# Introduction to Commutative Algebra
# Rings and Ideals

Hongwei.Wang[1]

[1] Xi'an Jiao Tong Liverpool Univercity

2024.8.1

**You should know before you start:** The article serves as a concise integration and summary of the book <Introduction to Commutative Algebra> by M.F.Atiyah and I.G.MacDonald as I delves into self-study of commutative algebra. I aim to integrate the book's content by providing a comprehensive overview and filling in some gaps present in the original text.

## 1 Introduction

Commutative Algebra is a subject of commutative structures, we know some groups or rings are not commutative, i.e. $GL_n\mathbb{R}$. We find if an algebra structure is commutative, say $\forall a, b \in A, ab = ba$, then there will be a lot of properties waiting for us to discover. In first chapter of Atiyah's book, we dicussed prime ideals and maximal ideals, which is the core of Ring theorem. Some proof or interpretation are rapidly mentioned, some even brushed aside. This note will supplement some missing proofs and provide a combing of the knowledge.

## 2 Rings and Ring Homomorphisms

**Definition 2.1** *We say a set $A$ is a ring if $A$ with two binary operations (+ and $\times$ ) such that*
*(a)* *(A, +) is an Abelian group.*
*(b)* $\exists$ $1 \in A$, *s.t.*$\forall x \in A, 1x = x1 = x$
*(c)* $\times$ *is associative, (xy)z = x(yz)*
*(d)* $\times$ *is distributive, (x(y+z)) = xy + xz*
*And we shall consider only rings which are commutative: xy = yx.*
*For those rings 1 might be equal to 0, if so, the $\forall x \in A$ we have:''*

$$x = x1 = x0 = 0$$

*Hence only one element $0 \in A$, we call $A$ the zero ring, denoted by 0*

**Definition 2.2** *A ring homomorphisms is a mapping f of ring A to ring B such that*
*(a)* *f is a abelian group homomorphisms from (A, +) to (B, +).*
*(b)* *f(xy) = f(x)f(y).*
*(c)* *$f(1_A) = 1_B$.*
*In other words, f respects additions, multiplication and the identity element.*

**Definition 2.3** *A subset S of A is a subring of A if*
*(a)* $(S, +) \leq (A, +)$
*(b)* $\forall x, y \in S, xy \in S$

*(c)* $1_A \in S$
*If $f : A \to B, g : B \to C$ are ring homomorphisms then so is $g \circ f$.*

# 3 Ideals and Quotient Rings

**Definition 3.1** *A subset $\alpha$ is a ideal of $A$ if*
*(a)* $(\alpha, +) \leq (A, +)$
*(b)* $A\alpha \subseteq \alpha$
*In other words, $x \in A$ and $y \in \alpha$ imply $xy \in \alpha$, and it is clear that ideal may not be subring, if $1 \in \alpha$, then*

$$\forall x \in A \text{ and } 1 \in \alpha \Longrightarrow x1 \in \alpha$$

*hence $\alpha = A$.*

**Definition 3.2** *$\alpha$ is ideal of $A$, the quotient group $A/\alpha$ inherits a uniquely defined multiplication from $A$ into a ring, called the quotient ring $A/\alpha$.*
*All the coset of $\alpha$ form a ring structure, and the mapping $\phi : A \longrightarrow A/\alpha$, $x \longmapsto x + A/\alpha$ is a surjective ring homomorphisms. $\forall x + \alpha \in A/\alpha$, $\exists\ x \in A$, s.t. $\phi(x) = x + \alpha$*

**Theorem 3.1** *If f:$A \longrightarrow B$ is any ring homomorphisms, the kernel of f is an ideal $\alpha \in A$, and $f(A) \leq B$, then f induces a ring isomorphism $A/\alpha \backsimeq C$.*

# 4 Zero-divisors, Nilpotent and Units

**Definition 4.1** *We say nonzero $x \in A$ is a zero-divisor if*

$$\exists\ y \in A, y \neq 0 \ s.t.\ xy = 0.$$

*A ring with all nonzero element is not zero-divisor called integral domain. i.e. $\mathbb{Z}$.*

**Definition 4.2** *We say $x \in A$ is nilpotent*

$$if\ x^n = 0,\ for\ some\ x > 0.$$

*A nilpotent is a zero-divisor, unless A = 0*

**Definition 4.3** *We say $x \in A$ is a unit, if*

$$\exists\ y \in A, s.t.\ xy = yx = 1$$

*All units in a ring form a multiplicative abelian group.*

**Definition 4.4** *We say the ideal*

$$(x) := ax, a \in A$$

*is the principal ideal generated by $x \in A$. x is a unit if and only if (x) = A = (1), this is trivial, since $xy \in (x), \forall y \in A$. Then consider $x^{-1}$, $xx^{-1} = 1 \in (x)$, and we have already showed that if $1 \in (x), (x) = A$.*

**Definition 4.5** *We say a ring $A$ is a field if $1_A \neq 0_A$ and every nonzero element is a unit. If we denoted the set of all units in $A$ as $A^*$, the $A$ is a field if $A^* = A \backslash \{0\}$. Every field is a integral domain.*

**Proposition 4.1** *Let $A \neq 0$ be a ring, then the following are equivalent:*
*(a)* *A is a field.*
*(b)* *(0) and (1) are the only ideals of A.*
*(c)* *every homomorphisms of A into a ring $B \neq 0$ is injective.*

**Proof** When show this by proof the equivalent circle:
$(a) \Rightarrow (b)$ (0) is always an ideal of A indeed, for those ideals $\alpha \neq 0$, $\exists\ x \in A, x \neq 0, s.t. x \in \alpha$, A is field so that x is a unit, hence $\alpha \supseteq (x) = (1) = A$.
$(b) \Rightarrow (c)$ We know if $f : A \to B$ is a ring homomorphisms, then ker(f) is an ideal of A, and f is a nonzero mapping, hence ker(f) = (0), f is injective.
$(c) \Rightarrow (a)$ Let $x \in A$ be a element that not a unit, then (x) $\neq$ (1), which A/(x) is not zero ring. Consider $\phi : A \to B$ a natrual homomorphisms with ker($\phi$) = (x). We have $\phi$ is injective, so (x) = (0). □

# 5 Prime Ideals and Maximal Ideals

**Definition 5.1** *An ideal $\mathcal{P} \subseteq A$ is prime if $\mathcal{P} \neq (1)$ and if $xy \in \mathcal{P}$, then $x \in \mathcal{P}$ or $y \in \mathcal{P}$.*

**Definition 5.2** *An ideal $\mathcal{M} \subseteq A$ is maximal if $\mathcal{M} \neq (1)$ and if $\exists$ ideal $\alpha \subseteq A$, s.t. $\mathcal{M} \subset \alpha \subseteq A$, then $\alpha = A$.*

**Proposition 5.1** *Equivalently:*

$$\begin{cases} \mathcal{P} \text{ is prime} & \Longleftrightarrow A/\mathcal{P} \text{ is an integral domain.} \\ \mathcal{M} \text{ is maximal} & \Longleftrightarrow A/\mathcal{M} \text{ is a field.} \end{cases}$$

**Proof** We first show two directions of the prime proposition.
($\Rightarrow$) Assume $\mathcal{P}$ is a prime ideal of A. Supppose $\exists\ a, b \in A, s.t.$

$$(a + \mathcal{P})(b + \mathcal{P}) = 0 + \mathcal{P} \in A/\mathcal{P}$$
$$(ab + \mathcal{P}) = 0 + \mathcal{P}$$

Hence we have $ab \in \mathcal{P}$, $\mathcal{P}$ is prime so that for $ab \in \mathcal{P} \Rightarrow a \in \mathcal{P}$ *or* $b \in \mathcal{P}$. Which is, $a + \mathcal{P} = 0$ or $b + \mathcal{P} = 0$. The only way for the product of two elements in A/$\mathcal{P}$ to be zero is one of them must be zero, so A/$\mathcal{P}$ is an integral domain.
($\Leftarrow$) Assume A/$\mathcal{P}$ is an integral domain. Supppose $ab \in \mathcal{P}$. Then

$$ab + \mathcal{P} = (a + \mathcal{P})(b + \mathcal{P}) = 0 + \mathcal{P}$$

A/$\mathcal{P}$ is integral domain so that $a + \mathcal{P} = 0$ or $b + \mathcal{P} = 0$, which is $a \in \mathcal{P}$ or $b \in \mathcal{P}$, hence $\mathcal{P}$ is prime.
Then we show two directions of the maximal proposition.
($\Rightarrow$) Assume $\mathcal{M}$ is a maximal ideal of A. Consider the element x $\in A$ but $x \notin \mathcal{M}$, we have $\mathcal{M} \subsetneq (a) + \mathcal{M} \subseteq A$, $\mathcal{M}$ is maximal so that $(a) + \mathcal{M} = A$, which $1_A \in (a) + \mathcal{M}$. That is to say

$$\begin{aligned} \exists\ r \in A, m \in \mathcal{M}\ , s.t.\ 1 &= ar + m \\ 1 + \mathcal{M} &= ar + \mathcal{M} \\ 1 + \mathcal{M} &= (a + \mathcal{M})(r + \mathcal{M}) \end{aligned}$$

Hence every nonzero element in A/$\mathcal{M}$ is a unit, A/$\mathcal{M}$ is a field.
($\Leftarrow$) Assume A/$\mathcal{M}$ is a field, take an ideal $\mathcal{I} \subseteq A$ *s.t.* $\mathcal{M} \subsetneq \mathcal{I} \subseteq A$, hence $\exists\ a \in \mathcal{I}$ *with* $a\ \notin \mathcal{M}, a + \mathcal{M} \in$

$A/\mathcal{M}\backslash\{0\}$, because we have A/$\mathcal{M}$ is a field so that:

$$\begin{gathered}\exists\ b+\mathcal{M} \in A/\mathcal{M}\ s.t. \\ (a+\mathcal{M})(b+\mathcal{M}) = 1+\mathcal{M} \\ (ab+\mathcal{M}) = 1+\mathcal{M} \\ ab-1 \in \mathcal{M} \subset \mathcal{I}\end{gathered}$$

we know that $a \in \mathcal{I}, so\ ab \in \mathcal{I}\ \forall\ b$, hence $1 \in \mathcal{I} \Rightarrow \mathcal{I} = A$ as required. □

**Lemma 5.1** ***Zorn's Lemma*** *Lex X be a poset in which every chain has an upper bound. Then X has at least one maximal element.*
*X to be a poset in other words is a non-empty partially ordered set, that is, we are given a relation $x \leqslant y$ on X which is reflexive and transitive, and the lemma indicate that if for every Chain T in A $\exists\ x \in A,\ s.t.\ t \leqslant x\ \forall\ t \in T$, then A has at least one maximal element.*
*We are not going to show this Lemma in sets theory. A very comprehensive proof is available in https://www.ime.usp.br/ tausk/texts/Zorn.pdf.*

**Theorem 5.1** *Every commutative ring $A \neq 0$ with identity has at least one maximal ideal.*

**Proof** This is trivial if we apply Zorn's lemma. Let $\Sigma$ be the set of all ideal $\alpha \neq (1)$ in A, $\Sigma \neq \emptyset$ because $(0) \in \Sigma$. Let $(\alpha_\chi)$ be any chain in $\Sigma$, for each pair of $\varepsilon\ and\ \delta$, either $\alpha_\epsilon \subseteq \alpha_\delta$ or $\alpha_\delta \subseteq \alpha_\epsilon$. Consider ideal $\xi = \cup_\chi \alpha_\chi \neq (1)$, which is an upper bound of the chain. □

**Corollary 5.1** *If $\alpha \neq (1)$ is an ideal of A, then there is a maximal ideal of A containing $\alpha$.*

**Proof** Asuume $\alpha \in A$ with $\alpha \neq (1)$, then the quotient ring $A/\alpha$ is nonzero. So by Theorem 5.1 there exists a maximal ideal $x+\alpha \in A/\alpha$, s.t. $0+\alpha \subseteq x+\alpha \in A/\alpha$. Keep in mind that there is a one-to-one corresponding between idealss $\dot{b}$ of A which $\alpha \subseteq b$ and the ideals $\ddot{b}$ of A/$\alpha$, we send back the $0+\alpha \in A/\alpha$ to $\alpha \subseteq A$ and finish the proof.

**Corollary 5.2** *Every non-unit of A is contained in a maximal ideal.*

**Proof** This is trivial after the proof of corollary 5.1, for every non-unit $x \in A$, consider the principal ideal (x), we have $(x) \neq (1)$ which is a proper ideal, then apply corollary 5.1. □

**Definition 5.3** *A ring A is called local ring if A has only one maximal ideal $\mathcal{M}$. i.e. all fields.*

**Definition 5.4** *For a local ring A with its maximal ideal $\mathcal{M}$, we call $k = A/\mathcal{M}$ the residue field of A.*

**Proposition 5.2** *(a) Let A be a ring and $\mathcal{M} \neq (1)$ an ideal of A s.t. every $x \in A - \mathcal{M}$ is a unit in A. Then A is a local ring and $\mathcal{M}$ is its maximal ideal. (b) Let A be a ring and $\mathcal{M}$ is its maximal ideal s.t. every element in 1 + $\mathcal{M}$ = {1 + x, x $\in \mathcal{M}$} is a unit in A. Then A is a local ring.*

**Proof** We first show proposition(a) which is trivial. Every proper ideal $\alpha \neq (1)$ must only has non-unit element, hence $\alpha \subseteq \mathcal{M}$, the only maximal ideal. Then we show proposition (b), let $x \in A - \mathcal{M}$, then (x) + $\mathcal{M}$ = (1), that is $\exists\ y \in A\ and\ t \in \mathcal{M},\ s.t.$

$$\begin{aligned}xy+t &= 1 \\ xy &= 1-t \in 1+\mathcal{M} \\ xy &\in A^*\end{aligned}$$

By proof in (a) we get (b) □

# 6 Nilradical and Jacobson Radical

**Definition 6.1** *We call the set $\mathfrak{N}$ containing all nilpotent element as the nilradical of $A$, which is*

$$\mathfrak{N} := \{x \in A : \ x^n = 0, \ \exists \ n > 0\}$$

**Proposition 6.1** *$\mathfrak{N}$ in ring $A$ is an ideal, and $A/\mathfrak{N}$ has no nilpotent element $\neq 0$.*

**Proof** We first show the closure under multiplication which is trivial,

$$x \in \mathfrak{N} \Longrightarrow ax \in \mathfrak{N}, \ \forall a \in A.$$

The closure under addition is a little complicated. Let $x, y \in \mathfrak{N}$, we want to show $x + y \in \mathfrak{N}$. Assume $x^m = 0 \ and \ y^n = 0$, consider $(x+y)^{m+n-1}$, the result shold be the sum of all possible product like the form of $x^r y^s$, where $r + s = m + n - 1$. Attention, then we have the fact that we can never have both $r < m$ and $s < n$! But all the product will vanish if there is $r > m$ or $s > n$, hence each of these products vanishes and we have $(x+y)^{m+n-1} = 0$, $(x+y) \in \mathfrak{N}$ as required.
For an element $\bar{x} \in A/\mathfrak{N}$, let $x \in A$ representes $\bar{x} \in A/\mathfrak{N}$. mentioned that to be nilpotent in $A/\mathfrak{N}$ is that

$$\begin{aligned} \bar{x}^n &= 0_{A/\mathfrak{N}}, \exists \ n > 0 \\ x^n &\in \mathfrak{N} \\ (x^n)^k &= 0, \exists \ n > 0 \\ x &\in \mathfrak{N} \end{aligned}$$

Hence $\bar{x} = 0_{A/\mathfrak{N}}$ □

**Proposition 6.2** *The nilradical of $A$ is the intersection of all the prime ideals of $A$, that is*

$$\mathfrak{N} = \cap_{i=1}^{n} \alpha_i, \ where \ \alpha_i \ is \ prime \ of \ A$$

**Proof** First we let $\mathfrak{N}' := \cap_{i=1}^{n} \alpha_i$, where $\alpha_i$ is prime. We want to show $\mathfrak{N} = \mathfrak{N}'$
We show this by first showing $\mathfrak{N} \subseteq \mathfrak{N}'$. $\forall \ f \in \mathfrak{N}$, $\exists \ n > 0$ s.t. $f^n = 0$. With the fact that every ideal in ring A is a subring of A, which

$$0_A \in \alpha_i, \ \forall i$$

that is

$$\begin{aligned} f^n = 0_a &\in \alpha_i, \ \forall i \\ f &\in \cap_{i=1}^{n} \alpha_i \\ f &\in \mathfrak{N}' \end{aligned}$$

This is because $f^n \in \alpha, \alpha \ is \ prime \Longrightarrow f \in \alpha$, this is trivial by induction with the definition of prime ideals: if $\alpha$ is prime and $f^r f^s \in \alpha$ with $r + s = n$, we have $f^r \in \alpha$ or $f^s \in \alpha$, then apply this process many times we can finally get $f \in \alpha$.
Then we show the other side $\mathfrak{N}' \subseteq \mathfrak{N}$, to reach this we proof the contrapositive instead, which is

$$f \notin \mathfrak{N} \Longrightarrow f \notin \mathfrak{N}'$$

We suppose $f \notin \mathfrak{N}$, which is

$$f^n \neq 0_A, \ \forall n > 0$$

Consider a set $\Sigma$ contains all the ideal have no powers of f, which is

$$\Sigma := \{\alpha \ is \ ideal \ of \ A : f^n \notin \alpha, \forall n > 0\}$$

We have the condition that $f \notin \Sigma$, so now our goal is to show there is a prime ideal $\mathcal{P} \in \Sigma$, which will indicates $f \notin \mathfrak{N}'$. To show this we proof by contrapositive agian that if $x \notin \alpha$ *and* $y \notin \alpha \Longrightarrow xy \notin \alpha$ then $\alpha$ is prime.

By our assumption $f^n \neq 0$, so $\Sigma \neq \emptyset$ because $0 \in \Sigma$, then by Zorn's lemma there is a maximal element $\mathfrak{M} \in \Sigma$, now we try to show such $\mathfrak{M}$ is prime. Let $x, y \notin \mathfrak{M}$, then consider

$$\mathfrak{M} \subsetneq \mathfrak{M} + (x) \Longrightarrow \mathfrak{M} + (x) \notin \Sigma$$
$$\mathfrak{M} \subsetneq \mathfrak{M} + (y) \Longrightarrow \mathfrak{M} + (y) \notin \Sigma$$

By the definition of $\Sigma$, we have

$$\begin{aligned} &\exists\ m, n > 0,\ s.t. \\ &f^m \in \mathfrak{M} + (x),\ f^n \in \mathfrak{M} + (y) \\ &f^{m+n} \in \mathfrak{M} + (xy) \end{aligned}$$

Hence $\mathfrak{M} + (xy) \notin \Sigma$, which gives us $xy \notin \mathfrak{M}$, hence $\mathfrak{M}$ is prime. Finally we find a prime ideal $\mathfrak{M}$, so that $f \notin \mathfrak{N}'$ □

**Definition 6.2** *The Jacobson redical $\mathfrak{R}$ of $A$ is defined as the intersection of all maximal ideal of $A$, which is*

$$\mathfrak{R} := \cap_{i=1}^{n} \mathcal{M}_i,\ where\ \mathcal{M}\ is\ maximal\ of\ A.$$

**Proposition 6.3** $x \in \mathfrak{R} \Longleftrightarrow 1 - xy \in A^*,\ \forall y \in A$

**Proof** We show this by proof both direction

($\Rightarrow$) We show this by show the contrapositive, assume $1 - xy$ not a unit. By Corollary 5.2 $\exists$ *maximal* $\mathcal{M}$ s.t. $1 - xy \in \mathcal{M}$. We suppose $x \in \mathfrak{R} \subseteq \mathcal{M}$, hence $1 \in \mathcal{M}$ which is contradiction. So we have $1 - xy \notin A^* \Longrightarrow x \notin \mathfrak{R}$, which is the contrapositive of want we want.

($\Leftarrow$) Also by contrapositive, suppose $x \notin \mathfrak{R}$, that is $x \notin \mathcal{M}$ for some maximal $\mathcal{M}$. Then $(x) + \mathcal{M} = (1)$, we have $xy + m = 1$ for some $y \in A$ and $m \in \mathcal{M}$, then $1 - xy \in \mathcal{M}$ which can never be unit. So we have $x \notin \mathfrak{R} \Longrightarrow 1 - xy \notin A^*$ as required. □

# 7 Operations on Ideals

**Definition 7.1** *Let $A$ by a ring $A$ with $\alpha$, $\beta$ are ideals, we define*

$$\alpha + \beta := \{x + y : x \in \alpha, y \in \beta\}$$
$$\alpha\beta := \{xy : x \in \alpha, y \in \beta\}$$
$$\alpha \cap \beta := \{z : z \in \alpha\ and\ z \in \beta\}$$

*It is trivial to show the sum and intersection of ideals are also ideal but product is not.*

**Example 7.1** *Consider (10),(12) $\subseteq \mathbb{Z}$, for the sum*

$$\begin{aligned} (10) + (12) &= \{10m + 12n : m, n \in \mathbb{Z}\} \\ &= \{2(5m + 6n) : m, n \in \mathbb{Z}\} \subseteq (2) \end{aligned}$$

*For the other side*

$$\begin{aligned} 2 &\in (10) + (12)\ with\ m = -1, n = 1 \\ (2) &\subseteq (10) + (12) \end{aligned}$$

*So (10) + (12)=(2).*
*Consider the product*

$$\begin{aligned}(10)(12) &= \{10m12n : m,n \in \mathbb{Z}\}\\ &= \{120mn : m,n \in \mathbb{Z}\}\\ &= (120)\end{aligned}$$

*Consider the intersection*

$$\begin{aligned}(10)\cap(12) &= \{n \in \mathbb{Z} : 10|n, 12|n\}\\ &= \{n \in \mathbb{Z} : 60|n\}\\ &= (60)\end{aligned}$$

*It is trivial to see for* $m,n \in \mathbb{Z}$

$$\begin{aligned}(m)+(n) &= (gcd(m,n))\\ (m)(n) &= (mn)\\ (m)\cap(n) &= (lcm(m,n))\end{aligned}$$

**Definition 7.2** *Two ideals* $\alpha$ *and* $\beta$ *are said to be coprime (comaximal) if* $\alpha+\beta=(1)$

**Proposition 7.1** *If* $\alpha$ *and* $\beta$ *are two coprime ideal, then* $\alpha\beta = \alpha\cap\beta$

**Proof** ($\subseteq$) This direction is trivial that they are all ideals hence

$$\begin{aligned}&\alpha\beta \subseteq \alpha,\ \alpha\beta\subseteq\beta\\ \Longrightarrow&\alpha\beta\subseteq\alpha\cap\beta\end{aligned}$$

($\supseteq$) For this direction we use the fact $\alpha+\beta=(1)$, consider

$$\begin{aligned}\alpha\cap\beta &= (\alpha\cap\beta)(\alpha+\beta)\\ &= (\alpha\cap\beta)\alpha + (\alpha\cap\beta)\beta\\ &\subseteq \beta\alpha+\alpha\beta\\ &\subseteq \alpha\beta\end{aligned}$$

as required. □

**Proposition 7.2** *We have* $\alpha_1,\alpha_2,...,\alpha_n$ *are ideals of A, if* $\alpha_i+\alpha_j=(1)$ *for* $i\neq j$*, then*

$$\prod \alpha_i = \cap\alpha_i$$

**Proof** We show this by induction. This is true for n = 2 by proposition 7.1, assume $\alpha_1,\alpha_2,...,\alpha_{n-1}$ are ideals of A, $\alpha_i+\alpha_j=(1)$ for $i\neq j \implies \prod_{i=1}^{n-1}\alpha_i = \cap_{i=1}^{n-1}\alpha_i$, we define

$$\beta := \prod_{i=1}^{n-1}\alpha_i = \cap_{i=1}^{n-1}\alpha_i$$

which is also ideal. We have the fact $\forall 1\leq i\leq n-1, \alpha_n+\alpha_i=(1)$, that is to say

$$\begin{aligned}\forall 1\leq i\leq n-1,\ \forall x_i\in\alpha_i,\ \exists\ &y_i\in\alpha_n\ s.t.\\ &x_i+y_i=1_A\\ &x_i\equiv 1-y_i\equiv 0\ (mod\ a_i)\end{aligned}$$

So we find the congruence of $y_i$ in those ideals

$$y_i \equiv 1 \ (mod \ a_i)$$
$$y_i \equiv 0 \ (mod \ a_n)$$

Hence

$$\beta = \prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1}(1 - y_i) \equiv 1 \ (mod \ a_n)$$
$$\beta \equiv 1 \ (mod \ a_n)$$

We get $\beta$ and $a_n$ are coprime which is proposition 7.1, that is

$$\beta\alpha_n = \prod_{i=1}^{n} \alpha_i = \beta \cap \alpha_n = \cap_{i=1}^{n}\alpha_i$$ □

**Proposition 7.3** *Define a homomorphisms of $A$ with $\alpha_1, ..., \alpha_n$ are ideals.*

$$\phi : A \longrightarrow \prod_{i=1}^{n}(A/\alpha_i)$$

*by the mapping $\phi(x) = (x + \alpha_1, x + \alpha_2, ..., x + \alpha_n)$, then*
*(a) $\phi$ is surjective $\iff \alpha_i + \alpha_j = (1), \ \forall \ i \neq j$.*
*(b) $\phi$ is injective $\iff \cap a_i = (0)$*

**Proof** (b) We show this for two directions
($\Rightarrow$ ) $\phi$ is surjective so $\exists \ x \in A$ s.t. $\phi(x) = (1, 0, ..., 0)$, hence

$$x \equiv 1 \ (mod \ \alpha_1), \ x \equiv 0 \ (mod \ \alpha_i), \ \forall 1 < i \leq n$$
$$1 = (1 - x) + x \in \alpha_1 + \alpha_i, \ \forall 1 < i \leq n$$

apply this for all $\alpha_i$ we get they are coprime to each other
($\Leftarrow$ ) Since $\alpha_1 + \alpha_i = (1), \forall \ i > 1$, that is to say

$$\forall \ u_i \in \alpha_1, \exists \ v_i \in \alpha_i, \ s.t.$$
$$u_i + v_i = 1_A$$

For fixed $u_i \in \alpha_1$, we define

$$X := \prod_{i=2}^{n} v_i \equiv 0 \ (mod \ a_i)$$
$$X = \prod_{i=2}^{n}(1 - u_i) \equiv 1 \ (mod \ a_1)$$

So $\phi(X) = (1, 0, ..., 0)$, apply this to $a_k$ for the other mapping with 1 on $k_{th}$ position. We get $\phi$ is surjective.
(c) Consider $\phi$, this is clear since $\cap\alpha_i = \ker(\phi)$ as required. □

**Proposition 7.4** *(a) Let $\mathcal{P}_1, ..., \mathcal{P}_n$ be prime ideals and $\alpha$ is an ideal, then*

$$\alpha \subseteq \cup_{i=1}^{n}\mathcal{P}_i \implies \alpha \subseteq \mathcal{P}_i \ for \ some \ i$$

*(b) Let $\alpha_1, ..., \alpha_n$ be ideals and $\mathcal{P}$ is an prime ideal, then*

$$\mathcal{P} \supseteq \cap_{i=1}^{n}\alpha_i \implies \mathcal{P} \supseteq \alpha_i \ for \ some \ i$$

*Moreover*

$$\mathcal{P} = \cap\alpha_i \implies \mathcal{P} = \alpha_i \ for \ some \ i$$

**Proof** We first give the proof of (a)
We show the contrapositive of this proposition, which is

$$\alpha \nsubseteq \mathcal{P}_i,\ \forall i \implies \alpha \nsubseteq \cup_{i=1}^n \mathcal{P}$$

For n = 1, it is certainly ture. By induction we assume

$$\alpha \nsubseteq \mathcal{P}_i,\ (1 \le i \le n-1) \implies \alpha \nsubseteq \cup_{i=1}^{n-1} \mathcal{P}$$

which is $\forall\ i, \exists\ x_i \in \alpha$ s.t. $x_i \notin \mathcal{P}_j, (i \neq j\ and\ 1 \le i, j \le n-1)$. For some i if $x_i \notin \mathcal{P}$, we are done. If not, which implies that $x_i \notin \mathcal{P}_i\ \forall\ i$, consider

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

such $y \in \alpha$ but $y \notin \mathcal{P}(1 \le i \le n)$, so $\alpha \nsubseteq \cup_{i=1}^n \mathcal{P}$ as required.
(b) We still show the contrapositive, which is

$$\mathcal{P} \nsupseteq \alpha_i,\ \forall i \implies \mathcal{P} \nsupseteq \cap_{i=1}^n$$

By assumption, $\exists\ x_i \in \alpha_i$ but $x_i \notin \mathcal{P}(1 \le i \le n)$, then

$$\prod x_i \in \prod \alpha_i \subseteq \cap \alpha_i$$

but $\prod x_i \notin \mathcal{P}$ since $\mathcal{P}$ is prime, so $\cap \alpha_i \nsubseteq \mathcal{P}$ as required. Moreover, if $\mathcal{P} = \cap \alpha_i$, then $\mathcal{P} \subseteq \alpha$, which must be $\mathcal{P} = \alpha_i$ for some i. □

**Definition 7.3** *Let $\alpha$ and beta be ideals of ring A, then their ideal quotient is*

$$(\alpha : \beta) := \{x \in A : x\beta \subseteq \alpha\}$$

*which is trivial an ideal.*

**Definition 7.4** *The ideal quotient of ideal $\alpha$ and (0) is called the annihilator of $\alpha$, denoted by Ann($\alpha$), which is*

$$Ann(\alpha) := (0, \alpha)$$

*with this notation, the set of all zero-divisor in A called D is*

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

**Definition 7.5** *Let $\alpha$ be ideal of ring A, the redical of $\alpha$ is*

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

**Proposition 7.5** *The radical of an ideal $\alpha$ is the intersection of the pirme ideals which contain $\alpha$, that is*

$$r(\alpha) = \cap_{\alpha \subseteq \mathcal{P}_i} \mathcal{P}_i$$

**Proof** By proposition 6.2, we have $\mathfrak{N} = \cap_{i=1}^n \alpha_i$ where $\alpha_i$ is prime. Consider the quotient A/$\alpha$, say all primes in A/$\alpha$ are $\mathcal{P}_1, ..., \mathcal{P}_n$, then $\mathfrak{N}_{A/\alpha} = \cap_{i=1}^n \mathcal{P}_i$. To be in $\mathfrak{N}_{A/\alpha}$, is to be in $r(\alpha)$. □

**Proposition 7.6** *Let D denote the set of all zero-divisors of A, then $D = \cup_{x \neq 0} r(Ann(x))$*

**Proof** This is trivial by D = r(D) = r($\cup_{x \neq 0 Ann(x)}$) $= \cup_{x \neq 0} r(Ann(x))$ □

**Proposition 7.7** *Let $\alpha$ and $\beta$ be ideals on ring A, then*

$$r(\alpha) + r(\beta) = (1) \implies \alpha + \beta = (1)$$

**Proof** This is trivial by r($\alpha$+$\beta$) = r(r($\alpha$) + $r(\beta)$) = r(1) = (1), so $\alpha$ + $\beta$ = (1) □

# 8 Extension and Contraction

**Definition 8.1** *Let f: $A \longrightarrow B$ a ring homomorphism, we have the fact that*

$$\alpha \subseteq A \textit{ is an ideal} \nRightarrow f(\alpha) \subseteq B \textit{ is an ideal} \tag{1}$$

$$\beta \subseteq B \textit{ is an ideal} \Rightarrow f^{-1}(\beta) \subseteq A \textit{ is an ideal} \tag{2}$$

*For an ideal $\alpha \subseteq A$, we define its extension under f as*

$$\alpha^e := Bf(\alpha) = \{y_i x_i : x_i \in f(\alpha), y_i \in B\}$$

*For an ideal $\beta \subseteq B$, we define its contraction undet f as*

$$\beta^c := f^{-1}(\beta)$$

*It is obvious that the extension of an ideal needs to multiply the image ring by the left, but contraction do not need to multiply the preimage. This is because we want to make both extension and contraction ideals, and the preimage of ideal is always ideal but the image of an ideal is not.*

**Proposition 8.1** *Let $\alpha \subseteq A$ and $\beta \subseteq B$ be ideals, and f is a ring homomorphism: $A \longrightarrow B$, then*
*(a) $\alpha \subseteq \alpha^{ec}, \beta \supseteq \beta^{ce}$.*
*(b) $\beta^c = \beta^{cec}, \alpha^e = \alpha^{ece}$*
*(c) If $E := \{\alpha^e \subseteq B : \alpha \subseteq A$ is an ideal$\}$ and $C := \{\beta^c \subseteq A : \beta \subseteq B$ is an ideal$\}$, then $\alpha \longmapsto \alpha^e$ is a bijective map of C onto E, whose inverse is $\beta \longmapsto \beta^c$.*

**Proof** We first show (a) and (b) comes from (a)
(a) Which is trivial that $f(\alpha) \subseteq Bf(\alpha)$, so $\alpha \subseteq Bf(\alpha)^c = \alpha^{ec}$, for $\beta$ we should know the fact that $\beta \supseteq f(f^{-1}(\beta))$, then we have $(\beta^c)^e \subseteq B\beta^c = B(f^{-1}(\beta)) \subseteq f(f^{-1}(\beta)) \subseteq \beta$
(b) We have already show $\alpha^e \subseteq \alpha^{ece}$ and $\beta^c \supseteq \beta^{cec}$ by (a), then the other side is trivial that with the fact $\alpha \supseteq \alpha^{ec}$, then $\alpha^e \supseteq \alpha^{ece}$, similar for $\beta$
(c) We consider C, if $\alpha \in C$, then $\alpha = \beta^c = \beta^{cec} = \alpha^{ec}$, then $\alpha$ is a contraction of $\alpha^e$. The proof is similar for E. □

# Waiting for supplement...