Definitions, Propositions and Theorems in Commutative Algebra

TRISCT

Contents

All rings are considered to be commutative rings with identity by default, unless otherwise specified.

1 General Ring Theory

1.1 Definitions

Ring Let R be a nonempty set equipped with an addition and a multiplication such that R is an abelian group under addition and multiplication is distributive over addition.

(i) If R is a semigroup under multiplication, then R is called a **ring**.

(ii) If R is a monoid under multiplication, then R is called a **ring with identity**.

(iii) If R is a commutative semigroup under multiplication, then E is called a **commutative ring**.

However, in this part from now on, we will use the word "ring" to refer to a commutative ring with identity and ignore other kinds of rings.

Ring homomorphism A **ring homomorphism** f is a mapping between two rings such that it

(i) **preserves addition**: $f(x+y) = f(x) + f(y)$;

(ii) **preserves multiplication**: $f(xy) = f(x)f(y)$;

(iii) **preserves the identity**: $f(1) = 1$;

Subring A **subring** is a subset of a ring that is a ring (with identity) in its own right (with operations inherited from the original ring).

Multiplicatively closed subset A **multiplicatively closed subset** S of a ring is a subset of the ring such that $1 \in S$ and S is closed under multiplication.

Ideal An **ideal** $\mathfrak{a}$ of a ring R is a subset such that

(i) $\mathfrak{a}$ is an additive subgroup;

(ii) $R\mathfrak{a} \subset \mathfrak{a}$.

Ideals can be operated on.

(i) (**Sum**) The **sum** $\mathfrak{a}+\mathfrak{b}$ of two ideals $\mathfrak{a}, \mathfrak{b}$ is the set

$$\mathfrak{a}+\mathfrak{b} = \{a+b : a \in \mathfrak{a}, b \in \mathfrak{b}\}$$

It is an ideal. The sum of any family is also an ideal.

(ii) (**Intersection**) The **intersection** $\mathfrak{a} \cap \mathfrak{b}$ of two ideal $\mathfrak{a}, \mathfrak{b}$ is the intersection of them as sets. It is an ideal. The intersection of any family is also an ideal.

(ii') The union of ideals is in general not an ideal. However, the union of an ascending chain is an ideal.

(iii) (**Product**) The **product** $\mathfrak{a}\mathfrak{b}$ of two ideals $\mathfrak{a}, \mathfrak{b}$ is the set

$$\mathfrak{a}\mathfrak{b} = \{\text{Finite sum } \sum_i a_i b_i : a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$$

In other words, $\mathfrak{a}\mathfrak{b}$ is the ideal generated by all products of elements of $\mathfrak{a}$ and $\mathfrak{b}$.

(iv) (**Radical**) The **radical** $\sqrt{\mathfrak{a}} = \operatorname{rad}(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is the set

$$\{a \in R : a^n \in \mathfrak{a} \text{ for some } n \geqslant 1\}$$

It is an ideal.

(v) (**Quotient**) The **ideal quotient** $(\mathfrak{a} : \mathfrak{b})$ of two ideals $\mathfrak{a}, \mathfrak{b}$ is the set

$$\{x \in R : x\mathfrak{b} \subset \mathfrak{a}\}$$

It is an ideal. In particular, $(0 : \mathfrak{b})$ is called the **annihilator** of $\mathfrak{b}$ and is denoted by $\operatorname{ann}(\mathfrak{b})$.

Note 1.1. Somehow it feels like

$$x\mathfrak{b} \subset \mathfrak{a} \implies x \in \frac{\mathfrak{a}}{\mathfrak{b}}$$

I guess that's why they call such x the ideal quotient, because it certainly seems like a quotient.

Quotient ring If $\mathfrak{a}$ is an ideal of a ring R, then $R/\mathfrak{a}$ has well-defined addition and multiplication that makes it into a ring, called the **quotient ring**.

Descriptors of elements Elements often have the following descriptors.

(i) (**Zero-divisor**) x is called a **zero-divisor** if $x \neq 0$ and $\exists y \in R, y \neq 0$, but $xy = 0$.

(ii) (**Nilpotent**) x is **nilpotent** if $x^n = 0$ for some $n \geqslant 1$.

(iii) (**Unit**) x is called a **unit** if x has a multiplicative inverse x^{-1}. The set of all units are denoted by R^*, which is a multiplicative subgroup of R.

(iv) (**Divisor**) If $a, b \in R$ and there exists $y \in R$ such that $ay = b$, then a is a **divisor** of b and b is a **multiple** of a, and we write $a\big|b$.

(v) (**Associate**) If $a\big|b$ and $b\big|a$, then a, b are said to be **associates** and we write $a \sim b$. This relation is an equivalent relation.

(vi) (**Prime**) If p is such that $p \notin R^* \cup \{0\}$, and

$$p\big|ab \implies p\big|a \text{ or } p\big|b$$

then p is called a **prime** element.

(vii) (**Irreducible**) If a is such that $a \notin R^* \cup \{0\}$, and

$$a = bc \implies b \in R^* \text{ or } c \in R^*$$

then a is called an **irreducible** element.

(viii) (**Regular**) An element $a \in R$ is called **regular** if $a \neq 0$, a is not a zero-divisor.

(ix) (**Quasi-regular**) An element $a \in R$ is called **quasi-regular** if $1 + a \in R^*$.

Descriptors of ideals and specific ideals Ideals often have the following descriptors.

(i) (**Principal ideal**) An ideal $\mathfrak{a}$ is called **principal** if it has the form $\mathfrak{a} = Rx = (x)$ for some $x \in R$. In other words, a principal ideal is an ideal generated by a single element.

Note 1.2. Its correspondence is the cyclic submodule.

(ii) (**Prime ideal**) An ideal $\mathfrak{p}$ is called **prime** if $\mathfrak{p} \neq (1)$ and

$$xy \in \mathfrak{p} \implies x \in \mathfrak{p} \text{ or } y \in \mathfrak{p}$$

(iii) (**Coprime/comaximal ideals**) Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are called **coprime** or **comaximal** if $\mathfrak{a} + \mathfrak{b} = (1)$.

(iii) (**Primary ideal**) An ideal $\mathfrak{q}$ is called **primary** if $\mathfrak{q} \neq (1)$ and

$$xy \in \mathfrak{q} \implies x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n \geqslant 1$$

For more about primary ideals, see Sect.**??**.

(iv) (**Maximal ideal**) An ideal $\mathfrak{m}$ is called **maximal** if $\mathfrak{m} \neq (1)$ and for any ideal $\mathfrak{a}$

$$\mathfrak{m} \subset \mathfrak{a} \subset (1) \implies \mathfrak{a} = \mathfrak{m} \text{ or } \mathfrak{a} = (1)$$

(v) (**Nilradical**) The **nilradical** of a ring R is the set of all nilpotent elements of R, or equivalently, the intersection of all prime ideals of R. It is an ideal, and it is denoted by $\mathrm{nilrad}(R)$

(vi) (**Jacobson radical**) The **Jacobson radical** of a ring R is the intersection of all maximal ideals of R. It is an ideal, and it is denoted by $\mathrm{rad}(R)$

(vii) (**Quasi-regular**) An ideal $\mathfrak{a} \subset R$ is called **quasi-regular** if every $a \in \mathfrak{a}$ is quasi-regular.

Descriptors of a ring Let R be a ring.

(i) (**Local, semi-local**) If R has only one maximal ideal $\mathfrak{m}$, then R is called a **local ring**. The field $R/\mathfrak{m}$ is called the **residue field** of R. If R has a finite number of maximal ideals then it is called **semi-local**

(ii) (**Integral domain, entire ring**) If R has no zero-divisors, then R is called an **integral domain** or **entire ring**.

(iii) (**Field**) If $1 \neq 0$ and $R^* = R \backslash \{0\}$, then R is called a **field**.

(iv) (**Unique factorization domain**) If R is an integral domain and any element in R can be written as a product of irreducible elements and a unit, and this representation is unique up to reordering and associates, then R is called a **unique factorization domain**.

(v) (**Principal ideal domain**) If R is an integral domain and each ideal of R is a principal ideal, then R is called a **principal ideal domain**.

1.2 Propositions

Prime ideal Let R be a ring.

(i) (**Equivalent conditions**)

$$\mathfrak{p} \text{ is prime } \iff R/\mathfrak{p} \text{ is an integral domain}$$

(ii) (**Complete inclusion property**[1] **1**) Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_n$ be prime ideals, and $\mathfrak{a}$ any ideal. Then

$$\mathfrak{a} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i \implies \mathfrak{a} \subset \mathfrak{p}_i \text{ for some } \mathfrak{p}_i$$

[1] Name invented by me.

(iii) (**Complete inclusion property 2**) Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be ideals, and $\mathfrak{p}$ a prime ideal. Then

$$\bigcap_{i=1}^{n} \mathfrak{a}_i \subset \mathfrak{p} \implies \text{some } \mathfrak{a}_i \subset \mathfrak{p}$$

(iv) (**Under a homomorphism**) The preimage of a prime ideal under a homomorphism is also prime, while the image may not be.

Counterexample 1.1. Consider $\mathbb{Z} \to \mathbb{Z}/(6)$. Then (0) is prime in $\mathbb{Z}$ but $(0)/(6)$ is not prime in $\mathbb{Z}/(6)$.

Maximal ideal Let R be a ring.

(i) (**Equivalent conditions**)

$$\mathfrak{m} \text{ is maximal} \iff R/\mathfrak{m} \text{ is a field}$$

(ii) There exists at least one maximal ideal. In particular, for any $\mathfrak{a} \neq R$, there exists a maximal ideal $\mathfrak{m} \supset \mathfrak{a}$. And for any nonunit element a, there exists a maximal ideal $\mathfrak{m} \ni a$.

(iii) (**Test of localness 1**) If an ideal $\mathfrak{m} \neq R$ is such that $R - \mathfrak{m} \subset R^*$, then $\mathfrak{m}$ is its unique maximal ideal.

(iv) (**Test of localness 2**) If a maximal ideal $\mathfrak{m} \neq R$ is such that $1 + \mathfrak{m} \subset R^*$, then $\mathfrak{m}$ is its unique maximal ideal.

(v) (**Under a homomorphism**) The preimage of a maximal ideal under a homomorphism is also maximal, while the image may not be.

Nilradical Let R be a ring.

(i) (**Equivalent conditions**)

$$\operatorname{nilrad}(R) = \{x \in R : \exists n \geqslant 1,\ x^n = 0\} = \bigcap_{\text{prime } \mathfrak{p}} \mathfrak{p}$$

(ii) $\operatorname{nilrad}(R/\operatorname{nilrad}(R)) = 0$, that is, $R/\operatorname{nilrad}(R)$ has no nonzero nilpotent elements.

Jacobson radical Let R be a ring.

(i) (**Equivalent conditions**)

$$\operatorname{rad}(R) = \{x \in R : \forall y \in R,\ 1 - xy \in R^*\} = \bigcap_{\text{maximal } \mathfrak{m}} \mathfrak{m}$$

(ii) $\mathrm{rad}(R/\mathrm{rad}(R)) = 0$

Ideal radical Let $\mathfrak{a} \subsetneq R$ be an ideal.

- (**Equivalent conditions**)

$$\sqrt{\mathfrak{a}} = \bigcap_{\substack{\text{prime } \mathfrak{p} \\ \mathfrak{p} \supset \mathfrak{a}}} \mathfrak{p}$$

Laws of usual operations

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

Note **1.3.** In general, $\mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) \neq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$, except in $\mathbb{Z}$.

(ii) (**Modular law**) $\mathfrak{b} \subset \mathfrak{a}$ or $\mathfrak{c} \subset \mathfrak{a} \implies \mathfrak{a} \cap (\mathfrak{b}+\mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$

(iii) $(\mathfrak{a}+\mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b}$

(iv) $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$ and further more

$$\mathfrak{a}, \mathfrak{b} \text{ are coprime } \implies \mathfrak{a}\mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}$$

If $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ are ideals, then

$$\mathfrak{a}_i, \mathfrak{a}_j \text{ are coprime when } i \neq j \implies \prod \mathfrak{a}_i = \bigcap \mathfrak{a}_i$$

Laws of operations regarding ideal quotients

(i) $\mathfrak{a} \subset (\mathfrak{a} : \mathfrak{b})$

(ii) $(\mathfrak{a} : \mathfrak{b})\mathfrak{b} \subset \mathfrak{a}$

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

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

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

Laws of taking the radical

(i) $\mathfrak{a} \subset \mathfrak{b} \implies \sqrt{\mathfrak{a}} \subset \sqrt{\mathfrak{b}}$

(ii) $\mathfrak{a} \subset \sqrt{\mathfrak{a}}$

Note **1.4.** The radical goes larger.

(iii) $\sqrt{\sqrt{\mathfrak{a}}} = \sqrt{\mathfrak{a}}$

(iv) $\sqrt{\mathfrak{a}\mathfrak{b}} = \sqrt{\mathfrak{a} \cap \mathfrak{b}} = \sqrt{\mathfrak{a}} \cap \sqrt{\mathfrak{b}}$

(v) $\sqrt{\mathfrak{a}} = (1) \iff \mathfrak{a} = (1)$

(vi) $\sqrt{\sqrt{\mathfrak{a}} + \sqrt{\mathfrak{b}}} = \sqrt{\mathfrak{a}+\mathfrak{b}}$

(vii) If $\mathfrak{p}$ is prime, then $\forall n \geqslant 1$, $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$

1.3 Theorems

Chinese Remainder Theorem Let $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ be ideals of R. Then the homomorphism

$$\begin{array}{rcl} \phi : R & \to & \frac{R}{\mathfrak{a}_1} \times \cdots \times \frac{R}{\mathfrak{a}_n} \\ x & \mapsto & (\overline{x}, \cdots, \overline{x}) \end{array}$$

satisfies

(i) ϕ is surjective $\iff$ $\mathfrak{a}_1, \cdots, \mathfrak{a}_n$ are pairwise coprime.

(ii) ϕ is injective $\iff$ $\bigcap_i \mathfrak{a}_i = 0$.

2 General Module Theory

2.1 Definitions

Module An R-**module** is a nonempty set M, together with an addition on it, and a scalar multiplication with some ring R such that

(i) M is an abelian group under addition;

(ii) Left and right distributivity;

(iii) Scalar associativity $(rs)u = r(su)$;

(iv) $1u = u$.

If A, B are rings and M is both an A-module and a B-module, and M the scalar multiplications by A, B are compatible in the sense that $a(xb) = (ax)b$, then M is called an (A, B)**-bimodule**. A subset N of an R-module M that is an R-module in its own right (with operations inherited from M) is called a **submodule**. For any submodule N, operations on M/N are well-defined and M/N is also an R-module called the **quotient module**.

Operations Let M be an R-module ,$N, \{M_i\}$ submodules of M, and $\mathfrak{a} \subset R$ an ideal. Then we can define the following.

(i) The **sum** $\sum_i M_i$ of submodules M_i is defined to be all finite sums $\sum_i x_i$ with $x_i \in M_i$. It is a submodule.

(ii) The **intersection** $\bigcap_i M_i$ of submodules M_i is defined to the intersection of them as sets. It is a submodule.

(iii) The **product** $\mathfrak{a}N$ of an ideal and a submodule is defined to be all finite sums $\sum_i a_i x_i$ with $a_i \in \mathfrak{a},\ x_i \in N$. It is a submodule.

Homomorphism A **(module) homomorphism** is a mapping $\phi : M \to N$ from an R-module M to another R-module N, which satisfies $\phi(rx + sy) = r\phi(x) + s\phi(y)$. The following important sets are respectively called:

(i) **Kernel** of ϕ:
$$\ker\phi = \{x \in M : \phi(x) = 0\}$$

(ii) **Image** of ϕ:
$$\mathrm{im}\phi = \phi(M)$$

(iii) **Cokernel** of ϕ:
$$\mathrm{coker}\phi = N/\mathrm{im}\phi$$

(iv) **Coimage** of ϕ:
$$\mathrm{coim}\phi = M/\ker\phi$$

Module quotient Let M be an R-module and N, P submodules of M. The set $(N : P)$ is defined as

$$(N : P) = \{a \in R : aP \subset N\}$$

It is an ideal of R. I myself call it the **module quotient**.

Annihilator The **annihilator** $\mathrm{ann}(M)$ of an R-module M is

$$\mathrm{ann}(M) = (0 : M) = \{a \in R : aM = 0\}$$

Descriptors of a module An R-module M is called

(i) **faithful** if $\mathrm{ann}(M) = 0$;

(ii) **cyclic** if $M = Rx$ for some $x \in M$;

(iii) **finitely generated** if $M = Rx_1 + \cdots + Rx_n$ for some finitely many $x_1, \cdots, x_n \in M$;

(iv) **simple** or **irreducible** if $M \neq 0$ and M has no nontrivial submodule;

Counterexample 2.1. There exists a non-simple module that contains no simple submodule.Q: what

(v) **semi-simple** if it is the sum of all simple submodules, or equivalently, the direct sum of some of its simple submodules;

(vi) **indecomposable** if $M = M_1 \oplus M_2 \implies M_1 = 0$ or $M_2 = 0$;

(vii) **free** if M has a basis, or equivalently, if there exists a set $\mathcal{B}$ such that $M \cong (R^{\mathcal{B}})_0$.

Note 2.1. For modules concerning torsion, see Sect.??.

Direct family of homorphisms Let M be an R-module and $\{M_i\}$ a family of R-modules. If the homomorphisms $\{\iota_i, \pi_i\}$:

$$M_i \xrightarrow{\iota_i} M \xrightarrow{\pi_i} M_i$$

are such that

(i) $\pi_i \iota_i = \mathrm{id}_{M_i}$;

(ii) $\beta \neq i \implies \pi_\beta \iota_i = 0$,

then $\{\iota_i, \pi_i\}$ is called a **direct family of homomorphisms**.

Direct sum/coproduct The **direct sum** or **coproduct** of a family $\{M_i\}_{i \in I}$ of R-modules can be defined in the following manners.

(i) (**As a direct family of homomorphisms**) The **direct sum** or **coproduct** of a family $\{M_i\}$ of R-modules is any triplet (M, ι_i, π_i), where M is an R-module and ι_i, π_i are homomorphisms $M_i \xrightarrow{\iota_i} M \xrightarrow{\pi_i} M_i$, satisfying

(i) $\{\iota_i, \pi_i\}$ is a direct family;

(ii) $\forall x \in M$, x can be written as a finite sum $x = \sum \iota_i x_i$ with $x_i \in M_i$.

More precisely, we say $\{\iota_i, p_i\}$ yields a **representation of M as a direct sum of M_i**.

Note 2.2. In this case, the following are true.

(a) x has a unique form as a sum;

(b) π_i can be defined using ι_i alone;

(c) All direct sums under definition (i) are isomorphic.

(ii) (**By the universal property**) The **direct sum** or **coproduct** of a family $\{M_i\}$ of R-modules is any pair (M, ι_i), where M is an R-module and $\iota_i : M_i \to M$ is are homomorphisms, such that for any R-module X and homomorphisms $\phi_i : M_i \to X$, there exists a unique homomorphism $\psi : M \to X$ such that the following diagram commutes for each i.

$$\begin{tikzcd}
M_i \arrow[r, "\iota_i"] \arrow[dr, "\phi_i"'] & M \arrow[d, "\psi"] \\
 & X
\end{tikzcd}$$

Note 2.3. All direct sums under definition (ii) are isomorphic.

Note 2.4. Definitions (i) and (ii) are equivalent. For (i) $\Longrightarrow$ (ii), notice that the following diagram commutes

$$\begin{tikzcd}
 & M \arrow[d, "\pi_i"] \\
M_i \arrow[ur, "\iota_i"] \arrow[r, "\mathrm{id}_{M_i}"'] \arrow[dr, "\phi_i"'] & M_i \arrow[d, "\phi_i"] \\
 & X
\end{tikzcd}$$

and that $\psi = \sum_i \phi_i \pi_i$ (the sum is well-defined, because each member of M is a finite sum). For (ii) $\Longrightarrow$ (i), one can show it by setting $X = M_i$ and $\phi_i = \mathrm{id}_{M_i}$.

(iii) (**By construction**) In practice, we need to prove such a direct sum exists, and even construct one. The construction is as follows. Let M be the set

$$M = \left\{ f : I \to \bigcup_i M_i \;\middle|\; f(i) \in M_i, f \text{ has finite support} \right\}$$

and M can be turned into an R-module by defining addition and scalar multiplication. It can be verified that M satisfies (ii)[2] (Q: what are the homomorphisms ι_i?), and hence (i). This direct sum is usually denoted by $\bigoplus_{i \in I} M_i$, or by $\coprod_{i \in I} M_i$ if we want to call it the coproduct.

Direct product The **direct product** of a family $\{M_i\}_{i \in I}$ of R-modules can be defined in the following manners.

(i) (**As a direct family of homomorphisms**) The **direct product** of a family $\{M_i\}$ of R-modules is any triplet (M, ι_i, π_i), where M is an R-module and ι_i, π_i are homomorphisms $M_i \xrightarrow{\iota_i} M \xrightarrow{\pi_i} M_i$, satisfying

(i) $\{\iota_i, \pi_i\}$ is a direct family;

(ii) $\forall \{x_i \in M_i\},\ \exists!\, x \in M,\ x_i = \pi_i x, \{x_i\}$.

More precisely, we say $\{\iota_i, p_i\}$ yields a **representation of M as a direct product of M_i.**

Note 2.5. In this case, the following are true.

(a) ι_i can be defined using π_i alone;

(b) All direct products under definition (i) are isomorphic.

[2] See assignment 3.5

(ii) (**By the universal property**) The **direct product** of a family $\{M_i\}$ of R-modules is any pair (M, π_i), where M is an R-module and $\pi_i : M \to M_i$ is are homomorphisms, such that for any R-module X and homomorphisms $\phi_i : X \to M_i$, there exists a unique homomorphism $\psi : X \to M$ such that the following diagram commutes for each i.

$$\begin{tikzcd}
M_i & M \arrow[l, "\pi_i"'] \\
 & X \arrow[ul, "\phi_i"] \arrow[u, "\psi"']
\end{tikzcd}$$

Note 2.6. All direct sums under definition (ii) are isomorphic.

Note 2.7. Definitions (i) and (ii) are equivalent.

(iii) (**By construction**) In practice, we need to prove such a direct product exists, and even construct one. The construction is as follows. Let M be the set

$$M = \left\{ f : I \to \bigcup_i M_i \;\middle|\; f(i) \in M_i \right\}$$

and M can be turned into an R-module by defining addition and scalar multiplication. It can be verified that M satisfies (ii)[3] (Q: what are the homomorphisms ι_i?), and hence (i). This direct product is usually denoted by $\prod_{i \in I} M_i$.

Note 2.8. A more intuitive way of defining the direct product and the direct sum is to say that

(i) Any collection of homomorphisms from a family of modules can be factored through the direct sum, or that the direct sum is the most *universal* injector from a family;

(ii) Any projection onto a family of modules can be factored through the direct product, or that the direct product is the most *universal* projector onto a family.

2.2 Propositions

Properties of $(N : P)$ Let M, N and P be R-modules.

(i) $\text{ann}(M) = 0 \implies M$ is faithful as an $R/\text{ann}(M)$-module;

(ii) $\text{ann}(M + N) = \text{ann}(M) + \text{ann}(N)$;

[3] See assignment 3.5

(iii) $(N : P) = \operatorname{ann}((N + P)/N)$.

Change of base ring Let M be an R-module. If there is a ring homomorphism $\phi : A \to R$, then M is also an A-module under

$$ax = \phi(a)x$$

Note that the two structures are compatible, hence M is an (R, A)-bimodule (if we formally write the multiplication by A on the right).

Note 2.9. In the language of category, this operation is a functor from $\mathbf{Mod}_R$ to $\mathbf{Mod}_A$.

Submodules Submodules can be operated on.

(i) (**Sum**) The sum $\sum_i M_i$ of an arbitrary family of submodules $\{M_i\}$ is a submodule.

(ii) (**Intersection**) The intersection $\bigcap_i M_i$ of an arbitrary family of submodules $\{M_i\}$ is a submodule.

(iii) (**Set of all submodules**) All submodules of a module form a complete lattice with respect to inclusion.

Mutual implications Some common and obvious ones are left out in order not to confuse readers.

$$\begin{tikzcd}
 & \text{simple} \arrow[dl, Rightarrow] \arrow[dr, Rightarrow] & \\
\text{semi-simple} & & \text{indecomposable} \arrow[d, Rightarrow] \\
 & & \text{cyclic} \arrow[d, Rightarrow] \\
 & & \text{finitely generated}
\end{tikzcd}$$

Faithful modules For any R-module M, M is a faithful $R/\operatorname{ann}(M)$-module.

Simple modules All simple R-modules are cyclic. Conversely, let $M = Rx$. Consider the epimorphism $\phi : R \to Rx$. We have $Rx \cong R/\ker\phi$. Then M is simple if and only if $R/\ker\phi$ is simple, i.e., $\ker\phi$ is a maximal ideal. Thus, we can conclude that any simple module on R has the form $R/\mathfrak{m}$ as an R-module.

Note 2.10. I wanted to say a field, but $R/\mathfrak{m}$ as an R-module has no multiplication defined on it. Q: what about Exercise 3.8?

And it follows each maximal ideal corresponds uniquely (Q: how unique?) to a simple module.

Semi-simple modules An R-module M is semi-simple if any of these equivalent conditions hold.

(0) $M = \sum_i S_i$ where the sum is taken over all simple submodules S_i.

(i) $M = \bigoplus_i S_i$ where the direct sum is taken over some submodules S_i.

(ii) Each submodule is a direct summand.

Any submodule or quotient module of a semi-simple module is semi-simple.

Properties of the direct sum

(i) (**The universal property**) See the definition part.

(ii) (**The induced isomorphism**) Let M and $\{N_i\}$ be R-modules. By the universal property, any family $\{\phi_i : N_i \to M\}$ of homomorphisms corresponds to a unique homomorphism $\psi_\phi : \coprod_i N_i \to M$. Then we have the isomorphism

$$\begin{array}{ccc} \prod_i \mathrm{Hom}_R(N_i, M) & \xrightarrow{\cong} & \mathrm{Hom}_R(\coprod_i N_i, M) \\ (\phi_i) & \mapsto & \psi_\phi \end{array}$$

Properties of the direct product

(i) (**The universal property**) See the definition part.

(ii) (**The induced isomorphism**) Let M and $\{N_i\}$ be R-modules. By the universal properties, any family $\{\phi_i : M \to N_i\}$ of homomorphisms corresponds to a unique homomorphism $\psi_\phi : M \to \prod_i N_i$. Then we have the isomorphism

$$\begin{array}{ccc} \prod_i \mathrm{Hom}_R(M, N_i) & \xrightarrow{\cong} & \mathrm{Hom}_R(M, \prod_i N_i) \\ (\phi_i) & \mapsto & \psi_\phi \end{array}$$

2.3 Theorems

The Isomorphism Theorems Let M, N, P be R-modules.

(i) Any homomorphism $f : M \to N$ induces an isomorphism

$$\begin{array}{rcccl} \overline{f} & : & \mathrm{coim}(f) & \xrightarrow{\cong} & \mathrm{im}(f) \\ & & \overline{x} & \mapsto & f(x) \end{array}$$

and a one-to-one correspondence

$$\begin{array}{rcl} \{\text{Submodules of } N\} & \to & \{\text{Submodules of } M \text{ containing } \ker f\} \\ H & \mapsto & f^{-1}(H) \end{array}$$

(ii) If $P \subset N \subset M$, then we have an isomorphism

$$\begin{array}{ccc} \frac{M/P}{N/P} & \xrightarrow{\cong} & M/N \\ \overline{x} & \mapsto & \overline{x} \end{array}$$

(iii) If $P, N \subset M$, then we have an isomorphism

$$\begin{array}{ccc} \frac{N+P}{P} & \xrightarrow{\cong} & \frac{N}{N \cap P} \\ \overline{x} & \to & \overline{x} \end{array}$$

3 Exact Sequences and the Tensor Product

3.1 Definitions

Exactness An **exact sequence** of algebraic structures and homomorphisms is a sequence of the form

$$\cdots \xrightarrow{f_{i-1}} M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \xrightarrow{f_{i+2}} \cdots$$

such that at each M_i we have $\ker f_{i+1} = \mathrm{im} f_i$. An exact sequence of form $0 \to M' \to M \to M'' \to 0$ is called a **short exact sequence**. A functor is called **exact** if it maps all exact sequences to exact sequences, or equivalently, if it maps all short exact sequences to short exact sequences.

Tensor product The **tensor product** of two R-modules M and N can be defined in the following manners.

(i) (**By the universal property**) The **tensor product** of two R-modules M and N is any pair (T, τ) satisfying for any R-bilinear form $f : M \times N \to P$, there exists a unique R-homomorphism $\phi : T \to P$, such that $f = \phi\tau$. That is, the following diagram commutes.

$$\begin{tikzcd} M \times N \arrow[r, "\tau"] \arrow[dr, "f"'] & T \arrow[d, "\exists !\phi"] \\ & P \end{tikzcd}$$

Note 3.1. All such tensor products are isomorphic.

(ii) (**By construction**) In practice, one needs to prove such a tensor product exists, and maybe even construct one. Let T be the quotient module

$$T = (R^{M\times N})_0/H$$

where $(R^{M\times N})_0$ is the free R-module generated by $M \times N$ and H is the so-called[4] **submodule of bilinear blockers**, that is, $H = \langle S\rangle$ where

$$S = \bigcup_{x,x'\in M, y,y'\in N, r\in R} \Big\{(x, y + y') - (x, y) - (x, y'), \\ (x + x', y) - (x, y) - (x, y'), \\ (rx, y) - r(x, y), \\ (x, ry) - r(x, y)\Big\}$$

The R-bilinear form τ is then set to $\tau : (x, y) \mapsto \overline{(x, y)}$ (easily verified). It remains to check the universal property. For any other R-bilinear form $f : M \times N \to P$, we first extend it to a homomorphism $F : (R^{M\times N})_0 \to P$, and then verify that any generator of H falls in $\ker F$ for f is bilinear, hence $H \subset \ker F$, by the universal property of the quotient $(R^{M\times N})_0/H$, there exists a unique homomorphism $\phi : (R^{M\times N})_0/H \to P$, such that $F = \phi\pi$. Let $\iota : M \times N \to (R^{M\times N})_0$ be the inclusion then $\tau = \pi\iota$ and $f = F\iota = \phi\pi\iota = \phi\tau$ as desired. The tensor product constructed in (ii) is usually denoted by $M \otimes_R N$.

Note 3.2. The tensor product of more than two modules can be constructed form a multilinear mapping, but as we will show later, it is isomorphic to recursively take the tensor product of two modules, so we will not go through that trouble again.

Flat module An R-module N is said to be **flat** if $M \mapsto M \otimes_R N$ is an exact functor on the category of R-modules. The following equivalent conditions can be taken as alternative definitions.

(0) $M \mapsto M \otimes_R N$ is exact.

(i) $M \mapsto M \otimes_R N$ preserves injective R-homomorphisms, i.e, is left-exact.

(i') If f is an R-monomorphism between finitely generated R-modules, then $f \otimes_R \mathrm{id}_N$ is also an R-monomorphism.

(ii) For any prime ideal $\mathfrak{p}$ of R, $N_\mathfrak{p}$ is a flat $R_\mathfrak{p}$-module.

(iii) For any maximal ideal $\mathfrak{m}$ of R, $N_\mathfrak{m}$ is a flat $R_\mathfrak{m}$-module.

[4] by me.

3.2 Propositions

Properties of the tensor product

(i) (**The universal property**) See the definition part.

(ii) (**The induced isomorphism**) Let M, N, P be R-modules. By the universal property of $M \otimes N$, for each bilinear form $\langle -, - \rangle : M \times N \to P$, there exists a unique homomorphism $f_{\langle -,- \rangle}$. Then we have an isomorphism

$$\boxed{\begin{array}{rcl} \mathrm{Hom}_R(M, \mathrm{Hom}_R(N, P)) & \xrightarrow{\cong} & \mathrm{Hom}_R(M \otimes N, P) \\ (x \mapsto \langle x, - \rangle) & \mapsto & f_{\langle -,- \rangle} \end{array}}$$

Note 3.3. The set on the left is just the set of all bilinear forms in another guise.

(ii) (**The canonical isomorphisms**) See the next entry.

Canonical isomorphisms regarding the tensor product Let M, N, P be R-modules.

(i)

$$\boxed{\begin{array}{rcl} M \otimes N & \xrightarrow{\cong} & N \otimes M \\ x \otimes y & \mapsto & y \otimes x \end{array}}$$

Proof. Consider $f : M \times N \to N \otimes M, (x, y) \mapsto y \otimes x$ and $g : N \times M \to M \otimes N, (y, x) \mapsto x \otimes y$, then the homomorphisms induced by them are mutually inverses.

(ii)

$$\boxed{\begin{array}{rcccl} (M \otimes N) \otimes P & \xrightarrow{\cong} & M \otimes (N \otimes P) & \xrightarrow{\cong} & M \otimes N \otimes P \\ (x \otimes y) \otimes z & \mapsto & x \otimes (y \otimes z) & \mapsto & x \otimes y \otimes z \end{array}}$$

Proof. For each fixed z, $(x, y) \mapsto x \otimes y \otimes z$ induces a homomorphism $f_z : M \otimes N \to M \otimes N \otimes P, x \otimes y \mapsto x \otimes y \otimes z$, and then $(t, z) \mapsto f_z(t)$ induces a homomorphism $(M \otimes N) \otimes P \to M \otimes N \otimes P$, whose inverse is even easier to construct.

(iii)

$$\boxed{\begin{array}{rcl} (M \oplus N) \otimes P & \xrightarrow{\cong} & (M \otimes P) \oplus (N \otimes P) \\ (x, y) \otimes z & \mapsto & (x \otimes z, y \otimes z) \end{array}}$$

(iii*) If $\{M_i\}$ is a family of R-modules, then

$$\boxed{\begin{array}{rcl} (\bigoplus_i M_i) \otimes P & \xrightarrow{\cong} & \bigoplus_i (M_i \otimes P) \\ (x_i) \otimes z & \mapsto & (x_i \otimes z) \end{array}}$$

(iv)

$$\boxed{\begin{array}{rcl} R \otimes M & \xrightarrow{\cong} & M \\ r \otimes x & \mapsto & rx \end{array}}$$

(v) If A, B are rings, M is an A-module, P is a B-module and N is an (A, B)-bimodule, then $M \otimes_A N$ is a B-module, $N \otimes_B P$ is an A-module and

$$\boxed{(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P)}$$

(Q: As what module? What is the isomorphism?)

Exactness properties of the tensor product Consider only the category of all R-modules.

(i) For any R-module N, both functors $M \mapsto M \otimes_R N$ and $M \mapsto N \otimes_R M$ are right-exact.

(ii) For a flat R-module, then $M \mapsto M \otimes_R N$ and $M \mapsto N \otimes_R M$ are exact.

Properties of a flat module Let M be a flat R-module.

(i) (**Equivalent conditions**) See the definition part.

(ii) (**Change of base ring**) If $\varphi : R \to A$ is a ring homomorphism, then $A \otimes_R M$ is a flat A-module.

3.3 Theorems

4 Rings and Modules of Fractions

4.1 Definitions

Multiplicatively closed subset A **multiplicatively closed subset** S of a ring is a subset of the ring such that $1 \in S$ and S is closed under multiplication.

Ring of fractions Let R be a ring and S a multiplicatively closed subgroup of it. Then an equivalence relation may be defined for pairs $(a, s) \in R \times S$ by

$$(a, s) \equiv (b, t) \iff (at - bs)u = 0 \text{ for some } u \in S$$

The equivalence class which (a, s) is in is then denoted by $\frac{a}{s}$, and the set of all equivalence classes is denoted by

$$S^{-1}R = \left\{ \frac{a}{s} : a \in R, s \in S \right\}$$

on which the addition and multiplication below are well-defined

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

$$\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$$

And we can verify that equipped with these operations $S^{-1}R$ is made into a ring, called the **ring of fractions of R with respect to S**. The ring homomorphism

$$\begin{array}{cccc} f & : & R & \rightarrow & S^{-1}R \\ & & x & \mapsto & \frac{x}{1} \end{array}$$

is a canonical homomorphism, but not an injection in general. These two cases are of particular interest.

(i) (**Field of fractions**) If R is an integral domain, then we can take $S = R \backslash \{0\}$, which is multiplicatively closed, and $S^{-1}R$ is then a field, called the **field of fractions** of R.

(ii) (**Localization**) If $\mathfrak{p}$ is a prime ideal of R, then we can take $S = R - \mathfrak{p}$, which is multiplicatively closed. In this case, $S^{-1}R$ is usually denoted by $R_{\mathfrak{p}}$ and called the **localization of R at $\mathfrak{p}$**.

(iii) (**Powers of an element**) If $a \in R$, let $S = \{a^n : n \geqslant 0\}$. The resulting ring is denoted $S^{-1}R = R_a$.

Module of fractions Let M be an R-module and S a multiplicatively closed subgroup of R. Then an equivalence relation may be defined for pairs $(a, s) \in M \times S$ by

$$(a, s) \equiv (b, t) \iff (at - bs)u = 0 \text{ for some } u \in S$$

The equivalence class which (a, s) is in is then denoted by $\frac{a}{s}$, and the set of all equivalence classes is denoted by

$$S^{-1}M = \left\{ \frac{a}{s} : a \in R, s \in S \right\}$$

on which the addition and scalar multiplication by $S^{-1}R$ below are well-defined

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{r}{s}\frac{a}{t} = \frac{ra}{st}$$

And we can verify that equipped with these operations $S^{-1}M$ is made into a $S^{-1}R$-module, called the **module of fractions of** M. For any R-homomorphism $f : M \to N$, u can be levitated to a unique R-homomorphism $S^{-1}f : S^{-1}M \to S^{-1}N$ that has the form $\frac{x}{s} \mapsto \frac{f(x)}{s}$.

$$\begin{tikzcd}
S^{-1}M \arrow[rrr, "S^{-1}f"] & & & S^{-1}N \\
& \frac{x}{1} \arrow[r, mapsto] & \frac{f(x)}{1} & \\
& x \arrow[u, mapsto] \arrow[r, mapsto] & f(x) \arrow[u, mapsto] & \\
M \arrow[uuu, "\tau"] \arrow[rrr, "f"] & & & N \arrow[uuu, "\sigma"']
\end{tikzcd}$$

As usual, if $\mathfrak{p}$ is a prime ideal of R, then we can take $S = R - \mathfrak{p}$, which is multiplicatively closed. In this case, $S^{-1}M$ is by $M_{\mathfrak{p}}$ and called the **localization of M at $\mathfrak{p}$.**

Note 4.1. Since we have a canonical homomorphism $R \to S^{-1}R, r \mapsto \frac{r}{1}$, any $S^{-1}R$-module is also an R-module with scalar multiplication defined by $rx = \frac{r}{1}x$ for $r \in R$.

4.2 Propositions

Properties of the ring of fractions Let $S^{-1}R$ be the ring of fractions of R, and $f : R \to S^{-1}R$ the canonical homomorphism.

(i) (**Universal property**) For any ring homomorphism $g : R \to A$ such that $g(S) \in A^*$, there exists a unique ring homomorphism $h : S^{-1}R \to A$ such that $h \circ f = g$. That is, any homomorphism that turns S in to invertible elements can be factored through $(S^{-1}R, f)$.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[dr, "g"'] & S^{-1}R \arrow[d, "\exists! h"] \\
& A
\end{tikzcd}$$

Note 4.2. To construct a ring of fractions it to put elements of S to the denominators, or more precisely, to make elements of S invertible. Clearly, if 0 is invertible, then $0 = 0 \cdot 0^{-1} = 1 \implies S^{-1}R = 0$. Conversely if $S^{-1}R = 0$, then $\frac{1}{1} = \frac{0}{1} \implies u = 0$ for some $u \in S$.

Note 4.3. One can also use the universal property to define the ring of fractions, and it is isomorphic to our previous construction.

(ii) (**Properties of** $(S^{-1}R, f)$)

(a) (**The zero**) $\frac{0}{1} = \frac{0}{s} = 0 \in S^{-1}R$ and $\frac{a}{1} = 0 \in S^{-1}R \iff au = 0$ for some $u \in S$

(b) (**The one**) $\frac{1}{1} = \frac{s}{s} = 1 \in S^{-1}R$

(c) (**The inverse**) $s \in S \implies \frac{s}{1} \in (S^{-1}R)^*$ and $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$

(d) (**The ideals**) Every ideal of $S^{-1}R$ has the form $S^{-1}\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of R.

–

(iii) (**Flatness of** $S^{-1}R$) $S^{-1}R$ is a flat R-module.

Properties of the module of fractions Let M be an R-module and S a multiplicatively closed subgroup of R. Let $\tau : M \to S^{-1}M$ be the canonical homomorphism.

(i) (**Universal property**) Let N be any $S^{-1}R$-module and $f : M \to N$ an R-homomorphism, then there exists a unique $S^{-1}R$-homomorphism $h : S^{-1}M \to N$ such that $h \circ \tau = f$. That is, any homomorphism that turns S in to invertible elements can be factored through $(S^{-1}R, f)$.

$$\begin{tikzcd}
M \arrow[r, "\tau"] \arrow[dr, "f"'] & S^{-1}M \arrow[d, "\exists ! h"] \\
 & N
\end{tikzcd}$$

Note 4.4. To construct a module of fractions is in essence to expand the base ring. Therefore, any other module on the expanded ring, namely, the ring of fractions, can be applied with the universal property.

(ii) (**Equivalent construction**) Let M be an R-module, which has S as a multiplicatively closed subgroup. Then

$$\begin{array}{ccc} S^{-1}R \otimes_R M & \xrightarrow{\cong} & S^{-1}M \\ \frac{a}{s} \otimes m & \mapsto & \frac{am}{s} \end{array}$$

is the unique isomorphism between the two $S^{-1}R$-modules.

(iii) (**Flatness**) Let M be an R-module and S a multiplicatively closed subgroup of R. Then $S^{-1}M$ is a flat $S^{-1}R$-module.

(iv) (**Properties of S^{-1}**) It is better to think of S^{-1} as a functor on the category of R-modules. See the next entry.

Properties of S^{-1} The functor

$$S^{-1} : \mathbf{Mod}_R \Rightarrow \mathbf{Mod}_{S^{-1}R}$$

has the following properties.

(i) (**Exact**) S^{-1} turns exact sequences to exact sequences.

(ii) (**On submodule operations**) Let N, P be submodules of an R-module.

  (a) $S^{-1}(N + P) = S^{-1}N + S^{-1}P$

  (b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$

  (c) $S^{-1}(M/N) \cong (S^{-1}M)/(S^{-1}N)$

(iii) (**On homomorphisms**) Let $M \xrightarrow{f} N \xrightarrow{g} P$. Then

$$S^{-1}(gf) = (S^{-1}g)(S^{-1}f)$$

(iv) (**Isomorphisms**) Let M, N be R-modules, which has S as a multiplicatively closed subgroup.

  (a) There is an isomorphism between the $S^{-1}R$-modules

$$\begin{array}{ccc} S^{-1}R \otimes_R M & \xrightarrow{\cong} & S^{-1}M \\ \frac{a}{s} \otimes m & \mapsto & \frac{am}{s} \end{array}$$

  Note 4.5. Very good point of view to see that the essence of S^{-1} is to expand the base ring.

  (b) There is an isomorphism between the $S^{-1}R$-modules

$$\begin{array}{ccc} S^{-1}M \otimes_{S^{-1}R} S^{-1}N & \xrightarrow{\cong} & S^{-1}(M \otimes_R N) \\ \frac{m}{s} \otimes \frac{n}{t} & \mapsto & \frac{m \otimes n}{st} \end{array}$$

  Note 4.6. In other words, S^{-1} commutes with $\otimes$.

Local properties

(i) (**On modules**) The following are equivalent for an R-module M.

  (a) $M = 0$

(b) $M_{\mathfrak{p}} = 0$ for all prime $\mathfrak{p}$

(c) $M_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m}$

(ii) (**On monomorphisms**) The following are equivalent for an R-homomorphism $\phi : M \to N$.

(a) $\ker \phi = 0$

(b) $\ker \phi_{\mathfrak{p}} = 0$ for all prime $\mathfrak{p}$

(c) $\ker \phi_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m}$

(iii) (**On epimorphisms**) The following are equivalent for an R-homomorphism $\phi : M \to N$.

(a) $\text{coker}\phi = 0$

(b) $\text{coker}\phi_{\mathfrak{p}} = 0$ for all prime $\mathfrak{p}$

(c) $\text{coker}\phi_{\mathfrak{m}} = 0$ for all maximal $\mathfrak{m}$

(iv) (**On flatness**) The following are equivalent for an R-module M.

(a) M is a flat R-module

(b) $M_{\mathfrak{p}}$ is a flat $R_{\mathfrak{p}}$-module for all prime $\mathfrak{p}$

(c) $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module for all maximal $\mathfrak{m}$

5 Finitely Generated Modules, Noetherian Modules, and Artinian Modules

5.1 Definitions and Properties

Finitely generated module An R-module M is called **finitely generated** if $M = Rx_1 + \cdots + Rx_n$ for some finitely many $x_1, \cdots, x_n \in M$.

Chain,minimal,maximal conditions A poset is said to satisfy

(i) the **ascending chain condition** or **ACC** if any ascending chain in it is eventually constant, or stationary;

(ii) the **descending chain condition** or **DCC** if any descending chain in it is eventually constant, or stationary;

(iii) the **maximal condition** if any subset of it has a maximal element;

(iv) the **minimal condition** if any subset of it has a minimal element;

Noetherian module/ring An R-module M is said to be a **Noetherian module** if it satisfies the ACC on submodules. Alternatively, the following equivalent conditions can also be taken as definitions for a Noetherian module.

(0) (**ACC**) M satisfies the ACC on submodules.

(i) (**Maximal condition**) M satisfies the maximal condition on submodules.

(ii) (**Finitely generated submodules**) Every submodule of M is finitely generated.

(iii) (**Noetherian submodules**) Every submodule of M is Noetherian.

(iv) (**Noetherian sub-/quotient modules 1**) For some submodule N, N and M/N are both Noetherian.

(v) (**Noetherian sub-/quotient modules 2**) For any submodule N, N and M/N are both Noetherian.

(vii) (**Noetherian sub-/quotient modules 3**) For any exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, M' and M'' are both Noetherian.

A ring R is said to be a **Noetherian ring** if it is Noetherian as an R-module. The following are equivalent conditions.

(0) (**ACC**) R satisfies the ACC on ideals.

(i) (**Maximal condition**) R satisfies the maximal condition on ideals.

(ii) (**Finitely generated ideal**) Every ideal of M is finitely generated.

(iii) (**Reflection by modules**) Every finitely generated R-module is Noetherian.

Aside from the equivalent conditions for Noetherian rings and modules, we have the following properties.

(i) (**Sum**) A finite sum of Noetherian modules is Noetherian.

(i') (**Direct sum**) A direct sum of Noetherian modules is Noetherian. Conversely, if a direct sum is Noetherian, then each summand is Noetherian.

(ii) (**Fg. module over a N-ring**) A finitely generated module over a Noetherian ring is Noetherian.

(iii) (**Quotient**) A quotient ring of a Noetherian ring is Noetherian.

(iv) (**Minimal prime**) A Noetherian ring contains only finitely many minimal prime ideals.

(v) (**Image**) A is Noetherian, $\phi : A \to B \implies \mathrm{im}(\phi)$ is Noetherian.

(vi) (**Fg. lifting**) $A \subset R$ is a Noetherian subring, and R is finitely generated over A. Then R is Noetherian.

(vii) (**Localization**) R is Noetherian $\implies S^{-1}R$ is Noetherian.

(viii) (**Nilpotent nilradical**) nilrad(R) is nilpotent for a Noetherian module R.

(ix) (**Power of radical**) For any ideal $\mathfrak{a}$ in a Noetherian ring, $\sqrt{\mathfrak{a}}^n \subset \mathfrak{a} \subset \sqrt{\mathfrak{a}}$ for some n.

Artinian module/ring An R-module M is said to be an **Artinian module** if it satisfies the DCC on submodules. Alternatively, the following equivalent conditions can also be taken as definitions for an Artinian module.

(0) (**DCC**) M satisfies the DCC on submodules.

(i) (**Minimal condition**) M satisfies the minimal condition on submodules.

(ii) (**Artinian sub-/quotient modules**) For any exact sequence $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, M' and M'' are both Artinian.

A ring R is said to be an **Artinian ring** if it is Artinian as an R-module. Aside from the equivalent conditions for Artin rings and modules, we have the following properties.

(i) (**Sum**) A direct sum of Artinian modules is Artinian.

(ii) (**Fg. over an A-ring**) A finitely generated module over a Artinian ring is Artinian.

(iii) (**Quotient**) A quotient ring of a Artinian ring is Artinian.

(iv) (**Prime, maximal**) In an Artinian ring, prime $\iff$ maximal, and nilrad = rad.

(v) Artinian $\implies$ semi-local.

(vi)

5.2 Propositions

5.3 Theorems

Structural Theorem for Finitely Generated Modules Let M be an R module.

$$M \text{ is finitely generated } \iff \exists n,\ M \cong R^n/N \text{ for some } N \leqslant R^n$$

Nakayama's Lemma Let M be a finitely generated R-module. We have

(i) (**Lemma 1**) If $\phi \in \mathrm{End}(M)$ is such that $\phi(M) \subset \mathfrak{a}M$ for some ideal $\mathfrak{a}$ of R, then for some $f(x) \in \mathfrak{a}[x]$, $f(\phi) = 0$.

(ii) (**Lemma 2**) If an ideal $\mathfrak{a}$ is such that $\mathfrak{a}M = M$, then there exists $a \in \mathfrak{a}$, $1 + a \in \mathrm{ann}(M)$.

(iii) (**Nakayama's Lemma**) If an ideal $\mathfrak{a} \subset \mathrm{rad}R$ is such that $\mathfrak{a}M = M$, then $M = 0$.

(iv) (**Corollary 1**) If there is a submodule $N \subset M$ and an ideal $\mathfrak{a} \subset \mathrm{rad}R$ such that $M = \mathfrak{a}M + N$, then $M = N$.

Hilbert Basis Theorem Let R be a Noetherian ring. The following are true.

(i) $R[X]$ is a Noetherian ring.

(ii) $R[[X]]$ is a Noetherian ring.

6 Primary Decomposition

We shall recall some definitions and propositions from Sect.**??**.

6.1 Definitions

Primary ideal An ideal $\mathfrak{q}$ is called **primary** if $\mathfrak{q} \neq (1)$ and

$$xy \in \mathfrak{q} \implies x \in \mathfrak{q} \text{ or } y^n \in \mathfrak{q} \text{ for some } n \geqslant 1$$

or equivalently,

$$R/\mathfrak{q} \neq 0, \text{ all zero-divisors of } R/\mathfrak{q} \text{ are nilpotent}$$

The radical $\mathfrak{p} = \sqrt{\mathfrak{q}}$ of a primary ideal $\mathfrak{q}$ is a prime ideal. Many different primary ideals $\mathfrak{q}_i$ may happen to have the same radical $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$. If $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then we say $\mathfrak{p}$ is the **prime ideal associated to** $\mathfrak{q}$ and that $\mathfrak{q}$ is p-primary.

Note 6.1. It is better to illustrate with this picture.

$$\begin{tikzcd}
\text{Prime ideal associated to } \mathfrak{q}_i & & & \mathfrak{p} & & \\
\mathfrak{p}\text{-primary ideals} & \mathfrak{q}_1 \arrow[urr, "\sqrt{\ }"] & \mathfrak{q}_2 \arrow[ur, "\sqrt{\ }"] & \cdots & \mathfrak{q}_n \arrow[ul, "\sqrt{\ }"'] & \cdots
\end{tikzcd}$$

Note 6.2. I am your primary means you are my radical.

Primary decomposition of an ideal A **primary decomposition** of an ideal $\mathfrak{a}$ in R, if it exists, is an expression of $\mathfrak{a}$ as a finite intersection of primary ideals, namely,

$$\mathfrak{a} = \bigcap_{i=1}^{n} \mathfrak{q}_i$$

where each $\mathfrak{q}_i$ is primary. If moreover,

(i) the prime ideals $\sqrt{\mathfrak{q}_i}$ associated to $\mathfrak{q}_i$ are distinct;

(ii) no factor of this decomposition can be left out, i.e., $\bigcap_{j \neq i} \mathfrak{q}_j \not\subset \mathfrak{q}_i$ for each i,

then the decomposition is called **minimal**.

7 Finitely Generated Modules over a PID

7.1 Definitions

Torsion elements and modules An element x in an R-module M is called a **torsion element** if $rx = 0$ for some $0 \neq r \in R$ (0 is excluded). The **torsion part** of M is $M_{\text{tor}} = \{x \in M : \exists r \in R,\ r \neq 0,\ rx = 0\}$, and it is a submodule if R is an integral domain, in which case the quotient module M/M_{tor} is defined and torsion-free. If $M_{\text{tor}} = 0$, then M is said to be **torsion-free**. If $M_{\text{tor}} = M$, then M is said to be a **torsion module**. For a given prime element $p \in R$, an element $x \in M$ is called **p-torsion** if $p^n x = 0$ for some $n \geqslant 1$. A module is called **p-torsion** if it is filled with p-torsion element. The p-torsion submodule $M(p)$ is the set of all p-torsion elements of M, which can be verified to be a submodule.

7.2 Propositions

Torsion submodule The torsion part M_{tor} of M is such that

(i) The ring needs to be integral to ensure M_{tor} is a submodule.

(ii) M/M_{tor} is always torsion-free.

(iii) Any homomorphism $f : M \to N$ maps torsion elements to torsion elements, i.e., $f(M_{\text{tor}}) \subset N_{\text{tor}}$

(iv) $M \cong N \implies M_{\text{tor}} \cong N_{\text{tor}},\ M/M_{\text{tor}} \cong N/N_{\text{tor}}$

Finitely generated free module over a PID Let M be a free module of rank n over a PID R. We are interested in the structure of submodules of M

(i) Any submodule $N \leqslant M$ is free with rank $d \leqslant n$.

Note 7.1. The proof is easy when M has finite rank, and this case may be generalized to infinite rank.

(ii) For any submodule $N \leqslant M$, there exists a basis $\mathcal{B} = \{e_1, \cdots, e_n\}$ of M and elements $r_1, \cdots, r_d \in R$ such that $\{r_1e_1, \cdots, r_de_d\}$ is a basis for N.

(iii) A spanning set S of size n is a basis.

(iv) (**Corollary of (i)**) Let P be an n-generated module over a PID, then any submodule is also n-generated.

Note 7.2. Finitely generated free module $\iff$ free module of finite rank.

Torsion-free and free A finitely generated torsion-free module M over a PID R is free.

Proof. The basic idea is to embed M into some free module and apply the last proposition. Such an embedding is of the form

$$a : M \to aM, x \mapsto ax \quad (0 \neq a \in R)$$

Note that this is an isomorphism because M is torsion-free (so that $ax = 0 \implies x = 0 \implies \ker a = 0$). It remains to find a free submodule N of M and choose a proper a. A free submodule can be generated by a linearly independent set, hence we need to find a maximal linearly independent subset (existence is ensure by M being torsion-free, so that any nonzero singleton is linearly independent):

$$\{u_1, \cdots, u_k\}$$

of some generating set

$$\{u_1, \cdots, u_k, v_1, \cdots, v_{n-k}\}$$

Linear dependence of $\{u_1, \cdots, u_k, v_i\}$ allows us to choose an element r_i to absorb v_i into $N = (u_1, \cdots, u_k)$. And hence $a = r_1 \cdots r_{n-k}$ absorbs M into $N = (u_1, \cdots, u_k)$, which is free, hence $M \cong aM \subset N$ is free.

Note 7.3. We may not have $N = M$, but the proof above says $\text{rank}(M) \leqslant \text{rank}(N) \leqslant (M) \implies \text{rank}(N) = \text{rank}(M)$.

7.3 Theorems

Structural Theorem for Finitely Generated Modules over a PID The decomposition is proved in steps. Let M be a finitely generated module over a PID R.

(i) (**Free-torsion decomposition**) There exists a free submodule M_{free} such that
$$M = M_{\text{free}} \oplus M_{\text{tor}}, \quad \text{with } M_{\text{free}} \cong M/M_{\text{tor}}$$
where both M_{free} and M_{tor} are finitely generated.

(ii) (**Torsion to p-torsion**) The finitely generated torsion module M_{tor} is a finite direct sum of p-torsion modules.
$$M = \bigoplus_{p \text{ is prime}} M(p)$$
and the sum is finite.

(iii) (**p-torsion to cyclic**) Any $x \in M(p)$ generates a direct summand Rx of $M(p)$. Moreover, if $p^n x = 0,\ p^{n-1}x \neq 0$, then
$$Rx \cong R/(p^n)$$
and if we keep decomposing $M_(p)$ by extracting direct summands of it, we obtain in the end
$$M(p) \cong R/(p^{n_1}) \oplus \cdots \oplus R/(p^{n_s})$$
where $n_1 n_1 \geqslant \cdots \geqslant n_s \geqslant 1$ are uniquely determined by $M(p)$.

(iv) (**Combining the above**) Combining all of the above we obtain
$$M \cong R^s \oplus \left(\bigoplus_{i=1}^{t} \bigoplus_{j=1}^{m_i} R/(p_i^{n_{ij}}) \right)$$
The ring elements $p_i^{m_ij}$ are called the **elementary factors**.

(v) (**Combining the coprime factors**)
$$M \cong R^s \oplus R/(d_1) \oplus \cdots \oplus R/(d_t)$$
where $d_1 \big| \cdots \big| d_t$ are called the **invariant factors**.

8 Valuation Rings

8.1 Definitions and Properties

Valuation ring If we do not introduce valuation first, we can only define the notion of valuation ring for integral domains. Let B be an integral domain and K its field of fractions. Then B is called a **valuation ring** of K if $x \neq 0 \implies$ either $x \in B$ or $x^{-1} \in B$ or both. The valuation ring B of K has the following properties.

(i) B is local.

(ii) Any ring extension of B in K is also a valuation ring.

(iii) B is integrally closed.

Conversely, for any field K, there exists a subring of K that is a valuation ring of K.

Valuation Let K be a field and Γ a totally ordered (additive) abelian group. A **valuation of K with values in Γ** is a mapping $K^* \to \Gamma$ such that

(i) $v(xy) = v(x) + v(y)$ (homomorphism)

(ii) $v(x+y) \geqslant \min(v(x), v(y))$

The set $R = \{x \in K^* : v(x) \geqslant 0\} \cup \{0\}$ is a valuation ring of K and is called the **valuation ring** of v, and $v(K^*)$ is the value group of v. But in practice, we more often consider discrete valuations. A **discrete valuation** on a field K is a mapping $v : K^* \to \mathbb{Z}$ such that

(i) v is surjective.

(ii) $v(xy) = v(x) + v(y)$ (homomorphism)

(iii) $v(x+y) \geqslant \min(v(x), v(y))$

Similarly, the set $R = \{x \in K^* : v(x) \geqslant 0\} \cup \{0\}$ is a valuation ring of K called the **valuation ring** of v. Usually we put $v(0) = \infty$. If the field is not given in advance, we say an integral domain A is a **discrete valuation ring** if there exists a discrete valuation v on its field of fractions K such that $A = \{x \in K^* : v(x) \geqslant 0\} \cup \{0\}$.