Introduction to Commutative Algebra

M. F. Atiyah & I. G. MacDonald

October 9, 2021

Contents

1 Rings and Ideals

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 $S_2 = \{\bar{\mathfrak{b}} : \bar{\mathfrak{b}} \text{ an ideal of } A/\mathfrak{a}\}$, π 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 φ is injective.

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

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

Proof. If $\mathfrak{m}$ is maximal and suppose $a \notin A$. 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, $B/\mathfrak{a}$ 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 Σ be the set of all ideals $\neq (1)$ in A. Order Σ by inclusion. Σ is not empty, since $0 \in \Sigma$. To apply Zorn's lemma we must show that every chain in Σ has an upper bound in Σ; let then $(\mathfrak{a}_\alpha)$ be a chain of ideals in Σ, so that for each pair of indices α, β 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 Σ 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 □

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

□

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

Example 1.1. n

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 $k > 0 \Rightarrow x \in \mathfrak{N} \Rightarrow \bar{x} = 0$ □

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

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 Σ be the set of ideals $\mathfrak{a}$ with the property

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

Then Σ is not empty because $0 \in \Sigma$. Zorn's lemma can be applied to the set Σ, ordered by inclusion, and therefore Σ 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 Σ; 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 Σ and therefore $xy \notin \mathfrak{p}$. Hence we have a prime ideal $\mathfrak{p}$ s.t. $f \notin \mathfrak{p}$, so that $f \notin \mathfrak{N}'$ $\square$

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 1.5 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. $\square$

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

3. ϕ 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 ϕ

□

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.

□

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

$\square$

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 $x^m = p_1 \cdots p_n \in \mathfrak{p}$

$\square$

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_α 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

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 □