Solutions to the exercises in *Introduction to Commutative Algebra* by M. F. Atiyah and I. G. Macdonald

Artem Mavrin, Garrett Williams

Updated: `2022-10-17T05:37:22Z`

Contents

1

Rings and Ideals

1. 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.

Solution. Let $y = -x$. Then y is also nilpotent, so choose a positive integer n such that $y^n = 0$. We have

$$(1 - y)(1 + y + y^2 + \cdots + y^{n-1}) = 1 - y^n = 1$$

which shows that $1 + x = 1 - y$ is a unit.

Next, let $x \in A$ be nilpotent and $u \in A$ a unit. Then $u^{-1}x$ is nilpotent, so $1 + u^{-1}x$ is a unit by the first part. Therefore

$$u + x = u(1 + u^{-1}x).$$

Since it is a product of units, $u + x$ is a unit. $\square$

Alternative Solution. Since x belongs to the Jacobson radical of A by Proposition 1.8, Proposition 1.9 implies that $1 - xy$ is a unit for every $y \in A$. In particular, $1 + x$ is a unit (take $y = -1$). The rest follows as before. $\square$

2. Let A be a ring and let $A[x]$ be the ring of polynomials in an indeterminate x, with coefficients in A. Let $f = a_0 + a_1x + \cdots + a_nx^n \in A[x]$. 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. [If $b_0 + b_1x + \cdots + b_mx^m$ is the inverse of f, prove by induction on r that $a_n^{r+1}b_{m-r} = 0$. Hence show that a_n is nilpotent, and then use Ex. 1.]

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

iii) f is a zero-divisor $\iff$ there exists $a \neq 0$ in A such that $af = 0$. [Choose a polynomial $g = b_0 + b_1x + \cdots + b_mx^m$ of least degree m such that $fg = 0$. Then $a_nb_m = 0$, hence $a_ng = 0$ (because a_ng annihilates f and has degree $< m$). Now show by induction that $a_{n-r}g = 0$ $(0 \leq r \leq n)$.]

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 $\iff$ f and g are primitive.

Solution, i). $(\Leftarrow)$ If $a_1, \ldots, a_n$ are nilpotent in A, then they are also nilpotent in $A[x]$. Since the nilradical of $A[x]$ is an ideal, $a_1x + \cdots + a_nx^n$ is nilpotent. Moreover, if a_0 is a unit, then

$$f = a_0 + (a_1x + \cdots + a_nx^n)$$

is a unit by Exercise 1.

$(\Rightarrow)$ Suppose f is a unit in $A[x]$, and let $g \in A[x]$ be its inverse, with constant term b_0. The constant term of the product $fg = 1$ is $a_0b_0 = 1$, so a_0 is a unit in A.

Next, let $\mathfrak{p}$ be a prime ideal of A, and let $\overline{f}$ and $\overline{g}$ be the reductions of f and g, respectively, modulo $\mathfrak{p}$. Since $(A/\mathfrak{p})[x]$ is an integral domain, the equality $\overline{f}\overline{g} = 1$ implies

$$\deg \overline{f} + \deg \overline{g} = 0.$$

Therefore $\overline{f}$ is a constant polynomial in $(A/\mathfrak{p})[x]$. It follows that $a_1, \ldots, a_n \in \mathfrak{p}$, and since $\mathfrak{p}$ was arbitrarily chosen, it follows from Proposition 1.8 that $a_1, \ldots, a_n$ are nilpotent. □

Alternative Solution, i). Here is another proof of the forward direction of ii); this one uses the hint in the statement of the exercise. Suppose f is a unit, and let $g = b_0 + b_1x + \cdots + b_mx^m \in A[x]$ be its inverse. As before, the equation $fg = 1$ implies that $a_0b_0 = 1$, so a_0 and b_0 are units. Without loss of generality, assume $n \geq 1$, or else $f = a_0$ and we are done. We claim that $a_n^{r+1}b_{m-r} = 0$ for every $r \in \{0, 1, \ldots, m\}$.

First, the highest-order term of $fg = 1$ is $a_n b_m = 0$. Moreover, suppose $r \in \{0, 1, \ldots, m-1\}$ satisfies $a_n^{s+1} b_{m-s} = 0$ for all $s \in \{0, 1, \ldots, r\}$. We claim that $a_n^{r+2} b_{m-r-1} = 0$. For convenience, write $b_k = 0$ for $k > m$, and look at the coefficient of $x^{n+m-r-1}$ in the equation $fg = 1$:

$$a_0 b_{n+m-r-1} + a_1 b_{n+m-r} + \cdots + a_n b_{m-r-1} = 0. \tag{1.2.1}$$

By hypothesis, multiplying (1.2.1) by a_n^{r+1} yields $a_n^{r+2} b_{m-r-1} = 0$. By induction, it follows that $a_n^{r+1} b_{m-r} = 0$ for every $r \in \{0, 1, \ldots, m\}$. In particular, $a_n^{m+1} b_0 = 0$, and b_0 is a unit, so a_n is nilpotent. Since f is a unit and a_n is nilpotent, Exercise 1 implies that $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} = f - a_n x^n$ is a unit. Repeating this argument until only a_0 is left, we see that $a_1, \ldots, a_{n-1}$ are also all nilpotent. □

Solution, ii). ($\Leftarrow$) If $a_0, \ldots, a_n$ are nilpotent in A, then they are also nilpotent in $A[x]$. Since the nilradical of $A[x]$ is an ideal (Proposition 1.7), it follows that $f = a_0 + a_1 x + \cdots + a_n x^n$ is nilpotent in $A[x]$.

($\Rightarrow$) Suppose f is nilpotent, and let $\mathfrak{p}$ be a prime ideal of A. The reduction of f modulo $\mathfrak{p}$ is nilpotent in the integral domain $(A/\mathfrak{p})[x]$, whence it is zero modulo $\mathfrak{p}$. Therefore $a_0, a_1, \ldots, a_n \in \mathfrak{p}$, and the arbitrary choice of $\mathfrak{p}$ implies that $a_0, \ldots, a_n$ are in the nilradical of A by Proposition 1.8. □

Solution, iii). ($\Leftarrow$) If there exists a nonzero $a \in A$ such that $af = 0$, then f is a zero-divisor by definition.

($\Rightarrow$)[1] Suppose f is a zero-divisor, and let $g \in A[x]$ be a nonzero polynomial of least degree m such that $gf = 0$. Write

$$g = b_0 + b_1 x + \cdots + b_m x^m.$$

The $(m+n)$th coefficient of the product $fg = 0$ is $a_n b_m = 0$, so $a_n g$ has degree less than m. Moreover, since $gf = 0$, we also have $(a_n g) f = 0$, so by the minimality of m, it follows that $a_n g = 0$.

Next, suppose $r \in \{0, \ldots, n-1\}$ satisfies

$$a_n g = a_{n-1} g = \cdots = a_{n-r} g = 0.$$

Then we have

$$\begin{aligned} 0 = fg &= a_0 g + a_1 g x + \cdots + a_n g x^n \\ &= a_0 g + a_1 g x + \cdots + a_{n-r-1} g x^{n-r-1}. \end{aligned}$$

[1]This appears in [7, Theorem 2].

The highest-degree coefficient of the final sum above is $a_{n-r-1}b_m = 0$, so $a_{n-r-1}g$ has degree less than m. Again we have $(a_{n-r-1}g)f = 0$, whence $a_{n-r-1}g = 0$ by the minimality of the degree of g.

By induction on r, we conclude that $a_{n-r}g = 0$ for $0 \leq r \leq n$. In particular, $a_j b_m = 0$ for $0 \leq j \leq n$, so that $b_m f = 0$. □

Solution, iv). Let

$$f = a_0 + a_1 x + \cdots + a_n x^n, \qquad g = b_0 + b_1 x + \cdots + b_m x^m$$

be polynomials in $A[x]$, and let

$$gf = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$$

be their product, where

$$c_k = \sum_{\substack{i+j=k \\ 0\leq i\leq n \\ 0\leq j\leq m}} a_i b_j.$$

Define the ideals $\mathfrak{a} = (a_0, \ldots, a_n)$, $\mathfrak{b} = (b_0, \ldots, b_m)$, and $\mathfrak{c} = (c_0, \ldots, c_{m+n})$ of A. Clearly $\mathfrak{c} \subseteq \mathfrak{a} \cap \mathfrak{b}$.

($\Rightarrow$) Suppose fg is primitive, so that $\mathfrak{c} = (1)$. Since $\mathfrak{c} \subseteq \mathfrak{a} \cap \mathfrak{b}$, it follows that $\mathfrak{a} = \mathfrak{b} = (1)$, so f and g are primitive.

($\Leftarrow$) Suppose fg is not primitive, so that $\mathfrak{c} \neq (1)$. Then by Corollary 1.4, there exists a maximal ideal $\mathfrak{m}$ of A with $\mathfrak{c} \subseteq \mathfrak{m}$. Let $\overline{f}$ and $\overline{g}$ be the reductions of f and g modulo $\mathfrak{m}$. Since $(A/\mathfrak{m})[x]$ is an integral domain and $\mathfrak{m}$ contains the coefficients of fg, it follows that $\overline{f}\overline{g} = 0$, so either $\overline{f} = 0$ or $\overline{g} = 0$. Thus, either the coefficients of f or the coefficients of g are contained in $\mathfrak{m}$, whence either $\mathfrak{a}$ or $\mathfrak{b}$ is not the unit ideal. Therefore either f is not primitive or g is not primitive. □

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

Solution. First, we generalize Exercise 2, ii).

Claim 1.3.1. *A polynomial $f \in A[x_1, \ldots, x_r]$ is nilpotent if and only if its coefficients are all nilpotent.*

Proof. ($\Leftarrow$) Same as the original proof of this direction of Exercise 2, ii).

($\Rightarrow$) We induct on r, with the $r = 1$ case being handled by Exercise 2, ii). Consider a nilpotent $f \in A[x_1, \ldots, x_r]$, with $r > 1$, and write f as a single-variable polynomial (in the indeterminate x_r) with coefficients in $A[x_1, \ldots, x_{r-1}]$:

$$f = f_0 + f_1 x_r + \cdots + f_n x_r^n,$$

with each $f_i \in A[x_1, \ldots, x_{r-1}]$. Since f is nilpotent, Exercise 2, ii) implies that each f_i is nilpotent in $A[x_1, \ldots, x_{r-1}]$. By induction, we conclude that the coefficients of each f_i are nilpotent, and therefore the coefficients of f are nilpotent. □

Next, we generalize Exercise 2, i).

Claim 1.3.2. *A polynomial $f \in A[x_1, \ldots, x_r]$ is a unit if and only if its constant term is a unit in A and the rest of the coefficients are nilpotent.*

Proof. ($\Leftarrow$) Same as the original proof of this direction of Exercise 2, i).

($\Rightarrow$) We induct on r, with the $r = 1$ case being handled by Exercise 2, i). Consider an invertible $f \in A[x_1, \ldots, x_r]$, with $r > 1$. Again, write

$$f = f_0 + f_1 x_r + \cdots + f_n x_r^n,$$

with each $f_i \in A[x_1, \ldots, x_{r-1}]$. By Exercise 2, i), f_0 is a unit and $f_1, \ldots, f_n$ are nilpotent. By Claim 1.3.1, the coefficients of $f_1, \ldots, f_n$ are nilpotent. Moreover, by induction the constant term of f_0 is a unit and its other coefficients are nilpotent. Therefore the constant term of f is a unit, and the remaining coefficients are nilpotent. □

Now we generalize Exercise 2, iii).

Claim 1.3.3. *A polynomial $f \in A[x_1, \ldots, x_r]$ is a zero-divisor if and only if there exists a nonzero $a \in A$ such that $af = 0$.*

Proof. ($\Leftarrow$) Nothing to prove.

($\Rightarrow$) We induct on r, with the $r = 1$ case being handled by Exercise 2, iii). Suppose $r > 1$ and $f \in A[x_1, \ldots, x_r]$ is a zero-divisor. As before, write

$$f = f_0 + f_1 x_r + \cdots + f_n x_r^n,$$

with each $f_i \in A[x_1, \ldots, x_{r-1}]$. Since f is a zero-divisor in the polynomial ring $A[x_1, \ldots, x_{r-1}][x_r]$, Exercise 2, iii) implies that there exists a nonzero

$g \in A[x_1, \ldots, x_{r-1}]$ such that $gf = 0$. In particular, $gf_i = 0$ for all i. Let d_i be the highest power of x_{r-1} occurring in f_i, and let

$$d = \max\{d_0, d_1, \ldots, d_n\} + 1.$$

Then, define

$$h = f_0 + f_1 x_{r-1}^d + \cdots + f_n x_{r-1}^{nd},$$

a polynomial in $A[x_1, \ldots, x_{r-1}]$. Then $gh = 0$, so by induction, there exists a non-zero $a \in A$ such that $ah = 0$. In particular, a annihilates all the coefficients of h, and these, by the construction of h, include the coefficients of $f_0, f_1, \ldots, f_n$. Thus $af_i = 0$ for each i, and hence $af = 0$. □

Finally, we generalize Exercise 2, iv).

Claim 1.3.4. *Suppose $f, g \in A[x_1, \ldots, x_r]$. Then fg is primitive if and only if f and g are primitive*

Proof. The same proof as that of Exercise 2, iv) works here if we define $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ to be the ideals generated by the coefficients of f, g, and fg, respectively. □

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

Solution. Let $\mathfrak{N}$ and $\mathfrak{R}$ be the nilradical and Jacobson radical of $A[x]$, respectively. We necessarily have $\mathfrak{N} \subseteq \mathfrak{R}$ (by Proposition 1.8), so it suffices to prove that $\mathfrak{R} \subseteq \mathfrak{N}$. Let $f \in \mathfrak{R}$ be given. By Proposition 1.9, $1 + xf$ is a unit in $A[x]$, so by Exercise 2, i), the coefficients of the non-constant terms of $1 + xf$ are nilpotent. Thus, the coefficients of xf, and hence of f itself, are nilpotent, and so f itself is nilpotent by Exercise 2, ii), whence $\mathfrak{R} \subseteq \mathfrak{N}$. □

5. 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.

ii) If f is nilpotent, then a_n is nilpotent for all $n \geq 0$. Is the converse true? (See Chapter 7, Exercise 2.)

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

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

Solution, i). ($\Rightarrow$) If $f \in A[[x]]$ is a unit with inverse $g \in A[[x]]$, then looking at the constant term of $fg = 1$ shows that a_0 is a unit.

($\Leftarrow$) Suppose a_0 is a unit. Define $b_0, b_1, b_2, \ldots \in A$ recursively as $b_0 = a_0^{-1}$ and, having defined $b_0, \ldots, b_{r-1}$, define

$$b_r = -a_0^{-1} \sum_{k=1}^{r} a_k b_{r-k}.$$

Now let $g = \sum_{n=0}^{\infty} b_n x^n \in A[[x]]$. Then $fg = \sum_{n=0}^{\infty} c_n x^n$, where

$$c_n = \sum_{k=0}^{n} a_k b_{n-k}.$$

It follows that $c_0 = a_0 b_0 = 1$ and

$$c_n = \sum_{k=1}^{n} a_k b_{n-k} + a_0 b_n = \sum_{k=1}^{n} a_k b_{n-k} - a_0 a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k} = 0$$

for $n \geq 1$. Therefore $fg = 1$, so f is invertible. $\square$

We will occasionally need to use the following result.

Claim 1.5.1. *If A is an integral domain, then $A[[x]]$ is an integral domain.*

Proof. Suppose $f, g \in A[[x]]$ are nonzero. Write

$$f = \sum_{n=0}^{\infty} a_n x^n, \qquad g = \sum_{n=0}^{\infty} b_n x^n, \qquad fg = \sum_{n=0}^{\infty} c_n x^n,$$

where

$$c_n = \sum_{i+j=n} a_i b_j.$$

Choose the least non-negative integers i_0 and j_0 such that $a_{i_0} \neq 0$ and $b_{i_0} \neq 0$. Thus, $a_{i_0} b_{j_0} \neq 0$, and $a_i = b_j = 0$ for $i < i_0$ and $j < j_0$. If $n = i_0 + j_0$, then

$$c_n = a_{i_0} b_{j_0} + \sum_{\substack{i+j=n \\ i \neq i_0}} a_i b_j. \tag{1.5.1}$$

In every term of the sum in (1.5.1), either $i < i_0$ or $j < j_0$, so the sum is zero. Thus, $c_n = a_{i_0} b_{j_0} \neq 0$, so $fg \neq 0$, whence $A[[x]]$ is an integral domain. □

Solution, ii). Suppose f is nilpotent, and let $\mathfrak{p}$ be a prime ideal of A. The reduction $\overline{f}$ of f modulo $\mathfrak{p}$ is a nilpotent element of $(A/\mathfrak{p})[[x]]$. Since $(A/\mathfrak{p})[[x]]$ is an integral domain by Claim 1.5.1, it follows that $\overline{f} = 0$. Therefore, all the coefficients of f belong to the arbitrarily-chosen prime ideal $\mathfrak{p}$, whence they are all nilpotent by Proposition 1.8.

The converse is not necessarily true (at least for non-Noetherian rings—cf. Chapter 7, Exercise 2 for the Noetherian case). For example, consider the ring

$$A = \mathbf{F}_2[t, t^{1/2}, t^{1/3}, \ldots]/(t)$$

and the formal power series

$$f = \sum_{n=1}^{\infty} t^{1/n} x^n \in A[[x]].$$

The coefficients of f are all nilpotent. Working in characteristic 2,

$$\begin{aligned} f^{2^k} &= \left(tx + t^{1/2}x^2 + \cdots + t^{1/m}x^m + \sum_{n=m+1}^{\infty} t^{1/n}x^n \right)^{2^k} \\ &= t^{2^k} x^{2^k} + t^{2^k/2} x^{2 \cdot 2^k} + \cdots + t^{2^k/m} x^{m 2^k} + \left(\sum_{n=m+1}^{\infty} t^{1/n} x^n \right)^{2^k} \end{aligned}$$

for all positive integers k, m, so that

$$f^{2^k} = \sum_{n=1}^{\infty} t^{2^k/n} x^{2^k n} \neq 0.$$

Now if m is a positive integer, choose a positive integer k such that $2^k \geq m$, in which case $f^{2^k} \neq 0$, so $f^m \neq 0$. Thus, f is not nilpotent.[2] □

[2]Another example of a non-nilpotent power series with nilpotent coefficients can be found in [3, Example 2].

Solution, iii). ($\Rightarrow$) Suppose f belongs to the Jacobson radical of $A[[x]]$. If $y \in A$, then $1 - yf$ is a unit by Proposition 1.9, so the constant term of $1 - yf$, which is $1 - ya_0$, is a unit by i). Thus a_0 belongs to the Jacobson radical of A by Proposition 1.9 again.

($\Leftarrow$) Suppose a_0 belongs to the Jacobson radical of A. Take $g \in A[[x]]$, and let y be its constant term. Then $1 - ya_0$ is a unit in A by Proposition 1.9, and $1 - ya_0$ is the constant term of $1 - gf$. Thus, $1 - gf$ is a unit in $A[[x]]$ by i), so f belongs to the Jacobson radical of $A[[x]]$ by Proposition 1.9. $\square$

Before proving iv), we make two claims.

Claim 1.5.2. *If $f = \sum_{n=0}^{\infty} a_n x^n \in A[[x]]$, then $f - a_0$ belongs to the Jacobson radical of $A[[x]]$.*

Proof. The constant term of $f - a_0$ is zero, so it belongs to the Jacobson radical of A. Thus, by iii), $f - a_0$ belongs to the Jacobson radical of $A[[x]]$. $\square$

Claim 1.5.3. *Let $\mathfrak{m}$ be a maximal ideal of $A[[x]]$. Then its contraction $\mathfrak{m}^c = \mathfrak{m} \cap A$ consists of the constant terms of the elements of $\mathfrak{m}$.*

Proof. If $a \in \mathfrak{m}^c$, then a is the constant term of itself when viewed as an element of $\mathfrak{m}$. Conversely, suppose $f = \sum_{n=0}^{\infty} a_n x^n \in \mathfrak{m}$. We will show that $a_0 \in \mathfrak{m}^c$. By Claim 1.5.2, $f - a_0$ belongs to the Jacobson radical of $A[[x]]$, so in particular $f - a_0 \in \mathfrak{m}$. It follows that $a_0 = f - (f - a_0) \in \mathfrak{m}$. $\square$

Solution, iv). Suppose $r \in A \setminus \mathfrak{m}^c$. Then $r \notin \mathfrak{m}$, so there exists an $f \in A[[x]]$ and $g \in \mathfrak{m}$ such that $rf + g = 1$. Let a_0 and b_0 be the constant terms of f and g, respectively. Then $ra_0 + b_0 = 1$. Since $b_0 \in \mathfrak{m}^c$ by Claim 1.5.3, it follows that $(r) + \mathfrak{m}^c = A$. Thus, $\mathfrak{m}^c$ is a maximal ideal of A.

Next, we claim that $\mathfrak{m}$ is generated by $\mathfrak{m}^c$ and x. First, note that x belongs to the Jacobson radical of $A[[x]]$ by Claim 1.5.2, so $x \in \mathfrak{m}$. Thus, the ideal generated by $\mathfrak{m}^c$ and x is contained in $\mathfrak{m}$. Conversely, if $f = \sum_{n=0}^{\infty} a_n x^n \in \mathfrak{m}$, then $a_0 \in \mathfrak{m}^c$ by Claim 1.5.3, and writing

$$f = a_0 + x \left(\sum_{n=0}^{\infty} a_{n+1} x^n \right)$$

shows that f belongs to the ideal generated by $\mathfrak{m}^c$ and x. $\square$

Solution, v). Let $\mathfrak{p}$ be a prime ideal of A, and let $\mathfrak{p}[[x]]$ be the ideal of $A[[x]]$ consisting of formal power series with coefficients in $\mathfrak{p}$. Then $\mathfrak{p}$ is the contraction of $\mathfrak{p}[[x]]$, and we claim that $\mathfrak{p}[[x]]$ is a prime ideal of $A[[x]]$. Moreover, $\mathfrak{p}[[x]]$ is the kernel of the surjective homomorphism $A[[x]] \to (A/\mathfrak{p})[[x]]$ which sends $f \in A[[x]]$ to the formal power series whose coefficients are the coefficients of f modulo $\mathfrak{p}$. Thus,

$$A[[x]]/\mathfrak{p}[[x]] \cong (A/\mathfrak{p})[[x]].$$

Since $(A/\mathfrak{p})[[x]]$ is an integral domain by Claim 1.5.1, it follows that $\mathfrak{p}[[x]]$ is a prime ideal of $A[[x]]$. $\square$

Alternative Solution, v). Here is another proof that $\mathfrak{p}[[x]]$ is a prime ideal of $A[[x]]$ when $\mathfrak{p}$ is a prime ideal of A. Suppose $f, g \in A[[x]]$ such that $f, g \notin \mathfrak{p}[[x]]$. If

$$f = \sum_{k=0}^{\infty} a_k x^k, \qquad g = \sum_{k=0}^{\infty} b_k x^k,$$

then there exist minimal non-negative integers m, n such that $a_m \notin \mathfrak{p}$ and $b_n \notin \mathfrak{p}$. Consider

$$fg = \sum_{k=0}^{\infty} c_k x^k, \qquad c_k = \sum_{i+j=k} a_i b_j.$$

Let $k = m + n$. Then

$$c_k - a_m b_n = \sum_{\substack{i+j=k \\ i \neq m}} a_i b_j \tag{1.5.2}$$

In each summand of the right-hand side of (1.5.2), either $i < m$, so $a_i \in \mathfrak{p}$, or $j < n$, so $b_j \in \mathfrak{p}$. Therefore, the right-hand side of (1.5.2) belongs to $\mathfrak{p}$, so $c_k - a_m b_n \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $a_m, b_n \notin \mathfrak{p}$, it follows that $a_m b_n \notin \mathfrak{p}$. Thus, $c_k \notin \mathfrak{p}$, so $fg \notin \mathfrak{p}[[x]]$, and hence $\mathfrak{p}[[x]]$ is a prime ideal. $\square$

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

Solution. Let $\mathfrak{N}$ and $\mathfrak{R}$ be the nilradical and Jacobson radical of A, respectively. Since $\mathfrak{N} \subseteq \mathfrak{R}$ necessarily, it suffices to prove that $\mathfrak{R} \subseteq \mathfrak{N}$. Suppose instead that $\mathfrak{R} \not\subseteq \mathfrak{N}$. Then by assumption there exists a nonzero idempotent $e \in \mathfrak{R}$. By Proposition 1.9, $1 - e$ is a unit in A, but we also have

$$e(1-e) = e - e^2 = 0,$$

so $1 - e$ is a zero-divisor. This is a contradiction, and so $\mathfrak{R} \subseteq \mathfrak{N}$. □

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

Solution. Let $\mathfrak{p}$ be a prime ideal of A. If $x \in A$, then there exists an integer $n > 1$ such that $x^n - x = 0 \in \mathfrak{p}$. Since

$$x^n - x = x(x^{n-1} - 1),$$

either $x \in \mathfrak{p}$ or $x^{n-1} - 1 \in \mathfrak{p}$. Thus, every $x \in A$ is either zero modulo $\mathfrak{p}$ or a unit modulo $\mathfrak{p}$, so the quotient $A/\mathfrak{p}$ is a field, whence $\mathfrak{p}$ is maximal. □

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

Solution. Since $A \neq 0$, the set Σ of prime ideals of A is nonempty, and Σ is partially ordered by inclusion. Let P be a nonempty totally ordered subset of Σ, and let $\mathfrak{p} = \bigcap P$, which is an ideal. We claim that $\mathfrak{p}$ is prime, in which case it will follow that an arbitrary totally ordered subset of Σ has a lower bound in Σ, so Zorn's lemma will imply that Σ has a minimal element with respect to inclusion.

Suppose $x, y \notin \mathfrak{p}$ for some $x, y \in A$. Then there exist $\mathfrak{q}_1, \mathfrak{q}_2 \in P$ such that $x \notin \mathfrak{q}_1$ and $y \notin \mathfrak{q}_2$. Without loss of generality, assume $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$. Then $y \notin \mathfrak{q}_1$, so $xy \notin \mathfrak{q}_1$ since $\mathfrak{q}_1$ is prime. Therefore, $xy \notin \mathfrak{p}$, whence $\mathfrak{p}$ is a prime ideal. □

9. 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.

Solution. ($\Rightarrow$) If $\mathfrak{a} = r(\mathfrak{a})$, then $\mathfrak{a}$ is the intersection of all prime ideal containing $\mathfrak{a}$ by Proposition 1.14.

($\Leftarrow$) Suppose $\mathfrak{a}$ is the intersection of prime ideals $(\mathfrak{p}_i)_{i \in I}$. If $a \in A$ and $a^n \in \mathfrak{a}$ for some positive integer n, then $a^n \in \mathfrak{p}_i$ for all $i \in I$, and so $a \in \mathfrak{p}_i$ for all $i \in I$. Consequently, $a \in \bigcap_{i \in I} \mathfrak{p}_i = \mathfrak{a}$, so $r(\mathfrak{a}) \subseteq \mathfrak{a}$. The reverse inclusion follows from Proposition 1.13, so $\mathfrak{a} = r(\mathfrak{a})$. □

10. Let A be a ring, $\mathfrak{N}$ its nilradical. Show that 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.

Solution. (i) $\Rightarrow$ ii) and iii)) Suppose A has exactly one prime ideal; by Proposition 1.8, this prime ideal must be $\mathfrak{N}$. Since $\mathfrak{N}$ is contained in a maximal ideal by Corollary 1.4, and all maximal ideals are prime, it follows that $\mathfrak{N}$ is the only maximal ideal of A. In particular, $A/\mathfrak{N}$ is a field, and if $x \in A$ is not a unit, then $x \in \mathfrak{N}$ by Corollary 1.5, so every element of A is either a unit or nilpotent.

(ii) $\Rightarrow$ iii)) Suppose every element of A is either a unit or nilpotent. Then every nonzero element of $A/\mathfrak{N}$ is a unit, so $A/\mathfrak{N}$ is a field.

(iii) $\Rightarrow$ i)) Suppose $A/\mathfrak{N}$ is a field. Then $\mathfrak{N}$ is a maximal ideal of A. But $\mathfrak{N}$ is the intersection of all prime ideals of A by Proposition 1.8, so $\mathfrak{N}$ must be the only prime ideal of A. □

11. 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 $x \in A$;

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

iii) every finitely generated ideal in A is principal.

Solution, i). If $x \in A$, then $x + 1 = (x+1)^2 = x^2 + 2x + 1$, so $2x = 0$. □

Claim 1.11.1. *If A is a Boolean ring and an integral domain, then A is a field with two elements.*

Proof. If $x \in A$, then $x(x-1) = x^2 - x = 0$ since $x^2 = x$, so either $x = 0$ or $x = 1$ (and not both) since A is an integral domain. Thus A is a field with two elements. □

Solution, ii). Let $\mathfrak{p}$ be a prime ideal of A. Then $A/\mathfrak{p}$ is an integral domain which is also Boolean, so Claim 1.11.1 implies that $A/\mathfrak{p}$ is a field with two elements. It follows, in particular, that $\mathfrak{p}$ is a maximal ideal. □

Solution, iii). By induction, it suffices to prove that any ideal of A generated by two elements is principal. Take $x, y \in A$, and consider $\mathfrak{a} = (x, y)$. Let $z = x + y + xy \in \mathfrak{a}$. By i) we have

$$xz = x^2 + xy + x^2y = x + xy + xy = x + 2xy = x.$$

Similarly, $y = yz$. It follows that $\mathfrak{a} \subseteq (z)$, so $\mathfrak{a} = (z)$. □

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

Solution. Let A be a local ring with maximal ideal $\mathfrak{m}$, and let $x \in A$ be idempotent. If x is a unit, then dividing the equation $x^2 = x$ by x yields $x = 1$. Otherwise, $x \in \mathfrak{m}$. In that case, $1 - x$ is a unit by Proposition 1.9, and

$$x(1-x) = x - x^2 = 0$$

since $x^2 = x$, so $x = 0$. □

***Construction of an algebraic closure of a field* (E. Artin)**

13. 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 $\mathfrak{a} \neq (1)$.

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.

Solution. Suppose $\mathfrak{a} = (1)$. Then there is a finite set $F \subseteq \Sigma$ and a family $(g_f)_{f \in F}$ of elements of A such that $\sum_{f \in F} g_f f(x_f) = 1$. Let G be the finite set of all $f \in \Sigma$ such that either $f \in F$ or x_f occurs in a non-zero term of g_h for some $h \in F$. Let $g_f = 0$ for $f \in G \setminus F$. Then

$$\sum_{f \in G} g_f f(x_f) = 1, \tag{1.13.1}$$

and there are only finitely many indeterminates occurring in (1.13.1): they are among the x_f, for $f \in G$.

Therefore, we may restate (1.13.1) as an equation in $K[x_1, \ldots, x_n]$ for some positive integer n: there are polynomials $g_1, \ldots, g_n \in K[x_1, \ldots, x_n]$ and $f_1, \ldots, f_n \in \Sigma$ such that

$$g_1 f_1(x_1) + \cdots + g_n f_n(x_n) = 1. \tag{1.13.2}$$

Moreover, we may choose n to be the smallest positive integer such that such an equation holds.

Define $B = K[x_1, \ldots, x_{n-1}]$, and let $\mathfrak{b}$ be the ideal of B generated by $f_1(x_1), \ldots, f_{n-1}(x_{n-1})$ (if $n = 1$, take $B = K$ and $\mathfrak{b} = (0)$). The minimality of n implies that $\mathfrak{b} \neq (1)$. Consequently, by Corollary 1.4, there is a maximal ideal $\mathfrak{m}$ of B such that $\mathfrak{b} \subseteq \mathfrak{m}$. Let $f_n^*(x_n)$ be the image of $f_n(x_n)$ in $(B/\mathfrak{m})[x_n]$. By (1.13.2), $f_n^*(x_n)$ is a unit. However, $f_n^*(x_n)$ is a non-constant, monic polynomial, and $B/\mathfrak{m}$ is a field, so $f_n^*(x_n)$ cannot be a unit by Exercise 2, i). Thus, we have arrived at a contradiction, whence $\mathfrak{a} \neq (1)$.

Next, using Corollary 1.4, choose a maximal ideal $\mathfrak{m}$ of A such that $\mathfrak{a} \subseteq \mathfrak{m}$, and let $K_1 = A/\mathfrak{m}$. Then K_1 is an extension field of K via the composition $K \to A \to A/\mathfrak{m}$. Moreover, if $f \in \Sigma$ and α_f denotes the image of $x_f \in A$ in K_1, then $f(\alpha_f) = 0$ since $f(x_f) \in \mathfrak{m}$. Thus, every polynomial in Σ (i.e., every monic, irreducible polynomial with coefficients in K) has a root in K_1.

Repeat this construction countably many times to get a sequence of field extensions $K \subseteq K_1 \subseteq K_2 \subseteq \cdots$, and let L be the union[3] $L = \bigcup_{n=1}^{\infty} K_n$.

[3]Formally, we have a direct system $K \to K_1 \to K_2 \to K_3 \to \cdots$, and L is the direct limit (a colimit) $L = \varinjlim K_n$. We identify each K_n with its image in L under the canonical ring homomorphism $K_n \to L$.

Then L is a field extension of K. Let $\overline{K}$ be the subfield of L consisting of all elements of L which are algebraic over K. Now suppose f is a monic, irreducible polynomial with coefficients in $\overline{K}$. There is some positive integer n such that all the coefficients of f belong to K_n, so f has a root $\alpha \in K_{n+1}$. Since $\overline{K}(\alpha)/\overline{K}$ is a finite extension and $\overline{K}/K$ is algebraic, it follows that α is algebraic over K, and so $\alpha \in \overline{K}$. Thus, every monic irreducible polynomial over $\overline{K}$ has a root in $\overline{K}$, so $\overline{K}$ is algebraically closed. Since $\overline{K}$ is also algebraic over K, it follows that $\overline{K}$ is an algebraic closure of K.[4] □

14. 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.

Solution. Without loss of generality assume $A \neq 0$, so that Σ is nonempty. Let C be a subset of Σ which is totally ordered by $\subseteq$. If $\mathfrak{a} = \bigcup C$, then $\mathfrak{a}$ is an ideal of A, and if $x \in \mathfrak{a}$, then $x \in \mathfrak{c}$ for some $\mathfrak{c} \in C$, so x is a zero-divisor. Thus, $\mathfrak{a}$ consists of zero-divisors, so $\mathfrak{a} \in \Sigma$. Consequently, Σ has maximal elements by Zorn's Lemma.

Let $\mathfrak{p}$ be a maximal element of Σ. Suppose $x, y \in A \setminus \mathfrak{p}$. Then $\mathfrak{p}$ is a proper subset of the ideal $\mathfrak{p} + (x)$, so by the maximality of $\mathfrak{p}$ in Σ, there is a non-zero-divisor $u \in \mathfrak{p} + (x)$. Similarly, there is a non-zero-divisor $v \in \mathfrak{p} + (y)$. It follows that uv is a non-zero-divisor, and

$$uv \in (\mathfrak{p} + (x))(\mathfrak{p} + (y)) \subseteq \mathfrak{p} + (xy).$$

Since $\mathfrak{p}+(xy)$ contains a non-zero-divisor, it properly contains $\mathfrak{p}$. In particular, $xy \notin \mathfrak{p}$, so $\mathfrak{p}$ is a prime ideal. Thus, maximal elements of Σ are prime.[5]

Finally, let $x \in A$ be a zero-divisor. The arguments above still hold when Σ is replaced by the set Σ_x of ideals of A which contain x and in which every element is a zero-divisor. In fact, Σ_x is nonempty since $(x) \in \Sigma_x$, so Σ_x has maximal elements by Zorn's lemma, and every such maximal element is a

[4] This construction is carried out in, e.g., [6, Chapter V, Theorem 2.5 and Corollary 2.6]. The construction is simplified in [4] by showing that K_1 itself contains an algebraic closure of K, so constructing $K_2, K_3, \ldots$ is redundant.

[5] This result is also a corollary of a general "Prime Ideal Principle" [5] which states that certain ideals which are maximal with respect to some property are prime. In particular, see [5, Corollary 3.2] for the result of Exercise 14.

prime ideal by the same proof as before. Thus, every zero-divisor in A belongs to a prime ideal which consists of only zero-divisors, so the set of zero-divisors in A is a union of prime ideals. $\square$

The prime spectrum of a ring

15. 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 $V(E) = V(\mathfrak{a}) = V(r(\mathfrak{a}))$.

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

iii) if $(E_i)_{i\in I}$ is any family of subsets of A, then

$$V\left(\bigcup_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i).$$

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.

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 $\operatorname{Spec}(A)$.

Solution, i). If $\mathfrak{p}$ is a prime ideal of A, then $E \subseteq \mathfrak{p}$ if and only if $\mathfrak{a} \subseteq \mathfrak{p}$, so $V(E) = V(\mathfrak{a})$. Moreover, $\mathfrak{a} \subseteq r(\mathfrak{a})$. so $V(r(\mathfrak{a})) \subseteq V(\mathfrak{a})$. Conversely, $r(\mathfrak{a}) = \bigcap V(\mathfrak{a})$ by Proposition 1.14, so if $\mathfrak{p}$ is a prime ideal of A such that $\mathfrak{a} \subseteq \mathfrak{p}$, then $r(\mathfrak{a}) \subseteq \mathfrak{p}$ as well. Consequently, $V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$. $\square$

Solution, ii). $V(0) = X$ since 0 belongs to every prime ideal of A. $V(1) = \emptyset$ since prime ideals do not contain units (because they are proper ideals). $\square$

Solution, iii). If $\mathfrak{p}$ is a prime ideal of A, then $\bigcup_{i\in I} E_i \subseteq \mathfrak{p}$ if and only if $E_i \subseteq \mathfrak{p}$ for all $i \in I$, so $V\left(\bigcup_{i\in I} E_i\right) = \bigcap_{i\in I} V(E_i)$. $\square$

Solution, iv). Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, it follows that $V(\mathfrak{a}\cap\mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$. Moreover, if $\mathfrak{p} \in V(\mathfrak{a}\mathfrak{b})$, then $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ since $\mathfrak{p}$ is prime. Thus, $V(\mathfrak{a}\mathfrak{b}) \subseteq V(\mathfrak{a})\cup V(\mathfrak{b})$.

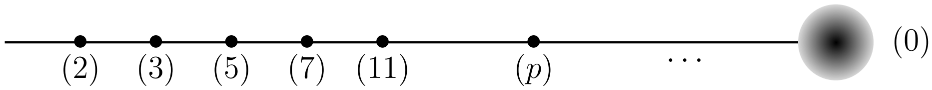

Figure 1.16.1: Spec($\mathbf{Z}$) consists of a closed point (p) for each positive prime number p, as well as a generic point corresponding to the minimal prime ideal (0).

Furthermore, since $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}$, it follows that $V(\mathfrak{a}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$, and likewise $V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$, so $V(\mathfrak{a}) \cup V(\mathfrak{b}) \subseteq V(\mathfrak{a} \cap \mathfrak{b})$, and we are done. $\square$

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

Solution. We draw inspiration from [2, Chapter II], [8, Chapter II, §1], and [9, Chapter 3].

(1) The ring $\mathbf{Z}$ is a principal ideal domain whose prime/irreducible elements are, up to a multiple of -1, exactly the positive prime integers. Consequently, the prime ideals of $\mathbf{Z}$ are the maximal ideals (p) for positive prime numbers p, and the zero ideal (0).

    Figure 1.16.1 is a picture of Spec($\mathbf{Z}$).

(2) The only prime ideal of the field $\mathbf{R}$ is the zero ideal. Thus, Spec($\mathbf{R}$) consists of a single point: $\bullet$. In fact, for any ring A, the space Spec(A) consists of a single point if and only if A is a field.

(3) The polynomial ring $\mathbf{C}[x]$ is a principal ideal domain, so its non-zero prime ideals are maximal and generated by monic, irreducible polynomials. Since $\mathbf{C}$ is algebraically closed, these polynomials are of the form $x - a$ for $a \in \mathbf{C}$. Also, the zero ideal (0) is prime and is a generic point of Spec($\mathbf{C}[x]$).

    If we identify the closed points of Spec($\mathbf{C}[x]$) (i.e., maximal ideals of $\mathbf{C}[x]$) with complex numbers via the correspondence $(x - a) \leftrightarrow a$, then the subspace topology on the set of closed points of Spec($\mathbf{C}[x]$) coincides with the classical Zariski topology on the affine line $\mathbf{A}^1_{\mathbf{C}} = \mathbf{C}$, in which the closed sets are sets on which a polynomial in one variable

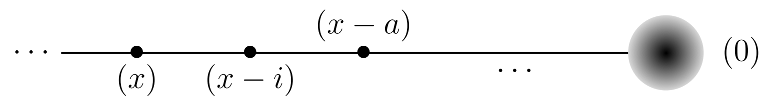

Figure 1.16.2: Spec($\mathbf{C}[\mathbf{x}]$) is the one-dimensional complex affine line consisting of a closed point $(x - a)$ for each $a \in \mathbf{C}$, as well as a generic point corresponding to the minimal prime ideal (0).

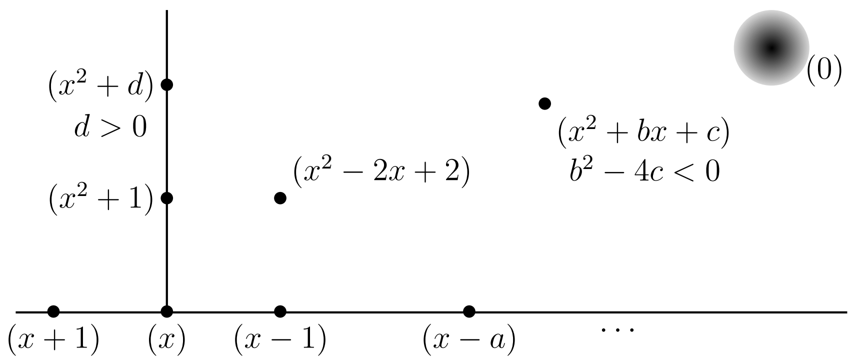

Figure 1.16.3: Spec($\mathbf{R}[x]$) can be visualized as the complex plane folded along the real axis, together with an extra generic point.

with complex coefficients vanishes (which, in the one-dimensional case, happens to be the cofinite topology).

Figure 1.16.2 is a picture of Spec($\mathbf{C}[x]$).

(4) The non-zero prime ideals of $\mathbf{R}[x]$ correspond to monic irreducible polynomials over $\mathbf{R}$. These are either of the form $x - a$ with $a \in \mathbf{R}$, or of the form $x^2 + bx + c$, with $b^2 - 4c < 0$. Each polynomial of the latter type corresponds to two conjugate complex numbers with non-zero imaginary part, the roots of the polynomial. Thus Spec($\mathbf{R}[x]$) can be seen as the complex plane folded along the real axis (or with conjugate points identified), together with an extra generic point, the zero ideal.

Figure 1.16.3 is a picture of Spec($\mathbf{R}[x]$).

(5) The non-zero prime ideals of $\mathbf{Z}[x]$ are of two forms. First, there are the principle prime ideals (f), where either $f \in \mathbf{Z}$ is a positive prime number or $f \in \mathbf{Z}[x]$ is a $\mathbf{Q}$-irreducible polynomial written with coefficients reduced to have g.c.d. $= 1$. Second, there are the maximal ideals, which

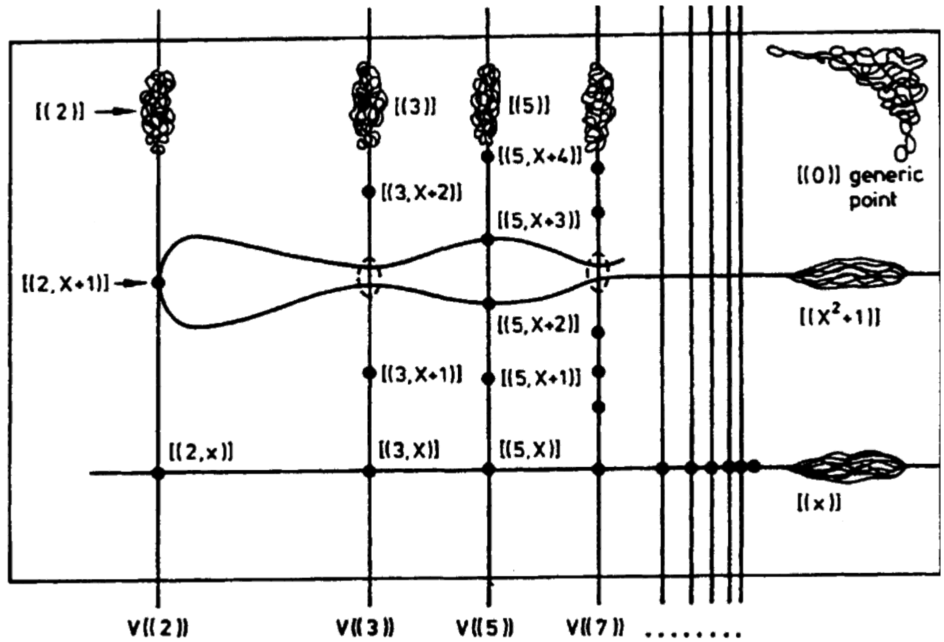

Figure 1.16.4: Picture of Spec($\mathbf{Z}[x]$) taken from [8, Chapter 2, §1, Example H]

are of the form (p, f), where p is a positive prime integer and $f \in \mathbf{Z}[x]$ is a monic polynomial which is irreducible modulo p.

Figure 1.16.4 is a picture of Spec($\mathbf{Z}[x]$) taken from [8, Chapter 2, §1, Example H].

17. For each $f \in A$, let X_f denote the complement of $V(f)$ in $X = \operatorname{Spec}(A)$. The sets X_f are open. Show that they form a basis of open sets for the Zariski topology, and that

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

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

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

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

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

vi) More generally, each X_f is quasi-compact.

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

The sets X_f are called *basic open sets* of $X = \operatorname{Spec}(A)$.

[To prove v), remark that it is enough to consider a covering of X by basic open sets X_{f_i} $(i \in I)$. Show that the f_i generate the unit ideal and hence that there is an equation of the form

$$1 = \sum_{i \in J} g_i f_i \qquad (g_i \in A)$$

where J is some *finite* subset of I. Then the X_{f_i} $(i \in J)$ cover X.]

Before proving the numbered parts of Exercise 17, we prove the following.

Claim 1.17.1. *The sets X_f, for $f \in A$, form a basis of open sets for the Zariski topology on X.*

Proof. It suffices to express every open subset of X as a union of sets of the form X_f. Take an open set $U \subseteq X$. Then there is some $E \subseteq A$ such that $U = X \setminus V(E)$. By Exercise 15, iii), we have

$$U = X \setminus V(E) = X \setminus \bigcap_{f \in E} V(f) = \bigcup_{f \in E} V(f). \qquad \square$$

Solution, i). By Exercise 15, iv), if $f, g \in A$, then

$$X_f \cap X_g = X \setminus (V(f) \cup V(g)) = X \setminus V(fg) = X_{fg}. \qquad \square$$

Solution, ii). If $f \in A$, then $X_f = \emptyset$ if and only if $V(f) = X$, which is the case if and only if f belongs to the nilradical of A by Proposition 1.8. $\square$

Solution, iii). If $f \in A$, then $X_f = X$ if and only if $V(f) = \emptyset$, which is the case if and only if f is a unit by Corollary 1.5. $\square$

Solution, iv). ($\Leftarrow$) If $r((f)) = r((g))$, then $V(f) = V(r((f))) = V(r((g))) = V(g)$ by Exercise 15, i), so $X_f = X_g$.

($\Rightarrow$) Suppose $X_f \subseteq X_g$, so that $V(g) \subseteq V(f)$. By Proposition 1.14, $r((f)) = \bigcap V(f)$ and $r((g)) = \bigcap V(g)$, so $r((f)) \subseteq r((g))$. Similarly, if $X_g \subseteq X_f$, then $r((g)) \subseteq r((f))$. Thus, if $X_f = X_g$, then $r((f)) = r((g))$. $\square$

Solution, v). This follows from vi) since $X = X_1$ by iii). $\square$

Solution, vi). Let $f \in A$, and suppose $(U_i)_{i\in I}$ is an open covering of X_f. For each $i \in I$, choose $E_i \subseteq A$ such that $U_i = X \setminus V(E_i)$. Then, as in the proof of Claim 1.17.1, we have $U_i = \bigcup_{g\in E_i} X_g$ for all $i \in I$. Letting $E = \bigcup_{i\in I} E_i$, it follows that $X_f = \bigcup_{g\in E} X_g$. Consequently, if we can find finitely many $g_1, \ldots, g_m \in E$ such that $X_f = X_{g_1} \cup \cdots \cup X_{g_n}$, then we can choose $i_1, \ldots, i_n \in I$ such that $g_k \in E_{i_k}$ for all $k \in \{1, \ldots, n\}$, whence $U_{i_1}, \ldots, U_{i_n}$ is a finite sub-covering of $(U_i)_{i\in I}$. Thus, it suffices to show that every covering of X_f by basic open sets has a finite sub-covering.

Suppose $(f_i)_{i\in I}$ is a family of elements of A with $X_f = \bigcup_{i\in I} X_{f_i}$. Let $\mathfrak{a}$ denote the ideal of A generated by $(f_i)_{i\in I}$. By Exercise 15, i) and Exercise 15, iii), we have

$$V(f) = \bigcap_{i\in I} V(f_i) = V\left((f_{i\in I})_{i\in I}\right) = V(\mathfrak{a}).$$

By Proposition 1.14, $r((f)) = r(\mathfrak{a})$. In particular, $f \in r(\mathfrak{a})$, so there is a positive integer n such that $f^n \in \mathfrak{a}$. Consequently, there exists a finite set $J \subseteq I$ and a finite family $(g_i)_{i\in J}$ of elements of A such that $f^n = \sum_{i\in J} g_i f_i$.

Now take a point $\mathfrak{p} \in X_f$ (so that $f \notin \mathfrak{p}$). Then there exists an $j \in J$ such that $f_j \notin \mathfrak{p}$ since, otherwise, $f^n = \sum_{i\in J} g_i f_i$ would belong to $\mathfrak{p}$, and hence f would belong to $\mathfrak{p}$. Thus, $\mathfrak{p} \in X_{f_j}$. It follows that $X_f = \bigcup_{i\in J} X_{f_i}$, so every covering of X_f by basic open sets has a finite sub-covering. Therefore X_f is quasi-compact. $\square$

Solution, vii). ($\Leftarrow$) Finite unions of open (respectively, compact) sets are open (respectively, compact) in any topological space. Consequently, a finite union of sets of the form X_f is open since each X_f is open, and quasi-compact since each X_f is quasi-compact by vi).

($\Rightarrow$) Suppose U is an open, compact subset of X. By openness and Claim 1.17.1, U is a union of basic open sets of the form X_f, so, by compactness, U is a finite union of such sets. $\square$

18. 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

$X = \mathrm{Spec}(A)$. 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 $\mathrm{Spec}(A)$ $\iff$ $\mathfrak{p}_x$ is maximal;

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

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

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 contains y, or else there is a neighborhood of y which does not contain x).

Solution, i). $\{x\}$ is closed if and only if $\{x\} = V(\mathfrak{p}_x)$ (by ii)), and this is the case if and only there is no prime ideal of A which properly contains $\mathfrak{p}_x$. By Corollary 1.4, it follows that $\{x\}$ is closed if and only if $\mathfrak{p}_x$ is maximal. $\square$

Solution, ii). Stare at iii). $\square$

Solution, iii). ($\Rightarrow$) Suppose $y \in \overline{\{x\}}$. Then y belongs to every closed subset of X to which x belongs. In particular, $V(\mathfrak{p}_x)$ is closed and $x \in V(\mathfrak{p}_x)$, so $y \in V(\mathfrak{p}_x)$, whence $\mathfrak{p}_x \subseteq \mathfrak{p}_y$.

($\Leftarrow$) Suppose $\mathfrak{p}_x \subseteq \mathfrak{p}_y$. Let C be a closed subset of X with $x \in C$. Choose $E \subseteq A$ such that $C = V(E)$. Since $x \in C$, we have $E \subseteq \mathfrak{p}_x \subseteq \mathfrak{p}_y$, so $y \in C$. Thus, y belongs to every closed subset of X to which x belongs, so $y \in \overline{\{x\}}$. $\square$

Solution, iv). Suppose $x, y \in X$ are distinct points. Then either $\mathfrak{p}_x \not\subseteq \mathfrak{p}_y$ or $\mathfrak{p}_y \not\subseteq \mathfrak{p}_x$. By iii), either $y \in X \setminus \overline{\{x\}}$ or $x \in X \setminus \overline{\{y\}}$. In the former case, $X \setminus \overline{\{x\}}$ is an open neighborhood of y which does not contain x, and in the latter case, $X \setminus \overline{\{y\}}$ is an open neighborhood of x which does not contain y. Thus, X is a T_0 space. $\square$

19. A topological space X is said to be irreducible if $X \neq \emptyset$ 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 $\mathrm{Spec}(A)$ is irreducible if and only if the nilradical of A is a prime ideal.

Solution. Let $X = \operatorname{Spec}(A)$.

($\Rightarrow$) Suppose X is irreducible. Take $f, g \in A$ such that fg is nilpotent. By Exercise 17, i) and Exercise 17, ii), $X_f \cap X_g = X_{fg} = \emptyset$. Thus, since X is irreducible, either $X_f = \emptyset$ or $X_g = \emptyset$. Again by Exercise 17, ii), either f is nilpotent or g is nilpotent. Therefore, the nilradical of A is a prime ideal.

($\Leftarrow$) Suppose the nilradical of A is a prime ideal. Let U and V be nonempty open subsets of X. Pick $x \in U$ and $y \in V$, and choose basic open sets X_f, X_g, for some $f, g \in A$, such that $x \in X_f \subseteq U$ and $y \in X_g \subseteq V$. Since X_f and X_g are non-empty, Exercise 17, ii) implies that f and g are not nilpotent, so, since the nilradical of A is a prime ideal, fg is also not nilpotent. Therefore, X_{fg} is nonempty (again by Exercise 17, ii)), so pick $z \in X_{fg}$. Moreover, $X_{fg} = X_f \cap X_g$ by Exercise 17, i), and $z \in X_{fg} = X_f \cap X_g \subseteq U \cap V$, so $U \cap V$ is nonempty. It follows that X is irreducible. $\square$

20. 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.

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

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?

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).

Solution, i). Let Y be an irreducible subspace of X, and let U, V be nonempty open subsets of $\overline{Y}$. Also, choose open subsets U', V' of X such that $U = \overline{Y} \cap U'$ and $V = \overline{Y} \cap V'$. In particular, $\overline{Y} \cap U'$ is nonempty, so $Y \cap U'$ is nonempty. Similarly, $Y \cap V'$ is nonempty. Since $Y \cap U'$ and $Y \cap V'$ are nonempty open subsets of the irreducible space Y, their intersection is nonempty. It follows that $U \cap V$ is nonempty, so $\overline{Y}$ is irreducible. $\square$

Solution, ii). Let Y be an irreducible subspace of X, and let Σ be the set of irreducible subspaces of X which contain Y. Let C be a subset of Σ which is totally ordered by $\subseteq$, and let $Z = \bigcup C$. In particular $Y \subseteq Z$. Moreover, suppose U, V are non-empty open subsets of Z. Choose open subsets U', V' of X such that $U = Z \cap U'$ and $V = Z \cap V'$. Pick points $u \in U$ and $v \in V$. Then $u, v \in W$ for some $W \in C$, and so $W \cap U'$ and $W \cap V'$ are non-empty open subsets of the irreducible space W, so their intersection is non-empty. Consequently, $U \cap V$ is nonempty, so Z is irreducible. Thus, $Z \in \Sigma$ is an upper bound for C. By Zorn's lemma, it follows that Σ has maximal elements. □

Solution, iii). If Y is a maximal irreducible subspace of X, then $\overline{Y}$ is irreducible by i), so $Y = \overline{Y}$ by the maximality of Y, whence Y is closed. Moreover, if $x \in X$, then the singleton $\{x\}$ is an irreducible subspace of X, and so it is contained in a maximal irreducible subspace by ii). Thus, maximal irreducible subspaces of X cover X.

In a Hausdorff space, any subspace with at least two distinct points has two open subsets which don't intersect (take non-intersecting open neighborhoods around two of the distinct points, which exist by the Hausdorff condition). Therefore, the irreducible components of a Hausdorff space are the singleton subspaces. □

Solution, iv). We begin with the following general proposition.

Claim 1.20.1. *A subset Y of $X = \operatorname{Spec}(A)$ is closed and irreducible if and only if $Y = V(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$ of A.*

Proof. ($\Rightarrow$) Suppose Y is a closed, irreducible subset of X. Since Y is closed, there is a set $E \subseteq A$ such that $Y = V(E)$. By Exercise 15, i) and Proposition 1.13, $Y = V(\mathfrak{p})$ where $\mathfrak{p}$ is the radical of the ideal of A generated by E. We claim that $\mathfrak{p}$ is prime.

Suppose $f, g \in A \setminus \mathfrak{p}$. By Proposition 1.14, $X_f \cap Y$ and $X_g \cap Y$ are non-empty. Thus, $X_f \cap Y$ and $X_g \cap Y$ are non-empty open subsets of Y, so by the irreducibility of Y, the intersection

$$(X_f \cap Y) \cap (X_g \cap Y) = (X_f \cap X_g) \cap Y = X_{fg} \cap Y$$

is nonempty ($X_f \cap X_g = X_{fg}$ by Exercise 17, i)). Consequently, there is a prime ideal of A which contains $\mathfrak{p}$ but not fg. By Proposition 1.14 again, $f, g \notin \mathfrak{p}$, so $\mathfrak{p}$ is a prime ideal.

($\Leftarrow$) Suppose $\mathfrak{p}$ is a prime ideal of A, and let $Y = V(\mathfrak{p})$. Let U, V be non-empty open subsets of Y. Since U and V are nonempty, choose $f, g \in A$ such that $\emptyset \neq X_f \cap Y \subseteq U$ and $\emptyset \neq X_g \cap Y \subseteq V$. Therefore, $f, g \notin \mathfrak{p}$, so $fg \notin \mathfrak{p}$. It follows that $X_{fg} \cap Y$ is nonempty, and $X_f \cap X_g = X_{fg}$ by Exercise 17, i), so $U \cap V$ is nonempty. Therefore, Y is irreducible. □

Returning to the proof of iv), note that Claim 1.20.1 implies that the assignment $\mathfrak{p} \mapsto V(\mathfrak{p})$ is an inclusion-reversing bijection between $\mathrm{Spec}(A)$ and the set of closed, irreducible subspaces of $\mathrm{Spec}(A)$. In particular, irreducible components correspond to minimal prime ideals. □

21. Let $\phi : A \to B$ be a ring homomorphism. Let $X = \mathrm{Spec}(A)$ and $Y = \mathrm{Spec}(B)$. 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 $\phi^* : Y \to X$. Show that

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

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

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

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

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

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

vii) Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$, and let K be the field of fractions of A. Let $B = (A/\mathfrak{p}) \times K$. Define $\phi : A \to B$ 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.

Solution, i)*.* If $f \in A$, then $\mathfrak{q} \in {\phi^*}^{-1}(X_f)$ if and only if $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q}) \in X_f$, which is the case if and only if $f \notin \phi^{-1}(\mathfrak{q})$, which occurs if and only if $\mathfrak{q} \in Y_{\phi(f)}$. Thus, ${\phi^*}^{-1}(X_f) = Y_{\phi(f)}$. Consequently, since preimages under ϕ^* of basic open sets in X are open in Y, it follows that ϕ^* is continuous. □

Solution, ii)*.* Let $\mathfrak{a}$ be an ideal of A. Suppose $\mathfrak{q} \in {\phi^*}^{-1}(V(\mathfrak{a}))$, so that

$\phi^{-1}(\mathfrak{q}) \in V(\mathfrak{a})$, or, in other words, $\mathfrak{a} \subseteq \phi^{-1}(\mathfrak{q})$. It follows that

$$\varphi(\mathfrak{a}) \subseteq \phi(\phi^{-1}(\mathfrak{q})) \subseteq \mathfrak{q}.$$

Consequently, $\mathfrak{a}^e \subseteq \mathfrak{q}$, so $\mathfrak{q} \in V(\mathfrak{a}^e)$. Thus, $\phi^{*-1}(V(\mathfrak{a})) \subseteq V(\mathfrak{a}^e)$.

Conversely, suppose $\mathfrak{q} \in V(\mathfrak{a}^e)$. Then $\mathfrak{a}^e \subseteq \mathfrak{q}$, so by Proposition 1.17, $\mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{a}^e) \subseteq \varphi^{-1}(\mathfrak{q})$. Thus, $\varphi^{-1}(\mathfrak{q}) \in V(\mathfrak{a})$, so $\mathfrak{q} \in \phi^{*-1}(V(\mathfrak{a}))$. It follows that $V(\mathfrak{a}^e) \subseteq \phi^{*-1}(V(\mathfrak{a}))$, so we conclude that $\phi^{*-1}(V(\mathfrak{a})) = V(\mathfrak{a}^e)$. $\square$

Solution, iii). Let $\mathfrak{b}$ be an ideal of B. Suppose $\mathfrak{p} \in \phi^*(V(\mathfrak{b}))$, so that there exists some $\mathfrak{q} \in V(\mathfrak{b})$ such that $\phi^{-1}(\mathfrak{q}) = \mathfrak{p}$. Then $\mathfrak{b} \subseteq \mathfrak{q}$, so $\mathfrak{b}^c \subseteq \mathfrak{p}$, whence $\mathfrak{p} \in V(\mathfrak{b}^c)$. Therefore, $\phi^*(V(\mathfrak{b})) \subseteq V(\mathfrak{b}^c)$, so, since $V(\mathfrak{b}^c)$ is closed, $\overline{\phi^*(V(\mathfrak{b}))} \subseteq V(\mathfrak{b}^c)$.

Conversely, suppose $\mathfrak{p} \in V(\mathfrak{b}^c)$, and let X_f, for some $f \in A$, be a basic open neighborhood of $\mathfrak{p}$. We claim that $\phi^*(V(\mathfrak{b})) \cap X_f$ is nonempty, whence it will follow that $\mathfrak{p} \in \overline{\phi^*(V(\mathfrak{b}))}$.

Since $r(\mathfrak{b}^c) = r(\mathfrak{b})^c$ by Exercise 1.18 in the text, Exercise 15, i) implies that $V(\mathfrak{b}^c) = V(r(\mathfrak{b})^c)$. In particular, $\mathfrak{p} \in V(r(\mathfrak{b})^c)$, so $r(\mathfrak{b})^c \subseteq \mathfrak{p}$. Since $\mathfrak{p} \in X_f$ (i.e., $f \notin \mathfrak{p}$) and $r(\mathfrak{b})^c \subseteq \mathfrak{p}$, it follows that $f \notin r(\mathfrak{b})^c$, so $\phi(f) \notin r(\mathfrak{b})$. Consequently, by Proposition 1.14 there exists a $\mathfrak{q} \in V(\mathfrak{b})$ such that $\phi(f) \notin \mathfrak{q}$. Thus, $f \notin \phi^*(\mathfrak{q})$, so $\phi^*(\mathfrak{q}) \in \phi^*(V(\mathfrak{b})) \cap X_f$. Therefore, $\phi^*(V(\mathfrak{b})) \cap X_f$ is nonempty, so $\mathfrak{p} \in \overline{\phi^*(V(\mathfrak{b}))}$, and hence $V(\mathfrak{b}^c) \subseteq \overline{\phi^*(V(\mathfrak{b}))}$. We conclude that $\overline{\phi^*(V(\mathfrak{b}))} = V(\mathfrak{b}^c)$. $\square$

Solution, iv). First, if $\mathfrak{q} \in Y$, then $\phi^*(\mathfrak{q}) \in V(\mathrm{Ker}(\phi))$ since $\phi(x) = 0 \in \phi^*(\mathfrak{q})$ for all $x \in \mathrm{Ker}(\phi)$. Thus, $\phi^*(Y) \subseteq V(\mathrm{Ker}(\phi))$.

Now suppose ϕ is surjective. Also, suppose $\mathfrak{a}$ is an ideal of A. Then $\phi(\mathfrak{a})$ is a subgroup of B (regardless of surjectivity). Moreover, if $y \in \phi(\mathfrak{a})$ and $b \in B$, then choose $x \in \mathfrak{a}$ and (since ϕ is surjective) $a \in A$ such that $\phi(x) = y$ and $\phi(a) = b$. Then $ax \in \mathfrak{a}$, so $by = \phi(ax) \in \phi(\mathfrak{a})$, and hence $\phi(\mathfrak{a})$ is an ideal of B.

Suppose $\mathfrak{p} \in V(\mathrm{Ker}(\phi))$. Then $\phi(\mathfrak{p})$ is an ideal of B by the previous paragraph. Moreover, $1 \notin \phi(\mathfrak{p})$ (otherwise, choose $x \in \mathfrak{p}$ such that $\phi(x) = 1 = \phi(1)$, in which case $x - 1 \in \mathrm{Ker}(\phi) \subseteq \mathfrak{p}$, which is impossible), so $\phi(\mathfrak{p})$ is a proper ideal of B. Finally, suppose $xy \in \phi(\mathfrak{p})$ for some $x, y \in B$. Choose $z \in \mathfrak{p}$ such that $\phi(z) = xy$ and, by surjectivity, $x', y' \in A$ such that $x = \phi(x')$ and $y = \phi(y')$. Then $z - x'y' \in \mathrm{Ker}(\phi) \subseteq \mathfrak{p}$, so $x'y' \in \mathfrak{p}$, whence $x' \in \mathfrak{p}$ or $y' \in \mathfrak{p}$, and hence $x = \phi(x') \in \phi(\mathfrak{p})$ or $y = \phi(y') \in \phi(\mathfrak{p})$. Thus, $\phi(\mathfrak{p})$ is a prime ideal of B whenever $\mathfrak{p} \in V(\mathrm{Ker}(\phi))$.

Next, it's necessarily the case that $\mathfrak{p} \subseteq \phi^*(\phi(\mathfrak{p}))$. Conversely, suppose $x \in \phi^*(\phi(\mathfrak{p}))$, so that $\phi(x) \in \phi(\mathfrak{p})$. Choose $y \in \mathfrak{p}$ such that $\phi(y) = \phi(x)$, so that $x - y \in \operatorname{Ker}(\phi) \subseteq \mathfrak{p}$, and hence $x \in \mathfrak{p}$. Thus, $\phi^*(\phi(\mathfrak{p})) = \mathfrak{p}$.

Summarizing the results so far, ϕ^* is a continuous (by i)) surjection of Y onto $V(\operatorname{Ker}(\phi))$. Next, suppose $\mathfrak{q}, \mathfrak{q}' \in Y$ such that $\phi^*(\mathfrak{q}) = \phi^*(\mathfrak{q}')$. Suppose $y \in \mathfrak{q}$, so that, since ϕ is surjective, there exists $x \in \phi^*(\mathfrak{q}) = \phi^*(\mathfrak{q}')$ such that $\phi(x) = y$, and hence $y \in \mathfrak{q}'$. Thus, $\mathfrak{q} \subseteq \mathfrak{q}'$, so $\mathfrak{q} = \mathfrak{q}'$ by symmetry, and hence ϕ^* is injective.

Lastly, to conclude that ϕ^* is a homeomorphism of Y onto $V(\operatorname{Ker}(\phi))$, it suffices to show that ϕ^* is a closed map. By iii), it suffices to show that $V(\mathfrak{b}^c) \subseteq \phi^*(V(\mathfrak{b}))$ whenever $\mathfrak{b}$ is an ideal of B. Thus, suppose $\mathfrak{p} \in V(\mathfrak{b}^c)$, so that $\phi^{-1}(\mathfrak{b}) \subseteq \mathfrak{p}$, and $\mathfrak{p} \in V(\operatorname{Ker}(\phi))$ since $\operatorname{Ker}(\phi) \subseteq \mathfrak{b}^c$. Since ϕ is surjective, $\mathfrak{b} = \phi(\phi^{-1}(\mathfrak{b})) \subseteq \phi(\mathfrak{p})$, so $\phi(\mathfrak{p}) \in V(\mathfrak{b})$, and hence $\mathfrak{p} = \phi^*(\phi(\mathfrak{p})) \in \phi^*(V(\mathfrak{b}))$. Therefore, $V(\mathfrak{b}^c) \subseteq \phi^*(V(\mathfrak{b}))$, and so ϕ^* is a homeomorphism of Y onto $V(\operatorname{Ker}(\phi))$. □

Solution, v). By iii), $V(\operatorname{Ker}(\phi)) = V((0)^c) = \overline{\phi^*(V(0))} = \overline{\phi^*(Y)}$ Thus, $\phi^*(Y)$ is dense in X if and only if $V(\operatorname{Ker}(\phi)) = X$, which is the case if and only if $\operatorname{Ker}(\phi)$ is contained in every prime ideal of A (i.e., by Proposition 1.8, if and only if $\operatorname{Ker}(\phi) \subseteq \mathfrak{N}$). □

Solution, vi). If $\mathfrak{q} \in \operatorname{Spec}(C)$, then $(\psi \circ \phi)^{-1}(\mathfrak{q}) = \phi^{-1}(\psi^{-1}(\mathfrak{q}))$. □

Solution, vii). Let A be an integral domain with just one non-zero prime ideal $\mathfrak{p}$, and let $X = \operatorname{Spec}(A)$. Then $X = \{(0), \mathfrak{p}\}$, where (0) is a generic point since A is an integral domain, and $\mathfrak{p}$ is a closed point by Exercise 18, i). Thus, the Zariski topology of X is $\{\emptyset, \{(0)\}, X\}$.

Moreover, let K be the field of fractions of A, let $B = (A/\mathfrak{p}) \times K$, and let $Y = \operatorname{Spec}(B)$. Then $Y = \{(A/\mathfrak{p}) \times (0), (0) \times K\}$; neither point of Y is generic, so automatically Y is not homeomorphic to X. In fact, both points of Y are maximal ideals of B, so both are closed points by Exercise 18, i), so the Zariski topology of Y is discrete.

Let $\phi : A \to B$ be the ring homomorphism given by $\phi(x) = (\bar{x}, x)$. Then $\phi^{-1}((A/\mathfrak{p}) \times (0)) = (0)$ and $\phi^{-1}((0) \times K) = \mathfrak{p}$, so $\phi^* : Y \to X$ is a continuous bijection. However, we've already observed that ϕ^* can't be a homeomorphism (e.g., $\phi^*(\{(A/\mathfrak{p}) \times K\}) = \{(0)\}$, so ϕ^* is not an open map). □

22. Let $A = \prod_{i=1}^n A_i$ be the 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 $\operatorname{Spec}(A_i)$.

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).

Solution. First, we claim that i) implies iii). Suppose $X = \operatorname{Spec}(A)$ is disconnected, and write $X = Y \cup Z$ for some disjoint, nonempty, and closed $Y, Z \subseteq X$. Choose ideals $\mathfrak{a}, \mathfrak{b}$ of A such that $Y = V(\mathfrak{a})$ and $Z = V(\mathfrak{b})$. Since Y and Z are nonempty, both $\mathfrak{a}$ and $\mathfrak{b}$ are proper ideals of A. Moreover, since $Y \cap Z = \emptyset$, there is no prime ideal of A which contains both $\mathfrak{a}$ and $\mathfrak{b}$, so $\mathfrak{a}$ and $\mathfrak{b}$ are coprime. Therefore there exist $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a+b = 1$. Since $ab \in \mathfrak{a}\mathfrak{b}$ and $V(\mathfrak{a}\mathfrak{b}) = Y \cup Z = X$ by Exercise 15, iv), Proposition 1.8 implies that ab is nilpotent, so $a^n b^n = 0$ for some positive integer n. Since $a \in r((a^n))$, $b \in r((b^n))$, and $a + b = 1$ it follows that $r((a^n))$ and $r((b^n))$ are coprime. Proposition 1.16 then implies that (a^n) and (b^n) are coprime. Choose $e \in (a^n)$ and $f \in (b^n)$ such that $e + f = 1$. Then $e - e^2 = e(1-e) = ef \in (a^n b^n) = (0)$, so $e - e^2 = 0$. Thus, e is idempotent. Moreover, $e \neq 0$ (since otherwise $1 = 1 - e = f \in (b^n) \subseteq \mathfrak{b}$), and $e \neq 1$ (since otherwise $1 = e \in (a^n) \subseteq \mathfrak{a}$). We conclude that i) implies iii).

Next, we claim that iii) implies ii). Suppose $e \in A$ is an idempotent such that $e \neq 0, 1$. Let $f = 1-e$. Since $e+f = 1$, the ideals (e) and (f) are coprime. In particular, it follows that $(e) \cap (f) = (ef)$. But $ef = e(1-e) = e - e^2 = 0$ since e is idempotent, so $(e) \cap (f) = (0)$. Now Proposition 1.10 implies that $A \cong A/(e) \times A/(f)$. Moreover, $A/(e)$ and $A/(f)$ are nonzero since $e \neq 0, 1$. Thus, iii) implies ii).

Finally, the following Claim 1.22.1 will imply both that ii) implies i) and—by induction—that the first part of the problem statement holds. $\square$

Claim 1.22.1. *Suppose $A = A_1 \times A_2$ for some rings A_1, A_2. Let $X = \mathrm{Spec}(A)$, $X_1 = \mathrm{Spec}(A_1)$ and $X_2 = \mathrm{Spec}(A_2)$. Let $\phi_1 : A \to A_1$ and $\phi_2 : A \to A_2$ be the projection homomorphisms, and let $\phi_1^* : X_1 \to X$ and $\phi_2^* : X_2 \to X$ be the associated continuous maps (cf. Exercise 21). Then the diagram*

$$X_1 \xrightarrow{\phi_1^*} X \xleftarrow{\phi_2^*} X_2$$

is a disjoint union.

Proof. Since ϕ_1 and ϕ_2 are surjective, Exercise 21, iv) implies that ϕ_1^* and ϕ_2^* are homeomorphisms onto their images, which are closed. Without loss of generality, identify their images with X_1 and X_2. Explicitly, X_1 consists of ideals of the form $\mathfrak{p} \times A_2$, where $\mathfrak{p}$ is a prime ideal of A_1, and X_2 consists of ideals of the form $A_1 \times \mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of A_2. In particular, $X_1 \cap X_2 = \emptyset$. Moreover, any prime ideal of A belongs to either X_1 or X_2, so $X = X_1 \cup X_2$, and we are done. $\square$

23. Let A be a Boolean ring (Exercise 11), and let $X = \mathrm{Spec}(A)$.

i) For each $f \in A$, the set X_f (Exercise 17) is both open and closed in X.

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

iii) The sets X_f are the only subsets of X which are both open and closed. [Let $Y \subseteq X$ be both open and closed. Since Y is open, it is a union of basic open sets X_f. Since Y is closed and X is quasi-compact (Exercise 17), Y is quasi-compact. Hence Y is a finite union of basic open sets; now use ii) above.]

iv) X is a compact Hausdorff space.

Claim 1.23.1. *Let $\mathfrak{p}$ be a prime ideal of a Boolean ring A, and let $f \in A$. Then exactly one of $f \in \mathfrak{p}$ and $1 - f \in \mathfrak{p}$ holds.*

Proof. Since A is a Boolean ring, $f(1-f) = f - f^2 = 0$, so $f(1-f) \in \mathfrak{p}$. Thus, either $f \in \mathfrak{p}$ or $1 - f \in \mathfrak{p}$ (and not both, or else $1 \in \mathfrak{p}$). $\square$

Solution, i). Suppose $f \in A$. If $\mathfrak{p}$ is a prime ideal of A, then $f \notin \mathfrak{p}$ if and only if $1 - f \in \mathfrak{p}$ by Claim 1.23.1. Thus, $X_f = V(1-f)$, so X_f is both open and closed. □

Solution, ii). Let $\mathfrak{a}$ be the ideal of A generated by $f_1, \ldots, f_n$. By Exercise 11, iii), there exists an $f \in A$ such that $\mathfrak{a} = (f)$. Consequently,

$$V(f_1) \cap \cdots \cap V(f_n) = V(\mathfrak{a}) = V(f)$$

by Exercise 15, so, taking complements, $X_{f_1} \cup \cdots \cup X_{f_n} = X_f$. □

Solution, iii). Suppose $Y \subseteq X$ is open and closed. Since X is quasi-compact by Exercise 17, v) and Y is closed, Y is quasi-compact. Since Y is open and quasi-compact, $Y = X_{f_1} \cup \cdots \cup X_{f_n}$ for some $f_1, \ldots, f_n \in A$ by Exercise 17, vii). Thus, $Y = X_f$ for some $f \in A$ by ii). Therefore, the sets X_f, for $f \in A$, are the only subsets of X which are both open and closed. □

Solution, iv). Since X is quasi-compact by Exercise 17, v), it suffices to prove that X is Hausdorff. Take $\mathfrak{p}, \mathfrak{q} \in X$ such that $\mathfrak{p} \neq \mathfrak{q}$. Without loss of generality, there exists $f \in \mathfrak{p}$ such that $f \notin \mathfrak{q}$. Consequently, $1 - f \notin \mathfrak{p}$ and $1 - f \in \mathfrak{q}$ by Claim 1.23.1. Then X_{1-f} and X_f are open neighborhoods of $\mathfrak{p}$ and $\mathfrak{q}$, respectively, and $X_f \cap X_{1-f} = \emptyset$ by Claim 1.23.1. Thus, X is Hausdorff. □

24. 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 $A(L)$.

Conversely, starting from a Boolean ring A, define an ordering on A as follows: $a \leq b$ means that $a = ab$. Show that, with respect to this ordering, A is a Boolean lattice. [The sup and inf are given by $a \vee b = a + b + ab$ and $a \wedge b = ab$, and the complement by $a' = 1 - a$.] In this way we obtain a one-to-one correspondence between (isomorphism classes of) Boolean rings and (isomorphism classes of) Boolean lattices.

25. 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.

26. Let A be a ring. The subspace of $\operatorname{Spec}(A)$ consisting of the *maximal* ideals of A, with the induced topology, is called the *maximal spectrum* of A and is denoted by $\operatorname{Max}(A)$. For arbitrary commutative rings it does not have the nice functorial properties of $\operatorname{Spec}(A)$ (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 $C(X) \to \mathbf{R}$ which takes f to $f(x)$. If $\tilde{X}$ denotes $\operatorname{Max}(C(X))$, we have therefore defined a mapping $\mu : X \to \tilde{X}$, namely $x \mapsto \mathfrak{m}_x$.

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

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 $U_{x_1}, \dots, U_{x_n}$, 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 $\mathfrak{m} = \mathfrak{m}_x$, since $\mathfrak{m}$ 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

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

Show that $\mu(U_f) = \tilde{U}_f$. The open sets U_f (resp. $\tilde{U}_f$) form a basis of the topology of X (resp. $\tilde{X}$) and therefore μ is a homeomorphism.

Thus X can be reconstructed from the ring of functions $C(X)$.

Affine algebraic varieties

27. Let k be an algebraically closed field and let

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

be a set of polynomial equations in n variables with coefficients in k. The set X of all points $x = (x_l, \dots, x_n) \in k^n$ which satisfy these equations is an *affine algebraic variety.*

Consider the set of all polynomials $g \in k[t_l, \dots, t_n]$ 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 $\tilde{X} = \mathrm{Max}(P(X))$, we have defined a mapping $\mu : X \to \tilde{X}$, 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 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).

28. Let $f_1, \ldots, f_m$ be elements of $k[t_1, \ldots, t_n]$. They determine a *polynomial mapping* $\phi : k^n \to k^m$: 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 $\phi : X \to Y$ 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 $P(Y) \to P(X)$.

2

Modules

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

Solution. Since m and n are coprime, m is a unit in $\mathbb{Z}/n\mathbb{Z}$. Moreover, $(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z})$ is generated by elements of the form $x \otimes y$, where $x \in \mathbb{Z}/m\mathbf{Z}$ and $y \in \mathbb{Z}/n\mathbf{Z}$, and $x \otimes y = x \otimes mm^{-1}y = mx \otimes m^{-1}y = 0 \otimes m^{-1}y = 0$. Therefore, $(\mathbf{Z}/m\mathbf{Z}) \otimes_{\mathbf{Z}} (\mathbf{Z}/n\mathbf{Z}) = 0$. □

In fact, here is a more general result that implies Exercise 1.

Claim 2.1.1. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a ring A. Then*

$$(A/\mathfrak{a}) \otimes_A (A/\mathfrak{b}) \cong A/(\mathfrak{a} + \mathfrak{b})$$

as A-algebras.

Proof. Suppose $a_1, a_2, b_1, b_2 \in A$ such that $a_1 - a_2 \in \mathfrak{a}$ and $b_1 - b_2 \in \mathfrak{b}$. Then

$$a_1 b_1 - a_2 b_2 = (a_1 - a_2) b_1 + a_2 (b_1 - b_2),$$

so $a_1 b_1 - a_2 b_2 \in \mathfrak{a} + \mathfrak{b}$. It follows that there is a well-defined function

$$f : (A/\mathfrak{a}) \times (A/\mathfrak{b}) \longrightarrow A/(\mathfrak{a} + \mathfrak{b}), \qquad f(x + \mathfrak{a}, y + \mathfrak{b}) = xy + \mathfrak{a} + \mathfrak{b}.$$

Moreover, f is A-bilinear, so by the universal property of the tensor product there is a unique A-linear map $\tilde{f} : (A/\mathfrak{a}) \otimes_A (A/\mathfrak{b}) \to A/(\mathfrak{a} + \mathfrak{b})$ such that

$\tilde{f}(a \otimes b) = f(a,b)$ for all $a \in A/\mathfrak{a}$ and $b \in A/\mathfrak{b}$. Note that not only is $\tilde{f}$ A-linear, it is in fact an A-algebra homomorphism.

Next, define the A-algebra homomorphism $g : A \to (A/\mathfrak{a}) \otimes_A (A/\mathfrak{b})$ by

$$g(x) = (x + \mathfrak{a}) \otimes (1 + \mathfrak{b}) = (1 + \mathfrak{a}) \otimes (x + \mathfrak{b})$$

for $x \in A$. Let $h_1 : A/\operatorname{Ker}(g) \to (A/\mathfrak{a}) \otimes_A (A/\mathfrak{b})$ denote the A-algebra homomorphism induced by g: $h(x + \operatorname{Ker}(g)) = g(x)$ for all $x \in A$. If $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$, then

$$g(x + y) = (x + \mathfrak{a}) \otimes (1 + \mathfrak{b}) + (1 + \mathfrak{a}) \otimes (b + \mathfrak{b}) = 0,$$

so $\mathfrak{a} + \mathfrak{b} \subseteq \operatorname{Ker}(g)$. It follows that there is an A-algebra homomorphism $h_2 : A/(\mathfrak{a} + \mathfrak{b}) \to A/\operatorname{Ker}(g)$ given by $h_2(x + \mathfrak{a} + \mathfrak{b}) = x + \operatorname{Ker}(g)$ for all $a \in A$. Now let

$$\tilde{g} \coloneqq h_1 \circ h_2 : A/(\mathfrak{a} + \mathfrak{b}) \longrightarrow (A/\mathfrak{a}) \otimes_A (A/\mathfrak{b}).$$

Then $\tilde{g}$ is an A-algebra homomorphism, and calculation shows that it is the inverse of $\tilde{f}$. The claim follows. $\square$

9. 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.

Solution. Let $f : M' \to M$ and $g : M \to M''$ be the A-module morphisms in the exact sequence. Choose generators $x_1, \ldots, x_m$ of M' and $z_1, \ldots, z_n$ of M''. Since g is surjective, choose $y_1, \ldots, y_n \in M$ such that $z_i = g(y_i)$ for $i \in \{1, \ldots, n\}$. We claim that $M = (f(x_1), \ldots, f(x_m), y_1, \ldots, y_n)$.

Take $y \in M$. Choose $b_1, \ldots, b_n \in A$ such that

$$g(y) = b_1 z_1 + \cdots + b_n z_n = g(b_1 y_1 + \cdots + b_n y_n).$$

Then $y - b_1 y_1 - \cdots - b_n y_n \in \operatorname{Ker}(g) = \operatorname{Im}(f)$, so there exists $x \in M'$ such that $f(x) = y - b_1 y_1 - \cdots - b_n y_n$. Now choose $a_1, \ldots, a_m \in A$ such that $x = a_1 x_1 + \cdots + a_m x_m$. Thus,

$$\begin{aligned} y &= f(x) + b_1 y_1 + \cdots + b_n y_n \\ &= a_1 f(x_1) + \cdots + a_m f(x_m) + b_1 y_1 + \cdots + b_n y_n, \end{aligned}$$

whence $M = (f(x_1), \ldots, f(x_m), y_1, \ldots, y_n)$ as claimed.[1] $\square$

[1]Did we need exactness at M'? Where (if anywhere) is the injectivity of f used?

Flatness and Tor

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

i) M is flat;

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

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

[To show that i) $\implies$ ii), take a free resolution of N and tensor it with M. Since M is flat, the resulting sequence is exact and therefore its homology groups, which are the $\mathrm{Tor}_n^A(M, N)$, are zero for $n > 0$. To show that iii) $\implies$ i), let $0 \to N' \to N \to N'' \to 0$ be an exact sequence. Then, from the Tor sequence,

$$\mathrm{Tor}_1(M, N) \longrightarrow M \otimes N' \longrightarrow M \otimes N \longrightarrow M \otimes N'' \longrightarrow 0$$

is exact. Since $\mathrm{Tor}_1(M, N'') = 0$ it follows that M is flat.]

Solution. Suppose M is flat, and let N be an A-module. Consider a free resolution $\cdots \to F_2 \to F_1 \to F_0 \to N \to 0$. Tensoring this exact sequence with M yields a chain complex

$$\cdots \longrightarrow F_2 \otimes_A M \longrightarrow F_1 \otimes_A M \longrightarrow F_0 \otimes_A M \longrightarrow 0$$

which is exact at each positive index since M if flat. Thus the homology groups of this chain complex, which are the $\mathrm{Tor}_n^A(M, N)$, are all zero. Thus i) implies ii).

Moreover, iii) follows immediately from ii).

Finally, suppose $\mathrm{Tor}_1^A(M, N) = 0$ for all A-modules N. Consider a short exact sequence $0 \to N' \to N \to N'' \to 0$ of A-modules. Then there is a canonical long exact sequence

$$\begin{array}{l} \cdots \longrightarrow \mathrm{Tor}_2^A(M, N') \longrightarrow \mathrm{Tor}_2^A(M, N) \longrightarrow \mathrm{Tor}_2^A(M, N'') \\ \hookrightarrow \mathrm{Tor}_1^A(M, N') \longrightarrow \mathrm{Tor}_1^A(M, N) \longrightarrow \mathrm{Tor}_1^A(M, N'') \\ \hookrightarrow M \otimes_A N' \longrightarrow M \otimes_A N \longrightarrow M \otimes_A N'' \longrightarrow 0. \end{array}$$

Since $\mathrm{Tor}_1^A(M, N'') = 0$, the end of this long exact sequence is the short exact sequence

$$0 \longrightarrow M \otimes_A N' \longrightarrow M \otimes_A N \longrightarrow M \otimes_A N'' \longrightarrow 0.$$

Thus, M is flat, so iii) implies i). $\square$

3

Rings and Modules of Fractions

1. 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 $sM = 0$.

Solution. ($\Leftarrow$) Suppose there exists an $s \in S$ such that $sM = 0$. Take $x \in S^{-1}M$, and write $x = y/t$ for some $y \in M$ and $t \in S$. Then $x = y/t = (sy)/(st) = 0/(st) = 0$. Thus, $S^{-1}M = 0$. (This direction does not use M being finitely generated.)

($\Rightarrow$) Suppose $S^{-1}M = 0$. Since M is finitely generated, pick generators $x_1, \ldots, x_n \in M$. Since $x_1 = \cdots = x_n = 0$ in $S^{-1}M$, there exist $s_1, \ldots, s_n \in S$ such that $s_1 x_1 = \cdots = s_n x_n = 0$ in M. Then $s \coloneqq s_1 \cdots s_n \in S$ since S is multiplicatively closed, and $sx_1 = \cdots = sx_n = 0$, so $sM = 0$. $\square$

7

Noetherian Rings

2. 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.

Solution. ($\Rightarrow$) This direction follows from Chapter 1, Exercise 5, ii), which does not use the Noetherian assumption.

($\Leftarrow$) Suppose each a_n is nilpotent. Let $\mathfrak{a}$ be the ideal generated by the a_n's, which is contained in the nilradical of A. Since A is Noetherian, there exist (necessarily nilpotent) $b_1, \dots, b_N \in A$ such that $\mathfrak{a} = (b_1, \dots, b_N)$. For each n, choose $r_{n,1}, \dots, r_{n,N} \in A$ such that

$$a_n = r_{n,1} b_1 + \cdots + r_{n,N} b_N.$$

Then we have

$$f = \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} \sum_{k=1}^{N} r_{n,k} b_k x^n = \sum_{k=1}^{N} b_k \left(\sum_{n=1}^{\infty} r_{n,k} x^n \right).$$

Since the nilradical of $A[[x]]$ is an ideal, f is nilpotent. $\square$

Bibliography

[1] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969, pp. ix+128.

[2] David Eisenbud and Joe Harris. *The geometry of schemes*. Vol. 197. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. x+294. DOI: 10.1007/b97680.

[3] David E. Fields. "Zero divisors and nilpotent elements in power series rings". *Proc. Amer. Math. Soc.* 27 (1971), pp. 427–433. DOI: 10.2307/2036469.

[4] Robert Gilmer. "A Note on the Algebraic Closure of a Field". *Amer. Math. Monthly* 75.10 (1968), pp. 1101–1102. DOI: 10.2307/2315743.

[5] T. Y. Lam and Manuel L. Reyes. "A prime ideal principle in commutative algebra". *J. Algebra* 319.7 (2008), pp. 3006–3027. DOI: 10.1016/j.jalgebra.2007.07.016.

[6] Serge Lang. *Algebra*. third. Vol. 211. Graduate Texts in Mathematics. Springer-Verlag, New York, 2002, pp. xvi+914. DOI: 10.1007/978-1-4613-0041-0.

[7] N. H. McCoy. "Remarks on divisors of zero". *Amer. Math. Monthly* 49 (1942), pp. 286–295. DOI: 10.2307/2303094.

[8] David Mumford. *The red book of varieties and schemes*. Vol. 1358. Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1999, pp. x+306. DOI: 10.1007/b62130.

[9] Ravi Vakil. "The Rising Sea: Foundations Of Algebraic Geometry". Nov. 2017. URL: http://math.stanford.edu/~vakil/216blog/index.html.