# Introduction to Commutative Algebra

M. F. Atiyah & I. G. MacDonald

November 19, 2021

## Contents



## 1 Rings and Ideals

A **ring** $A$ is a set with two binary operations s.t.

1. $A$ is an abelian group w.r.t. addition
2. Multiplication is associative ($(xy)z = x(yz)$) and distributive over addition ($x(y+z) = xy + xz, (y+z)x = yx + zx$)

A **ring homomorphism** is a mapping $f$ of a ring $A$ into a ring $B$ s.t.

1. $f(x+y) = f(x) + f(y)$
2. $f(xy) = f(x)f(y)$
3. $f(1) = 1$

An **ideal** $\mathfrak{a}$ of a ring $A$ is a subset of $A$ which is an additive subgroup and is s.t. $A\mathfrak{a} \subseteq \mathfrak{a}$. The quotient group $A/\mathfrak{a}$ inherits a uniquely defined multiplication from $A$ which makes it into a ring, called the **quotient ring** $A/\mathfrak{a}$. The elements of $A/\mathfrak{a}$ are the cosets of $\mathfrak{a}$ in $A$, and the mapping $\phi : A \to A/\mathfrak{a}$ which maps each $x \in A$ to its coset $x + \mathfrak{a}$ is a surjective ring homomorphism

**Proposition 1.1.** *There is a one-to-one order-preserving correspondence between the ideals* $\mathfrak{b}$ *of* $A$ *which contain* $\mathfrak{a}$*, and the ideals* $\bar{\mathfrak{b}}$ *of* $A/\mathfrak{a}$*, given by* $\mathfrak{b} = \phi^{-1}(\bar{\mathfrak{b}})$*.*

*Proof.* Let $S_1 = \{\mathfrak{b} : \mathfrak{b} \text{ an ideal of } A \text{ and } \mathfrak{a} \subseteq \mathfrak{b}\}$ and $S_2 = \{\bar{\mathfrak{b}} : \bar{\mathfrak{b}} \text{ an ideal of } A/\mathfrak{a}\}$, $\pi$ is the natural map $\pi(S) = S/\mathfrak{a}$, we prove that

$$\varphi : S_1 \to S_2 \qquad \mathfrak{b} \mapsto \pi(\mathfrak{b})$$

is an bijection.

First assume that $\mathfrak{a} \subseteq \mathfrak{b}$, we prove that $\pi^{-1}\pi(\mathfrak{b}) = \mathfrak{b}$. Apparently $\mathfrak{b} \subseteq \pi^{-1}\pi(\mathfrak{b})$. For any $b \in \pi^{-1}\pi(\mathfrak{b})$, there is a $s \in \mathfrak{b}$ s.t. $\pi(b) = \pi(s)$. Thus $b - s \in \ker \pi = \mathfrak{a}$. As $\mathfrak{a} \subseteq \mathfrak{b}$, we have $b \in \mathfrak{b}$. Hence $\pi^{-1}\pi(\mathfrak{b}) = \mathfrak{b}$.

Thus for any $\mathfrak{b}_1, \mathfrak{b}_2 \in S_1$ and $\varphi(\mathfrak{b}_1) = \pi(\mathfrak{b}_1) = \pi(\mathfrak{b}_2) = \varphi(\mathfrak{b}_2)$, we have $\pi^{-1}\pi(\mathfrak{b}_1) = \pi^{-1}\pi(\mathfrak{b}_2)$. Thus $\varphi$ is injective.

For any $\bar{\mathfrak{b}} \in S_2$, $\pi^{-1}(\bar{\mathfrak{b}})$ contains $\mathfrak{a} = \pi^{-1}(\{0\})$. Hence $\varphi$ is surjective

Order-preserving means $\mathfrak{a} \subseteq \mathfrak{b} \subseteq \mathfrak{c}$ iff $\bar{\mathfrak{b}} \subseteq \bar{\mathfrak{c}}$ □

If $f : A \to B$ is any ring homomorphism, the **kernel** of $f$ is an ideal $\mathfrak{a}$ of $A$, and the image of $f$ is a subring $C$ of $B$; and $f$ induces a ring isomorphism $A/\mathfrak{a} \cong C$

We shall sometimes use the notation $x \equiv y \mod \mathfrak{a}$; this means that $x - y \in \mathfrak{a}$

A **zero-divisor** in a ring $A$ is an element $x$ which divides 0, i.e., for which there exists $y \neq 0$ in $A$ s.t. $xy = 0$. A ring with no zero-divisor $\neq 0$ (and in which $1 \neq 0$) is called an **integral domain**.

An element $x \in A$ is **nilpotent** if $x^n = 0$ for some $n > 0$. A nilpotent element is a zero-divisor (unless $A = 0$)

A **unit** in $A$ is an element $x$ which "divides 1", i.e., an element $x$ s.t. $xy = 1$ for some $y \in A$. The element $y$ is then uniquely determined by $x$, and is written $x^{-1}$. The units in $A$ form a (multiplicative) abelian group

The multiples $ax$ of an element $x \in A$ from a **principal** ideal, denoted by $(x)$ or $Ax$. $x$ is a unit iff $(x) = A = (1)$. The **zero** ideal $(0)$ is denoted by 0

A **field** is a ring $A$ in which $1 \neq 0$ and every non-zero element is a unit. Every field is an integral domain

**Proposition 1.2.** *Let* $A$ *be a ring* $\neq 0$*. Then the following are equivalent:*

1. *$A$ is a field*
2. *the only ideals in $A$ are 0 and $(1)$*
3. *every homomorphism of $A$ into a non-zero ring $B$ is injective*

*Proof.* $2 \to 3$. Let $\phi : A \to B$ be a ring homomorphism. Then $\ker \phi$ is an ideal $\neq (1)$ in $A$, hence $\ker \phi = 0$, hence $\phi$ is injective

$3 \to 1$. Let $x$ be an element of $A$ which is not a unit. Then $(x) \neq (1)$, hence $B = A/(x)$ is not the zero ring. Let $\phi : A \to B$ be the natural homomorphism of $A$ onto $B$ with kernel $(x)$. By hypothesis, $\phi$ is injective, hence $(x) = 0$, hence $x = 0$ □

An ideal $\mathfrak{p}$ in $A$ is **prime** if $\mathfrak{p} \neq (1)$ and if $xy \in \mathfrak{p} \Rightarrow x \in \mathfrak{p}$ or $y \in \mathfrak{p}$

An ideal $\mathfrak{m}$ in $A$ is **maximal** if $\mathfrak{m}$ in $A$ is **maximal** if $\mathfrak{m} \neq (1)$ and if no ideal $\mathfrak{a}$ s.t. $\mathfrak{m} \subset \mathfrak{a} \subset (1)$ (**strict** inclusions). Equivalently

$$\mathfrak{p} \text{ is prime } \Leftrightarrow A/\mathfrak{p} \text{ is an integral domain}$$
$$\mathfrak{m} \text{ is maximal } \Leftrightarrow A/\mathfrak{m} \text{ is a field}$$

*Proof.* If $\mathfrak{m}$ is maximal and suppose $a \notin \mathfrak{m}$. Then $J = \{ra + i : i \in \mathfrak{m} \text{ and } r \in A\}$ is an ideal. Hence $J = A$. So there is $r \in A, \mathfrak{m} \in I$ s.t. $1 = ra + i$. So we have $1 \equiv ra \mod \mathfrak{m}$. Hence we find the inverse of $a + \mathfrak{m}$

If $A/\mathfrak{m}$ is a field and suppose $\mathfrak{m} \subset \mathfrak{n} \subset A$. Let $a \in \mathfrak{m} \setminus \mathfrak{n}$, then there exists a $b \in A$ s.t. $ab - 1 \in \mathfrak{m}$. So $ab + m = 1$ for some $m \in \mathfrak{m}$. But $ab \in \mathfrak{n}$ and $m \in \mathfrak{m} \subset \mathfrak{n}$, then we have $1 \in \mathfrak{n}$ and $\mathfrak{n} = A$. □

Hence a maximal ideal is prime. The zero ideal is prime iff $A$ is an integral domain

If $f : A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a prime ideal in $B$, then $f^{-1}(\mathfrak{q})$ is a prime ideal in $A$, for $A/f^{-1}(\mathfrak{q})$ is isomorphic to a subring of $B/\mathfrak{q}$ and hence has no zero-divisor $\neq 0$. (Explanation. Since $\mathfrak{q}$ is prime, $B/\mathfrak{q}$ is an integral domain and a subring of an integral domain is still an integral domain. Define the map $\varphi(a + f^{-1}(\mathfrak{q})) = f(a) + \mathfrak{q}$ and we need to show its a homomorphism. Then we show its injective.)

But if $\mathfrak{n}$ is a maximal ideal of $B$ it is not necessarily true that $f^{-1}(\mathfrak{n})$ is maximal in $A$; all we can say for sure is that it is prime. (Example: $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\mathfrak{n} = 0$).

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

*Proof.* This is the standard application of Zorn's lemma. Let $\Sigma$ be the set of all ideals $\neq (1)$ in $A$. Order $\Sigma$ by inclusion. $\Sigma$ is not empty, since $0 \in \Sigma$. To apply Zorn's lemma we must show that every chain in $\Sigma$ has an upper bound in $\Sigma$; let then $(\mathfrak{a}_\alpha)$ be a chain of ideals in $\Sigma$, so that for each pair of indices $\alpha, \beta$ we have either $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$ or $\mathfrak{a}_\beta \subseteq \mathfrak{a}_\alpha$. Let $\mathfrak{a} = \bigcup_\alpha \mathfrak{a}_\alpha$. Then $\mathfrak{a}$ is an ideal and $1 \notin \mathfrak{a}$. Hence $\mathfrak{a} \in \Sigma$ and is an upper bound of the chain. Hence $\Sigma$ has a maximal element □

**Corollary 1.4.** *If $\mathfrak{a} \neq (1)$ is an ideal of $A$, there exists a maximal ideal of $A$ containing $\mathfrak{a}$*

*Proof.* Apply 1.3 to $A/\mathfrak{a}$ and 1.3 $\square$

**Corollary 1.5.** *Every non-unit of $A$ is contained in a maximal ideal.*

A ring $A$ with exactly one maximal ideal $\mathfrak{m}$ is called a **local ring**. The field $k = A/\mathfrak{m}$ is called the **residue field** of $A$

**Proposition 1.6.**

1. *Let $A$ be a ring and $\mathfrak{m} \neq (1)$ an ideal of $A$ s.t. every $x \in A - \mathfrak{m}$ is a unit in $A$. Then $A$ is a local ring and $\mathfrak{m}$ its maximal ideal.*

2. *Let $A$ be a ring and $\mathfrak{m}$ a maximal ideal of $A$ s.t. every element of $1 + \mathfrak{m}$ is a unit in $A$. Then $A$ is a local ring*

*Proof.*

2. Let $x \in A - \mathfrak{m}$. Since $\mathfrak{m}$ is maximal, the ideal generated by $x$ and $\mathfrak{m}$ is $(1)$, hence there exist $y \in A$ and $t \in \mathfrak{m}$ s.t. $xy + t = 1$; hence $xy = 1 - t$ belongs to $1 + \mathfrak{m}$ and therefore is a unit. Now use 1

$\square$

A ring with only a finite number of maximal ideals is called **semi-local**

**Example 1.1.**

1. $A = k[x_1, \dots, x_n]$, $k$ a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal $(f)$ is prime

2. $A = \mathbb{Z}$. Every ideal in $\mathbb{Z}$ is of the form $(m)$ for some $m \geq 0$. The ideal $(m)$ is prime iff $m = 0$ or a prime number. All the ideals $(p)$, where $p$ is a prime number, are maximal: $\mathbb{Z}/(p)$ is the field of $p$ elements

3. A **principal ideal domain** is an integral domain in which every ideal is principal. In such a ring every non-zero prime ideal is maximal. For if $(x) \neq 0$ is a prime ideal and $(y) \supset (x)$, we have $x \in (y)$, say $x = yz$, so that $yz \in (x)$ and $y \notin (x)$, hence $z \in (x)$; say $z = tx$. Then $x = yz = ytx$, so that $yt = 1$ and therefore $(y) = (1)$.

**Proposition 1.7.** *The set $\mathfrak{N}$ of all nilpotent elements in a ring $A$ is an ideal, and $A/\mathfrak{N}$ has no nilpotent $\neq 0$*

*Proof.* If $x \in \mathfrak{N}$, clearly $ax \in \mathfrak{N}$ for all $a \in A$. Let $x, y \in \mathfrak{N}$: say $x^m = 0$, $y^n = 0$. By the binomial theorem, $(x+y)^{n+m-1}$ is a sum of integer multiples of products $x^r y^s$, where $r + s = m + n - 1$;

Let $\bar{x} \in A/\mathfrak{N}$ be represented by $x \in A$. Then $\bar{x}^n$ is represented by $x^n$, so that $\bar{x}^n = 0 \Rightarrow x^n \in \mathfrak{N} \Rightarrow (x^n)^k = 0$ for some $k > 0 \Rightarrow x \in \mathfrak{N} \Rightarrow \bar{x} = 0$ $\square$

The ideal $\mathfrak{N}$ is called the **nilradical** of $A$

Check When is nilradical not a prime ideal, which is related to Exercise 1.1.18.

**Proposition 1.8.** *The nilradical of $A$ is the intersection of all the prime ideals of $A$*

*Proof.* Let $\mathfrak{N}'$ denote the intersection of all the prime ideals of $A$. If $f \in A$ is nilpotent and if $\mathfrak{p}$ is a prime ideal, then $f^n = 0 \in \mathfrak{p}$ for some $n > 0$, hence $f \in \mathfrak{p}$. Hence $f \in \mathfrak{N}'$

Conversely, suppose that $f$ is not nilpotent. Let $\Sigma$ be the set of ideals $\mathfrak{a}$ with the property

$$n > 0 \Rightarrow f^n \notin \mathfrak{a}$$

Then $\Sigma$ is not empty because $0 \in \Sigma$. Zorn's lemma can be applied to the set $\Sigma$, ordered by inclusion, and therefore $\Sigma$ has a maximal element. We shall show that $\mathfrak{p}$ is a prime ideal. Let $x, y \notin \mathfrak{p}$. Then the ideals $\mathfrak{p} + (x)$, $\mathfrak{p} + (y)$ strictly contain $\mathfrak{p}$ and therefore do not belong to $\Sigma$; hence

$$f^m \in \mathfrak{p} + (x), \quad f^n \in \mathfrak{p} + (y)$$

for some $m, n$. It follows that $f^{m+n} \in \mathfrak{p} + (xy)$, hence the ideal $\mathfrak{p} + (xy)$ is not in $\Sigma$ and therefore $xy \notin \mathfrak{p}$. Hence we have a prime ideal $\mathfrak{p}$ s.t. $f \notin \mathfrak{p}$, so that $f \notin \mathfrak{N}'$ □

The **Jacobson radical** $\mathfrak{R}$ of $A$ is defined to be the intersection of all the maximal ideals of $A$. It can be characterized as follows:

**Proposition 1.9.** *$x \in \mathfrak{R}$ iff $1 - xy$ is a unit in $A$ for all $y \in A$*

*Proof.* $\Rightarrow$: Suppose $1 - xy$ is not a unit. By 1.1.4 it belongs to some maximal ideal $\mathfrak{m}$; but $x \in \mathfrak{R} \subseteq \mathfrak{m}$, hence $xy \in \mathfrak{m}$ and therefore $1 \in \mathfrak{m}$, which is absurd

$\Leftarrow$: Suppose $x \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Then $\mathfrak{m}$ and $x$ generate the unit ideal $(1)$, so that we have $u + xy = 1$ for some $u \in \mathfrak{m}$ and some $y \in A$. Hence $1 - xy \in \mathfrak{m}$ and is therefore not a unit. □

If $\mathfrak{a}, \mathfrak{b}$ are ideals in a ring $A$, their **sum** $\mathfrak{a} + \mathfrak{b}$ is the set of all $x + y$ where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the smallest ideal containing $\mathfrak{a}$ and $\mathfrak{b}$. More generally, we may define the sum $\sum_{i \in I} a_i$ of any family (possibly infinite) of ideals $\mathfrak{a}_i$ of $A$; is elements are all sums $\sum x_i$, where $x_i \in \mathfrak{a}_i$ for all $i \in I$ and almost all of the $x_i$ (i.e., all but a finite set) are zero. It is the smallest ideal of $A$ which contains all the ideals $\mathfrak{a}_i$

The **product** of two ideals $\mathfrak{a}, \mathfrak{b}$ in $A$ is the ideal $\mathfrak{a}\mathfrak{b}$ **generated** by all products $xy$, where $x \in \mathfrak{a}$ and $y \in \mathfrak{b}$. It is the set of all finite sums $\sum x_i y_i$ where each $x_i \in \mathfrak{a}$ and each $y_i \in \mathfrak{b}$

We have the **distributive law**

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

In the ring $\mathbb{Z}$, $\cap$ and $+$ are distributive over each other. This is not the case in general. **modular law**

$$\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a}\cap\mathfrak{b} + \mathfrak{a}\cap\mathfrak{b} \text{ if } \mathfrak{a} \supseteq \mathfrak{b} \text{ or } \mathfrak{a} \supseteq \mathfrak{c}$$

$$\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b} \text{ provided } \mathfrak{a}+\mathfrak{b} = (1)$$

If $x \in \mathfrak{a}\cap\mathfrak{b}$, there is $a+b=1$. Hence $xa+xb = x \in \mathfrak{a}\mathfrak{b}$

Two ideals $\mathfrak{a}, \mathfrak{b}$ are said to be **coprime** if $\mathfrak{a}+\mathfrak{b} = (1)$. Thus for coprime ideals we have $\mathfrak{a}\cap\mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Let $A$ be a ring and $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideals of $A$. Define a homomorphism

$$\phi : A \to \prod_{i=1}^{n}(A/\mathfrak{a}_i)$$

by the rule $\phi(x) = (x+\mathfrak{a}_1, \dots, x+\mathfrak{a}_n)$

**Proposition 1.10.** *1. If $\mathfrak{a}_i, \mathfrak{a}_j$ are coprime whenever $i \neq j$, then $\prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$*

2. *$\phi$ is surjective iff $\mathfrak{a}_i$, $\mathfrak{a}_j$ are coprime whenever $i \neq j$*

3. *$\phi$ is injective iff $\bigcap \mathfrak{a}_i = (0)$*

*Proof.* 1. Induction on $n$. The case $n=2$ is dealt with above. Suppose $n > 2$ and the result true for $\mathfrak{a}_1, \dots, \mathfrak{a}_{n-1}$, and let $\mathfrak{b} = \prod_{i=1}^{n-1}\mathfrak{a}_i = \bigcap_{i=1}^{n-1}\mathfrak{a}_i$. As we have $x_i + y_i = 1$ $(x_i \in \mathfrak{a}_i, y_i \in \mathfrak{a}_n)$ and therefore

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1-y_i) \equiv 1 \mod \mathfrak{a}_n$$

Hence $\mathfrak{a}_n + \mathfrak{b} = (1)$ and so

$$\prod_{i=1}^{n}\mathfrak{a}_i = \mathfrak{b}\mathfrak{a}_n = \mathfrak{b}\cap\mathfrak{a}_n = \bigcap_{i=1}^{n}\mathfrak{a}_i$$

2. $\Rightarrow$: Let's show for example that $\mathfrak{a}_1, \mathfrak{a}_2$ are coprime. There exists $x \in A$ s.t. $\phi(x) = (1, 0, \dots, 0)$; hence $x \equiv 1 \mod \mathfrak{a}_1$ and $x \equiv 0 \mod \mathfrak{a}_2$, so that

$$1 = (1-x) + x \in \mathfrak{a}_1 + \mathfrak{a}_2$$

$\Leftarrow$: It is enough to show, for example, that there is an element $x \in A$ s.t. $\phi(x) = (1, 0, \dots, 0)$. Since $\mathfrak{a}_1 + \mathfrak{a}_i = (1)$ $(i > 1)$ we have $u_i + v_i = 1$ $(u_i \in \mathfrak{a}_1, v_i \in \mathfrak{a}_i)$. Take $x = \prod_{i=2}^n v_i$, then $x = \prod(1 - u_i) \equiv 1 \mod \mathfrak{a}_1$. Hence $\phi(x) = (1, 0, \dots, 0)$

3. $\bigcap \mathfrak{a}_i$ is the kernel of $\phi$

□

**Proposition 1.11.** 1. *Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be prime ideals and let $\mathfrak{a}$ be an ideal contained in $\bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some $i$.*

2. *Let $\mathfrak{a}_1, \dots, \mathfrak{a}_n$ be ideals and let $\mathfrak{p}$ be a prime ideal containing $\bigcap_{i=1}^n \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some $i$. If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some $i$*

*Proof.* 1. induction on $n$ in the form

$$\mathfrak{a} \not\subseteq \mathfrak{p}_i (1 \leq i \leq n) \Rightarrow \mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$$

It is true for $n = 1$. If $n > 1$ and the result is true for $n - 1$, then for each $i$ there exists $x_i \in \mathfrak{a}$ s.t. $x_i \notin \mathfrak{p}_j$ whenever $j \neq i$. If for some $i$ we have $x_i \notin \mathfrak{p}_i$, we are through. If not, then $x_i \in \mathfrak{p}_i$ for all $i$. Consider the element

$$y = \sum_{i=1}^n x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n$$

we have $y \in \mathfrak{a}$ and $y \notin \mathfrak{p}_i$ $(1 \leq i \leq n)$. Hence $\mathfrak{a} \not\subseteq \bigcup_{i=1}^n \mathfrak{p}_i$

2. Suppose $\mathfrak{p} \not\supseteq \mathfrak{a}_i$ for all $i$. Then there exist $x_i \in \mathfrak{a}_i$, $x_i \notin \mathfrak{p}$ $(1 \leq i \leq n)$ and therefore $\prod x_i \in \prod \mathfrak{a}_i \subseteq \bigcap \mathfrak{a}_i$; but $\prod x_i \notin \mathfrak{p}$ since $\mathfrak{p}$ is prime. Hence $\mathfrak{p} \not\supseteq \bigcap \mathfrak{a}_i$

If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} \subseteq \mathfrak{a}_i$ and hence $\mathfrak{p} = \mathfrak{a}_i$ for some $i$.

□

For prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, if $\bigcap_{i=1}^n \mathfrak{p}_i = \mathfrak{p}$ is a prime ideal, then $\mathfrak{p} = \mathfrak{p}_i$ for some $i$. If there are more than one minimal ideal, this could never happen

If $\mathfrak{a}, \mathfrak{b}$ are ideals in a ring $A$, their **ideal quotient** is

$$(\mathfrak{a} : \mathfrak{b}) = \{x \in A : x\mathfrak{b} \subseteq \mathfrak{a}\}$$

which is an ideal. In particular, $(0 : \mathfrak{b})$ is called the **annihilator** of $\mathfrak{b}$ and is also denoted by $\mathrm{Ann}(\mathfrak{b})$: it is the set of all $x \in A$ s.t. $x\mathfrak{b} = 0$. In this notation the set of all zero-divisors in $A$ is

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x)$$

If $\mathfrak{b}$ is a principal ideal $(x)$, we shall write $(\mathfrak{a} : x)$ in place of $(\mathfrak{a} : (x))$

**Example 1.2.** If $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, $\mathfrak{b} = (n)$, where say $m = \prod_p p^{\mu_p}$, $n = \prod_p p^{\nu_p}$, then $(\mathfrak{a} : \mathfrak{b}) = (q)$ where $q = \prod_p p^{\gamma_p}$ and

$$\gamma_p = \max(\mu_p - \nu_p, 0) = \mu_p - \min(\mu_p, \nu_p)$$

Hence $q = m/(m,n)$, where $(m,n)$ is the h.c.f. of $m$ and $n$

*Exercise* 1.0.1.

1. $\mathfrak{a} \subseteq (\mathfrak{a} : \mathfrak{b})$
2. $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subseteq \mathfrak{a}$
3. $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = (\mathfrak{a} : \mathfrak{b}\mathfrak{c}) = ((\mathfrak{a} : \mathfrak{c}) : \mathfrak{b})$
4. $(\bigcap_i \mathfrak{a}_i : \mathfrak{b}) = \bigcap_i (\mathfrak{a}_i : \mathfrak{b})$
5. $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \bigcap (\mathfrak{a} : \mathfrak{b}_i)$

*Proof.*

3. $(\mathfrak{a} : \mathfrak{b}) : \mathfrak{c} = \{x \in A : x\mathfrak{c} \subseteq \mathfrak{a} : \mathfrak{b}\}$. for any $c \in \mathfrak{c}$, $xc\mathfrak{b} \subseteq \mathfrak{a}$. Hence $x\mathfrak{c}\mathfrak{b} \subseteq \mathfrak{a}$.

5. $(\mathfrak{a} : \sum_i \mathfrak{b}_i) = \{x \in A : x \sum_i \mathfrak{b}_i \subseteq \mathfrak{a}\}$

□

If $\mathfrak{a}$ is any ideal of $A$, the **radical** of $\mathfrak{a}$ is

$$r(\mathfrak{a}) = \{x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0\}$$

if $\phi : A \to A/\mathfrak{a}$ is the standard homomorphism, then $r(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}})$ and hence $r(\mathfrak{a})$ is an ideal by 1.7

*Exercise* 1.0.2.

1. $r(\mathfrak{a}) \supseteq \mathfrak{a}$
2. $r(r(\mathfrak{a})) = r(\mathfrak{a})$
3. $r(\mathfrak{a}\mathfrak{b}) = r(\mathfrak{a} \cap \mathfrak{b}) = r(\mathfrak{a}) \cap r(\mathfrak{b})$
4. $r(\mathfrak{a}) = (1)$ iff $\mathfrak{a} = (1)$.
5. $r(\mathfrak{a} + \mathfrak{b}) = r(r(\mathfrak{a}) + r(\mathfrak{b}))$

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

*Proof.* 5. $x \in r(\mathfrak{a}+\mathfrak{b})$ iff $x^n \in \mathfrak{a}+\mathfrak{b}$. $y \in r(r(\mathfrak{a})+r(\mathfrak{b}))$ iff $y^m = a+b$, where $a^{n_a} \in \mathfrak{a}$ and $b^{n_b} \in \mathfrak{b}$. Then $(y^m)^{n_a+n_b} = (a+b)^{n_a+n_b} \in \mathfrak{a}+\mathfrak{b}$

6. $x \in r(\mathfrak{p}^n)$ iff $x^m \in \mathfrak{p}^n$, then $x^m = p_1 \cdots p_n \in \mathfrak{p}$

□

**Proposition 1.12.** *The radical of an ideal* $\mathfrak{a}$ *is the intersection of the prime ideals which contain* $\mathfrak{a}$

*Proof.* Apply 1.8 to $A/\mathfrak{a}$.
Nilradical of $A/\mathfrak{a}$ is the radical of $\mathfrak{a}$. □

More generally, we may define the radical $r(E)$ of any **subset** $E$ of $A$ in the same way. It is **not** an ideal in general. We have $r(\bigcup_\alpha E_\alpha) = \bigcup r(E_\alpha)$ for any family of subsets $E_\alpha$ of $A$

**Proposition 1.13.** $D =$ *set of zero-divisors of* $A = \bigcup_{x \neq 0} r(\mathrm{Ann}(x))$

*Proof.* $D = r(D) = r(\bigcup_{x\neq 0} \mathrm{Ann}(x)) = \bigcup_{x \neq 0} r(\mathrm{Ann}(x))$ □

**Example 1.3.** If $A = \mathbb{Z}$, $\mathfrak{a} = (m)$, let $p_i$ $(1 \leq i \leq r)$ be the distinct prime divisors of $m$. Then $r(\mathfrak{a}) = (p_1 \cdots p_r) = \bigcap_{i=1}^n (p_i)$

**Proposition 1.14.** *Let* $\mathfrak{a}$, $\mathfrak{b}$ *be ideals in a ring* $A$ *s.t.* $r(\mathfrak{a})$, $r(\mathfrak{b})$ *are coprime. Then* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are coprime.*

*Proof.* $r(\mathfrak{a}+\mathfrak{b}) = r(r(\mathfrak{a})+r(\mathfrak{b})) = r(1) = (1)$, hence $\mathfrak{a}+\mathfrak{b} = (1)$ □

Let $f : A \to B$ be a ring homomorphism. If $\mathfrak{a}$ is an ideal in $A$, the set $f(\mathfrak{a})$ is not necessarily an ideal in $B$ (e.g. $\mathbb{Z} \to \mathbb{Q}$). We define the **extension** $\mathfrak{a}^e$ of $\mathfrak{a}$ to be the ideal $Bf(\mathfrak{a})$ generated by $f(\mathfrak{a})$ in $B$: explicitly, $\mathfrak{a}^e$ is the set of all sums $\sum y_i f(x_i)$ where $x_i \in \mathfrak{a}$, $y_i \in B$

If $\mathfrak{b}$ is an ideal of $B$, then $f^{-1}(\mathfrak{b})$ is always an ideal of $A$, called the **contraction** $\mathfrak{b}^c$ of $\mathfrak{b}$. If $\mathfrak{b}$ is prime, then $\mathfrak{b}^c$ is prime. If $\mathfrak{a}$ is prime, $\mathfrak{a}^e$ need not be prime ($f : \mathbb{Z} \to \mathbb{Q}$,$\mathfrak{a} \neq 0$, then $\mathfrak{a}^e = \mathbb{Q}$, which is not a prime ideal)

We can factorize $f$ as follows:

$$f \xrightarrow{p} f(A) \xrightarrow{j} B$$

where $p$ is surjective and $j$ is injective

**Example 1.4.** Consider $\mathbb{Z} \to \mathbb{Z}[i]$, where $i = \sqrt{-1}$. A prime ideal $(p)$ of $\mathbb{Z}$ may or may not stay prime when extended to $\mathbb{Z}[i]$. In fact $\mathbb{Z}[i]$ is a principal ideal domain (because it has a Euclidean algorithm, i.e., a Euclidean ring) and the situation is as follows:

1. $(2^e) = ((1+i)^2)$, the **square** of a prime ideal in $\mathbb{Z}[i]$
2. if $p \equiv 1 \mod 4$ then $(p)^e$ is the product of two distinct prime ideals (for example, $(5)^e = (2+i)(2-i)$)
3. if $p \equiv 3 \mod 4$ then $(p)^e$ is prime in $\mathbb{Z}[i]$

Let $f : A \to B$, $\mathfrak{a}$ and $\mathfrak{b}$ be as before. Then

**Proposition 1.15.** *1.* $\mathfrak{a} \subseteq \mathfrak{a}^{ec}$, $\mathfrak{b} \supseteq \mathfrak{b}^{ce}$

2. $\mathfrak{b}^c = \mathfrak{b}^{cec}$, $\mathfrak{a}^e = \mathfrak{a}^{ece}$
3. *If $C$ is the set of contracted ideals in $A$ and if $E$ is the set of extended ideals in $B$, then $C = \{\mathfrak{a} \mid \mathfrak{a}^{ec} = \mathfrak{a}\}$, $E = \{\mathfrak{b} \mid \mathfrak{b}^{ce} = \mathfrak{b}\}$, and $\mathfrak{a} \mapsto \mathfrak{a}^e$ is a bijective map of $C$ onto $E$, whose inverse is $\mathfrak{b} \mapsto \mathfrak{b}^c$.*

*Proof.* 3. If $\mathfrak{a} \in C$, then $\mathfrak{a} = \mathfrak{b}^c = \mathfrak{b}^{cec} = \mathfrak{a}^{ec}$; conversely if $\mathfrak{a} = \mathfrak{a}^{ec}$ then $\mathfrak{a}$ is the contraction of $\mathfrak{a}^e$.

□

*Proof.* 1.

□

*Exercise* 1.0.3. If $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals of $A$ and if $\mathfrak{b}_1, \mathfrak{b}_2$ are ideals of $B$, then

$$(\mathfrak{a}_1 + \mathfrak{a}_2)^e = \mathfrak{a}_1^e + \mathfrak{a}_2^e \quad (\mathfrak{b}_1 + \mathfrak{b}_2)^c \supseteq \mathfrak{b}_1^c + \mathfrak{b}_2^c$$

## 1.1 Exercise

**Proposition 1.16.** *For $f : X \to Y$, given any $B \subseteq Y$, $f(f^{-1}(B)) \subseteq B$. If $f$ is surjective, $f(f^{-1}(B)) = B$*

*Proof.* For any $x \in f(f^{-1}(B))$, there is $y \in f^{-1}(B)$ s.t. $f(y) = x$. Thus $x \in B$.

For any $y \in B$, as $f$ is surjective, there is $x \in X$ s.t. $f(x) = y$. So $x \in f^{-1}(B)$ and hence $y \in f(f^{-1}(B))$ □

*Exercise* 1.1.1. 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

*Proof.* $x$ is a element of a nilradical, which is the intersection all prime ideals. Since every maximal ideal is a prime ideal, then nilradical is a subset of Jacobson radical. Then $1 - (-u^{-1})x$ is a unit for some unit $u$, hence $u + x$ is a unit □

*Exercise* 1.1.2. Let $A$ be a ring and let $A[x]$ be the ring of polynomials in an indeterminate $x$, with coefficients in $A$. Let $f = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$. Prove that

1. $f$ is a unit in $A[x]$ iff $a_0$ is a unit in $A$ and $a_1, \dots, a_n$ are nilpotent [if $b_0 + b_1 x + \cdots + b_m x^m$ 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 Exercise 1.1.1]

2. $f$ is nilpotent iff $a_0, \dots, a_n$ is nilpotent

3. $f$ is a zero-divisor iff there exists $a \neq 0$ in $A$ s.t. $af = 0$

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

*Proof.*

1. Suppose $g = \sum_{i=0}^m b_i x^i$ s.t. $fg = 1$. For $r = 0$, $a_n b_m = 0$ obviously.

   Now suppose this is true for all $p < r$. Now we prove $a_n^{r+1} b_{m-r} = 0$. The $m + n - r$th term's coefficient is $\sum_{i=0}^r a_{n-i} b_{m-r+i} = 0$. Then

   $$a_n^{r+1} \sum_{i=0}^r a_{n-i} b_{m-r+i} = a_n^{r+1} b_{m-r} = 0$$

   Thus $a_n^{m+1} b_0 = 0$ and hence $a_n^{m+1} = 0$ as $b_0$ is a unit. So $f - a_n x^n$ is a unit and we can continue.

2. $\Rightarrow$. Goal: for any prime ideal $\mathfrak{p}$ in $A$, $f$ is 0 in $(A/\mathfrak{p})[x]$. This is because $f^n$ is 0 in $(A/\mathfrak{p})[x]$ and $A/\mathfrak{p}$ is an integral domain. Then for $a_0, \dots, a_n$ is contained in every prime ideal and hence are nilpotent

   If $f$ is nilpotent and $a_k$ is nilpotent, then $f - a_k x^k$ is still nilpotent since nilradical is an ideal

   $\Leftrightarrow$. Nilradical $\mathfrak{R}$ is an ideal. As $a_0, \dots, a_n$ is nilpotent in $A[x]$, their $A[x]$-combination is still nilpotent

3. Choose a polynomial $g = b_0 + b_1 x + \cdots + b_m x^m$ of least degree $m$ s.t. $fg = 0$. Then $a_n b_m = 0$ and $a_n g f = 0$. As $g$ is of least degree, we have $a_n g = 0$. Then $fg = a_0 g + \cdots + a_{n-1} x^{n-1} g + a_n g = a_0 g + \cdots + a_{n-1} x^{n-1} g = 0$. Hence for all $0 \le i \le n$, $a_i g = 0$. Arbitrary coefficient of $g$ is what we want

4. If $fg$ is primitive, then $(\sum_{\max\{0,k-m\}}^{\min\{n,k\}} a_i b_{k-i})_{k \in [0,n+m]} = (1)$. Change the coefficient one by one

   By extract, we can get $(a_0^k b_k)_{k \in [0,n+m]} = (1)$. Then $(b_k) = (1)$.

□

*Exercise* 1.1.3. In the ring $A[x]$, the Jacobson radical is equal to the nilradical

*Proof.* Suppose $\mathfrak{R}$ is the Jacobson radical and $f \in \mathfrak{R}$, then $1 - fx$is a unit by Proposition 1.9. By Exercise 1.1.2 (1) all coefficients of $f$ are nilpotent, then $f$ is nilpotent by Exercise 1.1.2 (2) □

*Exercise* 1.1.4. Let $A$ be the 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

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

2. If $f$ is nilpotent, then $a_n$ is nilpotent for all $n \ge 0$.

3. $f$ belongs to the Jacobson radical of $A[[x]]$ iff $a_0$ belongs to the Jacobson radical of $A$

4. 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 $x$.

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

*Proof.* 1. $\Leftarrow$. We compute $b_n$ from $a_0, \dots, a_n, b_0, \dots, b_{n-1}$ and $\sum_{i=0}^{n} a_i b_{n-i} = 0$. Multiply it with $a_0$, we get $b_n + a_0 \sum_{i=1}^{n} a_i b_{n-i} = 0$

2. Note that nilradical is an ideal. If $a_k$ is nilpotent in $A$, then $a_k x$ is nilpotent in $A[[x]]$, and $f - a_k x^k$ is nilpotent. And we continue

3. For any $b \in A$, $1 - bf$ is a unit, and by (1), $1 - ba_0$ is a unit.

4. From (3), a maximal ideal $\mathfrak{m}$ at least contains $xA[[x]]$. Let $\mathfrak{m} = \mathfrak{m}^c + xA[[x]]$. Now

$$A[[x]]/\mathfrak{m} \cong (A[[x]]/xA[[x]])/(\mathfrak{m}/xA[[x]]) \cong A/\mathfrak{m}^c$$

   Thus $\mathfrak{m}$ is maximal

5. Given a prime ideal $\mathfrak{p}$ of $A$, consider

$$\phi : A[[x]] \to A \to A/\mathfrak{p}$$

Then $\ker \phi = \mathfrak{p} + xA[[x]]$ and $A[[x]]/\ker \phi \cong A/\mathfrak{p}$ and hence $\ker \phi$ is a prime ideal.

□

*Exercise* 1.1.5. A ring $A$ is s.t. every ideal not contained in the nilradical contains a nonzero idempotent (that is, an element $e$ s.t. $e^2 = e \neq 0$). Prove that the nilradical and Jacobson radical of $A$ are equal

*Proof.* If there is a $x \in A$ s.t. $x \in \mathfrak{R}$ and $x \notin \mathfrak{N}$. Then $(x) \not\subseteq \mathfrak{N}$ and there is $y \in A$ s.t. $y^2x^2 = x^2$ and hence $(y^2 - 1)x^2 = 0$. As $x^2 \neq 0$, $y^2 = 1$. Hence $\mathfrak{R} = (1)$, which is not possible □

*Exercise* 1.1.6. Let $A$ be a ring where every element $x$ satisfies $x^n = x$ for some $n > 1$ (depending on $x$). Show that every prime ideal in $A$ is maximal

*Proof.* $\mathfrak{p}$ the prime ideal and $x \notin \mathfrak{p}$, as $x(x^{n-1} - 1) = 0 \in \mathfrak{p}$, $x^{n-1} - 1 \in \mathfrak{p}$. Then $x^{n-1} \equiv 1 \mod \mathfrak{p}$ and $(x + \mathfrak{p})(x^{n-2} + \mathfrak{p}) = 1 + \mathfrak{p}$. □

*Exercise* 1.1.7. Let $A$ be a ring $\neq 0$. Show that the set of prime ideals of $A$ has minimal elements w.r.t. inclusion

*Proof.* Equivalently to say that nilradical is prime. □

*Exercise* 1.1.8. 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

*Proof.* $\Rightarrow$. From Proposition 1.12
$\Leftarrow$. If $x^n \in \mathfrak{a}$, then $x \in \mathfrak{a}$. □

*Exercise* 1.1.9. Let $A$ be a ring, $\mathfrak{N}$ its nilradical. Show that the following are equivalent

1. $A$ has exactly one prime ideal
2. every element of $A$ is either a unit or nilpotent
3. $A/\mathfrak{N}$ is a field

*Proof.* $2 \to 3$. $\mathfrak{N}$ is maximal
$1 \to 2$. Obvious:D
$3 \to 1$. Then $\mathfrak{N}$ is maximal □

*Exercise* 1.1.10. A ring is **Boolean** if $x^2 = x$ for all $x \in A$. In a Boolean ring $A$, show that

1. $2x = 0$ for all $x \in A$
2. every prime ideal $\mathfrak{p}$ is maximal, and $A/\mathfrak{p}$ is a field with two elements
3. every finitely generated ideal in $A$ is principal

*Proof.*

1. $2x = x + x^2 = 0$
2. Maximality by Exercise 1.1.6. For any $x \notin \mathfrak{p}$, $(x+\mathfrak{p})(1+\mathfrak{p}) = 1+\mathfrak{p}$ and so $x \equiv 1 \mod \mathfrak{p}$. For any $x \in \mathfrak{p}$, $x \equiv 0 \mod \mathfrak{p}$.
3. Let $x, y$ be elements of an ideal $\mathfrak{a}$. Define $z := x + y + xy$, note that $xz = x + y + y = x$. Hence $(x, y) = (z)$

□

*Exercise* 1.1.11. A local ring contains no idempotent $\neq 0, 1$

*Proof.* If $\mathfrak{m}$ is the unique maximal ring. Then $x \in \mathfrak{m}$ iff for all $y \in A$, $1 - xy$ is a unit.

If $x^2 = x$, then $x(1-x) = 0$. As $1 - x$ is not a unit, $x \notin \mathfrak{m}$. □

*Construction of an algebraic closure of a field*

*Exercise* 1.1.12. Let $K$ be a field and let $\Sigma$ 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 indeterminate $x_f$, 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 $K$.

*Proof.* Irreducible polynomials have degree greater than 1. There is no linear combination that the degree of the sum is 0

Let $K_0 = K$ be a field. Given a non-negative integer $n$ for which the field, $K_n$, is defined, let $\Sigma_n$ be the set of monic irreducible elements of $K_n[x]$ and let $A_n$ be the polynomial ring over $K_n$ generated by the set of indeterminates $\{x_f \mid f \in \Sigma\}$. Define $\mathfrak{a}_n$ be the ideal of $A_n$ generated by the set $\{f(x_f) \in A \mid$

$f(\Sigma_n)\}$. Since $K_n$ is a field, $A_n$ is a domain. Thus every element of $\mathfrak{a}_n$ has positive degree and $\mathfrak{a}_n$ doesn't contain 1. Let $\mathfrak{m}_n$ be a maximal ideal of $A_n$ containing $\mathfrak{a}_n$ and define $K_{n+1} = A_n/\mathfrak{m}_n$. The map

$$K_n \to A_n \to A_n/\mathfrak{m}_n = K_{n+1}$$

given by the inclusion and quotient maps, is a field homomorphism. Thus it is injective and we may identify $K_n$ with a subfield of $K_{n+1}$. Note that for any $0 \neq k \in K_n$, $k \notin \mathfrak{m}$. Thus the kernel of the map is only $\{0\}$.

Let $\overline{K} = \bigcup_{n\geq 0} K_n$. If $x, y \in \overline{K}$ , then they are contained in some subfields $K_n, K_m$. Letting $k = \max\{m, n\}$, $x, y \in K_k$. Therefore the sum, difference, and product of $x, y$ are in $K_k$. Any field arithmetic of $\overline{K}$ can be performed in a subfield, $\overline{K}$ is a field.

Let $f$ be an irreducible monic polynomial in $\overline{K}[x]$. Since $f$ has only finitely many coefficients, there is some $n$ s.t. $f$ is an irreducible monic polynomial in $K_n[x]$. By construction, $f$ has a root in $K_{n+1}$, hence in $\overline{K}$. By the Euclidean division, $f$ must have degree 1. Therefore, $\overline{K}$ is algebraic closed.

By construction, the field extension $K_{n+1}/K_n$ is algebraic for every $n$. $\square$

*Exercise* 1.1.13. In a ring $A$, let $\Sigma$ be the set of all ideals in which every element is a zero-divisor. Show that the set $\Sigma$ has minimal elements and that every maximal element of $\Sigma$ is a prime ideal. Hence the set of zero-divisors in $A$ is a union of prime ideals

*Proof.* If $x$ is a zero-divisor, then $Ax$ is a set of zero-divisors. Thus $\Sigma$ is not empty and has a minimal element w.r.t. inclusion.

For a maximal ideal $\mathfrak{p}$ in $\Sigma$, suppose $x, y \notin \mathfrak{p}$, then $\mathfrak{p} + (x) + (y) \notin \Sigma$. Then there is an element $p + x'x + y'y$ that is not a zero-divisor. If $xy$ is zero-divisor, then $(p'xy)(p + x'x + y'y) = 0$, a contradiction $\square$

*The prime spectrum of a ring*

*Exercise* 1.1.14. 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

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

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

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

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

4. $V(\mathfrak{a}\cap\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b}) = V(\mathfrak{a})\cup V(\mathfrak{b})$ 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 as Spec$(A)$

*Proof.* 1. If $\mathfrak{a} = (E)$, then $\mathfrak{a}$ is the minimal ideal containing $E$. Hence $V(E) = V(\mathfrak{a})$. For any prime ideal $\mathfrak{p}$ containing $\mathfrak{a}$ and any $a \in r(\mathfrak{a})$. Then $a^n \in \mathfrak{a}$ for some $n$. Then $a^n \in \mathfrak{p}$, implying $a \in \mathfrak{p}$. Hence $V(\mathfrak{a}) \subseteq V(r(\mathfrak{a}))$.

2. Obvious

3. trivial

4. As $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, if $\mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{p}$ then $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$. On the other hand, if $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{p}$, then we have shown either $\mathfrak{a} \subseteq \mathfrak{p}$ or $\mathfrak{b} \subseteq \mathfrak{p}$ (Proposition 1.11). Thus $\mathfrak{a}\cap\mathfrak{b} \subseteq \mathfrak{p}$

□

*Exercise* 1.1.15. Draw pictures of Spec$(\mathbb{Z})$, Spec$(\mathbb{R})$, Spec$(\mathbb{C}[x])$, Spec$(\mathbb{R}[x])$, Spec$(\mathbb{Z}[x])$

*Proof.* $\mathbb{Z}$ is PID, for any $E \subseteq \mathbb{Z}$, let $n = \min\{m \in E \mid m > 1\}$. Let $\mathfrak{a} = (n)$. Then $(E) = \mathfrak{a}$. Suppose $n = p_1^{n_1} \dots p_r^{n_r}$, then $V(E) = \{p_1\mathbb{Z}, \dots, p_r\mathbb{Z}\}$.

$\mathbb{R}$ is a field and so there is only trivial ideals.

$\mathbb{C}[x]$ is a PID. Prime ideals are of the form $(f)$, where $f$ is a monic irreducible or $f = 0$. As irreducible elements of $\mathbb{C}[x]$ is of the form $x - a$. Thus Spec $\mathbb{C}[x]$ is actually the complex plane.

For any ideal $\mathfrak{a}$ of $\mathbb{C}[x]$, $\mathfrak{a} = (f)$. By the Fundamental Theorem of Algebra, $f = \prod_{i=1}^{k}(x - a_i)^{\alpha_i}$ for some complex numbers $a_1, \dots, a_k$ and positive integers $\alpha_1, \dots, \alpha_k$. Define $\sqrt{f}$ as $\prod_{i=1}^{k}(x - a_i)$. Since non-zero prime ideals of $\mathbb{C}[x]$ are maximal, we have

$$V(\mathfrak{a}) = V(f) = V(\sqrt{f}) = \bigcup_{i=1}^{k} V(x - a_i) = \{(x - a_1), \dots, (x - a_k)\}$$

Therefore non-empty open subsets of Spec $\mathbb{C}[x]$ are cofinite sets containing $\{0\}$

□

*Exercise* 1.1.16. For each $f \in A$, let $X_f$ denote the complement of $V(f)$ in $X = \text{Spec}(A)$. The sets $X_f$ are open. Show that they form a basis of open sets for the Zariski topology, and that

1. $X_f \cap X_g = X_{fg}$
2. $X_f = \emptyset$ iff $f$ is nilpotent
3. $X_f = X$ iff $f$ is a unit
4. $X_f = X_g$ iff $r((f)) = r((g))$
5. $X$ is quasi-compact (that is, every open covering of $X$ has a finite sub-covering)
6. More generally, each $X_f$ is quasi-compact
7. An open subset of $X$ is quasi-compact iff it is a finite union of sets $X_f$

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

*Proof.* For any $\mathfrak{p} \in X$, let $x \in A \setminus \mathfrak{p}$. Then $\mathfrak{p} \notin V(x)$. Hence $\mathfrak{p} \in X_x$

If $\mathfrak{p} \in X_f \cap X_g$, then as $V(f) \cup V(g) = V(fg)$, then $\mathfrak{p} \in X_{fg}$. Hence this form a basis of open sets for the Zariski topology

1. $X_f \cap X_g = V(f)^c \cap V(g)^c = (V(f) \cup V(g))^c = (V(fg))^c = X_{fg}$
2. $X_f = \emptyset$ iff $V(f) = X$ iff $f \in \mathfrak{N}$
3. $X_f = X$ iff $V(f) = \emptyset$. Note that any ideal can be extended to a maximal ideal which is prime, thus $f$ is not contained in any ideal, which means $f$ is a unit
4. $r((f)) \subseteq r((g))$ iff every ideal containing $(g)$ contains $(f)$ iff $V(f) \subseteq V(g)$.
5. A collection $\mathcal{C}$ of closed sets has finite intersection property iff for any finite $V(E_1), \dots, V(E_n) \in \mathcal{C}$, $\bigcap V(E_i) = V(\bigcup E_i) \neq \emptyset$ iff for any finite $V(E_1), \dots, V(E_n) \in \mathcal{C}$, $\bigcup E_i$ doesn't contain a unit. Thus $\bigcup_{\mathcal{C}} V(E_i)$ doesn't contain a unit and hence $\bigcap_{\mathcal{C}} V(E_i) \neq \emptyset$

Let $\{X_f\}_{f\in E}$ be an open cover of $X$. Taking complements shows that $V(E)$ is empty. Therefore $(E) = (1)$. This in turn implies that there are $f_1, \dots, f_n \in E$ and $a_1, \dots, a_n \in A$ s.t. $1 = \sum_{i=1}^n a_i f_i$. Thus $V(f_1, \dots, f_n)$ is empty

6. Suppose an open covering $\{X_g\}_{g\in E}$ of $X_f$, then $\bigcap_{g\in E} V(g) = V(\bigcup_{g\in E} g) = V(E) \subseteq V(f)$, which means that every prime containing $E$ contains $f$, then $f \in r((E))$ (Proposition 1.12). So there are $g_1, \dots, g_n \in E$, $a_1, \dots, a_n \in A$ and a positive integer $m$ s.t. $f^m = \sum_{i=1}^n a_i g_i$. Thus $V(f) \supseteq V(g_1, \dots, g_n)$. Hence $X_f \subseteq \bigcup_{i=1}^n X_{g_i}$
7. For any quasi-compact open sets $U$ of $X$, $U = \bigcup_{f\in E} X_f$. And as it's quasi-compact, there is $E_0 \subseteq_f E$ s.t. $U = \bigcup_{f\in E_0} X_f$

□

*Exercise* 1.1.17. 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 $\mathfrak{p}_x$. Show that

1. the set $\{x\}$ is closed (we say that $x$ is a "closed point") in $\mathrm{Spec}(A)$ iff $\mathfrak{p}_x$ is maximal
2. $\overline{\{x\}} = V(\mathfrak{p}_x)$
3. $y \in \overline{\{x\}}$ iff $\mathfrak{p}_x \subseteq \mathfrak{p}_y$
4. $X$ is a $T_0$-space (this means that if $x, y$ are disjoint points of $X$, then either there is a neighborhood of $x$ which does not contain $y$, or else there is a neighborhood of $y$ which does not contain $x$)

*Proof.* 1. $\{x\}$ is closed iff there is $E \subseteq A$ s.t. $\{x\} = V(E)$ which means $\mathfrak{p}_x$ cannot be expanded anymore

2. $y \in \overline{\{x\}}$ iff $\forall$ open $U \ni y$, $x \in U$ iff $\forall E$ $y \notin V(E)$, $x \notin V(E)$ iff $\forall E$ $x \in V(E) \Rightarrow y \in V(E)$. As $x \in V(x)$, $y \in V(x)$. If $y \in V(x)$, for any $x \in V(E)$, we have $y \in V(x) \subseteq V(E)$
3. $y \in \overline{\{x\}}$ iff $y \in V(x)$ iff $x \subseteq y$
4. If $x \subseteq y$, then $x \notin V(y)$ and $y \in V(y)$. If $x \not\subseteq y$, then $(x) \not\subseteq y$ and so $y \notin V(x)$.

   If every neighborhood of $x$ contains $y$ and vice versa. Then $y \in \overline{\{x\}}$ and $x \in \overline{\{y\}}$. So $x = y$

□

*Exercise* 1.1.18. 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 iff the nilradical of $A$ is a prime ideal

*Proof.* $\mathrm{Spec}(A)$ is irreducible iff for any $V(E)^c, V(F)^c \neq \emptyset$, $V(E)^c \cap V(F)^c = (V(E) \cup V(F))^c = V(EF)^c \neq \emptyset$ iff $V(E), V(F) \neq X \Rightarrow V(EF) \neq X$ iff $V(EF) = X \Rightarrow V(E) = X \vee V(F) = X$.

For any $xy \in \mathfrak{N}$, $x^n y^n = 0$. Thus $V(xy) = X$ and hence either $V(x) = X$ or $V(y) = X$. Thus either $x \in \mathfrak{N}$ or $y \in \mathfrak{N}$.

If $\mathfrak{N}$ is prime and if $V(EF) = X$, then $EF \subseteq \mathfrak{N}$ and either $E \subseteq \mathfrak{N}$ or $F \subseteq \mathfrak{N}$. Note that $V(\mathfrak{N}) = X$ □

*Exercise* 1.1.19. Let $X$ be a topological space

1. If $Y$ is an irreducible subspace of $X$, then the closure $\overline{Y}$ of $Y$ in $X$ is irreducible

2. Every irreducible subspace of $X$ is contained in a maximal irreducible subspace

3. 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?

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

*Proof.*

1. For any open $U, V \subseteq X$, then $U \cap Y \neq \emptyset \wedge V \cap Y \neq \emptyset \Rightarrow U \cap V \cap Y \neq \emptyset$.

   Let $U, V$ be open subsets of $X$ s.t. $U \cap \overline{Y}$ and $V \cap \overline{Y}$ are nonempty. By the definition of closure, $U \cap Y$ and $V \cap Y$ are nonempty and hence $U \cap V \cap Y$ is nonempty, which is a subset of $U \cap V \cap \overline{Y}$

2. If $Y$ is an irreducible subspace of $X$, let $\Sigma$ be the set of irreducible subspaces of $X$ containing $Y$, ordered by inclusion. Let $\{Z_n\}_{n \geq 1}$ be a chain in $\Sigma$ and let $Z = \bigcup_{i=1}^{n} Z_n$. Suppose $U \cap Z \neq \emptyset$ and $V \cap Z \neq \emptyset$. Then there is $i, j$ s.t. $U \cap Z_i \neq \emptyset$ and $V \cap Z_j \neq \emptyset$. So $U \cap V \cap Z_{\max\{i,j\}} \neq \emptyset$. Then by Zorn's Lemma

3. Note that $\{x\}$ is irreducible subspace.

   In Hausdorff space, any subspace with more than one point has disjoint non-empty open sets, and is thus not irreducible

4. Show $V(\mathfrak{p})$ is irreducible and maximal

   For any $E, F \subseteq A$, suppose $V(E)^c \cap V(\mathfrak{p})$ and $V(F)^c \cap V(\mathfrak{p})$ are nonempty, then there is $\mathfrak{p} \subseteq \mathfrak{m} \in V(E)^c \cap V(\mathfrak{p})$ and $\mathfrak{p} \subseteq \mathfrak{n} \in V(F)^c \cap V(\mathfrak{p})$. As $\mathfrak{p}$ is minimal, $\mathfrak{p} \subseteq \mathfrak{m} \cap \mathfrak{n} \in V(E)^c \cap V(F)^c \cap V(\mathfrak{p})$

   If $V(\mathfrak{p})$ is not maximal, then there is $E$ s.t. $V(\mathfrak{p}) \subsetneq V(E)$, which implies that $(E) \subsetneq \mathfrak{p}$, a contradiction

   Given any irreducible components $V(E) = V((E)) = V(\mathfrak{a})$ of $X$. If $\mathfrak{a}$ is not minimal, then there is $\mathfrak{b} \subsetneq \mathfrak{a}$ and $V(\mathfrak{b}) \supseteq V(\mathfrak{a})$. Then $V(\mathfrak{b})$ is an irreducible component

□

*Remark.* Let $X = \text{Spec}(A)$ and $Y \subseteq X$. Note that $Y \subseteq V(\mathfrak{a}) \Leftrightarrow \mathfrak{a} \subseteq \bigcap_{y \in Y} y$. Thus

$$\begin{aligned}
\overline{Y} &= \bigcap \{V(\mathfrak{a}) : Y \subseteq V(\mathfrak{a})\} = \bigcap \left\{ V(\mathfrak{a}) : \mathfrak{a} \subseteq \bigcap_{y \in Y} y \right\} \\
&= V\left( \bigcup \{\mathfrak{a} : \mathfrak{a} \subseteq \bigcap_{y \in Y} y\} \right) = V\left( \bigcap_{y \in Y} y \right)
\end{aligned}$$

*Exercise* 1.1.20. Let $\phi : A \to B$ be a ring homomorphism. Let $X = \text{Spec}(A)$ and $Y = \text{Spec}(B)$. If $\mathfrak{q} \in Y$, then $\phi^{-1}(\mathfrak{q})$ is a prime ideal, i.e., a point of $X$. Hence $\phi$ induces a mapping $\phi^* : Y \to X$. Show that

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

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

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

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

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

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

7. 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 $\phi^*$ is bijection but not a homeomorphism

*Proof.* 1. $\mathfrak{q} \in X_{\phi(f)}$ iff $\mathfrak{q} \notin V(\phi(f))$. $\phi^*(\mathfrak{q}) \in X_f$ iff $\phi^*(\mathfrak{q}) \notin V(f)$ iff $\phi^{-1}(\mathfrak{q}) \notin V(f)$.

If $\phi^{-1}(\mathfrak{q}) \in V(f)$, then $(f) \subseteq \phi^{-1}(\mathfrak{q})$, then $\phi((f)) \subseteq \mathfrak{q}$. Now we show $\phi((f)) = (\phi(f))$. $x \in \phi((f))$ iff $x = \phi(af)$ iff $x = \phi(a)\phi(f)$ iff $x \in (\phi(f))$. Thus $(\phi(f)) \subseteq \mathfrak{q}$ and so $\mathfrak{q} \in V(\phi(f))$.

If $\mathfrak{q} \in V(\phi(f))$, then $(\phi(f)) \subseteq \mathfrak{q}$, $\phi(f) \in \mathfrak{q}$ and so $\phi^{-1}(\phi(f)) \in \phi^{-1}(\mathfrak{q})$.

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

2. $x \in \phi^{*-1}(V(\mathfrak{a}))$ iff $\phi^*(x) \in V(\mathfrak{a})$ iff $\phi^{-1}(x) \in V(\mathfrak{a})$ iff $\mathfrak{a} \subseteq \phi^{-1}(x)$ iff $\phi(\mathfrak{a}) \subseteq x$ iff $\mathfrak{a}^e \subseteq x$ iff $x \in V(\mathfrak{a}^e)$

$$\mathfrak{q} \in \phi^{*-1}(V(\mathfrak{a})) \Leftrightarrow \phi^*(\mathfrak{q}) \in V(\mathfrak{a}) \Leftrightarrow \mathfrak{a} \subseteq \phi^*(\mathfrak{q}) \Leftrightarrow \mathfrak{a}^e \subseteq \mathfrak{q} \Leftrightarrow \mathfrak{q} \in V(\mathfrak{a}^e)$$

3. By remark, $\overline{\phi^*(V(\mathfrak{b}))}$ is the set of prime ideals containing $\bigcap \phi^*(V(\mathfrak{b}))$, which equals

$$\bigcap\{\mathfrak{q}^c : \mathfrak{q} \in V(\mathfrak{b})\} = \bigcap\{\mathfrak{q}^c : \mathfrak{b} \subseteq \mathfrak{q}\} = \left(\bigcap_{\mathfrak{b}\subseteq\mathfrak{q}\in Y} \mathfrak{q}\right)^c = r(\mathfrak{b})^c = r(\mathfrak{b}^c)$$

$$x \in \bigcap_{\mathfrak{q}\in X} \mathfrak{q}^c \Leftrightarrow \forall \mathfrak{q} \in X(x \in \mathfrak{q}^c) \Leftrightarrow \forall \mathfrak{q} \in X(f(x) \in \mathfrak{q})$$

$$\Leftrightarrow f(x) \in \bigcap_{\mathfrak{q}\in X} \mathfrak{q} \Leftrightarrow x \in (\bigcap \mathfrak{q})^c$$

$$x \in r(\mathfrak{b})^c \Leftrightarrow f(x)^n \in \mathfrak{b} \Leftrightarrow f(x^n) \in \mathfrak{b} \Leftrightarrow x^n \in \mathfrak{b}^c \Leftrightarrow x \in r(\mathfrak{b}^c)$$

4. If $\phi : A \to B$ is surjective, then the image of ideal of $A$ is an ideal of $B$. Image of prime ideal. For any $x \in V(\ker(\phi))$, $\phi(x)$ is prime and is its preimage. If $\phi^*(y_1) = \phi^*(y_2)$, then $\phi^{-1}(y_1) = \phi^{-1}(y_2)$. Hence $y_1 = y_2$ as $\phi$ is surjective. Thus $\phi$ is a bijection

For any $Y_f \in Y$

$$\mathfrak{q} \in \phi^*(Y_f) \Leftrightarrow \mathfrak{q} = \phi^*(\mathfrak{p}) \notin \phi^*(f) \Leftrightarrow \phi^{-1}(f) \notin \mathfrak{q} \Leftrightarrow \mathfrak{q} \in X_{\phi^{-1}(x)}$$

So $\phi^*(Y_f) = X_{\phi^{-1}(f)}$

Consider the canonical map $\phi : A \to A/\mathfrak{N}$. Then we have $\mathrm{Spec}(A/\mathfrak{N}) \cong V(\mathfrak{N}) = \mathrm{Spec}(A)$

5. Note that $\phi^*(Y) = V(\ker(\phi))$. Thus

$$\overline{\phi^*(Y)} = V(\bigcap \phi^*(Y)) = V(\bigcap V(\ker(\phi)) = V(r(\ker(\phi))) = V(\ker(\phi))$$

6. For any $\mathfrak{p} \in Z = \mathrm{Spec}(C)$

$$(\psi \circ \phi)^*(\mathfrak{p}) = (\psi \circ \phi)^{-1}(\mathfrak{p}) = \phi^{-1}(\psi^{-1}(\mathfrak{p})) = \phi^* \circ \psi^*(\mathfrak{p})$$

7. $\mathfrak{p}$ is maximal and $A/\mathfrak{p}$ is a field. Thus $B$ has ideal $0 \times 0$, $0 \times K$, $(A/\mathfrak{p}) \times 0$ and $(A/\mathfrak{p}) \times K$

   $A$ has prime ideals $(0)$ and $\mathfrak{p}$. $B$ has prime ideals $0 \times K$ and $(A/\mathfrak{p}) \times 0$. In $\mathrm{Spec}(B) = \{\mathfrak{q}_1, \mathfrak{q}_2\}$, we have $\{\mathfrak{q}_1\} = V(\mathfrak{q}_1)$ is closed as $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$, but $\phi^*(\mathfrak{q}_1)$ is not closed in $\mathrm{Spec}(A)$ as $0$ is not a maximal ideal of $A$

□

*Exercise* 1.1.21. Let $A = \prod_{i=1}^n A_i$ be the direct product of rings $A_i$. Show that $\mathrm{Spec}(A)$ is the disjoint union of open (and closed) subspaces $X_i$, where $X_i$ is canonically homeomorphic with $\mathrm{Spec}(A_i)$

Conversely let $A$ be any ring. Show that TFAE

1. $X = \mathrm{Spec}(A)$ is disconnected

2. $A \cong A_1 \times A_2$ where neither of the rings $A_1, A_2$ is the zero ring

3. $A$ contains an idempotent $\neq 0, 1$

In particular, the spectrum of a local ring is always connected (Exercise 1.1.11)

*Proof.* Let $\pi_i : A \to A_i$ be the canonical projection, and $\mathfrak{b}_i = \prod_{j \neq i} A_j$ its kernel; then by 1.1.20 (4) $\pi_i^*$ is a homeomorphism $\mathrm{Spec}(A_i) \cong V(\mathfrak{b}_i)$. Since $\bigcap_{i=1}^n \mathfrak{b}_i = 0$, it follows that $\bigcup V(\mathfrak{b}_i) = V(\bigcap \mathfrak{b}_i) = V(0) = \mathrm{Spec}(A)$, so that $V(\mathfrak{b}_i)$ cover $\mathrm{Spec}(A)$. Since $\mathfrak{b}_i + \mathfrak{b}_j = A$ for $i \neq j$ and hence $V(\mathfrak{b}_i) \cap V(\mathfrak{b}_j) = V(\mathfrak{b}_i + \mathfrak{b}_j) = V(1) = \emptyset$, it follows that $V(\mathfrak{b}_j)$ are disjoint. Since the complement $\bigcup_{j \neq i} V(\mathfrak{b}_j)$ of each $V(\mathfrak{b}_i)$ is a finite union of closed sets, the $V(\mathfrak{b}_i)$ are also open. (VERY NICE PROOF)

$2 \to 1$ follows as above

$X$ is disconnected iff there is non-zero $\mathfrak{a}$ and $\mathfrak{b}$ s.t. $X = V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a}\mathfrak{b})$ and $\emptyset = V(\mathfrak{a}) \cap V(\mathfrak{b}) = V(\mathfrak{a} \cup \mathfrak{b}) = V(\mathfrak{a} + \mathfrak{b})$. Thus $\mathfrak{a} + \mathfrak{b} = (1)$ and $r(\mathfrak{a}\mathfrak{b}) = \mathfrak{N}$. There are $f \in \mathfrak{a}, g \in \mathfrak{b}, n \in \mathbb{N}_+$ s.t. $f + g = 1$ and $(fg)^n = 0$. Since $(f, g) \subseteq r((f^n, g^n))$ and $V(f, g)$ is not empty, $V(f^n, g^n)$ is not empty. Thus $(f^n) + (g^n) = (1)$.

$1 \to 3$. the Chinese Remainder Theorem implies that $A \to (A/(f^n)) \times (A/(g^n))$ is an isomorphism. Neither of $f, g$ is a unit, because they are elements of the proper ideals $\mathfrak{a}, \mathfrak{b}$

$1 \to 2$. we can find $e \in (f^n)$ s.t. $1 - e \in (g^n)$. We then have $e - e^2 = e(1-e) \in (ab)^n = 0$, so $e = e^2$

$3 \to 2$. Suppose $e \neq 0, 1$ is an idempotent. Then $1 - e$ is also an idempotent $\neq 0, 1$, and neither is a unit. This means $(e)$ and $(1 - e)$ are proper, nonzero ideals, and they are coprime since $e + (1 - e) = 1$. Since $(e)(1 - e) = (e - e^2) = 0$, then $(e) \cap (1 - e) = (0)$. Hence we have an isomorphism $\phi : A \to (A/(e)) \times (A/(1 - e))$. $\square$

*Exercise* 1.1.22. Let $A$ be a Boolean ring and let $X = \text{Spec}(A)$

1. For each $f \in A$ the set $X_f$ is both open and closed in $X$
2. Let $f_1, \dots, f_n \in A$ .Show that $X_{f_1} \cup \cdots \cup X_{f_n} = X_f$ for some $f \in A$
3. The sets $X_f$ are the only subsets of $X$ which are both open and closed
4. $X$ is a compact Hausdorff space

*Proof.*
1. For any $\mathfrak{p} \in X$, $f(1 - f) = 0 \in \mathfrak{p}$ and hence either $f \in \mathfrak{p}$ or $1 - f \in \mathfrak{p}$. Thus $X = X_f \cup X_{1-f}$
2. $x \in X_{f_1} \cup \cdots \cup X_{f_n}$ iff $x \in V(f_1)^c \cup \cdots \cup V(f_n)^c$ iff $x \in (V(f_1) \cap \cdots \cap V(f_n))^c$ iff $x \in (V((f_1, \dots, f_n)))^c$. By Exercise 1.1.10, $(f_1, \dots, f_n) = (g)$ for some $g$. Hence $X_{f_1} \cup \cdots \cup X_{f_n} = X_g$
3. 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 1.1.16), $Y$ is quasi-compact. Hence $Y$ is a finite union of basic open sets and hence equals a basic open sets.
4. For any $\mathfrak{p} \neq \mathfrak{q} \in X$, $\mathfrak{p}$ and $\mathfrak{q}$ are maximal according to Exercise 1.1.10. Hence $\mathfrak{p} \in V(\mathfrak{p})$ and $\mathfrak{q} \notin V(\mathfrak{q})$

$\square$

*Exercise* 1.1.23. Let $L$ be a lattice, where 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

1. $L$ has a least element and a greatest element (denoted by 0,1 respectively)

2. Each of $\vee$, $\wedge$ is distributive over the other

3. Each $a \in L$ has a unique "complement" $a' \in L$ s.t. $a \vee a' = 1$ and $a \wedge a' = 0$

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

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

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 $a = ab$. Show that, w.r.t. this ordering, $A$ is a Boolean lattice. In this way we obtain a one-to-one correspondence between (isomorphism classes of) Boolean rings and (isomorphism classes of) Boolean lattices

*Proof.* De Morgan's laws: $(x \vee y)' = x' \wedge y'$ and $(x \wedge y)' = x' \vee y'$

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

As complement is unique, $x' \wedge y' = (x \vee y)'$

$a + a = (a \wedge a') \vee (a' \wedge a) = a \wedge a' = 0$. Thus $a + a = 0$. $a + b = b + a$.

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

$(ab)c = a(bc)$. $x^2 = x \wedge x = x$

$a \vee b = a + b + ab$, $a \wedge b = ab$. 0 and 1 are minimum and maximum respectively. $a \wedge (b \vee c) = a(b + c + bc) = ab + ac + abc = ab + ac + a^2bc = (ab) \vee (ac)$. As $a + a = 0$, $a \vee a = a + a + a^2 = a$.

$a \vee a' = a + a' + aa' = 1$, $a \wedge a' = aa' = 0$. Hence $a' = 1 - a$. □

*Exercise* 1.1.24. 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

*Proof.* Given a Boolean lattice $L$, define

$$\phi : L \to \mathcal{P}(\text{Spec}(A(L))) : f \mapsto X_f$$

if $f \leq g$, then $f = fg$ and so $X_f \cap X_g = X_{fg} = X_f$, which yields $X_f \subseteq X_g$.

If $X_f = X_g$, then as $1 + g = g'$, then $g \in \mathfrak{p}$ iff $g' \notin \mathfrak{p}$

$$X_f = X_g = X^c_{(1+g)}$$

So $X_f \cap X_{(1+g)} = X_{f(1+g)}$ is empty. Therefore $f(1+g)$ is nilpotent. Then $f^n(1+g)^n = f^{n-1}(1+g)^{n-1} = \cdots = f(1+g) = 0$. In particular $f = -fg = fg$. So $f \leq g$.

On the other hand, the image of $\phi$ is precisely the class of open-and-closed subspaces of the compact Hausdorff space $\square$

*Exercise* 1.1.25. Let $A$ be a ring. The subspace of Spec$(A)$ consisting of the *maximal* ideals of $A$, with the induced topology, is called the **maximal spectrum** of $A$ is denoted by Max$(A)$. For arbitrary commutative rings it does not have the nice functorial properties of Spec$(A)$ (Exercise 1.1.20), because the inverse image of a maximal ideal under a ring homomorphism need not be maximal (consider $i : \mathbb{Z} \to \mathbb{Q}$, as $\mathbb{Q}$ is a field, its maximal ideal is $(0)$, which is not a maximal ideal in $\mathbb{Z}$)

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 $f \in C(X)$ s.t. $f(x)$. The ideal $\mathfrak{m}_x$ is maximal, because it is the kernel of the (surjective) homomorphism $C(X) \to \mathbb{R}$ which takes $f$ to $f(x)$. If $\tilde{X}$ denotes Max$(C(X))$, we have therefore defined a mapping $\mu : X \to \tilde{X}$, namely $x \mapsto \mathfrak{m}_x$

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

1. 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 $f_x \in \mathfrak{m}$ s.t. $f_x(x) \neq 0$. Since $f_x$ is continuous, there is an open neighborhood $U_x$ of $x$ in $X$ on which $f_x$ does not vanish. By compactness a finite number of the neighborhoods, say $U_{x_1}, \ldots, U_{x_n}$, cover $X$. Let

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

   Then $f$ does not vanish at any point of $X$, hence is a unit in $C(X)$. But this contradicts $f \in \mathfrak{m}$, hence $V$ is not empty

   Let $x \in V$. Then $\mathfrak{m} \subseteq \mathfrak{m}_x$, hence $\mathfrak{m} = \mathfrak{m}_x$ because $\mathfrak{m}$ is maximal. Hence $\mu$ is surjective

2. By Urysohn's lemma, the continuous functions separate the points of $X$. Hence $x \neq y \Rightarrow \mathfrak{m}_x \neq \mathfrak{m}_y$, and therefore $\mu$ is injective

3. 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 set $U_f$ (resp. $\tilde{U}_f$) form a basis of the topology of $X$ (resp. $\tilde{X}$) and therefore $\mu$ is a homeomorphism

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

*Affine algebraic variesties*

*Exercise* 1.1.26. Let $k$ be an algebraic 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 $x = (x_1, \dots, x_n) \in k^n$ which satisfy these equations is an **affine algebraic variety**

Consider the set of all polynomials $g \in k[t_1, \dots, t_n]$ 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

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

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

Let $\xi_i$ be the image of $t_i$ in $P(X)$. The $\xi_i$ $(1 \leq i \leq n)$ are the **coordinate functions** on $X$: if $x \in X$, then $\xi_i(x)$ is the $i$th 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

# 2 Modules

### Modules and Module Homomorphisms

Let $A$ be a ring (commutative, as always). An $A$**-module** is an abelian group $M$ (written additively) on which $A$ acts linearly: more precisely, it is a pair $(M, \mu)$, where $M$ is an abelian group and $\mu$ is a mapping of $A \times M$ into $M$, s.t., if we write $ax$ for $\mu(a, x)$, the following axioms are satisfied for $a, b \in A$ and $x, y \in M$

$$\begin{aligned} a(x+y) &= ax + ay \\ (a+b)x &= ax + bx \\ (ab)x &= a(bx) \\ 1x &= x \end{aligned}$$

Equivalently, $M$ is an abelian group together with a ring homomorphism $A \to E(M)$, where $E(M)$ is a ring of endomorphisms of the abelian group $M$

**Example 2.1.**

1. An ideal $\mathfrak{a}$ of $A$ is an $A$-module. In particular $A$ itself is an $A$-module
2. If $A$ is a field $k$, then $A$-module = $k$-vector space
3. $A = \mathbb{Z}$, then $\mathbb{Z}$-module = abelian group (define $nx$ to $x + \cdots + x$)
4. $A = k[x]$ where $k$ is a field; an $A$-module is a $k$-vector space with a linear transformation.
5. $G$=finite group, $A = k[G]$=group-algebra of $G$ over the field $k$ (thus $A$ is not commutative, unless $G$ is). Then $A$-module=$k$-representation of $G$

Let $M, N$ be $A$-modules. A mapping $f : M \to N$ is an $A$**-module homomorphism** (or is $A$**-linear**) if

$$\begin{aligned} f(x+y) &= f(x) + f(y) \\ f(ax) &= a \cdot f(x) \end{aligned}$$

for all $a \in A$ and all $x, y \in M$. Thus $f$ is a homomorphism of abelian groups which commutes with the action of each $a \in A$. If $A$ is a field, an $A$-module homomorphism is the same thing as a linear transformation of vector space

The composition of $A$-module homomorphism is again an $A$-homomorphism

The set of all $A$-module homomorphism from $M$ to $N$ can be turned into an $A$-module as follows: we define $f + g$ and $af$ by the rules

$$\begin{aligned} (f+g)(x) &= f(x) + g(x) \\ (af)(x) &= a \cdot f(x) \end{aligned}$$

for all $x \in M$. This $A$-module is denoted by $\mathrm{Hom}_A(M, N)$

Homomorphisms $u : M' \to M$ and $v : N \to N''$ induces mappings

$$\bar{u} : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N) \quad \text{and} \quad \bar{v} : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N'')$$

defined as follows

$$\bar{u}(f) = f \circ u, \quad \bar{v}(f) = v \circ f$$

For any module $M$ there is a natural isomorphism $\mathrm{Hom}(A, M) \cong M$: any $A$-module homomorphism $f : A \to M$ is uniquely determined by $f(1)$, which can be any element of $M$

### Submodules and Quotient Modules

A **submodule** $M'$ of $M$ is a subgroup of $M$ which is closed under multiplication by elements of $A$. Then abelian group $M/M'$ then inherits an $A$-module structure from $M$, defined by $a(x + M') = ax + M'$. The $A$-module $M/M'$ is the **quotient** of $M$ by $M'$. There is a one-to-one order-preserving correspondence between submodules of $M$ which contain $M'$, and submodules $M'' = M/M'$

If $f : M \to N$ is an $A$-module homomorphism, the **kernel** of $f$ is the set

$$\ker(f) = \{x \in M : f(x) = 0\}$$

and is a submodule of $M$. The **image** of $f$ is the set

$$\mathrm{im}(f) = f(M)$$

and is a submodule of $N$. The **cokernel** of $f$ is

$$\mathrm{coker}(f) = N/\mathrm{im}(f)$$

which is a quotient module of $N$.

If $M'$ is a submodule of $M$ s.t. $M' \subseteq \ker(f)$, then $f$ give rise to a homomorphism $\bar{f} : M/M' \to N$ defined as follows: if $\bar{x} \in M/M'$ is the image of $x \in M$, then $\bar{f}(\bar{x}) = f(x)$. The kernel of $\bar{f}$ is $\ker(f)/M'$

### Operations on Submodules

Let $M$ be an $A$-module and let $(M_i)_{i \in I}$ be a family of submodules of $M$. Their **sum** $\sum M_i$ is the set of all (finite) sums $\sum x_i$, where $x_i \in M_i$ for all $i \in I$, and almost all the $x_i$ are zero. $\sum M_i$ is the smallest submodule of $M$ which contains all the $M_i$

The intersection $\bigcap M_i$ is again a submodule of $M$. Thus the submodules of $M$ form a complete lattice w.r.t. inclusion

**Proposition 2.1.** *1. If $L \supseteq M \supseteq N$ are $A$-modules, then*

$$(L/N)/(M/N) \cong L/M$$

*2. If $M_1, M_2$ are submodules of $M$, then*

$$(M_1 + M_2)/M_1 \cong M_2/(M_1 \cap M_2)$$

*Proof.* 1. Define $\theta : L/N \to L/M$ by $\theta(x+N) = x+M$. Then $\theta$ is a well-defined $A$-module homomorphism of $L/N$ onto $L/M$, and its kernel is $M/N$;

2. The composite homomorphism $M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1$ is surjective, and its kernel is $M_1 \cap M_2$

□

We cannot in general define the **product** of two submodules, but we can define the product $\mathfrak{a}M$ where $\mathfrak{a}$ is an ideal and $M$ an $A$-module; it is the set of all finite sums $\sum a_i x_i$ with $a_i \in \mathfrak{a}$, $x_i \in M$ and is a submodule of $M$

If $N, P$ are submodule of $M$, we define $(N : P)$ to be the set of all $a \in A$ s.t. $aP \subseteq N$; it is an **ideal** of $A$. In particular, $(0 : M)$ is the set of all $a \in A$ s.t. $aM = 0$; this ideal is called the **annihilator** of $M$ and is also denoted by $\text{Ann}(M)$. If $\mathfrak{a} \subseteq \text{Ann}(M)$, we may regard $M$ as an $A/\mathfrak{a}$-module as follows: if $\bar{x} \in A/\mathfrak{a}$ is represented by $x \in A$, define $\bar{x}m$ to be $xm$

An $A$-module is **faithful** if $\text{Ann}(M) = 0$. If $\text{Ann}(M) = \mathfrak{a}$, then $M$ is faithful as an $A/\mathfrak{a}$-module

*Exercise* 2.0.1. 1. $\text{Ann}(M + N) = \text{Ann}(M) \cap \text{Ann}(N)$

2. $(N : P) = \text{Ann}((N + P)/N)$

*Proof.* 2. $a((N + P)/N) = 0$ iff $a(N + P) \subseteq N$ iff $aP \subseteq N$

□

If $x \in M$, the set of all multiples $ax$ $(a \in A)$ is a submodule of $M$, denoted by $Ax$ or $x$. If $M = \sum_{i \in I} Ax_i$, the $x_i$ are said to be a **set of generators** of $M$. An $A$-module is said to be **finitely generated** if it has a finite set of generators

### Direct Sum and Product

If $M, N$ are $A$-modules, their **direct sum** $M \oplus N$ is the set of all pairs $(x, y)$ with $x \in M$, $y \in N$. This is an $A$-module if we define addition and scalar multiplication in the obvious way:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$
$$a(x, y) = (ax, ay)$$

More generally, if $(M_i)_{i \in I}$ is any family of $A$-modules, we can define their **direct sum** $\bigoplus_{i \in I} M_i$; its elements are families $(x_i)_{i \in I}$ s.t. $x_i \in M_i$ for each $i \in I$ and almost all $x_i$ are 0. If we drop the restriction on the number of non-zero $x$'s we have the **direct product** $\prod_{i \in I M_i}$.

Suppose that the ring $A$ is a direct product $\prod_{i=1}^{n} A_i$. Then the set of all elements of $A$ of the form

$$(0, \dots, 0, a_i, 0, \dots, 0)$$

with $a_i \in A_i$ is an **ideal** $\mathfrak{a}_i$ of $A$. The ring $A$, considered as an $A$-module, is the direct sum of the ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n$. Conversely, given a module decomposition

$$A = \mathfrak{a}_1 \oplus \cdots \oplus \mathfrak{a}_n$$

of $A$ as a direct sum of ideals, we have

$$A \cong \prod_{i=1}^{n} (A/\mathfrak{b}_i)$$

where $\mathfrak{b}_i = \oplus_{j \neq i} \mathfrak{a}_j$. Each ideal $\mathfrak{a}_i$ is a ring (isomorphic to $A/\mathfrak{b}_i$). The identity element $e_i$ of $\mathfrak{a}_i$ is an idempotent in $A$, and $\mathfrak{a}_i = (e_i)$

### Finitely Generated Modules

A **free** $A$-module is one which is isomorphic to an $A$-module of the form $\bigoplus_{i \in I} M_i$, where each $M_i \cong A$ (as an $A$-module). The notation $A^{(I)}$ is sometimes used. A finite generated free $A$-module is therefore isomorphic to $A \oplus \cdots \oplus A$ ($n$ summands), which is denoted by $A^n$. (Conventionally, $A^0$ is the zero module, denoted by 0)

**Proposition 2.2.** *$M$ is a finitely generated $A$-module iff $M$ is isomorphic a quotient of $A^n$ for some integer $n > 0$*

*Proof.* $\Rightarrow$. Let $x_1, \dots, x_n$ generate $M$. Define $\phi : A^n \to M$ by $\phi(a_1, \dots, a_n) = a_1x_1 + \dots + a_nx_n$. Then $\phi$ is an $A$-module homomorphism onto $M$, and therefore $M \cong A^n / \ker(\phi)$

$\Leftarrow$. We have an $A$-module homomorphism $\phi$ of $A^n$ onto $M$. If $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ (the 1 being in the $i$th place), then the $e_i$ generate $A^n$, hence the $\phi(e_i)$ generate $M$ $\square$

**Proposition 2.3.** *Let $M$ be a finitely generated $A$-module, let $\mathfrak{a}$ be an ideal of $A$, and let $\phi$ be an $A$-module endomorphism of $M$ s.t. $\phi(M) \subseteq \mathfrak{a}M$ and let $\psi : A \to \mathrm{End}_A(M)$ be the natural morphism. Then $\phi$ satisfies an equation of the form*

$$\phi^n + \psi(a_1)\phi^{n-1} + \dots + \psi(a_n) = 0$$

*where the $a_i \in \mathfrak{a}$.*

*Proof.* Let $x_1, \dots, x_n$ be a set of generators of $M$. Then each $\phi(x_i) \in \mathfrak{a}M$, so that we have to say $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ ($1 \le i \le n; a_{ij} \in \mathfrak{a}$), i.e.,

$$\sum_{j=1}^n (\delta_{ij}\phi - a_{ij})x_j = 0$$

where $\delta_{ij}$ is the Kronecker delta. By multiplying on the left by the adjoint of the matrix $(\delta_{ij}\phi - a_{ij})$ it follows that $\det(\delta_{ij}\phi - a_{ij})$ annihilates each $x_i$, hence is the zero endomorphism of $M$. Expanding out the determinant, we have an equation of the required form

Explanation Consider the commutative ring $R = A[\phi] \subset \mathrm{End}_A(M)$ generated by $\phi$; then $R$ acts on $M$, and thus $M_n(R)$ acts $M^n$. The equations

$$\phi(x_j) = \sum_{i=1}^n a_{ij}x_i$$

for $j = 1, \dots, n$ can be reinterpreted with the action of $M_n(R)$ on $M^n$: write

$$B = \begin{pmatrix} a_{11} - \phi & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} - \phi & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} - \phi & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \in M_n(R) \quad \text{and} \quad X = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \in M^n$$

Then the $n$ equations we wrote are equivalent to

$$BX = 0$$

Since $R$ is commutative, we have

$$\text{Adj}(B) \times B = \det(B) I_n = B \times \text{Adj}(B)$$

which is an equation which holds in $M_n(R)$ (NEED TO VERIFY). If we multiply the previous equation on the left by $\text{Adj}(B)$, we get

$$0 = \text{Adj}(B)BX = \begin{pmatrix} \det(B) & & & \\ & \det(B) & & \\ & & \ddots & \\ & & & \det(B) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \det(B)x_1 \\ \det(B)x_2 \\ \vdots \\ \det(B)x_n \end{pmatrix}$$

Since the $x_i$ generate $M$, this is equivalent to say that $\det(B)$, which is an element of $R$, hence an endomorphism of $M$, **is the zero endomorphism of** $M$.

The determinant $\det(B) \in R \subset \text{End}_A(M)$ can be calculated by the standard formula

$$\det(B) = \sum_{\sigma \in \mathfrak{S}_n} (-1)^\sigma \prod_{j=1}^{n} B_{\sigma(j),j}$$

which is polynomial in $\phi$ of degree $n$ with coefficients in the ideal $\mathfrak{a}$. The coefficient in front of $\phi^n$ is $(-1)^n$ and since $\det(B) = 0$, we get

$$\phi^n + a_1\phi^{n-1} + \cdots + a_{n-1}\phi + a_n id_M = 0$$

□

**Corollary 2.4.** *Let $M$ be a finitely generated $A$-module and let $\mathfrak{a}$ be an ideal of $A$ s.t. $\mathfrak{a}M = M$. Then there exists $x \equiv 1 \mod \mathfrak{a}$ s.t. $xM = 0$*

*Proof.* Take $\phi = \text{id}$, then $1 + a_1 + \cdots + a_n = 0 \in \text{End}_A(M)$. Let $x = 1 + a_1 + \cdots + a_n \in \mathfrak{a}$ by 2.3 □

**Proposition 2.5** (Nakayama's lemma)**.** *Let $M$ be a finitely generated $A$-module and $\mathfrak{a}$ an ideal of $A$ contained in the Jacobson radical $\mathfrak{R}$ of $A$. Then $\mathfrak{a}M = M$ implies $M = 0$*

*First Proof.* By 2.4 we have $xM = 0$ for some $x \equiv 1 \mod \mathfrak{R}$. By 1.9 $x$ is a unit in $A$, hence $M = x^{-1}xM = 0$ □

*Second Proof.* Suppose $M \neq 0$, and let $u_1, \ldots, u_n$ be a minimal set of generators of $M$. Then $u_n \in \mathfrak{a}M$ hence we have an equation of the form $u_n = a_1u_1 + \cdots + a_nu_n$ with the $a_i \in \mathfrak{a}$. Hence

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1}$$

Since $a_n \in \mathfrak{R}$, it follows from 1.9 that $1 - a_n$ is a unit in $A$. Hence $u_n$ belongs to the submodule of $M$ generated by $u_1, \dots, u_{n-1}$, a contradiction $\square$

**Corollary 2.6.** *Let $M$ be a finitely generated $A$-module, $N$ is a submodule of $M$, $\mathfrak{a} \subseteq \mathfrak{R}$ an ideal. Then $M = \mathfrak{a}M + N \Rightarrow M = N$*

*Proof.* Apply 2.5 to $M/N$, observing that $\mathfrak{a}(M/N) = \mathfrak{a}M/N = (\mathfrak{a}M + N)/N$. Thus $M/N = \mathfrak{a}(M/N)$ and thus $M/N = 0$. $\square$

Let $A$ be a local ring, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field. Let $M$ be a finitely generated $A$-module. $M/\mathfrak{m}M$ is annihilated by $\mathfrak{m}$, hence is naturally an $A/\mathfrak{m}$-module, i.e., a $k$-vector space, and as such is finite-dimensional

**Proposition 2.7.** *Let $x_i$ $(1 \leq i \leq n)$ be elements of $M$ whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then the $x_i$ generate $M$*

*Proof.* Let $N$ be the submodule of $M$ generated by the $x_i$. Then the composite map $N \to M \to M/\mathfrak{m}M$ maps $N$ onto $M/\mathfrak{m}M$, hence $N + \mathfrak{m}M = M$, hence $N = M$ by 2.6 $\square$

If $A = C/B$, then $A + B = C$

### Exact Sequences

A sequence of $A$-modules and $A$-homomorphisms

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

is said to be **exact at** $M_i$ if $\operatorname{im}(f_i) = \ker(f_{i+1})$. The sequence is **exact** if it is exact at each $M_i$. In particular

1. $0 \to M' \xrightarrow{f} M$ is exact $\Leftrightarrow$ $f$ is injective

2. $M \xrightarrow{g} M'' \to 0$ is exact $\Leftrightarrow$ $g$ is surjective

3. $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact $\Leftrightarrow$ $f$ is injective, $g$ is surjective and $g$ induces an isomorphism of $\operatorname{coker}(f) = M/f(M')$ onto $M''$. $M'' \cong M/\ker(g) = M/\operatorname{im}(f)$

A sequence of type 3 is called a **short exact sequence**. Any long exact sequence can be split up into short exact sequences: if $N_i = \operatorname{im}(f_i) = \ker(f_{i+1})$, we have short exact sequences $0 \to N_i \to M_i \to N_{i+1} \to 0$ for each $i$

**Proposition 2.8.** 1. *Let*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \longrightarrow 0$$

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

$$0 \longrightarrow \mathrm{Hom}(M'', N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N) \xrightarrow{\bar{u}} \mathrm{Hom}(M', N)$$

*is exact*

2. *Let*

$$0 \longrightarrow N' \xrightarrow{u} N \xrightarrow{v} N''$$

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

$$0 \longrightarrow \mathrm{Hom}(M, N') \xrightarrow{\bar{u}} \mathrm{Hom}(M, N) \xrightarrow{\bar{v}} \mathrm{Hom}(M, N'')$$

*Proof.*

$$\begin{tikzcd}
M' \arrow[r, "u"] \arrow[drr] & M \arrow[rr, "v"] \arrow[dr] & & M'' \arrow[r] \arrow[dl] & 0 \arrow[dll] \\
& & N & &
\end{tikzcd}$$

Need to modify a bit ☐

**Proposition 2.9.** *Let*

$$\begin{tikzcd}
0 \arrow[r] & M' \arrow[r, "u"] \arrow[d, "f'"'] & M \arrow[r, "v"] \arrow[d, "f"'] & M'' \arrow[r] \arrow[d, "f''"] & 0 \\
0 \arrow[r] & N' \arrow[r, "u'"'] & N \arrow[r, "v'"'] & N'' \arrow[r] & 0
\end{tikzcd}$$

*be a commutative diagram of A-modules and homomorphisms, with the rows exact. Then there exists an exact sequence*

$$0 \longrightarrow \ker(f') \xrightarrow{\bar{u}} \ker(f) \xrightarrow{\bar{v}} \ker(f'') \xrightarrow{d}$$

$$\mathrm{coker}(f') \xrightarrow{\bar{u}'} \mathrm{coker}(f) \xrightarrow{\bar{v}'} \mathrm{coker}(f'') \longrightarrow 0$$

*Proof.* $\bar{u} = u \restriction \ker(f')$. For any $m \in \ker(f')$, $f(\bar{u}(m)) = fu(m) = u'f'(m) = 0$. Thus $\bar{u}(m) \in \ker(f)$. $\bar{u}$ is injective as $u$ is.

$\bar{v} = v \restriction \ker(f)$. For any $m \in \operatorname{im}(\bar{u}) = u(\ker(f'))$, $\operatorname{im}(u) = \ker(v)$. $\ker(\bar{v}) = \ker(f) \cap \ker(v)$. $\operatorname{im}(\bar{u}) = u(\ker(f'))$. $x \in \ker(\bar{v}) \Leftrightarrow x \in \ker(v) \cap \ker(f) \Leftrightarrow x \in \operatorname{im}(u) \cap \ker(f) \Leftrightarrow x \in \operatorname{im}(\bar{u})$

The **boundary homomorphism** $d$ is defined as follows: if $x'' \in \ker(f'')$, we have $x'' = v(x)$ for some $x \in M$ and $v'(f(x)) = f''(v(x))$, hence $f(x) \in \ker(v') = \operatorname{im}(u')$, so that $f(x) = u'(y')$ for some $y' \in N'$. Then $d(x'')$ is defined to be the image of $y'$ in $\operatorname{coker}(f')$.

Suppose there is $x_1, x_2$ s.t. $x'' = v(x_1) = v(x_2)$. Then $f(x_1) = u'(y_1')$ and $f(x_2) = u'(y_2')$.

$$\begin{aligned}
y_1' + \operatorname{im}(f') = y_2' + \operatorname{im}(f') &\Leftrightarrow \exists x_0' \in M' \; y_1' - y_2' = f(x_0') \\
&\Leftrightarrow \exists x_0' \in M' \; u'^{-1}(f(x_1)) - u'^{-1}f(x_2) = f'(x_0') \\
&\Leftrightarrow \exists x_0' \in M' \; f(x_1 - x_2) = u'f'(x_0') = fu(x_0') \\
&\Leftrightarrow \exists x_0' \in M' \; f(x_1 - x_2 - u(x_0')) = 0 \\
&\Leftrightarrow \exists y \in \operatorname{im}(u) = \ker(v) \; x_1 - x_2 - y \in \ker(f)
\end{aligned}$$

But as $x_1 - x_2 \in \ker(v)$, we can simply take $y = x_1 - x_2$

Define $\bar{u}'$ as $x' + \operatorname{im}(f') \mapsto u'(x') + \operatorname{im}(f)$. For any $x'' \in M''$, then $x'' = v(x)$. Suppose $f(x) = u'(y')$. Then $\bar{u}'(y' + \operatorname{im}(f')) = u'(y') + \operatorname{im}(f) = f(x) + \operatorname{im}(f) = \operatorname{im}(f)$. Hence $\operatorname{im}(d) = \ker(\bar{u}')$. $\square$

$$\begin{tikzcd}
0 \arrow[r] & \ker f \arrow[r] & \ker a \arrow[r] \arrow[d] & \ker b \arrow[r] \arrow[d] & \ker c \arrow[d] \arrow[dddll, bend left, "d"] & & \\
& & A \arrow[r, "f"] \arrow[d, "a"] & B \arrow[r, "g"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 & \\
& 0 \arrow[r] & A' \arrow[r, "f'"'] \arrow[d] & B' \arrow[r, "g'"'] \arrow[d] & C' \arrow[d] & & \\
& & \operatorname{coker} a \arrow[r] & \operatorname{coker} b \arrow[r] & \operatorname{coker} c \arrow[r] & \operatorname{coker} g' \arrow[r] & 0
\end{tikzcd}$$

Let $C$ be a class of $A$-modules and let $\lambda$ be a function on $C$ with values in $\mathbb{Z}$ (or, more generally, with values in an abelian group $G$). The function $\lambda$ is **additive** if, for each short exact sequence in which all the terms belongs to $C$, we have $\lambda(M') - \lambda(M) + \lambda(M'') = 0$

**Example 2.2.** Let $A$ be a field $k$, and let $C$ be the class of all finite-dimensional $k$-vector spaces $V$. Then $V \mapsto \dim V$ is an additive function on $V$

**Proposition 2.10.** *Let $0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$ be an exact sequence of $A$-modules where all the modules $M_i$ and the kernels of all the homomorphisms belong to $C$. Then for any additive function $\lambda$ on $C$ we have*

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0$$

*Proof.* Split up the sequence into short exact sequences

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

$(N_0 = N_{n+1} = 0$ and $\lambda(M_0) = \lambda(M_n) = 2\lambda(0))$. Then we have $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. $\square$

### Tensor Product of Modules

Let $M, N, P$ be three $A$-modules. A mapping $f : M \times N \to P$ is said to be $A$-**bilinear** if for each $x \in M$ the mapping $y \mapsto f(x, y)$ of $N$ into $P$ is $A$-linear, and for each $y \in N$ the mapping $x \mapsto f(x, y)$ of $M$ into $P$ is $A$-linear

We shall construct an $A$-module $T$, called the **tensor product** of $M$ and $N$, with the property that the $A$-bilinear mappings $M \times N \to P$ are in a natural one-to-one correspondence with the $A$-linear mappings $T \to P$, for all $A$-modules $P$. More precisely:

**Proposition 2.11.** *Let $M, N$ be $A$-modules. Then there exists a pair $(T, g)$ consisting of an $A$-module $T$ and an $A$-bilinear mapping $g : M \times N \to T$, with the following property:*

*Given any $A$-module $P$ and any $A$-bilinear mapping $f : M \times N \to P$, there exists a unique $A$-linear mapping $f' : T \to P$ s.t. $f = f' \circ g$*

*Moreover, if $(T, g)$ and $(T', g')$ are two pairs with this property, then there is a unique isomorphism $j : T \to T'$ s.t. $j \circ g = g'$*

*Proof.*

1. Uniqueness. Replacing $(P, f)$ by $(T', g')$ we get a unique $j : T \to T'$ s.t. $g' = j \circ g$.

2. Existence. Let $C$ denote the free $A$-module $A^{(M \times N)}$. The elements of $C$ are formal linear combinations of elements of $M \times N$ with coefficients in $A$, i.e., they are expressions of the form $\sum_{i=1}^{n} a_i \cdot (x_i, y_i)$ $(a_i \in A, x_i \in M, y_i \in N)$ here $(x_i, y_i) = (0, \dots, 0, 1, 0, \dots, 0)$ where $(x_i, y_i)$th position is not 0 i think. And direct sum only admits finite sum

Let $D$ be the submodule of $C$ generated by all elements of $C$ of the following types:

$$(x+x',y)-(x,y)-(x',y)$$
$$(x,y+y')-(x,y)-(x,y')$$
$$(ax,y)-a\cdot(x,y)$$
$$(x,ay)-a\cdot(x,y)$$

Let $T=C/D$. For each basis element $(x,y)$ of $C$, let $x\otimes y$ denote its image in $T$. Then $T$ is generated by the elements of the form $x\otimes y$ and from our definition we have

$$(x+x')\otimes y=x\otimes y+x'\otimes y,\quad x\otimes(y+y')=x\otimes y+x\otimes y'$$
$$(ax)\otimes y=x\otimes(ay)=a(x\otimes y)$$

Equivalently, the mapping $g:M\times N\to T$ defined by $g(x,y)=x\otimes y$ is $A$-bilinear

Any map $f$ of $M\times N$ into an $A$-module $P$ extends by linearity to an $A$-module homomorphism $\bar{f}:C\to P$ $\bar{f}(\sum_{i=1}^{n}a_i\cdot(x_i,y_i))=\sum_{i=1}^{n}a_i\cdot f(x_i,y_i)$ Suppose in particular that $f$ is $A$-bilinear. Then, from the definitions, $\bar{f}$ vanishes on all the generators of $D$, hence on the whole of $D$, and therefore induces a well-defined $A$-homomorphism $f'$ of $T=C/D$ into $P$ s.t. $f'(x\otimes y)=f(x,y)$

□

*Remark.* 1. The module $T$ constructed above is called the **tensor product** of $M$ and $N$, and is denoted by $M\otimes_A N$. It is generated as an $A$-module by the "products" $x\otimes y$. If $(x_i)_{i\in I},(y_i)_{j\in J}$ are families of generators of $M,N$ respectively, then the elements $x_i\otimes y_j$ generated $M\otimes N$

2. The notation $x\otimes y$ is inherently ambiguous unless we specify the tensor product to which it belongs. Let $M',N'$ be submodules of $M,N$ respectively, and let $x\in M'$ and $y\in N'$. Then it can happen that $x\otimes y$ as an element of $M\otimes N$ is zero whilst $x\otimes y$ as an element of $M'\otimes N'$ is non-zero. For example, take $A=\mathbb{Z},M=\mathbb{Z},N=\mathbb{Z}/2\mathbb{Z}$, and let $M'$ be the submodule $2\mathbb{Z}$ of $\mathbb{Z}$, whilst $N'=N$. Let $x$ be the non-zero element of $N$ and consider $2\otimes x$. As an element of $M\otimes N$, it is zero because $2\otimes x=1\otimes 2x=1\otimes 0=0$. But as an element of $M'\otimes N'$ it is not zero

**Corollary 2.12.** *Let $x_i\in M$, $y_i\in N$ be s.t. $\sum x_i\otimes y_i=0$ in $M\otimes N$. Then there exist finitely generated submodules $M_0$ of $M$ and $N_0$ of $N$ s.t. $\sum x_i\otimes y_i=0$ in $M_0\otimes N_0$*

*Proof.* If $\sum x_i \otimes y_i = 0$, then $\sum(x_i, y_i) \in D$ and therefore $\sum(x_i, y_i)$ is a finite sum of generators of $D$. Let $M_0$ be the submodule of $M$ generated by the $x_i$ and all the elements of $M$ which occur as first coordinates in these generators of $D$, and define $N_0$ similarly. Then $\sum x_i \otimes y_i = 0$ as an element of $M_0 \otimes N_0$ □

*Remark.*

3. We shall never again need to use the construction of the tensor product given in 2.11. What is essential to keep in mind is the defining property of the tensor product

4. Instead of starting with bilinear mappings we could have started with multilinear mappings $f : M_1 \times \cdots \times M_r \to P$ defined in the same way.

**Proposition 2.13.** *Let $M_1, \dots, M_r$ be A-modules. Then there is a pair $(T, g)$ consisting of an A-module $T$ and an A-multilinear mapping $g : M_1 \times \cdots \times M_r \to T$ with the following property:*

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

*Moreover, if $(T, g)$ and $(T', g')$ are two pairs with this property, then there exists a unique isomorphism $j : T \to T'$ s.t. $j \circ g = g'$*

**Proposition 2.14.** *Let $M, N, P$ be A-modules. Then there exist unique isomorphisms*

1. $M \otimes N \to N \otimes M$
2. $(M \otimes N) \otimes P \to M \otimes (N \otimes P) \to M \otimes N \otimes P$
3. $(M \oplus N) \otimes P \to (M \otimes P) \oplus (N \otimes P)$
4. $A \otimes M \to M$

*s.t., respectively*

1. $x \otimes y \mapsto y \otimes x$
2. $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \to x \otimes y \otimes z$
3. $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$
4. $a \otimes x \mapsto ax$

*Proof.*

1. commute

$$\begin{array}{ccccc} M \otimes N & \dashrightarrow & N \otimes M & \dashrightarrow & M \otimes N \\ \uparrow & & \uparrow & & \uparrow \\ M \times N & \longrightarrow & N \times M & \longrightarrow & M \times N \end{array}$$

2. We shall construct homomorphisms

$$(M \otimes N) \otimes P \xrightarrow{f} M \otimes N \otimes P \xrightarrow{g} (M \otimes N) \otimes P$$

s.t. $f((x \otimes y) \otimes z) = x \otimes y \otimes z$ and $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$ for all $x \in M, y \in N, z \in P$

To construct $f$, fix the element $z \in P$. The mapping $(x, y) \mapsto x \otimes y \otimes z$ is bilinear and therefore induces a homomorphism $f_z : M \otimes N \to M \otimes N \otimes P$. Next consider the mapping $(t, z) \mapsto f_z(t)$ of $(M \otimes N) \times P$ into $M \otimes N \otimes P$. This is bilinear in $t$ and $z$ and therefore induces a homomorphism

$$f : (M \otimes N) \otimes P \to M \otimes N \otimes P$$

s.t. $f((x \otimes y) \otimes z) = x \otimes y \otimes z$

To construct $g$, consider the mapping $(x, y, z) \mapsto (x \otimes y) \otimes z$ of $M \times N \times P$ into $(M \otimes N) \otimes P$. This is linear in each variable and therefore induces a homomorphism

$$g : M \otimes N \otimes P \to (M \otimes N) \otimes P$$

s.t. $g(x \otimes y \otimes z) = (x \otimes y) \otimes z$

Clearly $f \circ g$ and $g \circ f$ are identity, hence $f$ and $g$ are isomorphisms

3. Show For any $p \in P$, $f(m, n, ap) = af(m, n, p)$. For any $(m, n) \in M \times N$, $f(am, an, p) = af(m, n, p)$.

Define

$$g_1 : M \otimes P \to (M \oplus N) \otimes P$$

as $g_1(m \otimes p) = (m, 0) \otimes p$

4. Let $f : a \otimes m \mapsto am$ and $g : m \mapsto 1 \otimes m$. Then $gf(a \otimes m) = g(am) = 1 \otimes am = a \otimes m$ and $fg(m) = f(1 \otimes m) = m$. Hence we get an isomorphism

$\square$

*Exercise* 2.0.2. Let $A, B$ be rings, let $M$ be an $A$-module, $P$ a $B$-module and $N$ an $(A, B)$-bimodule (that is, $N$ is simultaneously an $A$-module and a $B$-module and the two structures are compatible in the sense that $a(xb) = (ax)b$ for all $a \in A, b \in B, x \in N$). Then $M \otimes_A N$ is naturally a $B$-module, $N \otimes_B P$ an $A$-module and we have

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

*Proof.* Define $b : M \times N \to M \otimes_A N$ by $(m, n) \mapsto m \otimes (nb)$. Fix $m$, we have $b_m(n) = m \otimes_A (nb)$. Then we have

$$\begin{aligned}
&b_m(an) = m \otimes_A ((an)b) = m \otimes_A (a(nb)) = a(m \otimes_A (nb)) = ab_m(n) \\
&b_m(n + n') = m \otimes_A ((n + n')b) = m \otimes_A (nb + n'b) \\
&= m \otimes_A (nb) + m \times_A (n'b) = b_m(n) + b_m(n')
\end{aligned}$$

Hence $b$ is bilinear and we have a unique linear injection $\bar{b} : M \otimes_A N \to M \otimes_A N$ with $\bar{b}(m \otimes_A n) = m \otimes_A (nb)$. $(\bar{b} + \bar{b}')(m \otimes_A n) = m \otimes_A (n(b + b')) = m \otimes_A (nb) + m \otimes_A (nb') = \bar{b}(m \otimes_A n) + \bar{b}'(m \otimes_A n)$

Similarly, $N \otimes_B P$ is an $A$-module

First we construct homomorphism $f : (M \otimes_A N \otimes_B P \to M \otimes_A (N \otimes_B P)$ which contains two phases

$$\begin{tikzcd}
M \times N \arrow[d] \arrow[dr, "g_z"] & \\
M \otimes_A N \arrow[r, dashed, "\bar{g}_z"] & M \otimes_A (N \otimes_B P)
\end{tikzcd}$$

$$\begin{tikzcd}
(M \otimes_A N) \times P \arrow[d] \arrow[dr, "g"] & \\
(M \otimes_A N) \otimes_B P \arrow[r, dashed, "\bar{g}"] & M \otimes_A (N \otimes_B P)
\end{tikzcd}$$

First, we fix an element $z \in P$ and therefore $g_z : (x, y) \mapsto x \otimes_A (y \otimes_B z)$ is bilinear.

$$\begin{aligned}
g_z(x + x', y) &= (x + x') \otimes_A (y \otimes_B z) = x \otimes_A (y \otimes_B z) + x' \otimes_A (y \otimes_B z) \\
&= g_1(x, y) + g_1(x', y) \\
g_z(x, y + y') &= x \otimes_A ((y + y') \otimes_B z) = x \otimes_A (y \otimes_B z + y' \otimes_B z) \\
&= x \otimes_A (y \otimes_B z) + x \otimes_A (y' \otimes_B z) = g_1(x, y) + g_1(x, y')
\end{aligned}$$

Thus we have a unique linear map $\bar{g}_z : M \otimes_A N \to M \otimes_A (N \otimes_B P)$. Let $g(x \otimes_A y, z) = g_z(x \otimes_A y)$. $g$ is bilinear as

$$\begin{aligned}
g(x \otimes_A y, z + z') &= g_{z+z'}(x \otimes_A y) = x \otimes_A (y \otimes_B (z + z')) \\
&= x \otimes_A (y \otimes_B z + y \otimes_B z') \\
&= g(x \otimes_A y, z) + g(x \otimes_A y, z') \\
g(x \otimes_A y + x' \otimes_A y', z) &= g_z(x \otimes_A y + x' \otimes_A y') \\
&= g_z(x \otimes_A y) + g_z(x' \otimes_A y') \\
&= g(x \otimes_A y) + g(x' \otimes_A y')
\end{aligned}$$

To construct $h : M \otimes_A (N \otimes_B P) \to (M \otimes_A N) \otimes_B P$, fix $M$ and do similar things □

Let $f : M \to M'$, $g : N \to N'$ be homomorphisms of $A$-modules. Define $h : M \times N \to M' \otimes N'$ by $h(x, y) = f(x) \otimes f(y)$. It is easily checked that $h$ is $A$-bilinear and therefore induces an $A$-module homomorphism

$$f \otimes g : M \otimes N \to M' \otimes N'$$

s.t.

$$(f \otimes g)(x \otimes y) = f(x) \otimes g(y) \quad (x \in M, y \in N)$$

Let $f' : M' \to M''$ and $g' : N' \to N''$ be homomorphisms of $A$-modules. Then clearly the homomorphism $(f' \circ f) \otimes (g' \circ g)$ and $(f' \otimes g') \circ (f \otimes g)$ agree on all elements of the form $x \otimes y \in M \otimes N$. Since these elements generates $M \otimes N$, it follows that

$$(f' \circ f) \otimes (g' \circ g) = (f' \otimes g') \circ (f \otimes g)$$

**Restriction and Extensions of Scalars**

Let $f : A \to B$ be a homomorphism of rings and let $N$ be a $B$-module. Then $N$ has an $A$-module structure defined as follows: if $a \in A$ and $x \in N$, then $ax$ is defined be to $f(a)x$. This $A$-module is said to be obtained from $N$ by **restriction of scalars**. In particular, $f$ defines in this way an $A$-module structure on $B$

**Proposition 2.15.** *Suppose $N$ is finitely generated as a $B$-module and that $B$ is finitely generated as an $A$-module. Then $N$ is finitely generated as an $A$-module*

*Proof.* Let $y_1, \dots, y_n$ generate $N$ over $B$ and let $x_1, \dots, x_m$ generated $B$ as an $A$-module. Then the $mn$ products $x_i y_j$ generate $N$ over $A$ □

Now let $M$ be an $A$-module. Since, as we have just seen, $B$ can be regarded as an $A$-module, we can form the $A$-module $M_B = B \otimes_A M$. In fact, $M_B$ carries a $B$-module structure s.t. $b(b' \otimes x) = bb' \otimes x$ for all $b, b' \in B$ and all $x \in M$. The $B$-module $M_B$ is said to be obtained from $M$ by **extension of scalars**

**Proposition 2.16.** *If $M$ is finitely generated as an $A$-module, then $M_B$ is finitely generated as a $B$-module*

*Proof.* If $x_1, \ldots, x_m$ generate $M$ over $A$, then the $1 \otimes x_i$ generated $M_B$ over $B$ □

### Exactness Properties of the Tensor Product

Let $f : M \times N \to P$ be an $A$-bilinear mapping. For each $x \in M$ the mapping $y \mapsto f(x, y)$ of $N$ into $P$ is $A$-linear, hence $f$ gives rise to a mapping $M \to \mathrm{Hom}(N, P)$ which is $A$-linear because $f$ is linear in the variable $x$. Conversely any $A$-homomorphism $\phi : M \to \mathrm{Hom}_A(N, P)$ defines a bilinear map, namely $(x, y) \mapsto \phi(x)(y)$. Define $f(x, y) = \phi(x)(y)$. Then $f(x + x', y) = \phi(x + x')(y)$. As $\phi$ is $A$-linear, $\phi(x + x') = \phi(x) + \phi(x')$. Then as $\mathrm{Hom}_A(N, P)$ is an $A$-module, $(\phi(x) + \phi(x'))(y) = \phi(x)(y) + \phi(x')(y)$.

$f(x, y + y') = \phi(x)(y + y') = \phi(x)(y) + \phi(x')(y)$ since $\phi(x)$ is $A$-linear

Hence the set $S$ of $A$-bilinear mappings $M \times N \to P$ is in natural one-to-one correspondence with $\mathrm{Hom}(M \otimes N, P)$, by the defining property of the tensor product. Hence we have a canonical isomorphism

$$\mathrm{Hom}(M \otimes N, P) \cong \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \tag{1}$$

**Proposition 2.17.** *Let*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{$\star$}$$

*be an exact sequence of $A$-modules and homomorphisms, and let $N$ be any $A$-module. Then the sequence*

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0 \tag{$\star\star$}$$

*(where 1 denotes the identity mapping on $N$) is exact*

*Proof.* Let $E$ denote the sequence $(\star)$ and let $E \otimes N$ denote the sequences $(\star\star)$. Let $P$ be any $A$-module. Since $(\star)$ is exact, the sequence $\mathrm{Hom}(E, \mathrm{Hom}(N, P))$

$$0 \longrightarrow \mathrm{Hom}(M'', \mathrm{Hom}(N, P)) \xrightarrow{\bar{g}} \mathrm{Hom}(M, \mathrm{Hom}(N, P)) \xrightarrow{\bar{f}} \mathrm{Hom}(M', \mathrm{Hom}(N, P))$$

is exact by 2.8. Hence by (1) the sequence $\mathrm{Hom}(E \otimes N, P)$ is exact. By 2.8 again, it follows that $E \otimes N$ exact $\square$

*Remark.* 1. Let $T(M) = M \otimes N$ and let $U(P) = \mathrm{Hom}(N, P)$. Then (1) takes the form $\mathrm{Hom}(T(M), P) = \mathrm{Hom}(M, U(P))$ for all $A$-modules $M$ and $P$.

2. It is **not** in general true that, if $M' \to M \to M''$ is an exact sequence of $A$-modules and homomorphisms, the sequence $M' \otimes N \to M \otimes N \to M'' \otimes N$ is exact

**Example 2.3.** Take $A = \mathbb{Z}$ and consider the exact sequence $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$, where $f(2) = 2x$ for all $x \in \mathbb{Z}$. If we tensor with $N = \mathbb{Z}/2\mathbb{Z}$, the sequence $0 \to \mathbb{Z} \otimes N \xrightarrow{f\otimes 1} \mathbb{Z} \otimes N$ is **not** exact, because for any $x \otimes y \in \mathbb{Z} \otimes N$, we have

$$(f \otimes 1)(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0$$

so that $f \otimes 1$ is the zero mapping, whereas $\mathbb{Z} \otimes N \neq 0$

The functor $T_N : M \mapsto M \otimes_A N$ on the category of $A$-modules and homomorphisms is therefore not in general exact. If $T_N$ is exact, that is to say if tensoring with $N$ transforms all exact sequences into exact sequences, then $N$ is said to be a **flat** $A$-module

**Proposition 2.18.** *For an $A$-module $N$, T.F.A.E.:*

1. *$N$ is flat*
2. *If $0 \to M' \to M \to M'' \to 0$ is any exact sequence of $A$-modules, the tensored sequence $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ is exact*
3. *If $f : M' \to M$ is injective, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective*
4. *If $f : M' \to M$ is injective and $M, M'$ are finitely generated, then $f \otimes 1 : M' \otimes N \to M \otimes N$ is injective*

*Proof.* $1 \to 2$ by definition.

$2 \to 1$. Given a exact sequence

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

Consider the exact sequence

$$0 \longrightarrow \mathrm{im}(f_i) \xhookrightarrow{\mathrm{in}} M_i \xrightarrow{f_{i+1}} \mathrm{im}(f_{i+1}) \longrightarrow 0$$

Then

$$0 \longrightarrow \mathrm{im}(f_i) \otimes N \xrightarrow{\mathrm{in}\otimes 1} M_i \otimes N \xrightarrow{f_{i+1}\otimes 1} \mathrm{im}(f_{i+1}) \otimes N \longrightarrow 0$$

Then $\mathrm{im}(\mathrm{in} \otimes 1) = \ker(f_{i+1} \otimes 1)$. But $\mathrm{im}(\mathrm{in} \otimes 1) = \mathrm{im}(f_i) \otimes N = \mathrm{im}(f_i \otimes 1)$. Thus $\mathrm{im}(f_i \otimes 1) = \ker(f_{i+1} \otimes 1)$.

$2 \to 3$. Consider $0 \to M' \xrightarrow{f} M$

$3 \to 2$. 3 says that if $0 \to M' \to M$ is exact, then $0 \to M' \otimes N \to M \otimes N$ is exact. Combine this and 2.17

$3 \to 4$. Obvious

$4 \to 3$. Let $f : M' \to M$ be injective and let $u = \sum x_i' \otimes y_i \in \ker(f \otimes 1)$, so that $\sum f(x_i') \otimes y_i = 0$ in $M \otimes N$. Let $M_0'$ be the submodule of $M'$ generated by the $x_i'$ and let $u_0$ denote $\sum x_i' \otimes y_i$ as an element of $M_0' \otimes N$. By 2.12 there exists a finitely generated submodule $M_0$ of $M$ containing $f(M_0')$ and s.t. $\sum f(x_i') \otimes y_i = 0$ as an element of $M_0 \otimes N$. If $f_0 : M_0' \to M_0$ is the restriction of $f$, this means that $(f_0 \otimes 1)(u_0) = 0$. Since $M_0$ and $M_0'$ are finitely generated, $f_0 \otimes 1$ is injective and therefore $u_0 = 0$, hence $u = 0$. $\square$

*Exercise* 2.0.3. If $f : A \to B$ is a ring homomorphism and $M$ is a flat $A$-module, then $M_B = B \otimes_A M$ is a flat $B$-module

*Proof.* Note that $B$ is a $(A, B)$-bimodule

Given $B$-modules $N, N'$ and suppose $f : N' \to N$ is injective. $N' \otimes_B (B \otimes_A M) \to N \otimes_B (B \otimes_A M)$ is injective iff $(N' \otimes_B B) \otimes_A M \to (N \otimes_B B) \otimes_A M$ is injective (2.0.2) which is implied by $N' \otimes_B B \to N \otimes_B B$ is injective, but $N \otimes_B B \cong N$ by 2.14 $\square$

### Algebras

Let $f : A \to B$ be a ring homomorphism. If $a \in A$ and $b \in B$, define a product

$$ab = f(a)b$$

This definition of scalar multiplication makes the ring $B$ into an $A$-module. Thus $B$ has an $A$-module structure as well as a ring structure, and these two structures are compatible in a sense which the reader will be able to formulate for himself. The ring $B$, equipped with this $A$-module structure, is said to be **$A$-algebra**. Thus an $A$-algebra is, by definition, a ring $B$ together with a ring homomorphism $f : A \to B$

*Remark.* 1. If $A$ is a field $K$ (and $B \neq 0$) then $f$ is injective by 1.2 and therefore $K$ can be canonically identified with its image in $B$. Thus a $K$-algebra ($K$ a field) is effectively a ring containing $K$ as a subring

2. Let $A$ be any ring. Since $A$ has an identify element there is a unique homomorphism of the ring of integers $\mathbb{Z}$ into $A$, namely $n \mapsto n \cdot 1$. Thus every ring is automatically a $\mathbb{Z}$-algebra

Let $f : A \to B$, $g : A \to C$ be two ring homomorphisms. An **$A$-algebra homomorphism** $h : B \to C$ is a ring homomorphism which is also an $A$-module homomorphism. $h$ is an $A$-algebra homomorphism iff $h \circ f = g$

A ring homomorphism $f : A \to B$ is **finite**, and $B$ is a **finite $A$-algebra**, if $B$ is finitely generated as an $A$-module. The homomorphism $f$ is **of finite type**, and $B$ is a **finitely-generated $A$-algebra**, if there exists a finite set of elements $x_1, \dots, x_n$ in $B$ s.t. every element of $B$ can be written as a polynomial in $x_1, \dots, x_n$ with coefficients in $f(A)$; or equivalently if there is an $A$-algebra homomorphism from a polynomial ring $A[t_1, \dots, t_n]$ onto $B$

A ring $A$ is said to be **finitely generated** if it is finitely generated as a $\mathbb{Z}$-algebra. This means that there exist finitely many elements $x_1, \dots, x_n$ in $A$ s.t. every element of $A$ can be written as a polynomial in the $x_i$ with rational integer coefficients

**Tensor Product of Algebras**

Let $B, C$ be two $A$-algebras, $f : A \to B$, $g : A \to C$ the corresponding homomorphisms. Since $B$ and $C$ are $A$-modules we may form their tensor product $D = B \otimes_A C$, which is an $A$-module. We shall now define a multiplication on $D$

Consider the mapping $B \times C \times B \times C \to D$ defined by

$$(b, c, b', c') \mapsto bb' \otimes cc'$$

This is $A$-linear in each factor and therefore, by 2.13, induces an $A$-module homomorphism

$$B \otimes C \otimes B \otimes C \to D$$

hence by 2.14 an $A$-module homomorphism

$$D \otimes D \to D$$

and this in turn by 2.11 corresponds to an $A$-bilinear mapping

$$\mu : D \times D \to D$$

which is s.t.

$$\mu(b \otimes c, b' \otimes c) = bb' \otimes cc$$

We have therefore defined a multiplication on the tensor product $D = B \otimes_A C$: for elements of the form $b \otimes c$ it is given by

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc'$$

and in general by

$$\left(\sum_i (b_i \otimes c_i)\right)\left(\sum_j (b'_j \otimes c'_j)\right) = \sum_{i,j} (b_i b'_j \otimes c_i c'_j)$$

Check this multiplication $D$ is a commutative ring, with identity element $1 \otimes 1$

## 2.1 Exercises

*Exercise* 2.1.1. Show that $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$ if $m, n$ are coprime

*Proof.* As $m$ and $n$ are coprime, there is $u, s \in \mathbb{Z}$ s.t. $um + sn = 1$, which means $u(m+n\mathbb{Z}) = um+n\mathbb{Z} = 1+n\mathbb{Z}$ and $s(n+m\mathbb{Z}) = sn+m\mathbb{Z} = 1+m\mathbb{Z}$. Hence Let $a = (1 + m\mathbb{Z}) \otimes_{\mathbb{Z}} (1 + n\mathbb{Z})$, then $a = s(n + m\mathbb{Z}) \otimes u(m + n\mathbb{Z}) = usmna$ and hence $(1 - usmn)a = 0$. But $usmn \neq 0$, hence $a = 0$ which is $(1 + m\mathbb{Z}) \otimes_{\mathbb{Z}} (1 + n\mathbb{Z}) = 0$.

Thus for any $i, j \in \mathbb{Z}$, $(i+m\mathbb{Z})\otimes(j+n\mathbb{Z}) = ij((1+m\mathbb{Z})\otimes(1+n\mathbb{Z})) = 0$ □

*Exercise* 2.1.2. Let $A$ be a ring, $\mathfrak{a}$ an ideal, $M$ an $A$-module. Show that $(A/\mathfrak{a})\otimes_A M$ is isomorphic to $M/\mathfrak{a}M$

*Proof.* As

$$0 \to \mathfrak{a} \to A \to A/\mathfrak{a} \to 0$$

is exact, we have exact sequence

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

Hence

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

Alternative way:

Define $f : \mathfrak{a} \times M \to \mathfrak{a}M$ by $f(a, m) = am$ and $g : (A/\mathfrak{a}) \times M \to M/\mathfrak{a}M$ by $g(a + \mathfrak{a}, m) = am + \mathfrak{a}M$. Then $f, g$ are both $A$-bilinear

$$\begin{tikzcd}
 & \mathfrak{a} \otimes_A M \arrow[r] \arrow[d, "\bar{f}"] & A \otimes_A M \arrow[r] \arrow[d, "\cong"] & (A/\mathfrak{a}) \otimes_A M \arrow[r] \arrow[d, "\bar{g}"] & 0 \\
0 \arrow[r] & \mathfrak{a}M \arrow[r] & M \arrow[r] & M/\mathfrak{a}M \arrow[r] & 0
\end{tikzcd}$$

Applying the Snake Lemma we get

$$0 \to \ker \bar{g} \to \operatorname{coker} \bar{f} = 0$$

Therefore $\ker \bar{g} = \{0\}$ and $\bar{g}$ is injective. Given $\bar{g}$ is surjective as well, then $\bar{g}$ is an isomorphism ☐

*Exercise* 2.1.3. Let $A$ be a local ring, $M$ and $N$ finitely generated $A$-modules. Prove that if $M \otimes N = 0$, then $M = 0$ or $N = 0$

*Proof.* Let $\mathfrak{m}$ be the maximal ideal, $k = A/\mathfrak{m}$ the residue field. Let $M_k = k \otimes_A M \cong M/\mathfrak{m}M$ by Exercise 2.1.2. By Nakayama's lemma 2.5, $M_k = 0 \Rightarrow M = 0$. But $M \otimes_A N = 0 \Rightarrow (M \otimes_A N)_k = 0 \Rightarrow M_k \otimes_k N_k = 0 \Rightarrow M_k = 0$ or $N_k = 0$, since $M_k$ and $N_k$ are vector spaces over a field

Suppose $(M \otimes_A N)_k = 0 = k \otimes_A (M \otimes_A N)$, we now prove $M_k \otimes_k N_k = 0 = (k \otimes_A M) \otimes_k (k \otimes_A N)$ ☐

# 3 TODO Problems

1.1: need more field knowledge to deal with $\mathbb{R}[x]$ and $\mathbb{Z}[x]$

2: need more matrix

1: need to check this after knowing the adjoint functor

Errata

Acknowledge: solution1 solution2 solution3