Algebraic Number Theory: Study Notes

Bilal Ahmad Kalas

Note

These notes provide a gradual introduction to algebraic number theory, beginning with the necessary algebraic foundations before developing the theory of number field. The exposition emphasizes clear definitions, rigorous proofs, and intuition, with the aim of building a solid understanding of the subject. This is a living document that will be continually revised, expanded, and refined as my study of algebraic number theory progresses, with new material, examples, and references incorporated over time.

Contents

Chapter 1

Introduction to Commutative Algebra

1.1 Rings and Ideals

Commutative algebra begins with the study of rings and their ideals. These objects form the basic language for much of modern algebra, algebraic geometry, and number theory. In this chapter we introduce the fundamental definitions and properties that will be used throughout the text.

1.1.1 Rings and ring homomorphisms

A *ring* R is a set equipped with two binary operations, addition and multiplication, such that:

1. $(R, +)$ is an abelian group with identity element 0;
2. multiplication is associative and distributive over addition;
3. R has an identity element 1 such that $1x = x1 = x$ for all $x \in R$;
4. the ring is commutative if, in addition, $xy = yx$ for all $x, y \in R$;

A subset S of a ring R which is also a ring under same binary operations is defined as *subring* of the ring R denoted as $S < R$. Unless stated otherwise, every ring in this text is assumed to be commutative and to have identity. The case $1 = 0$ is allowed; then the ring consists of a single element and is called the *zero ring*.
A *ring homomorphism* is a map $f : R \to S$ such that

$$f(x + y) = f(x) + f(y), \qquad f(xy) = f(x)f(y), \qquad f(1) = 1.$$

A subset $A \subseteq R$ is called a *subring* if it is closed under addition and multiplication and contains 1.

1.1.2 Ideals and quotient rings

A *left/right ideal* I of a ring R is an additive subgroup of R such that

$$RI/IR \subseteq I.$$

Equivalently, for every $r \in R$ and $a \in I$ we have $ra/ar \in I$.

Definition 1.1. A non-empty subset of a ring R is called a (two-sided) ideal of R if it is both left and right ideal. *i.e.*,

1. $a, b \in I \implies a - b \in I$, and
2. $a \in I, r \in R \implies ra, ar \in I$.

Remark 1.2. For a commutative ring, left ideal, right ideal, and two-sided ideal coincide. Since, in this text, we will mostly consider commutative rings, we only talk about ideal in general by considering any of the descriptions above.

Notation 1.3. If I is an ideal of ring R, we denote it as

$$I \lhd R.$$

Definition 1.4. Let $I \lhd R$, define a relation on R as; for $a, b \in R$,a is related to b iff $a - b \in I$ and write

$$a \equiv b(mod I).$$

Then this relation is an equivalence relation on R and class of a, $cl(a) = I + a =$ the coset of I by a in R.

1. $I + a = I + b \iff a - b \in I$ and
2. $I + a = I \iff a \in I$.

Then $R/I = \{I + a : a \in R\}$, the set of all cosets $I + a; a \in R$ is defined as quotient(factor) set of R by I.

If $I \lhd R$, then the quotient group R/I becomes a ring under the rules

$$(I + a) + (I + b) = I + (a + b)\, and$$

$$(I = a)(I + b) = I + ab.$$

This ring is called the *quotient(factor) ring* or *residue class ring* of R modulo I.

Remark 1.5. The subrings of R/I are of the form J/I where $I \subseteq J < R$. And the ideals of R/I are of the form J/I where J is an ideal of R containg I.

From above remark, we have the following fact:

Proposition 1.6. *There is a one-to-one order-preserving correspondence between the ideals of J of R containing I and the ideals $\bar{J}$ of R/I given by $J = \phi^{-1}(\bar{J})$.*

There is a natural surjective ring homomorphism

$$\phi : R \to R/I, \qquad r \mapsto r + I,$$

whose kernel is precisely I.

Definition 1.7. A non-zero element $x \in R$ is a *zero-divisor* if there exists $y \neq 0$ in R such that $xy = 0$. A ring with no zero-divisors is called an *integral domain*. For example, $\mathbb{Z}$ is an Integral Domain.

Definition 1.8. An element $x \in R$ is a *unit* if there exists $y \in R$ such that $xy = 1$. The set of all units of R forms a multiplicative group.

Definition 1.9 (Field)**.** A commutative ring with unity in which $1 \neq 0$ is called as *field* if its every non-zero element is a unit.

Every field is an Integral Domain but not conversely as $\mathbb{Z}$ is an integral domain but not a field.

Remark 1.10. If$f : A \longrightarrow B$ is any ring homomorphism, the kernel of $f(= f^{-1}(0))$, denoted by $kerf$ is an ideal of A, and the image of $f(= f(A))$ is a subring C of B; and f induces a ring isomorphism $A/kerf \cong C$.

1.2 Classification of ideals

$P \lhd R$ is called *prime* if

$$xy \in P \implies x \in P \text{ or } y \in P.$$

$M \lhd R \, s.t \, M \neq R$, is called *maximal* if there is no ideal J such that

$$M \lhd J \lhd R.$$

i.e., if $M \subsetneq I \subsetneq R$; where $I \lhd M$, then either $M = I$ or $I = R$.

Remark 1.11. Below are few observations about prime and maximal ideals (Remember that "ring" means commutative ring with unity 1):

- P is prime if and only if R/P is an integral domain;
- M is maximal if and only if R/M is a field;
- Every maximal ideal is prime;
- In a finite ring, every prime ideal is maximal;
- the zero ideal (0) is prime iff R is an Integral Domain. That is, if R contains no zero divisors;
- $p\mathbb{Z}$ is both prime and maximal in $\mathbb{Z}$ for all prime p.

If $f : A \longrightarrow B$ is a ring homomorphism and Q is a prime ideal in B, then $f^{-1}(Q)$ is a prime ideal in A, for $A/f^{-1}(Q)$ is isomorphic to a subring of B/Q and hence has no zero-divisor $\neq 0$. But if M is a maximal ideal of B it is not necessarily true that $f^{-1}(M)$ is maximal in A; all we can say for sure is that it is prime. (Example: $A = \mathbb{Z}$, $B = \mathbb{Q}$, $M = (0)$.)

Definition 1.12. Let $S \subseteq R$; where R is any ring, then the smallest ideal I containing S is defined as the ideal generated by S. It is, symbolically, denoted by $I = (S)$. That is, if $S \subseteq J \lhd R$ then $I \subseteq J$.

$$i.e., (S) = \bigcap_{S \subseteq J \lhd R} J$$

Now, consider the following

$$I = (a) = ma + ra + sa : m \in \mathbb{Z}, r, s \in R.$$

If $m = 0$, $s = 0$ then

$$\forall \, r \in R, ra \in I = (a)$$
$$\implies Ra \subseteq (a);$$

And, if $m = 0$, $r = 0$ then

$$aR \subseteq (a);$$

If R is a commutative ring with unity then, $\forall r \in R, a \in Ra, aR \implies (a) \subseteq Ra, aR$

$$\implies (a) = Ra = aR$$

Definition 1.13. An ideal generated by a single element is called as *Principle ideal.* That is, I is a principle ideal iff $I = (a)$ for some $a \in R$.

If $U \lhd R$ such that it contains unity then $U = R$. If $I \lhd R$ such that it contains a unit of R then $I = R$. The ideal $\{0\} = (0)$ often denoted by 0 and $R = (1)$. We note the following observation:

Observation 1.14. *$r \in R$ is a unit iff $(r) = R = (1)$.*

Proposition 1.15. *Let R be a non-zero ring. Then the following are equivalent:*

(i) *R is a field.*

(ii) *The only ideals of R are 0 and (1).*

(iii) *Every ring homomorphism from R into a non-zero ring is injective.*

Proof. (i) $\Rightarrow$ (ii). Let $I \neq 0$ be an ideal of R. Then I contains a non-zero element x. Since R is a field, x is a unit. Hence

$$I \supseteq (x) = R,$$

and therefore $I = R$.

(ii) $\Rightarrow$ (iii). Let

$$\varphi : R \longrightarrow S$$

be a ring homomorphism, where $S \neq 0$. Since $\ker(\varphi)$ is an ideal of R, hypothesis (ii) implies that either

$$\ker(\varphi) = 0$$

or

$$\ker(\varphi) = R.$$

The latter is impossible because then $\varphi(1) = 0$, forcing S to be the zero ring. Hence

$$\ker(\varphi) = 0,$$

so φ is injective.

(iii) $\Rightarrow$ (i). Let $x \in R$ be a non-zero element. Suppose that x is not a unit. Then the principal ideal $< x >$ is a proper ideal of R, so the quotient ring

$$R/(x)$$

is non-zero. Let

$$\pi : R \longrightarrow R/ < x >$$

be the natural quotient homomorphism. By hypothesis, π is injective. Since

$$\ker(\pi) = (x),$$

it follows that

$$(x) = (0),$$

which implies $x = 0$, a contradiction. Therefore every non-zero element of R is a unit, and hence R is a field. □

Theorem 1.16. *Every ring $R \neq \{0\}$ has at least one maximal ideal.*

Proof. We use Zorn's Lemma. Let Σ be the set of all ideals $\neq (1)$ in R. 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 (I_α) be a chain of ideals in Σ. So that for each pair of indices α, β we have either $I_\alpha \subseteq I_\beta$ or $I_\beta \subseteq I_\alpha$. Let $I = \cup_\alpha I_\alpha$. Then I is an ideal: For if $a, b \in I$ and $r \in R$, then $\exists\, \alpha, \beta$ such that $a \in I_\alpha, b \in I_\beta$, we may assume $I_\alpha \subseteq I_\beta$ then $a, b \in I_\beta$ where $I_\beta \triangleleft R$ and hence $a - b \in I_\beta$ and $ra \in I_\beta$. Consequently, $a - b \in I$ and $ra \in I$.
Now, $1 \notin I$ because $1 \notin I_\alpha \ \forall\ \alpha$. Hence $I \in \Sigma$ and I is an upper bound of the chain. Hence, by Zorn's lemma, Σ has a maximal element. □

Corollary 1.17. *f $I \neq (1)$ is an ideal of R, there exists a maximal ideal of R containing a.*

Proof. Applying Theorem 1.16 on R/I, we obtain a maximal ideal $\bar{M} = M/I$ of R/I. Then, by Remark 1.5 and Proposition 1.6, the desired conclusion follows. □

Corollary 1.18. *Every non-unit of R is contained in a maximal ideal.*

Remark 1.19. There exist rings with exactly one maximal ideal, for example fields. A ring R with exactly one maximal ideal M is called a local ring. The field $K = R/M$ is called the residue field of R.

Proposition 1.20. *i) Let R be a ring and $M \neq (1)$ an ideal of R such that every $x \in R - M$ is a unit in R. Then R is a local ring and M its maximal ideal.*

ii) Let R be a ring and M a maximal ideal of R, such that every element of $1+M$ (i.e., every $1+x$, where $x \in M$) is a unit in R. Then R is a local ring.

Proof. i) Every ideal $\neq 1$ consists of non-units, hence is contained in M. Hence M is the only maximal ideal of R.

ii) Let $x \in R - M$. Since M is maximal, the ideal generated by x and M is (1), hence there existy $y \in R$ and $t \in M$ such that $xy + t = 1$; hence $xy = 1 - t$ belongs to $1 + M$ and therefore is a unit. Now use (i) to obtain to conclusion.

□

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

Example 1.21. 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.

Definition 1.22. 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 $(y) = (1)$.

1.2.1 Nilradical and Jacobsan Radical

Definition 1.23. An element $x \in R$ is *nilpotent* if $x^n = 0$ for some $n > 0$.

Definition 1.24. The set η_R of all nilpotent elements in a ring R is an ideal, and R/η_R has no nilpotent element $\neq 0$.

Proof. If $x \in \eta_R$, clearly $rx \in \eta_R$ for all $r \in R$. Let $x, y \in \eta_R$; then $x^m = 0, y^n = 0$ for some $n, m \in \mathbb{N}$.
By the binomial theorem (which is valid in any commutative ring), $(x + y)^{m+n-1}$ is a sum of integer multiples of products $x^r y^s$, where $r + s = m + n - 1$; we cannot have both $r < m$ and $s < n$, hence each of these products vanishes and therefore $(x+y)^{m+n-1} = 0$. Hence $x+y \in \eta_R$ and therefore η_R is an ideal.
Let $\bar{x} \in R/\eta_R$ be represented by $x \in R$. Then $\bar{x}^n$ is represented by x^n, so that $\bar{x}^n = 0 \implies x^n \in \mathcal{A} \implies (x^n)^k = 0$ for some $k > 0 \implies x \in \eta_R \implies \bar{x} = 0$. □

Definition 1.25 (Nilradical)**.** The ideal η_R is called the *nilradical* of R.

Proposition 1.26. *The nilradical of R is the intersection of all the prime ideals of R.*

Proof. Let $\mathcal{R}'$ denote the intersection of all the prime ideals of R. If $a \in R$ is nilpotent and if P is a prime ideal, then $a^n = 0 \in P$ for some $n > 0$, hence $a \in P$ (because P is prime). Hence $a \in \mathcal{R}'$.
Conversely, suppose that a is not nilpotent. Let Σ be the set of ideals I with the property

$$n > 0 \implies a^n \notin I$$

Then Σ is not empty because $(0) \in \Sigma$. As in Theorem 1.16 Zorn's lemma can be applied to the set Σ, ordered by inclusion, and therefore Σ has a maximal element. Let $\mathcal{P}$ be a maximal element of Σ. We shall show that $\mathcal{P}$ is a prime ideal. Let $x, y \notin \mathcal{P}$. Then the ideals $\mathcal{P} + (x)$, $\mathcal{P} + (y)$ strictly contain $\mathcal{P}$ and therefore do not belong to Σ; hence $a^n \in \mathcal{P} + (x)$, $a^m \in \mathcal{P} + (y)$ for some n, m. It follows that $a^{m+n} \in \mathcal{P} + (xy)$, hence the ideal $\mathcal{P} + (xy)$ is not in Σ and therefore $xy \notin \mathcal{P}$. Hence we have a prime ideal $\mathcal{P}$ such thatf $a \notin \mathcal{P}$, so that $a \notin \mathcal{R}'$. □

Definition 1.27. The *Jacobson radical* J_R of a ring R is defined to be the intersection of all the maximal ideals of R.

Proposition 1.28. *Let J_R denote the Jacobson radical of a ring R. Then*

$$x \in J_R \iff 1 - xy \text{ is a unit in } R \text{ for all } y \in R.$$

Proof. ($\Rightarrow$) Suppose that $1 - xy$ is not a unit. Then, by corollary 1.18, it belongs to some maximal ideal M. Since

$$x \in J_R \subseteq M,$$

we have $xy \in M$, and therefore

$$1 = (1 - xy) + xy \in M,$$

which is impossible.
($\Leftarrow$) Suppose that $x \notin M$ for some maximal ideal M. Then M and x generate the unit ideal (1), so there exist $u \in M$ and $y \in R$ such that

$$u + xy = 1.$$

Hence

$$1 - xy = u \in M,$$

and therefore $1 - xy$ is not a unit. □

Exercise 1.29. If $x \in \eta_A$, then $1 + x$ is a unit in A. Hence deduce that sum of a unit and nilpotent element is also a unit.

Solution. Let $x \in \eta_A \Rightarrow x^n = 0$ for some $n > 0$.
Consider

$$(1 + x)(1 - x + x^2 - x^3 + \cdots + (-1)^n x^n) = 1 + (-1)^n x^{n+1} = 1 + 0 = 1$$

$\because x^n = 0 \Rightarrow x^{n+1} = 0$

$$\therefore \quad 1 + x \text{ is a unit element.}$$

Let u be a unit in a ring A, Then

$$(u^{-1}x)^n = u^{-n}x^n = 0$$

$$\Rightarrow (u^{-1}x)^n = 0$$

$$\Rightarrow u^{-1}x \in \eta_A$$

$$\Rightarrow 1 + u^{-1}x \text{ is a unit}$$

$$\Rightarrow u(1 + u^{-1}x) \text{ is a unit}$$

$$\Rightarrow u + x \text{ is a unit, as required.}$$

Theorem 1.30. *Let A be a ring. Then following are equivalent:*

(i) A has exactly one prime ideal.

(ii) Every element of A is either a unit or nilpotent.

(iii) $\dfrac{A}{\eta_A}$ is a field.

Proof. $(i) \Rightarrow (ii)$. Suppose P is the only prime ideal of A. Then $\eta_A = P$.
Also P is contained in some maximal ideal of A.
Then P is maximal as every maximal is prime.
Let $x \in A - \eta_A$.
If x is a unit, we are done.
Suppose x is not a unit, then x is contained in some maximal ideal i.e;

$$x \in P = \eta_A.$$

Therefore x is then a nilpotent element.
$(ii) \Rightarrow (iii)$. Suppose (ii) holds good.
Then $x \in A - \eta_A$ is a unit. Therefore η_A is the only maximal ideal in A. Hence

$$\frac{A}{\eta_A}$$

is a field.
$(iii) \Rightarrow (i)$. Suppose $\frac{A}{\eta_A}$ is a field. Then η_A is a maximal ideal.
Let P be a prime ideal of A, so

$$\eta_A = \bigcap_{P \in \Delta} P \subseteq P$$

$$\Rightarrow \eta_A \subseteq P$$

But η_A is maximal, so $P = \eta_A$.

$$\therefore P \text{ is the only prime ideal of } A.$$

□

1.3 More on Ideals

If I and J are ideals of R, then their *sum*, *intersection*, and *product* are defined by

$$I + J = \{x + y : x \in I,\ y \in J\},$$

$$I \cap J = \{x : x \in I \,\&\, x \in J\},$$

and

$$IJ = \left\{ \sum_k x_k y_k : x_k \in I,\ y_k \in J \right\},$$

where the sum runs over finite number of terms. Similarly we define the product of any finite family of ideals. In particular the powers $I^n (n > 0)$ of an ideal I are defined; conventionally, $a^0 = (1)$. Thus $a^n (n > 0)$ is the ideal generated by all products $x_1 x_2 \dots x_n$ in which each factor x_i belongs to I.
These operations satisfy the usual commutative and associative laws, and the product distributes over sum:

$$I(J + K) = IJ + IK.$$

Two ideals I and J are said to be *coprime ot comaximal* if

$$I + J = R.$$

In this case,

$$I \cap J = IJ.$$

Clearly two ideals I, J are coprime if and only if there exist $x \in I$ and $y \in J$ such that $x + y = 1$.
Two distince maximal ideals are always comaximal, since if $M \neq N$ are maximal ideals, then

$$M + N = R.$$

However, distinct prime ideals need not be comaximal. For example, in the ring $\mathbb{K}[x, y]$; $\mathbb{K}$ is a field, (x) and (x, y) but $(x) + (x, y) = (x, y) \neq R$.

Remark 1.31. Arbitrary intersection of ideals, product of two ideals, and sum of two ideals are again ideals of the same ring.

Example 1.32. If $R = \mathbb{Z}$, $I = (m)$, $J = (n)$ then $I + J$ is the ideal generated by the h.c.f. of m and n; $I \cap J$ is the ideal generated by their l.c.m.; and $IJ = (mn)$. Thus (in this case) $IJ = I \cap J \iff m, n$ are coprime.

Example 1.33. $R = k[x_1, \dots, x_n]$, $I = (x_1, \dots, x_n) =$ ideal generated by $x_1, \dots, x_n$. Then I^m is the set of all polynomials with no terms of degree $< m$.

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

$$I \cap (J + K) = I \cap J + I \cap K \quad \text{if } I \supseteq J \text{ or } I \supseteq K.$$

Again, in $\mathbb{Z}$, we have $(I + J)(I \cap J) = IJ$; but in general we have only

$$(I + J)(I \cap J) \subseteq IJ$$

(since $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$).
Clearly $IJ \subseteq I \cap J$,

$$I \cap J = IJ \quad \text{provided } I + J = (1).$$

Let $R_1, \ldots, R_n$ be rings. Their *direct product*

$$R = \prod_{i=1}^{n} R_i$$

is the set of all sequences $x = (x_1, \ldots, x_n)$ with $x_i \in R_i$ $(1 \leq i \leq n)$ and componentwise addition and multiplication. R is a commutative ring with identity element $(1, \ldots, 1)$. We have projections $p_i : R \to R_i$ defined by $\pi_i(x) = x_i$; they are ring homomorphisms.
Let R be a ring and $I_1, \ldots, I_n$ ideals of R. Define a homomorphism

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

by the rule $\phi(x) = (x + I_1, \ldots, x + I_n)$. We have the following result:

Proposition 1.34. *1. If I_i, I_j are coprime whenever $i \neq j$, then $\prod I_i = \cap I_i$.*

2. ϕ is surjective $\iff$ I_i, I_j are coprime whenever $i \neq j$.

3. ϕ is injective $\iff$ $\cap I_i = (0)$.

Proof. i) by induction on n. The case $n = 2$ is dealt with above. Suppose $n > 2$ and the result is true for $n - 1$, and let $A = \prod_{i=1}^{n-1} I_i = \cap_{i=1}^{n-1} I_i$. Since $I_i + I_n = (1)$ $(1 \leq i \leq n-1)$ we have equations $x_i + y_i = 1$ $(x_i \in I_i,\ y_i \in I_n)$ and therefore

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) \equiv 1 \pmod{I_n}.$$

Hence $B + I_n = (1)$ and so

$$\prod_{i=1}^{n} I_i = BI_n = B \cap I_n = \cap_{i=1}^{n} I_i.$$

ii) $\Rightarrow$: Let us show for example that I_1, I_2 are coprime. There exists $x \in R$ such that $\phi(x) = (\bar{1}, \bar{0}, \ldots, \bar{0})$; hence $x \equiv 1 \pmod{I_1}$ and $x \equiv 0 \pmod{I_2}$, so that

$$1 = (1 - x) + x \in I_1 + I_2.$$

$\Leftarrow$: It is enough to show, for example, that there is an element $x \in R$ such that $\phi(x) = (1, 0, \ldots, 0)$. Since $I_1 + I_i = (1)$ $(i > 1)$ we have equations $u_i + v_i = 1$ $(u_i \in I_1,\ v_i \in I_i)$. Take $x = \prod_{i=2}^{n} v_i$, then $x \equiv \prod_{i=2}^{n} (1 - u_i) \equiv 1 \pmod{I_1}$, and $x \equiv 0 \pmod{I_i}$, $i > 1$. Hence $\phi(x) = (1, 0, \ldots, 0)$ as required.

iii) We know that ϕ is injective iff $ker\phi = (0)$.

$$\begin{aligned} \text{Now, } ker\phi = \{x \in R : \phi(x) &= \{(\bar{0}, \bar{0}, \ldots, \bar{0})\} \\ &= \{x \in R : (x + I_1, x + I_2, \ldots, x + I_n) = (I_1, I_2, \ldots, I_n)\} \\ &= \{x \in R : x \in I_1, x \in I_2, \ldots, x \in I_n\} \\ &= \cap_{i=1}^{n} I_i. \end{aligned}$$

Then, the result follows immediately.

□

The union $I \cup J$ of ideals is not, in general, an ideal.

Theorem 1.35 (Chinese Remainder Theorem)**.** *Let R be a ring and $I_1, I_2, \ldots, I_n$ be ideals in R such that*

$$I_i + I_j = (1), \qquad \forall\, i \neq j.$$

Then

(i) If $a_1, a_2, \ldots, a_n \in R$, then $\exists\, a \in R$ such that

$$a \equiv a_i \pmod{I_i}, \qquad \forall\, i.$$

(ii) If $b \in R$ is such that

$$b \equiv a_i \pmod{I_i}, \qquad \forall\, i,$$

then

$$b \equiv a \pmod{\bigcap_{i=1}^{n} I_i}.$$

(iii)

$$\frac{R}{\bigcap\limits_{i=1}^{n} I_i} \cong \prod_{i=1}^{n} \frac{R}{I_i}.$$

Proof. Since any two distinct ideals in R are comaximal, so

$$I_1 + I_j = (1), \qquad \forall\, j = 2, 3, \ldots, n.$$

Therefore

$$\exists\, x_1 \in I_1,\ y_j \in I_j$$

such that

$$x_1 + y_j = 1, \qquad \forall\, j = 2, 3, \ldots, n.$$

Hence we've

$$\prod_{j=2}^{n} (x_1 + y_j) = 1. \tag{i}$$

Clearly L.H.S. of (i) consists of 2^{n-1} terms where each term is product of $n-1$ elements chosen from

$$\{x_1, y_2, \ldots, y_n\}.$$

Also each term in L.H.S. of (i) belongs to I_1, except the term

$$y_2 y_3 \cdots y_n = \prod_{j=2}^{n} y_j = c_1 \quad \text{(say)}.$$

Thus

$$1 - c_1 = \prod_{j=2}^{n} (x_1 + y_j) - \prod_{j=2}^{n} y_j \in I_1,$$

which implies

$$c_1 \equiv 1 \pmod{I_1}.$$

Also

$$c_1 = \prod_{j=2}^{n} y_j \in I_j,$$

so

$$c_1 \equiv 0 \pmod{I_j}, \qquad \forall\, j \neq 1.$$

In general, for $i = 1, 2, \ldots, n$, we've

$$c_i \equiv 1 \pmod{I_i}$$

and

$$c_i \equiv 0 \pmod{I_j}, \qquad \forall\, j \neq i.$$

Let

$$a_1, a_2, \ldots, a_n \in R.$$

Setting

$$a = \sum_{i=1}^{n} a_i c_i.$$

Then

$$a - (a_1c_1 + a_2c_2 + \cdots + a_nc_n) = 0$$

implies

$$a \equiv (a_1c_1 + a_2c_2 + \cdots + a_nc_n) \pmod{I_i},$$

since $0 \in I_i$.
Hence

$$a \equiv a_i \pmod{I_i},$$

because $c_i \equiv 1 \pmod{I_i}$ and $c_j \equiv 0 \pmod{I_i}$, $\quad j \neq i$. This proves (i).

(ii) Suppose $b \in R$ is such that

$$b \equiv a_i \pmod{I_i}, \qquad \forall\, i.$$

Then

$$b \equiv a \pmod{I_i}, \qquad \forall\, i$$

(by part (i)).
Hence

$$b - a \in I_i, \qquad \forall\, i,$$

which implies

$$b - a \in \bigcap_{i=1}^{n} I_i.$$

Therefore

$$b \equiv a \pmod{\bigcap_{i=1}^{n} I_i}.$$

(iii) Define a map

$$\phi : R \longrightarrow \prod_{i=1}^{n} \frac{R}{I_i}$$

by

$$\phi(a) = (a + I_1,\ a + I_2,\ \ldots,\ a + I_n).$$

Note that ϕ is a ring homomorphism.
Also ϕ is surjective.
Let

$$(a_1 + I_1,\ a_2 + I_2,\ \ldots,\ a_n + I_n) \in \prod_{i=1}^{n} \frac{R}{I_i}.$$

Then ϕ is surjective if there exists $a \in R$ such that

$$\phi(a) = (a_1 + I_1, \ldots, a_n + I_n).$$

That is,

$$(a + I_1, \ldots, a + I_n) = (a_1 + I_1, \ldots, a_n + I_n),$$

which implies

$$a + I_i = a_i + I_i, \qquad \forall\, i = 1, 2, \ldots, n,$$

or equivalently,

$$a - a_i \in I_i, \qquad \forall\, i = 1, 2, \ldots, n,$$

which is true by part (i).
Hence ϕ is surjective.
Therefore, by the First Isomorphism Theorem,

$$\frac{R}{\ker \phi} \cong \prod_{i=1}^{n} \frac{R}{I_i}.$$

Now

$$\begin{aligned} \ker \phi &= \{a \in R : \phi(a) = (I_1, I_2, \ldots, I_n)\} \\ &= \{a \in R : a \in I_i,\ \forall\, i \in \{1, 2, \ldots, n\}\} \\ &= \bigcap_{i=1}^{n} I_i. \end{aligned}$$

Thus

$$\frac{R}{\bigcap_{i=1}^{n} I_i} \cong \prod_{i=1}^{n} \frac{R}{I_i}.$$

□

Proposition 1.36 (Prime Avoidance Lemma)**.** *1. Let $P_1, \ldots, P_n$ be prime ideals and let I be an ideal contained in $\cup_{i=1}^{n} P_i$. Then $I \subseteq P_i$ for some i.*

2. Let $I_1, \ldots, I_n$ be ideals and let P be a prime ideal containing $\cap_{i=1}^{n} I_i$. Then $P \supseteq I_i$ for some i. If $P = \cap I_i$, then $P = I_i$ for some i.

Proof. i) Suppose $I \nsubseteq P_i$ for any i, we show that

$$I \nsubseteq \bigcup_{i=1}^{n} P_i,$$

by induction on n.

If $n = 1$, then there is nothing to prove.

Assume that $n > 1$ and the result is true for $n - 1$.

If

$$I \nsubseteq P_j, \qquad \forall\, j = 1, 2, \ldots, i-1, i+1, \ldots, n,$$

then

$$I \nsubseteq \bigcup_{\substack{j=1 \\ j \neq i}}^{n} P_j.$$

$$\Rightarrow \exists \text{ some } x_i \in I \text{ such that } x_i \notin P_j, \qquad \forall\, j = 1, 2, \ldots, i-1, i+1, \ldots, n.$$

Suppose $x_i \notin P_i,\ \forall\, i = 1, 2, \ldots, n$. Then

$$x_i \notin \bigcup_{i=1}^{n} P_i,$$

and so

$$I \nsubseteq \bigcup_{i=1}^{n} P_i.$$

Therefore the result holds in this case.

Now if $x_i \in P_i$, let's consider the element

$$y = x_2 x_3 \cdots x_n + x_1 x_3 \cdots x_n + \cdots + x_1 x_2 \cdots x_{n-1},$$

i.e.,

$$\begin{aligned} y &= \sum_{i=1}^{n} x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n \\ &= \sum_{i=1}^{n} \prod_{\substack{j=1 \\ j \neq i}}^{n} x_j. \end{aligned}$$

Clearly $y \in I$ (as each $x_i \in I$). But $y \notin P_i$ as each monomial $x_1 x_2 \cdots x_{i-1} x_{i+1} \cdots x_n$ is not in P_i.

$$\therefore \quad y \notin \bigcup_{i=1}^{n} P_i.$$

$$\Rightarrow \quad I \nsubseteq \bigcup_{i=1}^{n} P_i.$$

This proves part (i).

ii) Assume $I_i \nsubseteq P$ for all $i = 1, 2, \ldots, n$. Then there exists some

$$x_i \in I_i \quad \text{such that} \quad x_i \notin P.$$

Now

$$\prod_{i=1}^{n} x_i = x_1 x_2 \cdots x_n \in \prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i.$$

But

$$\prod_{i=1}^{n} x_i \notin P \qquad (\text{as } P \text{ is prime and no } x_i \in P).$$

$$\therefore \quad \bigcap_{i=1}^{n} I_i \nsubseteq P.$$

Hence

$$\bigcap_{i=1}^{n} I_i \subseteq P \quad \Rightarrow \quad I_i \subseteq P \text{ for some } i.$$

□

Definition 1.37. If I, J are ideals in a ring R, then the *ideal quotient*(colon) if I and J is defined as

$$(I : J) = \{x \in R : xJ \subseteq I\}$$

Lemma 1.38. *The ideal quotient of two ideals is an ideal.*

Proof. We show that $(I : J)$ is an ideal.
Let $x, y \in (I : J)$. Then

$$xJ \subseteq I \quad \text{and} \quad yJ \subseteq I.$$

Hence

$$xj \in I \quad \text{and} \quad yj \in I, \qquad \forall\, j \in J.$$

Now

$$(x + y)j = xj + yj \in I, \qquad \forall\, j \in J.$$

Therefore,

$$x + y \in (I : J).$$

Also, for any $a \in R$, we have

$$(ax)j = a(xj) \in I, \qquad \forall\, j \in J,$$

since I is an ideal.
Hence

$$ax \in (I : J).$$

Thus $(I : J)$ is an ideal of R. □

Notation 1.39. If $I = (x)$ and $J = (y)$, then we shall write

$$(I : J) = (x : y).$$

Definition 1.40. $(0 : J) = \{a \in R : aJ \subseteq 0\} = \{a \in R : aJ = 0\} = \{a \in R : aj = 0,\ \forall\, j \in J\}$. This is called the *annihilator* of J in R and is denoted by

$$\mathrm{Ann}_R(J).$$

Remark 1.41.

1. Let D_R be the set of all zero divisors in a ring R. Then

$$\mathrm{Ann}(x) = \{a \in R : ax = 0\} = \{a \in R : a(x) = 0\} = (0 : x).$$

Hence

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

2. If $x = 0$, then

$$\mathrm{Ann}(x) = R.$$

If J is a principal ideal (x), we shall write $(I : x)$ in place of $(I : (x))$.

Theorem 1.42. *Let I, J, K be ideals in a ring R. Then*

1. $I \subseteq (I : J)$.
2. $(I : J)J \subseteq I$.
3. $((I : J) : K) = (I : JK)$.
4. $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$.

5. $(I : \sum_i J_i) = \bigcap_i (I : J_i)$.

Proof. 1. Let $x \in I$. Then for every $a \in R$,

$$xa \in I,$$

i.e.,

$$xR \subseteq I.$$

Hence

$$xJ \subseteq I,$$

since $J \subseteq R$.

Therefore

$$x \in (I : J).$$

Thus

$$I \subseteq (I : J).$$

2. Let $x \in (I : J)$. Then

$$xJ \subseteq I.$$

Since this is true for every $x \in (I : J)$,

$$(I : J)J \subseteq I.$$

3. Let

$$x \in ((I : J) : K).$$

Then

$$xk \in (I : J), \qquad \forall\, k \in K.$$

Hence

$$xkJ \subseteq I, \qquad \forall\, k \in K,$$

which implies

$$xkj \in I, \qquad \forall\, k \in K,\ \forall\, j \in J.$$

Since multiplication is associative,

$$xjk \in I, \qquad \forall\, j \in J,\ \forall\, k \in K.$$

Therefore

$$xJK \subseteq I,$$

so

$$x \in (I : JK).$$

Hence

$$((I : J) : K) \subseteq (I : JK). \qquad (*)$$

Now let

$$y \in (I : JK).$$

Then

$$yjk \in I, \qquad \forall\, j \in J,\ \forall\, k \in K,$$

or equivalently,

$$ykj \in I, \qquad \forall\, k \in K,\ \forall\, j \in J.$$

Hence

$$yk \in (I : J), \qquad \forall\, k \in K,$$

which implies

$$y \in ((I : J) : K).$$

Therefore

$$(I : JK) \subseteq ((I : J) : K). \qquad (**)$$

Combining $(*)$ and $(**)$, we obtain

$$((I : J) : K) = (I : JK).$$

4. Let

$$x \in \left(\bigcap_i I_i : J \right).$$

Then

$$xJ \subseteq \bigcap_i I_i$$

if and only if

$$xJ \subseteq I_i, \qquad \forall\, i.$$

This is equivalent to

$$x \in (I_i : J), \qquad \forall\, i,$$

which is equivalent to

$$x \in \bigcap_i (I_i : J).$$

Hence

$$\left(\bigcap_i I_i : J \right) = \bigcap_i (I_i : J).$$

5. Let

$$x \in \left(I : \sum_i J_i \right).$$

Then

$$x \sum_i J_i \subseteq I.$$

Since

$$J_i \subseteq \sum_i J_i,$$

we have

$$xJ_i \subseteq x \sum_i J_i \subseteq I.$$

Hence

$$xJ_i \subseteq I, \qquad \forall\, i,$$

so

$$x \in (I : J_i), \qquad \forall\, i.$$

Therefore

$$x \in \bigcap_i (I : J_i).$$

Thus

$$\left(I : \sum_i J_i\right) \subseteq \bigcap_i (I : J_i).$$

Conversely, let

$$y \in \bigcap_i (I : J_i).$$

Then

$$y \in (I : J_i), \qquad \forall\, i,$$

so

$$yJ_i \subseteq I, \qquad \forall\, i.$$

Hence

$$y \sum_i J_i \subseteq I,$$

which implies

$$y \in \left(I : \sum_i J_i\right).$$

Therefore

$$\bigcap_i (I : J_i) \subseteq \left(I : \sum_i J_i\right).$$

Thus

$$\left(I : \sum_i J_i\right) = \bigcap_i (I : J_i).$$

□

Definition 1.43 (Radical)**.** Let I be any ideal in a ring R. Then the *radical* of I is denoted by $r(I)$ and is defined as

$$r(I) = \{a \in R : a^n \in I \text{ for some } n > 0\}.$$

Remark 1.44. $r(I)$ is an ideal of R.
Indeed, let

$$\pi : R \longrightarrow R/I$$

be the canonical projection, and let

$$\eta_{R/I}$$

be the nilradical of R/I. Then

$$\pi^{-1}(\eta_{R/I})$$

is an ideal of R, since $\eta_{R/I}$ is an ideal of R/I and π is a ring homomorphism; hence inverse images of ideals are ideals.
Now

$$\begin{aligned}
\pi^{-1}(\eta_{R/I}) &= \{a \in R : \pi(a) \in \eta_{R/I}\} \\
&= \{a \in R : a + I \in \eta_{R/I}\} \\
&= \{a \in R : a^n + I = I \text{ for some } n > 0\} \\
&= \{a \in R : a^n \in I \text{ for some } n > 0\} \\
&= r(I).
\end{aligned}$$

Thus $r(I)$ is an ideal of R.

Theorem 1.45. *Let I and J be any two ideals in a ring A. Then*

(i) $I \subseteq J \implies r(I) \subseteq r(J)$.

(ii) $I \subseteq r(I)$.

(iii) $r(IJ) = r(I \cap J) = r(I) \cap r(J)$.

(iv) $r(I) = (1) \iff I = (1)$.

(v) $r(I + J) = r(r(I) + r(J))$.

(vi) If P is prime ideal, then for any $n > 0$

$$r(P^n) = r(P) = P.$$

Proof. (i) Assume $I \subseteq J$ and let $x \in r(I)$. Then $\exists\ n > 0$ s.t. $x^n \in I \subseteq J$,
so $x^n \in J$
$\Rightarrow x \in r(J)$.
$\therefore\ r(I) \subseteq r(J)$.

(ii) Let $x \in I$, i.e. $x^1 \in I \Rightarrow x \in r(I)$.
$\therefore\ I \subseteq r(I)$.

(iii) To show: $r(IJ) = r(I \cap J) = r(I) \cap r(J)$.
Since $IJ \subseteq I \cap J$, so

$$r(IJ) \subseteq r(I \cap J). \qquad (a)$$

Let $x \in r(I \cap J)$, so $\exists\, n > 0$ s.t. $x^n \in I \cap J$
i.e. $x^n \in I$ and $x^n \in J$
$\Rightarrow x \in r(I) \cap r(J)$.
$\therefore\ r(I \cap J) \subseteq r(I) \cap r(J)$. $\qquad (b)$
Now let $x \in r(I) \cap r(J)$, then $\exists\ m, n > 0$ s.t.

$$x^n \in I \quad \text{and} \quad x^m \in J,$$

$$\Rightarrow x^n x^m \in IJ$$

or

$$x^{n+m} \in IJ \qquad \text{where } n + m > 0.$$

Hence $x \in r(IJ)$, so that

$$r(I) \cap r(J) \subseteq r(IJ). \qquad (c)$$

From (a), (b) & (c), weve

$$r(IJ) = r(I \cap J) = r(I) \cap r(J).$$

(iv) To show: $r(I) = (1) \iff I = (1)$.
If $I = (1)$, then

$$1 \in I \Rightarrow 1^n \in I\ \forall\, n > 0$$

$$\therefore\ 1 \in r(I)$$

$$\therefore\ r(I) = (1).$$

Conversely if $r(I) = (1)$,

$$\Rightarrow \exists\, n > 0 \text{ s.t. } 1^n \in I \text{ i.e. } 1 \in I$$

$$\therefore\ I = (1).$$

(v) To show $r(I + J) = r(r(I) + r(J))$.
Since by (ii), $I \subseteq r(I)$ and $J \subseteq r(J)$

$$\therefore\ I + J \subseteq r(I) + r(J)$$

$$\therefore\ r(I + J) \subseteq r[r(I) + r(J)] \qquad \text{by (i)}$$

Now let $x \in r[r(I) + r(J)] \Rightarrow \exists\, n > 0$ s.t.

$$x^n \in r(I) + r(J).$$

$$\Rightarrow x^n = a + b \quad \text{for some } a \in r(I)\ \&\ b \in r(J).$$

$$\Rightarrow \exists\ r, s > 0 \text{ s.t. } a^r \in I,\ b^s \in J,$$

so that

$$(x^n)^{r+s+1} = (a + b)^{r+s+1}$$

$$= \left(\sum_{k=0}^{r+s+1} \binom{r+s+1}{k} a^k b^{r+s+1-k} \right) \in I + J.$$

$$\therefore\ x^{n(r+s+1)} \in I + J$$

$$\Rightarrow x \in r(I + J)$$

$$\therefore\ r[r(I) + r(J)] \subseteq r[I + J] \subseteq r[r(I) + r(J)],$$

as required.

(vi) Let P be any prime ideal. Clearly $P \subseteq r(P)$.
Also if $x \in r(P)$, then $\exists\, n > 0$ s.t. $x^n \in P \Rightarrow x \in P$

$$\therefore\ r(P) \subseteq P \subseteq r(P) \Rightarrow P = r(P).$$

Now let $n > 0$. Then $P^n \subseteq P \qquad (\because P \text{ is prime ideal})$

$$\Rightarrow r(P^n) \subseteq r(P) = P.$$

If $x \in P$, then $x \cdot x \cdots x = x^n \in P^n$

$$\Rightarrow x \in r(P^n)$$

$$\Rightarrow P \subseteq r(P^n).$$

$$\therefore\ r(P^n) = P = r(P), \qquad \forall\, n > 0.$$

□

Proposition 1.46. *The radical of an ideal I is the intersection of the prime ideals in a ring A which contain I.*

Proof. Let

$$\pi : A \longrightarrow \frac{A}{I}$$

be the canonical projection and $\eta_{\frac{A}{I}}$ be the nilradical of $\frac{A}{I}$, then

$$\pi^{-1}\Big(\eta_{\frac{A}{I}}\Big) = r(I).$$

Let

$$\{\bar{P}_\alpha\}_{\alpha\in\Lambda}$$

be the collection of all prime ideals in $\frac{A}{I}$. Then

$$\eta_{\frac{A}{I}} = \bigcap_{\alpha\in\Lambda} \bar{P}_\alpha,$$

Therefore it follows that

$$r(I) = \pi^{-1}\left[\bigcap_{\alpha\in\Lambda} \bar{P}_\alpha\right],$$

i.e.,

$$r(I) = \bigcap_{\alpha\in\Lambda} \pi^{-1}(\bar{P}_\alpha). \tag{1}$$

Since inverse image of a prime ideal under ring homomorphism is a prime ideal, so

$$\pi^{-1}(\bar{P}_\alpha)$$

is a prime ideal in A, $\forall\, \alpha \in \Lambda$.
Also $\pi^{-1}(\bar{P}_\alpha)$ contains I as there is a one-one correspondence between the ideals of $\frac{A}{I}$ and the ideals of A containing I.
Therefore, by equation (1), $r(I)$ is the intersection of the prime ideals in A that contain I. □

More generally, we may define the radical $r(E)$ of any subset E of R in the same way. It is not an ideal in general. We have

$$r\Big(\cup_\alpha E_\alpha\Big) = \cup_\alpha r(E_\alpha),$$

for any family of subsets E_α of R.

Proposition 1.47. *D = set of zero-divisors of $R = \bigcup_{x\neq 0} r(\mathrm{Ann}(x))$.*

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

Example. If $R = \mathbb{Z}$, $I = (m)$, let p_i $(1 \leq i \leq r)$ be the distinct prime divisors of m. Then

$$r(I) = (p_1 \cdots p_r) = \cap_{i=1}^{r}(p_i).$$

Proposition 1.48. *Let I, J be ideals in a ring R such that $r(I), r(J)$ are coprime. Then I, J are coprime.*

Proof.

$$r(I + J) = r(r(I) + r(J)) = r(1) = (1),$$

hence $I + J = (1)$. □

1.4 Extension and Contraction of Ideals

Let $\phi : A \to B$ be a homomorphism from a ring A to a ring B. Then let I be any ideal in A; $\phi(I)$ need not be an ideal in B. For example, let ϕ be an embedding of $\mathbb{Z}$ in $\mathbb{Q}$, and take any ideal I in $\mathbb{Z}$. Then $\phi(I)$ need not be an ideal in $\mathbb{Q}$.

Definition 1.49. We define the *extension* I^e of I to be the ideal generated by $\phi(I)$, i.e. $B\phi(I)$, in B. Explicitly, I^e is the set of all sums $\sum_i y_i\phi(x_i)$, where $x_i \in I$, $y_i \in B$.

Definition 1.50. If J is an ideal of B, then $\phi^{-1}(J)$ is always an ideal of A, and we call it the contraction of J, denoted by J^c.

Remark 1.51. If J is prime in B, then J^c is prime in A.

Remark 1.52. If I is prime in A, then I^e need not be prime in B.

For example: $\phi : \mathbb{Z} \to \mathbb{Q}$, $I \neq 0$, then $I^e = (\phi(I)) = \mathbb{Q}$, which is not prime in $\mathbb{Q}$.

Proposition 1.53. *Let $\phi : A \to B$ be a ring homomorphism, and I be an ideal in A, and J be an ideal in B. Then*

i) $I \subseteq I^{ec}$,

ii) $J \supseteq J^{ce}$,

iii) $I^e = I^{ece}$,

iv) $J^c = J^{cec}$,

v) If $\mathcal{C}$ is the set of contracted ideals in A and $\mathcal{E}$ is the set of extended ideals in B, then

$$\mathcal{C} = \{I : I^{ec} = I\} \quad \text{and} \quad \mathcal{E} = \{J : J^{ce} = J\},$$

and $I \mapsto I^e$ is a bijective map of $\mathcal{C}$ onto $\mathcal{E}$, whose inverse is $J \mapsto J^c$.

Proof. i) Let $x \in I$, then $\phi(x) \in I^e$, hence $x \in I^{ec}$. Therefore $I \subseteq I^{ec}$.

ii)

$$\begin{aligned} J^{ce} &= (J^c)^e \\ &= \left(\phi^{-1}(J)\right)^e \\ &= B\phi(\phi^{-1}(J)) \\ &\subseteq BJ \\ &= J, \end{aligned}$$

so $J \supseteq J^{ce}$.

iii) To show $I^e = I^{ece}$.

By (ii), we have $I^e \supseteq I^{ece}$. Also by (i), $I^e \subseteq I^{ece}$. Hence

$$I^e = I^{ece}.$$

iv) To show $J^c = J^{cec}$.

Here, we have $J^{ce} \subseteq J$ (by (ii)), hence

$$J^{cec} \subseteq J^c.$$

Also $J^c \subseteq J^{cec}$ (by (i)). Therefore

$$J^c = J^{cec}.$$

v) Let $I \in \mathcal{C}$. Then $I = I^{ec}$. Thus

$$(I^e)^c = I^{ec} = I,$$

so $I^e \in \mathcal{E}$.

Now let $J \in \mathcal{E}$. Then $J = J^{ce}$. Hence

$$(J^c)^e = J^{ce} = J,$$

so $J^c \in \mathcal{C}$.

Therefore the map $X : \mathcal{C} \to \mathcal{E}$ given by

$$X(I) := I^e$$

is bijective, and its inverse is $J \mapsto J^c$.

□

Proposition 1.54. *Let $\phi : A \to B$ be a ring homomorphism, I_1, I_2 be ideals in A, and J_1, J_2 be ideals in B. Then*

i) $(I_1 + I_2)^e = I_1^e + I_2^e$,

ii) $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$,

iii) $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$,

iv) $(J_1 \cap J_2)^c = J_1^c \cap J_2^c$,

v) $(I_1 I_2)^e = I_1^e I_2^e$,

vi) $(J_1 J_2)^c \supseteq J_1^c J_2^c$,

vii) $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$,

viii) $(J_1 : J_2)^c \subseteq (J_1^c : J_2^c)$,

ix) $r(I)^e \subseteq r(I^e)$,

x) $r(J)^c = r(J^c)$.

Proof. i) To show $(I_1 + I_2)^e = I_1^e + I_2^e$, let

$$y \in (I_1 + I_2)^e.$$

Then

$$\begin{aligned} y \in (\phi(I_1 + I_2)) &\iff y \in (\phi(I_1) + \phi(I_2)) \\ &\iff y \in B[\phi(I_1) + \phi(I_2)] \\ &\iff y \in B\phi(I_1) + B\phi(I_2) \\ &\iff y \in I_1^e + I_2^e. \end{aligned}$$

ii) To show $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$, let

$$x \in J_1^c + J_2^c.$$

Then $x = c_1 x_1 + d_1 x_2$, where $c_1 x_1 \in \phi^{-1}(J_1)$ and $d_1 x_2 \in \phi^{-1}(J_2)$. Hence

$$\phi(x) = \phi(c_1 x_1) + \phi(d_1 x_2) \in J_1 + J_2,$$

so

$$x \in \phi^{-1}(J_1 + J_2) = (J_1 + J_2)^c.$$

iii) To show $(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e$, let

$$y \in (I_1 \cap I_2)^e.$$

Then

$$y = \sum_i c_i \phi(x_i), \quad x_i \in I_1 \cap I_2.$$

So $\phi(x_i) \in \phi(I_1) \cap \phi(I_2)$, hence

$$y \in I_1^e \cap I_2^e.$$

Therefore

$$(I_1 \cap I_2)^e \subseteq I_1^e \cap I_2^e.$$

iv) Let

$$x \in (J_1 \cap J_2)^c.$$

Then

$$\begin{aligned} x \in \phi^{-1}(J_1 \cap J_2) &\iff \phi(x) \in J_1 \cap J_2 \\ &\iff \phi(x) \in J_1 \text{ and } \phi(x) \in J_2 \\ &\iff x \in J_1^c \text{ and } x \in J_2^c \\ &\iff x \in J_1^c \cap J_2^c. \end{aligned}$$

Thus

$$(J_1 \cap J_2)^c = J_1^c \cap J_2^c.$$

v) Let $y \in (I_1 I_2)^e$

$$\begin{aligned} &\iff y \in B\phi(I_1 I_2) \\ &\iff y = \sum_i c_i \phi(x_i y_i) \\ &\iff y = \sum_i c_i \phi(x_i)\phi(y_i) \end{aligned}$$

Note that $\phi(x_i)\phi(y_i) \in I_1^e I_2^e$, so

$$y \in (I_1 I_2)^e \iff y \in I_1^e I_2^e$$

vi) To show $(J_1 J_2)^c \supseteq J_1^c J_2^c$, let $x \in J_1^c J_2^c$. Then $x \in \phi^{-1}(J_1)\phi^{-1}(J_2)$

$$\begin{aligned} &\implies x = \sum_i c_i x_i y_i \text{ where } x_i \in \phi^{-1}(J_1),\ y_i \in \phi^{-1}(J_2) \\ &\implies \phi(x) = \sum_i c_i' \phi(x_i)\phi(y_i) \\ &\implies \phi(x) \in J_1 J_2 \\ &\implies x \in \phi^{-1}(J_1 J_2) = (j_1 J_2)^c \end{aligned}$$

vii) To show $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$, let $y \in (I_1 : I_2)^e$.
Then $y \in B\phi((I_1 : I_2))$. So $y = \sum_i c_i \phi(x_i)$, where $x_i I_2 \subseteq I_1$. Hence

$$\phi(x_i)\, I_2^e \subseteq I_1^e$$

for each i, and therefore

$$y \in (I_1^e : I_2^e).$$

viii) To show $(J_1 : J_2)^c \subseteq (J_1^c : J_2^c)$, let

$$x \in (J_1 : J_2)^c.$$

Then $\phi(x) \in (J_1 : J_2)$, so

$$\phi(x)J_2 \subseteq J_1.$$

Hence

$$\phi^{-1}(\phi(x))J_2^c \subseteq J_1^c,$$

and therefore

$$x \in (J_1^c : J_2^c).$$

ix) To show $r(I)^e \subseteq r(I^e)$, let $y \in r(I)^e$. Then $y = \sum_i c_i\phi(x_i)$, where $x_i^{m_i} \in I$ for some $m_i > 0$. Then

$$[\phi(x_i)]^{m_i} \in \phi(I) \subseteq (\phi(I)) = I^e.$$

So $\phi(x_i) \in r(I^e)$. Hence $y \in r(I^e)$.

x) To show $r(J)^c = r(J^c)$, let $x \in (r(J))^c$. Then

$$\begin{aligned} x \in \phi^{-1}(r(J)) &\iff \phi(x) \in r(J) \\ &\iff \phi(x)^m \in J \text{ for some } m > 0 \\ &\iff \phi(x^m) \in J \text{ for some } m > 0 \\ &\iff x^m \in \phi^{-1}(J) = J^c \\ &\iff x \in r(J^c). \end{aligned}$$

Thus $(r(J))^c = r(J^c)$.

□

Remark 1.55. Converse of (ix).
Consider $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$ to be a trivial homomorphism, i.e. $\phi(x) = 0x$ for all $x \in \mathbb{Z}_4$.
Let $I = \{0, 2\} = (2)$.
Then

$$I^e = (0) = 0 \qquad \Rightarrow \qquad r(I^e) = \{0, 2\},$$

and

$$r(I) = \{0, 2\},$$

and

$$(r(I))^e = 0.$$

So

$$r(I^e) \neq (r(I))^e.$$

Chapter 2

Modules

One of the things which distinguishes the modern approach to commutative algebra is the greater emphasis on modules, rather than only on ideals. This extra flexibility gives greater clarity and simplicity. For instance, an ideal I of a ring R and its quotient ring R/I are both examples of R-modules and, to a certain extent, can be treated on an equal footing. In this chapter we give the definition and elementary properties of modules. We also give a brief treatment of direct sums and finitely generated modules, together with a discussion of Nakayama's lemma and its consequences.

2.1 Modules and module homomorphisms

Let R be a commutative ring with identity.
An *R-module* is an abelian group M (written additively) together with a scalar multiplication map $R \times M \to M$, $(r, m) \mapsto rm$, such that for all $r, s \in R$ and $x, y \in M$,

$$\begin{aligned} r(x+y) &= rx + ry, \\ (r+s)x &= rx + sx, \\ (rs)x &= r(sx), \\ 1x &= x. \end{aligned}$$

Equivalently, M is an abelian group together with a ring homomorphism $R \to E(M)$, where $E(M)$ denotes the ring of endomorphisms of the abelian group M.
An R-module M is called *unitary* if $1x = x$ for every $x \in M$. Throughout this chapter, all modules are assumed to be unitary.
The notion of a module is a common generalization of several familiar concepts, as the following examples show.

An ideal I of R is an R-module. In particular, R itself is an R-module.

If R is a field k, then an R-module is the same thing as a k-vector space.

If $R = \mathbb{Z}$, then a $\mathbb{Z}$-module is the same thing as an abelian group, where nx means $x + \cdots + x$ (n times) for $n \geq 0$.

If $R = k[x]$, where k is a field, then an R-module is a k-vector space together with a linear transformation.

If I is an ideal of R, then the quotient ring R/I is naturally an R-module under

$$r(x + I) = rx + I.$$

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

$$f(x+y) = f(x) + f(y),$$
$$f(rx) = rf(x)$$

for all $r \in R$ and all $x, y \in M$.
Thus f is a homomorphism of abelian groups which commutes with the action of each $r \in R$. If R is a field, then an R-module homomorphism is just a linear transformation of vector spaces.
The composition of R-module homomorphisms is again an R-module homomorphism.
The set of all R-module homomorphisms from M to N may itself be turned into an R-module as follows. For $f, g \in \mathrm{Hom}_R(M, N)$ and $r \in R$, define

$$(f+g)(x) = f(x) + g(x),$$
$$(rf)(x) = r \cdot f(x)$$

for all $x \in M$. This R-module is denoted by $\mathrm{Hom}_R(M, N)$, or simply $\mathrm{Hom}(M, N)$ when there is no ambiguity about the ring R.
Homomorphisms $u : M' \to M$ and $v : N \to N''$ induce maps

$$\overline{u} : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M', N), \qquad \overline{v} : \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N''),$$

defined by

$$\overline{u}(f) = f \circ u, \qquad \overline{v}(f) = v \circ f.$$

These maps are R-module homomorphisms.
For any R-module M, there is a natural isomorphism

$$\mathrm{Hom}_R(R, M) \cong M.$$

Indeed, any R-module homomorphism $f : R \to M$ is uniquely determined by $f(1)$, and any element of M may occur as $f(1)$.

2.2 Submodules and quotient modules

A subset $M' \subseteq M$ is called a *submodule* of M if M' is a subgroup of the additive group of M and $rm' \in M'$ for all $r \in R$ and all $m' \in M'$.
If M' is a submodule of M, then the quotient group M/M' becomes an R-module under

$$r(m + M') = rm + M'.$$

The R-module M/M' is called the *quotient module* of M by M'. The natural map $M \to M/M'$ is an R-module homomorphism.
There is a one-to-one order-preserving correspondence between submodules of M containing M', and submodules of M/M'. This is the module-theoretic analogue of the corresponding statement for ideals.
If $f : M \to N$ is an R-module homomorphism, the *kernel* of f is

$$\mathrm{Ker}(f) = \{x \in M : f(x) = 0\},$$

and is a submodule of M. The *image* of f is

$$\mathrm{Im}(f) = f(M),$$

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 $M' \subseteq \mathrm{Ker}(f)$, then f induces an R-module homomorphism

$$\overline{f} : M/M' \to N$$

defined by

$$\overline{f}(x + M') = f(x).$$

The kernel of $\overline{f}$ is $\mathrm{Ker}(f)/M'$. In particular, taking $M' = \mathrm{Ker}(f)$, we obtain an isomorphism of R-modules

$$M/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

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

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

Proof. Define $\theta : L/N \to L/M$ by $\theta(x + N) = x + M$. This is a well-defined R-module homomorphism onto L/M, and its kernel is M/N. Hence the result follows. □

Proposition 2.2. *If M_1 and M_2 are submodules of M, then*

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

Proof. Consider the composite homomorphism

$$M_2 \to M_1 + M_2 \to (M_1 + M_2)/M_1.$$

It is surjective, and its kernel is $M_1 \cap M_2$. The result follows. □

2.3 Operations on submodules

Most of the operations on ideals considered in Chapter 1 have their counterparts for modules. Let $(M_i)_{i\in I}$ be a family of submodules of M. Their sum $\sum_i M_i$ is the set of all finite sums $\sum_i x_i$, where $x_i \in M_i$ for all $i \in I$, and almost all x_i are zero. It is the smallest submodule of M containing all the M_i.
The intersection $\bigcap_i M_i$ is again a submodule of M. Thus the submodules of M form a complete lattice with respect to inclusion.
We cannot in general define the product of two submodules, but we can define the product IM, where I is an ideal of R and M is an R-module; it is the set of all finite sums $\sum_j a_j x_j$ with $a_j \in I$ and $x_j \in M$, and is a submodule of M.

Definition 2.3. If N and P are submodules of M, we define

$$(N : P) = \{r \in R : rP \subseteq N\}.$$

It is an ideal of R. In particular,

$$(0 : M) = \{r \in R : rM = 0\},$$

which is called the *annihilator* of M and is denoted by $\mathrm{Ann}(M)$.
If $I \subseteq \mathrm{Ann}(M)$, then M may be regarded as an R/I-module, defined by

$$\overline{r}\, x = rx,$$

where $\overline{r}$ is the image of $r \in R$ in R/I. This is well-defined because $IM = 0$.

Definition 2.4. An R-module M is called *faithful* if $\mathrm{Ann}(M) = 0$. If $\mathrm{Ann}(M) = I$, then M is faithful as an R/I-module.

Exercise 2.5. 1. $\mathrm{Ann}(M+N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

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

If x is an element of M, the set of all multiples rx ($r \in R$) is a submodule of M, denoted by Rx or (x). If $M = \sum_{i \in I} Rx_i$, the x_i are said to be a *set of generators* of M; this means that every element of M can be expressed as a finite linear combination of the x_i with coefficients in R. An R-module M is said to be *finitely generated* if it has a finite set of generators.

2.4 Direct sums and products

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

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2), \qquad r(x, y) = (rx, ry).$$

More generally, if $(M_i)_{i \in I}$ is any family of R-modules, we can define their direct sum $\bigoplus_{i \in I} M_i$; its elements are families $(x_i)_{i \in I}$ such that $x_i \in M_i$ for each $i \in I$ and almost all x_i are zero. If we drop the restriction on the number of non-zero components, we obtain the direct product $\prod_{i \in I} M_i$. The direct sum and direct product are the same if the index set I is finite, but not otherwise in general.
If $M_1, \ldots, M_n$ are submodules of M, we say that M is the *direct sum* of $M_1, \ldots, M_n$ if every element $m \in M$ can be written in a unique manner as

$$m = m_1 + \cdots + m_n,$$

where $m_i \in M_i$ for each i. In this case we write

$$M = M_1 \oplus \cdots \oplus M_n.$$

As in the case of vector spaces, if $M = M_1 \oplus \cdots \oplus M_n$, then M is isomorphic, as an R-module, to the set of all n-tuples $(m_1, \ldots, m_n)$ with $m_i \in M_i$, where addition and scalar multiplication are componentwise.

2.5 Free, cyclic, and finitely generated modules

A free R-module is one which is isomorphic to a direct sum of copies of R. A finitely generated free R-module is therefore isomorphic to R^n for some $n \geq 0$. Conventionally, R^0 is the zero module.

Definition 2.6. An R-module M is said to be *cyclic* if there exists an element $m_0 \in M$ such that every element $m \in M$ is of the form

$$m = rm_0$$

for some $r \in R$.

For $R = \mathbb{Z}$, a cyclic R-module is nothing more than a cyclic abelian group.
We shall also need the following standard characterization.

Proposition 2.7. *An R-module M is finitely generated if and only if it is isomorphic to a quotient of R^n for some integer $n > 0$.*

Proof. If $x_1, \ldots, x_n$ generate M, define $\phi : R^n \to M$ by

$$\phi(r_1, \ldots, r_n) = r_1 x_1 + \cdots + r_n x_n.$$

Then ϕ is an R-module homomorphism onto M, so

$$M \cong R^n / \ker(\phi).$$

Conversely, if M is a quotient of R^n, then the images of the standard basis vectors generate M. □

Proposition 2.8. *Let M be a finitely generated R-module, let I be an ideal of R, and let ϕ be an R-module endomorphism of M such that $\phi(M) \subseteq IM$. Then ϕ satisfies an equation of the form*

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

where $a_1, \ldots, a_n \in I$.

Proof. Let $x_1, \ldots, x_n$ be a set of generators of M. Since $\phi(x_i) \in IM$, we may write

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

with $a_{ij} \in I$. Hence

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

for each i. Multiplying by the adjoint of the matrix $(\delta_{ij}\phi - a_{ij})$ shows that $\det(\delta_{ij}\phi - a_{ij})$ annihilates each x_i, hence is the zero endomorphism of M. Expanding the determinant gives the desired relation. □

Corollary 2.9. *Let M be a finitely generated R-module and let I be an ideal of R such that $IM = M$. Then there exists $x \in R$ with $x \equiv 1 \pmod{I}$ and*

$$xM = 0.$$

Proof. Apply the preceding proposition to the identity endomorphism of M. □

2.6 Nakayama's lemma

Let $\mathfrak{J}$ denote the Jacobson radical of R.

Proposition 2.10 (Nakayama's lemma)**.** *Let M be a finitely generated R-module and let I be an ideal of R contained in $\mathfrak{J}$. Then*

$$IM = M \implies M = 0.$$

Proof. By the previous corollary, there exists $x \equiv 1 \pmod{\mathfrak{J}}$ such that $xM = 0$. Since x is a unit, it follows that $M = 0$. □

Second proof. Suppose $M \neq 0$, and let $u_1, \ldots, u_n$ be a minimal set of generators of M. Since $IM = M$, each u_i can be written as a linear combination of the u_j with coefficients in I. By a standard elimination argument, one obtains a contradiction to minimality. □

Corollary 2.11. *Let M be a finitely generated R-module, N a submodule of M, and $I \subseteq \mathfrak{J}$ an ideal. Then*

$$M = IM + N \implies M = N.$$

Proof. Apply Nakayama's lemma to M/N, observing that

$$I(M/N) = (IM + N)/N.$$

□

If R is a local ring, let $\mathfrak{m}$ be its maximal ideal and $k = R/\mathfrak{m}$ its residue field. Let M be a finitely generated R-module. Then $M/\mathfrak{m}M$ is naturally a k-vector space, and hence finite-dimensional.

Proposition 2.12. *Let $x_1, \ldots, x_n$ be elements of M whose images in $M/\mathfrak{m}M$ form a basis of this vector space. Then $x_1, \ldots, x_n$ generate M.*

Proof. Let N be the submodule generated by $x_1, \ldots, x_n$. The images of the x_i generate $M/\mathfrak{m}M$, so

$$N + \mathfrak{m}M = M.$$

By the previous corollary, $N = M$. □

Corollary 2.13. *If M is a finitely generated module over a local ring R, then the minimum number of generators of M equals the dimension of the vector space $M/\mathfrak{m}M$ over $k = R/\mathfrak{m}$.*

Remarks

Modules provide the natural setting for many constructions in commutative algebra. Ideals, quotient rings, kernels, images, generators, and exactness are all most naturally formulated in the language of modules. This point of view will be used repeatedly in later chapters, especially in the study of Noetherian rings, localization, and algebraic number theory.