak{b}^m = \sum_{j<m} p_m + \mathfrak{b}^m = b_m + \mathfrak{b}^m$ for each m.

[A]$llstablea—filtrationsonMdeterminethesametopologyonM, namelythea—topology.(p.106)$

The proof of (10.6) shows any stable $\mathfrak{a}$-filtrations $\langle M_n \rangle$ and $\langle M'_n \rangle$ have bounded difference, so we may fix n_0 such that for all $n \in N$ we have $M_{n+n_0} \subseteq M'_n$ and $M'_{n+n_0} \subseteq M_n$. Let $x \in M$. For any $\langle M_n \rangle$-basic neighborhood $x + M_n$ each point $y \in x + M_n$ has a $\langle M'_n \rangle$-basic neighborhood $y + M'_{n+n_0} \subseteq y + M_n = x + M_n$, so $x + M_n$ is open in the $\langle M'_n \rangle$-topology, and thus the $\langle M'_n \rangle$-topology contains the $\langle M_n \rangle$-topology. The converse holds by symmetry. Thus all stable $\mathfrak{a}$-filtrations on M induce the same topology the stable filtration $\langle \mathfrak{a}^n M \rangle$ does, namely the $\mathfrak{a}$-topology.

Let A be a ring (not graded), $\mathfrak{a}$ an ideal of A. Then we can form a graded ring $A^* = \bigoplus_{n=0}^{\infty} \mathfrak{a}^n$. Similarly, if M is an A-module and M_n is an $\mathfrak{a}$-filtration of M, then $M^* = \bigoplus_n M_n$ is a graded A^*-module, since $\mathfrak{a}^m M_n \subseteq M_{m+n}$. (p. 107)

We can afford some clarification of what is going on here. Writing $A_n = \mathfrak{a}^n$, we have $A^* = \bigoplus A_n$, and our multiplication takes $A_m \times A_n \to A_{m+n}$. The slightly confusing thing is that there also is an $\mathfrak{a}^m \subseteq A = A_0$, for instance, and if we multiply that by A_n, we get a subset of $\mathfrak{a}^{m+n} \subseteq A_n$. So what the book is saying is that if we multiply A_m by the n^{th} summand M_n of M^*, we get a subset of the $(m+n)^{th}$ summand M_{m+n}; we are not considering, say, $M_n \subseteq M$ in the zeroth summand of M^*.

Proposition 10.3$\frac{1}{2}$*. *Using (10.3) or otherwise it is clear that $\mathfrak{a}$-adic completion commutes with finite direct sums. (p. 108)*

By induction it will suffice to show $\mathfrak{a}$-adic completion distributes over binary direct sums. It is possible to use (10.3) and the diagrammatic definition of direct sums to do this, but easier to just give an explicit isomorphism. The $\mathfrak{a}$-adic filtration on $M \oplus N$ is $\langle \mathfrak{a}^n M \oplus \mathfrak{a}^n N \rangle$. It is clear $\big\langle \langle x_n + \mathfrak{a}^n M \rangle, \langle y_n + \mathfrak{a}^n N \rangle \big\rangle \mapsto \big\langle \langle x_n, y_n \rangle + \mathfrak{a}^n (M \oplus N) \big\rangle$ gives a well-defined, homomorphic bijection $\phi \colon \hat{M} \oplus \hat{N} \longleftrightarrow \widehat{M \oplus N}$ since we have natural isomorphisms $(M/\mathfrak{a}^n M) \oplus (N/\mathfrak{a}^n N) \xrightarrow{\sim} (M \oplus N)/\mathfrak{a}^n (M \oplus N)$ and $\langle x_{n+1}, y_{n+1} \rangle \equiv \langle x_n, y_n \rangle \; \big(mod\, \mathfrak{a}^n (M \oplus N)\big)$ if and only if $x_{n+1} \equiv x_n \pmod{\mathfrak{a}^n M}$ and $y_{n+1} \equiv y_n \pmod{\mathfrak{a}^n N}$.

[I]$fF \cong A^n$ *we have* $\hat{A} \otimes_A F \cong \hat{F}$.

$$\hat{A} \otimes_A F \cong \hat{A} \otimes_A A^n = \hat{A} \otimes_A \bigoplus_{j=1}^{n} A \overset{(2.14.iii)}{\cong} \bigoplus_{j=1}^{n} (\hat{A} \otimes_A A) \overset{(2.14.iv)}{\cong} \bigoplus_{j=1}^{n} \hat{A} \overset{(10.3\frac{1}{2}*)}{\cong} \widehat{\bigoplus_{j=1}^{n} A} = \hat{F}$$

Given an A-module homomorphism $\phi \colon N \to F$, the following square commutes:

$$\begin{tikzcd}
\hat{A} \otimes_A N \arrow[r] \arrow[d] & \hat{A} \otimes_A F \arrow[d] \\
\hat{N} \arrow[r] & \hat{F}.*
\end{tikzcd}$$

The map around the upper-right is the composition

$$\hat{A} \otimes_A N \to \hat{A} \otimes_A F \to \hat{A} \otimes_A \hat{F} \to \hat{A} \otimes_{\hat{A}} \hat{F} \to \hat{F} \quad \textit{taking}$$

$$\langle a_n + \mathfrak{a}^n \rangle \otimes x \mapsto \langle a_n + \mathfrak{a}^n \rangle \otimes \phi(x) \mapsto \langle a_n + \mathfrak{a}^n \rangle \otimes \big\langle \phi(x) + \mathfrak{a}^n F \big\rangle \mapsto \langle a_n + \mathfrak{a}^n \rangle \otimes \big\langle \phi(x) + \mathfrak{a}^n F \big\rangle \mapsto \big\langle a_n \phi(x) + \mathfrak{a}^n F \big\rangle,$$

and the map around the lower-left is the composition $\hat{A} \otimes_A N \to \hat{A} \otimes_A \hat{N} \to \hat{A} \otimes_{\hat{A}} \hat{N} \to \hat{N} \to \hat{F}$ given by

$$\langle a_n + \mathfrak{a}^n \rangle \otimes x \mapsto \langle a_n + \mathfrak{a}^n \rangle \otimes \langle x + \mathfrak{a}^n N \rangle \mapsto \langle a_n + \mathfrak{a}^n \rangle \otimes \langle x + \mathfrak{a}^n N \rangle \mapsto \langle a_n x + \mathfrak{a}^n N \rangle \mapsto \big\langle \phi(a_n x) + \mathfrak{a}^n F \big\rangle.$$

[In the following diagram, if the rows are exact, γ is surjective, and β is injective, then a] little diagram chasing proves that α is injective:

$$\begin{tikzcd}
\bar{N} \arrow[r, "\zeta"] \arrow[d, two heads, "\gamma"] & \bar{F} \arrow[r, "\eta"] \arrow[d, tail, "\beta"] & \bar{M} \arrow[r] \arrow[d, two heads, "\alpha"] & 0 \\
\hat{N} \arrow[r, "\epsilon"'] & \hat{F} \arrow[r, "\delta"'] & \hat{M}.
\end{tikzcd}$$

Suppose $\bar{m} \in \ker(\alpha)$. There is $\bar{f} \in \eta^{-1}(\bar{m})$, and $\delta\beta\bar{f} = \alpha\eta\bar{f} = 0$. Since the bottom row is exact, there is $\hat{n} \in \hat{N}$ with $\epsilon\hat{n} = \beta\bar{f}$, and since γ is surjective, there is $\bar{n} \in \gamma^{-1}(\hat{n})$. Now $\epsilon\gamma\bar{n} = \beta\zeta\bar{n} = \beta\bar{f}$, so by injectivity of β we get $\bar{f} = \zeta\bar{n}$, and thus $\bar{m} = \eta\bar{f} = \eta\zeta\bar{n} = 0$, showing α is injective.

[C]heck that $\bar{x}_m\bar{x}_n$ does not depend on the particular representatives chosen. [Here we have a ring A with ideal $\mathfrak{a}$ and are given $x_m \in \mathfrak{a}^m$, $x_n \in \mathfrak{a}^n$. We write $\bar{x}_m \in \mathfrak{a}^m/\mathfrak{a}^{m+1}$, $\bar{x}_n \in \mathfrak{a}^n/\mathfrak{a}^{n+1}$, $\bar{x}_m\bar{x}_n := \overline{x_m x_n} \in \mathfrak{a}^{m+n}/\mathfrak{a}^{m+n+1}$]* (p. 111)

As sets we have $(x_m + \mathfrak{a}^{m+1})(x_n + \mathfrak{a}^{n+1}) = x_m x_n + x_n\mathfrak{a}^{m+1} + x_m\mathfrak{a}^{n+1} + \mathfrak{a}^{m+n+2} \subseteq x_m x_n + \mathfrak{a}^{m+n+1}$.

Similarly, if M is an A-module and $\langle M_n\rangle$ is an $\mathfrak{a}$-filtration of M, …

$$G(M) = \bigoplus_{n=0}^{\infty} M_n/M_{n+1}$$

… is a graded $G(A)$-module in a natural way.

Let $a_k \in \mathfrak{a}^k$ and $x_n \in M_n$; since $\langle M_n\rangle$ is an $\mathfrak{a}$-filtration, $a_k x_n \in M_{n+k}$. Note that

$$(a_k + \mathfrak{a}^{k+1})(x_n + M_{n+1}) = a_k x_n + \mathfrak{a}^{k+1}x_n + a_k M_{n+1} + \mathfrak{a}^{k+1}M_{n+1} \subseteq a_k x_n + M_{n+k+1},$$

so for $\bar{a}_k \in \mathfrak{a}^k/\mathfrak{a}^{k+1}$ and $\bar{x}_n \in M_n/M_{n+1}$ we can define $\bar{a}_k\bar{x}_n := \overline{a_k x_n} \in M_{n+k}/M_{n+k+1}$ uniquely. Extend this definition by distributivity to a product $G(A) \times G(M) \to G(M)$, so that to finish checking $G(M)$ is a $G(A)$-module, it only remains to check $\bar{1}x = x$ and $(ab)x = a(bx)$ for a, $b \in A$ and for $x \in G(M)$. Using distributivity, we only need to check for homogeneous elements; but then it is obvious, for $\bar{1}\bar{x}_n = \overline{1x_n} = \bar{x}_n$ and

$$(\bar{a}_k\bar{b}_\ell)\bar{x}_n = \overline{a_k b_\ell}\,\bar{x}_n = \overline{a_k b_\ell x_n} = \bar{a}_k\overline{b_\ell x_n} = \bar{a}_k(\bar{b}_\ell\bar{x}_n) \quad \text{in } M_{k+\ell+n}/M_{k+\ell+n+1}$$

simply because the associative rule holds for the A-module M. To see $G(M)$ is a graded $G(A)$-module, note that by construction $G_k(A)G_n(M) = (\mathfrak{a}^k/\mathfrak{a}^{k+1})(M_n/M_{n+1}) \subseteq M_{n+k}/M_{n+k+1} = G_{n+k}(M)$.

If $\beta \circ \phi = \hat{\phi} \circ \alpha$ with $\beta\colon M \to \hat{M}$ injective, α a bijection, and $\hat{\phi}$ surjective, then ϕ is surjective.* (p. 113)

Write $\psi = \hat{\phi} \circ \alpha$; it is surjective since α and $\hat{\phi}$ are. Thus $\hat{M} = \operatorname{im}(\psi) = \beta\big(\operatorname{im}(\phi)\big) \subseteq \beta(M)$; so β is surjective as well, hence a bijection. Thus surjectivity of ϕ follows from that of ψ.

EXERCISES

Let $\alpha_n\colon \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be the injection of Abelian groups given by $\alpha_n(1) = p^{n-1}$ and let $\alpha\colon A \to B$ be the direct sum of all the α_n (where A is a countable direct sum of copies of $\mathbb{Z}/p\mathbb{Z}$, and B is the direct sum of the $\mathbb{Z}/p^n\mathbb{Z}$). Show that the p-adic completion of A is just A but that the completion of A for the topology induced from the p-adic topology on B is the direct product of the $\mathbb{Z}/p\mathbb{Z}$. Deduce that the p-adic completion is not a right-exact functor on the category of all $\mathbb{Z}$-modules.

Since $pA = 0$, the sequence A/p^nA is $\cdots A \xrightarrow{\text{id}} A \xrightarrow{\text{id}} A$, the coherent sequences of which are constant sequences $\langle a\rangle$, giving an obvious isomorphism $\varprojlim A/p^nA \cong A$.

To make coordinate references easier, let G_n be the n^{th} copy of $\mathbb{Z}/p\mathbb{Z}$ in A. We have $p^nB = \bigoplus_{j>n} p^n\mathbb{Z}/p^j\mathbb{Z}$. As $\operatorname{im}(\alpha_j) = p^{j-1}\mathbb{Z}/p^j\mathbb{Z}$, which is contained in $p^n\mathbb{Z}/p^j\mathbb{Z}$ so long as $j > n$, it follows $\alpha_j^{-1}(p^n\mathbb{Z}/p^j\mathbb{Z})$ is $\mathbb{Z}/p\mathbb{Z}$ if $j > n$ and 0 otherwise. Then $A_n := \alpha^{-1}(p^nB)$ is the subgroup $\bigoplus_{j>n} G_j$ of $A = \bigoplus_{j=1}^{\infty} G_j$, so $A/A_n \cong \bigoplus_{j=1}^{n} G_j$. The projection $A/A_{n+1} \to A/A_n$ kills the $(n+1)^{st}$ component and preserves the others; the inverse system associated to the topology on A induced by α is thus essentially $\cdots \to (\mathbb{Z}/p\mathbb{Z})^3 \to (\mathbb{Z}/p\mathbb{Z})^2 \to \mathbb{Z}/p\mathbb{Z}$. Writing $\pi_j\colon A/A_{n+1} \to G_j$ for the projection, in a coherent sequence $\langle\xi_n\rangle$, the component $\pi_n(\xi_n) \in G_n$ determines (is equal to) the the components $\pi_n(\xi_j)$ of all the later members ξ_j, $j \geq n$, so the map $\phi\colon \varprojlim A/A_n \to \prod_{n=1}^{\infty} G_n$ taking $\langle\xi_n\rangle \mapsto \langle\pi_n(\xi_n)\rangle$ is an isomorphism.

Consider the short exact sequence $0 \to A \xrightarrow{\alpha} B \to B/\alpha(A) \to 0$. If we topologize the groups by the filtrations $\langle\alpha^{-1}(p^nB)\rangle$, $\langle p^nB\rangle$, and $\langle p^nB/\alpha(A)\rangle$, then by (10.3) the corresponding sequence of completed systems is exact; so if we instead give A the p-adic (discrete) topology $\langle p^nA = 0\rangle$, then, assuming the map $\hat{A} \to \hat{B}$ remains defined, the resulting sequence should not still be exact. Indeed, we have maps $A/p^nA \cong A \to \alpha(A) \hookrightarrow B \to B/p^nB$ compiling into an inverse system, so we have a short sequence $0 \to A \to \hat{B} \to \widehat{B/\alpha(A)} \to 0$. Since $A \ncong \prod_n \mathbb{Z}/p\mathbb{Z}$, this sequence is not exact at $\hat{B}$, so p-adic completion is not right-exact. (Though it does preserve surjectivity, because if $\rho\colon B \twoheadrightarrow C$ is a surjection, we have $\rho(p^nB) = p^nC$, so we have a surjective map $\langle B/p^nB\rangle \to \langle C/p^nC\rangle$ of surjective inverse systems, and (10.3) gives us

$\hat{B} \twoheadrightarrow \hat{C}$.)[6] p-adic completion is not left-exact, by the same example; the essential reason is that given a general homomorphism $\alpha \colon A \to B$ (in our example, an injection), we needn't have $\alpha(p^n A) = \alpha(A) \cap p^n B$, so the p-adic topology on A is not that induced from B and the hypotheses of (10.3) are not met.

In Exercise 1, let $A_n = \alpha^{-1}(p^n B)$, and consider the exact sequence

$$0 \to A_n \to A \to A/A_n \to 0.$$

Show that $\varprojlim$ is not right exact, and compute $\varprojlim^1 A_n$.

We can rewrite the sequence as $0 \to \bigoplus_{j=n+1}^{\infty} G_j \to \bigoplus_{j=1}^{\infty} G_j \to \bigoplus_{j=1}^{n} G_j \to 0$. The inclusions $A_{n+1} \hookrightarrow A_n$, identity map id_A, and projections $A/A_{n+1} \twoheadrightarrow A/A_n$ give us an exact sequence of inverse systems. (10.2) gives us an exact sequence

$$0 \to \varprojlim A_n \to \varprojlim A \to \varprojlim A/A_n \to \varprojlim{}^1 A_n \to \varprojlim{}^1 A \to \varprojlim{}^1 A/A_n \to 0.$$

To show $\varprojlim$ is not right exact, it will be enough, by this sequence, to show $\varprojlim^1 A_n \neq 0$. Since $\langle A \rangle$ and $\langle A/A_n \rangle$ are surjective systems, the proof of (10.2) shows us $\varprojlim^1 A$ and $\varprojlim^1 A/A_n$ are 0. As in the last problem, $\varprojlim A = A$ and $\varprojlim A/A_n \cong \prod_{j=1}^{\infty} G_j$. For $\varprojlim A_n$, since the maps are inclusions, any coherent sequence is a constant sequence, which means its lone term must be in each A_n. But $\bigcap_{n=1}^{\infty} A_n = 0$. Thus our exact sequence actually gives us a short exact sequence

$$0 \to A \xrightarrow{\psi} \varprojlim A/A_n \to \varprojlim{}^1 A_n \to 0.$$

To identify the last term it remains to describe the injection ψ. We claim it is basically the inclusion $\bigoplus_{j=1}^{\infty} G_j \hookrightarrow \prod_{j=1}^{\infty} G_j$. Indeed, since the maps $A \to A/A_n$ are quotient maps, the map from $A \cong \varprojlim A \subsetneq \prod_{n=1}^{\infty} A$ to $\varprojlim A/A_n \subsetneq \prod_{n=1}^{\infty} A/A_n$ is given by $a \mapsto \langle a \rangle \mapsto \langle a \pmod{A_n} \rangle$. Composing with the isomorphisms $A/A_n \cong \bigoplus_{j=1}^{n} G_j$, this gives $a \mapsto \big\langle \langle \pi_j(a) \rangle_{j=1}^{n} \big\rangle_{n=1}^{\infty}$, sending $a \in \prod_{j=1}^{\infty} G_j$ to a list of truncations. Using our isomorphism $\phi \colon \langle \xi_n \rangle \mapsto \langle \pi_n(\xi_n) \rangle$ from the last problem finally gives $a \mapsto \langle \pi_n(a) \rangle = a$. Thus $\varprojlim^1 A_n \cong \big(\prod_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z} \big) / \big(\bigoplus_{n=1}^{\infty} \mathbb{Z}/p\mathbb{Z} \big)$.

Let A be a Noetherian ring, $\mathfrak{a}$ an ideal and M a finitely-generated A-module. Using Krull's Theorem and Exercise 14 of Chapter 3, prove that

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n M = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \ker(M \to M_{\mathfrak{m}}),$$

where $\mathfrak{m}$ runs over all maximal ideals containing $\mathfrak{a}$.

Krull's Theorem (10.17) says that the left-hand side is the set of elements of M annihilated by $1 + a$ for some $a \in \mathfrak{a}$, so it remains to show the same is true of the right. Let $x \in M$. For all maximal $\mathfrak{m} \supseteq \mathfrak{a}$ we have $1 + \mathfrak{a} \subseteq 1 + \mathfrak{m} \subseteq A \backslash \mathfrak{m}$ so if $(1+a)x = 0$ for some $a \in \mathfrak{a}$, then by [3.1], $x/1 = 0$ in $M_{\mathfrak{m}}$ for all maximal $\mathfrak{m} \supseteq \mathfrak{a}$. On the other hand if $x/1 = 0$ in $M_{\mathfrak{m}}$ for all maximal $\mathfrak{m} \supseteq \mathfrak{a}$, then the submodule $Ax \subseteq M$ is such that $(Ax)_{\mathfrak{m}} = 0$, and then [3.14] gives $Ax = \mathfrak{a}x$, so in particular there is $a \in \mathfrak{a}$ such that $x = ax$, or $(1-a)x = 0$.

Deduce that

$$\hat{M} = 0 \iff \mathrm{Supp}(M) \cap V(\mathfrak{a}) = \varnothing \quad \big(\text{in } \mathrm{Spec}(A)\big).$$

Recall that the module above is the kernel of the canonical map $M \to \hat{M}$, so that $\hat{M} = 0 \iff M = \bigcap_{\mathfrak{m} \supseteq \mathfrak{a}} \ker(M \to M_{\mathfrak{m}})$. That in turn means that $M_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m} \supseteq \mathfrak{a}$, or in the language of [3.19], that none of these maximal ideals are in $\mathrm{Supp}(M)$. Let $\mathfrak{p} \in \mathrm{Spec}(A)$ be contained in a maximal $\mathfrak{m}$, so that $S_{\mathfrak{m}} \subseteq S_{\mathfrak{p}}$. Then if $x \in M$ is annihilated by an element of $S_{\mathfrak{m}}$, it is a fortiori annihilated by an element of $S_{\mathfrak{p}}$, so by [3.1], if $M_{\mathfrak{m}} = 0$, then also $M_{\mathfrak{p}} = 0$. Thus $M_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m} \supseteq \mathfrak{a}$ if and only if $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in V(\mathfrak{a})$, or in other words, $\mathrm{Supp}(M) \cap V(\mathfrak{a}) = \varnothing$.

[6] We embarrassingly were unable to make the connection between the above and the fact that p-adic completion is not exact, mostly because we were trying to prove surjectivity was not preserved and to find an exact sequence where A, with the alternate topology, occurred as the last nonzero term. This paragraph adapts Yimu Yin's solution: http://pitt.edu/~yimuyin/research/AandM/exercises10.pdf

Let A be a Noetherian ring, $\mathfrak{a}$ an ideal in A, and $\hat{A}$ the $\mathfrak{a}$-adic completion. For any $x \in A$, let $\hat{x}$ be the image of x in $\hat{A}$. Show that

$$x \text{ not a zero-divisor in } A \implies \hat{x} \text{ not a zero-divisor in } \hat{A}.$$

Let $x \in A$ not be a zero-divisor, so multiplication by x is injective; the book's suggested sequence $0 \to A \xrightarrow{x} A$ is then exact. Taking inverse limits gives an exact sequence $0 \to \hat{A} \to \hat{A}$ by (10.3), where the map on $\hat{A} \subseteq \prod A/\mathfrak{a}^n$ is given by $\langle \xi_n \rangle \mapsto \langle x\xi_n \rangle$, i.e., by multiplication by $\hat{x}$. Thus multiplication by $\hat{x}$ is injective, so $\hat{x}$ is not a zero-divisor.

Alternately, but very similarly, one can use the A-algebra structure $A \to \hat{A}$ to tensor the sequence with $\hat{A}$. Since A is Noetherian, $\hat{A}$ is flat by (10.14), so the map $x \otimes \mathrm{id}\colon A \otimes_A \hat{A} \to A \otimes_A \hat{A}$ is injective. By (2.14.iv) we have an isomorphism $\phi\colon A \otimes_A \hat{A} \to \hat{A}$, and $\phi \circ (x \otimes \mathrm{id}) \circ \phi^{-1}\colon \hat{A} \to \hat{A}$ is multiplication by $\hat{x}$.

Does this imply that

$$A \text{ is an integral domain} \implies \hat{A} \text{ is an integral domain?}$$

Not a priori, *for in general not all elements of $\hat{A}$ are images of elements of A. In fact,[7] if we write $A^{\mathfrak{a}}$ for the completion of A at $\mathfrak{a}$, then if A is an integral domain and $\mathfrak{a}, \mathfrak{b} \lhd A$ are coprime ideals, we can show $A^{\mathfrak{a}\mathfrak{b}}$ is not an integral domain. Since for each $\mathfrak{a}^n$ and $\mathfrak{b}^n$ remain coprime for $n \geq 1$ (see the footnote to [9.8]), by the Chinese Remainder Theorem (1.10), each map $A/(\mathfrak{a}\mathfrak{b})^n \to A/\mathfrak{a}^n \times A/\mathfrak{b}^n$ given by $x + (\mathfrak{a}\mathfrak{b})^n \mapsto \langle x + \mathfrak{a}^n,\, x + \mathfrak{b}^n \rangle$ is an isomorphism, and the square diagrams to the right commute, where the vertical maps on the right are $\langle x + \mathfrak{a}^{n+1},\, y + \mathfrak{b}^{n+1} \rangle \mapsto \langle x + \mathfrak{a}^n,\, y + \mathfrak{b}^n \rangle$. Thus we have an isomorphism between $A^{\mathfrak{a}\mathfrak{b}}$ and the inverse limit on the right, which ring consists of coherent sequences $\big\langle \langle \xi_n, \eta_n \rangle \big\rangle_n$ of pairs in $\prod (A/\mathfrak{a}^n \times A/\mathfrak{b}^n)$, which correspond to pairs $\big\langle \langle \xi_n \rangle_n, \langle \eta_n \rangle_n \big\rangle$ of coherent sequences in $\big(\prod A/\mathfrak{a}^n\big) \times \big(\prod A/\mathfrak{b}^n\big)$ under the obvious isomorphism, so that $A^{\mathfrak{a}\mathfrak{b}} \cong A^{\mathfrak{a}} \times A^{\mathfrak{b}}$, and hence is not an integral domain.*

$$\begin{tikzcd}
A/(\mathfrak{a}\mathfrak{b})^{n+1} \arrow[r, "\sim"] \arrow[d] & A/\mathfrak{a}^{n+1} \times A/\mathfrak{b}^{n+1} \arrow[d] \\
A/(\mathfrak{a}\mathfrak{b})^{n} \arrow[r, "\sim"] & A/\mathfrak{a}^{n} \times A/\mathfrak{b}^{n}
\end{tikzcd}$$

Let A be a Noetherian ring and let $\mathfrak{a}, \mathfrak{b}$ be ideals in A. If M is any A-module, let $M^{\mathfrak{a}}, M^{\mathfrak{b}}$ denote its $\mathfrak{a}$-adic and $\mathfrak{b}$-adic completions respectively. If M is finitely generated, prove that $(M^{\mathfrak{a}})^{\mathfrak{b}} \cong M^{\mathfrak{a}+\mathfrak{b}}$.

Since (10.13) tells us $M^{\mathfrak{a}} = A^{\mathfrak{a}} \otimes_A M$, by (2.14) it is enough to prove that $A^{\mathfrak{b}} \otimes_A A^{\mathfrak{a}} \cong A^{\mathfrak{a}+\mathfrak{b}}$, but it is not obvious how to do this. Instead, we follow the book's instructions to complete a proof that is unfortunately lengthy when fully fleshed out.

Following the book's suggestion, we can $\mathfrak{a}$-adically complete the sequences $0 \to \mathfrak{b}^m M \to M \to M/\mathfrak{b}^m M \to 0$ to get sequences $0 \to (\mathfrak{b}^m M)^{\mathfrak{a}} \to M^{\mathfrak{a}} \to (M/\mathfrak{b}^m M)^{\mathfrak{a}} \to 0$, which are exact by (10.12). Using the isomorphisms (10.13) we see the map $(\mathfrak{b}^m M)^{\mathfrak{a}} \to M^{\mathfrak{a}}$ is the composition $(\mathfrak{b}^m M)^{\mathfrak{a}} \xrightarrow{\sim} A^{\mathfrak{a}} \otimes_A \mathfrak{b}^m M \rightarrowtail A^{\mathfrak{a}} \otimes_A M \xrightarrow{\sim} M^{\mathfrak{a}}$. Since the isomorphism $A^{\mathfrak{a}} \otimes_A M \to A^{\mathfrak{a}} \otimes_A M^{\mathfrak{a}} \to A^{\mathfrak{a}} \otimes_{A^{\mathfrak{a}}} M \to M^{\mathfrak{a}}$ is given by $\langle a_n \rangle \otimes x \mapsto \langle a_n \rangle \otimes \langle x \rangle \mapsto \langle a_n x \rangle$, it follows that the image of $(\mathfrak{b}^m M)^{\mathfrak{a}} \to M^{\mathfrak{a}}$ is $\mathfrak{b}^m M^{\mathfrak{a}}$. Then exactness gives $M^{\mathfrak{a}}/\mathfrak{b}^m M^{\mathfrak{a}} \cong (M/\mathfrak{b}^m M)^{\mathfrak{a}}$.

Therefore

$$(M^{\mathfrak{a}})^{\mathfrak{b}} = \varprojlim M^{\mathfrak{a}}/\mathfrak{b}^m M^{\mathfrak{a}} \cong \varprojlim (M/\mathfrak{b}^m M)^{\mathfrak{a}} \cong \varprojlim_m \varprojlim_n \left(\frac{M}{\mathfrak{b}^m M} \middle/ \frac{\mathfrak{a}^n M + \mathfrak{b}^m M}{\mathfrak{b}^m M} \right),$$

since $(\mathfrak{a}^n M + \mathfrak{b}^m M)/\mathfrak{b}^m M$ is the image of $\mathfrak{a}^n M$ under $M \twoheadrightarrow M/\mathfrak{b}^m M$. But by the third isomorphism theorem (2.1.i), the terms on the right-hand side are isomorphic to $M/(\mathfrak{a}^n M + \mathfrak{b}^m M) =: M_{m,n}$.

An element of $\varprojlim_n M_{m,n}$ is represented by a sequence $\langle x_{m,n} \rangle_n$ of elements $x_{m,n} \in M_{m,n}$ coherent under the quotient maps $M_{m,n+1} \to M_{m,n}$, and an element of $\varprojlim_m \varprojlim_n M_{m,n}$ is represented by a sequence $\big\langle \langle x_{m,n} \rangle_n \big\rangle_m$ of such sequences, coherent under the reductions $m+1 \mapsto m$, which act on the n^{th} coordinates $x_{m+1,n}$ (the inverse limit being a submodule of $\prod_n M_{m+1,n}$) as the quotient maps $M_{m+1,n} \to M_{m,n}$. Note that whenever $n \leq n'$ and $m \leq m'$, the iterated quotient maps $M_{m',n'} \to M_{m',n} \to M_{m,n}$ and $M_{m',n'} \to M_{m,n'} \to M_{m,n}$ are equal. Thus an element of the double limit is really just an infinite array $\langle x_{m,n} \rangle_{m,n}$ coherent in both directions. Given such a coherent array, each $x_{p,p}$ uniquely determines all $x_{m,n}$ with $m, n \leq p$. Therefore, to specify a coherent array uniquely, one need only specify a coherent diagonal sequence $\langle x_{p,p} \rangle \in \varprojlim_p M_{p,p}$. This sets up a bijection $\varprojlim_m \varprojlim_n M_{m,n} \leftrightarrow \varprojlim M_{p,p}$ that obviously preserves the operations and hence is an isomorphism.

Finally, since

$$(\mathfrak{a}+\mathfrak{b})^{2n} \subseteq \mathfrak{a}^n + \mathfrak{b}^n \subseteq (\mathfrak{a}+\mathfrak{b})^n,$$

[7] This is taken, after our own failure, from [KarpukSol].

the topology on M induced by the filtration $\langle(\mathfrak{a}^n+\mathfrak{b}^n)M\rangle$ is the same as that induced by $\langle(\mathfrak{a}+\mathfrak{b})^n M\rangle$, so the corresponding completions should be isomorphic. But the former is the inverse limit from above, isomorphic to $(M^{\mathfrak{a}})^{\mathfrak{b}}$, and the latter is $M^{\mathfrak{a}+\mathfrak{b}}$.

Let A be a Noetherian ring and $\mathfrak{a}$ an ideal in A. Prove that $\mathfrak{a}$ is contained in the Jacobson radical of A if and only if every maximal ideal of A is closed for the $\mathfrak{a}$-topology. (A Noetherian topological ring in which the topology is defined by an ideal contained in the Jacobson radical is called a Zariski ring. Examples are local rings and (by (10.15)(iv)) $\mathfrak{a}$-adic completions.

This proof oddly requires no use of the Noetherian hypothesis. We show a maximal ideal $\mathfrak{m}$ is closed in the $\mathfrak{a}$-topology if and only if $\mathfrak{a}\subseteq\mathfrak{m}$. This implies the result because $\mathfrak{a}$ is contained in all maximal ideals if and only it is contained in their intersection, the Jacobson radical. Note that a set $C\subseteq A$ is closed if and only if each $x\in A\backslash C$ has a basic neighborhood $x+\mathfrak{a}^n$ disjoint from C. Let $\mathfrak{m}\lhd A$ be a maximal ideal.

If $\mathfrak{a}\subseteq\mathfrak{m}$ and $x\notin\mathfrak{m}$, then so $x+\mathfrak{a}^n\subseteq x+\mathfrak{m}$ is disjoint from $\mathfrak{m}$ for all n.

If $\mathfrak{a}\not\subseteq\mathfrak{m}$, any element of $\mathfrak{a}\backslash\mathfrak{m}$ descends to a unit in the field $A/\mathfrak{m}$, and so has a multiple $x\equiv 1 \pmod{\mathfrak{m}}$, with $x\in\mathfrak{a}$. Then $x^n\in\mathfrak{a}^n$ and $x^n\equiv 1 \pmod{\mathfrak{m}}$, so $1-x^n\in(1+\mathfrak{a}^n)\cap\mathfrak{m}$ for all n even though $1\notin\mathfrak{m}$, and $\mathfrak{m}$ is not closed.

Let A be a Noetherian ring, $\mathfrak{a}$ an ideal of A, and $\hat{A}$ the $\mathfrak{a}$-adic completion. Prove that $\hat{A}$ is faithfully flat over A (Chapter 3, Exercise 16) if and only if A is a Zariski ring (for the $\mathfrak{a}$-topology).

We again seem to be able, alarmingly, to prove the result without using the Noetherian hypothesis. By (10.14), $\hat{A}$ is flat, and by [3.16.iii], the condition will be met if and only if the extensions $\mathfrak{m}\hat{A}\neq\hat{A}$ for all maximal $\mathfrak{m}\lhd A$. Since a Noetherian ring A is Zariski if and only if $\mathfrak{a}$ is in all maximal $\mathfrak{m}$, it will be enough to show that for each maximal $\mathfrak{m}$ we have $\mathfrak{a}\subseteq\mathfrak{m}\iff\mathfrak{m}\hat{A}\neq\hat{A}\iff$ (IS THIS REALLY THE SAME?) for no element $x\in\mathfrak{m}$ is $\hat{x}$ a unit in $\hat{A}$.

If $\mathfrak{a}\subseteq\mathfrak{m}$, then $\mathfrak{m}/\mathfrak{a}^n$ is a proper ideal of $A/\mathfrak{a}^n$ for all n, and so no element of $\mathfrak{m}$ can become invertible.

If $\mathfrak{a}\not\subseteq\mathfrak{m}$, then $\mathfrak{a}+\mathfrak{m}=(1)$, and there are $x\in\mathfrak{m}$ and $a\in\mathfrak{a}$ with $x=1-a$. Inductively, given y_{2^n} such that $xy_{2^n}=1-a^{2^n}$, multiplying both sides by $1+a^{2^n}$ gives $xy_{2^n}(1+a^{2^n})=1-a^{2^{n+1}}$, showing x is a unit modulo $\mathfrak{a}^{2^{n+1}}$. Now $y_{2^{n+1}}:=y_{2^n}(1+a^{2^n})\equiv y_{2^n} \pmod{\mathfrak{a}^{2^n}}$, so if we set $y_m=y_{2^{n+1}}$ for $2^n<m\leq 2^{n+1}$, we see $\langle y_n+\mathfrak{a}^n\rangle$ is an element of $\hat{A}$ inverse to $\hat{x}$.

Alternately[8] (and using the Noetherian hypothesis), if $\hat{A}$ is faithfully flat, then by [3.16.iii], $\mathfrak{m}^e\neq\hat{A}$ for any maximal $\mathfrak{m}\lhd A$, so there is a maximal $\mathfrak{n}\lhd\hat{A}$ containing it. By [1.5.iv], $\mathfrak{n}^c\supseteq\mathfrak{m}^{ec}\supseteq\mathfrak{m}$ is maximal, so $\mathfrak{n}^c=\mathfrak{m}$. (10.15.iv) says $\hat{\mathfrak{a}}$ is in $\mathfrak{R}(\hat{A})$, so $\hat{\mathfrak{a}}\subseteq\mathfrak{n}$. Therefore $\mathfrak{a}\subseteq\hat{\mathfrak{a}}^c\subseteq\mathfrak{n}^c=\mathfrak{m}$, and $\mathfrak{a}$ is contained in $\mathfrak{R}(A)$.

The book also has a suggested proof. Since $\hat{A}$ is flat by (10.14), to prove faithful flatness [3.16.v] says it is enough to check that the canonical maps $M\to\hat{A}\otimes_A M$ are injective for all A-modules M. If this fails, some nonzero $x\in M$ is killed, so the composition $Ax\hookrightarrow M\to\hat{A}\otimes_A M$ is already not injective. Since $\hat{A}$ is flat, again by (10.14), $\hat{A}\otimes_A Ax\to\hat{A}\otimes_A M$ is injective, so the map $Ax\to\hat{A}\otimes_A Ax$ is not. Thus we only need to check injectivity for cyclic modules M; in this case, (10.13) tells us $\hat{A}\otimes_A M\cong\hat{M}$, so we are concerned with the maps $M\to\hat{M}$.

If $\mathfrak{a}$ is contained in the Jacobson radical of A, then since A is Noetherian and M is finitely generated, by (10.19), the kernel of $M\to\hat{M}$ is 0.

If $\mathfrak{a}$ is not contained in the Jacobson radical, there is a maximal ideal $\mathfrak{m}\notin V(\mathfrak{a})$; write $M=A/\mathfrak{m}$. Since $\mathfrak{m}\subseteq A$ is not closed by [10.6], it follows that $\{0\}\subseteq M$ is not closed, and so cannot be the kernel of $M\to\hat{M}$. Alternately, since each $\mathfrak{a}^n+\mathfrak{m}=(1)$, it follows that $\mathfrak{a}^n M=M$ for each n, so the kernel is M. Looked at yet another way, by (3.19.v), $\mathrm{Supp}(M)=V\big(\mathrm{Ann}(M)\big)=\{\mathfrak{m}\}$, which is disjoint from $V(\mathfrak{a})$, so by [10.3], $\hat{M}=0$.

Let A be the local ring of the origin in $\mathbb{C}^n$ (i.e., the ring of all rational functions $f/g\in\mathbb{C}(z_1,\ldots,z_n)$ with $g(0)\neq 0$), let B be the ring of power series in $z_1,\ldots,z_n$ which converge in some neighborhood of the origin, and let C be the ring of formal power series in $z_1,\ldots,z_n$, so that $A\subsetneq B\subsetneq C$. Show that B is a local ring and that its completion for the maximal ideal topology is C. Assuming that B is Noetherian, prove that B is A-flat.

To sensibly talk about B, we first must pick a notion of convergence for power series in several variables; we use absolute convergence, because it is independent of which sequence of partial sums we take the limit of.

The surjective ring homomorphism $h\mapsto h(0)\colon B\twoheadrightarrow\mathbb{C}$ shows the ideal $\mathfrak{m}=(z_1,\ldots,z_n)$ of power series with zero constant term is maximal. To show B is local, we demonstrate a power series f with nonzero constant term is a unit. If the

[8] http://pitt.edu/~yimuyin/research/AandM/exercises10.pdf

reader is willing to accept that a formal multiplicative inverse of a power series with positive multiradius of convergence likewise has positive multiradius of convergence, then we need only produce an $f^{-1} \in C$; and we can do this by an induction starting at $n = 0$, for by [1.5.i], $f \in \mathbb{C}[[z_1, \ldots, z_n, w]]$ is a unit just if $f(z, 0) \in \mathbb{C}[[z_1, \ldots, z_n]]$ is a unit. Otherwise, please consult the footnote.[9] This also shows that $A \subseteq B$, since any $g \in \mathbb{C}[z]$ with $g(0) \neq 0$ has an inverse in B. But $A \subsetneq B$, since for example $\exp(z) \notin A$. We see $B \subsetneq C$ since $\sum j! z_1^j \in C$ but $j!|\zeta^j| \to \infty$ for $\zeta \neq 0$.

To compute $\hat{B}$, write $\mathfrak{n} = \mathfrak{m} \cap A$ and note that the inclusion $A \hookrightarrow B$ induces isomorphisms $A/\mathfrak{n}^m \xrightarrow{\sim} B/\mathfrak{m}^m$ for all $m \in \mathbb{N}$, basically because the truncations of power series below a given total degree are just polynomials. Since these isomorphisms respect the quotient maps $A/\mathfrak{n}^{m+1} \twoheadrightarrow A/\mathfrak{n}^m$, we have an isomorphism of inverse systems, so $\hat{B} \cong \hat{A}$, which, as pointed out in the proof of (10.27), is C.

Since A and B are local rings with topologies defined by their maximal ideals (which are their Jacobson radicals), and we are told B is Noetherian ([7.4.ii] contains a proof in the $n = 1$ case; can we do an induction?), they are Zariski rings. By [10.7], $C = \hat{B} = \hat{A}$ is faithfully flat over A and B, so it follows from [3.17] that B is A-flat.

Let A be a local ring, $\mathfrak{m}$ its maximal ideal. Assume that A is $\mathfrak{m}$-adically complete. For any polynomial $f(x) \in A[x]$, let $\bar{f}(x) \in (A/\mathfrak{m})[x]$ denote its reduction mod. $\mathfrak{m}$. Prove Hensel's lemma: if $f(x)$ is monic of degree n and if there exist coprime monic polynomials $\bar{g}(x), \bar{h}(x) \in (A/\mathfrak{m})[x]$ of degrees $r, n-r$ with $\bar{f}(x) = \bar{g}(x)\bar{h}(x)$, then we can lift $\bar{g}(x), \bar{h}(x)$ back to monic polynomials $g(x), h(x) \in A[x]$ such that $f(x) = g(x)h(x)$.

There is a more general version stated as [Eisenbud, Thm. 7.18], proved there in two exercises whose extensive hints we follow.

First, we show that given a ring B and coprime, monic $p, q \in B[x]$ with $\deg p = r$, any $c \in B[x]$ admits an expression $c = ap + bq$ with $\deg b < r$. (In the case $q = 1$, this is the division algorithm. This implies the book's suggested lemma, for if $\deg q = n - r$ and $\deg c \leq n$, we have $\deg bq < n$, forcing $\deg a \leq n - r$.) Indeed, $B[x]/(p)$ is generated by $\bar{q}$ since $(p, q) = B[x]$, so there is $b \in B[x]$, such that $\bar{b}\bar{q} = \bar{c}$ in $B[x]/(p)$. Since p is monic of degree r, the elements $1, \bar{x}, \ldots, \bar{x}^{r-1}$ freely generate $B[x]/(p)$ as a B-module, so we may assume $\deg b < r$. Since q is monic, this choice of b is unique. Now $c \equiv bq \pmod{(p)}$, and p, being monic, is by [1.2.ii] not a zero-divisor, so $ap = c - bq$ has a unique solution $a \in B[x]$.[10, 11]

Second, we claim that if $\mathfrak{b} \subseteq \mathfrak{R}(A)$ is an ideal of A and we are given $g, h \in A[x]$ with g monic, then if $(\bar{g}, \bar{h}) = (1)$ in $(A/\mathfrak{b})[x]$, we have $(g, h) = A[x]$. Indeed, if $M = A[x]/(g)$, and $N = hM$, then since $\mathfrak{b}A[x] + (g, h) = A[x]$, we have

[9] This is adapted from a proof where $n = 1$ in [Lang, Ch. II, Thm. 3.3]. As convergence is unaffected by taking constant multiples, we may assume without loss of generality that $f(0) = 1$. Here we set up some notation. We will work in the rings $\mathbb{C}[[z, w]] = \mathbb{C}[[z_1, \ldots, z_n, w]]$ and $\mathbb{C}[[w]]$. If $\alpha = \langle \alpha_1, \ldots, \alpha_n \rangle \in \mathbb{N}^n$ is a multi-index, $x^\alpha = \prod x_m^{\alpha_m}$, whether $x_m = z_m$ or $x_m \in \mathbb{C}$. If $|a_j| \leq r_j$ for $a_j \in \mathbb{C}$ and $r_j \geq 0$, write $\sum a_j w^j \prec \sum r_j w^j$ in $\mathbb{C}[[w]]$; this is a transitive relation. The following fact is helpful: if $f, g \in \mathbb{C}[[w]]$ and $\omega \in \mathbb{C}$ are such that $f \prec g$ and $g(\omega)$ converges, then $f(\omega)$ converges.

To see f^{-1} converges in a neighborhood of the origin, set $g = 1 - f$; then formally, $f^{-1} = (1-g)^{-1} = \sum_k g^k$, using the geometric series. Write $g = \sum a_j w^j \in \mathbb{C}[[z, w]]$ for $a_j \in \mathbb{C}[[z]]$. Since g converges absolutely some neighborhood of the origin, we can find a closed polydisk $\{\langle \zeta, \omega \rangle : \zeta_m \leq \epsilon_m,\ \ \omega \leq \delta\}$ on which g converges absolutely. In particular, the a_j converge absolutely on $\bar{D} = \{\zeta : \zeta_m \leq \epsilon_m\}$. If we write $a_j = \sum c_\alpha z^\alpha$ for $c_\alpha \in \mathbb{C}$, then their maximal values on $\bar{D}$ are the finite numbers $r_j = \sum |c_\alpha| \epsilon^\alpha$, and so to show $f^{-1}(\zeta, \omega)$ converges for all $\zeta \in \bar{D}$ it suffices to show $f^{-1}(r, \omega) \coloneqq f^{-1}(r_1, \ldots, r_n, \omega)$ converges. If we had $r_j \geq \delta^{-j}$ for infinitely many j, the series $g(r, \delta)$ would not converge; as we know it does, $r_j < \delta^{-j}$ for all but finitely many j, and thus there is a constant $R \geq \delta^{-1}$ such that $r_j < R^j$ for all j. We now have $g(r, w) \prec \sum_{j=1}^\infty R^j w^j = \frac{Rw}{1-Rw}$, so

$$f^{-1}(r, w) \prec \sum_{k=0}^{\infty} g(r, w)^k \prec \sum_{k=0}^{\infty} \left(\frac{Rw}{1-Rw} \right)^k = \frac{1}{1 - \frac{Rw}{1-Rw}} = \frac{1-Rw}{1-2Rw} = (1-Rw) \sum_{k=0}^{\infty} (2Rw)^k \prec (1+Rw) \sum_{k=0}^{\infty} (2Rw)^k,$$

showing f^{-1} converges on $\bar{D} \times \{\omega : |\omega| < 1/2R\}$.

[10] There is actually a mistake here ([EisenEmail]), as the author does not require q to be monic. We need $\bar{q}$ to not be a zero-divisor for the uniqueness claim. This will also be the case if $B[x]/(p)$ is an integral domain, but we cannot make any guarantees on p in the rest of the proof.

[11] Here is a proof of the book's lemma that if monic $p, q \in B[x]$ of respective degrees $r, n - r$ are coprime, then for any polynomial c of degree $\leq n$ there are $a, b \in B[x]$, of respective degrees $\leq n - r, r$, such that $ap + bq = c$. Since $(p, q) = (1)$, this is obviously possible if we drop the restriction on degrees. If $a = a_j x^j + (\deg < j)$ and $b = b_m x^m + (\deg < m)$ with $a_j, b_m \neq 0$, and $j > n - r$, we will polynomials a', b' of degrees respectively $< j, m$ such that again $a'p + b'q = c$; applying this repeatedly eventually achieves the desired restriction on degrees. Since $\deg c \leq n < j + r$, it follows that the leading term $a_j x^{j+r}$ of ap cancels the leading term $b_m x^{m+n-r}$, so $a_j = -b_m$ and $j + r = m + n - r$, or $j - (n - r) = m - r$. (This also shows $r < m$.) If we let $a' = a - a_j x^{j-(n-r)} q$ and $b' = b - b_m x^{m-r} p$, then $\deg a' < j$ and $\deg b' < m$, and

$$a'p + b'q = (ap + bq) - (a_j x^{j-(n-r)} + b_m x^{m-r}) pq = c.$$

$\mathfrak{b}M + N = M$. Since M is finitely generated by $\bar{1}, \bar{x}, \ldots, \bar{x}^{\deg g-1}$, Nakayama's Lemma (2.7) applies to show $hM = M$, so that $(g, h) = (1)$ in $A[x]$.

Now we prove the result. We need only assume that A is complete with respect to some ideal $\mathfrak{a}$; we do not necessarily need $\mathfrak{a}$ maximal or A local. We inductively construct sequences $\langle g_k \rangle$ and $\langle h_k \rangle$ of monic polynomials of the right degrees in $A[x]$ with $f - g_k h_k \equiv 0 \pmod{\mathfrak{a}^k}$ and $g_k \equiv g_j$, $h_k \equiv h_j \pmod{\mathfrak{a}^j}$ for $j < k$. Coefficient by coefficient, the g_k and the h_k will form Cauchy sequences with respect to the $\mathfrak{a}$-topology, and so converge to unique limits $g, h \in A[x]$ with $g \equiv g_k$, $h \equiv h_k \pmod{\mathfrak{a}^k}$ for all $k \geq 1$. We will then have $f - gh = (f - g_k h_k) + (g_k h_k - gh) \equiv 0 \pmod{\mathfrak{a}^k}$ for all k. Since A is $\mathfrak{a}$-adically complete, $\bigcap \mathfrak{a}^k = 0$, so $f = gh$, as hoped.

If g_1, h_1 are lifts of the appropriate degrees of $\bar{g}, \bar{h}$ to $A[x]$, by assumption, $f - g_1 h_1 \equiv 0 \pmod{\mathfrak{a}}$ (really meaning modulo $\mathfrak{a}[x]$). The Eisenbud version of the induction step follows; the one from the book is in the footnote.[12] Suppose inductively we have found $g_k, h_k \in A[x]$ such that $g_k \equiv g_j$, $h_k \equiv h_j \pmod{\mathfrak{a}^{2^{j-1}}}$ for all $j < k$ and $f - g_k h_k = c \equiv 0 \pmod{\mathfrak{a}^{2^{k-1}}}$. Since by (10.15.iv), $\mathfrak{a}^{2^{k-1}} \subseteq \mathfrak{R}(A)$, it follows from the second claim, with $\mathfrak{b} = \mathfrak{a}^{2^{k-1}}$, that $(g_k, h_k) = A[x]$. By the first claim, with $B = A$, $p = g_k$, $q = h_k$, there are unique $a, b \in A[x]$ with $\deg b < r$ and $ag_k + bh_k = c$. Descending to $A/\mathfrak{a}^{2^{k-1}}[x]$, where we take $B = A/\mathfrak{a}^{2^{k-1}}$ in the first claim and use uniqueness, we see that since $\bar{c} = 0$ we also have $\bar{a} = \bar{b} = 0$, or $a, b \in \mathfrak{a}^{2^{k-1}}[x]$. Set $g_{k+1} = g_k + b \in g_k + \mathfrak{a}^{2^k}[x]$ and $h_{k+1} = h_k + a \in h_k + \mathfrak{a}^{2^k}[x]$, so

$$f - g_{k+1} h_{k+1} = (f - g_k h_k) - (ag_k + bh_k) - ab = c - c + ab = ab \in \mathfrak{a}^{2^k}[x].$$

i) With the notation of Exercise 9, deduce from Hensel's lemma that if $\bar{f}(x)$ has a simple root $\alpha \in A/\mathfrak{m}$, then $f(x)$ has a simple root $a \in A$ such that $\alpha = a \mod \mathfrak{m}$.

If α is a simple root of $\bar{f}$, we have a factorization $\bar{f} = (x - \alpha)\bar{g}$, where $\bar{g}$ is coprime to $x - \alpha$. Since we assume $\bar{f}$ is monic, so is $\bar{g}$. By [10.9], there exist monic lifts h of $x - \alpha$ and g of $\bar{g}$ to $A[x]$; since $\deg h = 1$, we must be able to write $h = x - a$ for some $a \in A$, and $a \mapsto \alpha$ under $A \to A/\mathfrak{m}$. Since $x - a$ is irreducible, if it divided g, then $(x - \alpha)^2$ would divide $\bar{f}$, contrary to assumption, so a is a simple root of f.

ii) Show that 2 is a square in the ring of 7-adic integers.

2 is be a square if and only if $x^2 - 2 \in \mathbb{Z}_7[x]$ has a solution, if and only if it splits into linear factors. $x^2 - \bar{2}$ has simple roots $\pm\bar{3}$ in $\mathbb{Z}_7/7\mathbb{Z}_7 \cong \mathbb{Z}/7\mathbb{Z}$, so by i), 2 has two square roots in $\mathbb{Z}_7$.

iii) Let $f(x, y) \in k[x, y]$, where k is a field, and assume that $f(0, y)$ has $y = a_0$ as a simple root. Prove that there exists a formal power series $y(x) = \sum_{n=0}^{\infty} a_n x^n$ such that $f\big(x, y(x)\big) = 0$.
(This gives the "analytic branch" of the curve $f = 0$ through the point $(0, a_0)$.)

Write $A = k[[x]]$ and $\mathfrak{m} = (x)$, so $A/\mathfrak{m} = k$. Considering $f(x, y)$ as an element of $A[y] \supsetneq k[x][y] = k[x, y]$, the image of f in $k[y]$ is $f(0, y)$, which by assumption has a simple root $a_0 \in k$. By i), $f(x, y)$ has a simple root $y(x) \in k[[x]]$ with constant term a_0.

Show that the converse of (10.26) is false, even if we assume that A is local and that $\hat{A}$ is a finitely-generated A-module.

Since (10.26) says that completing a Noetherian ring A with respect to an ideal $\mathfrak{a}$ produces a Noetherian $\hat{A}$, the converse would presumably be that if the $\mathfrak{a}$-completion $\hat{A}$ of a ring A is Noetherian, then A was already Noetherian. It then falls to us to find a non-Noetherian local ring with finitely generated, Noetherian completion.

Following the book's hint, let $A = C_0^{\infty}(\mathbb{R})$ be the set of germs $[f]$ at $0 \in \mathbb{R}$ of C^{∞} real-valued functions f. The homomorphism $[f] \mapsto f(0)$ surjects onto the field $\mathbb{R}$, showing the functions vanishing at 0 form a maximal ideal $\mathfrak{a}$. To

[12] Let $g_k, h_k \in A[x]$ be given. Since $\bar{g}_k = \bar{g}$, $\bar{h}_k = \bar{h}$, we have $(\bar{g}_k, \bar{h}_k) = (1)$ in $(A/\mathfrak{a})[x]$, so there are $m_j \in \mathfrak{a}^k$ such that $f - g_k h_k = \sum_{j=0}^{n} m_j x^j$, and for $0 \leq j \leq n$ there exist $a_j, b_j \in A[x]$ of degrees $\leq n - r$, r such that $\bar{a}_j \bar{g}_k + \bar{b}_j \bar{h}_k = \bar{x}^j$ in $(A/\mathfrak{a})[x]$. Then there are $r_j \in \mathfrak{a}[x]$ with $\deg r_j \leq n$ such that $a_j g_k + b_j h_k + r_j = x^j$ in $A[x]$ (this paraphrases the solution in [PapaSol]; I had not seen the necessity of working coefficient by coefficient and gotten stuck). We then can write

$$f - g_k h_k = \sum m_j (a_j g_k + b_j h_k + r_j) = g_k \sum m_j a_j + h_k \sum m_j b_j + \sum m_j r_j.$$

Now $g_{k+1} = g_k + \sum m_j b_j \in g_k + \mathfrak{a}^{k+1}[x]$ and $h_{k+1} = h_k + \sum m_j a_j \in h_k + \mathfrak{a}^{k+1}[x]$ satisfy the degree restrictions, and

$$f - g_{k+1} h_{k+1} = (f - g_k h_k) - g_k \sum m_j a_j - h_k \sum m_j b_j - \sum_j \sum_\ell m_j m_\ell a_j b_\ell = \sum m_j r_j - \sum_j \sum_\ell m_j m_\ell a_j b_\ell \in \mathfrak{a}^{k+1}[x].$$

see this is the only maximal ideal, suppose f represents an $[f] \notin \mathfrak{a}$; then by continuity $f \neq 0$ on some neighborhood of 0, so f locally admits a multiplicative inverse g, and $[f][g] = [1]$, showing $[f]$ is a unit.

Write $\mathfrak{b}_n := \big\{[f] \in A : f^{(j)}(0) = 0 \text{ for } 0 \leq j < n\big\}$; we want to show $\mathfrak{a}^n = \mathfrak{b}_n = (x^n)$. Suppose inductively that $\mathfrak{a}^n \subseteq \mathfrak{b}_n$. Then if $[f] \in \mathfrak{a}^{n+1}$, we can write f as a sum of elements gh for $[g] \in \mathfrak{a}$ and $[h] \in \mathfrak{a}^n$. By the generalized product rule, $(gh)^{(n)} = \sum_{j=0}^{n} \binom{n}{j} g^{(j)} h^{(n-j)}$; since $g(0) = 0$, and $h^{(n-j)}(0) = 0$ for $j \geq 1$, we see $f^{(n)}(0) = 0$, so $[f] \in \mathfrak{b}_{n+1}$. For the reverse inclusion, we use Taylor's theorem with remainder: for any open interval $U \subseteq \mathbb{R}$ and $f \in C^\infty(U)$, we can write $f(x) = \sum_{j=0}^{n-1} \frac{1}{j!} f^{(j)}(0) x^j + g_n(x) x^n$ on U, where $g_n \in C^\infty(U)$ and $g_n(0) = \frac{1}{n!} f^{(n)}(0)$.[13] Thus $\mathfrak{b}_n \subseteq (x^n) \subseteq \mathfrak{a}^n$.

Since $x^n g_n \in \mathfrak{a}^n$, and any polynomial is its own Maclaurin series, truncations of Maclaurin series yield isomorphisms $A/\mathfrak{a}^n \longrightarrow \mathbb{R}[x]/(x^n)$ compatible with the quotient homomorphisms given by $n+1 \mapsto n$. By Example 1 on p. 105, $\hat{A} \cong \mathbb{R}[[x]]$, which is Noetherian by (7.5) because $\mathbb{R}$ is a field. However, by (10.18), since $0 \neq e^{-1/x^2} \in \bigcap \mathfrak{a}^n$ (its Maclaurin series is 0), A is not Noetherian. By Borel's theorem that every power series is the Taylor series of a C^∞ function, $A \to \hat{A}$ is surjective, so that $\hat{A}$ is finitely generated.*

If A is Noetherian, then $A[[x_1, \ldots, x_n]]$ is a faithfully flat A-algebra.

By [2.5], $A \to A[x_1, \ldots, x_n]$ is flat, and by (10.14) and our proof above that the latter is the completion of the former, $A[x_1, \ldots, x_n] \to A[[x_1, \ldots, x_n]]$ is flat, so [2.8.ii] says $A \to A[[x_1, \ldots, x_n]]$ is flat. For any $\mathfrak{a} \lhd A$ we have $\mathfrak{a}^e = \mathfrak{a} + \mathfrak{a} \cdot (x_1, \ldots, x_n)$, so that $\mathfrak{a}^{ec} = \mathfrak{a}$; thus, by [3.16.i], $A[[x_1, \ldots, x_n]]$ is faithfully flat over A.

[13] For a proof, note that by the chain rule, $\frac{d}{dt} f(tx) = x f'(tx)$. Integrating both sides from 0 to 1 and using the fundamental theorem of calculus gives $f(x) - f(0) = x \int_0^1 f'(tx)\,dt$. Write $g(x) = \int_0^1 f'(tx)\,dt$; then $g(0) = \int_0^1 f'(0)\,dt = f'(0)$. Thus $f(x) = f(0) + x g(x)$ for a C^∞ function g with $g(0) = f'(0)$. See [Tu, Lemma 1.4] for a generalization of this result to real-valued functions on open subsets of $\mathbb{R}^n$, star-shaped with respect to some point (specialized to 0 for us).

Applying the above to g and iterating, we get expressions $f(x) = f(0) + \sum_{j=1}^{n-1} g_j(0) x^j + g_n(x) x^n$, so $f^{(n)}(0) = n! g_n(0)$ for all n.

This differs slightly from the usual form of the theorem, which assumes only that f is n times differentiable at 0 and gets a remainder term $h_{n-1}(x) x^{n-1}$ with $\lim_{x \to 0} h_{n-1}(x) = 0$ instead of our $g_n(x) x^n$; see e.g. [WPTaylor].

Dimension Theory

$$(1-t)^{-d} = \sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k. \quad \textit{(p. 117)}$$

$(1-t)^{-1} = 1+t+t^2+\cdots$, *so we want to check that the coefficient of* t^k *in its* d^{th} *power is* $\binom{d+k-1}{d-1}$. *This coefficient is the number of possible ways of forming a product* $\prod_{j=1}^{d} t^{k_j}$ *with* $\sum_{j=1}^{d} k_j = k$, *which is the number of ordered partitions of a row of* k *objects into* d *groups. This is the same as the number of ways of inserting* $d-1$ *dividers into the row of* k *objects, or of choosing* $d-1$ *objects out of* $k+d-1$ *to serve as dividers, namely* $\binom{d+k-1}{d-1}$.

Example. *Let* $A = A_0[x_1, \ldots, x_s]$, *where* A_0 *is an Artin ring and the* x_i *are independent indeterminates. Then* A_n *is a free* A_0*-module generated by the monomials* $x_1^{m_1} \cdots x_s^{m_s}$ *where* $\sum m_i = n$; *there are* $\binom{s+n-1}{s-1}$ *of these, hence* $P(A, t) = (1-t)^{-s}$. *(p. 118)*

The coefficient of t^n *in* $P(A, t)$ *is* $l(A_n)$. *Since* $A_n \cong A_0^{\binom{s+n-1}{s-1}}$ *as an* A_0*-module, it follows* $l(A_n) = \binom{s+n-1}{s-1} l(A_0)$. *Then by the expression above,* $P(A, t) = l(A_0)(1-t)^{-s}$. *This is not the expression that the book gives unless* $l(A_0) = 1$. *The degree* $d(A) = d\big(G_{\mathfrak{m}}(A)\big)$ *as defined on p. 119 is unaffected by this change, and hence so is the dimension* n *of* $k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$ *in the example on p. 121 and* $d\big(G_{\mathfrak{q}}(A)\big)$ *in the proof of (11.20).*

Given a polynomial $f(x) \in \mathbb{Z}[x]$, *the sum* $g(n) = \sum_{j=0}^{n} f(j)$ *is a polynomial in* n.* *(p. 119)*

We can write $f(n) = \sum_k a_k n^k$, *so it will be enough to show that for each* n *the function* $g_k(n) = \sum_{j=0}^{n} j^k$ *is a polynomial.*[1] *Note that* $g_0(n) = n+1$. *Suppose inductively that* $g_j(n)$ *is a polynomial for* $j \leq k$. *By the binomial theorem we have* $(m+1)^{k+1} - m^{k+1} = \sum_{j=0}^{k} \binom{k+1}{j} m^j$. *Summing both sides from* $m = 0$ *to* n *gives* $(n+1)^{k+1} = \sum_{j=0}^{k} \binom{k+1}{j} g_j(n)$, *and rearranging, we see* $g_k(n) = (n+1)^{k+1} - \sum_{j=0}^{k-1} \binom{k+1}{j} g_j(n)$ *is a polynomial in* n.

If $0 \to N \hookrightarrow M \to M' \to 0$ *is exact and* $\mathfrak{q} \lhd A$, *then* $0 \to N/(N \cap \mathfrak{q}^n M) \to M/\mathfrak{q}^n M \to M'/\mathfrak{q}^n M' \to 0$ *is exact.* * *(p. 120)*

This is a special case of a similar result in the beginning notes to Ch. 10.

EXERCISES

Let $f \in k[x_1, \ldots, x_n]$ *be an irreducible polynomial over an algebraically closed field* k. *A point* P *on the variety* $f(x) = 0$ *is* non-singular $\Longleftrightarrow$ *not all the partial derivatives* f/x_i *vanish at* P. *Let* $A = k[x_1, \ldots, x_n]/(f)$, *and let* $\mathfrak{m}$ *be the maximal ideal of* A *corresponding to the point* P. *Prove that* P *is non-singular* $\Longleftrightarrow$ $A_{\mathfrak{m}}$ *is a regular local ring.*

Write $k[x] = k[x_1, \ldots, x_n]$ *and let* $P = \langle a_1, \ldots, a_n \rangle$, *so that* $\mathfrak{m}$ *is the image in* A *of* $\mathfrak{m}_P = (x_1 - a_1, \ldots, x_n - a_n) \lhd k[x]$. *Since* $f(P) = 0$, *we have* $f \in \mathfrak{m}_P$, *so there are* $p_j \in k[x]$ *(possibly zero) such that* $f = \sum (x_j - a_j) p_j$. *Then* $f/x_i = p_i + (x_i - a_i)(p_i/x_i) + \sum_{j \neq i} (x_j - a_j) p_j/x_i$. *All terms but possibly* p_i *are in* $\mathfrak{m}_P$; *so it follows that* P *is a singular point of the variety* $f(x) = 0 \Longleftrightarrow$ *all the* f/x_i *vanish at* $P \Longleftrightarrow$ *each* $p_i \in \mathfrak{m}_P \Longleftrightarrow f \in \mathfrak{m}_P^2$.

Now we work to rephrase regularity of $A_{\mathfrak{m}}$ *in terms of* f. *Since* $A = k[x]/(f)$ *and the quotient map* $k[x] \to A$ *takes* $S_{\mathfrak{m}_P} \to S_{\mathfrak{m}}$, *by (3.4.iii) and [3.4], we have* $k[x]_{\mathfrak{m}_P}/(f)_{\mathfrak{m}_P} \cong \big(k[x]/(f)\big)_{\mathfrak{m}} = A_{\mathfrak{m}}$. *Since* $\dim k[x]_{\mathfrak{m}_P} = n$, *by (11.18),* $\dim A_{\mathfrak{m}} = n-1$. *By the third isomorphism theorem (2.1.i) and (3.4.iii),* $k \cong k[x]/\mathfrak{m}_P \cong A/\mathfrak{m} \cong A_{\mathfrak{m}}/\mathfrak{m}A_{\mathfrak{m}}$, *so, using (3.4.iii) again,* $A_{\mathfrak{m}}$ *is a regular local ring just if* $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = \dim_k(\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2 A_{\mathfrak{m}}) = n-1$. *Now* $\mathfrak{m} = \mathfrak{m}_P/(f)$, *and* $\mathfrak{m}^2$ *is the image of* $\mathfrak{m}_P^2$ *under* $k[x] \to A$, *which is* $\big(\mathfrak{m}_P^2 + (f)\big)/(f)$, *so that by (2.1.i) again,* $\mathfrak{m}/\mathfrak{m}^2 = \frac{\mathfrak{m}_P}{(f)} \Big/ \frac{\mathfrak{m}_P^2 + (f)}{(f)} \cong \mathfrak{m}_P/\big(\mathfrak{m}_P^2 + (f)\big)$. *If* $f \in \mathfrak{m}_P^2$, *then this is* $\mathfrak{m}_P/\mathfrak{m}_P^2$, *which has dimension* n, *so* $A_{\mathfrak{m}}$ *is not regular. Otherwise* $\mathfrak{m}_P^2 + (f)$ *strictly contains* $\mathfrak{m}_P^2$, *so* $\dim_k(\mathfrak{m}/\mathfrak{m}^2) < n$. *But by (11.15),* $\dim_k(\mathfrak{m}/\mathfrak{m}^2) \geq n-1$.

[1] adapted from `http://mathforum.org/library/drmath/view/56920.html`

In (11.21) assume that A is complete. Prove that the homomorphism $k[[t_1, \ldots, t_d]] \to A$ given by $t_i \mapsto x_i$ ($1 \leq i \leq d$) is injective and that A is a finitely-generated module over $k[[t_1, \ldots, t_d]]$.

The first thing to check is that this homomorphism is well defined. If $\mathfrak{n} = (t_1, \ldots, t_d) \lhd k[t] \coloneqq k[t_1, \ldots, t_d]$, then the $\mathfrak{n}^n$ form a neighborhood basis of 0 in $k[t]$, and the map $k[t] \to A$ given by $t_i \mapsto x_i$ sends $\mathfrak{n}^n \to \mathfrak{q}^n \subseteq \mathfrak{m}^n$. Thus a Cauchy sequence in $k[t]$ is sent to a Cauchy sequence in A, which converges to a point of A by completeness, so since $k[[t]] \coloneqq k[[t_1, \ldots, t_d]]$ is the completion of $k[t]$ with respect to $\mathfrak{n}$, we have a well defined map $k[[t]] \to A$ as asserted, making A a $k[[t]]$-module.

For injectivity, let $p(t) \in k[[t]]$ be in the kernel. Writing $\mathfrak{q} = (x_1, \ldots, x_d)$, by (7.16.iii), $p(x) = 0 \iff p(x) \in \mathfrak{q}^n$ for every n. Write $p_n(t)$ for the n^{th} homogeneous component of $p(t)$; since $p_0(x) = 0$, it follows $p_0(t) = 0$. Inductively suppose $p_j(t) = 0$ for all $j \leq n$. Now $p(x) - p_n(x) \in \mathfrak{q}^{n+1}$, and $p(x) = 0 \in \mathfrak{q}^{n+1}$, so $p_n(x) \in \mathfrak{q}^{n+1}$ By (11.20), the coefficients of $p_n(t)$ are in $k \cap \mathfrak{m} = 0$. Thus each $p_n(t) = 0$, so $p(t) = 0$.

Now $\langle \mathfrak{q}^n \rangle$ is a $\hat{\mathfrak{n}}$-filtration of A, $k[[t]]$ is complete, and A is Hausdorff (since complete) with respect to the $\mathfrak{q}$-topology (which by (7.16.iii) is the $\mathfrak{m}$-topology), so by (10.24), A will be a finitely-generated $k[[t]]$-module if $G_{\mathfrak{q}}(A)$ is a finitely-generated $G_{\hat{\mathfrak{n}}}\big(k[[t]]\big)$-module. By (10.22.ii), $G_{\hat{\mathfrak{n}}}\big(k[[t]]\big) \cong G_{\mathfrak{n}}\big(k[t]\big)$ and the latter is isomorphic to $k[t]$ under $\bar{t}_i \mapsto t_i$. But the map $k[t] \to G_{\mathfrak{q}}(A)$ taking $t_i \mapsto \bar{x}_i$ is a quotient map.

Extend (11.25) to non-algebraically-closed fields.

By Noether normalization [5.16], if $d = \dim V$, there are algebraically independent $x_1, \ldots, x_d \in A(V)$ such that $A(V)$ is integral over the polynomial subring $B = k[x_1, \ldots, x_d]$. Since B is a UFD, as noted on p. 63, it is integrally closed. Following the book's hint, note that $\bar{k}$ is integral over $k \subsetneq B$, and trivially the x_i are integral over B, so that by (5.3) the ring $C = \bar{k}[x_1, \ldots, x_d]$ is integral over B. As V is an irreducible variety, $A(V)$ is an integral domain, so that (11.26) applies to the inclusion $B \subseteq A(V)$: for any maximal ideal $\mathfrak{m} \lhd A(V)$, then, $\dim A(V)_{\mathfrak{m}} = \dim B_{\mathfrak{m}^c}$, where $\mathfrak{m}^c$ is maximal by (5.8). It remains to show that $\dim B_{\mathfrak{n}} = d$ for all maximal ideals $\mathfrak{n} \lhd B$. By (5.10), since C is integral over B, there is a prime of C lying over $\mathfrak{n}$, and by (1.4), there is a maximal ideal $\mathfrak{q} \lhd C$ containing that prime, whose contraction to B is then a prime ideal containing $\mathfrak{n}$, which must be $\mathfrak{n}$ itself. As (11.26) also applies to the inclusion $B \subseteq C$, we have $\dim B_{\mathfrak{n}} = \dim C_{\mathfrak{q}}$. But we already established in (11.25) that $\dim C_{\mathfrak{q}} = d$.

An example of a Noetherian domain of infinite dimension (Nagata). Let k be a field and let $A = k[x_1, x_2, \ldots, x_n, \ldots]$ be a polynomial ring over k in a countably infinite set of indeterminates. Let $m_1, m_2, \ldots$ be an increasing [or even just unbounded] sequence of positive integers such that $m_{i+1} - m_i > m_i - m_{i-1}$ for all $i > 1$. [Actually, set $m_1 = 0$.] Let $\mathfrak{p}_i = (x_{m_i+1}, \ldots, x_{m_{i+1}})$ and let S be the complement in A of the union of the ideals $\mathfrak{p}_i$.

Each $\mathfrak{p}_i$ is a prime ideal and therefore the set S is multiplicatively closed. The ring $S^{-1}A$ is Noetherian by Chapter 7, Exercise 9. Each $S^{-1}\mathfrak{p}_i$ has height equal to $m_{i+1} - m_i$, hence $\dim S^{-1}A = \infty$.

Note that the complement S of the union of a set P of primes in A is multiplicatively closed, as follows: $x, y \in S \iff \forall \mathfrak{p} \in P\ (x, y \notin \mathfrak{p}) \iff \forall \mathfrak{p} \in P\ (xy \notin \mathfrak{p}) \iff xy \in S$.

The prime ideals of A that persist in $S^{-1}A$ are by (3.11.iv) those that don't meet S, so the maximal ideals of $S^{-1}A$ are $S^{-1}\mathfrak{p}$ for prime $\mathfrak{p} \lhd A$ maximal with respect to not meeting S. Suppose $\mathfrak{a} \lhd A$ doesn't meet S, so it is contained in the union of the $\mathfrak{p}_i$; we claim it is contained in some $\mathfrak{p}_i$. Given $(a_1, \ldots, a_\ell) \subseteq \mathfrak{a}$, the a_j only involve finitely many indeterminates, so for some n we have $(a_1, \ldots, a_\ell) \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$. By (1.11.i), $(a_1, \ldots, a_\ell) \subseteq \mathfrak{p}_i$ for some $i \leq n$. If we append $a_{\ell+1} \in \mathfrak{a}$, we again have an $n' \in \mathbb{N}$ such that $(a_1, \ldots, a_\ell, a_{\ell+1}) \subseteq \mathfrak{p}_i$ for some $i \leq n'$; but $n' \leq n$, since we don't have $a_1 \in \mathfrak{p}_i$ for $i > n$ by assumption. Thus appending a generator can only decrease our collection of candidate $\mathfrak{p}_i$. If for any $b \in \mathfrak{a}$ we have $b \notin \mathfrak{p}_i$, we can choose $a_{\ell+1} = b$ and pick a new $\mathfrak{p}_i$ with $i \leq n$. Since there are only finitely many of these, this is eventually no longer possible, and then we are done.

Thus the maximal ideals of $S^{-1}A$ are the $S^{-1}\mathfrak{p}_i$. We claim the localizations with respect to these are Noetherian. Without loss of generality, take $i = 1$. Note $\big(S^{-1}A \backslash S^{-1}\mathfrak{p}_1\big)^{-1} = \big(S^{-1}(A \backslash \mathfrak{p}_1)\big)^{-1} = \big(S^{-1}S_{\mathfrak{p}_1}\big)^{-1} = S_{\mathfrak{p}_1}^{-1}S = S_{\mathfrak{p}_1}^{-1}$ since $S = A \backslash \bigcup \mathfrak{p}_j \subseteq A \backslash \mathfrak{p}_1 = S_{\mathfrak{p}_1}$ and $S_{\mathfrak{p}_1}$ is multiplicatively closed. Thus the localization

$$(S^{-1}A)_{S^{-1}\mathfrak{p}_1} = \big(S^{-1}A \backslash S^{-1}\mathfrak{p}_1\big)^{-1}(S^{-1}A) = S_{\mathfrak{p}_1}^{-1}S^{-1}A = S_{\mathfrak{p}_1}^{-1}A = A_{\mathfrak{p}_1}.$$

If we let K be the field $k(x_{m_2+1}, \ldots, x_{m_2+n}, \ldots)$, then $A_{\mathfrak{p}_1} = K[x_1, \ldots, x_{m_2}]_{(x_1, \ldots, x_{m_2})}$ as a subset of the field of fractions of A. Since $K[x_1, \ldots, x_{m_2}]$ is Noetherian by the Hilbert Basis Theorem (7.6), $A_{\mathfrak{p}_1}$ is Noetherian by (7.4). By (3.13), the height of $S^{-1}\mathfrak{p}_1$ is $\dim (S^{-1}A)_{S^{-1}\mathfrak{p}_1} = \dim A_{\mathfrak{p}_1} = \dim K[x_1, \ldots, x_{m_2}]_{(x_1, \ldots, x_{m_2})}$; this is m_2 by the example on p. 121.

Since each nonzero $a \in A$ only uses finitely many indeterminates, it can only be in finitely many $\mathfrak{p}_i$, and so each nonzero $a/s \in S^{-1}A$ can only be in finitely many maximal ideals $S^{-1}\mathfrak{p}_i$. This and the fact that the $(S^{-1}A)_{S^{-1}\mathfrak{p}_i}$ are Noetherian are the hypotheses of [7.9], which tells us $S^{-1}A$ is Noetherian.

Reformulate (11.1) in terms of the Grothendieck group $K(A_0)$ (Chapter 7, Exercise 25).

We recall the hypotheses and definitions. $A = \bigoplus A_n$ is a Noetherian graded ring, generated as an algebra over its summand A_0 by finitely many homogeneous elements x_j, $j = 1, \ldots, r$, of respective degrees $k_j > 0$. $M = \bigoplus M_n$ is a finitely generated graded A-module, so that each M_n is a finitely generated A_0-module. λ is an additive function from the the class of finitely generated A_0-modules to $\mathbb{Z}$. The Poincaré series of M with respect to λ is $P_\lambda(M, t) = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[[t]]$. (11.1) states that, with $q = \prod_{j=1}^{r}(1 - t^{k_j})$ and the standard definition for reciprocals of power series, $P_\lambda(M, t) \in q^{-1}\mathbb{Z}[t] \subsetneq \mathbb{Z}[[t]]$.

I feel my attempts to say something meaningful about this situation in terms of $K(A_0)$ have come up a little short, but here goes.

Write $\mathscr{F}_{\mathrm{gr}}(A)$ for the category of finitely generated graded A-modules and degree-preserving A-module homomorphisms. Define the graded Grothendieck group $K_{\mathrm{gr}}(A)$ of A from the $\mathscr{F}_{\mathrm{gr}}(A)$ using the same process by which we defined the original K-group: form the free abelian group on the set of isomorphism classes of $\mathscr{F}_{\mathrm{gr}}(A)$ and take the quotient by the subgroup generated by $[N]-[M]+[P]$ for all short exact sequences $0 \to N \to M \to P \to 0$ (where now the isomorphisms defining the classes and the maps in the sequences are degree-preserving). Write $\gamma_{\mathrm{gr}}(M)$ for the class of M in $K_{\mathrm{gr}}(A)$ and $\gamma(M_n)$ for the class of M_n in $K(A_0)$. As a degree-preserving homomorphism of graded A-modules induces an A_0-module homomorphism on each component, there is a natural map $\Phi\colon K_{\mathrm{gr}}(A) \to K(A_0)[[t]]$ given by $\gamma_{\mathrm{gr}}(M) \mapsto \sum \gamma(M_n)t^n$, where $K(A_0)[[t]]$ is just an additive group. There does not seem to be a reason to expect Φ to be either surjective or injective.

Since λ is additive, it induces a homomorphism $\lambda_0\colon K(A_0) \to \mathbb{Z}$ as in [7.26.i], which we can apply to each component in $K(A_0)[[t]]$; call this process Λ_0]. Then we can factor $P_\lambda(-, t)$ as

$$\begin{aligned} &\mathscr{F}_{\mathrm{gr}}(A) \xrightarrow{\gamma_{\mathrm{gr}}} K_{\mathrm{gr}}(A) \xrightarrow{\Phi} K(A_0)[[t]] \xrightarrow{\Lambda_0} \mathbb{Z}[[t]]: \\ &\quad M \mapsto \gamma_{\mathrm{gr}}(M) \mapsto \sum \gamma(M_n)t^n \mapsto \sum (\lambda_0 \circ \gamma)(M_n)t^n = \sum \lambda(M_n)t^n. \end{aligned}$$

From this one can see that the original additive function λ doesn't matter so much as the associated $\lambda_0 \in \operatorname{Hom}\bigl(K(A_0), \mathbb{Z}\bigr)$. Thus $\operatorname{im}(\Phi \circ \gamma_{\mathrm{gr}}) \subsetneq K(A_0)[[t]]$ is a collection of "universal Poincaré series" for finitely generated graded A-modules, each of which, when subjected to any $\lambda_0 \in \operatorname{Hom}\bigl(K(A_0), \mathbb{Z}\bigr)$, produces an element of $q^{-1}\mathbb{Z}[t] \subsetneq \mathbb{Z}[[t]]$.[2] Thus, finally, the best we can do in the general case is to say that the Poincaré series yields a bilinear map

$$Q\colon \operatorname{Hom}\bigl(K(A_0), \mathbb{Z}\bigr) \times K_{\mathrm{gr}}(A) \to \mathbb{Z}[[t]]$$

with $\operatorname{im} Q = q^{-1}\mathbb{Z}[t]$. This looks a bit different than the original, but is not much more interesting.[3]

Let A be a ring (not necessarily Noetherian). Prove that

$$1 + \dim A \le \dim A[x] \le 1 + 2\dim A.$$

If $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ is any ascending chain of length r in $\operatorname{Spec}(A)$, then $\mathfrak{p}_0[x] \subsetneq \mathfrak{p}_1[x] \subsetneq \cdots \subsetneq \mathfrak{p}_r[x] \subsetneq \mathfrak{p}_r + (x)$ is an ascending chain of length $r+1$ in $\operatorname{Spec}\bigl(A[x]\bigr)$; the last ideal is prime since it is the kernel of $A[x] \twoheadrightarrow A/\mathfrak{p}_r$ and the others by [2.7]. Thus $1 + \dim A \le \dim A[x]$.

By [3.21.iv], for $\mathfrak{p} \in \operatorname{Spec}(A)$ we have a homeomorphism between the set of primes of $A[x]$ lying over $\mathfrak{p}$ and $\operatorname{Spec}\bigl(k(\mathfrak{p}) \otimes_A A[x]\bigr)$, where $k(\mathfrak{p})$ is the field $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$. By [2.6], $k(\mathfrak{p}) \otimes_A A[x] \cong k(\mathfrak{p})[x]$; but $\dim k(\mathfrak{p})[x] = 1$, because any nonzero prime is maximal, so a chain of primes of $A[x]$ over a given $\mathfrak{p}$ has length no more than one, and hence contains at most two primes. Thus a chain of length r in $\operatorname{Spec}(A)$, containing $r+1$ primes, is the contraction of a chain of at most $2r+2$ primes of $A[x]$, which has length $2r+1$. Taking suprema over chains in $\operatorname{Spec}(A)$ gives $\dim A[x] \le 1 + 2\dim A$.

[2] One would like to lift the result about the image up to $K(A_0)[[t]]$, and say something like "$\operatorname{im}(\Phi \circ \gamma_{\mathrm{gr}}) \subseteq q^{-1}K(A_0)[t]$," but since $K(A_0)$ doesn't usually have a ring structure, multiplication and hence q^{-1} have no obvious meaning in $K(A_0)[[t]]$.

[3] With more restrictive hypotheses, we can say more; see http://math.stackexchange.com/questions/217612/exercise-11-5-from-atiyah-macdonald-hilbert-serre-theorem-and-grothendieck-grou and the articles by William Smoke linked therein.

Let A be a Noetherian ring. Then

$$\dim A[x] = 1 + \dim A,$$

and hence, by induction on n,

$$\dim A[x_1, \dots, x_n] = n + \dim A.$$

By [11.6], we have $\dim A[x] \geq 1 + \dim A$.

For the other direction, it will be enough to show that height $\mathfrak{P} \leq$ height $\mathfrak{p} + 1$ *whenever $\mathfrak{P}$ is a prime of $A[x]$ and* $\mathfrak{p} = \mathfrak{P}^c \lhd A$. *If we form rings of fractions of both rings with respect to $A \backslash \mathfrak{p}$ to get $\mathfrak{P}_\mathfrak{p} \lhd A_\mathfrak{p}[x]$ lying over $\mathfrak{p}_\mathfrak{p} \lhd A_\mathfrak{p}$, we see by (3.11.iv) that these have the same heights as $\mathfrak{P}$ and $\mathfrak{p}$, respectively, so we may assume A is local with maximal ideal* $\mathfrak{p}$.

Following the book's hint, we first show height $\mathfrak{p}[x] =$ height $\mathfrak{p}$. *If* height $\mathfrak{p} = m$, *then since A is a local Noetherian ring, there is by (11.13) a $\mathfrak{p}$-primary ideal $\mathfrak{q}$ of A generated by m elements.* $\mathfrak{q}[x]$ *is $\mathfrak{p}[x]$-primary by [4.7.iii], and is generated over $A[x]$ by the m generators of* $\mathfrak{q}$, *so by (11.16),* height $\mathfrak{p}[x] \leq m$. *We proved $m \leq$* height $\mathfrak{p}[x]$, *on the other hand, in [11.6].*

Now we show, by induction on height $\mathfrak{p}$, *that* height $\mathfrak{P} \leq$ height $\mathfrak{p}+1$. *For* height $\mathfrak{p} = 0$, *the result is again implied by the proof of [11.6]. Suppose that* height $\mathfrak{p} = m$ *and the result holds for primes of height $< m$. To show* height $\mathfrak{P} \leq m + 1$, *we need to see* height $\mathfrak{Q} \leq m$ *for each prime $\mathfrak{Q} \subsetneq \mathfrak{P}$. If $\mathfrak{Q}^c \subsetneq \mathfrak{p}$, then* height $\mathfrak{Q}^c < m$, *so* height $\mathfrak{Q} \leq m$ *by induction. If $\mathfrak{Q}^c = \mathfrak{p}$, then $\mathfrak{p}[x] \subseteq \mathfrak{Q} \subsetneq \mathfrak{P}$, and so, recalling from our proof of [11.6] that the longest chain of primes in $A[x]$ lying over $\mathfrak{p}$ contains two primes, we see $\mathfrak{Q} = \mathfrak{p}[x]$, whose height is m.*

Bibliography

[A–M] M. F. Atiyah and I. G. Macdonald, Introduction to Commutative Algebra, *Addison–Wesley, Boston, 1969,* http://www.math.toronto.edu/jcarlson/A--M.pdf.

[DoTh] Guram Donadze and Viji Thomas, “On a conjecture on the weak global dimension of Gaussian rings,” preprint, 3 July 2011. http://arxiv.org/abs/1107.0440. *Retrieved 20 Nov 2012.*

[Eisenbud] David Eisenbud, Commutative Algebra with a View Toward Algebraic Geometry, *Graduate Texts in Mathematics* **150**, *Springer, New York, 1995.*

[EisenEmail] David Eisenbud, private communication, 25 June 2012.

[GuoEmail] Hao Guo, private communication, 20 Apr 2015.

[KarpukSol] Dave Karpuk, “Solutions to Atiyah-Macdonald” (various dates), http://www-users.math.umd.edu/~karpuk/commalg.html. *Retrieved 24 Nov 2012*

[Kemper] Gregor Kemper, A Course in Commutative Algebra, *Graduate Texts in Mathematics* **256**, *Springer, New York, 2011*

[Lang] Serge Lang, Complex Analysis, *4th ed., Graduate Texts in Mathematics* **103**, *Springer, New York, 1999.*

[Milne] J.S. Milne, Algebraic Geometry, *Version 5.20, 14 Sept 2009,* http://jmilne.org/math/CourseNotes/AG.pdf. *Retrieved 20 Nov 2012.*

[Morandi] Patrick Morandi, “Artin’s Construction of an Algebraic Closure,” 8 Oct 2004, http://sierra.nmsu.edu/morandi/notes/algebraicclosure.pdf. *Retrieved 20 Nov 2012.*

[LeBruyn] Lieven LeBruyn, “Mumford’s treasure map,” December 13, 2008, http://neverendingbooks.org/index.php/mumfords-treasure-map.html. *Retrieved 20 Nov 2012.*

[MOPseud] http://mathoverflow.net/questions/45185/pseudonyms-of-famous-mathematicians/45195#45195

[Mollin] Richard A. Mollin, Advanced Number Theory With Applications, *CRC Press, Boca Raton, FL, 2010,* http://books.google.com/books?id=6I1setlljDYC&pg=PA154&q=rabinowitsch+rainich&f=false#v=onepage&q=rabinowitsch%20rainich&f=false. *Retrieved 24 Nov 2012.*

[MWBezout] mathwizard, “Bezout’s lemma (number theory)” (version 7), PlanetMath.org. http://planetmath.org/BezoutsLemma.html. *Retrieved 7 Dec 2012.*

[Nark] Władysław Narkiewicz, Rational Number Theory in the 20th Century: From PNT to FLT, *Springer, New York, 2011,* http://books.google.com/books?id=3SWNZaDM6iMC&pg=PA38&q=rabinowitsch+rainich. *Retrieved 24 Nov 2012.*

[Pahio] J. Pahikkala, “Prüfer ring” (version 85), PlanetMath.org, http://planetmath.org/PruferRing.html. *Retrieved Retrieved 20 Nov 2012.*

[PapaSol] Athanasios Papaioannou, “Solutions to Atiyah and MacDonald’s Introduction to Commutative Algebra,*” 5 Aug 2004,* http://classes7.com/Solutions-to-Atiyah-and-MacDonald%E2%80%99s-Introduction-to-Commutative-download-w40947.pdf. *Retrieved 20 Nov 2012.*

[Rabinowitsch] J.L. Rabinowitsch, (1929), “Zum Hilbertschen Nullstellensatz”, Math. Ann. **102** *(1): 520, doi:10.1007/BF01782361.*

[Tu] Loring Tu, An Introduction to Manifolds, *2nd ed., Springer, New York, 2011.*

[WooBezout] Chi Woo, "Bezout domain" (version 7), PlanetMath.org, `http://planetmath.org/BezoutDomain.html`*. Retrieved 20 Nov 2012.*

[WooGCD] Chi Woo, “gcd domain” (version 23), PlanetMath.org, `http://planetmath.org/GcdDomain.html`*. Retrieved 20 Nov 2012.*

[WooGCD2] Chi Woo, “properties of a gcd domain” (version 6), PlanetMath.org, `http://planetmath.org/PropertiesOfAGcdDomain.html`*. Retrieved 20 Nov 2012.*

[WPBezout] “Bézout domain,” Wikipedia: The Free Encyclopedia, *4 Nov 2012, 08:14 UTC, Wikimedia Foundation, Inc.,* `http://en.wikipedia.org/w/index.php?title=B%C3%A9zout_domain&oldid=521347068`*. Retrieved 20 Nov 2012.*

[WPGalois] “Galois connection,” Wikipedia: The Free Encyclopedia, *25 Sept 2012, 05:12 UTC, Wikimedia Foundation, Inc.,* `http://en.wikipedia.org/w/index.php?title=Galois_connection&oldid=514460687`*. Retrieved 21 Nov 2012.*

[WPGauss] “Gauss’s lemma (polynomial),” Wikipedia: The Free Encyclopedia, *19 Nov 2012, 16:33 UTC, Wikimedia Foundation, Inc.,* `http://en.wikipedia.org/w/index.php?title=Gauss's_lemma_(polynomial)&oldid=523900844`*. Retrieved 20 Nov 2012.*

[WPTaylor] “Taylor’s Theorem,” Wikipedia: The Free Encyclopedia, *19 November 2012, 14:06 UTC, Wikimedia Foundation, Inc.,* `http://en.wikipedia.org/w/index.php?title=Taylor%27s_theorem&oldid=523879884`*. Retrieved 20 Nov 2012.*