Assignment for Algebra III

Zhang Chi (201828001207022)
zhangchi2018@itp.ac.cn

July 8, 2021

Exercise 1

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

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

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

(d) $(\cap_i \mathfrak{a}_i : \mathfrak{b}) = \cap_i (\mathfrak{a}_i : \mathfrak{b})$

(e) $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \cap_i (\mathfrak{a} : \mathfrak{b}_i)$

Proof. **(a)** For any $x \in \mathfrak{a}$, we have $x\mathfrak{b} = \mathfrak{b}x \subseteq \mathfrak{a}$, so $x \in (\mathfrak{a} : \mathfrak{b})$. This shows that $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$.

(b) For any $x \in (\mathfrak{a} : \mathfrak{b})$, by definition $x\mathfrak{b} \subseteq \mathfrak{a}$ holds. Thus $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$.

(c) First we prove

$$((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}), \tag{1}$$

then prove

$$(\mathfrak{a} : (\mathfrak{b} : \mathfrak{c})) = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}). \tag{2}$$

For (1), take any $x \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c})$, we have

$$x\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b}),$$

which is equivalent to say that

$$x\mathfrak{c}\mathfrak{b} = x\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a}.$$

So $x \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$, completing one direction. Conversely, for any $y \in (\mathfrak{a} : \mathfrak{b}\mathfrak{c})$, we have

$$y\mathfrak{c}\mathfrak{b} = y\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{a},$$

by which we conclude

$$y\mathfrak{c} \subseteq (\mathfrak{a} : \mathfrak{b}),$$

furthermore

$$y \in ((\mathfrak{a} : \mathfrak{b}) : \mathfrak{c}),$$

completing the other direction.

For (2), for any $z \in (\mathfrak{a} : (\mathfrak{b} : \mathfrak{c}))$, we have

$$z(\mathfrak{b} : \mathfrak{c}) \subseteq \mathfrak{a}$$

(d) If $x \in (\cap_i \mathfrak{a}_i, \mathfrak{b})$, we have

$$x\mathfrak{b} \subseteq \cap_i \mathfrak{a}_i,$$

hence

$$x\mathfrak{b} \subseteq \mathfrak{a}_i$$

holds for all i. But this is equivalent to saying that

$$x \in (\mathfrak{a}_i : \mathfrak{b})$$

for all i, which implies that

$$x \in \cap_i (\mathfrak{a}_i : \mathfrak{b}).$$

Conversely, if $y \in \cap_i (\mathfrak{a}_i : \mathfrak{b})$,

$$y\mathfrak{b} \subseteq \mathfrak{a}_i$$

for all i. Thus

$$y\mathfrak{b} = \cap_i \mathfrak{a}_i,$$

which means that

$$y \in (\cap_i \mathfrak{a}_i : \mathfrak{b}).$$

(e) If $x \in (\mathfrak{a} : \sum_i \mathfrak{b}_i)$, we have

$$x(\sum_i \mathfrak{b}_i) = \sum_i x\mathfrak{b}_i \subseteq \mathfrak{a},$$

in particular

$$x\mathfrak{b}_i \subseteq \mathfrak{a}$$

holds for each i, thus

$$x \in (\mathfrak{a} : \mathfrak{b}_i)$$

for each i and equivalently

$$x \in \cap_i (\mathfrak{a} : \mathfrak{b}_i).$$

Conversely, if $y \in \cap_i (\mathfrak{a} : \mathfrak{b}_i)$, we have

$$y\mathfrak{b}_i \subseteq \mathfrak{a}$$

for all i, thus

$$y(\sum_i \mathfrak{b}_i) \subseteq \mathfrak{a},$$

or equivalently

$$y \in (\mathfrak{a} : \sum_i \mathfrak{b}_i).$$

□

Exercise 2

If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of A and if $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals of B, then

$$\begin{aligned}
&(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e, (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c,\\
&(\mathfrak{a}_1 \cap \mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e \cap \mathfrak{a}_2^e, (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c = \mathfrak{b}_1^c \cap \mathfrak{b}_2^c,\\
&(\mathfrak{a}_1\mathfrak{a}_2)^e = \mathfrak{a}_1^e\mathfrak{a}_2^e, (\mathfrak{b}_1\mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c\mathfrak{b}_2^c,\\
&(\mathfrak{a}_1 : \mathfrak{a}_2)^e \subseteq (\mathfrak{a}_1^e : \mathfrak{a}_2^e), (\mathfrak{b}_1 : \mathfrak{b}_2)^c \subseteq (\mathfrak{b}_1^c : \mathfrak{b}_2^c),\\
&(\sqrt{\mathfrak{a}})^e \subseteq \sqrt{\mathfrak{a}^e}, (\sqrt{\mathfrak{b}})^c = \sqrt{\mathfrak{b}^c}.
\end{aligned}$$

The set of ideals E is closed under sum and product, and C is closed under the other three operations.

Proof. **Sum**. We naturally have $(\mathfrak{a}_1+\mathfrak{a}_2)^e \subseteq \mathfrak{a}_1^e + \mathfrak{a}_2^e$. For the converse, taking any $\sum_i y_i f(x_i) \in \mathfrak{a}_1^e$, we have

$$\sum_i y_i f(x_i) = \sum_i y_i f(x_i + 0) \subseteq (\mathfrak{a}_1+\mathfrak{a}_2)^e,$$

showing that

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

Anagolously,

$$\mathfrak{a}_2^e \subseteq (\mathfrak{a}_1+\mathfrak{a}_2)^e,$$

implying that

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

This shows that

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

The other identity about sum is easier to prove, since for any $f^{-1}(x)+f^{-1}(y) \in \mathfrak{b}_1^c + \mathfrak{b}_2^c$, we have $f^{-1}(x)+f^{-1}(y) = f^{-1}(x+y) \in (\mathfrak{b}_1+\mathfrak{b}_2)^c$, showing that

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

Intersection For $\sum_i y_i f(x_i) \in (\mathfrak{a}_1 \cap \mathfrak{a}_2)^e$ with all $y_i \in B$ and $x_i \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, since $x_i \in \mathfrak{a}_1$ and $x_i \in \mathfrak{a}_2$, we have

$$\sum_i y_i f(x_i) \in \mathfrak{a}_1^e$$

and

$$\sum_i y_i f(x_i) \in \mathfrak{a}_2^e.$$

So

$$\sum_i y_i f(x_i) \in \mathfrak{a}_1^e \cap \mathfrak{a}_2^e,$$

implying

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

If $f^{-1}(y) \in (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c$ with $y \in \mathfrak{b}_1 \cap \mathfrak{b}_2$, we have $f^{-1}(y) \in \mathfrak{b}_1^c$ and $f^{-1}(y) \in \mathfrak{b}_2^c$, as $y \in \mathfrak{b}_1$ and $y \in \mathfrak{b}_2$. Thus $f^{-1}(y) \in \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$, showing that $(\mathfrak{b}_1 \cap \mathfrak{b}_2)^c \subseteq \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$. Conversely, if $x \in \mathfrak{b}_1^c \cap \mathfrak{b}_2^c$, then $x \in \mathfrak{b}_1^c$ and $x \in \mathfrak{b}_2^c$ hence $f(x) \in \mathfrak{b}_1$ and $f(x) \in \mathfrak{b}_2$. So $f(x) \in \mathfrak{b}_1 \cap \mathfrak{b}_2$ and $x = f^{-1}(f(x)) \in (\mathfrak{b}_1 \cap \mathfrak{b}_2)^c$, as desired.

Production. Taking

$$\sum_i y_i f(x_i) \in (\mathfrak{a}_1\mathfrak{a}_2)^e,$$

with $y_i \in B$ and $x_i \in \mathfrak{a}_1\mathfrak{a}_2$, we can expand

$$x_i = \sum_j u_j^i v_j^i$$

with $u_j^i \in \mathfrak{a}_1$ and $v_j^i \in \mathfrak{a}_2$. So we write

$$\sum_i y_i f(x_i) = \sum_i y_i f(\sum_j u_j^i v_j^i) = \sum_i \sum_j y_i f(u_j^i) f(v_j^i).$$

Since all $f(u_j^i)f(v_j^i) \in \mathfrak{a}_1^e\mathfrak{a}_2^e$, their sum $\sum_i\sum_j y_i f(u_j^i)f(v_j^i)$ also lies in $\mathfrak{a}_1^e\mathfrak{a}_2^e$, namely $\sum_i y_i f(x_i) \in \mathfrak{a}_1^e\mathfrak{a}_2^e$, showing that

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

For the other direction, suppose we have

$$\sum_i z_i w_i \in \mathfrak{a}_1^{\mathrm{e}} \mathfrak{a}_2^{\mathrm{e}}$$

with $z_i = \sum_j a_j^i f(u_j^i)$ and $w_i = \sum_k b_k^i f(v_k^i)$. Then

$$\sum_i z_i w_i = \sum_i \sum_j \sum_k a_j^i b_k^i f(u_j^i) f(v_k^i) = \sum_j \sum_k a_j^i b_k^i f(\sum_i u_j^i v_k^i).$$

Since all $f(\sum_i u_j^i v_k^i) \in (\mathfrak{a}_1 \mathfrak{a}_2)^{\mathrm{e}}$, their sum $\sum_j \sum_k a_j^i b_k^i f(\sum_i u_j^i v_k^i) = \sum_i z_i w_i$ lies in $(\mathfrak{a}_1 \mathfrak{a}_2)^{\mathrm{e}}$. This shows that

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

Similarly, if we have

$$\sum_i f^{-1}(u_i) f^{-1}(v_i) \in \mathfrak{b}_1^{\mathrm{c}} \mathfrak{b}_2^{\mathrm{c}},$$

each $f^{-1}(u_i v_i) = f^{-1}(u_i) f^{-1}(v_i)$ lies in $(\mathfrak{b}_1 \mathfrak{b}_2)^{\mathrm{c}}$, so does the sum $\sum_i f^{-1}(u_i v_i)$. Thus

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

Quotient. For the first identity, assume that $x \in (\mathfrak{a}_1 : \mathfrak{a}_2)^{\mathrm{e}}$. We want to show that $x \in (\mathfrak{a}_1^{\mathrm{e}} : \mathfrak{a}_2^{\mathrm{e}})$, or namely

$$x \mathfrak{a}_2^{\mathrm{e}} \subseteq \mathfrak{a}_1^{\mathrm{e}}.$$

We can expand x as

$$x = \sum_i y_i f(x_i)$$

with $x_i \mathfrak{a}_2 \subseteq \mathfrak{a}_1$ for each i. Also note that every element z in $\mathfrak{a}_2^{\mathrm{e}}$ has the form

$$z = \sum_j w_j f(z_j),$$

with $z_j \in \mathfrak{a}_2$. So, with a little computation, we have

$$xz = (\sum_i y_i f(x_i))(\sum_j w_j f(z_j)) = \sum_i \sum_j y_i w_j f(x_i) f(z_j) = \sum_i \sum_j y_i w_j f(x_i z_j) \in \mathfrak{a}_1^{\mathrm{e}}, \tag{3}$$

since

$$x_i z_j \in \mathfrak{a}_1$$

for all i, j. Thus (3) tells us that $x \mathfrak{a}_2^{\mathrm{e}} \subseteq \mathfrak{a}_1^{\mathrm{e}}$, as desired.

For the other identity, assume that $x \in (\mathfrak{b}_1 : \mathfrak{b}_2)^{\mathrm{c}}$, or equivalently

$$x \in f^{-1}(\mathfrak{b}_1 : \mathfrak{b}_2) \Leftrightarrow f(x) \in (\mathfrak{b}_1 : \mathfrak{b}_2) \Leftrightarrow f(x) \mathfrak{b}_2 \subseteq \mathfrak{b}_1, \tag{4}$$

we want to show that

$$x \in (\mathfrak{b}_1^{\mathrm{c}}, \mathfrak{b}_2^{\mathrm{c}}).$$

To do this, take any $f^{-1}(y) \in \mathfrak{b}_2^{\mathrm{c}}$, we have

$$f(x f^{-1}(y)) = f(x) y \in \mathfrak{b}_1,$$

by (4). This shows that

$$x f^{-1}(y) \in \mathfrak{b}_1^{\mathrm{c}}$$

for all $y \in \mathfrak{b}_2$, hence

$$x \mathfrak{b}_2^{\mathrm{c}} \subseteq \mathfrak{b}_1^{\mathrm{c}},$$

as desired. **Root**. Suppose
$$\sum_i y_i f(x_i) \in (\sqrt{\mathfrak{a}})^{\mathrm{e}} \tag{5}$$
with $x_i \in \sqrt{\mathfrak{a}}$, or $x_i^{m_i} \in \mathfrak{a}$ for some $m_i \in \mathbb{N}$ for each i. Since only finitely many y_i in (5) are not zero, the sum $\sum_i m_i$ makes sense. Note that
$$(\sum_i y_i f(x_i))^{\sum_i m_i} \in \mathfrak{a}^{\mathrm{e}},$$
so we have
$$\sum_i y_i f(x_i) \in \sqrt{\mathfrak{a}^{\mathrm{e}}}.$$
This means $(\sqrt{\mathfrak{a}})^{\mathrm{e}} \subseteq \sqrt{\mathfrak{a}^{\mathrm{e}}}$.

For the other identity, suppose we have
$$f^{-1}(y) \in (\sqrt{\mathfrak{b}})^{\mathrm{c}}$$
with $y \in \sqrt{\mathfrak{b}}$. Then there is some $n \in \mathbb{N}$ making
$$(f^{-1}(y))^m = f^{-1}(y^m) \in f^{-1}(\mathfrak{b}) = \mathfrak{b}^{\mathrm{c}},$$
hence
$$f^{-1}(y) \subseteq \sqrt{\mathfrak{b}^{\mathrm{c}}},$$
showing that
$$(\sqrt{\mathfrak{b}})^{\mathrm{c}} \subseteq \sqrt{\mathfrak{b}^{\mathrm{c}}}.$$
Conversely, if $x \in \sqrt{\mathfrak{b}^{\mathrm{c}}}$, there is some $m \in \mathbb{N}$ such that
$$x^m \in \mathfrak{b}^{\mathrm{c}}.$$
So we have
$$(f(x))^m = f(x^m) \in \mathfrak{b},$$
which means that
$$f(x) \in \sqrt{\mathfrak{b}},$$
or equivalently
$$x \in (\sqrt{\mathfrak{b}})^{\mathrm{c}}.$$
So we have shown that
$$\sqrt{\mathfrak{b}^{\mathrm{c}}} \subseteq (\sqrt{\mathfrak{b}})^{\mathrm{c}}.$$
□

Exercise 3

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 coefficient in A. Show that

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

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

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

(d) 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.

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

Proof. **(a)** $\Rightarrow$ Suppose that $f = \sum_{i=0}^{\infty} a_i x^i$ is a unit in $A[[x]]$, then there is some $g = \sum_{j=0}^{\infty} b_j x^j \in A[[x]]$ such that

$$1 = fg = (\sum_{i=0}^{\infty} a_i x^i)(\sum_{j=0}^{\infty} b_j x^j) = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^{i+j} = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots .$$

Comparing the coefficients of both sides, we have at least

$$a_0 b_0 = 1,$$

showing that a_0 is a unit in A.

$\Leftarrow$ Assume that a_0 in $f = \sum_{i=0}^{\infty} a_i x^i$ is a unit in A, we need to show that there is some $g \in A[[x]]$ such that $fg = 1$. Let $g = \sum_{j=0}^{\infty} b_j x^j$, we construct b_j inductively. For $j = 0$, we simply take $b_0 := (a_0)^{-1}$ by the assumption that a_0 is a unit in A. Suppose we have constructed $b_0, b_1, \ldots, b_{j-1}$ for $j \in \mathbb{N}$, we may let

$$b_j := -b_0(b_{j-1}a_1 + b_{j-2}a_2 + \cdots + b_1 a_{j-1} + b_0 a_j),$$

which satisfies

$$b_j a_0 + b_{j-1}a_1 + \cdots + b_1 a_{j-1} + b_0 a_j = 0$$

manifestly. With these b_j's we have

$$fg = \sum_{n=0}^{\infty} \sum_{i+j=n} a_i b_j x^{i+j} = 1,$$

completing the other direction.

(b) We prove this by induction on n. When $n = 0$, as f is nilpotent, there is some $m_0 \in \mathbb{N}$ such that

$$0 = f^{m_0} = (\sum_{i=0}^{\infty} a_i x^i)^{m_0},$$

which at least implies

$$a_0^{m_0} = 0$$

by comparing the coefficients of the both sides. To show that a_n is nilpotent, we apply the induction hypothesis that $a_0, a_1, \ldots, a_{n-1}$ are all nilpotent, that is, there are $m_0, m_1, \ldots, m_{n-1} \in \mathbb{N}$ making

$$\begin{aligned} a_0^{m_0} &= 0, \\ a_1^{m_1} &= 0, \\ &\vdots \\ a_{n-1}^{m_{n-1}} &= 0. \end{aligned}$$

Let $m_n := m_0 + m_1 + \cdots + m_{n-1}$, we have

$$0 = (f - a_0 - a_1 x - \cdots a_{n-1}x^{n-1})^{m_n} = (a_n x^n + a_{n+1}x^{n+1} + \cdots)^{m_n}.$$

So we have

$$a_n^{m_n} = 0$$

by comparing the coefficients, which shows that a_n is nilpotent.

(c) We know that f belongs to $J(A[[x]])$ iff $1 - fg$ is a unit of $A[[x]]$ for all $g = \sum_{j=0}^{\infty} b_j x^j \in A[[x]]$. By **(a)**, the last condition holds iff $1 - a_0 b_0$ is a unit in A for all $b_0 \in A$, iff a_0 is in $J(A)$.

(d) We denote by $i : A \hookrightarrow A[[x]]$ the natural inclusion. If $\mathfrak{m}$ is a maximal of $A[[x]]$, we need to show that $i^{-1}(\mathfrak{m})$ is a maximal ideal of A. If $f \in \mathfrak{m} \cap i(A)$, f is a constant and can be viewed as an element of A. Since $\mathfrak{m}$ is maximal in $A[[x]]$, $1 - f$ is a unit in $A[[x]]$, and via $i : A \hookrightarrow A[[x]]$ $1 - f = 1 - i^{-1}(f)$ is a unit in A. Since all elments in $\mathfrak{m}^{\mathrm{c}}$ are of the form $i^{-1}(f)$, the elements of $1 - \mathfrak{m}^{\mathrm{c}}$ are all unit in A, so $\mathfrak{m}^{\mathrm{c}}$ is maximal in A.

(e) Let $\mathfrak{p} \subseteq A$ be a prime ideal of A, note that

$$\mathfrak{p}^{\mathrm{e}} := i(\mathfrak{p})A[[x]] = \mathfrak{p}[[x]] = \left\{ f \in A[[x]] \;\middle|\; f = \sum_{i=0}^{\infty} a_i x^i, a_i \in \mathfrak{p} \right\},$$

and

$$\mathfrak{p}[[x]]^{\mathrm{c}} = \mathfrak{p}.$$

So if we can show that $\mathfrak{p}[[x]]$ is a prime ideal of $A[[x]]$, we are done. To show this, we can pick any two $f, g \in A[[x]]$ and assume that neither of them are in $\mathfrak{p}[[x]]$, and we need to show that

$$fg \notin \mathfrak{p}[[x]].$$

Expanding f, g in x as before,

$$f = \sum_{i=0}^{\infty} a_i x^i,$$
$$g = \sum_{j=0}^{\infty} b_j x^j,$$

we know that there exist some minimal $m, n \in \mathbb{N}$ such that $a_m, b_n \notin \mathfrak{p}$ and $a_i, b_j \in \mathfrak{p}, 0 \leq i \leq m-1, 0 \leq j \leq n-1$, by assumption. Now we consider the sum

$$a_{m+n}b_0 + a_{m+n-1}b_1 + \cdots + a_m b_n + a_{m-1}b_{n+1} + \cdots + a_0 b_{m+n}, \tag{6}$$

which is the coefficient of the term x^{m+n} in the expansion of fg. We claim that (6) is an element of $\mathfrak{p}$. Otherwise, if it were in $\mathfrak{p}$, and by the assumption that $a_i \in \mathfrak{p}, 0 \leq i \leq m-1$ and $b_j \in \mathfrak{p}, 0 \leq j \leq n-1$, we have

$$a_m a_n \in \mathfrak{p},$$

showing that either a_m or b_n is an element of $\mathfrak{p}$, a contradiction. Thus our claim holds and hence $fg \notin \mathfrak{p}[[x]]$, as desired. □

Exercise 4

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

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

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

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

$$V(\cup_{i \in I} E_i) = \cap_{i \in I} V(E_i).$$

(d) $V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ 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 Spec$A$.

Proof. **(a)** We first prove that

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

If $\mathfrak{p} \in V(\mathfrak{a})$, then $E \subseteq \mathfrak{a} \subseteq \mathfrak{p}$, showing that $\mathfrak{p} \in V(E)$. Conversely, If $\mathfrak{p} \in V(E)$, we have $E \subseteq \mathfrak{p}$. Thus

$$\sum_i a_i e_i \in \mathfrak{p}$$

for all $e_i \in E$ and $a_i \in A$, which is equivalent to say that

$$\mathfrak{a} = \langle E \rangle \subseteq \mathfrak{p},$$

as desired.

Then we prove that

$$V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}}).$$

If $\mathfrak{q} \in V(\sqrt{\mathfrak{a}})$, then

$$\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \subseteq \mathfrak{q},$$

showing that $\mathfrak{q} \in V(\mathfrak{a})$. Conversely, if $\mathfrak{q} \in V(\mathfrak{a})$, we have $\mathfrak{a} \subseteq \mathfrak{q}$. We want to show that $\sqrt{\mathfrak{a}} \subseteq \mathfrak{q}$ as well. Indeed, for any $x \in \sqrt{\mathfrak{a}}$, there is some $m \in \mathbb{N}$ such that

$$x^m \in \mathfrak{a} \subseteq \mathfrak{q}.$$

Since $\mathfrak{q}$ is prime, we conclude that $x \in \mathfrak{p}$, this shows that $\sqrt{\mathfrak{a}} \subseteq \mathfrak{q}$.

(b) Since 0 is contained in all prime ideals of A, so we have

$$V(0) = X.$$

Since no proper prime ideals contain 1, we have

$$V(1) = \varnothing.$$

(c) If $\mathfrak{p} \in \cap_{i=I} V(E_i)$, we have

$$E_i \subseteq \mathfrak{p}$$

for all $i \in I$, which implies

$$\cup_{i \in I} E_i \subseteq \mathfrak{p}.$$

Conversely, if $\mathfrak{q} \in V(\cup_{i \in I} E_i)$, we have

$$\cup_{i \in I} E_i \subseteq \mathfrak{q},$$

thus

$$E_i \subseteq \cup_{i \in I} \subseteq \mathfrak{q}.$$

This means that

$$\mathfrak{q} \in V(E_i)$$

for all $i \in I$, thus

$$\mathfrak{q} \in \cap_{i \in I} V(E_i).$$

(d) Since $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$, if any prime ideal contains $\mathfrak{a} \cap \mathfrak{b}$, it also contains $\mathfrak{a}\mathfrak{b}$. So we have $V(\mathfrak{a} \cap \mathfrak{b}) \subseteq V(\mathfrak{a}\mathfrak{b})$. For the other direction, assume that $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}$, we want to show that $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{q}$. Indeed, for any $x \in \mathfrak{a} \cap \mathfrak{b}$, we have $x^2 \in \mathfrak{a}\mathfrak{b} \subseteq \mathfrak{q}$. Since $\mathfrak{q}$ is prime, $x \in \mathfrak{q}$, as desired. $\square$

Exercise 5

Let A be a ring and $\mathfrak{a} \subseteq A$ be an ideal. Let M be a finite A-module. Prove that

$$\sqrt{\operatorname{Ann}(M/\mathfrak{a}M)} = \sqrt{\operatorname{Ann}(M) + \mathfrak{a}}.$$

Proof. $\supseteq$ If $x \in \sqrt{\operatorname{Ann}(M) + \mathfrak{a}}$, there is some $m \in \mathbb{N}$ such that $x^m \in \operatorname{Ann}(M) + \mathfrak{a}$. Thus

$$x^m M \subseteq (\operatorname{Ann}(M) + \mathfrak{a})M = \mathfrak{a}M,$$

which means that

$$x^m(M/\mathfrak{a}M) = 0$$

in $M/\mathfrak{a}M$. So $x^m \in \operatorname{Ann}(M/\mathfrak{a}M)$, or $x \in \sqrt{\operatorname{Ann}(M/\mathfrak{a}M)}$.

$\subseteq$ Conversely, if $y \in \sqrt{\operatorname{Ann}(M/\mathfrak{a}M)}$, then there is some $n \in \mathbb{N}$ such that $y^n \in \operatorname{Ann}(M/\mathfrak{a}M)$, or equivalently, $y^n M \subseteq \mathfrak{a}M$. Note that M is a faithful $(A/\operatorname{Ann}(M))$-module, and we denote $\bar{y}$ by the image of y in the quotient ring $(A/\operatorname{Ann}(M))$. So we have

$$\bar{y}^n M \subseteq \mathfrak{a}M,$$

by which we claim that $\bar{y}^n \in \mathfrak{a}$. Indeed, since there is always some $f \in \mathfrak{a}$ making

$$\bar{y}^n M = fM$$

by the finiteness of M, we have $\bar{y}^n = f$, as M is faithful as an $(A/\operatorname{Ann}(M))$-module. But $\bar{y}^n \in \mathfrak{a}$ implies that

$$y^n \in \mathfrak{a} + \operatorname{Ann}(M),$$

or equivalently

$$y \in \sqrt{\mathfrak{a} + \operatorname{Ann}(M)}.$$

□

Exercise 6

Let A be a ring, and $0 \to L \to M \to N \to 0$ be an exact sequence of A-modules.

(a) If L and N are both of finite presentation, then so is M.

(b) If L is finitely generated and M is of finite presentation, then N is of finite presentation.

Proof. **(a)** Since L and N are both of finite presentation, we the following commutative diagram with exact row and columns

$$\begin{tikzcd}
 & A^n \arrow[d, "k"] & & A^q \arrow[d, "u"] & \\
 & A^m \arrow[d, "h"] & & A^p \arrow[d, "v"] & \\
0 \arrow[r] & L \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & & 0 &
\end{tikzcd}.$$

Thus there exists a unique $\tilde{v} : A^p \to M$ lifting $v : A^p :\to N$. Further $f \circ h : A^m \to M$ and $\tilde{v} : A^p \to M$ induce a morphism $i : A^{m+p} = A^m \oplus A^p \to M$. By the same reason there is a morphism $j : A^{n+q} \to A^{m+p}$. So the above commutative diagram can be extended to the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & A^n \arrow[r] \arrow[d, "k"] & A^{n+q} \arrow[r] \arrow[d, "j"] & A^q \arrow[r] \arrow[d, "u"] & 0 \\
0 \arrow[r] & A^m \arrow[r] \arrow[d, "h"] & A^{m+p} \arrow[r] \arrow[d, "i"] & A^p \arrow[r] \arrow[d, "v"] & 0 \\
0 \arrow[r] & L \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
& 0 & 0 & 0 &
\end{tikzcd},$$

where the second column is exact by construction. This shows that M is of finite presentation.

(b) Since L is finitely generated and M is finitely presented, we have the following commutative diagram.

$$\begin{tikzcd}
& & A^q \arrow[d, "u"] & & \\
& A^m \arrow[r, dotted, "k"] \arrow[d, "h"] & A^p \arrow[d, "v"] & & \\
0 \arrow[r] & L \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] \arrow[d] & N \arrow[r] & 0 \\
& 0 & 0 & &
\end{tikzcd},$$

where $k : A^m \to A^p$ is the unique lift of $f \circ h : A^m \to M$ along $v : A^p \to M$, by the projectivity of A^m.

Then we denote by $\psi : A^{m+q} \to A^p$ the morphism induced by $k : A^m \to A^p$ and $u : A^q \to A^p$, and $\phi : A^p \to N$ the composition of $g : M \to N$ and $v : A^p \to M$, as in the following commutative diagram

$$\begin{tikzcd}
& A^{m+q} \arrow[r] \arrow[d] \arrow[dr, "\psi"] & A^q \arrow[d, "u"] & & \\
& A^m \arrow[r, dotted, "k"] \arrow[d, "h"] & A^p \arrow[d, "v"] \arrow[dr, "\phi"] & & \\
0 \arrow[r] & L \arrow[r, "f"] \arrow[d] & M \arrow[r, "g"] \arrow[d] & N \arrow[r] & 0 \\
& 0 & 0 & &
\end{tikzcd}.$$

By construction,

$$A^{m+q} \xrightarrow{\psi} A^p \xrightarrow{\phi} N \to 0$$

is an exact sequence of A-modules, thus a presentation of N. This shows that N is finitely presented, completing the proof.

□

Exercise 7

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?

Proof. If $0 \neq x \in A$ is nilpotent, then there is some $n \in \mathbb{N}$ making $x^n = 0$. For any prime ideal $\mathfrak{p}$, consider $x/1 \in A_\mathfrak{p}$. Then $(x/1)^n = 0$ in $A_\mathfrak{p}$ since $1 \cdot x^n = x^n = 0$, a contradiction to the assumption that there are no non-zero nilpotent element in $A_\mathfrak{p}$. Is being integral a local property? □

Exercise 8

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

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

Prove that

(a) S is saturated $\Leftrightarrow$ $A - S$ is a union of prime ideals.

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

If $S = 1 + \mathfrak{a}$, where $\mathfrak{a}$ is an ideal of A, find $\bar{S}$.

Proof. **(a)** $\Leftarrow$ Suppose $A - S = \cup_i \mathfrak{p}_i$, with $\mathfrak{p}_i$ running over prime ideals that don't meet S. Clearly S is multiplicatively closed. To see this, take any $x \in S$ and $y \in S$. Thus $x \notin \mathfrak{p}_i$ and $y \notin \mathfrak{p}_i$ for all i, so does xy. Then $xy \notin \cup_i \mathfrak{p}_i$, so $xy \in S$. Now suppose $xy \in S$, then $xy \notin \mathfrak{p}_i$ for all $\mathfrak{p}_i$, hence $x \notin \mathfrak{p}_i$ and $y \notin \mathfrak{p}_i$ for all $\mathfrak{p}_i$, or $x \in S$ and $y \in S$.

$\Rightarrow$ Suppose that S is saturated. We want to show that for any $x \notin S$, there is a prime ideal $\mathfrak{p}$ containing x and not meeting S. This direction is slightly non-trivial than the other, as we will conclude the existence of such a prime ideal $\mathfrak{p}$ by Zorn's Lemma. We define Σ to be the set

$$\Sigma := \{ \text{ideals containing } x \text{ that don't meet } S \},$$

and endow Σ the partial order $\subseteq$. Thus Σ is a poset that is non-empty. Indeed, by saturation, the ideal (x) generated by the single element $x \notin S$ doesn't meet S. Otherwise, if there is some $a \in A$ making $ax \in S$ we have $a \in S$ and $x \in S$, a contradiction. Now we consider the total order subset T of Σ. For any $\mathfrak{a}, \mathfrak{b} \in T$, there is either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$. By Zorn's Lemma, there is a maximal element $\mathfrak{p}$ of T. We want to show that $\mathfrak{p}$ is prime. Take any $y \notin \mathfrak{p}$ and $z \notin \mathfrak{p}$, the ideals $(y) + \mathfrak{p}$ and $(z) + \mathfrak{p}$ are not in T. So $(y) + \mathfrak{p}$ and $(z) + \mathfrak{p}$ intersect with S. Take $s \in ((y) + \mathfrak{p}) \cap S$ and $t \in ((z) + \mathfrak{p}) \cap S$, st is again in S by saturation. On the other hand $st \in ((y) + \mathfrak{p})((z) + \mathfrak{p}) \subseteq (yz) + \mathfrak{p}$. So $st \in ((yz) + \mathfrak{p}) \cap S$, showing that $(yz) + \mathfrak{p}$ is not an element of Σ. Then $yz \notin \mathfrak{p}$. This shows that $A - S \subseteq \cup_i \mathfrak{p}_i$, with $\mathfrak{p}_i$ running over prime ideals not meeting S.

The other direction $\cup_i \mathfrak{p}_i \subseteq A - S$ is trivial, since each $\mathfrak{p}_i$ doesn't intersect with S, their union neither.

(b) The "$\Leftarrow$" part of **(a)** shows that $\bar{S}$ is saturated. Now we are going to show it is minimal. Suppose there is a saturated multiplicative subset T such that $S \subseteq T$. By **(a)**, we have

$$T = A - \cup \mathfrak{q}$$

with $\mathfrak{q}$ running over prime ideals that don't meet T, and

$$\bar{S} = A - \cup\mathfrak{p}$$

with $\mathfrak{p}$ running over prime ideals that don't meet S. Since $\cup\mathfrak{q} \subseteq \cup\mathfrak{p}$, we have $T \supseteq \bar{S}$, showing that $\bar{S}$ is minimal.

If $S = 1 + \mathfrak{a}$, then

$$\bar{S} = \cup\mathfrak{p}$$

with $\mathfrak{p}$ running over all primes ideals such that $\mathfrak{p} \cap \mathfrak{a} = \varnothing$. □

Exercise 9

Let S be a multiplicatively closed subset of an integral domain A. Show that $T(S^{-1}M) = S^{-1}(TM)$. Deduce that the following are equivalent:

(a) M is torsion-free.

(b) $M_\mathfrak{p}$ is torsion-free for all prime ideals $\mathfrak{p}$.

(c) $M_\mathfrak{m}$ is torsion-free for all maximal ideals $\mathfrak{m}$.

Proof. We first show that $T(S^{-1}M) = S^{-1}(TM)$.

$\subseteq$ If $m/r \in T(S^{-1}M)$ is a torsion element, then we can find some $x/t \in S^{-1}A$ such that

$$0 = \frac{x}{t} \cdot \frac{m}{r} = \frac{x \cdot m}{tr}.$$

The last condition is equivalent to

$$zx \cdot m = 0$$

for some $z \in S$, showing that m is a torsion element in M, or $m \in TM$. Thus $m/r \in S^{-1}(TM)$.

$\supseteq$ If $n/s \in S^{-1}(TM)$, then $n \in TM$ is a torsion element. So we can find $y \in A$ such that

$$y \cdot n = 0.$$

This implies that in $S^{-1}M$

$$\frac{y}{1} \cdot \frac{n}{s} = \frac{y \cdot n}{s} = 0,$$

since $wy \cdot n = 0$ holds for all $w \in S$. Thus we have shown that $n/s \in T(S^{-1}M)$.

Taking $S = A - \mathfrak{p}$, we have

$$T(M_\mathfrak{p}) = (TM)_\mathfrak{p},$$

while taking $S = A - \mathfrak{m}$, we have

$$T(M_\mathfrak{m}) = (TM)_\mathfrak{m}.$$

Finally note that the conditions

(a') $TM = 0$.

(b') $(TM)_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$.

(c') $(TM)_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$.

are all equivalent, as we have proved in class. So we are done. □

Exercise 10

Let $f : A \to B$ be an integral homomorphism of rings. Show that $f^* : \mathrm{Spec}B \to \mathrm{Spec}A$ is a **closed** mapping, *id est* that it maps closed sets to closed sets.

Proof. Any closed set of $\mathrm{Spec}B$ is of the form $V(\mathfrak{b})$, with $\mathfrak{b} \subseteq B$ an ideal of B. If we can prove that

$$f^* V(\mathfrak{b}) = V(\mathfrak{b}^c), \tag{7}$$

then we can conclude that $f^* : \mathrm{Spec}B \to \mathrm{Spec}A$ is closed.

$\subseteq$ If $\mathfrak{q} \in V(\mathfrak{b})$, then $f^*(\mathfrak{q}) = \mathfrak{q}^c \in V(\mathfrak{b}^c)$, since the contraction of a prime ideal is again prime, and the relation $\mathfrak{b} \subseteq \mathfrak{q}$ implies $\mathfrak{b}^c \subseteq \mathfrak{q}^c$.

$\supseteq$ If $\mathfrak{p} \in V(\mathfrak{b}^c)$, there is always a prime ideal $\mathfrak{q} \subseteq B$ such that $\mathfrak{q}^c = \mathfrak{p}$, as B is integral over A ([AM, Theorem 5.10.]). So $\mathfrak{p} = q^c \in f^* V(\mathfrak{b})$. So (7) indeed holds and we are done. □

Exercise 11

(a) 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 $C[x]$.

(b) Prove the same result without assuming that B (or A) is an integral domain.

Proof. **(a)** Take K to be the fraction field of B, there is a field extension $K \subseteq L$ with L a splitting field of fg. Then we write

$$fg = \prod_i (x - \xi_i) \prod_j (x - \eta_j),$$

where ξ_i are all the roots of f and η_j all the roots of g. Since $(fg)(\xi_i) = 0$ and $(fg)(\eta_j) = 0$ for all ξ_i and η_j, plus the fact that fg is monic, we know that ξ_i and η_j are all integral over C. But C is the integral closure of A, it is integral closed. So all ξ_i and η_j are in C. As

$$f = \prod_i (x - \xi_i)$$

and

$$g = \prod_j (x - \eta_j),$$

we know that the coefficients of f are symmetrical polynomials of ξ_i and the coefficients of g are symmetrical polynomials of η_j. Thus the coefficients of f are in C and the coefficients of g are in C, or $f, g \in C[x]$, as desired.

(b) If we can construct a larger ring $\bar{B}$ such that f and g split over L, then we can repeat the argument in **(a)** to compelete the proof, just replacing L with $\bar{B}$. The idea is quite simple: we add all roots of f and g into B, and $\bar{B}$ is the ring generated by these roots over B. Consider the ring $B_1 := B[x]/(f(x))$, in which $f(x)$ has a root $\xi_1 = \bar{x}$, with $\bar{x}$ the image of x in B_1. Then consider the ring $B_1[y]$, we claim that in $B_1[y]$ we have a factorization

$$f(y) = (y - \xi_1) f_1(y),$$

with $f_1(y)$ some monic polynomial in $B_1[y]$. Indeed, we consider the map $B_1[y] \to B_1[y]/(y - \xi_1)$, in whose kernel lies $f(y)$, since

$$\overline{f(y)} = f(\bar{y}) = f(\xi_1) = 0.$$

This shows that $f(y)$ lies in the ideal $(y - \xi_1)$ of $B_1[y]$. So $f(y) = (y - \xi_1) f_1(y)$ for some $f_1(y)$. Both $y - \xi_1$ and $f(y)$ are monic in y, so is $f_1(y)$. If $\deg f = n$, we have

$$\deg f_1 = \deg f - 1.$$

Using induction on the degree of f, we can construct a ring $\tilde{B}$, on which f splits. Then we begin with the ring $\tilde{B}$ and use induction on the degree of g, the final output ring $\bar{B}$ is the ring on which both f, g split. □

Exercise 12

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 $B[x]$.

Proof. If $f \in B[x]$ is integral over $A[x]$, or namely there are $g_1, g_2, \ldots, g_m \in A[x]$ such that

$$f^m + g_1 f^{m-1} + \cdots + g_m = 0, \tag{8}$$

we want to show that $f \in C[x] = \bar{A}[x]$.Then let r be an integer such that

$$r > \max\{\deg f, \deg g_1, \ldots, \deg g_m\},$$

and let $f_1 := f - x^r$. If we can show that $f_1 \in C[x]$, then $f = f_1 + x^r \in C[x]$.

To show this, we plug $f = f_1 + x^r$ in to (8) to get

$$(f_1 + x^r)^m + g_1(f + x^r)^{m-1} + \cdots + g_m = 0,$$

or

$$f_1^m + h_1 f_1^{m-1} + \cdots + h_m = 0,$$

where $h_m = x^{rm} + g_1 x^{rm-r} + \cdots + g_m$. Since $g_i \in A[x], 1 \le i \le m$, we have $h_m \in A[x] \subseteq \bar{A}[x] = C[x]$. Note that

$$h_m = (-f_1)(f_1^{m-1} + h_1 f_1^{m-2} + \cdots + h_{m-1}),$$

and both $-f_1$, $f_1^{m-1} + h_1 f_1^{m-2} + \cdots + h_{m-1}$ are monic in $B[x]$, so now we can apply **Exercise 5(b)**, to get that $-f_1 \in C[x]$. This shows that $f = -(-f_1) + x^r \in C[x]$, completing the proof. □

Exercise 13

Let $I_1, I_2, \ldots, I_n$ be ideals of a ring A such that $I_1 \cap \cdots \cap I_n = (0)$. Prove that if each A/I_i is a Noetherian ring, then A is also Noetherian.

Proof. We consider the homomorphism

$$\phi : A \to \bigoplus_{i=1}^{n} (A/I_i)$$

induced by the natural map $A \to A/I_i$. We claim that ϕ is injective. Indeed, if there exists some $x \in A$ such that $\phi(x) = 0$, then we have $x \in I_i, i = 1, \ldots, n$, thus $x \in I_1 \cap \cdots \cap I_n = (0)$, showing that $x = 0$ in A. Thus any ascending chain

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_2 \subseteq \cdots \tag{9}$$

in A can be viewed as an ascending chain in $\bigoplus_{i=1}^{n}(A/I_i)$ via ϕ. So if we can show that $\bigoplus_{i=1}^{n}(A/I_i)$ is Noetherian, then (9) terminates and we are done. But this is indeed true, since each A/I_i is Noetherian, their direct sum $\bigoplus_{i=1}^{n}(A/I_i)$ is again Noetherian. This completes the proof. □

Exercise 14

Let $k = \mathbb{F}_q$ be the finite field of q elements, and $k[X,Y]$ the polynomial ring in X and Y. Set $f = X^qY - XY^q$ and $A = k[X,Y]/(f)$. Let x, y be the image of X, Y in A respectively. For every $a \in k$, prove that A is not a finitely generated R-module with $R := k[y - ax]$.

Proof. Observe that $x^q y = xy^q$ in A, so that every monomial in A can be written as $bx^i y^j$, with $b \in k, i \in \mathbb{N}$ and $0 \le j < q$. Now suppose that A is a finitely generated R-module, with generators $\xi_1(x,y), \dots, \xi_n(x,y) \in A$. Thus for $g(x,y) \in A$, there exist $a_1, \dots, a_n \in R = k[y - ax]$, such that

$$g(x,y) = a_1(y-ax)\xi_1(x,y) + \cdots + a_n(y-ax)\xi_n(x,y). \tag{10}$$

For any $h(x,y) \in A$, we denote $\deg_x h(x,y)$ by the degree of $h(x,y)$ in variable x, and $\deg_y h(x,y)$ the degree of $h(x,y)$ in variable y. Here we make some important observations: we have that

$$\deg_x a_i(y-ax) = \deg_y a_i(y-ax), 0 \le i \le n,$$

and that

$$\deg_x(a_i(y-ax)\xi_i(x,y)) \ge \deg_x \xi_i(x,y) + \deg_x a_i(y-ax), 0 \le i \le n, \tag{11}$$

for any $a_i \in R$. Now we pick such $d \in \mathbb{N}$ that

$$d < \min\{\deg_x \xi_1(x,y), \deg_x \xi_2(x,y), \dots, \deg_x \xi_n(x,y)\},$$

and take $g(x,y)$ in (10) to be

$$g(x,y) = x^d.$$

But from (11), we know that $\deg_x$ of the right hand side of (10) is strictly greater than d, a contradiction. So we have shown that A is not a finitely generated R-module, completing the proof. □

Exercise 15

Let A be a ring and B a faithfully flat A-algebra. If B is Noetherian, show that A is Noetherian.

Proof. Since B is faithfully flat over A, then we have $\mathfrak{a}^{\mathrm{ec}} = \mathfrak{a}$ for all ideal $\mathfrak{a}$ of A. Since the composition of the extension and the contraction is the identity, the map $\mathfrak{a} \mapsto \mathfrak{a}^{\mathrm{e}}$ is injective. So any ideal of A can be viewed as an ideal of B. Now we want to show that A is Noetherian. We argue by *reductio ad absurdum*. If A were not Noetherian, we would find a strictly ascending chain of ideals

$$0 \subsetneq \mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$$

in A that doesn't stabilize. Thus the chain of ideals

$$0 \subsetneq \mathfrak{a}_1^{\mathrm{e}} \subsetneq \mathfrak{a}_2^{\mathrm{e}} \subsetneq \cdots$$

is again strictly ascending and doesn't terminate in B. Thus we reach a contradiction, since B is Noetherian by assumption. This shows that A must be Noetherian, completing the proof. □

Exercise 16

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?

Proof. To show that the decomposition $\mathfrak{a} = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{m}^2$ is reduced, we need to verify that

$$\begin{aligned}\mathfrak{p}_1 &\not\supseteq \mathfrak{p}_2 \cap \mathfrak{m}^2,\\ \mathfrak{p}_2 &\not\supseteq \mathfrak{p}_1 \cap \mathfrak{m}^2,\\ \mathfrak{m}^2 &\not\supseteq \mathfrak{p}_1 \cap \mathfrak{p}_2.\end{aligned}$$

Indeed, note that $y^2 \in \mathfrak{p}_1$ but $y^2 \notin \mathfrak{p}_2 \cap \mathfrak{m}^2$, thus the first relation holds. Also note that $z^2 \in \mathfrak{p}_2$ but $z^2 \notin \mathfrak{p}_1 \cap \mathfrak{m}^2$, which proves the second relation; and that $y^2 \in \mathfrak{m}^2$ but $y^2 \notin \mathfrak{p}_1 \cap \mathfrak{p}_2$, which proves the third relation. Thus we have shown that the decomposition is reduced.

The prime ideals associated with $\mathfrak{a}$ are $\mathfrak{p}_1$, $\mathfrak{p}_2$ and $\mathfrak{m}$, and clearly $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are minimal and $\mathfrak{m}$ is embedded. So the components $\mathfrak{p}_1, \mathfrak{p}_2$ are isolated, and the component $\mathfrak{m}^2$ is embedded. $\square$

Exercise 17

Let A be a ring and $\mathfrak{p}$ a prime ideal of A. The **nth symbolic power of $\mathfrak{p}$** is defined to be the ideal

$$\mathfrak{p}^{(n)} = S_{\mathfrak{p}}(\mathfrak{p}^n)$$

where $S_{\mathfrak{p}} = A - \mathfrak{p}$. Show that

(a) $\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal;

(b) if $\mathfrak{p}^n$ has a primary decomposition, then $\mathfrak{p}^{(n)}$ is its $\mathfrak{p}$-primary component;

(c) if $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ has a primary decomposition, then $\mathfrak{p}^{(m+n)}$ is its $\mathfrak{p}$-primary component;

(d) $\mathfrak{p}^{(n)} = \mathfrak{p}^n \iff \mathfrak{p}^n$ is $\mathfrak{p}$-primary.

Proof. **(a)** By definition, we have $\mathfrak{p}^{(n)} = (\mathfrak{p}^n)^{\mathrm{ec}}$, where the contraction and extension is along the canonical map $A \to A_{\mathfrak{p}} := S_{\mathfrak{p}}^{-1}A$. So

$$\sqrt{\mathfrak{p}^{(n)}} = \sqrt{(\mathfrak{p}^n)^{\mathrm{ec}}} = \left(\sqrt{(\mathfrak{p}^n)^{\mathrm{e}}}\right)^{\mathrm{c}}.$$

But since localization commutes with taking radical, and $(\mathfrak{p}^n)^{\mathrm{e}} = S_{\mathfrak{p}}^{-1}(\mathfrak{p}^n)$, we have

$$\left(\sqrt{(\mathfrak{p}^n)^{\mathrm{e}}}\right)^{\mathrm{c}} = (\sqrt{\mathfrak{p}^n})^{\mathrm{ec}} = \mathfrak{p}^{\mathrm{ec}} = \mathfrak{p}.$$

This shows that $\sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p}$, or equivalently, that $\mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

(b) Suppose $\mathfrak{p}^n = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ is a primary decomposition of $\mathfrak{p}^n$, we need first to show that $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ for some $1 \le i \le m$. This is indeed true, since taking radical commutes with intersection, we have $\mathfrak{p} = \sqrt{\mathfrak{p}^n} = \sqrt{\mathfrak{q}_1} \cap \cdots \cap \sqrt{\mathfrak{q}_m}$. By [AM, Proposition 1.11. ii)], we have $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ for some $1 \le i \le m$.

We then need to show that $\mathfrak{p}^{(n)}$ is the smallest $\mathfrak{p}$-primary ideal containing $\mathfrak{p}^n$, this assures that $\mathfrak{p}^{(n)}$ appears in the minimal primary decomposition of $\mathfrak{p}^n$, so we can conclude that $\mathfrak{p}$ is belong to $\mathfrak{p}^n$ and $\mathfrak{p}^{(n)}$ its $\mathfrak{p}$-primary component. To see this, we have to take a closer look of $\mathfrak{p}^{(n)}$. We claim that

$$\mathfrak{p}^{(n)} = \bigcup_{s \in S_\mathfrak{p}} (\mathfrak{p}^n : s) = \{ x \in A \mid \exists s \in S_\mathfrak{p}, xs \in \mathfrak{p}^n \}. \tag{12}$$

For any $x \in A$, $x \in \mathfrak{p}^{(n)}$ iff $x/1 \in S_\mathfrak{p}^{-1}\mathfrak{p}^n$. But the last condition is equivalent to that $x/1 = a/s, \exists s \in S_\mathfrak{p}, \exists a \in \mathfrak{p}^n$, iff there exist $t, s \in S_\mathfrak{p}$ and $a \in \mathfrak{p}^n$ such that $tsx = ta \in S_\mathfrak{p}\mathfrak{p}^n = \mathfrak{p}^n$. So $x \in \mathfrak{p}^{(n)}$ iff $S_\mathfrak{p} x \cap \mathfrak{p}^n \neq \varnothing$, which happens exactly when $x \in \bigcup_{s \in S_\mathfrak{p}} (\mathfrak{p}^n : s)$. Thus (12) is proved. Now back to our concern on the minimality of $\mathfrak{p}^{(n)}$. If there is any $\mathfrak{p}$-primary ideal $\mathfrak{q}$ satisfying $\mathfrak{p}^n \subseteq \mathfrak{q}$, we want to show that $\mathfrak{p}^{(n)} \subseteq \mathfrak{q}$. If $y \in \mathfrak{p}^{(n)}$, by (12) we there exists $s \in S_\mathfrak{p} = A - \mathfrak{p}$ such that $sy \in \mathfrak{p}^n \subseteq \mathfrak{q}$. Since $s \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, we have $y \in \mathfrak{q}$, as $\mathfrak{q}$ is primary.

(c) This can be proved using the same strategy as for **(b)**. By [AM, Exercise 1.13. iii)] and **(a)**, we have $\sqrt{\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}} = \sqrt{\mathfrak{p}^{(m)}} \cap \sqrt{\mathfrak{p}^{(n)}} = \mathfrak{p} \cap \mathfrak{p} = \mathfrak{p}$. This shows that $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$ is also $\mathfrak{p}$-primary. As in **(b)**, if $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)} = \cap \mathfrak{q}_i$, we have $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ for some i. This shows that $\mathfrak{p}$ belongs to $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$.

Now we are left to show that $\mathfrak{p}^{(m+n)}$ is the minimal $\mathfrak{p}$-primary containing $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$. This is easy. If $\mathfrak{q}$ is another $\mathfrak{p}$-primary containing $\mathfrak{p}^{(m)}\mathfrak{p}^{(n)}$, we need to show that $\mathfrak{p}^{(m+n)} \subseteq \mathfrak{q}$. Take $x \in \mathfrak{p}^{(m+n)}$, by (12), there exists $s \in S_\mathfrak{p}$ making $sx \in \mathfrak{p}^{m+n} = \mathfrak{p}^m\mathfrak{p}^n \subseteq \mathfrak{p}^{(m)}\mathfrak{p}^{(n)} \subseteq \mathfrak{q}$, where the last "=" holds because $\mathfrak{p}^{m+n}$ is defined inductively. Since $s \notin \mathfrak{p} = \sqrt{\mathfrak{q}}$, $x \in \mathfrak{q}$ as $\mathfrak{q}$ is $\mathfrak{p}$-primary.

(d) $\Rightarrow$ By **(a)**, $\mathfrak{p}^n = \mathfrak{p}^{(n)}$ is $\mathfrak{p}$-primary.

$\Leftarrow$ By **(b)**, $\mathfrak{p}^{(n)}$ is the minimal $\mathfrak{p}$-primary containing $\mathfrak{p}^n$. On the other hand, we assume $\mathfrak{p}^n$ is itself $\mathfrak{p}$-primary, so there must be $\mathfrak{p}^n = \mathfrak{p}^{(n)}$, by the uniqueness of the isolated components of $\mathfrak{p}^n$. $\square$

Exercise 18

Let k be a field and A a finitely generated k-algebra. Prove that the following are equivalent:

(a) A is Artinian;

(b) A is a finite k-algebra.

Proof. **(a)** $\implies$ **(b)** If we can show that the implication holds in the case when A is local, then by the structure theorem for Artin rings [AM, Theorem 8.7.], the implication holds for general A. So we may assume that A is local Artin with a unique maximal ideal $\mathfrak{m}$, and is finitely generated over k. Then $K := A/\mathfrak{m}$ is a field and is also finitely generated over k. By [AM, Corollary 5.24.] K is a finite algebraic extension of k, hence is a finite dimensional k-linear space. As A is a finitely generated Artin ring, it is Noetherian with dimension 0; plus the assumption that A is local, the only prime ideal in A is $\mathfrak{m}$. If we view A as a finitely generated A-module, then there is a composition series of finite length

$$0 = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_n = A,$$

with each quotient $M_i/M_{i=1} = A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is some prime ideal of A. But all prime ideals in A are just $\mathfrak{m}$, so all the quotients M_i/M_{i-1} are isomorphic to K for $1 \leq i \leq n$. Thus we have exact sequences A-modules

$$0 \to M_{i-1} \to M_i \to K \to 0$$

with i running through 1 to n. These exact sequence can be viewed as exact sequence of k-modules. When $n = 0$, $M_1 \simeq K$, which is a finite-dimensional k-linear space. Now we assume that all M_i with $1 \leq i \leq n-1$ are finite-dimensional k-linear spaces, then the exact sequence

$$0 \to M_{n-1} \to A \to K \to 0$$

tells us that A is also a finite-dimensional k-linear space.

(b) $\Longrightarrow$ (a) This direction is rather easy. Since A is a finitely generated k-module, there exists an integer m such that there is a surjection $k^m \to A$ of k-linear spaces. Thus A is also a finite dimensional k-linear space. By [AM, Proposition 6.10.], A is finite-dimensional iff the descending chain condition holds for all chains of k-submodules of A. In particular, all chains of ideals of A satisfy the descending chain condition, thus A is Artinian. □

Exercise 19

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.

Proof. Note that ideals containing $\mathfrak{q}$ of A are in one-to-one correspondence with ideals of $A/\mathfrak{q}$; whilst ideals contained in $\mathfrak{p}$ of A are in one-to-one correspondence with ideals of $A_{\mathfrak{p}}$. Hence chains of ideals from $\mathfrak{q}$ to $\mathfrak{p}$ in A are in one-to-one correspondence with chains of ideals in the ring $B := (A/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$. Since primary ideals stay invariant under localization, chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$ of A are in bijection with chains of primary ideals of the local ring B. It suffices to show that all chains of primary ideals in B are of finite length, and all such maximal chains have the same length.

Since A is Noetherian, so the quotient ring $A/\mathfrak{q}$ is Noetherian, as well as the localization B of the quotient ring $A/\mathfrak{q}$. So B is a Noetherian local ring. Since A is Noetherian and $\sqrt{\mathfrak{q}} = \mathfrak{p}$, by [AM, Proposition 7.14.] there exists some integer n such that $\mathfrak{p}^n \subseteq \mathfrak{q}$. But this means that the maximal ideal $\mathfrak{m} := \mathfrak{p}/\mathfrak{q}$ satisfies that $\mathfrak{m}^n = 0$. By [AM, Proposition 8.6.ii)], the Noetherian local ring B is an Artinian local ring. Thus for any proper ideal $\mathfrak{b} \subseteq B$, $(0) = \mathfrak{m}^n \subseteq \mathfrak{b} \subseteq \mathfrak{m}$, by [AM, Corollary 7.16.], $\mathfrak{b}$ is primary.

So far we have shown that all proper ideals of B is primary. Then the chains of primary ideals from $\mathfrak{p}$ to $\mathfrak{q}$ of A are in bijection with chains of *ideals* of B. Since B is Artinian local, all its chains of ideals are of finite length. A maximal chain is a composition series, and all composition series have the same length. □

Exercise 20

Let A be an integral domain, K its field of fractions. Show that the following are equivalent:

(a) A is a valuation ring of K;

(b) If $\mathfrak{a}, \mathfrak{b}$ are any two ideals of A, then either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$.

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.

Proof. **(a) $\Longrightarrow$ (b)** Assume that $\mathfrak{a} \nsubseteq \mathfrak{b}$, we must show that $\mathfrak{b} \subseteq \mathfrak{a}$. By assumption, there is an element $0 \neq x \in A$ whilst $x \notin \mathfrak{b}$. Then for any $0 \neq y \in \mathfrak{b}$, both x/y and y/x are non-zero elements of K. Since A is a valuation ring of K, either $x/y \in A$ or $y/x \in A$. If were the former, then $x = (x/y)y \in A\mathfrak{b} = \mathfrak{b}$, a contradiction. So the latter must hold, that is, $y/x \in A$. Then $y = (y/x)x \in A\mathfrak{a} = \mathfrak{a}$, implying that $\mathfrak{b} \subseteq \mathfrak{a}$, as desired.

(b) $\Longrightarrow$ (a) To show that A is a valuation ring of K, we must show that for any $0 \neq x/y \in K$, either $x/y \in A$ or $y/x \in A$. By assumption, either $(x) \subseteq (y)$ or $(y) \subseteq (x)$ holds in A. If the former holds, $x \in (y) \iff x = uy$ for some $u \in A$; then $x/y = uy/y = u \in A$. If the latter holds, $y \in (x) \iff y = vx$ for some $v \in A$; then $y/x = vx/x = v \in A$, as desired.

Note that the ideals of $A_\mathfrak{p}$ are in one-to-one correspondence with ideals of A contained in $\mathfrak{p}$, while the ideals of $A/\mathfrak{p}$ are in one-to-one correspondence with ideals of A containing $\mathfrak{p}$. So if $\mathfrak{a}, \mathfrak{b}$ are two ideals of $A_\mathfrak{p}$, we consider their contractions $\mathfrak{a}^c, \mathfrak{b}^c$ along $A \to A_\mathfrak{p}$. By assumption that A is a valuation ring, either $\mathfrak{a}^c \subseteq \mathfrak{b}^c$ or $\mathfrak{b}^c \subseteq \mathfrak{a}^c$, by **(b)**. Extending them back, we have $\mathfrak{a} = \mathfrak{a}^{ce}$ and $\mathfrak{b} = \mathfrak{b}^{ce}$, alongside either $\mathfrak{a} \subseteq \mathfrak{b}$ or $\mathfrak{b} \subseteq \mathfrak{a}$, showing that $A_\mathfrak{p}$ is a valuation ring of $\mathrm{Frac}(A_\mathfrak{p})$. The proof for $A/\mathfrak{p}$ is *mutatis mutandis*. □

Exercise 21

Let k be a field, $R := k[x, y, z]$ be the polynomial ring in x, y, z. Set $\mathfrak{a} = (xy, z - yz)$ and

$$\mathfrak{q}_1 = (x, z), \mathfrak{q}_2 = (y^2, x - yz).$$

Show that $\mathfrak{a} = \mathfrak{q}_1 \cap \mathfrak{q}_2$ and that this decomposition is a minimal primary decomposition.

Exercise 22

Let A be a Noetherian ring and M be an A-module, N be a submodule of M, then let $x \in A$. Prove that if $x \notin \mathfrak{p}$ for any $\mathfrak{p} \in \mathrm{Ass}(M/N)$, then $xM \cap N = xN$.

Proof. Since A is Noetherian, we claim that

$$\bigcup_{\mathfrak{p} \in \mathrm{Ass} M} \mathfrak{p} = \bigcup_{m \in M} (0 : m), \tag{13}$$

for any A-module M. If $x \notin \mathfrak{p}$ for any $\mathfrak{p}$ associated to M/N, then $x \notin \mathrm{Ann}_R(M/N)$, which means that the map $M/N \xrightarrow{x} M/N$ given by multiplying x is injective. Equivalently, if any $m \in M$ satisfying $xm \in N$, then $m \in N$. The last condition holds iff $xM \cap N \subseteq xN$. On the other hand $xN \subseteq xM \cap N$ holds trivially, thus $xM \cap N = xN$.

Now we prove the claim. If $x \in \mathfrak{p}$ with $\mathfrak{p}$ associated to M, then by definition there is some $m \in M$ annihilated by $\mathfrak{p}$, hence by x. Then $x \in (0 : m)$.

Conversely, if $x \in (0 : m)$ for some $m \in M$, then $Am \neq 0$. Since A is Noetherian, Am has an associated prime $\mathfrak{p} = \mathrm{Ann}_A(ym)$. Since $xm = 0$, $xym = yxm = 0$, so $x \in \mathfrak{p}$. But $\mathfrak{p} \in \mathrm{Ass} Am \subseteq \mathrm{Ass} M$, therefore $x \in \bigcup_{\mathfrak{p} \in \mathrm{Ass} M} \mathfrak{p}$.

The existence of $\mathfrak{p} = \mathrm{Ann}_A(ym)$ holds as follows. Let Σ be the set of all annihilators of nonzero elements of the submodule Am. Since A is Noetherian, there is a maximal element $\mathfrak{p} = \mathrm{Ann}_A(ym)$ with $y \in A, ym \neq 0$. If we can show that $\mathfrak{p}$ is prime, then the claim holds. Let $ab \in \mathfrak{p}$ with $a \notin \mathfrak{p}$, then $abym = 0$ but $aym \neq 0$, so $b \in \mathrm{Ann}_A(aym)$. But $\mathfrak{p} = \mathrm{Ann}_A(ym) \subseteq \mathrm{Ann}_A(aym)$, and the maximality of $\mathfrak{p}$ gives that $\mathfrak{p} = \mathrm{Ann}_A(aym)$. Consequently, $b \in \mathfrak{p}$. □

Exercise 23

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.

Proof. Note that ideals containing $\mathfrak{q}$ of A are in one-to-one correspondence with ideals of $A/\mathfrak{q}$; whilst ideals contained in $\mathfrak{p}$ of A are in one-to-one correspondence with ideals of $A_\mathfrak{p}$. Hence chains of ideals from $\mathfrak{q}$ to $\mathfrak{p}$ in A are in one-to-one correspondence with chains of ideals in the ring $B := (A/\mathfrak{q})_{\mathfrak{p}/\mathfrak{q}}$. Since primary ideals stay invariant under localization, chains of primary ideals from $\mathfrak{q}$ to $\mathfrak{p}$ of A are in bijection with chains of primary ideals of the local ring B. It suffices to show that all chains of primary ideals in B are of finite length, and all such maximal chains have the same length.

Since A is Noetherian, so the quotient ring $A/\mathfrak{q}$ is Noetherian, as well as the localization B of the quotient ring $A/\mathfrak{q}$. So B is a Noetherian local ring. Since A is Noetherian and $\sqrt{\mathfrak{q}} = \mathfrak{p}$, by [AM, Proposition 7.14.] there exists some integer n such that $\mathfrak{p}^n \subseteq \mathfrak{q}$. But this means that the maximal ideal $\mathfrak{m} := \mathfrak{p}/\mathfrak{q}$ satisfies that $\mathfrak{m}^n = 0$. By [AM, Proposition 8.6.ii)], the Noetherian local ring B is an Artinian local ring. Thus for any proper ideal $\mathfrak{b} \subseteq B$, $(0) = \mathfrak{m}^n \subseteq \mathfrak{b} \subseteq \mathfrak{m}$, by [AM, Corollary 7.16.], $\mathfrak{b}$ is primary.

So far we have shown that all proper ideals of B is primary. Then the chains of primary ideals from $\mathfrak{p}$ to $\mathfrak{q}$ of A are in bijection with chains of *ideals* of B. Since B is Artinian local, all its chains of ideals are of finite length. A maximal chain is a composition series, and all composition series have the same length. $\square$

Exercise 24

Let k be a field and s be a homogeneous polynomial of degree s in $k[X_1, \dots, X_n]$. Compute the Hilbert polynomial of $A := k[X_1, \dots, X_n]/(f)$.

Proof. By definition, the Hilbert polynomial $g(m)$ is the length $l(A_m)$ of the k-module, or equivalently, the dimension of the k-vector space A_m. There is a canonical k-linear basis for A_m, namely the image of the basis $\left\{ X_1^{l_1} \cdots X_n^{l_n} \,\middle|\, \sum_{i=1}^n l_i = m \right\}$, by which we may calculate $\dim_k A_m$. When $m < s$, where $s = \deg f$, the image of $\left\{ X_1^{l_1} \cdots X_n^{l_n} \,\middle|\, \sum_{i=1}^n l_i = m \right\}$ in A can be identified with itself, and we have

$$g(m) = \dim_k A_m = \binom{n+m-1}{n-1}.$$

When $m \geq s$ there is only one linear constraint exerted

$$f(X_1, \dots, X_n) = 0$$

exerted on A_m, in which case

$$g(m) = \dim_k A_m = \binom{n+m-1}{n-1} - 1.$$

In summary, we have computed that

$$g(m) = \begin{cases} \binom{n+m+1}{n-1}, & m < s, \\ \binom{n+m+1}{n-1} - 1, & m \geq s. \end{cases}$$

$\square$

Exercise 25

Let $f \in k[x_1, \dots, x_n]$ be an irreducible polynomial over an algebraically closed field k. A point P on the variety $f(x) = 0$ is non-singular $\iff$ not all the partial derivatives $\partial f/\partial x_i$ vanish at P. Let $A = k[x_1, \dots, x_n]/(f)$, and let $\mathfrak{m}$ be the maximal ideal of A corresponding to the point P. Prove that P is non-singular $\iff$ $A_\mathfrak{m}$ is a regular local ring.

Exercise 26

Prove the following generalization of Krull's principal ideal theorem. Let A be a Noetherian ring

(a) If $\mathfrak{a} \subseteq A$ is an ideal generated by n elements, then evry minimial prime ideal containing $\mathfrak{a}$ has height $\leq n$.

(b) Conversely, if $\mathrm{ht}(\mathfrak{p}) \leq n$, then $\mathfrak{p}$ contains some ideal $\mathfrak{a}$ which can be generated by n elements such that $\mathfrak{p}$ is a minimal ideal containing $\mathfrak{a}$.

Proof. **(a)** Let $\mathfrak{a} = (x_1, \ldots, x_n)$, and let $\mathfrak{p}$ be a primary ideal belonging to $\mathfrak{a}$. Then after localizing to $\mathfrak{p}$, $\mathfrak{a}$ becomes $\mathfrak{p}$-primary, by the dimension theorem, the least number of generators of $\mathfrak{a}$ of $A_\mathfrak{p}$ is equal to $\mathrm{ht}(\mathfrak{p})$, thus $\mathrm{ht}(p) \leq n$, since $\mathfrak{a}$ may be generated by $\leq n$ generators.

(b) Again we localize to the given prime ideal $\mathfrak{p}$. Then $A_\mathfrak{p}$ is a local Noetherian ring and $\dim A_\mathfrak{p} = \mathrm{ht}(\mathfrak{p}) \leq n$. It suffices to find a $\mathfrak{p}$-primary ideal $\mathfrak{a}$ of $A_\mathfrak{p}$ that can be generated by n elements. *A fortiori*, such ideal $\mathfrak{a}$ exists and can be generated by d elements $x_1, \ldots, x_d$, with $d := \mathrm{ht}(\mathfrak{p}) = \dim A_\mathfrak{p}$. To see this, we construct $x_1, \ldots, x_d$ inductively in such a way that every prime ideal containing $(x_1, \ldots, x_i)$ has height $\geq i$, for each i. Suppose $i > 0$ and $x_1, \ldots, x_{i-1}$ constructed. Let $\mathfrak{p}_j, 1 \leq j \leq s$ be the minimal prime ideals of $(x_1, \ldots, x_{i-1})$ which have height exactly $i - 1$. Since $i - 1 < d$, we have $\mathfrak{p}_j \neq \mathfrak{p}$, hence $\mathfrak{p} \neq \cup_{j=1}^{s} \mathfrak{p}_j$. Choose $x_i \in \mathfrak{p}$ that isn't in any of those $\mathfrak{p}_j, 1 \leq j \leq s$ and let $\mathfrak{q}$ be any prime containing $(x_1, \ldots, x_i)$. Then $\mathfrak{q}$ contains some minimal prime ideal $\mathfrak{r}$ of $(x_1, \ldots, x_{i-1})$. If $\mathfrak{r} = \mathfrak{p}_j$ for some j, we have $x_i \in \mathfrak{q}, x_i \notin \mathfrak{r}$, hence $\mathfrak{r} \subsetneq \mathfrak{q}$ and therefore $\mathrm{ht}(\mathfrak{q}) \geq i$; if $\mathfrak{r} \neq \mathfrak{p}_j$, then $\mathrm{ht}(\mathfrak{r}) > i - 1$, hence $\mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(\mathfrak{r}) \geq i$. Thus every prime ideal containing $(x_1, \ldots, x_i)$ has height $\geq i$.

We then consider $\mathfrak{a} := (x_1, \ldots, x_d)$. If $\mathfrak{p}'$ is another ideal of $A_\mathfrak{p}$ containing $\mathfrak{a}$, then $\mathrm{ht}(\mathfrak{p}') \geq d$ by construction. Hence $\mathfrak{p}' = \mathfrak{p}$. Hence the ideal $\mathfrak{a}$ is $\mathfrak{p}$-primary.

□

References

[AM] Michael F. Atiyah and Ian G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics. Westview Press, 22 edition.