Algebra II

Instructor: Olivier Bernardi
Scribe: Alan Hou

Contents

Last Updated: November 14, 2024

Part I

Representation Theory

1

Algebras and Representation

1.1 Basic Definitions

Definition 1.1.1. Let K be a ring, then a $K-$**algebra** $(A, +, \cdot, \times)$ is a $K-$module $(A, +, \cdot)$ together with a bilinear operation multiplication $\times : A \times A \to A$ such that

$$\exists 1 \in A, 1 \times x = x \times 1 = x, \forall x \in A,$$

$$x \times (y \times z) = (x \times y) \times z.$$

Equivalently, $(A, +, \cdot)$ is $K-$module, $(A, +, \times)$ is a ring, and $\times$ is bilinear, $(k \cdot x) \cdot y = x \times (k \cdot y) = k \cdot (x \times y)$.

From now on, K is a field, so the $K-$algebras are $K-$vector spaces (in particular, have basis).

Example 1.1.2. (1). Let $K = \mathbb{R}$, $A = \mathbb{R}[X_1, \cdots, X_n]$ polynomials in n commuting variables.

(2). Let $K = \mathbb{R}$, $A = \mathbb{R}\langle X_1, \cdots, X_n \rangle$ polynomials in n non-commuting variables.

(3). For V a $K-$vector space, $A = (\mathrm{End}(V), +, \cdot, \circ)$ is a $K-$algebra, where $\mathrm{End}(V)$ is linear maps from V to V.

(4). Let $B = (\mathrm{Mat}_n(K), +, \cdot, \times)$ is a $K-$algebra, where Mat_n is $n \times n$ matrices and is isomorphic to $(\mathrm{End}(K^n), +, \cdot, \circ)$ as representation of linear map of matrices.

Definition 1.1.3. Let A, B be $K-$algebra, $f : A \to B$ is an **algebra homomorphism** if respects the operations $+, \cdot, \times$. Equivalently, f is $K-$linear map and ring homomorphism.

Note that f is isomorphism if bijective and homomorphism and $A \simeq B$ means "isomorphic": $\exists f : A \to B$ isomorphism.

Remark 1.1.4. The ring-quotient construction gives an algebra quotient: if I is a (two-sided) ideal of A then $A/I = \{x+I, x \in A\}$ has structure of algebra $(k(x+I) = kx + I)$.

Example 1.1.5. We see $\mathbb{R}[X]/X^n$ and $\mathbb{R}[X]/(X^n - 1)$ are algebras.

Remark 1.1.6. The fundamental isomorphism theorems for rings hold for algebras. In particular, if $f : A \to B$ is algebra homomorphism then $\mathrm{Im}(f) \simeq A/\ker(f)$ as algebras.

Definition 1.1.7. Let G be a group. The **group algebra** $K[G]$ is the $K-$vector space with basis G and multiplication in $K[G]$ obtained by extending multiplication in G $K-$linearly.

Example 1.1.8. Let $G = S_3, K = \mathbb{C}$ and $x = 2\mathrm{Id} + 5(1,3), y = \mathrm{Id} - (1,2,3) \in \mathbb{C}[S_3]$. Then $x \times y = (2\mathrm{Id} + 5(1,3)) \times (\mathrm{Id} - (1,2,3)) = 2\mathrm{Id} - 2(1,2,3) + 5(1,3) - 5(1,2)$.

Remark 1.1.9. We see $K[G]$ is a natural setting to do computations about G.

Example 1.1.10. We take $x = \sum_{1 \leqslant i < j \leqslant n}(i,j) \in \mathbb{C}[S_n]$ sum of all transpositions. Then $x^k = \sum_{\pi \in S_n} c_\pi \pi$ where c_π = number of ways of getting π as product of $K-$transpositions.

Definition 1.1.11. Let A be a $K-$algebra, a **representation** of A is (V, ρ) where V is a nonzero $K-$vector space and ρ is a homomorphism of algebra $A \to \mathrm{End}(V)$.

This is $\forall a \in A, \rho(a) \in \mathrm{End}(V)$ is a linear map, that is, $\forall a, b \in A, \rho(a+b) = \rho(a) + \rho(b), \rho(a \times b) = \rho(a) \circ \rho(b), \rho(1) = \mathrm{Id}$ and $\rho(ka) = k\rho(a)$.

Equivalently, upon denoting $a \cdot v$ for $\rho(a)(v)$ where $a \in A, v \in V$, we must have this action is bilinear and associative: $(a \times b) \cdot v = a \cdot (b \cdot v), 1 \cdot v = v$.

Definition 1.1.12. The **dimension** of (V, ρ) is $\dim_K(V)$. Also (V, ρ) is **finite dimensional** (f.d.) if $\dim_K(V)$ is finite.

Remark 1.1.13. If $\dim V = n$, then $V \simeq K^n$ as vector spaces and we can view $\rho(a)$ as a matrix.

Example 1.1.14. Let $A = \mathbb{R}[X]$, given $f \in \mathrm{End}(K^n)$, we can define a representation (V, ρ) by $V = K^n, \rho(P) = P(f)$ where $P = \sum c_i x^i$ and $P(f) = \sum c_i \underbrace{f \circ \cdots \circ f}_{i}$. In matrix term, $\rho(P) = P(M) = \sum c_i M^i$ where M is matrix representing f.

Remark 1.1.15. If $\{g_i\}$ are generators of A, then a representation of A is determined by $\{\rho(g_i)\}$. The linear maps $\rho(g_i)$ must satisfy the same relations as g_i.

Example 1.1.16. A representation for $\mathbb{R}[X]/(X^n - 1)$ is determined by $\rho(X)$ satisfying $\rho(X)^n = \mathrm{Id}$.

Remark 1.1.17. For $A = K[G]$ a group algebra representations are uniquely determined by a group homomorphism

$$\rho : G \longrightarrow \mathrm{GL}(V),$$

where $\mathrm{GL}(V)$ are invertible matrices (for all $g \in G, \rho(g) \in \mathrm{GL}(V)$ since $\rho(g^{-1}) = \rho(g)^{-1}$). The representations (V, ρ) of $K[G]$ is then determined by linear extension $\rho(\sum c_g g) = \sum c_g \rho(g)$.

Example 1.1.18. (1). Let $G = C_n = \langle x \rangle / \langle\langle x^n = 1 \rangle\rangle$ cyclic group with n elements. For $M \in \mathrm{Mat}_n(K)$ such that $M^n = \mathrm{Id}$ we can define $\rho(x) = M$ (Here $K[C_n] \simeq \mathbb{R}[X]/(X^n - 1)$).

(2). For instance, for $K = \mathbb{C}, M = [\omega], \omega = e^{2i\pi/m}$ the $m-$th root of unity gives a $1-$dimensional representation $\rho(x^m) = [\omega^m]$.

Definition 1.1.19. The **regular representation** of A is $(V_{\text{reg}}, \rho_{\text{reg}})$ where $V_{\text{reg}} = A$ as $K-$vector space, $\rho_{\text{reg}}(a)$ is left multiplication by a, i.e., $\forall a \in A, v \in V_{\text{reg}} = A$, we have $a \cdot v = \rho(a)(v) = a \times v$ where $\cdot$ is action and $\times$ is multiplication in A.

Goal of Representation Theory:
(1). Describe all the A representations (in particular, ρ_{reg}) - decomposition into "irreducible representations".
(2). Use this description to simplify computation in A.

Remark 1.1.20. For G a group, the representation of the group algebra is specified by endomorphisms $\rho(g), g \in G$ such that $\rho(1) = \mathrm{Id}$, and

$$\rho(gh) = \rho(g) \circ \rho(h), \forall g, h \in G. \tag{$\star$}$$

Observe that $\forall g \in G, \rho(g)\rho(g^{-1}) = \rho(1) = \mathrm{Id}$. Hence $\forall g \in G, \rho(g) \in \mathrm{Aut}(V)$ which are invertible linear maps $V \to V$. Note that $(\star)$ means that $\rho : G \to \mathrm{Aut}(V)$ is group homomorphism.

In summary, for a group G, the $K-$representations of the group algebra $K[G]$ are uniquely determined by the group homomorphism $\rho : G \to \mathrm{Aut}(V)$, where V is $K-$vector space.

The representation (V, ρ) is then extended to $K[G]$ by linearity, i.e., $\rho(\sum c_g g) = \sum c_g \rho(g)$. In terms of operations: $(\sum c_g g) \cdot v = \sum c_g (g \cdot v)$.

Example 1.1.21. (1). Let $A = K[G], V = k, \rho(g) = \mathrm{Id}_K$ for g, the trivial representation with dimension 1.

(2). Let $A = \mathbb{C}[c_m], c_m = \langle g \rangle / \langle\langle g^m = 1 \rangle\rangle = \{g^0 = 1, g^1, \cdots, g^{m-1}\}$. Then $V = \mathbb{C}, \rho(g^k) = \omega^k \mathrm{Id}_K$ where $\omega^m = 1$.

(3). Let $A = K[S_m], V = K^m, \forall \pi \in S_m, \rho(\pi) =$ "permutation matrices". $\pi \cdot e_j = e_{\pi(j)}, e_j = (0, \cdots, 1, 0, \cdots, 0)$ where the only 1 is at the $j-$th coordinate as e_j basis of K^m. Then $\pi \cdot (x_1, \cdots, x_m) = (x_{\pi^{-1}(1)}, \cdots, x_{\pi^{-1}(m)})$.

(4). Let $A = K[G]$, for any $G-$set S, we can define K^S =vector space with basis S and representation given by $\rho(g) \cdot s = g \cdot s$ where the latter $\cdot$ is g action. (Hence $\rho(g)(\sum c_S S) = \sum c_S(g \cdot S)$, $\rho(g)$ is a representation in basis S).

Remark 1.1.22. The regular representation $K[G]$ is of this form (action $G \curvearrowright G$ by left translation).

Definition 1.1.23. Let $(V, \rho), (V', \rho')$ be representation of $K-$algebra A, a **homomorphism of representation** is $\phi : V \to V'$ linear such that

$$\forall a \in A, \forall v \in V, \phi(a \cdot v) = a \cdot \phi(v),$$

where the first $\cdot$ is the action on ρ and the second $\cdot$ is the action on ρ'.

For notation, $\mathrm{Hom}_A(V, V')$ is the vector space of representation homomorphism $V \to V'$ (ρ, ρ' are implicit).

Definition 1.1.24. The **isomorphism of representations** is bijective homomorphism of representations.

We say $V \simeq V'$ if there exists isomorphism $V \to V'$.

Remark 1.1.25. If $(V, \rho) \simeq (V', \rho')$, then there exists matrix P such that $\forall a \in A, P\rho(a)P^{-1} = \rho'(a)$ (Indeed, if P represents the isomorphism $V \to V'$, then $P\rho(a) = \rho'(a)P$). Equivalently, the matrices $\rho(a)$ and $\rho(a')$ are equal up to a change of basis.

Example 1.1.26 (Toy model). Let $A = \mathbb{C}[c_m], c_m = \langle g \rangle / \langle\langle g^m = 1 \rangle\rangle$, then

(1). In the basis $\{g^0, \cdots, g^{m-1}\}$ we have

$$\rho_{\mathrm{reg}}(g^j) = \begin{array}{cc} \begin{array}{cccccc} & & & m-j & & \end{array} & \\ \begin{pmatrix} 0 & 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & 0 & \ddots & 1 \\ 0 & 0 & 0 & 0 & 0 & \vdots \\ 1 & 0 & 0 & 0 & 0 & 0 \\ \vdots & \ddots & 0 & 0 & 0 & 0 \\ 0 & \cdots & 1 & 0 & 0 & 0 \end{pmatrix} & \begin{array}{c} \\ \\ \\ j \\ \\ \\ \end{array} \end{array}.$$

Hence $\rho_{\mathrm{reg}}(\sum_{i=0}^{m-1} k_i g^i)$ is the matrix with all 1 entries. Let $\omega = e^{2\pi i/m}$ and consider basis $h_0, \cdots, h_{m-1}$ where $h_j = \sum_{j=0}^{m-1} \omega^{jd} g^j$. In this basis, we have

$$\rho_{\mathrm{reg}}(g^j) = \begin{pmatrix} \omega^{-(1-1)j} = 1 & & 0 \\ & \ddots & \\ 0 & & \omega^{-(m-1)j} \end{pmatrix},$$

the diagonal matrix.

(2) The change of basis $(g^0, \cdots, g^{m-1})$ to $(h_0, \cdots, h_{n-1})$ simplifies computation. Actually this is equivalent to discrete Fourier transform (DFT). That is, regard $\sum k_i g^i$ as "function with value k_i" and h_i pointwise waves. Change of basis: write functions as linear combination of waves.

$$\text{Convolution of function} \xleftrightarrow{DFT} \text{pointwise multiplication.}$$

Useful for fast multiplication of polynomial or numbers.

1.2 Decomposition of Representation and Schur's Lemma

Definition 1.2.1. Let (V, ρ) be a $A-$representation, then

- a **subrepresentation** is a subspace $0 \neq W$ of V such that $\forall a \in A, a \cdot W \subseteq W$. In this case, $(W, \rho|_W)$ is a $A-$representation; and
- the representation (V, ρ) is **irreducible** if it has no proper subrepresentation.

Remark 1.2.2. For all $v \in V, A \cdot v = \langle a \cdot v, a \in A\rangle$ is a subrepresentation of V. Hence V is irreducible if and only if $\forall v \in V, Av = V$.

Lemma 1.2.3. *If A is finite dimensional (e.g., $A = K[G]$ where G is finite), then any irreducible representation of A is also finite dimensional.*

Proof. We have V irreducible $\Longrightarrow Av = V$ where $\dim Av \leqslant \dim A < \infty$. □

We say "irreps" to mean finite dimensional irreducible representations.

Remark 1.2.4. If $\phi \in \mathrm{Hom}_A(V, W)$, then $\mathrm{Im}(\phi), \ker(\phi)$ are subrepresentations.

Lemma 1.2.5 (1st Isomorphism Theorem)**.** *We have that*

- *if V is $A-$representation, and $W \subseteq V$ subrepresentation, then $V/W = \{v+W, v \in V\}$ has structure of $A-$representation: $a \cdot \overline{v} = \overline{a \cdot v}$ where $\overline{v} = v + W$; and*
- *if $\phi \in \mathrm{Hom}_A(V, W)$ then $\mathrm{Im}(\phi) = V/\ker(\phi)$.*

Definition 1.2.6. Let $V_1, \cdots, V_k$ be $A-$representations, the **direct sum** is the representation $V_1 \oplus \cdots \oplus V_k$ with $A-$action $a \cdot (v_1, \cdots, v_k) = (a \cdot v_1, \cdots, a \cdot v_k)$. The direct sum can be viewed as vector spaces $\{(v_1, \cdots, v_k)\}$ where $v_i \in V_i$. In terms of matrices we have

$$\rho(a) = \begin{pmatrix} \rho_1(a) & & 0 \\ & \ddots & \\ 0 & & \rho_n(a) \end{pmatrix},$$

where each $\rho_i(a)$ is a block instead of just an entry.

For notation, we use mV to denote $V \oplus \cdots \oplus V$ for m times.

Lemma 1.2.7. *If $W, W' \subseteq V$ subrepresentations such that $W + W' = V, W \cap W' = \{0\}$, then $V \simeq W \oplus W'$ as $A-$representations.*

Proof. It suffices to consider the homomorphism:

$$\phi : W \oplus W' \longrightarrow V,$$

$$(w, w') \longmapsto w + w'.$$

Then the statement follows. □

Example 1.2.8. (1). Let $A = K[S_m]$ and (V, ρ) representation defined by $\pi \cdot \rho_i = \rho_{\pi(i)}$, then $W = \{(x, \cdots, x), x \in K\}$, which is isomorphic to the trivial representation, is subrepresentation. Also consider $W' = \{(x_1, \cdots, x_n), \sum x_i = 0\}$ is a subrepresentation.

(2). Let $A = \mathbb{C}[S_3], \pi \cdot \rho_i = \rho_{\pi(i)}$. In basis $\{(1,1,1), (1,-1,0), (1,0,-1)\}$ where the first term is from W and the latter two are from W', we get

$$\rho((1,2)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \rho((1,3)) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & -1 \end{pmatrix},$$

and we have $\rho(a) = \begin{pmatrix} \star & 0 & 0 \\ 0 & \star & \star \\ 0 & \star & \star \end{pmatrix}$.

Lemma 1.2.9 (Matschke). *Let G be a finite group, suppose $\operatorname{char}(k)$ does not divide $|G|$. Then any finite representation of G is isomorphic to a sum of irreps.*

Proof. It suffices to show that $\forall W \subseteq V$ subrepresentations W, there exists $\overline{W} \subseteq V$ subrepresentations such that $V \simeq W \oplus \overline{W}$. That is, it suffices to show $W + \overline{W} = V$ and $W \cap \overline{W} = \{0\}$. We start with $W' \subseteq V$ subspace such that $W + W' = V$ and $W \cap W' = \{0\}$.

Let $\phi : V \to V$ linear such that $\phi|_W = \mathrm{Id}_W$ and $\phi|_{W'} = 0$. We have $W' = \ker \phi$ but $\phi \notin \mathrm{End}_{K[G]}(V)$ and W' not subrepresentation a priori.

Let $\psi = \sum_{g \in G} \rho(g^{-1}) \circ \phi \circ \rho(g)$ (i.e., $\psi(v) = \sum_{g \in G} g^{-1}\phi(gv)$). Thus we have

- $\psi \in \mathrm{End}_{K[G]}(V)$ because $\forall h \in G, \forall v \in V$, we have

$$\psi(hv) = \sum_{g \in G} g^{-1}\phi(ghv) = h \sum_{g \in G} h^{-1}g^{-1}\phi(ghv) = h \sum_{g \in G} g^{-1}\phi(gv) = h\psi(v).$$

Hence $\overline{W} = \ker \psi$ is a subspace. We have

- $\text{Im}\psi = W$ because first $\text{Im}\psi \subseteq \sum_g g^{-1}\text{Im}\phi = \sum_g g^{-1}w \subseteq \sum w = W$. Second, we have $\forall w \in W, \psi(w) = \sum g^{-1}\phi(gw) = \sum_g g^{-1}gw = |G|w \neq 0$ in k (this is why we need the condition for $\text{char}(k)$). Thus $w = \psi(\frac{w}{|G|})$ and $w \in \text{Im}\psi$. We have

- $\text{Im}\psi \cap \ker\psi = \{0\}$ because $\forall v \in \text{Im}\psi \cap \ker\psi$ we have $v = \psi(\frac{v}{|G|}) = 0$. We have

- $\text{Im}\psi + \ker\psi = V'$ because $v = \psi(\frac{v}{|G|}) + (v - \psi(\frac{v}{|G|}))$.

Hence the lemma. □

Lemma 1.2.10 (Schur's Lemma)**.** *Let K be algebraically closed, let A be a $K-$algebra, let V, W be irreducible representations of A, then*

$$\dim(\text{Hom}_A(V, W)) = \begin{cases} 1 & \text{if } V \simeq W, \\ 0 & \text{otherwise} \end{cases}.$$

Proof. Let $\phi \in \text{Hom}_A(V, W), \phi \neq 0$ and $\ker(\phi)$ is subspace of V irreducible, then $\ker\phi = 0$. Similarly, $\text{Im}\phi$ is subspaces of W irreducible, thus $\text{Im}\phi = W$. Hence ϕ is isomorphism. Thus if $V \not\simeq W$ then $\text{Hom}_A(V, W) = \{0\}$.

Suppose now $V \simeq W$. Then up to composing by an isomorphism, we can assume $W = V$. We want to show $\dim(\text{End}_A(V)) = 1$. We claim $\text{End}_A(V) = \{\lambda\text{Id}_V, \lambda \in k\}$. Now for one direction $\supseteq$, it is obvious. For the other direction $\subseteq$, let $\phi \in \text{End}_A(V), \forall\lambda \in k$, we have $\phi - \lambda\text{Id} \in \text{End}_A(V) = \text{Aut}_A(V) \cup \{0\}$. Since k is algebraically closed, $\exists\lambda \in k$ eigenvalue of ϕ (root of characteristic polynomial), then $\ker(\phi - \lambda\text{Id}) \neq 0$. Therefore $\phi - \lambda\text{Id}$ is not isomorphism thus $\phi - \lambda\text{Id} = 0$. □

Corollary 1.2.11. *Let K be algebraically closed, let $V_1, \cdots, V_k$ be non-isomorphic irreps of A, then*

$$\dim(\text{Hom}_A(\bigoplus_{i=1}^k n_iV_i, \bigoplus_{j=1}^k m_jV_j)) = \sum_{i=1}^k n_im_i.$$

In particular, if $U \simeq \bigoplus m_iV_i$, then $m_i = \dim(\text{Hom}_A(V_i, U))$. So the multiplicities of irreps in a representation are uniquely defined.

Before proving this corollary, we first claim and prove some lemma.

Lemma 1.2.12. *Let $V, V_1, \cdots, V_k$ be $A-$representations, then*

(1). $\text{Hom}_A(V, \bigoplus_i V_i) \simeq \bigoplus_i \text{Hom}_A(V, V_i)$ *as vector spaces; and*

(2). $\text{Hom}_A(\bigoplus_i V_i, V) \simeq \bigoplus_i \text{Hom}_A(V_i, V)$ *as vector spaces.*

Hence, $\text{Hom}_A(\bigoplus_i V_i, \bigoplus W_j) \simeq \bigoplus_{i,j} \text{Hom}_A(V_i, W_j)$.

Proof of Lemma 1.2.12. (1). Consider isomorphism given by

$$\bigoplus_i \mathrm{Hom}_A(V, V_i) \longrightarrow \mathrm{Hom}_A(V, \bigoplus_i V_i),$$

$$(\phi_1, \cdots, \phi_k) \longmapsto (\phi : v \mapsto (\phi_1(v), \cdots, \phi_k(v))).$$

(2). Consider isomorphism given by

$$\bigoplus_i \mathrm{Hom}_A(V_i, V) \longrightarrow \mathrm{Hom}_A(\bigoplus_i V_i, V),$$

$$(\phi_1, \cdots, \phi_k) \longmapsto (\phi : (v_1, \cdots, v_k) \mapsto \sum_i \phi_i(v_i)).$$

Hence the lemma. □

Then we can prove the corollary.

Proof of Corollary 1.2.11. We have

$$\begin{aligned}
\dim(\mathrm{Hom}_A(\bigoplus_i n_i V_i, \bigoplus_j m_j V_j)) &= \dim(\bigoplus_{i,j} n_i m_j \mathrm{Hom}_A(V_i, V_j)) \\
&= \sum_{i,j} n_i m_j \dim(\mathrm{Hom}_A(V_i, V_j)) \\
&= \sum_{i,j} n_i m_j \delta_{ij} = \sum_{i=1}^{k} n_i m_j,
\end{aligned}$$

where δ_{ij} is Kronecker delta by Schur's Lemma. □

2 Representations of Finite Groups

2.1 Fundamental Isomorphisms

Assumptions: Let G be a finite group, K be algebraically closed, $\mathrm{char}(K) \nmid |G|$ (so Matschke's and Schur's Lemmas hold). "Irreps of G" is the irreps of $K[G]$.

Theorem 2.1.1. *Group G has finitely many (non-isomorphic) irreducible representations $V_1, \cdots, V_r$. Moreover $V_{\mathrm{reg}} \simeq \bigoplus_{i=1}^{r} \dim(V_i)V_i$ as $G-$representations.*

Example 2.1.2. Let $K = \mathbb{C}, G = S_3$. We know 3 irreps already. They are

V_1 = trivial representation. ($\rho_1(\pi) = \mathrm{Id}_{\mathbb{C}}$),

V_2 = sign representation. ($\rho_2(\pi) = \mathrm{sgn}(\pi)\mathrm{Id}_{\mathbb{C}}$),

V_3 of dimension 2 determined by

$$\rho((1,2)) = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \rho((1,3)) = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

There are no other irreps and

$$\mathbb{C}[S_3] \simeq V_1 \oplus V_2 \oplus 2V_3$$

as S_3-representations.

Equivalently, there exists basis of $\mathbb{C}[S_3]$ in which

$$\rho_{\mathrm{reg}}((1,2)) = \begin{pmatrix} 1 & & & & & \\ & -1 & & & & \\ & & -1 & -1 & & \\ & & 0 & 1 & & \\ & & & & -1 & -1 \\ & & & & 0 & 1 \end{pmatrix},$$

and

$$\rho_{\text{reg}}((1,3)) = \begin{pmatrix} 1 & & & & & \\ & -1 & & & & \\ & & 1 & 0 & & \\ & & -1 & -1 & & \\ & & & & 1 & 0 \\ & & & & -1 & -1 \end{pmatrix}.$$

Proof of Theorem 2.1.1. By Matschke's Lemma, we have $V_{\text{reg}} \simeq \bigoplus_i m_i V_i$ for some $m_i \geqslant 0, V_i$ irreps. By Schur's Lemma, we have $m_i = \dim(\text{Hom}_G(V_{\text{reg}}, V_i))$.

For $(V,\rho), G-$representations, let $H_V = \text{Hom}_G(V_{\text{reg}}, V)$. We claim that

$$H_V = \{\epsilon_v, v \in V\}, \text{where } \epsilon_v : V_{\text{reg}} = K[G] \longrightarrow V,$$

$$x \longmapsto x \cdot v.$$

For one direction $(\supseteq)$: we have for all $v \in V$, that $\epsilon_v \in H_V$ since $\forall a \in K[G]$, we have $\epsilon_v(a \cdot x) = (a \cdot x) \cdot v = (a \times x) \cdot v = a \cdot (x \cdot v) = a \cdot \epsilon_v(x)$.
For the other direction $(\subseteq)$: for all $\phi \in H_V$, we have $\phi = \epsilon_{\phi(1_G)}$, indeed, $\forall x \in V_{\text{reg}}$, we have $\phi(x) = \phi(x \cdot 1_G) = x \cdot \phi(1_G) = \epsilon_{\phi(1_G)}(x)$.

Conclusion:

$$\epsilon : V \longrightarrow H_v,$$

$$v \longmapsto \epsilon_v,$$

is a surjective linear map. Also, ϵ is injective since $v \in \ker(\epsilon)$ implies $\epsilon_v(1_G) = 0$, which means $1_G \cdot v = 0$ so $v = 0$.

Hence ϵ is bijective linear map. Hence $\dim(H_V) = \dim(V)$. This concludes the proof. □

Theorem 2.1.3 (Fundamental Isomorphism for Group Algebra). *Let $V_1, \cdots, V_R$ be the non-isomorphic irreps of V. Then*

$$\Gamma : K[G] \longrightarrow \bigoplus_{i=1}^{R} \text{End}(V_i),$$

$$x \longmapsto (\rho_1(x), \cdots, \rho_R(x)),$$

is an isomorphism of algebras.

Example 2.1.4. (1). Let $G = S_3, K = \mathbb{C}, R = 3$, we have

$$\rho((1,2)) = ([1], [-1], \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}), \rho((1,3)) = ([1], [-1], \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}),$$

and $\mathbb{C}[S_3]$ isomorphic to algebra of matrix in $\mathrm{Mat}_4(\mathbb{C})$ of form $\begin{pmatrix} \star & & & \\ & \star & & \\ & & \star & \star \\ & & \star & \star \end{pmatrix}$.

(2). Let $G = C_n, K = \mathbb{C}, \Gamma$ is given by DFT, we have

$$\rho_{\text{reg}}(g^k) = \begin{pmatrix} \omega^{-(1-1)k} = 1 & & 0 \\ & \ddots & \\ 0 & & \omega^{-(m-1)k} \end{pmatrix}.$$

We have $\mathbb{C}[S_n] \overset{\Gamma = DFT}{\longleftrightarrow}$ algebra of diagonal matrices.

Proof of Theorem 2.1.3. By definition of $G-$representations, for all i, ρ_i is a homomorphism of algebra, hence Γ is a homomorphism of algebra.

We have $\dim(K[G]) = |G|$. We see $\dim(\bigoplus \mathrm{End}(V_i)) = \sum \dim(\mathrm{End}(V_i)) = \sum \dim(V_i)^2$. Moreover, by Theorem 1.3.1., we have

$$\dim(K[G]) = \dim(\bigoplus \dim(V_i)V_i) = \sum \dim(V_i)\dim(V_i).$$

We have Γ is injective since $x \in \ker(\Gamma)$, which implies $\forall i, \rho_i(x) = 0$. This means that $\rho_{\text{reg}}(x) = 0$ and hence $x = x \cdot 1_G = \rho_{\text{reg}}(x)(1) = 0$. $\square$

Corollary 2.1.5. *We have number of non-isomorphic irreps of G = number of conjugacy classes.*

Example 2.1.6. For S_n, we have number of irreps = number of "cyclic types" = number of partitions of n.

Proof of Corollary 2.1.5. Theorem 2.1.3 implies $Z(K[G]) \overset{\Gamma}{\simeq} Z(\bigoplus_{i=1}^R \mathrm{End}(V_i))$, we take dimension on both sides, then $Z(\bigoplus \mathrm{End}(V_i)) = \bigoplus Z(\mathrm{End}(V_i))$. Moreover, $Z(\mathrm{End}(V_i)) = \{\lambda \mathrm{Id}_{V_i}, \lambda \in k\}$ has $\dim = 1$. This implies that $\dim(\bigoplus_{i=1}^R \mathrm{End}(V_i)) = \sum_{i=1}^R \dim(\mathrm{End}(V_i)) = R$.

Also $x \in Z(K[G])$ if and only if $\forall h \in G, hxh^{-1} = x$. Hence $x = \sum_{g \in G} C_g g \in Z$ if and only if $\forall g, g'$ conjugate, we have $C_g = C_{g'}$ (i.e., coefficients are constant over conjugate class).

Together we see that basis of Z is $\mathcal{C}_1, \cdots, \mathcal{C}_k$ where $\mathcal{C}_i = \sum_{g \in G_i} g$, where G_i are conjugacy class of G. Hence $\dim(Z)$ = number of conjugacy classes and hence $\sum_{i=1}^n \dim(\mathrm{End}(V_i)) = R$ = number of irreps. $\square$

Consider $x = \sum_{i<j} (i,j) \in Z(\mathbb{C}[S_n])$. What is x^k? Let $V_1, \cdots, V_R$ be irreps of G, and let $P_i = \Gamma^{-1}(0, \cdots, \mathrm{Id}_{V_i}, \cdots, 0)$. Since $(0, \cdots, \mathrm{Id}_{V_i}, \cdots, 0)$ form a basis of $Z(\bigoplus \mathrm{End}(V_i))$, we have $\{P_1, \cdots, P_R\}$ is a basis of $Z(K[G])$. Then we have the following definition:

Definition 2.1.7. This basis satisfies $P_iP_j = \delta_{ij}P_i$ where the δ_{ij} is the Kronecker delta. These are the **idempotents** of the group algebra.

They make computation in $Z(K[G])$ easy. For instance, if $x = \sum c_iP_i$ then $x^k = \sum c_i^kP_i$. In the C_n example, P_i are the pointwise waves and multiplication in $\mathbb{C}[C_n]$ is "simplified" by DFT.

2.2 Characters

Definition 2.2.1. Let A be a $K-$algebra, let (V, ρ) be $A-$representations, the **character** of (V, ρ) is

$$\chi_V : A \longrightarrow k,$$

$$a \longmapsto \mathrm{Tr}(\rho(a)),$$

where Tr is the trace of the matrices.

This is well-defined, that is, does not depend on basis used to write $\rho(a)$ because the trace of $\mathrm{Tr}(P^{-1}MP) = \mathrm{Tr}(PP^{-1}M) = \mathrm{Tr}(M)$.

Example 2.2.2. If (V, ρ) is the $G-$representations associated to a $G-$set S, then $\forall g \in G$, we have $\chi(g) =$ number of elements of S fixed by g.

Remark 2.2.3. We have

- $\chi_V(1_A) = \mathrm{Tr}(\mathrm{Id}_V) = \dim(V)$.
- We have $\chi_V \in A^* = \mathrm{Hom}(A, K)$ the dual space.
- If $V \simeq W$, then $\chi_V = \chi_W$ because V, W are equal up to change of basis and $\mathrm{Tr}(PMP^{-1}) = \mathrm{Tr}(M)$.

Notation: Let G be a finite group, then we say

$$\mathcal{F}(G) = K[G]^*(\overset{bijective}{\longleftrightarrow} \{f : G \to K\}).$$

Also we define

$$\mathcal{CF}(G) = \{\phi \in F(G) | \phi(g) = \phi(g'), \forall g, g' \text{ conjugate in } G\}$$

$$(\overset{bijective}{\longleftrightarrow} \{f : G \to K \text{ such that } f \text{ is constant on conjugacy class}\}).$$

Vector space of **class functions** on G.

Remark 2.2.4. We have $\mathcal{F}(G) = K[G]^* \simeq K[G]$ as vector spaces and $\mathcal{CF}(G) \simeq Z(K[G])^* \simeq Z(K[G])$ as vector spaces.

In fact, we have that $\chi_V \in \mathcal{CF}(G)$.

Theorem 2.2.5. *Let G be finite group, let $V_1, \cdots, V_R$ be the irreps, the characters $\chi_1, \cdots, \chi_R$ of the irreps form a basis of $\mathcal{CF}(G)$.*

Example 2.2.6. Let $G = S_3$, $K = \mathbb{C}$, denote V_1 trivial representation, V_2 sign representation, V_3 defining trivial, then we have the table

Character			
	χ_1	χ_2	χ_3
$\mathcal{C}_1 = \{\mathrm{Id}\}$	1	1	2
$\mathcal{C}_2 = \{(1,2),(2,3),(1,3)\}$	1	-1	0
$\mathcal{C}_3 = \{(1,2,3),(3,2,1)\}$	1	1	-1

and we have $\chi_3 =$ number of fixed points -1. Theorem 1.4.5 says χ_1, χ_2, χ_3 form a basis of $\mathcal{CF}(S_3) \equiv \mathbb{C}^3$ (i.e., columns are basis of $\mathbb{C}^3$).

Proof of Theorem 2.2.5. First we have $\dim(\mathcal{CF}(G)) =$ number of conjugacy classes $=$ number of irreps $= R$. This means that it suffices to show $\chi_1, \cdots, \chi_R$ are independent. Now we show this claim.

Indeed, consider $P_i = \Gamma^{-1}(0, \cdots, \mathrm{Id}_{V_i}, \cdots, 0)$ idempotents. We have

$$\chi_j(P_i) = \mathrm{Tr}(\rho_j(P_i)) = \mathrm{Tr}(\delta_{ij}\mathrm{Id}_{V_i}) = \delta_{ij}\dim(V_j).$$

In particular, we have $\sum_{j=0}^n k_j\chi_j = 0$ thus $\forall j, \sum k_j\chi_j(P_i) = 0$. Hence for any i, we have $k_i = 0$. $\square$

Remark 2.2.7. Recall that $\{P_1, \cdots, P_R\}$ forms a basis of $Z(K[G])$. Proof shows that $\{\frac{\chi_1}{\dim(V_1)}, \cdots, \frac{\chi_R}{\dim(V_R)}\}$ is the dual basis $\{P_1^* \cdots P_R^*\}$ of $Z(K[G])^* \simeq \mathcal{CF}(G)$.

2.3 Frobenius Formula and Orthogonality

Notation:

- Let $\mathcal{C}_1, \cdots, \mathcal{C}_R$ be the conjugacy classes of G, let $\chi_1, \cdots, \chi_R$ be the characters of irreps of G, let $\chi_i(\mathcal{C}_j) = \chi_i(g)$ for any $g \in \mathcal{C}_j$.

- For $\mathcal{D}_1, \cdots, \mathcal{D}_k$ be conjugacy classes ($\mathcal{D}_i \in \{\mathcal{C}_1, \cdots, \mathcal{C}_R\}$), we denote

$$F(\mathcal{D}_1, \cdots, \mathcal{D}_k) = \text{ cardinality of } \{(g_1, \cdots, g_k) | g_i \in \mathcal{D}_i, g_1, \cdots, g_k = 1_G\}.$$

Then we have the theorem:

Theorem 2.3.1 (Frobenius Formula). *For any $k \geqslant 1$ and for any $\mathscr{D}_1, \cdots, \mathscr{D}_k$, we have*

$$F(\mathscr{D}_1, \cdots, \mathscr{D}_k) = \frac{|\mathscr{D}_1| \cdots |\mathscr{D}_k|}{|G|} \sum_{i=1}^{R} \frac{\chi_i(\mathscr{D}_1) \cdots \chi_i(\mathscr{D}_k)}{\dim(V_i)^{k-2}}.$$

Proof. Let $D_i = \sum_{g \in \mathscr{D}_i} g \in Z(K[G])$, note that $F(\mathscr{D}_1, \cdots, \mathscr{D}_n) =$ coefficients of 1_G in $D_1 \cdots D_k$. Then observe that

$$\chi_{\text{reg}}(g) = \begin{cases} |G| & \text{if } g \in 1_G, \\ 0 & \text{otherwise (because } gh \neq h, \forall h \in G) \end{cases}.$$

Thus $\chi_{\text{reg}}(x) = |G|$ multiplies the coefficient of 1_G in x. Hence $F(\mathscr{D}_1, \cdots, \mathscr{D}_n) = \frac{1}{|G|}\chi_{\text{reg}}(D_1 \cdots D_k)$. Moreover, $V_{\text{reg}} \simeq \bigoplus \dim(V_i) V_i$ thus $\chi_{\text{reg}} = \sum (V_i)\chi_i$. Therefore, we have

$$F(\mathscr{D}_1, \cdots, \mathscr{D}_n) = \frac{1}{|G|} \sum_{i=1}^{R} \dim(V_i)\chi_i(D_1 \cdots D_n).$$

By fundamental isomorphism $\Gamma : K[G] \to \text{End}(V_i)$, we have $D_j \in Z(K[G])$ which implies that for any i, $\rho_i(D_j) = k_{ij}\text{Id}_{V_i}$ for some $k_{ij} \in k$. Moreover, $\chi_i(D_j) = k_{ij} \dim(V_i)$ thus we see

$$k_{ij} = \frac{\chi_i(D_j)}{\dim(V_i)} = \frac{|\mathscr{D}_j|\chi_i(\mathscr{D}_j)}{\dim(V_i)}$$

$$\implies \forall i, \rho_i(D_1 \cdots D_j) = \rho_i(D_1) \cdots \rho_i(D_k) = \prod_{j=1}^{k} \left(\frac{\mathscr{D}_j \chi_i(\mathscr{D}_j)\text{Id}_{V_i}}{\dim(V_i)}\right)$$

$$\implies \forall i, \chi_i(D_1 \cdots D_j) = \frac{\prod_{j=1}^{k} |\mathscr{D}_j|\chi_i(\mathscr{D}_j)}{\dim(V_i)^{k-1}}$$

$$\implies F(\mathscr{D}_1 \cdots \mathscr{D}_n) = \frac{1}{|G|} \sum_{i=1}^{R} \frac{\prod_{j=1}^{k} |\mathscr{D}_j|\chi_i(\mathscr{D}_j)}{\dim(V_i)^{k-2}}.$$

$\square$

From now on we take $K = \mathbb{C}$.

Definition 2.3.2. We define an **inner product** $\langle , \rangle$ on $\mathscr{F}(G) = K[G]^*$ by such that for all $\phi, \psi \in \mathscr{F}(G)$, we have

$$\langle \phi, \psi \rangle = \frac{1}{|G|} \sum_{g \in G} \phi(g)\overline{\psi(g)},$$

where $\bar{\cdot}$ is complex conjugate.

Theorem 2.3.3 (Orthogonal Relations). *Let $\chi_1, \cdots, \chi_R$ be the characters of irreps. We have*

(1). For all $i, j, \langle \chi_i, \chi_j \rangle = \delta_{ij}$. In other words, $\chi_1, \cdots, \chi_R$ forms an orthogonal basis of $\mathcal{CF}(G)$.

(2). For all i, j, we have

$$\sum_{k=1}^{R} \chi_k(\mathcal{C}_i)\overline{\chi_k(\mathcal{C}_j)} = \delta_{i,j}\frac{|G|}{|\mathcal{C}_i|},$$

where $\mathcal{C}_1, \cdots, \mathcal{C}_R$ are the conjugacy classes.

Lemma 2.3.4. *Let χ be a character of G, then we have*

$$\chi(g^{-1}) = \overline{\chi(g)}, \forall g \in G.$$

Proof. Exercise. □

Proof of Theorem 2.3.3. For (2), we have

$$\sum_{k=1}^{R} \chi_k(\mathcal{C}_i)\overline{\chi_k(\mathcal{C}_j)} = \sum_{k=1}^{R} \chi_k(\mathcal{C}_i)\chi_k(\mathcal{C}_j^{-1}) = \frac{|G|}{|\mathcal{C}_i||\mathcal{C}_j|}F(\mathcal{C}_i, \mathcal{C}_j^{-1})$$

$$= \frac{|G|}{|\mathcal{C}_i||\mathcal{C}_j|}\delta_{ij}|\mathcal{C}_i| = \frac{|G|}{|\mathcal{C}_i|}\delta_{ij}.$$

For (1), let $M = (\frac{\sqrt{|\mathcal{C}_i|}\chi_j(\mathcal{C}_i)}{\sqrt{|G|}})$, then we have

$$(2) \implies M \cdot \overline{M^T} = \mathrm{Id} \implies M^T \cdot \overline{M} = \mathrm{Id}$$

$$\implies \frac{1}{|G|}\sum_k |\mathcal{C}_k|\chi_i(\mathcal{C}_k)\overline{\chi_j(\mathcal{C}_k)} = \delta_{ij} \iff \frac{1}{|G|}\sum_{g\in G} \chi_i(g)\overline{\chi_j(g)} = \delta_{ij}.$$

Hence the corollary. □

Corollary 2.3.5. *Let V, V' be finite dimensional $G-$representations and let χ, χ' be their characters. Then we have*

$$V \simeq V' \iff \chi = \chi'.$$

Proof. ($\Longrightarrow$): If $V \simeq V'$, then there exists an invertible matrix P such that

$$\forall x \in K[G], \rho'(x) = P^{-1}\rho(x)P.$$

Hence

$$\forall x \in K[G], \chi'(x) = \mathrm{Tr}(\rho'(x)) = \mathrm{Tr}(P^{-1}\rho(x)P) = \mathrm{Tr}(\rho(x)) = \chi(x).$$

($\Longleftarrow$): Suppose $\chi = \chi'$, we can decompose V, V' into irreps:

$$V \simeq \bigoplus_{i=1}^{r} m_i V_i \text{ and } V' \simeq \bigoplus_{i=1}^{r} m_i' V_i.$$

This gives $\chi = \sum_{i=1}^{r} m_i \chi_i = \chi = \chi' = \sum_{i=1}^{r} m_i' \chi_i$. Hence by Theorem 2.2.5, we have $m_i = m_i'$ for all i. Thus $V \simeq V'$. $\square$

Corollary 2.3.6. *Suppose $K = \mathbb{C}$. Let V, V' be $G-$representations and let χ, χ' be their characters. Let $\chi_1, \cdots, \chi_r$ be the characters of the irreps $V_1, \cdots, V_r$ of G. Then*

(a). The multiplicity m_k of V_k in V is $\langle \chi, \chi_k \rangle$.

(b). We have $\langle \chi, \chi' \rangle = \sum_{k=1}^{r} m_k m_k' = \dim(\mathrm{Hom}_G(V, V'))$ where we have m_k, m_k' multiplicities of V_k in V, V'.

Proof. The characters χ_1, χ_r are orthonormal for the inner product, so

(a). We have $V \simeq \bigoplus_{i=1}^{r} m_i V_i \Longrightarrow \chi = \sum_{i=1}^{r} m_i \chi_i \Longrightarrow \langle \chi, \chi_k \rangle = \langle \sum_i m_i \chi_i, \chi_k \rangle = m_k$.

(b). We have $\langle \chi, \chi' \rangle = \langle \sum_i m_i \chi_i, \sum_j m_j' \chi_j \rangle = \sum_{k=1}^{r} m_k m_k' = \dim(\mathrm{Hom}_G(V, V'))$ where the last equality is by the corollary of Schur's Lemma.

Hence the corollary. $\square$

Exercise: Let $G = S_n$ and let V be the representation given by $V = C^n$ and $\pi \cdot e_i = e_{\pi(i)}$ for all i in $[n]$. Multiplicity of trivial representation in $V =$?

We see $\langle \chi_V, \chi_{trivial} \rangle = \frac{1}{n!} \sum_{\pi \in S_n} \mathrm{fix}(\pi) =$ average number of fixed points $= 1$ where $\mathrm{fix}(\pi)$ is the number of fixed points of π.

Note that V is the sum of 2 irreps $\Longleftrightarrow \langle \chi_V, \chi_V \rangle = \frac{1}{n!} \sum_{\pi \in S_n} \mathrm{fix}(\pi)^2 = 2$.

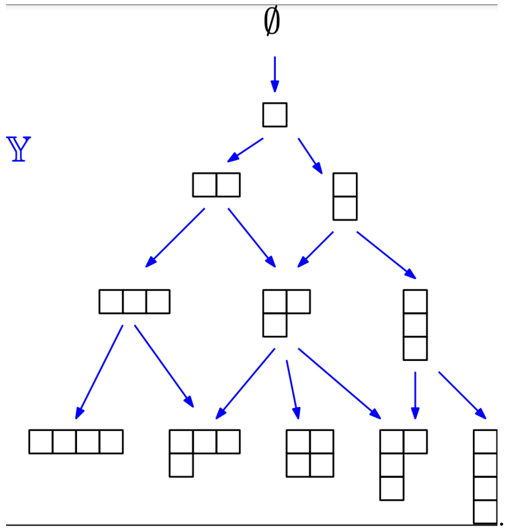
2.4 Restricted and Induced Representations

Definition 2.4.1. Let H be a subgroup of G. Any representation (V, ρ) of G gives a representation of H by taking the restriction $\rho|_H : H \to \mathrm{End}(V)$. We denote by $V_{G \to H}$ this **restricted representation** of H.

Remark 2.4.2. For an irreducible repres of G, the restriction may not be irreducible.

Example 2.4.3. Irreps of symmetric group (not proved in this class).

Recall conjugacy classes of $S_n \Longleftrightarrow$ cyclic types $\Longleftrightarrow$ "partitions of n" = ways of writing n as a sum of positive integers $n = n_1 + \cdots + n_k$ (with n_i arranged in weakly decreasing order) $\Longleftrightarrow$ "Young diagram",



Hence the number of irreps of S_n = number of partitions of n = Young diagrams with n boxes.

Fact: one can index the irreps of S_n by the Young diagram in such a way that the set of irreps of S_n is V_λ, λ Young diagram of size n and

$$(V_\lambda)_{S_n \to S_{n-1}} = \bigoplus_{\mu \subset \lambda \text{ obtained by deleting one corner box}} V_\mu.$$

Corollary 2.4.4. *We have* $\dim(V_\lambda)$ = *number of paths from* $\varnothing$ *to* λ *in the Young lattice.*

Question: For $H \lhd G$, how can we get a repres of G from a repres of H?

Reminder: We have G acts on G/H by left-translation: If $G/H = \{a_1 H, \cdots, a_k H\}$, this action is

$$\alpha : G \longrightarrow \mathrm{Perm}(G/H),$$

$$\alpha(g) : a_i H \longmapsto g a_i H.$$

This action gives a representation (W, τ) where the matrices $\tau(g) = (t_{i,j})_{i,j \in [k]}$ are permutation matrices: $t_{i,j} = 1$ if $g a_j H = a_i H$ and 0 otherwise.

Definition 2.4.5. Let H be a subgroup of G. Let $a_1, \cdots, a_k$ in G be representatives of left-cosets: $G/H = \{a_1 H, \cdots, a_k H\}$. Let (V, ρ) be a $H-$representation. The **induced representation** $(V_{H \to G}, \rho_{H \to G})$ (for our choice $a_1, \cdots, a_k$) is the

$G-$representation with matrices

$$\forall g \in G, \rho_{H\to G}(g) = \begin{pmatrix} M_{1,1}(g) & & M_{1,k}(g) \\ & \ddots & \\ M_{k,1}(g) & & M_{k,k}(g) \end{pmatrix},$$

where $M_{i,j}(g) = \begin{cases} \rho(a_i^{-1}ga_j) & \text{if } ga_jH = a_iH(\text{ equivalently } a_i^{-1}ga_j \in H), \\ 0 & \text{otherwise.} \end{cases}$

Lemma 2.4.6. *We have the following:*

(1). The tuple $(V_{H\to G}, \rho_{H\to G})$ is indeed a representation: this means that for all g, g', we have $\rho_{H\to G}(gg') = \rho_{H\to G}(g) \circ \rho_{H\to G}(g')$.

(2). Changing the representatives a_i gives an isomorphic representation.

(3). The character $\chi_{H\to G}$ of $V_{H\to G}$ is related to the character χ of V as follows:

$$\forall g \in G, \chi_{H\to G}(g) = \frac{1}{|H|} \sum_{f\in G|f^{-1}gf\in H} \chi(f^{-1}gf).$$

Proof. We prove (1), (3), and (2) respectively.

(1). Multiplying by blocks we get

$$\rho_{H\to G}(g)\rho_{H\to G}(g') = \begin{pmatrix} & B_{i,j} & \\ & & \\ & & \end{pmatrix}, B_{i,j} = \sum_{d=1}^{k} M_{i,d}(g)M_{d,j}(g'),$$

with $B_{i,j} = 0$ unless there exists d in $[k]$ such that $g'a_jH = a_dH$ and $ga_dH = a_iH$ (and this occurs if and only if $gg'a_jH = a_iH$). In this case, we have

$$B_{i,j} = M_{i,d}(g)M_{d,j}(g') = \rho(a_i^{-1}ga_d)\rho(a_d^{-1}g'a_j) = \rho(a_i^{-1}gg'a_j) = M_{i,j}(gg').$$

Hence $\rho_{H\to G}(g) \circ \rho_{H\to G}(g') = \rho_{H\to G}(gg')$.

(3). We have

$$\chi_{H\to G}(g) = \sum_{i|a_i^{-1}ga_i\in H} \chi(a_i^{-1}ga_i) = \sum_{i|a_i^{-1}ga_i\in H} \frac{1}{|H|} \sum_{h\in H} \chi(h^{-1}a_i^{-1}ga_ij)$$

$$= \frac{1}{|H|} \sum_{f\in G|f^{-1}gf\in H} \chi(f^{-1}gf),$$

where $f = a_ih$ and the last equality is from if $aH = bH$, then $a^{-1}ga \in H$ if and only if $b^{-1}gb \in H$.

(2). By (3), character does not depend on $a_1, \cdots, a_k$. Since a different choice of $a_1, \cdots, a_k$ gives the same character, the corresponding repres are isomorphic (by a previous corollary). □

Corollary 2.4.7 (Frobenius Reciprocity)**.** *Suppose $K = \mathbb{C}$, let H be a subgroup of G, let V be a representation of H with character χ and let V' be a representation of G with character χ'. Then we have*

$$\langle \chi_{H\to G}, \chi' \rangle = \langle \chi, \chi'_{G\to H} \rangle \text{ (inner product of } C[G]^* \text{ and } C[H]^*).$$

Proof. We have

$$\langle \chi_{H\to G}, \chi' \rangle = \frac{1}{|G|} \sum_{g\in G} \chi_{H\to G}(g)\overline{\chi'(g)} = \frac{1}{|G||H|} \sum_{g,f\in G | f^{-1}gf\in H} \chi(f^{-1}gf)\overline{\chi'(g)}$$

$$= \frac{1}{|G||H|} \sum_{g,f\in G | f^{-1}gf\in H} \chi(f^{-1}gf)\overline{\chi'(f^{-1}gf)},$$

hence

$$\langle \chi_{H\to G}, \chi' \rangle = \frac{1}{|G||H|} \sum_{h\in H} \sum_{g,f\in G|f^{-1}gf=h} \chi(h)\overline{\chi'(h)} = \frac{1}{|G||H|} \sum_{h\in H} |G|\chi(h)\overline{\chi'(h)}$$

$$= \langle \chi, \chi'_{G\to H} \rangle.$$

Hence the proof. □

Remark 2.4.8. For V, V' irreps of H and G respectively, this means that (via a previous corollary) multiplicity of V' in $V_{H\to G}$ = multiplicity of V in $V'_{H\to G}$.

Example 2.4.9. Consider $S_{n-1} \lhd S_n$. For any Young diagram λ we have

$$(V_\lambda)_{S_{n-1}\to S_n} = \bigoplus_{\mu\supset\lambda \text{ obtained by adding one box}} V_\mu.$$

3

Finite Dimensional Algebras

3.1 Fundamental Isomorphism

Throughout this subsection, we assume k algebraically closed, A is finite dimensional $K-$algebra (we do not have the Matschke Lemma).

Theorem 3.1.1 (Density Theorem)**.** *Let $(V_1, \rho_1), \cdots, (V_R, \rho_R)$ be non-isomorphic irreps of A, that is, for $v \in V_i$, $A \cdot v = V_i$. Let*

$$\Gamma : A \longrightarrow \bigoplus_{i=1}^{R} \mathrm{End}(V_i),$$

$$x \longmapsto (\rho_1(x), \cdots, \rho_R(x)).$$

Then Γ is a surjective algebra homomorphism.

Lemma 3.1.2. *Any subrepresentations of a sum of irreps is isomorphic to a sum of irreps.*

Proof. (1). Claim: Let $\phi : V \to W$ be representation homomorphism such that there exists $\psi : W \to V$ representation homomorphism and $\phi \circ \psi = \mathrm{Id}_W$. Then $V \simeq \ker\phi \oplus \mathrm{Im}\phi$. Proof of claim as exercise.

(2). Let W be subrepresentations of $V = \bigoplus m_i V_i$, and V_i are irreps, we show $W \simeq$ sum of V_i by induction on $\sum m_i$.

Base case $\sum m_i = 0$ trivial.

Induction step: Let $W \overset{\phi}{\hookrightarrow} \bigoplus m_i V_i$ inclusion map, let U be irreducible subrepresentation of W, then ϕ decomposes: there exists $\phi_{k,j} : W \to V_k, k \in [R], j \in [m_k]$ representation homomorphism such that

$$\phi(x) = (\phi_{k,j}(x))_{k\in[R],j\in[m_k]}.$$

We have $\phi_{k,j}|_U : U \to V_k$ is 0 as isomorphism since U, V_k irreducible. Also there exists k, j such that $\phi_{k,j}|_U$ is isomorphism. Thus $U \simeq V_k$ and there exists $\psi := (\phi_{k,j}|_U)^{-1}$ such that $\phi_{k,j} \circ \psi = \mathrm{Id}_{V_k}$. By previous choice $W \simeq \mathrm{Im}(\phi_{k,j}) \oplus \ker(\phi_{k,j})$ where the first component is V_k and the second component is isomorphic to $\bigoplus m_i' V_i$ where $m_k' = m_k - 1, m_i = m_i, \forall i \neq k$. By the induction hypothesis, $\ker(\phi_{k,j}) \simeq$ sum of irreps and hence $W \simeq$ sum of irreps.

Hence the lemma. □

Proof of Theorem 3.1.1. Let $n_k = \dim(V_k)$, let $(e_{k,1}, \cdots, e_{k,n_k})$, let

$$\psi : A \longrightarrow \bigoplus m_k V_k,$$

$$x \longmapsto (x \cdot e_{k,j})_{k \in [R], j \in [n_k]}.$$

Note that $x \cdot e_{k,j} = \rho_k(x)(e_{k,j}) =$ "$j-$th column of $\rho_k(x)$". Therefore Γ surjective $\iff \psi$ surjective. Now we want to show ψ is surjective.

Since $\mathrm{Im}\psi \subseteq \bigoplus n_k V_k, \mathrm{Im}\psi \simeq \bigoplus n_k V_k$ by lemma. To prove surjectivity, it suffices to show $m_k = n_k$ for all k (by dimension argument). Consider the map

$$\phi : \bigoplus m_k V_k \simeq \mathrm{Im}(\psi) \hookrightarrow \bigoplus n_k V_k,$$

where ϕ from the first term on the left to the last term with ϕ being representation homomorphism. Decomposition of homomorphism ϕ : there is $\phi_{l,i,k,j} : V_l \to V_k$ with

$$\phi((V)_{l,i})_{l \in [R], i \in [m_l]} = (\sum_{l,i} \phi_{l,i,k,j}(V_{l,i}))_{k \in [R], j \in [m_k]}.$$

By Schur Lemma, $\phi_{l,i,k,j} = \begin{cases} 0 & \text{if } l \neq k, \\ c_{ij}^{(k)} \mathrm{Id} V_k & \text{if } l = k, c_{ij}^{(k)} \in k. \end{cases}$

Note that $(e_{k,j})_{k \in [R], j \in [n_k]} = \psi(1_A) \in \mathrm{Im}(\phi)$. Therefore we have for all $k \in [R], \exists V_{k,1}, \cdots, V_{k,m_k} \in V_k$ such that

$$\left(c_{ij}^{(a)}\right) \begin{pmatrix} V_{k,1} \\ V_{k,2} \\ \vdots \\ V_{k,m_k} \end{pmatrix} = \begin{pmatrix} e_{k,1} \\ e_{k,2} \\ \vdots \\ e_{k,m_k} \end{pmatrix}.$$

Hence $V_{k,1}, \cdots, V_{k,m_k}$ generates the basis $e_{k,1}, \cdots, e_{k,n_k}$. Therefore $m_k \geqslant n_k, \forall k$. □

Definition 3.1.3. Let $\mathrm{rad}(A) = \{x \in A | \forall (V, \rho) \text{ irreps } \rho(x) = 0\}$ be the **Jacobson radical** of A.

Theorem 3.1.4 (Fundamental Isomorphism). *Let A be finite dimensional algebra over algebraically closed field k. There are finitely many (non-isomorphic) irreps of A. They are $(V_1, \rho_1), \cdots, (V_R, \rho_R)$ and*

$$\Gamma : A/\mathrm{rad}(A) \longrightarrow \bigoplus \mathrm{End}(V_i),$$

$$x + \mathrm{rad}(A) \longmapsto (\rho_1(x), \cdots, \rho_R(x)),$$

is isomorphism of algebra.

Proof. We have

- By density theorem, if $V_1, \cdots, V_k$ non-isomorphism irreps of A, then $A \to \bigoplus \mathrm{End}(V_i)$ is surjective. Hence $\dim(A) \geqslant \sum \dim(\bigoplus \mathrm{End}(V_i)) \geqslant k$. Hence at most $\dim(A)$ irreps.
- By density theorem, the map

$$\Lambda : A \longrightarrow \bigoplus \mathrm{End}(V_i),$$

$$x \longmapsto (\rho_1(x), \cdots, \rho_R(x))$$

  is surjective. Hence by basis isomorphism, $A/\ker(\Lambda) \simeq \bigoplus \mathrm{End}(V_i)$.
- We have $\ker \Gamma = \{a \in A | \rho_1(a) = 0, \cdots, \rho_R(a)\} = \mathrm{rad}(A)$.

Hence the theorem. □

Theorem 3.1.5. *Let A be finite dimensional algebra, then*

$$\mathrm{rad}(A) \overset{(1)}{=} \{x \in A | \exists n > 0, (x)^n = \{0\}\} \overset{(2)}{=} \bigcap_{M \text{ maximized left-ideal of } A} M,$$

where (x) is two-sided ideal generated by x. Then $I \times J = \{\sum_{i=1}^k xy, x_i \in I, y_i \in J\}$ product of ideal which implies $I^n = \{\sum_{i=1}^k x_{i1}, \cdots, x_{im} | x_{i,k} \in I\}$.

Lemma 3.1.6. *For any finite dimensional representations A, there is* ***filtration*** $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$ *subrepresentations such that V_i/V_{i-1} is irreducible.*

Proof. Induction on $\dim(V)$.

Let V_1 be an irreducible subrepresentation, by induction hypothesis V/V_1 has a filtration, then

$$U_0 \subset U_1 \subset \cdots \subset U_k = V/V_1 \cdots V_i/V_{i-1} \text{ irreducible}.$$

By basic isomorphism,

$$\{\text{subrepresentation of } V/V_1\} \overset{\text{bijection}}{\longleftrightarrow} \{\text{subrepresentations of } V \text{ containing } V_1\},$$

$$W/W_1 \longleftarrow W.$$

Hence there exists $W_0 \subseteq W_1 \subseteq \cdots \subseteq W_k \subseteq V$ such that $U_i = \frac{W_i}{V_1}$ and $W_i/W_{i-1} \simeq (W_i/V_1)/(W_{i-1}/V_1) = U_i/U_{i-1}$ irreducible. Thus $0 \subseteq W_0 = V_1 \subseteq W_1 \subseteq \cdots \subseteq W_k = V$ is a filtration for V. $\square$

Proof of Theorem 3.1.5. For part (1):

Suppose $x \notin \operatorname{rad}(A)$, then there is (V, ρ) irreps such that $\rho(x) \neq 0$. Since $(x) \cdot V$ is a nondegenrate subrepresentations, we get $(x) \cdot V = V$. Hence for all m, $(x)^m V = V$ implies that for all m, $(x)^m \neq 0$.

Let $0 = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_m = V_{\text{reg}}$ subrepresentation such that V_i/V_{i-1} irreducible. For all $x \in \operatorname{rad}(A)$, for all i, we have $xV_i/V_{i-1} = 0$ hence $xV_i \subseteq V_{i-1}$. Therefore for all $x \in (\operatorname{rad}(A))^m, xV_m \subseteq V_0 = 0$. Hence $(\operatorname{rad}(A))^m = 0$ and $\forall x \in \operatorname{rad}(A), (x)^m \subseteq (\operatorname{rad}(A))^m = 0$ therefore $x \cdot 1_A = 0$ thus $x = 0$.

For part (2):

Remark: We have I is left ideal of A if and only if I is subrepresentation of $V_{\text{reg}} = A$. Also M is maximal left ideal of A if and only if V_{reg}/M are irreducible representations.

($\subseteq$:) Let $x \in \operatorname{rad}(A)$. By (1), there is $m, (x)^m = 0$ hence for all $a \in A, (ax)^m = 0$. Therefore $\forall a \in A, 1 - ax$ is invertible become $(1 - ax)(1 + ax + (ax)^2 + \cdots + (ax)^{m-1}) = 1 - (ax)^m = 1$. Hence $x \in \bigcap_{M \text{ max left ideal}} M$. Indeed if $x \notin M$ on maximal left ideal, then $Ax + M = A$ where Ax is left ideal. Hence $\exists m \in M, a \in A$ such that $ax + m = 1_A$. Therefore $m = 1 - ax$ invertible by above and contradicts $M \neq A$.

($\supseteq$:) Homework: $x \in \bigcap M \implies x \in \bigcap_{i, v \in V_i} \operatorname{Ann}_{\rho_i}(v) = \operatorname{rad}(A)$. $\square$

3.2 Semisimplicity

Definition 3.2.1. An $A-$representation is **semisimple** if it is isomorphic to a sum of irreducible.

Example 3.2.2. If $A = K[G]$ is a group algebra over k of $\operatorname{char}(k) \nmid |G|$. Then any $A-$representation is semisimple by Matschke lemma.

Theorem 3.2.3. *Let k be algebraically closed field, and let A be a finite dimensional $K-$algebra, the following are equivalent:*

(1). Any finite dimensional $A-$representation is semisimple (= decomposible into irreps);

(2). The regular representation is semisimple;

(3). The radical $\operatorname{rad}(A) = 0$;

(4). *There is finite dimensional vector spaces $V_1, \cdots, V_R$ such that $A \simeq \bigoplus_{i=1}^R \mathrm{End}(V_i)$ as algebra.*

*We call A **semisimple** in this case. In this case, $V_1, \cdots, V_R$ can be given the structure of $A-$representations as follows: if*

$$\Gamma : A \longrightarrow \bigoplus \mathrm{End}(V_i),$$

$$a \longmapsto (\rho_1(a), \cdots, \rho_R(a)),$$

is isomorphism of algebra, then (V_i, ρ_i) is $A-$representation for all i. Moreover

(a). *The spaces $V_1, \cdots, V_R$ be all the irreps of A up to isomorphism.*

(b). *The regular $V_{\mathrm{reg}} \simeq \bigoplus_{i=1}^R \dim(V_i)V_i$ as $A-$representations.*

Proof. $(1) \Longrightarrow (2)$ is trivial.

$(2) \Longrightarrow (3)$: suppose $V_{\mathrm{reg}} \simeq \bigoplus m_i V_i$ are irreps, there is $1_a \in V_{\mathrm{reg}}$ implies that there is $v = (v_{i,j})_{i\in[n],j\in[m_i]} \in \bigoplus m_i V_i$ such that for all $a \in A\backslash\{0\}, a \cdot v \neq 0$ since $a \cdot 1_A \neq 0$. Let $a \in A\backslash\{0\}$ and let $a \cdot v = (a \cdot V_{ij})$, there is $i, j, a \cdot V_{ij} \neq 0 \Longrightarrow \rho_i(a)(V_{ij}) \neq 0 \Longrightarrow \rho_i(a) \neq a \Longrightarrow a \notin \mathrm{rad}(A)$.

$(3) \Longrightarrow (4)$: Proved as corollary of the density theorem.

It remains to show $(4) \Longrightarrow (1), (a), (b)$.

$(4) \Longrightarrow (b)$: Sketch: The representation $V_{\mathrm{reg}} \overset{\Gamma}{\simeq} \bigoplus \mathrm{End}(V_i) \simeq \bigoplus \dim(V_i)V_i$. We give $\mathrm{End}(V_i)$ the structure of $A-$representations as follows. For any $a \in A$, for all $f \in \mathrm{End}(V_i)$, we have $a \cdot f = \rho_i(a) \circ f$. The map Γ is a homomorphism of A representation since

$$a \cdot \Gamma(x) = a(\rho_1(x), \cdots, \rho_R(x)) = (a\rho_1(x), \cdots, a\rho_R(x))$$

$$= (\rho_1(a) \circ \rho_1(x), \cdots, \rho_R(a) \circ \rho_R(x)).$$

Therefore

$$\Gamma(a \cdot x) = (\rho_1(ax), \cdots, \rho_R(ax)) = (\rho_1(a) \circ \rho_1(x), \cdots, \rho_1(a) \circ \rho_R(x)).$$

Hence $V_{\mathrm{reg}} \overset{\Gamma}{\simeq} \bigoplus \mathrm{End}(V_i)$. Hence $\mathrm{End}(V_1) \simeq \dim(V_i)V_i$. Indeed, if $\{e_1, \cdots, e_d\}$ is a basis of V_i, then an isomorphism is given by

$$\rho : \mathrm{End}(V_1) \longrightarrow \dim(V_i)V_i,$$

$$f \longmapsto (f(e_1), \cdots, f(e_d)).$$

(check this!) Lastly V_i is irreducible since for all $v \in V_i\backslash\{0\}$ we have $A \cdot v = \mathrm{End}(V_i) \cdot V = V_i$.

$(4) \implies (1) + (a)$: It actually suffices to show that any finite dimensional $A-$representation is isomorphic to subrepresentation of mV_{reg} for some m (since subrepresentations of sum of irreps is isomorphic to sum of irreps).

We give the dual vector space A^* the structure of $A-$representations: for all $a \in A$, for all $f \in A^*$, we have

$$a \cdot f = \begin{cases} A \to K \\ x \to f(xa) \end{cases} .$$

[Check A^* is an $A-$representation].

We have the following claim:

Claim 1: Any $A-$representations (V, ρ) of $\dim d$ is isomorphic to a subrepresentation of aA^*.

Claim 2: We have $(4) \implies A \simeq A^*$ as representations where the left hand side is V_{reg}.

Proof of Claim 1: For $f \in V^*$ and $v \in V$ we define

$$f^v : A \longrightarrow k,$$

$$x \longmapsto f(x \cdot v).$$

Clearly $f^v \in A^*$, moreover $f^{av} = af^v$ ($f^{av}(x) = f(xav) = (af^v)(x)$). Hence

$$V \longrightarrow A^*,$$

$$v \longmapsto f^v,$$

is a homomorphism of A representations. Let $f_1, \cdots, f_d$ be a basis of V^*, by above

$$\phi \cdot v \longrightarrow dA^*,$$

$$v \longmapsto (f_1^v, \cdots, f_d^v),$$

is $A-$representations homomorphism. Moreover ϕ is injective since $\phi(v) = 0 \implies \forall i, f_1^v(1_A) = 0 \implies \forall i, f_i(v) = 0 \implies v = 0$. Hence $V \simeq \operatorname{Im}(\phi) \subseteq dA^*$.

Proof of Claim 2: Let $A = \bigoplus \operatorname{End}(V_i)$, let

$$\phi : A \longrightarrow A^*,$$

$$(\rho_1, \cdots, \rho_R) = a \longmapsto \left(\begin{array}{l} A \to K \\ (f_1, \cdots, f_R) \mapsto \sum_{i=1}^R T_R(f_i \circ \rho_i) \end{array} \right).$$

This is isomorphism of $A-$representations. Thus we see homomorphism (check), $\dim(A) = \dim(A^*)$ checked, how about injectivity?

We see ϕ is injective because $\phi(\rho_1, \cdots, \rho_R) = 0$ implies that all the coefficients in the matrices of $\rho_1, \cdots, \rho_R$ are 0. Hence $\rho_1, \cdots, \rho_R = 0$. □

Theorem 3.2.4 (Wedderburn's Theorem)**.** *We have*

- *Radical* $\mathrm{rad}(A) = 0$ *implies that* $A \simeq \bigoplus \mathrm{Mat}_{M_i}(k)$ *if* k *is algebraically closed.*
- *Radical* $\mathrm{rad}(A) = 0$ *implies that* $A \simeq \bigoplus \mathrm{Mat}_{M_i}(D_i)$ *division algebra over* k *in general.*

Part II

Commutative Algebra

We are studying the correspondence

$$\text{Geometry} \longleftrightarrow \text{Algebra},$$

$$p(a) = 0 \longleftrightarrow p \in \mathbb{C}[x_1, \cdots, x_n], a \in \mathbb{C}^n,$$

$$a \text{ belong to locus of 0 of } p \longleftrightarrow p \text{ belong to the ideal } \ker(p_{V^{\mathbb{C}}}).$$

Throughout we assume all rings are commutative unless otherwise stated.

4 Preliminaries on Ideals

4.1 Basic Operations

Definition 4.1.1. Let R be a commutative ring, $I \subseteq R$ is **ideal** if it is closed under $+, -$ and $RI \subseteq I$.

Remark 4.1.2. If I, J are ideals, then $I \cap J$ is an ideal.

Definition 4.1.3. For $S \subseteq R$, we say $(S) = \bigcap\limits_{S \subseteq I \text{ ideal}} I$ is the **ideal generated by** S.

Remark 4.1.4. Ideal $I \neq R$ if and only if I does not contain a unit (invertible element).

Definition 4.1.5. Let I, J ideals, then we define the **sum of ideals** $I + J = \{x + y | x \in I, y \in J\} = (I \cup J)$.

We define the **product of ideals** $IJ = (\{xy | x \in I, y \in J\}) = \{\sum_{i=1}^{n} x_i y_i | m \geqslant 0, x_i \in I, y_i \in I\}$.

We define the **ideal quotient** $(I : J) = \{r \in R | rJ \subseteq I\}$.

Definition 4.1.6. We say ideal I is **prime** if $R \backslash I$ is closed under multiplication $(\forall x_1, \cdots, x_n \notin I \Longrightarrow x_1 \cdots x_n \notin I)$.

Remark 4.1.7. Let $x \notin I$ prime ideal, for all m we have $x^m \notin I$.

Definition 4.1.8. Let $I \subseteq R$ be ideal, the **radical** of I is $r(I) = \{x \in R | \exists m > 0, x^m \in I\}$. The **nilradical** of R is $r(0) = \{x \in R | \exists m > 0, x^m = 0\}$.

Example 4.1.9. Take $R = \mathbb{Z}, I = (m)$, then we have $r(I) = (p_1 \cdots p_k)$ where $p_1 \cdots p_k$ be distinct primes of $m = \bigcap_{i=1}^{k} (p_i)$.

Proposition 4.1.10. *For all $I \subseteq R$ ideal, we have $r(I) = \bigcap_{I \subseteq P \text{ prime}} P$ (in particular, $r(I)$ is an ideal).*

Proof. $(\subseteq)$: Consider $x \in r(I)$ we have $\exists m > 0, x^m \in I \implies \forall I \subseteq P$ prime, $x^m \in P \implies \forall I \subseteq P$ prime, $x \in P \implies x \in \bigcap_{I \subseteq P \text{ prime}} P$.

$(\supseteq)$: Let $x \notin r(I)$, let $\Omega = \{J \subseteq R | I \subseteq J, J \cap \{x, x^2, x^3, \cdots\} = \varnothing\}$. Note $I \in \Omega$ hence $\Omega \neq \varnothing$. Let P be a maximal element of Ω for inclusion (such a maximal element exists by Zorn's Lemma). We claim that P is prime.

Let $a, b \notin P \implies P + (a), P + (b) \notin \Omega \implies \exists m, n > 0$ such that $x^m \in P + (a), x^n \in P + (b) \implies x^{m+n} \in (P + (a))(P + (b)) = P + (ab) \implies P + (ab) \notin \Omega \implies ab \notin P$. Therefore $x \in P \implies x \in \bigcap_{I \subseteq Q \text{ prime}} Q$. □

Lemma 4.1.11. *We have*

- $I \subseteq r(I)$,
- $r(r(I)) = r(I)$,
- $r(I) = R \iff I = R$,
- $r(IJ) = r(I \cap J) = r(I) \cap r(J)$,
- *I prime* $\implies r(I) = I \implies \forall m > 0, r(I^m) = I$.

Proof. Easy check. □

4.2 Extension and Contraction of Ideals

Definition 4.2.1. Let $f : R \to T$ be a ring homomorphism, then we define

- For I ideal of R, the $f-$**extension of** I is $I^e = (f(I))$ the ideal generated by $f(x), x \in I$.
- For J ideal of T, the $f-$**contraction of** J is $J^c = f^{-1}(J) = \{x \in I | f(x) \in J\}$.

Remark 4.2.2. We have J^c is an ideal since $f(x), f(y) \in J \implies f(x + y) \in J, f(rx) \in J$. This gives

$$\{\text{ideals of } R\} \underset{c}{\overset{e}{\rightleftharpoons}} \{\text{ideals of } T\}.$$

Remark 4.2.3. We have $J \subset T$ prime $\implies J^c$ prime. Note that $I \subseteq R$ prime does not imply I^e is prime ($f(x), f(y) \notin J \implies f(xy) = f(x)f(y) \in J$).

Example 4.2.4 (Example of I prime, I^e not prime.)**.** Let

$$f : \mathbb{Z} \longrightarrow \mathbb{Z}[i],$$

$$n \longmapsto n,$$

and let $I = 5\mathbb{Z}$. We see I prime but $I^e = 5\mathbb{Z}[i]$ not prime since $(2 + i)(2 - i) = 5$ since the left hand side terms are not in I^e and the right hand side term is in I^e.

Definition 4.2.5. Given $f : R \to T$, and ideal I of R is called **contracted** if there is J, such that $I = J^c$. Similarly, an ideal J of T is called **extended** if there is I such that $J = I^e$.

Lemma 4.2.6. *We have*

$$\forall I \subseteq R, I^{ec} \supseteq I,$$
$$\forall J \subseteq T, J^{ce} \subseteq J.$$

Further we have

$$\forall I \subseteq R, I^{ece} = I^e,$$
$$\forall J \subseteq T, J^{cec} = J^c.$$

Proof. First two statements are routine check. For the last two, we see $I^{ece} = (I^e)^{ce} \subseteq I^e$. Also we have $I^{ece} = (I^{ec})^e \supseteq I^e$. Same for J. □

Corollary 4.2.7. *We have that for all $I \subseteq R$ contracted $I^{ec} = I$. For all $J \subseteq R$ extended $J^{ce} = J$. Hence*

$$\{I \subseteq R \text{ contracted}\} \underset{c}{\overset{e}{\rightleftharpoons}} \{J \subseteq T \text{ extended}\}$$

are bijections.

Lemma 4.2.8. *Let $f : R \to T$ ring homomorphism, let I_1, I_2 ideals of R and J_1, J_2 ideals of T, we have*

(1). $(I_1 + I_2)^e = I_1^e + I_2^e$,

(2). $(I_1 I_2)^e = I_1^e I_2^e$,

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

(4). $r(I)^e \subseteq r(I^e)$,

(5). $(I_1 : I_2)^e \subseteq (I_1^e : I_2^e)$.

On the other hand,

(1). $(J_1 + J_2)^c \supseteq J_1^c + J_2^c$,

(2). $(J_1 J_2)^c \supseteq J_1^c J_2^c$,

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

(4). $r(J)^c = r(J^c)$,

(5). $(J_1 : J_2)^c = (J_1^e : J_2^e)$.

Proof. Routine check. □

Proposition 4.2.9. *Let $f : R \to T$ be ring homomorphism. Then $I \subseteq R$ is prime and contracted $\overset{(1)}{\iff}$ I contraction of a prime ideal. Also $J \subseteq T$ prime and extended $\overset{(2)}{\implies}$ J extension of a prime ideal.*

Proof. $(\overset{(1)}{\impliedby})$: $I = J^c$ with J prime implies that I prime as seen above.

$(\overset{(2)}{\implies})$: J extended $\implies (J^c)^e = J$. Then J prime implies that J^c prime hence J is extension of prime.

$(\overset{(1)}{\implies})$: To be completed. □

Corollary 4.2.10. *If $f : R \to T$ homomorphism such that every ideal of T is extended. Then*

$$\{\textit{contracted ideals of } R\} \underset{c}{\overset{e}{\rightleftharpoons}} \{\textit{ideals of } T\}$$

are bijective and

$$\{\textit{prime ideals of } R\} \underset{c}{\overset{e}{\rightleftharpoons}} \{\textit{prime ideals of } T\}.$$

Example 4.2.11 (Example of quotient map)**.** Let $K \subseteq R$ be an ideal of R and let

$$f : R \longrightarrow R/K,$$

$$x \longmapsto x + K$$

be the quotient map. Then we have

(1). For all $I \subseteq R, I^e = (\{x + K, x \in I\}) = (I + K)/K$.

(2). Every ideal of R/K is extended. Ideal J of R/K is $I^e = I/K$ for $I = \bigcup_{x+K\in J} x + K$.

(3). The contracted ideals of R are the ideals of R containing K. For $K \subseteq I \subseteq R$, we have $I^e = I/K$.

Hence $I \overset{e}{\longrightarrow} I/K$ gives a bijection, we see

$$\{\text{ideals } I, K \subseteq I \subseteq R\} \overset{\text{bijection}}{\longrightarrow} \{\text{ideals of } R/K\},$$

$$\{\text{prime ideals } I, K \subseteq I \subseteq R\} \overset{\text{bijection}}{\longrightarrow} \{\text{prime ideals of } R/K\}.$$

5 Rings of Fractions

5.1 Definitions and Universal Properties

Let R be a commutative ring.

Definition 5.1.1. We call $S \subseteq R$ a **multiplicative set** if $1 \in S, 0 \notin S$, and S is closed under multiplication.

Definition 5.1.2. Let $S \subseteq R$ be a multiplicative set. The **ring of fraction** is

$$S^{-1}R = \{\frac{x}{s} | x \in R, s \in S\}/ \sim,$$

where $\frac{x}{s} \sim \frac{y}{t}$ if $\exists u \in S$ such that $uxt = usy$. We can see $\frac{x}{s} + \frac{y}{t} = \frac{xt+ys}{st}$ and $\frac{x}{s} \times \frac{y}{t} = \frac{xy}{st}$ well defined (with respected to equivalence relation).

Proposition 5.1.3. *The data $(S^{-1}R, +, \times, \frac{0}{1}, \frac{1}{1})$ is a ring. The map*

$$\epsilon : R \longrightarrow S^{-1}R,$$

$$x \longmapsto \frac{x}{1},$$

is a ring homomorphism, which we call the "fraction map".

Notation: The set of **units** (invertible elements for multiplication) in a ring R is denoted by $U(R)$.

Remark 5.1.4. The image of map $\epsilon(S) = \{\frac{s}{1}, s \in S\} \subseteq U(S^{-1}R)$.

Proposition 5.1.5 (Universal Property)**.** *Let $S \subseteq R$ as a multiplicative set. Then*

1. *If $\phi : R \to T$ is a ring homomorphism such that $\phi(S) = U(T)$, then there exists a unique $\widetilde{\phi} : S^{-1}R \to T$ ring homomorphism such that $\phi = \widetilde{\phi} \circ \epsilon$ such that the diagram*

$$\begin{tikzcd} R \arrow[rr, "\forall\phi"] \arrow[dr, "\epsilon"'] & \circlearrowright & T \\ & S^{-1}R \arrow[ur, "\exists!\widetilde{\phi}"'] & \end{tikzcd}$$

commutes.

2. *The ring $S^{-1}R$ is uniquely determined by this property.*

5.2 Ideal Correspondence for the Fraction Map

Notation: Let $S \subseteq R$ be a multiplicative set. Let $I \subseteq R$, we denote $S^{-1}I = \{\frac{x}{s} | x \in I, s \in S\}$.

Lemma 5.2.1. *Let $S \subseteq R$ be a multiplicative set, let*

$$\epsilon : R \longrightarrow S^{-1}R,$$

$$x \longmapsto \frac{x}{1}.$$

The extension and contraction of ideals through ϵ satisfy

(1). For all $I \subseteq R, I^e = S^{-1}I$

(2). Every ideal J of $S^{-1}R$ is $\epsilon-$extended. The ideal $J = S^{-1}I$ for some ideal I of R.

(3). We have $S^{-1}I \neq S^{-1}R$ if and only if $I \cap S = \varnothing$.

Proof. (1). By definition, we have $I^e = (\{\frac{x}{1}, x \in I\}) = \{\sum_{k=1}^{n} \frac{x_k}{s_k} | x_k \in I, s_k \in S\}$, then by putting to same denominators we have $\{\frac{x}{s} | x \in I, s \in S\} = S^{-1}I$.

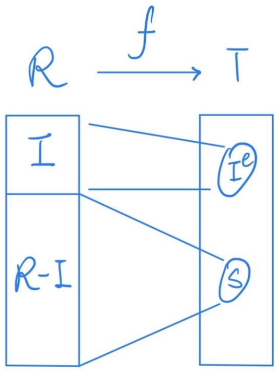
(2). Let J be ideal of $S^{-1}R$, let $I = \{x \in R | \frac{x}{1} \in J\}$. Easy to check I is ideal of R and $J = S^{-1}I$.

(3). We have

$$\begin{aligned} S^{-1}I = S^{-1}R &\iff \exists x \in I, \exists s \in S, \frac{x}{s} = \frac{1}{1} \\ &\iff \exists x \in I, \exists u, s \in S, ux = us \\ &\iff \exists y \in I, \exists t \in S, y = t \iff I \cap S \neq \varnothing. \end{aligned}$$

Hence the lemma. □

Proof of the one direction of Proposition 4.2.9 (1). Let $f : R \to T$ be a ring homomorphism and let $I \subseteq R$ be prime contracted ideal. Let $S = f(R\backslash I) = \{f(x)|x \in R\backslash I\}$. Then I contracted implies that $I^{ec} = I$ from previous results. Then $I^e \cap S = \varnothing$ (see picture).

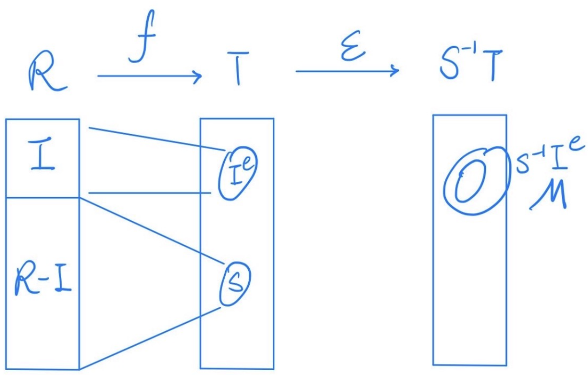


Then I prime implies that S is a multiplicative set (indeed $x, y \in R\backslash I$ implies that $f(x)f(y) = f(xy) \in S$ and $1 = f(1) \in S$ and $0 \notin S$ since $I^e \cap S = \varnothing$.

Let

$$\epsilon : T \longrightarrow S^{-1}T,$$
$$x \longmapsto \frac{x}{1},$$

be the fraction map. The corresponding picture we will need is below.



Then $I^e \cap S = \varnothing$ with the previous result implies that $S^{-1}I^e \neq S^{-1}T$. This implies that there exists a maximal ideal M of $S^{-1}T$ containing $S^{-1}I^e$. Since any ideal of $S^{-1}T$ is $\epsilon-$extended, we have $M = S^{-1}P$ where P is the $\epsilon-$contraction of M. Then M prime implies P prime. Further $S^{-1}P \notin S^{-1}T$ implies that $P \cap S = \varnothing$. Thus $I^e \subseteq P \subseteq T\backslash S$. Hence $P^c = I$ which shows I is contraction of a prime ideal. $\square$

Proposition 5.2.2. *Let $S \subseteq R$ be multiplicative set and let*

$$\epsilon : R \longrightarrow S^{-1}R,$$

$$x \longmapsto \frac{x}{1},$$

then

(1). *Every ideal of $S^{-1}R$ is extended and $I^e = S^{-1}I$.*

(2). *The contracted ideals are $I \subseteq R$ such that $x \notin I, s \in S \Longrightarrow sx \notin I$.*

(3). *The contracted prime ideals are $I \subseteq R$ prime such that $I \cap S = \varnothing$. Hence $I \overset{e}{\longmapsto} S^{-1}I$ gives bijection*

$$\{I \subseteq R \text{ ideal s.t.} \forall x \notin I, \forall s \in S, sx \notin I\} \overset{bij}{\longleftrightarrow} \{\text{ideal of } S^{-1}R\},$$

$$\{I \subseteq R \text{ prime ideal}, I \cap S = \varnothing\} \overset{bij}{\longleftrightarrow} \{\text{prime ideal of } S^{-1}R\}.$$

Proof. (1). Already proved.

(2). Ideal I contracted if and only if $I^{ec} = I$. Let $x \in R$, then

$$x \in I^{ec} \Longleftrightarrow x \in (S^{-1}I)^c \Longleftrightarrow \frac{x}{1} \in S^{-1}I$$

$$\Longleftrightarrow \exists y \in I, s \in S, \frac{x}{1} = \frac{y}{s} \Longleftrightarrow \exists y \in I, u, s \in S, usx = uy$$
$$\Longleftrightarrow \exists t \in S, tx \in I.$$

Hence $I^{ec} = \{x \in R | \exists t \in S, tx \in I\}$. We have I contracted if and only if $I^{ec} = I$ if and only if $\forall x \notin I, \forall t \in S, tx \notin I$.

(3). Let $I \subseteq R$ prime, then $I \cap S = \varnothing$ implies $\forall x \notin I, \forall s \in S, sx \notin I$ implies that I is contracted. Also $I \cap S \notin \varnothing$ implies that $I^e = S^{-1}R$ implies that $I^{ec} \notin I$ implies that I not contracted. Hence I prime is contracted if and only if $I \cap S = \varnothing$.

Hence the proposition is proved. □

We have the bijection

$$\{I \subseteq R \backslash S \text{ prime ideal}\} \overset{I \mapsto S^{-1}I}{\longrightarrow} \{\text{prime ideal of } S^{-1}R\}.$$

Notation: Let $P \subseteq R$ be prime ideal, $S = R\backslash P$ is a multiplicative set and we denote $R_P = S^{-1}R$. For $I \subseteq R$, we denote $I_P = S^{-1}I$.

Remark 5.2.3. For $P \subseteq R$ prime ideal, one has the following ideal correspondences

$$\{I \text{ prime ideal of } R, I \subseteq P\} \overset{bij}{\longleftrightarrow} \{\text{prime ideal of } R_P\},$$

$$\{I \text{ prime ideal of } R, I \supseteq P\} \overset{bij}{\longleftrightarrow} \{\text{prime ideal of } R/P\}.$$

Remark 5.2.4. For $P \subseteq R$ prime ideal, by above bijections we see that P_P is the unique maximal ideal of R_P. Hence R_P is a **local ring** and R_P/P_P is a field (residue field of R_P at P_P). The fraction map

$$R \longrightarrow R_P,$$

$$x \longmapsto \frac{x}{s},$$

is called **localization at** P.

Example 5.2.5. Let $R = \mathbb{C}[X_1, \cdots, X_n]$, $P \subseteq R$ be prime ideal. Then the local ring $R_P = \{\frac{f}{g} | f, g \text{ polynomial}, g \notin P\} \subseteq \mathbb{C}(X_1, \cdots, X_n)$.

Let $Z(P) = \{(x_1, \cdots, x_n) \in \mathbb{C}^n | \forall f \in P, f(x_1, \cdots, x_n) = 0\}$, this is the "algebraic variety defined by P". Then R_P is the ring of rational functions which are defined "almost everywhere" on $Z(P)$. We see P_P is rational functions which are 0 on $Z(P)$. The quotient R_P/P_P "identify rational functions if they have same value on $Z(P)$.

6

Localizations of Modules

6.1 Definitions and Construction as “Extension of Scalars”

Definition 6.1.1 (Module of Fraction)**.** Let R be a ring and $S \subseteq R$ be multiplicative set. For a $R-$module M, we define the $S^{-1}R-$module $S^{-1}M$ as follows

- The module $S^{-1}M = \{\frac{x}{s} | x \in M, s \in S\}/\sim$, where $\frac{x}{s} \sim \frac{y}{t}$ if $\exists u \in S, utx = usy$.
- The sum $\frac{x}{s} + \frac{y}{t} = \frac{tx+sy}{st}$.
- The product $\frac{r}{s} \cdot \frac{x}{t} = \frac{rx}{st}$ where $\frac{r}{s} \in S^{-1}R$ and $\frac{x}{t} \in S^{-1}M$.

Claim: The operations are well defined (with respect to equivalence relation) and give $S^{-1}M$ the structure of $S^{-1}R-$module (if $\frac{x}{s} \sim \frac{y}{t}$ then $\frac{x}{s} \sim \frac{utx}{uts} = \frac{usy}{uts} \sim \frac{y}{t}$).

Proof. Exercise. □

Remark 6.1.2. Note that the module $S^{-1}M$ is actually a $(R, S^{-1}R)-$bimodule (with $R-$action, $r\frac{x}{s} := \frac{rx}{s}$). This is a restriction of scalar construction corresponding to the homomorphism $\epsilon : R \to S^{-1}R$.

Proposition 6.1.3. *We have $S^{-1}M \simeq S^{-1}R \otimes_R M$ as $S^{-1}R-$module.*

Remark 6.1.4. This shows that $S^{-1}M$ is an “extension of scalar” construction corresponding to $\epsilon : R \to S^{-1}R$.

Reminder: Let R, T be commutative rings, then

(1). The data M is a $(R, T)-$**bimodule** if it is $R-$module and $T-$module and for all $r \in R$, for all $t \in T$, for all $x \in M$, we have $r(tx) = t(rx)$.

(2). If $f : R \to T$ is a ring homomorphism, then any $T-$module M is automatically a $(R, T)-$bimodule when defining the action of R by $\forall r \in R, \forall x \in M, rx = f(r)x$ where the left hand side is r action and the right hand side is t action. This is the **restriction of scalars**. Example: The map $f = \epsilon$ fraction operation.

(3). If M is $R-$module and N is $(R, T)-$bimodule, then the tensor $M \otimes_R N$ is a $(R, T)-$bimodule when defining the action of T by: $\forall t \in T, \forall x \in M, \forall y \in N$, we have $t(x \otimes y) = x \otimes (ty)$.

(4). If $f : R \to T$ is a ring homomorphism, then T is a $(R, T)-$bimodule by restriction of scalar. Hence for any $R-$module M, we have $T \otimes_R M$ is a $(R, T)-$bimodule. This is **extension of scalars**.

Example 6.1.5. The module $S^{-1}R \otimes_R M$ is a $(R, S^{-1}R)-$bimodule (using $f = \epsilon$ the fraction map).

Proposition 6.1.6. *For all $R-$module M, then $S^{-1}M \simeq S^{-1}R \otimes_R M$ as $S^{-1}R-$module with isomorphism such that $\frac{x}{s} \mapsto \frac{1}{s} \otimes x$.*

Remark 6.1.7. If $A \simeq B$ as $S^{-1}R-$module then $A \simeq B$ as $(R, S^{-1}R)-$module (by restriction of scalars).

Proof. We prove by

- Consider the map
$$\begin{aligned} g : S^{-1}M &\longrightarrow S^{-1}R \otimes M, \\ \frac{x}{s} &\longmapsto \frac{1}{s} \otimes x, \end{aligned}$$
is well defined (respects equivalence relation since $\forall u \in S, g(\frac{ux}{us}) = \frac{1}{us} \otimes ux = \frac{1}{s} \otimes x = g(\frac{x}{s})$) and is $S^{-1}R-$bimodule.

- The map
$$\begin{aligned} f : S^{-1}R \times M &\longrightarrow S^{-1}M, \\ (\frac{r}{s}, x) &\longmapsto \frac{rx}{s}, \end{aligned}$$
is $R-$linear. Hence there exists $f^* : S^{-1}R \otimes M \to S^{-1}M$ such that $\frac{r}{s} \otimes x \mapsto \frac{rx}{s}$.

- Easy to check that $f^* g = \mathrm{Id}$ and $g f^* = \mathrm{Id}$.

Hence f^*, g are isomorphisms of $S^{-1}R-$module. □

Corollary 6.1.8. *Let M, N be $R-$modules, then*

(1). *We have $S^{-1}M \oplus S^{-1}N \simeq S^{-1}(M \oplus N)$ as $S^{-1}R-$module with isomorphism such that $(\frac{x}{s}, \frac{y}{t}) \mapsto \frac{(tx,sy)}{st}$.*

(2). *We have $S^{-1}M \otimes S^{-1}N \simeq S^{-1}(M \otimes N)$ as $S^{-1}R-$module with isomorphism such that $\frac{x}{s} \otimes \frac{y}{t} \mapsto \frac{x \otimes y}{st}$.*

Proof. We have the isomorphisms

$$S^{-1}M \oplus S^{-1}N \simeq (S^{-1}R \otimes M) \oplus (S^{-1}R \otimes N) \simeq S^{-1}R \otimes (M \oplus N) \simeq S^{-1}(M \oplus N)$$

given by the maps

$$(\frac{x}{s}, \frac{y}{t}) \mapsto (\frac{1}{s} \otimes x, \frac{1}{t} \otimes y) = (\frac{1}{st} \otimes tx, \frac{1}{st} \otimes sy) \mapsto \frac{1}{st} \otimes (tx, sy) \mapsto \frac{(tx, sy)}{st}.$$

Similarly consider the isomorphism

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \simeq S^{-1}M \otimes_{S^{-1}R} S^{-1}R \otimes_R N$$

$$\simeq (S^{-1}M \otimes_{S^{-1}R} S^{-1}R) \otimes_R N \simeq S^{-1}M \otimes_R (M \otimes_R N) = S^{-1}R(M \otimes N),$$

where the isomorphisms are given similarly (...). □

Lemma 6.1.9. *If A is $R-$module, B is $(R, T)-$bimodule and C is $T-$module then*

$$(A \otimes_R B) \otimes_T C \simeq A \otimes_R (B \otimes_T C)$$

with isomorphism such that

$$(x \otimes y) \otimes z \longmapsto x \otimes (y \otimes z).$$

6.2 Flatness for Modules of Fractions

Reminder:

(1). A sequence of $R-$module homomorphism

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

is **exact** if $\mathrm{Im}(f_i) = \ker(f_{i+1})$. A short exact sequence is an exact sequence of the form

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0.$$

(2). A functor $\mathfrak{F} : \mathcal{R} - \mathcal{M}od \to \mathcal{R} - \mathcal{M}od$ is called **exact** if for all sequence exact, we have $\mathfrak{F}(seq)$ is exact.

Remark 6.2.1. If $\mathfrak{F}$ is exact, then

(1). If f is injective then $\mathfrak{F}(f)$ is injective (Using $0 \to A \xrightarrow{f} B$ exact).

(2). If f surjective then $\mathfrak{F}(f)$ surjective ($A \xrightarrow{f} B \longrightarrow 0$).

(3). We have $\mathfrak{F}(M/N) \simeq \mathfrak{F}(M)/\mathfrak{F}(N)$. Using $0 \to N \to M \to M/N \to 0$ exact hence $0 \to \mathfrak{F}(N) \to \mathfrak{F}(M) \to \mathfrak{F}(M/N) \to 0$ exact hence $\mathfrak{F}(M/N) \simeq \mathfrak{F}(M)/\mathfrak{F}(N)$ by first isomorphism theorem.

Lemma 6.2.2. *The functor $\mathfrak{F}$ is exact if and only if for all sequence short exact, $\mathfrak{F}(seq)$ is short exact. That is, there exists N_i such that the diagram*

$$\begin{tikzcd}
\cdots \arrow[r] & M_i \arrow[rr] \arrow[dr] \arrow[rr, phantom, "\circlearrowright"', shift right=3ex] & & M_{i+1} \arrow[rr] \arrow[dr] \arrow[rr, phantom, "\circlearrowright"', shift right=3ex] & & M_{i+2} \arrow[r] & \cdots \\
& & N_i \arrow[ur] & & N_{i+1} \arrow[ur] \arrow[d] & & \\
{} \arrow[rr, bend left] & & 0 \arrow[u] \arrow[rr, bend left] & & 0 \arrow[rr, bend left] & & {}
\end{tikzcd}$$

commutes.

Reminder (3). Let M be a $R-$module, we define $\mathfrak{F}_M : \mathcal{R} - \mathcal{Mod} \to \mathcal{R} - \mathcal{Mod}$ by $\mathfrak{F}_M(A) = M \otimes A$ and $\mathfrak{F}_M(g) = \mathrm{Id}_M \otimes g$. Module M is called **flat** if $\mathfrak{F}_M$ is exact.

Example 6.2.3. We have R is a flat $R-$module (deduced from the isomorphism $R \otimes A \simeq A$).

Lemma 6.2.4. *Let seq be $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ of $R-$module. Then for all $R-$module M, seq is exact implies that $\mathfrak{F}_M(seq)$ is exact.*

Proof. Suppose seq is exact, then β is surjective and $\mathrm{Im}(\alpha) = \ker(\beta)$. Want to show $\mathrm{Id}_M \otimes \beta$ surjective and $\mathrm{Im}(\mathrm{Id} \otimes \alpha) = \ker(\mathrm{Id} \otimes \beta)$. Then we see

- For all $x \in M$, for all $c \in C$, we have $x \otimes c \in \mathrm{Im}(\mathrm{Id} \otimes \beta)$ because there exists $b \in B, \beta(b) = c$ and $x \otimes c = (\mathrm{Id} \otimes \beta)(x \otimes b)$. Pure tensors $x \otimes c$ generate $M \otimes c$ hence $\mathrm{Id} \otimes \beta$, say.

- We have $\beta \circ \alpha \Longrightarrow (\mathrm{Id} \otimes \beta) \circ (\mathrm{Id} \otimes \alpha) = (\mathrm{Id} \otimes (\beta \circ \alpha)) = 0$. Hence this implies $\mathrm{Im}(\mathrm{Id} \otimes \alpha) \subseteq \ker(\mathrm{Id} \otimes \beta)$.

- Let $I = \mathrm{Im}(\mathrm{Id} \otimes \alpha)$ and let $\phi : M \otimes B \to M \otimes B/I$ be the quotient map. Let

$$f : M \otimes B/I \longrightarrow M \otimes C,$$

$$y + I \longmapsto (\mathrm{Id} \otimes \beta)(y),$$

then f is well defined since $I \subseteq \ker(\mathrm{Id} \otimes \beta)$. Moreover $\mathrm{Id} \otimes \beta = f \circ \phi$. In order to prove $\ker(\mathrm{Id} \otimes \beta) = I$ it suffices to prove f is injective. Let

$$g : M \times C \longrightarrow (M \otimes B)/I,$$

$$(x, c) \longmapsto x \otimes b + I,$$

where $b \in \beta^{-1}(C)$. We see g is well defined: if $b, b' \in \beta^{-1}(C)$ then $x \otimes b + I = x \otimes b' + I$ (because $b - b' \in \ker(\beta) = \mathrm{Im}(\alpha) \implies x \otimes b - x \otimes b' \in I$). Since g is bilinear, there exists $g^* : M \otimes C \to M \otimes B/I$ such that $x \otimes c \mapsto x \otimes b + I$ with $b \in \beta^{-1}(C)$. Moreover $g^* \circ f = \mathrm{Id}$ since $g^* \circ f(x \otimes b + I) = g^*(x \otimes \beta(b)) = x \otimes b + I$. Hence f is injective.

Hence If $A \to B \to C \to 0$ exact then $\forall M, F_M(A \to B \to C \to 0)$ is exact. $\square$

Corollary 6.2.5. *A $R-$module M is flat ($\mathfrak{F}_M$ is exact) if and only if $\forall \alpha : A \to B$ injective, the $R-$module homomorphism $\mathrm{Id}_M \otimes \alpha$ is injective.*

Proof. ($\Longrightarrow$): Clear: $0 \longrightarrow A \xrightarrow{\alpha} B$ exact implies $0 \longrightarrow M \otimes A \xrightarrow{\mathrm{Id}_M \otimes \alpha} M \otimes B$ exact.

($\Longleftarrow$): Suppose for all α injective, $\mathrm{Id}_M \otimes \alpha$ injective, then together with the above property, we have $\mathfrak{F}_M(shortexact)$ is short exact. Hence $\mathfrak{F}_M$ is exact. $\square$

Corollary 6.2.6. *For all $S \subseteq R$ multiplicative set, the $R-$module $S^{-1}R$ is flat.*

Proof. Let $\alpha : A \to B$ be an injective $R-$module homomorphism, want to show $\ker(\mathrm{Id}_{S^{-1}R} \otimes \alpha) = 0$. Any element of $S^{-1}R \otimes A$ can be written as $\frac{1}{s} \otimes x$, where $s \in S, x \in A$. Then

$$\mathrm{Id}_{S^{-1}R} \otimes \alpha(\frac{1}{s} \otimes x) = 0 \Longrightarrow \frac{1}{s} \otimes \alpha(a) = 0$$

$$\Longrightarrow \frac{\alpha(a)}{s} = 0 \text{ in } S^{-1}A \Longrightarrow \exists u \in S, u\alpha(x) = 0$$

$$\Longrightarrow \exists u \in S, \alpha(ux) = 0$$

$$\Longrightarrow \exists u \in S, ux = 0 \text{ since } \alpha \text{ injective}$$

$$\Longrightarrow \frac{x}{s} = 0 \text{ in } S^{-1}B$$

$$\Longrightarrow \frac{1}{s} \otimes x = 0 \text{ by isomorphism.}$$

$\square$

Notation: For $S \subseteq R$ multiplicative set and $\alpha : A \to B$ $R-$module homomorphism, we define

$$S^{-1}\alpha : S^{-1}A \longrightarrow S^{-1}B,$$
$$\frac{x}{s} \longmapsto \frac{\alpha(x)}{s}.$$

Remark 6.2.7. The isomorphism $f_A : S^{-1}R \otimes A \to S^{-1}A$ "send" the homomorphisms $\mathrm{Id}_{S^{-1}R} \otimes \alpha$ to $S^{-1}\alpha$ in the following sense:

$$\begin{tikzcd}
S^{-1}R \otimes A \arrow[r, "Id_{S^{-1}R}\otimes\alpha"] \arrow[d, "\simeq"] & S^{-1}R \otimes B \arrow[d, "\simeq"'] \\
S^{-1}A \arrow[r, "S^{-1}\alpha"] & S^{-1}B
\end{tikzcd}.$$

Up to this "change of notation", Corollary 6.2.6 says that for any exact sequence of $R-$module

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

The sequence

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

is exact sequence of $S^{-1}R-$modules.

Corollary 6.2.8. *We have*

- *The map α is injective $\implies S^{-1}\alpha$ is injective,*
- *The map β surjective $\implies S^{-1}\beta$ surjective,*
- *We have the isomorphism $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ with isomorphism $\frac{x+N}{s} \leftrightarrow \frac{x}{s} + S^{-1}N$.*

Proof. We see

- The sequence $0 \to A \xrightarrow{\alpha} B$ exact $\implies \cdots$,
- The sequence $A \xrightarrow{\beta} B \to 0$ exact $\implies \cdots$,
- The sequence $0 \to N \to M \to M/N \to 0$ exact with the middle map $x \mapsto x + N$. Also $0 \to S^{-1}N \to S^{-1}M \to S^{-1}(M/N) \to 0$ exact with the middle map $\frac{x}{s} \mapsto \frac{x+N}{s}$. By first isomorphism theorem, this gives $S^{-1}(M/N) \simeq S^{-1}M/S^{-1}N$ with the claimed isomorphism.

Hence the corollary. $\square$

Remark 6.2.9. Let $Q \subseteq P$ be ideals of R, with P prime, by above corollary, we have $(R/Q)_P \simeq R_P/Q_P$ are isomorphic $R-$module. But in fact it implies $(R/Q)_{P/Q} \simeq R_P/Q_P$ as rings with the isomorphism $\frac{x+Q}{s+Q} \leftrightarrow \frac{x}{s} + Q_P$.

Example 6.2.10. Homework 6...

Example 6.2.11. Extension of scalars preserve flatness. Let $\phi : R \to T$ ring homomorphism. If M is flat $R-$module, then $T \otimes_R M$ is a flat $T-$module.

Corollary 6.2.12. *The module M is a flat $R-$module implies that $S^{-1}M$ is a flat $S^{-1}R-$module.*

6.3 Local Properties of Modules and Rings

Notation: For $P \subseteq R$ prime ideal, we denote $R_P = S^{-1}R$ where $S = R \backslash P$. We denote $M_P := S^{-1}M$ for $R-$module M and $\alpha_P := S^{-1}\alpha$ for homomorphism α.

Definition 6.3.1. A property of a ring/module/homomorphism is **local** if X has property if and only if X_P has property for all $P \subseteq R$ prime.

Proposition 6.3.2. *The following are equivalent:*

(1). The module $M = 0$,

(2). The module $M_P = 0$ for all $P \subseteq R$ prime ideal,

(3). The module $M_P = 0$ for all $P \subseteq R$ maximal ideal.

Proof. $(1) \implies (2) \implies (3)$ are obvious.

For $(3) \implies (1)$, let M be such that $M_P = 0$ for all P maximal ideal. Suppose for contradiction there exists $x \neq 0$ in M, let $\mathrm{Ann}(x) = \{r \in R | rx = 0\}$. This is a proper ideal because it does not contain 1. This implies that $\exists P$ maximal at $\mathrm{Ann}(x) \subseteq P$. Then $M_P = 0 \implies \frac{x}{1} = 0$ in $M_P \implies \exists u \notin P, ux = 0$. Hence $u \in \mathrm{Ann}(x) \backslash P$, a contradiction. □

Proposition 6.3.3. *The following are equivalent for $\phi \in \mathrm{Hom}_R(A, B)$,*

(1). The map ϕ is injective,

(2). The map ϕ_P is injective for all $P \subseteq R$ prime ideal,

(3). The map ϕ_P is injective for all $P \subseteq R$ maximal ideal.

Proof. $(1) \implies (2)$ already proved.

$(2) \implies (3)$ is obvious.

$(3) \implies (1)$: Suppose ϕ_P injective for all P maximal. Let $M = \ker(\phi)$, the seq that $0 \to M \to A \xrightarrow{\phi} B$ is exact implies that for all P maximal, the sequence $0 \to M_P \to A_P \xrightarrow{\phi_P} B_P$ exact. The map ϕ_P is injective implies that $\forall P$ maximal ideal $M_P = 0$ which implies $M = 0$ by proposition above. $\square$

Proposition 6.3.4. *Same as the above proposition but with "surjective".*

Proposition 6.3.5. *The following are equivalent for a $R-$module M,*

(1). The map M is flat $R-$module,

(2). The map M_P is flat R_P-module for all $P \subseteq M$ prime,

(3). The map M_P is flat R_P-module for all $P \subseteq M$ maximal.

Proof. $(1) \implies (2)$: Already "proved" (extensions of scalars preserves flatness).

$(2) \implies (3)$: Obvious.

$(3) \implies (1)$: Sketch: Suppose M_P is flat for all P maximal, want to show for all ϕ injective, the map $\mathrm{Id}_M \otimes \phi$ is injective. For all $P, \mathrm{Id}_{M_P} \otimes \phi_P$ injective. Also $\mathrm{Id}_{M_P} \otimes \phi_P \simeq (\mathrm{Id}_M \otimes \phi)_P$ via isomorphism implies $(\mathrm{Id}_M \otimes \phi)_P$ is injective for all P. This implies that $\mathrm{Id}_M \otimes \phi$ is injective. $\square$

7

Noetherian Rings, Noetherian Modules and Hilbert's Nullstellensatz

7.1 Closure Property for Noetherian

Reminder: Let M be a $R-$module, the following are equivalent:

- Any strictly increasing sequence of submodule is finite,
- Any submodule is finitely generated.

If these property hold, then M is called **Noetherian**.

Definition 7.1.1. A ring R is **Noetherian** if it is Noetherian as $R-$module. That is to say

(1). Any strictly increasing sequence of ideals is finitely generated.

(2). Any ideal is finitely generated.

Proposition 7.1.2. *Let M be a $R-$module, and $N \subseteq M$ submodule, then M is Noetherian if and only if N and M/N are Noetherian.*

Proof. ($\Longrightarrow$): The submodule of N and M/N are in bijection with subsets of submodules of M, hence no infinite strictly increasing sequence.

($\Longleftarrow$): Suppose N and M/N are Noetherian, let $P \subseteq M$ be submodule, then $P/(P \cap N) \simeq (P+N)/N$ is finitely generated and $P \cap N$ is finitely generated (generators $x_1 + P \cap N, \cdots, x_k + P \cap N$ and generators $y_1, \cdots, y_l$). That is P is finitely generated (generators $x_1, \cdots, x_k, y_1, \cdots, y_l$). $\square$

Corollary 7.1.3. *The module M_1, M_2 are Noetherian if and only if $M_1 \oplus M_2$ is Noetherian.*

Proof. Let $\widetilde{M_1} = \{(x, 0), x \in M_1\} \subseteq M_1 \oplus M_2$. Then $\widetilde{M_1} \simeq M_1$ and $(M_1 \oplus M_2)/M_1 \simeq M_2$. Apply previous prop to $M = M_1 \oplus M_2$ and $N = \widetilde{M_1}$. $\square$

Corollary 7.1.4. *If R is Noetherian, then M is Noetherian $R-$module if and only if M is finitely generated $R-$module.*

Proof. $(\Longleftarrow)$: Obvious.

$(\Longrightarrow)$: If M is finitely generated, then $M \simeq R^k/N$ for some $N \subseteq R^k$. Moreover, R^k is Noetherian by Corollary 7.1.3. $\square$

Theorem 7.1.5 (Hilbert's Basis Theorem). *If R is Noetherian ring, then for any n, we have $R[X_1, \cdots, X_n]$ is Noetherian ring.*

Proof. It suffices to show R is Noetherian implies $R[X]$ is Noetherian. Let R be Noetherian, let $I \subseteq R[X]$ be an ideal, we want to show I is finitely generated.

Suppose it is not, let $P_0 = 0$ and for all $j > 0$, let $P_j \in I \backslash (P_0, \cdots, P_{j-1})$ such that P_j is of minimal degree in this set (note that $\deg(P_j)$ is weakly increasing).

Let a_j be the leading coefficient of P_j, since $R[X]$ is Noetherian, it has an infinite increasing chain of ideals. There exists $k > 0, a_k \in (a_1, \cdots, a_{k-1})$, hence $a_k = \sum_{j=1}^{k-1} r_j a_j, r_j \in R$. Let $P = P_k - \sum_{j=1}^{k-1} r_j X^{\deg(P_k) - \deg(P_j)} P_j$, then $P \in I \backslash (P_0, \cdots, P_{k-1})$, and the degree $\deg(P) < \deg(P_k)$. This contradicts the choice of P_k. $\square$

Recall that T is a finitely generated $R-$algebra if there is $x_1, \cdots, x_n \in T$ such that any $t \in T$ can be written as a polynomial in $x_1, \cdots, x_n$ with coefficients in R. Equivalently, there is surjective $R-$algebra homomorphism from $R[X_1, \cdots, X_n]$ to T.

Corollary 7.1.6. *If R is a Noetherian ring, and T is a finitely generated $R-$algebra, then T is a Noetherian ring.*

Proof. The algebra T is the image of Noetherian ring $R[X_1, \cdots, X_n]$ hence Noetherian (quotient of Noetherian is Noetherian). $\square$

7.2 Hilbert's Nullstellensatz

Theorem 7.2.1 (Hilbert's Nullstellensatz). *Let K be algebraically closed field, let $R = K[X_1, \cdots, X_n]$ and let $I \subseteq R$ ideal and let $Z(I) = \{x \in K^n | \forall g \in I, g(x) = 0\}$. For polynomial f, we have that $f(x) = 0, \forall x \in Z(I)$ if and only if $f \in r(I)$.*

Example 7.2.2. Let $I = (X_1^2, X_2), Z(I) = \{(0, 0)\}$. The theorem tells us $f((0, 0)) = 0$ if and only if $f \in r(I) = (X_1, X_2)$.

Lemma 7.2.3 (Zariski's Lemma). *Let $K \subseteq E$ be a field extension, if E is finitely generated $K-$algebra, then E is finite dimensional (hence algebraic) over K.*

Proof of Theorem 7.2.1, "Hilbert's Nullstellensatz". $(\Longleftarrow)$: We have $f \in r(I) \implies \exists k \geqslant 0, f^k \in I \implies \exists k \geqslant 0, f^k(0) = 0, \forall x \in Z(I) \implies f(x) = 0, \forall x \in Z(I)$.

$(\implies)$: Let $f \notin r(I)$, we want to show that there exists $x \in Z(I)$ such that $f(x) \neq 0$.

Idea: Any ring homomorphism $\phi : R \to K$ such that $\phi|_K = \mathrm{Id}$ is an evaluation map $\mathrm{ev}_x : g \longmapsto g(x)$ for some $x \in K^n$ $(x = (x_1, \cdots, x_n), x_i = \phi(x_i))$. Hence any ring homomorphism $\phi : R \to K$ such that $\phi|_K = \mathrm{Id}$ and $\phi|_I = 0$ is ev_x for some $x \in Z(I)$. Therefore need to find a ring homomorphism $\phi : R \to K$ such that $\phi|_K = \mathrm{Id}$ and $\phi|_I = 0, \phi(f) \neq 0$.

Let $S = \{f^k | k \geqslant 0\}$. This is a multiplicative set of R, and we have $f \notin r(I) \implies S \cap I = \varnothing \implies S^{-1}I$ is proper ideal of $S^{-1}R \implies S^{-1}I \subseteq M$ maximal ideal of $S^{-1}R$. Let

$$\begin{tikzcd}
\phi : R \arrow[rr] \arrow[dr, "fractions"'] & & I = S^{-1}R/M \\
& S^{-1}R \arrow[ur, "quotient"'] &
\end{tikzcd}.$$

We observe $\phi|_I = 0$ since $S^{-1}I \subseteq M$ and $\phi(f) \neq 0$ since $\frac{f}{1}$ is invertible in $S^{-1}R \implies \frac{f}{1} \notin M$. Moreover $T \simeq K$. Indeed, T is a field since M is maximal ideal. Also T is finitely generated over K (indeed $S^{-1}R = \{\frac{P}{f^k}, P \in R, k \geqslant 0\}$ with generators $\frac{x_1}{1}, \cdots, \frac{x_n}{1}, \frac{1}{f}$). Hence $T = S^{-1}R/M$ is finitely generated. Hence by Zariski's Lemma (Lemma 7.2.3), we have T is algebraic over K. Then K is algebraically closed implies that $T = \widetilde{K}$, where $\widetilde{K}$ is copy of K inside T. Hence up to composing by an isomorphism $\widetilde{K} \to K$ we get $\widetilde{\phi} : R \to K$ such that $\phi|_K = \mathrm{Id}, \phi(I) = 0, \phi(f) \neq 0$. □

It remains to prove Zariski's Lemma. We first claim a lemma.

Lemma 7.2.4. *Let $R \subseteq S \subseteq T$ be ring (hence S, T are $R-$algebras), suppose:*

- *ring R is Noetherian,*
- *T is finitely generated $R-$algebra and finitely generated $S-$module,*

then S is finitely generated $R-$algebra.

Proof. Let $x_1, \cdots, x_n$ be generators of T as $R-$algebra, $y_1, \cdots, y_m$ be generators of T as $S-$module. Then $y_1, \cdots, y_m$ generators implies that there is $s_{ij} \in S, x_i \in \sum_j s_{ij}y_j$, hence there is $s_{ijk} \in S, y_iy_j = \sum_k s_{ijk}y_k$. Let $S' = R[\{s_{ij}, s_{ijk}\}]$ be $R-$algebra generated by s_{ij}, s_{ijk}, we have $R \subseteq S' \subseteq S \subseteq T$.

Since S' is a finitely generated $R-$algebra, S' is Noetherian ring. Any $x \in T$ is a polynomial in the x_i, hence a linear combination of y_k with coefficients in S'. Hence T is a finitely generated S' module. Therefore T is Noetherian $S'-$module (since S' Noetherian).

Further, S submodule of T implies that it is a finitely generated $S'-$module. Lastly, S' finitely generated $R-$algebra and S finitely generated $S'-$algebra implies that S is finitely generated $R-$algebra. □

Now we are to prove the Zariski's Lemma.

Proof of Lemma 7.2.3, "Zariski's Lemma". Let $K \subseteq E$ be a field extension such that E is finitely generated $K-$algebra, we want to show E is finite dimensional over K.

Let $x_1, \cdots, x_n$ be generators of E as $K-$algebra, it suffices to show that $x_1, \cdots, x_r$ are algebraic over K.

Suppose not and order the x_i such that $\forall i = 1, \cdots, r, x_i$ is not algebraic over $K(x_1, \cdots, x_{i-1})$ and $\forall i = r+1, \cdots, n, x_i$ is algebraic over $K(x_1, \cdots, x_r)$. Let $F = K(x_1, \cdots, x_r) \subseteq E$ be field generated by $x_1, \cdots, x_r \simeq K(x_1, \cdots, x_r)$ fields of rational functions in n variables. Then $E = F(x_{r+1}, \cdots, x_n)$ is finite $F-$module and E is finitely generated $K-$algebra together with previous lemma implies that F is finitely generated $K-$algebra.

Let $f_1, \cdots, f_k$ be generators of $K(x_1, \cdots, x_r)$ over K. Let $P_1, \cdots, P_l$ be the irreducible polynomial dividing the denominators of $f_1, \cdots, f_k$. Then any denominators of $K[f_1, \cdots, f_k]$ is constant or multiple of one of the P_i.

But $\frac{1}{\prod_i P_i + 1}$ is not of this form, which is a contradiction. □

7.3 Some Link to Algebraic Geometry

Definition 7.3.1. Let K be an algebraically closed field, let $R = K[X_1, \cdots, X_n]$, then

- For $Y \subseteq K^n$, we define $I(Y) = \{f \in R | f(x) = 0, \forall x \in Y\}$,
- For $S \subseteq R$, we define $Z(S) = \{x \in K^n | f(x) = 0, \forall f \in S\}$.

A set of points of the form $Z(S)$ is called **algebraic set**.

(**Claim**: Any algebraic set is of the form $Z(J)$ where J is a **radical ideal** (that is, $r(J) = J$) and $\{Y \subseteq K^n \text{ algebraic set}\} \underset{Z}{\overset{I}{\rightleftharpoons}} \{J \subseteq R \text{ radical ideal}\}$ are inclusion reserving bijections.)

Remark 7.3.2. (1). The map I, Z are inclusion reserving, that is

$$Y \subseteq Y', I(Y) \supseteq I(Y'),$$

$$S \subseteq S', Z(S) \supseteq Z(S').$$

(2). For all $S \subset R$, we have $Z(S) = Z((S)) = Z(r(S))$.

Example 7.3.3. We have $Z(\{X_1^2\}) = Z((X_1^2)) = Z((X_1))$.

By above, any algebraic set is of the form $Z(J)$ where J is radical ideal.

Remark 7.3.4. (1). For all $Y, I(Y)$ is clearly an ideal and a radical ideal.

(2). Hilbert's Nullstellensatz can be stated as follows: for all J ideal, we have $I(Z(J)) = r(J)$ (no more than $r(J)$).

Example 7.3.5. We see $I(Z(X_1^2)) = (X_1)$.

Consequently, we have

- for all J radical ideal, $I(Z(J)) = J$,
- for all Y algebraic set, there exists J radical ideal such that $Y = Z(J)$, hence, $Z(I(Y)) = Z(I(Z(J))) = Z(J) = Y$.

Corollary 7.3.6. *We have I, Z are inclusion reversing bijections that*

$$\{Y \subseteq K^n \text{ algebraic set}\} \underset{Z}{\overset{I}{\rightleftharpoons}} \{J \subseteq R \text{ radical ideal}\}.$$

Remark 7.3.7. We have that

(a). The identity $I(Y_1 \cup Y_2) = I(Y_1) \cap I(Y_2)$,

(b). If J_1, J_2 are radical ideals, then $J_1 \cap J_2$ is radical ideal and $Z(J_1 \cap J_2) = Z(J_1) \cup Z(J_2)$.

Proof. (a). Clear.

(b). We have $J_1 \cap J_2$ radical ideal because $r(J_1 \cap J_2) = r(J_1) \cap r(J_2) = J_1 \cap J_2$. Then $I(Z(J_1 \cap J_2)) = J_1 \cap J_2 = I(Z(J_1)) \cap I(Z(J_2)) \overset{(a)}{=} I(Z(J_1) \cup Z(J_2))$ and I is a bijection.

□

Remark 7.3.8. Part (b) above implies that finite union of algebraic set is algebraic set. Also since arbitrarity the intersection of algebraic set is algebraic set (homework).

Definition 7.3.9. An **affine algebraic variety (AAV)** is an algebraic set which is not the union of smaller algebraic set.

Corollary 7.3.10. *We have I, Z are bijection*

$$\varnothing \neq \{Y \subseteq K^n,\ AAV\} \longleftrightarrow \{I \subseteq R \text{ prime ideal}\}.$$

Proof. By Remark 7.3.7 (b), we have Y is affine algebraic variety if and only if $Y = Z(J)$ with J **irreducible** radical ideal, where **irreducible** means "not intersection of bigger ideals". Moreover,

- if J is prime then J is radical and irreducible (exercise from homework 4 shows that prime means irreducible, $P = \cap I_j \implies P = I_j$).
- Conversely, suppose J is radical and irreducible, then J radical implies that $J = r(J) = \bigcap_{J \subseteq P \text{ prime}} P$. Also J irreducible implies that J is one of the P, hence prime.

Hence the bijection. □

Definition 7.3.11. Let $Y \subseteq K^n$ be algebraic set, then $R(Y) = R/I(Y)$ is called **affine coordinate ring** ("polynomial f on Y").

Remark 7.3.12. We have

- The set Y is affine algebraic variety if and only if $R(Y)$ is a domain.
- $\{$point on $Y\}$ is in bijection with $\{$maximal ideals of R containing $Y\}$, which is in bijection with $\{$maximal ideals of $R(Y)\}$.

Explicitly $y \in Y \mapsto M(Y, y) = \{\widetilde{f} \in R(Y) | f(y) = 0\}$.

Definition 7.3.13. Let $Y \subseteq K^n$ be affine algebraic variety, then

- $U \subseteq Y$ is an **open set** if $U = Y \backslash Z(S)$ for some $S \subseteq R$,
- A **regular function** of $U \subseteq Y$ is $\rho : Y \longrightarrow K$ such that $\exists f, g \in R, \forall x \in U, g(x) \neq 0$ and $\rho(x) = \frac{f(x)}{g(x)}$.

Notation: We say $O(Y) = \{$regular function on $Y\}$ and $O(Y, y) = \{(U, \rho) | y \in U$ open set of Y, ρ regular on $U\}$ where $(U, \rho) \sim (U', \rho')$ if and only if there exists V open set $y \subseteq V \subseteq U \cap U'$ such that $\rho|_V = \rho'|_V$.

Theorem 7.3.14. *We have*

(1). the isomorphism $O(Y) \simeq R(Y)$ as rings, where the isomorphism is given

$$\alpha : R(Y) \longrightarrow O(Y),$$

$$\widetilde{f} \longmapsto f|_Y \text{ as a function.}$$

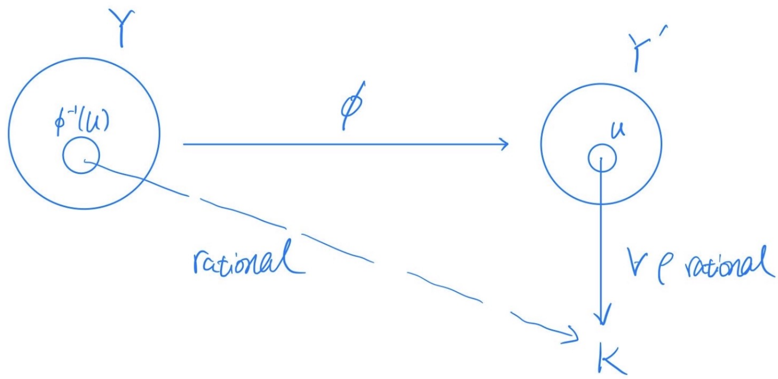
(2). *for all* $y \in Y, O(Y,y) \simeq R(Y)_{M(Y,y)} \longleftarrow \{\tilde{g} \in R(Y) | g(y) = 0\}$ *where the right hand side of the isomorphism is a localization at* $M(Y,y)$. *The isomorphism is given by*

$$\beta : R(Y)_{M(Y,y)} \longrightarrow O(Y,y),$$

$$\frac{\tilde{f}}{\tilde{g}} \longmapsto (v, \frac{f}{g}|_v), \text{ where } U = \{x \in Y | g(x) \neq 0\}.$$

Definition 7.3.15. Let Y, Y' be affine algebraic varieties, a function $\phi : Y \to Y'$ is a **morphism of affine algebraic varieties**, if $U \subseteq Y'$ open, for all $\rho : U \to K$ regular, then $\rho \circ \phi$ regular on $\phi^{-1}(U)$.

The definition can be viewed as the following commutative diagram:



Theorem 7.3.16. *We have* $Y \simeq Y'$ *if and only if* $R(Y) \simeq R(Y')$. *In fact there is function* $F : Y \to R(Y)$ *such that* $\mathcal{F} : \mathrm{Hom}(Y, Y') \to \mathrm{Hom}(R(Y'), R(Y))$ *is a bijection.*

8 Primary Decomposition of Ideals

8.1 Reduced Primary Decomposition

Motivation:

- decomposing algebraic set into variety,
- “replacing” factorization of elements in Noetherian rings which are not UFD.

Example 8.1.1. Consider $R = \mathbb{Z}[i\sqrt{5}] \subseteq \mathbb{C}$, it is Noetherian but not UFD since $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.

However, there is “semisimple” factorization of ideals.

Definition 8.1.2. Let R be a (commutative) ring. Any ideal $Q \subseteq R$ is **primary** if $Q \neq R$ and $x \notin Q, y \notin r(Q)$ implies that $xy \notin Q$. It has some equivalent phrasing:

- If $xy \in Q$ then either $x \in Q$ or $y \in r(Q)$,
- If $xy \in Q, x, y \notin Q$ then there is some $n > 0$ such that $x^n \in Q$ **and** $y^n \in Q$.

Remark 8.1.3. Prime implies primary.

Example 8.1.4. Take $R = \mathbb{Z}$, the primary ideal are of the form $I = (p^k), p$ prime integer.

Example 8.1.5. If M is a maximal ideal then for all k, M^k is primary.

Proposition 8.1.6. *If Q is primary, then $r(Q)$ is the smallest prime ideal containing Q.*

Definition 8.1.7. We say Q is $P-$**primary** if $r(Q) = P$.

Proof. Since $r(Q) = \bigcap_{Q \subseteq P \text{ prime}} P$, it suffices to show $r(Q)$ is prime. We have $xy \in r(Q) \implies \exists k, x^k y^k \in Q$ with Q being P primary it then implies that $\exists k, m$,such that $x^k \in Q$ or $y^{km} \in Q$. Hence x or y is in $r(Q)$. □

Definition 8.1.8. Let $I \subseteq R$ be ideal, then

- A **primary decomposition of** I is an expression of the form $I = \bigcap_{i=1}^{k} Q_i$ with Q_i primary.
- A primary decomposition is **reduced** if
  (a). for all $j, \bigcap_{i \neq j} Q_i \nsubseteq Q_j$,
  (b). all the $r(Q_i)$ are distinct.

We call this **reduced primary decomposition** as RPD.

Example 8.1.9. If $R = \mathbb{Z}$, there exists unique RPD for any ideal. The RPD of $(p_1^{k_1} \cdots p_m^{k_m})$ is $\bigcap_{i=1}^{m} (p_i^{k_i})$.

Lemma 8.1.10. *If Q_1, Q_2 are primary such that $r(Q_1) = r(Q_2)$, then $Q = Q_1 \cap Q_2$ is primary and $r(Q) = r(Q_1) = r(Q_2)$. Thus from any primary decomposition one can create a RPD.*

Proof. We see

- $r(Q) = r(Q_1 \cap Q_2) = r(Q_1) \cap r(Q_2) = r(Q_1)$.
- Q is primary, $xy \in Q$ and $y \notin r(Q) = r(Q_1) = r(Q_2)$ implies that $x \in Q_1 \cap Q_2 = Q$.
- Thus if $Q_i = Q_j$, reduce Q_i, Q_j by $Q_i \cap Q_j$.

Hence the lemma. □

Example 8.1.11. Take $R = \mathbb{C}[X, Y]$, then $I = (X^2, XY)$ has (at least) 2 RPD:

$$I = (X) \cap (X^2, XY, Y^2) = (X) \cap (X^2, Y).$$

Notation: For $I \subseteq R$ ideal, and $z \in R$, we say $(I : z) = \{r \in R | rz \in I\}$ (this is an ideal containing I).

Theorem 8.1.12. *If $I = \bigcap_{i=1}^{m} Q_i$ is RPD then*

$$\{r(Q_1), \cdots, r(Q_m)\} = \{\text{prime ideals of the form } r(I : x), x \in R\}.$$

Example 8.1.13. Take $R = \mathbb{C}[X, Y], I = (X^2, XY)$, then $r(X) = (X) = r(I : Y)$ and $r((X^2, XY, Y^2)) = r((X^2, Y)) = (X, Y) = r(I : X)$. For any $z \neq X, Y$ either $r(I : z) = (X)$ or (X, Y) or is not prime.

Lemma 8.1.14. *If $Q \subseteq R$ is primary then for any $x \in R$, we have*

$$r(Q:x) = \begin{cases} R & \text{if } x \in Q, \\ r(Q) & \text{if } x \notin Q. \end{cases}$$

Proof. We have

- $x \in Q \Longrightarrow (Q:x) = R \Longrightarrow r(Q:x) = R$,
- $x \notin Q, y \in r(Q:x) \Longleftrightarrow \exists n \geqslant 0, y^n x \in Q \overset{Q \text{ primary}}{\Longleftrightarrow} \exists m > 0, y^m \in Q \Longleftrightarrow y \in r(Q)$.

This gives the lemma. □

Proof of Theorem 8.1.12. Let $I = \bigcap_{i=1}^n Q_i$ RPD, observe that $r(I:x) = r((\bigcap Q_i) : x) = r(\bigcap(Q_i : x)) = \bigcap(r(Q_i:x)) = \bigcap_{i \text{ such that } x \notin Q_i} r(Q_i)$. Now we want to show $\{r(Q_1), \cdots, r(Q_m)\} = \{r(I:x) \text{ prime}\}$.

($\subseteq$): **reduced** decomposition implies that for all j, there is $x_j \in \bigcap_{i \neq j} Q_i \backslash Q_j$. Hence $r(I:x_j) = r(Q_j)$.

($\supseteq$): Suppose $r(I:x)$ is prime, $r(I:x) = \bigcap_{i, x \notin Q_i} r(Q_i)$ since prime ideals are irreducible (cannot be written as intersection of bigger ideals), we get $r(I:x) = r(Q_i)$ for some I. □

Theorem 8.1.15 (Weak Second Uniqueness Theorem)**.** *Suppose $I = \bigcap_{i=1}^n Q_i$ is RPD, if $j \in [n]$ is such that $r(Q_j)$ does not contain $r(Q_i), \forall i \neq j$, then Q_j appears in every RPD of I.*

Example 8.1.16. Consider the ideal $I = (X^2, XY) \subseteq \mathbb{C}[X,Y]$ and $I = (X) \cap (X^2, XY, Y^2), r(X) = (X)$ does not contain $r(Q_i), i \neq j$. Hence (X) will appear in every RPD.

Stronger version: for all $S \subseteq \{r(Q_i)\}$ closed downward, $\bigcap_{r(Q_i) \in S} Q_i$ is independent of RPD.

Lemma 8.1.17. *Let $Q \subseteq R$ primary ideal and let $S \subseteq R$ be multiplicative set, then $Q \cap S = \varnothing$ implies*

(a). $r(Q) \cap S \neq \varnothing$,

(b). Q is a contraction (for the fraction map $\epsilon : R \to S^{-1}R$),

(c). $S^{-1}Q$ is also primary.

Proof. We check one by one.

(a). Suppose $r(Q) \cap S \neq \varnothing$, then $\exists x \in R, n \geqslant 0, x \in S, x^n \in Q$ hence $x^n \in Q \cap S$ which implies $Q \cap S \neq \varnothing$, a contradiction.

(b). Recall Q is contraction if and only if $s \in S, x \notin Q \Longrightarrow sx \notin Q$. Let $s \in S, x \notin Q$, then S multiplicative set implies that $\forall n, s^n \in S$ thus $\forall n, s^n \notin Q$. Hence $s \notin r(Q)$. Then Q is primary so $x \notin Q, s \in r(Q) \Longrightarrow sx \notin Q$.

(c). Easy check.

Hence the lemma. □

Remark 8.1.18. Easy to check that the contradiction of a primary ideal is primary. Thus (b) above implies

$$\{\text{primary ideal } I \subseteq R\backslash S\} \overset{bijection}{\longleftrightarrow} \{\text{primary ideal of } S^{-1}R\},$$

$$I \longmapsto S^{-1}I.$$

Proof of Theorem 8.1.15. Let $I = \bigcap_{i=1}^n Q_i = \bigcap_{i=1}^n Q_i'$ such that $r(Q_i) = r(Q_i')$. Suppose $r(Q_j)$ does not contain $r(Q_i)$ for all $i \neq j$. Want to show $Q_j = Q_j'$. Let $S = R\backslash r(Q_j), \forall i \neq j, r(Q_i) \cap S \neq \varnothing \overset{(a)}{\Longrightarrow} Q_i \cap S \neq \varnothing \Longrightarrow S^{-1}Q_i = S^{-1}R$.

Thus $S^{-1}I = S^{-1}(\bigcap_i Q_i) = \bigcap_i(S^{-1}Q_i) = S^{-1}Q_j$. Since $r(Q_i') = r(Q_i)\forall i$, the same holds and $S^{-1}I = S^{-1}(\bigcap_i Q_i') = \bigcap_i(S^{-1}Q_i') = S^{-1}Q_j'$. hence $S^{-1}Q_j = S^{-1}Q_j'$ and since Q_j, Q_j' are contractions, $Q_j = (S^{-1}Q_j)^c = (S^{-1}Q_j')^c = Q_j'$. □

Theorem 8.1.19. *If R is Noetherian, then any ideal admits a RPD.*

Lemma 8.1.20. *If R is Noetherian, then any ideal is a finite intersection of irreducible ideals.*

Proof. Suppose for contradiction that I cannot be written as finite intersection of irreducibles. In this case there is I_1, J_1 ideals of $I = J_1 \cap I_1$ with $I \subsetneq I_1$ and I_1 cannot be written as intersections of ideals, $I = J_1 \cap J_2 \cap I_2, I_1 \subseteq I_2$, and I_2.... We get (I_n) strictly increasing infinite chain of ideals. It is impossible in R Noetherian. □

Lemma 8.1.21. *If R is Noetherian, then I irreducible implies I primary.*

Proof. Let I be irreducible, let $x, y \in R, xy \in I, x \notin I$, we need to show $y \in r(I)$ (consider ideals $(I : y^n) = \{r \in R, xy^n \in I\}$). This is a weakly increasing chain of ideal implies that $\exists n, (I : y^n) = (I : y^{n+1})$.

We claim $(I + x) \cap (I + y^n) = I$. Indeed let $z \in (I + x) \cap (I + y^n)$, then $z \in (I + x) \Longrightarrow zy \in I$. And $z \in (I + y^n) \Longrightarrow z = ry^n + z', r \in R, z' \in I \Longrightarrow ry^{n+1} \in I \Longrightarrow r \in (I : y^{n+1}) = (I : y^n) \Longrightarrow ry^n \in I \Longrightarrow z \in I$.

Since I is irreducible, (and $I + x \neq I$), we get $I + y^n = I$. Hence $y^n \in I \Longrightarrow y \in r(I)$ as wanted. □

Hence we showed

- The existence of RPD if R is Noetherian,
- First uniqueness: $r(Q_i)$ is uniquely determined,
- Second uniqueness: Q_i of "small" $r(Q_i)$ uniquely determined.

Example 8.1.22. If R is Noetherian, then any radical ideal I has unique decomposition $I = \bigcap_{i=1}^n P_i, P_i$ prime, $P_j \not\supseteq \bigcap_{i=j} P_i$. This induces that any algebraic set can be written uniquely as finite union of AAVs.

8.2 Dimensions

Remark 8.2.1. In $\mathbb{Z}$ any ideal has a **unique** RPD. This is related to the fact that $\dim(\mathbb{Z}) = 1$.

Definition 8.2.2. The **dimension of a ring** R is the maximal k such that there exists $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_k \subsetneq R$ prime ideal.

Example 8.2.3. We have $\dim(\mathbb{Z}) = 1, P_0 = (0), P_1 = (p)$ where p prime integers.

Remark 8.2.4. A domain R has dimension 0 if and only if R is a field.

A domain R has dimension 1 if and only if any prime ideal that is not 0 is maximal.

Proposition 8.2.5. *In a Noetherian domain of dimension* 1*, any ideal has a* ***unique*** *RPD.*

Proof. If R is Noetherian, this means that any ideal I has RPD $I = \bigcap Q_i$. Moreover (if $I \neq 0$), $r(Q_i)$ is maximal for all i, hence second uniqueness theorem gives Q_i are uniquely determined. $\square$

Remark 8.2.6. If R is domain of dimension 1, then $I = \bigcap Q_i$ RPD if and only if $I = \prod Q_i, Q_i$ primary and $r(Q_i)$ distinct.

Indeed, $r(Q_i)$ maximal distinct means that $r(Q_i) + r(Q_j) = R$ for all $i \neq j$ which implies that $Q_i + Q_j = R, \forall i \neq j$. This implies that $\bigcap Q_i = \prod Q_i$ (Exercise).

Coming next: In integrally closed Noetherian domain of dimension 1, any ideal can uniquely be written as product of prime ("Dedekind domain").

9 Integral Dependence and Nakayama Lemma

9.1 Nakayama Lemma

Lemma 9.1.1. *Let M be a finitely generated $R-$module, let $\phi \in \mathrm{End}_R(M)$ and let $I \subseteq R$ ideal such that $\mathrm{Im}(\phi) \subseteq I \cdot M$ ($I \cdot M = \{\sum r_i x_i | r_i \in I, x_i \in M\}$). Then $\exists n > 0, r_1, \cdots, r_n \in I$ such that $\phi^n + r_1\phi^{n-1} + \cdots + r_n \mathrm{Id} = 0$.*

Proof (generalization of Caylay-Hamilton Proof). Let $x_1, \cdots, x_n$ generators of M. For all i, there exists $a_{ij} \in I$ such that $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$, then

$$A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \text{ where } A = (\delta_{ij}\phi - a_{ij}\mathrm{Id})_{ij \in [n]} \in \mathrm{Mat}_n(\mathrm{End}_R(M)).$$

Let $B =$ adjoint of $A = {}^t$(cofactors of A), then

$$B \cdot A = \begin{pmatrix} \det(A) & & 0 \\ \vdots & \ddots & \vdots \\ 0 & & \det(A) \end{pmatrix} \text{ where } \det(A) = \det(\delta_{ij}\phi - a_{ij}\mathrm{Id}) \in \mathrm{End}_R(M),$$

where the right hand side is $\sum_{\delta \in S_n} \mathrm{sgn}(\delta)$.

We have $BA \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = 0$ implies that for all i, $\det(A)(x_i) = 0$ which means $\det(A) = 0$. □

Corollary 9.1.2 (Nakayama). *If M is finitely generated $R-$module, and $I \subseteq R$ ideal such that $I \cdot M = M$, then $\exists x \in I, (1 - x)M = 0$.*

Proof. For $\phi = \mathrm{Id}_M$, we have $\mathrm{Im}(\phi) \subseteq I \cdot M$. This implies that $\exists r_1, \cdots, r_n \in I$ such that $(1 + r_1 + \cdots + r_n)\mathrm{Id}_M = 0$. Take $x = -(r_1 + \cdots + r_n)$. □

Definition 9.1.3. The **Jacobson ideal of** R is $J = \bigcap_{P \subseteq R \text{ maximal}} P$ (it is a radical ideal).

Proposition 9.1.4. *We have* $J = \{x \in R | \forall r \in R, 1 + rx \text{ is unit}\}$.

Proof. Homework 8. □

Corollary 9.1.5. *If* M *is finitely generated* $R-$*module and* $J \cdot M = M$*, then* $M = 0$.

Proof. By Corollary 9.1.2, there is $x \in J, (1 - x)M = 0$. Hence $x \in J \implies 1 - x$ is a unit hence $M = 0$. □

Corollary 9.1.6. *Let* M *be finitely generated* $R-$*module, and* $N \subseteq M$ *submodule, such that* $M = N + J \cdot M$*. Then* $M = N$.

Proof. We have $M = N + J \cdot M \implies J \cdot M/N = (N + J \cdot M)/N = M/N \implies M/N = 0$. □

Corollary 9.1.7. *Let* R *be local ring and let* P *be its maximal ideal, let* M *be finitely generated* $R-$*module and let* $x_1, \cdots, x_n \in M$ *such that* $\{x_1 + P \cdot M, \cdots, x_n + P \cdot M\}$ *generates* $M/P \cdot M$ *as* $R/P-$*vector space. Then* $x_1, \cdots, x_n$ *are generators of* M *over* R.

Proof. Let $N = R\langle x_1, \cdots, x_n\rangle \subseteq M$ submodule generated by $x_1, \cdots, x_n$. We have $M = N + P \cdot M$, since $J = \bigcap_{I \max} I = P$. This implies $M = N$. □

9.2 Integral Dependence

Definition 9.2.1. Let $R \subseteq T$ be rings, $\alpha \in T$ is **integral over** R if $\exists n > 0, r_1, \cdots, r_n \in R$ such that $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$.

Example 9.2.2. We have

- Any $\alpha \in R$ is integral over R.
- For R field, α integral over R if and only if α algebraic over R.
- For $R = \mathbb{Z}, T = \mathbb{Q}$, only integers are integral over $\mathbb{Z}$. If $\alpha = \frac{a}{b} \in \mathbb{Q}\backslash\mathbb{Z}$, then we can take $\gcd(a, b) = 1$ by $(\frac{a}{b})^n + r_1(\frac{a}{b})^{n-1} + \cdots + r_n = 0$. Then a^n divisible by b, which is impossible.

Notation: For $R \subseteq T$ and $\alpha \in T$, we denote $R[\alpha] = R\langle \alpha, \alpha^2, \cdots\rangle$.

Proposition 9.2.3. *Let* $R \subseteq T$*, the following are equivalent for* $\alpha \in T$*:*

(1). The element α is integral over R,

(2). The module $R[\alpha]$ is a finitely generated $R-$module,

(3). There exists $S \supseteq R[\alpha]$ ring which is finitely generated $R-$module.

Proof. (1)$\Longrightarrow$(2) because $\alpha^n + r_1\alpha^{n-1} + \cdots + r_1 = 0$, then $R[\alpha] = R\langle \alpha, \cdots, \alpha^{n-1}\rangle$.
(2)$\Longrightarrow$(3): Take $S = R[\alpha]$.
(3)$\Longrightarrow$(1): Let $\phi = \alpha \mathrm{Id}_S : S \to S$ is a $R-$module endomorphism. Then S is finitely generated implies that $\exists r_1, \cdots, r_n \in R$ such that $\phi^n + r_1\phi^{n-1} + \cdots + r_n\mathrm{Id} = 0$. Applying this to 1_S gives $\alpha^n + r_1\alpha^{n-1} + \cdots + r_m = 0$. □

Corollary 9.2.4. *We have $\alpha_1, \cdots, \alpha_n$ integral over R if and only if $R[\alpha_1, \cdots, \alpha_n]$ is a finitely generated $R-$module. Hence sums, difference, product of integral elements are integral over R.*

Proof. ($\Longrightarrow$): Easy by induction on n ((1)$\Longrightarrow$(2)).
($\Longleftarrow$): Already proved ((3)$\Longrightarrow$(1)). □

Thus any element in $R[\alpha_1, \cdots, \alpha_n]$ is integral ((3)$\Longrightarrow$(1)).

Definition 9.2.5. Let $R \subseteq T$ be rings. The **integral closure of R in T** is $\overline{R}^T = \{\alpha \in T | \alpha \text{ integral over } R\}$.

Example 9.2.6. We have $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$.

Definition 9.2.7. Let $R \subseteq T$, then

- If $\overline{R}^T = T$, then T is called **integral over** R.
- If $\overline{R}^T = R$, then R is called **integrally closed in** T.

Remark 9.2.8. The closure $\overline{R}^T$ is subring of T (since sum, difference, product of integral are integral).

Lemma 9.2.9. *Let $R \subseteq S \subseteq T$ be rings, if S is integral over R, and T is integral over S, then T is integral over R.*

Proof. Let $\alpha \in T$, then $\exists s_1, \cdots, s_n \in S$ such that $\alpha^n + s_1\alpha^{n-1} + \cdots + s_n = 0$. Hence $R[s_1, \cdots, s_n, \alpha]$ is finitely generated $R[s_1, \cdots, s_n]-$module and $R[s_1, \cdots, s_n]$ is finitely generated $R-$module. Therefore $R[s_1, \cdots, s_n, \alpha]$ is finitely generated $R-$module. Then α is integral over R. □

Corollary 9.2.10. *The closure $\overline{R}^T$ is integrally closed in T.*

Proof. Apply lemma, $R \subseteq \overline{R}^T \subseteq \overline{\overline{R}^T}^T$. By lemma any element of $\overline{\overline{R}^T}^T$ is integral over R hence in $\overline{R}^T$. Thus $\overline{\overline{R}^T}^T = \overline{R}^T$. □

Lemma 9.2.11. *Let $R \subseteq T$ be rings, with T integral over R, then*

(1). for all $J \subseteq T$ ideal, T/J is integral over $(R+J)/J(\simeq R/(R \cap J))$.

(2). For all $S \subseteq R$ multiplicative set, $S^{-1}T$ is integral over $S^{-1}R$.

Proof. Need to prove that

(1). For all $\alpha \in T, \alpha + J$ is integral over $(R+J)/J$.

(2). For all $\alpha \in T$, for all $s \in S$, $\frac{\alpha}{s}$ is integral over $S^{-1}R$.

Exercise. □

Lemma 9.2.12 (Localization commutes with integral closure)**.** *Let $R \subseteq T$ be rings, and let $S \subseteq R$ multiplicative set, then $\overline{S^{-1}R}^{S^{-1}T} = S^{-1}(\overline{R}^T)$.*

Proof. ($\supseteq$): By statement (2) in previous lemma ($\overline{R}^T$ is integral over R implies that $S^{-1}\overline{R}^T$ is integral over $S^{-1}R$).

($\subseteq$): We have $\frac{t}{s} \in \overline{S^{-1}R}^{S^{-1}T} \implies \exists r_i \in R, s_i \in R, (\frac{t}{s})^n + (\frac{r_1}{s_1})(\frac{t}{s})^{n-1} + \cdots + (\frac{r_n}{s_n}) = 0$. Then multiply by $(ss_1 \cdots s_n)^n$ implies that $(ts_1 \cdots s_n)^n + \cdots = 0$. Thus $ts_1 \cdots s_n$ is integral over R. Hence $\frac{t}{s} = \frac{ts_1 \cdots s_n}{ss_1 \cdots s_n} \in S^{-1}\overline{R}^T$. □

Definition 9.2.13. A domain R is called **integrally closed** if it is integrally closed in its field of fraction.

Example 9.2.14. We have

- $\overline{\mathbb{Z}}^{\mathbb{Q}} = \mathbb{Z}$ hence $\mathbb{Z}$ is integrally closed.
- Any UFD is integrally closed (same proof as for $\mathbb{Z}$).

Proposition 9.2.15 (Integrally closed is a local property)**.** *For a domain R, the following are equivalent:*

(1). The domain R is integrally closed.

(2). The local ring R_P is integrally closed for all $P \subseteq R$ prime ideal.

(3). The local ring R_P is integrally closed for all $P \subseteq R$ maximal ideal.

Proof. Let K be the field of fraction of R, for all P prime, we have $R \subseteq R_P \subseteq K = R_{\{0\}}$. Hence K is a field of fractions of R_P. Let $C = \overline{R}^K$. By previous lemma, $C_P = (\overline{R_P})^K$. Let

$$\phi : R \longrightarrow C,$$

$$r \longmapsto r,$$

be embedding map, and for $P \subseteq R$ prime, let

$$\phi_P : R_P \longrightarrow C_P,$$

$$\frac{r}{s} \longmapsto \frac{r}{s},$$

localization of ϕ at P, we have

$$(1) \iff \phi \text{ surjective},$$

$$(2) \iff \phi_P \text{ surjective } \forall P \subseteq R \text{ prime},$$

$$(3) \iff \phi_P \text{ surjective } \forall P \subseteq R \text{ maximal}.$$

The 3 statements are equivalent since "being surjective is a local property". □

9.3 Going Up/Down Theorems

Remark 9.3.1. Let $R \subseteq T$ be rings such that for all $J \subseteq T$ ideal, $J \cap R$ is ideal, and $\forall J \subseteq T$ prime ideal, $J \cap R$ prime (indeed $R \cap J$ is contraction of J for embedding map $R \hookrightarrow T$). We will show that if T integral over R, then any prime ideal of R is of this form.

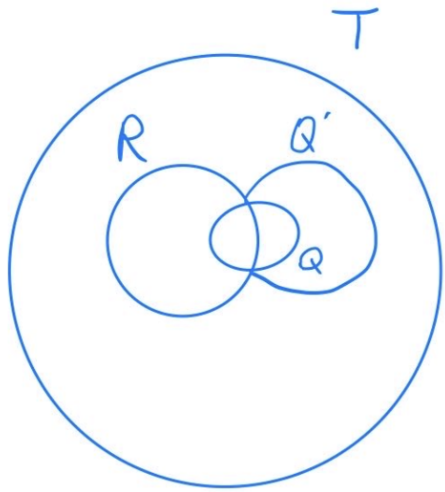
Lemma 9.3.2. *Let $R \subseteq T$ be domains and T is integral over R, then T is a field if and only if R is a field.*

Proof. Exercise. □

Corollary 9.3.3. *Let $R \subseteq T$ be a ring such that T is integral over R, let $Q \subseteq T$ be a maximal ideal of T, then Q is maximal in T if and only if $Q \cap R$ is maximal in R.*

Proof. We have $T/Q, R/R \cap Q$ are domains (since $Q, Q \cap R$ are prime). By lemma, T/Q is integral over $(R + Q)/Q \simeq R/R \cap Q$. Hence Q is maximal if and only if T/Q is a field if and only if $R/R \cap Q$ is a field if and only if $R \cap Q$ is maximal. □

Corollary 9.3.4. *Let $R \subseteq T$ be rings, T integral over R, let $Q \subseteq Q' \subseteq T$ be prime ideals. If $Q \cap R = Q' \cap R$ then $Q = Q'$.*



Proof. Assume $Q \cap R = Q' \cap R$, then the ideal $P = Q \cap R$ is prime ideal of R. By lemma, T_P is integral over R_P (here $T_P = S^{-1}T, S = R\backslash P$). The localization of Q_P, Q'_P satisfy $Q_P \cap R_P = Q'_P \cap R_P = (Q \cap R)_P = P_P$ maximal ideal of R_P. By Corollary 9.3.3, Q_P, Q'_P are maximal ideals of T_P. Since $Q_P \subseteq Q'_P$, we get $Q_P = Q'_P$. Moreover, Q and Q' are prime and not intersecting $S = R\backslash P$. Hence they are contractions via localization at P. Hence $Q = Q_P^C = Q_P^{C'} = Q'$. $\square$

Theorem 9.3.5. *Let $R \subseteq T$ be rings, T integral over R, for all $P \subseteq R$ prime ideal of R, there is $Q \subseteq T$ prime ideal of T such that $P = Q \cap R$.*

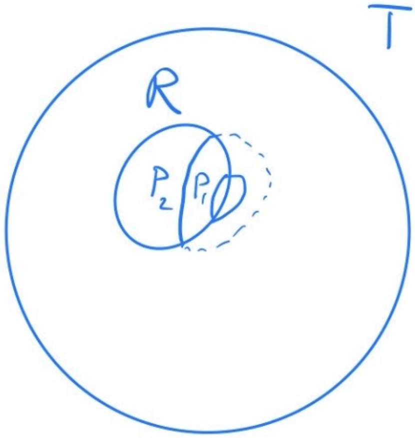
Proof. We have that T_P integral over R_P. Moreover, the diagram

$$\begin{tikzcd} R \arrow[r, hook, "\alpha"] \arrow[d, "\phi"'] & T \arrow[d, "\psi"] \\ R_P \arrow[r, "\beta"'] & T_P \end{tikzcd},$$

where α, β embedding map, ϕ, ψ localization maps is commutative ($r \mapsto \frac{r}{1} \in T_P$).

Let M be a maximal ideal of T_P, then $\beta^{-1}(M) = M \cap R_P$ is maximal ideal of R_P (by Corollary 9.3.3). Hence $\beta^{-1}(M) = P_P$ and thus $\phi^{-1}(\beta^{-1}(M)) = P$. Therefore $P = \alpha^{-1}(\psi^{-1}(M)) = R \cap \psi^{-1}(M)$ where the last term is prime ideal of T. $\square$

Corollary 9.3.6 (Going Up Theorem)**.** *Let $R \subseteq T$ be rings, T integral over R, let $P_1 \subseteq P_2 \subseteq R$ be prime ideal, let Q_1 prime ideal of T, such that $P_1 = Q_1 \cap R$, then $\exists Q_2 \supseteq Q_1$, prime ideal of T such that $P_2 = Q_2 \cap R$.*



Proof. By previous lemma, T/Q is integral over $R + Q_1/Q_1 \simeq R/P_1$, and P_2/P_1 is prime in R/P_1. Hence by previous theorem, there is $\overline{Q_2} \subseteq T/Q_1$ such that $P_2/P_1 = \overline{Q_2} \cap R/P_1$ and $\overline{Q_2} = Q_2/Q_1$ for some $Q_2 \supseteq Q_1$ prime ideal of T. Hence $P_2/P_1 = (Q_2 \cap R)/P_1$. Therefore, $P_2 = Q_2 \cap R$. $\square$

Corollary 9.3.7. *The dimension* $\dim R = \dim T$.

10

Dedekind Domains and Discrete Valuation Rings

10.1 Basic Definitions and Results

Recall:

- A **Dedekind domain** is a Noetherian domain of dimension 1 which is integrally closed.
- In Noetherian domain of dimension 1, any ideal $I \neq 0$ can be written uniquely as $I = \prod Q_i$ with Q_i primary with distinct radicals.

Goal: show that in Dedekind domain, $I \neq 0$ has a unique factorization $I = \prod P_i^{d_i}$ where P_i are prime ideals.
Motivations:

Definition 10.1.1. We say

- An **algebraic number field** is a finite algebraic extension L of $\mathbb{Q}$.
- Its **ring of integers** is $\overline{\mathbb{Z}}^L$.

Example 10.1.2. Let $L = \mathbb{Q}[i]$ be an algebraic number field and then $\mathbb{Z}[i]$ is its ring of integers.

Theorem 10.1.3. *The ring of integers $\overline{\mathbb{Z}}^L$ of any algebraic number field is a Dedekind domain.*

Lemma 10.1.4. *Let R be a domain integrally closed in its field of fraction K. If L is a finite separable extension of K, then there exists $b_1, \cdots, b_n$ basis of L over K such that $\overline{R}^L \subseteq \langle b_1, \cdots, b_n \rangle$.*

Proof. Skipped (field theory). $\square$

Proof of Theorem 10.1.3. To show Dedekind domain, we are to show

- it is Noetherian domain,
- it is dimension 1,
- it is integrally closed.

We see

- $\overline{\mathbb{Z}}^L$ is a domain since it is included in L, which is a field.
- Since $K = \mathbb{Q}$ has characteristic zero, any extension of $\mathbb{Q}$ is separable.

Hence lemma gives $\overline{\mathbb{Z}}^L \subseteq \mathbb{Z}\langle b_1, \cdots, b_n\rangle$ is finitely generated $\mathbb{Z}-$module. Since $\mathbb{Z}$ is PID, we have $\overline{\mathbb{Z}}^L$ is finitely generated $\mathbb{Z}-$module. Also since $\mathbb{Z}$ is Noetherian, we have $\overline{\mathbb{Z}}^L$ is Noetherian (finitely generated algebraic over Noetherian). Hence we have

- $\overline{\mathbb{Z}}^L$ is integrally closed in its field of fraction K since $K \subseteq L$,
- $\dim(\overline{\mathbb{Z}}^L) = \dim(\mathbb{Z}) = 1$ since dimension of integral extension equals the dimension of the ring.

Hence the theorem is proved. □

Definition 10.1.5. Let K be a field. A **discrete valuation** is $v : K^\times \longrightarrow \mathbb{Z}$ such that

- v is surjective,
- $v(xy) = v(x) + v(y)$,
- $v(x + y) \geqslant \min(v(x), v(y))$.

(v is surjective group homomorphism $(K^\times, \times) \longrightarrow (\mathbb{Z}, +)$). We get $v(0) = +\infty$.

Example 10.1.6. Let $K = \mathbb{Q}$, given p prime number we define $v_p(q) = k$ if $q = p^k \frac{a}{b}$ where $p \nmid a, p \nmid b$.

Remark 10.1.7. We have $v(1) = 0, v(x^{-1}) = -v(x), v(-1) = -v(-1) = 0, v(-x) = v(x)$. We also have $K_v = \{x \in K | v(x) \geqslant 0\}$ is a subring of K.

Definition 10.1.8. The ring R is a **discrete valuation ring (d.v.r)** if $R = K_v$ for some field K and discrete valuation v.

Example 10.1.9. We have $\mathbb{Z}_{(p)} = \{\frac{a}{b} | p \nmid b\}$ is a d.v.r since $\mathbb{Z}_{(p)} = \mathbb{Q}_{v_p}$ with v_p defined as before.

Remark 10.1.10. We have the following facts:

- For any d.v.r $K_v, \forall x \in K$, either x or x^{-1} is in K_v.
- An element $x \in K_v$ is invertible if and only if $v(x) = 0$.
- If $0 \leqslant v(x) \leqslant v(y)$ then $x|y$ in K_v (because $yx^{-1} \in K_v$).

Theorem 10.1.11. *Let R be a ring, then R is a local Dedekind domain if and only if R is a d.v.r. Moreover, the following are equivalent properties for a local Noetherian domain of dimension 1:*

(1). The ring R is integrally closed (hence local Dedekind).

(2). The maximal ideal $M \subseteq R$ is principal (generated by a single element).

(3). Every ideal $I \neq 0$ is a power of the maximal ideal M.

(4). There exists $p \in R$ such that every ideal is of the form (p^k).

(5). The ring R is a d.v.r.

Proof. ($\Longleftarrow$): We see

- Let R be a d.v.r. Let $p \in R, v(p) = 1$. For $I \neq 0$ ideal, and let $k = \min_{x \in I}(v(x))$. Then there exists $x \in I, v(x) = k = v(p^k)$. This implies $p^k \in I$ (since $x|p^k$) and $I = (p^k)$ (since for all $y \in I, v(p^k) \leqslant v(y) \Longrightarrow p^k|y$). Given that the nonzero ideal are $(p) \supseteq (p^2) \supseteq (p^3) \supseteq \cdots$, it is clear that R is Noetherian, local of dimension 1 (unique nonzero prime ideal is (p)).
- Lastly R is integrally closed, let $\alpha \in K$ field of fractions of R. Suppose $\exists r_1, \cdots, r_n \in R$ such that $\alpha^n + r_1\alpha^{n-1} + \cdots + r_n = 0$. If $\alpha \notin R$, then $\alpha^{-1} \in R$ (since R is d.v.r). Hence $\alpha = -r_1 - r_2\alpha^{-1} - \cdots - r_n(\alpha^{-1})^{n-1} \in R$.

($\Longrightarrow$): It suffices to show $(1) \Longrightarrow (2) \Longrightarrow (3) \Longrightarrow (4) \Longrightarrow (5)$ (we have already proved $(5) \Longrightarrow (1)$). We prove

$(1) \Longrightarrow (2)$ and $(2) \Longrightarrow (3)$ are left as homework.

$(3) \Longrightarrow (4)$: We have $M^2 \subseteq M$ and $M^2 \neq M$ (because $M = J$ Jacobson radical), hence there exists $p \in M \backslash M^2$. Then $\exists n, (p) = M^n$ implies that $(p) = M$ and thus for all $k, M^k = (p^k)$.

$(4) \Longrightarrow (5)$: Take $M = (p)$ is the unique maximal ideal, hence $(p) = J$ Jacobson radical, for all k, $(p^{k+1}) \neq (p^k)$ (because $J \cdot N = N$ implies $N = 0$). Hence for any $x \in R\backslash\{0\}, \exists! k \geqslant 0, (x) = (p^k)$ and we define $v(x) = k$. We extend v to the field of fractions K of R by $v(\frac{a}{b}) = v(a) - v(b)$. It is easy to see that $R = K_v$ is a d.v.r. $\square$

Theorem 10.1.12. *Let R be a Noetherian domain of dimension 1, the following are equivalent:*

(a). R is integrally closed (hence Dedekind).

(b). For all $P \subseteq R$ prime, R_P is a local Dedekind (equivalent to a d.v.r).

(c). Every primary ideal is a power of prime ideal.

(d). Every nonzero ideal has a unique factorization into prime ideals.

Lemma 10.1.13. *Ideal P maximal implies that P^n primary for all n (homework).*

Proof of Theorem 10.1.12. $(a) \Longrightarrow (b)$: integrally closed is a local property.

$(b) \Longrightarrow (c)$: Let Q be primary ideal and let $P = r(Q)$, then Q primary implies that $Q = Q^{ec}$ for $R \longrightarrow R_P$. Then R_P local Dedekind implies that $Q^e = Q_P$ is a power of the maximal P_P. Hence $Q = (P_P^k)^c = ((P^k)_P)^c = (P^k)^{ec} = P^k$ where P^k is primary as power of maximal.

$(c) \Longrightarrow (b)$: Let P be prime ideal, want to show R_P is local Dedekind by previous theorem, it suffices to show that any ideal of R_P is a power of P_P. [We skip the fact that Q has RPD and localizations].

$(c) \Longrightarrow (d)$: Existence: $I = \prod Q_i$ with Q_i primary (already shown) implies that $I = \prod P_i^{d_i}$ by (c). Uniqueness: We have $\{Q_1, \cdots, Q_n\}$ is unique (already shown). Hence we see $P^d = P'^{d'}$ which implies $r(P^d) = r(P'^{d'})$ hence $P = P'$. Further, $P^d = P^{d'}$ implies $d = d'$ because $P^k = P^{k+1}$ implies $P_P^k = P_P^{k+1}$ implies $P_P = 0$ by Nakayama lemma, hence impossible (since it is a domain).

$(d) \Longrightarrow (c)$: Let Q be primary, $Q = \prod P_i^{d_i}$ implies that $r(Q) = \bigcap r(P_i^{d_i}) = \bigcap P_i$. Also $r(Q)$ prime hence $r(Q) = \bigcap P_i$ hence $r(Q) = P_i$ for some i. This shows $Q = P_i^{d_i}$. $\square$

Part III

Homological Algebra

11

Motivational Examples

11.1 Chains of Modules

Let R be a ring, $\mathcal{R}-\mathcal{M}od$ = category of $R-$modules (left $R-$modules).

Definition 11.1.1. A **chain complex** (in $\mathcal{R}-\mathcal{M}od$) is $C_* = (C_n)_{n\geqslant 0}$ and $d_* = (d_n)_{n>0}$ where C_n is $R-$module, $d_n : C_n \to C_{n-1}$ is $R-$module homomorphism such that $d_n \circ d_{n+1} = 0$

$$\cdots \longrightarrow C_2 \xrightarrow{d_2} C_1 \xrightarrow{d_1} C_0.$$

Example 11.1.2. Take C_* associated to the simplicial complex such that $C_n = \mathbb{Z}\langle n-cell\rangle, d_n$:"boundary maps".

Definition 11.1.3. Let (C_*, d_*) be chain complex (in $\mathcal{R}-\mathcal{M}od$), we denote that $Z_n(C_*) = \ker(d_n) \subseteq C_n$, namely the "**cycles**" and $B_n(C_*) = \operatorname{Im}(d_{n+1}) \subseteq C_n$ "**boundaries**". Since $d_n d_{n+1} = 0$ and $B_n \subseteq Z_n$ and we can take quotient $H_n(C_*) = Z_n/B_n$, the $n-$**th homology group of** C_*.

Example 11.1.4. Consider the torus with $H_1(C_*) = \mathbb{Z}$ cycles/$\mathbb{Z}$ contractible cycles.

Remark 11.1.5. Chain C_* is exact if and only if $H_n(C_*) = 0 \forall n$. Hence $H_n(C_*)$ is the measure of non-exactness of the $n-$th step.

Definition 11.1.6. Let C_*, C'_* be chain complexes. A **chain map** $f_* : C_* \longrightarrow C'_*$ is $f_* = (f_n)_n \geqslant 0$, and $f_n : C_n \longrightarrow C'_n$ module homomorphism such that "every squares commute" in

$$\begin{tikzcd}
\cdots \arrow[r] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"'] & C_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & \cdots \arrow[r] & C_0 \\
\cdots \arrow[r] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r] & \cdots \arrow[r] & C'_0
\end{tikzcd}$$

and $df = fd'$.

Example 11.1.7. If C_*, C'_* are associated with some simplicial complexes... To be filled.

Remark 11.1.8. If $f_* : C_* \longrightarrow C'_*$ is a chain map, then for all n, f_n sends cycles to cycles (boundaries to boundaries).

In $f(Z_n(C_*)) \subseteq Z_n(C'_*)$ because $df(Z_n(C_*)) = fd(Z_n(C_*)) = f0 = 0$. Moreover, $f_n(B_n(C_n)) \subseteq B_n(C'_*)$ because $f(d_{C_{n+1}}) = df(C_{n+1}) \subseteq \mathrm{Im} d$.

Definition 11.1.9. Let $f_* : C_* \longrightarrow C'_*$ be a chain map, by preceding remark we can define

$$\overline{f_n} : H_n(C_*) \longrightarrow H_n(C'_*),$$
$$\alpha + B_n(C_*) \longmapsto f_n(\alpha) + B_n(C'_*)$$

where $\alpha \in Z_n(C_*)$. This is a well-defined homomorphism by preceding remark (sends boundaries to boundaries).

Remark 11.1.10. Composition of chain maps are chain maps, that is, $\overline{f_n} \circ \overline{g_n} = \overline{f_n \circ g_n}$ (functoriality).

Definition 11.1.11 (Chain Homotopy)**.** Let $f_*, g_* : C_* \longrightarrow C'_*$ be chain maps. We say that f_*, g_* are **homotopy equivalent** if there exists $h = (h_n)_{n \geqslant 0}, h_n : C_n \to C'_{n+1}$ $R-$module homomorphism such that for all n, $f_n - g_n = h_{n-1}d_n + d'_{n+1}h_n$. It can be viewed as

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[dl, "h_n"'] \arrow[d, shift right, "f_n"'] \arrow[d, shift left, "g_n"] & C_{n-1} \arrow[r] \arrow[dl, "h_{n-1}"'] \arrow[d, shift right, "f_{n-1}"'] \arrow[d, shift left, "g_{n-1}"] & \cdots \\
\cdots \arrow[r] & C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

where we have notation $f_* \underset{h}{\simeq} g_*$.

Example 11.1.12. To be filled.

Lemma 11.1.13. *If chain maps $f_*, g_* : C_* \longrightarrow C'_*$ are homotopy equivalent, then $\overline{f_n} = \overline{g_n} : H_n(C_*) \to H_n(C'_*)$.*

Proof. Suppose $f_* \underset{h}{\simeq} g_*$, for all $\alpha \in Z_n(C_*)$, $f_n(\alpha) - g_n(\alpha) = dh(\alpha) + hd(\alpha) = dh(\alpha) \in B_n(C'_*)$. Hence $\overline{f_n}(\alpha) = f_n(\alpha) + B_n(C'_*) = g_n(\alpha) + B_n(C'_*) = \overline{g_n}(\alpha)$. □

Definition 11.1.14. Two chain complex C_*, C'_* are **homotopy equivalent** if there is chain maps $f_* : C_* \longrightarrow C'_*$ and $g_* : C'_* \longrightarrow C_*$ such that $g_* \circ f_* \simeq \mathrm{Id}_{C_*}$, $f_* \circ g_* \simeq \mathrm{Id}_{C'_*}$.

Corollary 11.1.15. *If C_*, C'_* are homotopy equivalent then for all n, we have $H_n(C_*) \simeq H_n(C'_*)$ isomorphism of $R-$module.*

Proof. By lemma $\overline{g_n} \circ \overline{f_n} = \mathrm{Id}_{H_n(C_*)}$ and $\overline{f_n} \circ \overline{g_n} = \mathrm{Id}_{H_n(C'_*)}$. Hence $\overline{f_n}, \overline{g_n}$ are isomorphism. $\square$

Definition 11.1.16. We have the following definitions:

- A **resolution** for a $R-$module M is an exact sequence of the form $\cdots \longrightarrow C_2 \longrightarrow C_1 \longrightarrow C_0 \longrightarrow M \longrightarrow 0$. Abbreviated by $C_* \longrightarrow M \longrightarrow 0$.
- A **free resolution** is a resolution such that for all n, C_n is free $R-$module: $(C_* \longrightarrow M \longrightarrow 0)$.

Lemma 11.1.17. *We have the following statements:*

(a). For any $R-$module N, there exists free $R-$module F and $\phi : F \longrightarrow N$ surjective $R-$module homomorphism. That is, $\exists$free $F \underset{\exists \phi}{\twoheadrightarrow} \forall N$.

(b). For any F free, for any $\phi : F \to N$, for any $\psi : N' \twoheadrightarrow N$ surjective homomorphism, there exists ϕ' such that $\psi \circ \phi' = \phi$. That is, the diagram

$$\begin{tikzcd}
F \text{ free} \arrow[d, dotted, "\exists \phi'"'] \arrow[dr, "\forall \phi"] & \\
N' \arrow[r, two heads, "\forall \psi"'] & N
\end{tikzcd}$$

commutes.

Proof. Exercise. Easy consequence of the fact that if F is free with basis $\{b_i\}$, then for any M module, for all $\{x_i\} \subseteq M$, there is $\phi : F \longrightarrow M$ such that $\phi(b_i) = x_i$. $\square$

Theorem 11.1.18 (Fundamental Theorem of Homological Algebra). *We have*

- *for all M, $R-$module, there is free resolution $C_* \longrightarrow M \longrightarrow 0$, and*
- *for all $f : M \to M'$ homomorphism, for any free resolution, $C_* \longrightarrow M \longrightarrow 0$ and $C'_* \longrightarrow M' \longrightarrow 0$. There is $f_* : C_* \longrightarrow C'_*$ chain map "lifting f", the diagram*

$$\begin{tikzcd}
\cdots \arrow[r] & C_0 \arrow[r, "d_0"] \arrow[d, "f_0"] & M \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r] & C'_0 \arrow[r, "d'_0"] & M' \arrow[r] & 0
\end{tikzcd}$$

commutes with $d'_0 f_0 = f d_0$. Moreover, we have

  - *the free resolution C_* of M is unique up to homotopy, and*
  - *the lifting f_* of f is unique up to homotopy.*

Proof. We see

- Existence of free resolution: applying (a) to $N = M$ gives C_0, d_0 that $C_0 \overset{d_0}{\twoheadrightarrow} M \to 0$. Applying (a) to $N = \ker(d_0)$ gives $C_1, d_1, \cdots$, etc.

- Existence of chain map lifting f :

$$\begin{tikzcd}
C_n \arrow[r] \arrow[d, "?"] \arrow[dr, bend left] & C_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] & \cdots \arrow[r] \arrow[d] & C_0 \arrow[r] \arrow[d] & M = C_{-1} \arrow[r] \arrow[d, "f=f_{-1}"] & 0 \\
C'_n \arrow[r] & C'_{n-1} \arrow[r] & \cdots \arrow[r] & C'_0 \arrow[r] & M' = C'_{-1} \arrow[r] & 0
\end{tikzcd}$$

  for all $n \geqslant 0$, we need to find f_n from f_{n-1} (such that $d'f = fd$).

  Observe that $f_{n-1} \circ d_n(C_n) \subseteq \ker(d'_{n-1})$ since $d'_{n-1} \circ f_{n-1} \circ d_n = d'_{n-2} \circ d'_{n-1} \circ f_n = 0$ since $d'_{n-2} \circ d'_{n-1} = 0$. So we have

$$\begin{tikzcd}
C_n \text{ free} \arrow[d, dotted, "\exists"'] \arrow[dr, "f_{n-1}d_n"] & \\
C'_n \arrow[r, two heads, "d'_n"'] & \mathrm{Im}(d'_n) = \ker(d'_{n-1})
\end{tikzcd}$$

  By (b), there is $f_n : C_n \longrightarrow C'_n$ such that $d'_n f_n = f_{n-1} d_n$.

Then we see

- Uniqueness of f_* up to homotopy. Suppose f_*, g_* both lift $f : M \to M'$. Then $l_n = f_n - g_n$ lifts $0 : M \to M'$. We want to find $(h_n), h_n : C_n \to C'_{n+1}$ such that $l = hd + d'h$. How about h_0? We have the diagram

$$\begin{tikzcd}
 & C_0 \arrow[r, "d_0"] \arrow[d, "l_0"] \arrow[dl, dotted, "h_0"'] & M \arrow[d, "l=0"] \\
C'_1 \arrow[r, dotted, "d'_1"'] & C'_0 \arrow[r, "d'_0"'] & M'
\end{tikzcd}$$

  and want $l_0 = d'_1 h_0$. Since $d'_0 l_0 = 0 d_0 = 0$, we have

$$\begin{tikzcd}
 & C_0 \arrow[d, "l_0"] \arrow[dl, dotted, "\exists h_0"'] \\
C'_1 \arrow[r, two heads, "d'_1"'] & \ker(d'_0) = \mathrm{Im}(d'_1)
\end{tikzcd}$$

  commutes. By (b), there is h_0 such that $l_0 = d'_1 \circ h_0$.

For $n > 0$, we want h_n such that $d'_{n+1}h_n = l_n - h_{n-1}d_n$ such that

$$\begin{tikzcd} & C_n \arrow[r, "d_n"] \arrow[dl, dotted, "h_n"'] \arrow[d, "l_n"] & C_{n-1} \arrow[dl, "h_{n-1}"] \\ C'_{n+1} \arrow[r, "d'_{n+1}"'] & C'_n & \end{tikzcd}$$

commutes. We have also

$$\begin{tikzcd} & C_n \arrow[d, "l_n - h_{n-1}d_n"] \\ C'_{n+1} \arrow[r, two heads] & \ker(d'_n) = \mathrm{Im}(d'_{n+1}) \end{tikzcd}.$$

(Indeed, $d'_n(l_n - h_{n-1}d_n) = l_{n-1}d_n - d'_n h_{n-1}d_n = (l_{n-1} - d'_n h_{n-1})d_n = h_{n-2}d_{n-1}d_n = 0$). By (b), there is h_n such that $d'_{n+1}h_n = l_n - h_{n-1}d_n$.

- Uniqueness of free resolution up to homotopy: let $C_* \to M \to 0, C'_* \to M \to 0$ be free resolution of M. There is $f_* : C_* \to C'_*$ lifted $\mathrm{Id} : M \to M$, and $g_* : C'_* \to C_*$ lifted $\mathrm{Id} : M \to M$. Then $g_*f_* : C_* \to C_*$ lifts Id_M implies that $g_*f_* \simeq \mathrm{Id}_{C_*}$ and $f_*g_* : C'_* \to C'_*$ lifts Id_M implies that $f_*g_* \simeq \mathrm{Id}_{C'_*}$.

Generalizations? Projective modules. □

11.2 Projective Modules

Definition 11.2.1. A $R-$module P is **projective** if it satisfies

$$\begin{tikzcd} P \arrow[d, dotted, "\exists \phi'"'] \arrow[dr, "\forall \phi"] & \\ M \arrow[r, two heads, "\forall \psi \text{ surjective}"'] & N \end{tikzcd}$$

commuting (prop (b) of free module).

Remark 11.2.2. We have

- By lemma 11.1.17 (b), any free module is projective. By (a), for any $N \in \mathcal{R} - \mathcal{M}od$, there is P projective and $\phi : P \twoheadrightarrow N$ surjective. "$\mathcal{R} - \mathcal{M}od$ has enough projective." This implies that for any $M \in \mathcal{R} - \mathcal{M}od$, there exists $P^* \to M \to 0$ projective resolution of M.

- The theorem remains true if we replace "free" by "projective" everywhere. (existence of projective resolution by above, existence of f^*, uniqueness up to homotopy only use (b) = definition of projective).
- Reversing arrows.

Definition 11.2.3. A $R-$module E is **injective** if it satisfies

$$\begin{tikzcd} M \arrow[r, tail, "\forall\psi \text{ injective}"] \arrow[d, "\forall\phi"'] & N \arrow[dl, dotted, "\exists\phi'"] \\ E & \end{tikzcd}$$

commuting.

Definition 11.2.4. An **injective coresolution** for a $R-$module M is

$$0 \longrightarrow M \xrightarrow{d_0} E_0 \xrightarrow{d_1} E_1 \longrightarrow E_2 \longrightarrow \cdots$$

exact sequence with E_n injective module.

Question: Do they exist? Existence amounts to showing for any N, there exists E injective and $N \rightarrowtail E$ injective homomorphism.

Exercise: show that when they exist, injective coresolution are unique up to homotopy.

More general categories: How to define "exact sequence" in a category? How about surjective, injective, kernel, images ($H_n = Z_n/B_n$)? This leads us to Abelian categories

$$\begin{tikzcd} C_* \arrow[r] \arrow[d, "F"'] \arrow[loop left] & M \arrow[r] & 0 \\ F(C_*) \arrow[r] & FM \arrow[r] & 0 \end{tikzcd}.$$

12

Additive Categories

12.1 Category Notations

Let $\mathcal{C}$ be a category, then

- $A \in \mathcal{C}$ means A is an object of $\mathcal{C}$.
- For objects $A, B \in \mathcal{C}$, we denote $\mathcal{C}(A, B)$, which is the set $\mathcal{Mor}_{\mathcal{C}}(A, B)$ of $\mathcal{C}-$morphisms from A to B.
- We denote $\mathcal{Set}$ the category of sets.
- We denote $\mathcal{R} - \mathcal{Mod}$ category of left $R-$module, and $\mathcal{Mod} - \mathcal{R}$ category of right $R-$module.
- We denote $\mathcal{Ab} = \mathbb{Z}-\mathcal{Mod}$ category of Abelian group.

Definition 12.1.1. We have

- $f \in \mathcal{C}(A, B)$ is a **monomorphism** if for all $X \in \mathcal{C}, \forall g_1 \neq g_2 \in \mathcal{C}(X, A)$, we have $fg_1 \neq fg_2$, that is

$$\begin{tikzcd} X \arrow[r, bend left, "g_1"] \arrow[r, bend right, "g_2"'] & A \arrow[r, "f"] & B \end{tikzcd}$$

(i.e., $fg_1 = fg_2$ implies $g_1 = g_2$ can simplify f on the left). We write $f : A \rightarrowtail B$ to indicate f is a monomorphism.

- $f \in \mathcal{C}(A, B)$ is an **epimorphism** if for any $X \in \mathcal{C}, \forall g_1 \neq g_2 \in \mathcal{C}(B, X), g_1 f \neq g_2 f$. We write $f : A \twoheadrightarrow B$, that is,

$$\begin{tikzcd} A \arrow[r, "f"] & B \arrow[r, bend left, "g_1"] \arrow[r, bend right, "g_2"'] & X \end{tikzcd}.$$

Example 12.1.2. In $\mathcal{Set}$ and in $\mathcal{R} - \mathcal{Mod}$, f is monomorphism if and only if f is injective. Also f is epimorphism if and only if f is surjective.

Notation: For $f \in \mathcal{C}(A, B)$, we denote $f_\# : g \mapsto fg$ where g is in $\mathcal{C}(X, A)$ and fg in $\mathcal{C}(X, B)$. Similarly we denote $_\# f : g \mapsto gf$ where the first g is in $\mathcal{C}(B, X)$ and gf in $\mathcal{C}(A, X)$.

Remark 12.1.3. We have f is monomorphism if and only if $f_\#$ is injective. And f is epimorphism if and only if $_\# f$ injective.

Remark 12.1.4. We have f is isomorphism implies that f is monomorphism and epimorphism (converse not always true).

Definition 12.1.5. An object $P \in \mathcal{C}$ is **projective** if it satisfies

$$\begin{tikzcd} P \arrow[d, dotted, "\exists g'"'] \arrow[dr, "\forall g"] & \\ A \arrow[r, two heads, "h"'] & B \end{tikzcd}$$

and for all $A, B \in \mathcal{C}, \forall g : P \to B, \forall h : A \twoheadrightarrow B$, there is $g' : P \to A$ such that $hg' = g$.

Similarly, an object $E \in \mathcal{C}$ is **injective** if it satisfies

$$\begin{tikzcd} A \arrow[r, tail, "h"] \arrow[dr, "g"'] & B \arrow[d, dotted, "\exists g'"] \\ & E \end{tikzcd}.$$

12.2 Additive Categories

Definition 12.2.1. An **additive category** is a category $\mathcal{C}$ such that for any $A, B \in \mathcal{C}$, $\mathcal{C}(A, B)$ is an additive group and we have the following:

(1). Operation is biadditive $(f_1 + f_2)g = f_1 g + f_2 g$ and $g(f_1 + f_2) = gf_1 + gf_2$.

(2). The category $\mathcal{C}$ has a zero object $0_{\mathcal{C}}$.

(3). Any finite tuple of objects $A_1, \cdots, A_n$ have a product. That is, $\prod_{i=1}^n A_i$ and a coproduct $\coprod_{i=1}^n A_i$.

Lemma 12.2.2. *In $\mathcal{C}$ additive category, we have $\prod_{i=1}^n A_i \simeq \coprod_{i=1}^n A_i$.*

Example 12.2.3. Some examples of additive category:

- $\mathcal{R} - \mathcal{M}od, \mathcal{M}od - \mathcal{R}$.
- $\mathcal{R} - mod, mod - \mathcal{R}$, the category of finitely generated $R-$module.

Definition 12.2.4. Let $f \in \mathcal{C}(A, B)$, a **kernel** of f is $K \in \mathcal{C}$ and $q \in \mathcal{C}(K, A)$ such that

(1). we have $fq = 0$, and

(2). for any $X \in \mathcal{C}$, for any $g \in \mathcal{C}(X, A)$ such that $fg = 0$, there exists $\widetilde{g}$ such that $g = q\widetilde{g}$. We have the diagram

$$\begin{tikzcd} & X \arrow[dl, dotted, "\exists \widetilde{g}"'] \arrow[d, "\forall g"'] \arrow[dr, "0"] & \\ K \arrow[r, "q"] & A \arrow[r, "f"] & B \end{tikzcd}$$

commutes.

Example 12.2.5. In $\mathcal{R} - \mathcal{M}od$, and f as $R-$module homomorphism, let $K = \{a \in A | f(a) = 0\}$, and

$$q : K \longrightarrow A,$$

$$a \longmapsto a.$$

Then (K, q) is the kernel of f in $\mathcal{R} - \mathcal{M}od$.

Lemma 12.2.6. *When f has a kernel, they are unique up to $\mathcal{C}-$isomorphism, that is, we have K, q kernel if the diagram*

$$\begin{tikzcd} \forall X \arrow[r, dotted, "\exists !"] \arrow[d, "g"'] \arrow[dr, "0"] & K \arrow[d] \\ A \arrow[r, "f"'] & B \end{tikzcd}$$

commutes.

Remark 12.2.7. Let $\mathcal{C}$ be additive category and let $f \in \mathcal{C}(A, B)$, for any $X \in \mathcal{C}$, the map

$$f_{\#} : \mathcal{C}(X, A) \longrightarrow \mathcal{C}(X, B),$$
$$g \longmapsto fg,$$

is homomorphism of additive group. Its kernel (in group sense) is $\ker(f_{\#}) = \{g | fg = 0\}$.

Lemma 12.2.8. *Let $\mathcal{C}$ be additive category and $f \in \mathcal{C}(A, B)$, then (K, q) is the kernel of f if and only if for any $X \in \mathcal{C}$, we have*

- $\mathrm{Im}(q_{\#}) = \ker(f_{\#})(\exists\widetilde{g})$,
- $q_{\#}$ *injective* $(\exists!\widetilde{g})$.

That is, we have the diagram

$$\begin{tikzcd} & X \arrow[dl, dotted, "\exists!\widetilde{g}"'] \arrow[d, "\forall g"'] \arrow[dr, "0"] & \\ K \arrow[r, "q"'] & A \arrow[r, "f"'] & B \end{tikzcd}$$

commutes if and only if for any $X \in \mathcal{C}$, we have $0 \longrightarrow \mathcal{C}(X, K) \xrightarrow{q_{\#}} \mathcal{C}(X, A) \xrightarrow{f_{\#}} \mathcal{C}(X, B)$ is exact sequence of additive group.

Corollary 12.2.9. *A $\mathcal{C}-$morphism f is a monomorphism if and only if $(0, 0)$ is the kernel of f.*

Proof. We have f monomorphism if and only if $f_{\#}$ is injective if and only if $\ker(f_{\#}) = 0$.

$(\Longleftarrow)$: if $(0, 0)$ is a kernel of f, then $\ker(f_{\#}) = \mathrm{Im}(0_{\#}) = 0$, hence f is monomorphism.

$(\Longrightarrow)$: If f is monomorphism, then $\ker(f_{\#}) = 0$ implies that $q = 0_{\mathcal{C}(0,A)}$ satisfies

- $\mathrm{Im}(q_{\#}) = 0 = \ker(f_{\#})$,
- $q_{\#}$ is injective (since $\mathcal{C}(X, 0) = \{0\}$).

Hence the corollary. □

Remark 12.2.10. If (K, q) is kernel of f then q is monomorphism (since $q_{\#}$ is injective).

Definition 12.2.11. A **cokernel** of $f \in \mathcal{C}(A, B)$ is $(C, p), C \in \mathcal{C}, p \in \mathcal{C}(B, C)$ such that

(1). $pf = 0$,

(2). for any $X \in \mathcal{C}, \forall g \in \mathcal{C}(B, X)$ such that $gf = 0$, there exists unique $\overline{g} : C \to X$ such that $g = p\overline{g}$, that is, the diagram

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "0"'] & B \arrow[r, "p"] \arrow[d, "\forall g"] & C \arrow[dl, dotted, "\exists! \overline{g}"] \\ & X & \end{tikzcd}$$

commutes.

Remark 12.2.12. In $\mathcal{R} - \mathcal{Mod}$, let $f \in \mathrm{Hom}(A, B)$, let $C = B/\mathrm{Im}(f), p : B \to C$ quotient map, then (C, p) is a cokernel of f in $\mathcal{R} - \mathcal{Mod}$. Indeed, if $gf = 0$, it means that $\mathrm{Im}(f) \subseteq \ker(g)$, and we can define

$$\overline{g} : C \longrightarrow X,$$

$$b + \mathrm{Im}(f) \longmapsto g(b),$$

and it is unique choice.

Lemma 12.2.13. *Cokernels are unique up to $\mathcal{C}-$isomorphism. Further, we have that (C, p) cokernel of f if and only if we have both*

- $\ker({}_{\#}f) = \mathrm{Im}({}_{\#}p)$*, and*
- ${}_{\#}p$ *is injective*

are satisfied, if and only if $\forall X \in \mathcal{C}$, we have $0 \to \mathcal{C}(C, X) \xrightarrow{\#p} \mathcal{C}(B, X) \xrightarrow{\#f} \mathcal{C}(A, X)$ is exact (recall that ${}_{\#}p : g \mapsto gp$).

Remark 12.2.14. If (C, p) is a cokernel then ${}_{\#}p$ is epimorphism.

12.3 Exact Sequences, Exact Functors

Definition 12.3.1. Let $\mathcal{C}$ be additive category, a **left exact sequence** in $\mathcal{C}$ is $0 \to A \xrightarrow{f} B \xrightarrow{g} C$ with (A, f) is kernel of g.

Similarly, a **right exact sequence** in $\mathcal{C}$ is $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ with (C, g) is cokernel of g.

Further, a **short exact sequence** in $\mathcal{C}$ is $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, with (A, f) is kernel of g and (C, g) cokernel of f.

Remark 12.3.2. Match the classical definitions in $\mathcal{R} - \mathcal{Mod}$.

Definition 12.3.3. Let $\mathcal{C}, \mathcal{D}$ be additive categories, a covariant or contravariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is **left exact** if $\mathcal{F}(\mathscr{shortexact})$ is left exact.

Similarly, a covariant or contravariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is **right exact** if $\mathcal{F}(\mathscr{shortexact})$ is right exact.

Further, we say a covariant or contravariant functor $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ is **exact** if $\mathcal{F}(\mathscr{shortexact})$ is short exact.

Explicitly, functor $\mathcal{F}$ covariant left exact if $0 \to A \to B \to C \to 0$ exact implies that $0 \to \mathcal{F}A \to \mathcal{F}B \to \mathcal{F}C$ exact. Functor $\mathcal{F}$ contravariant left exact if $0 \to A \to B \to C \to 0$ exact implies that $0 \to \mathcal{F}C \to \mathcal{F}B \to \mathcal{F}A$ exact.

Definition 12.3.4. Let $\mathcal{C}$ be additive category and let $X \in \mathcal{C}$, we define

- $\mathrm{Hom}_{\mathcal{C}}(X, -)$ to be the **covariant functor** $\mathcal{C} \to \mathcal{Ab}$ defined by

$$A \longmapsto \mathcal{C}(X, A),$$

$$f \in \mathcal{C}(A, B) \longmapsto f_{\#} : \mathcal{C}(X, A) \to \mathcal{C}(X, B).$$

- $\mathrm{Hom}_{\mathcal{C}}(-, X)$ to be the **contravariant functor** $\mathcal{C} \to \mathcal{Ab}$ defined by

$$A \longmapsto \mathcal{C}(A, X),$$

$$f \longmapsto_{\#} f.$$

Remark 12.3.5. By lemmas about kernel, cokernel, we use that $\mathrm{Hom}_{\mathcal{C}}(-, X)$ and $\mathrm{Hom}_{\mathcal{C}}(X, -)$ are left exact.

Proposition 12.3.6. *We have*

- *if $X \in \mathcal{C}$ is injective, then $\mathrm{Hom}_{\mathcal{C}}(-, X)$ exact.*
- *We have $X \in \mathcal{C}$ is projective implies that $\mathrm{Hom}_{\mathcal{C}}(X, -)$ exact.*

Proof. Homework. $\square$

13

Abelian Categories, Chains, and Homology

13.1 Abelian Categories

Definition 13.1.1. An additive category $\mathcal{C}$ is **abelian** if

(a). Every $\mathcal{C}-$morphism has a kernel and a cokernel.

(b). If $f \in \mathcal{C}(A, B)$ is monomorphism and $g \in \mathcal{C}(B, C)$ is epimorphism, then (A, f) is a kernel of g if and only if (C, g) is cokernel of f (in this case $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact).

(c). Every $\mathcal{C}-$morphism f can be factored as $f = f'f''$ with f'' epimorphism and f' monomorphism, that is, we have the diagram

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, two heads, "f''"'] & & B \\ & X \arrow[ur, tail, "f'"'] & \end{tikzcd}$$

commutes.

Lemma 13.1.2. *Let $\mathcal{C}$ abelian category, let $f \in \mathcal{C}(A, B)$, suppose $f = f'f''$ where f' monomorphism and f'' epimorphism, then*

(a). We have (K, q) is kernel of f if and only if (K, q) is kernel of f''. In this case $0 \to K \xrightarrow{q} A \xrightarrow{f''} X \to 0$ exact.

(b). We have (C, p) is cokernel of f if and only of (C, p) cokernel of f'. In this case $0 \to X \xrightarrow{f'} B \xrightarrow{p} C \to 0$ is exact.

Proof of Part (a). Since f' monomorphism, we have $f''g = 0$ if and only if $fg = 0$. Also (K, q) kernel of f if and only if $(fg = 0 \implies \exists!\widetilde{g}, g = q\widetilde{g})$ if and only if $(f''g = 0 \implies \exists!\widetilde{g}, g = q\widetilde{g})$ if and only if (K, q) kernel of f''. □

Definition 13.1.3. Let $\mathcal{C}$ abelian category and let $f \in \mathcal{C}(A, B)$. If

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, two heads, "f''"'] & & B \\ & X \arrow[ur, "f'"'] & \end{tikzcd}$$

commutes, then we call X an **image** of f and write $X = \mathrm{Im}(f)$.

Lemma 13.1.4. *Let $\mathcal{C}$ be abelian category, the image $\mathrm{Im}(f)$ is unique up to $\mathcal{C}-$isomorphism. Moreover, $\mathrm{Im}(f) \simeq \mathrm{coker}(\ker(f)) \simeq \ker(\mathrm{coker}(f))$.*

Proof. Suppose

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, two heads, "f''"'] & & B \\ & X \arrow[ur, "f'"'] & \end{tikzcd}$$

commutes, we need to show $X = \mathrm{coker}(\ker(f))$. Let (K, q) be a kernel of f, then $0 \to K \xrightarrow{q} A \xrightarrow{f'} X \to 0$ is exact, which implies that $X = \mathrm{coker}(q) = \mathrm{coker}(\ker(f))$. Same for other formula. □

13.2 Chains

Definition 13.2.1. Let $\mathcal{C}$ abelian category, a $\mathcal{C}-$**chain** is $C_* = (C_n)_{n \geqslant 0}, d_* = (d_n)_{n>0}$ where $d_n \in \mathcal{C}(C_n, C_{n-1}), d_{n+1}d_n = 0$. A **morphism of** $\mathcal{C}-$**chains** from C_* to C'_* is $f_* = (f_n)_{n \geqslant 0}$ and $f_n \in \mathcal{C}(C_n, C'_n)$ such that $f_{n-1}d_n = d'_n f_n$.

Remark 13.2.2. We have $\mathcal{C}-$chains and their morphisms form a category denoted $\mathcal{C} - \boldsymbol{\mathcal{chain}}$.

Proposition 13.2.3. *We have that $\mathcal{C}$ additive category then $\mathcal{C} - \boldsymbol{\mathcal{chain}}$ is additive category. Similarly, $\mathcal{C}$ abelian category implies $\mathcal{C} - \boldsymbol{\mathcal{chain}}$ abelian category.*

Proof. We have

- $f_* + g_* = (f_n + g_n)$, and

- Direct sum of chains? We have $C_* \oplus C'_* = (C_n \oplus C'_n)$ defined by

$$\begin{tikzcd} C_n \oplus C'_n \arrow[rr, "d_n \oplus d'_n"] \arrow[dr, "d_n p_n"] \arrow[ddr, "d'_n p'_n"'] & & C_{n-1} \oplus C'_{n-1} \\ & C_{n-1} \arrow[ur, "q_n"] & \\ & C'_{n-1} \arrow[uur, "q'_n"'] & \end{tikzcd}$$

component wise and commutes. Exercise: Show that this is a direct sum in $\mathcal{C} - \boldsymbol{chain}$.

- Kernels? Let $f_* : C_* \to C'_*$, we have

$$\begin{tikzcd} \ker(f_n) \arrow[r, "q_n"] \arrow[d, dotted, "\exists! \alpha_n"'] & C_n \arrow[r, "f_n"] \arrow[d, "d_n"] & C'_n \arrow[d, "d'_n"] \\ \ker(f_{n-1}) \arrow[r, "q_{n-1}"] & C_{n-1} \arrow[r, "f_{n-1}"] & C'_{n-1} \end{tikzcd}$$

commutes and $(\ker(f_n), (\alpha_n))$ is kernel of f_*.

- Cokernels, factorization, etc...

Hence the result. $\square$

Definition 13.2.4 (Homology)**.** Let $\mathcal{C}$ be an abelian category, let C_*, d_* be a $\mathcal{C} - \boldsymbol{chain}$, let (Z_n, q_n) be kernel of d_n, then (since $d_n d_{n+1} = 0$), there exists unique $\widetilde{d_{n+1}}$ such that

$$\begin{tikzcd} C_{n+1} \arrow[rr, "d_{n+1}"] \arrow[dr, dotted, "\widetilde{d_{n+1}}"'] & & C_n \\ & Z_n \arrow[ur, tail, "q_n"'] \arrow[d, two heads, "p_n"] & \\ & H_n(C_*) & \end{tikzcd}$$

commutes. We define the **homology** $H_n(C_*) = \operatorname{coker}(\widetilde{d_{n+1}})$.

Example 13.2.5. In $\mathcal{R} - \boldsymbol{Mod}$, we have

$$\widetilde{d_{n+1}} : C_{n+1} \longrightarrow Z_n = \ker(d_n)$$
$$x \longmapsto d_{n+1}(x).$$

Then $H_n = \operatorname{coker}(\widetilde{d_{n+1}}) = \ker(d_n)/\operatorname{Im}(d_{n+1})$.

Lemma 13.2.6. *We have $H_n(C_*)$ unique up to isomorphism.*

Definition 13.2.7. Let $f_* : C_* \to C'_*$ be morphism of $\mathcal{C} - \boldsymbol{chain}$, then we have

- there exists unique $\widetilde{f_n}$ such that

$$\begin{tikzcd}
C_{n+1} \arrow[rr, "d_{n+1}"] \arrow[dr, "\widetilde{d_{n+1}}"] \arrow[ddd, "f_{n+1}"'] & & C_n \arrow[ddd, "f_n"] \\
& Z_n \arrow[ur, "q_n"] \arrow[d, "\widetilde{f_n}"] & \\
& Z'_n \arrow[dr, "q'_n"] & \\
C'_{n+1} \arrow[ur] \arrow[rr] & & C'_n
\end{tikzcd}$$

commutes by definition of (Z'_n, q'_n) the kernel of d'_n.

- There exists $\overline{f_n}$ such that

$$\begin{tikzcd}
C_{n+1} \arrow[r, "\widetilde{d_{n+1}}"] \arrow[d, "f_{n+1}"'] & Z_n \arrow[r, "p_n"] \arrow[d, "\widetilde{f_n}"] & H_n(C_*) \arrow[d, "\exists ! \overline{f_n}"] \\
C'_{n+1} \arrow[r] & Z'_n \arrow[r] & H_n(C'_*)
\end{tikzcd}$$

commutes. We define $H_n(f_*) = \overline{f_n}$.

Lemma 13.2.8. *For any n, we have H_n is a functor from $\mathcal{C} - \boldsymbol{chain}$ to $\mathcal{C}$ such that $[H_n(f_*g_*) = H_n(f_*)H_n(g_*), H_n(\mathrm{Id}_*) = \mathrm{Id}]$ which is addtive, that is, $H_n(f_* + g_*) = H_n(f_*) + H_n(g_*)$.*

13.3 Dually, Cochain, etc

Definition 13.3.1. We define

- A $\mathcal{C} - \boldsymbol{cochain}$ is $C_0 \xrightarrow{d_1} C_1 \xrightarrow{d_2} C_2 \longrightarrow \cdots$ such that $d^2 = 0$.
- A **morphism** of $\mathcal{C} - \boldsymbol{cochain}$ is (f_n) such that $fd = d'f$.

- For (C_*, d_*) cochain, there exists $\widetilde{d_{n+1}}$ such that

$$\begin{tikzcd}
C_n \arrow[rr, "d_{n+1}"] \arrow[dr, "p_n"'] & & C_{n+1} \\
& \operatorname{coker}(d_n) \arrow[ur, "\widetilde{d_{n+1}}"'] &
\end{tikzcd}$$

  commutes. We say the **cohomology** $H^n(C_*) = \ker(\widetilde{d_{n+1}})$.

Example 13.3.2. In $\mathscr{R} - \mathcal{Mod}$, we have $\operatorname{coker}(d_n) = C_n/\operatorname{Im}(d_n)$. Here $\widetilde{d_{n+1}} : x + \operatorname{Im}(d_n) \to d_{n+1}(x)$. Then $H^n(C_*) = \ker(\widetilde{d_{n+1}}) = \ker(d_{n+1})/\operatorname{Im}(d_n)$.

Definition 13.3.3 (Homotopy)**.** We say chain morphisms $f_*, g_* : C_* \to C'_*$ are **homotopy equivalent** if there exists $(h_n)_{n \geqslant 0}$ in $\mathcal{C}(C_n, C'_{n+1})$ such that $f_n - g_n = h_{n-1}d_n + d'_{n+1}h_n$. That is, we have

$$\begin{tikzcd}
C_{n+1} \arrow[r, "d_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[dl, "h_n"'] \arrow[d, shift right, "f_n"'] \arrow[d, shift left, "g_n"] & C_{n-1} \arrow[dl, "h_{n-1}"] \\
C'_{n+1} \arrow[r, "d'_{n+1}"] & C'_n \arrow[r, "d'_n"] & C'_{n-1}
\end{tikzcd}$$

commutes. We denote $f_* \underset{h}{\simeq} g_*$.

Lemma 13.3.4. *If $f_* \underset{h}{\simeq} g_*$ then $H_n(f_*) = H_n(g_*)$.*

Proof. We have H_n is additive, hence we have $H_n(f_*) - H_n(g_*) = H_n(\delta_n)$ where $\delta_n = h_{n-1}d_n + d'_{n+1}h_n$. Want to show $H_n(\delta_n) = 0$. We have the diagram

$$\begin{tikzcd}
\cdots \arrow[r, "\widetilde{d_{n+1}}"] & Z_n \arrow[r, "p_n"] \arrow[d, "\widetilde{\delta_n}"] & H_n(C_*) \arrow[d, "\overline{\delta_n} = H_n(\delta_*)"] \\
\cdots \arrow[r, "\widetilde{d_{n+1}}'"'] & Z'_n \arrow[r, "p'_n"'] & H_n(C'_*)
\end{tikzcd}$$

and it suffices to show $p'_n\widetilde{\delta_n} = 0$. From the diagram

$$\begin{tikzcd}
C_{n+1} \arrow[rr, "d_{n+1}"] \arrow[dr, "\widetilde{d_{n+1}}"] \arrow[ddd, "\delta_{n+1}"'] & & C_n \arrow[ddd, "\delta_n"] \\
& Z_n \arrow[ur, "q_n"] \arrow[d, "\widetilde{\delta_n}"] & \\
& Z'_n \arrow[dr, "q'_n"] & \\
C'_{n+1} \arrow[ur] \arrow[rr] & & C'_n
\end{tikzcd}$$

we have $q'_n\widetilde{\delta_n} = \delta_n q_n = (f_{n-1}d_n + d'_{n+1}h_n)q_n = d'_{n+1}h_nq_n = q'_n\widetilde{d'_{n+1}}h_nq_n$. Since q'_n is monomorphism, we have that $\widetilde{\delta_n} = \widetilde{d_{n+1}}h_nq_n$. Hence $p'_n\widetilde{\delta_n} = p'_n\widetilde{d_{n+1}}h_nq_n = 0$ since $p'_n\widetilde{d_{n+1}} = 0$. $\square$

Corollary 13.3.5. *If C_*, C'_* are homotopy equivalent $\mathcal{C} - \boldsymbol{chain}$ (that is, there exists $f_* : C_* \to C'_*, g_* : C'_* \to C_*$ such that $f_*g_* = \mathrm{Id}, g_*f_* = \mathrm{Id}$), then $H_n(C_*) \simeq H_n(C'_*)$ in $\mathcal{C}$.*

14

Derived Functors

14.1 Projective Resolutions, Injective Coresolutions

Definition 14.1.1. Let $\mathcal{C}$ be abelian category, a sequence of $\mathcal{C}-$morphism $(f_n)_{a\leqslant n\leqslant b}$ is **exact** if there exists p_n monomorphism, q_n epimorphism such that $f_n = q_n p_n$, and we have the diagram

$$\begin{tikzcd} A_n \arrow[rr, "f_n"] \arrow[dr, two heads, "p_n"'] & & A_{n+1} \\ & X_n \arrow[ur, tail, "q_n"'] & \end{tikzcd}$$

commutes and

$$0 \longrightarrow X_n \xrightarrow{q_n} A_{n+1} \xrightarrow{p_{n+1}} X_{n+1} \longrightarrow 0$$

short exact.

Remark 14.1.2. The sequence (f_n) exact if $\operatorname{Im}(f_n) = \ker(f_{n+1})$ for any $a \leqslant n \leqslant b$, where $\operatorname{Im}(f_n) = (X_n, p_n)$ by abuse of notation.

Definition 14.1.3. A **projective resolution** of $A \in \mathcal{C}$ is C_*, d_* such that

$$\cdots \longrightarrow C_1 \xrightarrow{d_1} C_0 \xrightarrow{d_0} A \longrightarrow 0$$

exact and C_n projective for any n.

Definition 14.1.4. We say that $\mathcal{C}$ has "**enough projective**" if for any $X \in \mathcal{C}$, there is $P \in \mathcal{C}$ projective and $f : P \twoheadrightarrow X$ epimorphism.

Lemma 14.1.5. *If $\mathcal{C}$ has enough projective then any object has a projective resolution.*

Proof. Consider the diagram

$$\begin{tikzcd} \cdots \arrow[r] & C_1 \arrow[rr, dotted] \arrow[dr, two heads] & & C_0 \arrow[r, two heads, "d_0"] & A \\ & & \ker(d_0) \arrow[ur, tail] & & \end{tikzcd}$$

etc... □

Proposition 14.1.6. *We have*

- *If $C_* \to A, C'_* \to A'$ are projective resolution, then any $f \in \mathcal{C}(A, A')$ can be lifted to a chain map $f_* : C_* \to C'_*$ such that*

$$\begin{tikzcd} C_1 \arrow[r] \arrow[d, "f_1"] & C_0 \arrow[r] \arrow[d, "f_0"] & A \arrow[d, "f"] \\ C'_1 \arrow[r] & C'_0 \arrow[r] & A' \end{tikzcd}$$

  commutes.

- *Projective resolution are unique up to homotopy.*

Proof. "Same" as in $\mathcal{R} - \mathcal{Mod}$. □

Then we define things dually:

Definition 14.1.7. An **injective coresolution** for $A \in \mathcal{C}$ is

$$0 \longrightarrow A \xrightarrow{d_0} C_0 \xrightarrow{d_1} C_1 \longrightarrow \cdots$$

exact with C_i injective.

Definition 14.1.8. We say $\mathcal{C}$ has "**enough injective**" if for any $X \in \mathcal{C}$, we have $X \rightarrowtail E$ injective object.

Theorem 14.1.9. *If $\mathcal{C}$ has enough injective, then any object has a injective coresolution and it is unique up to homotopy. Moreover, any $\mathcal{C}$−morphism can be lifted to a cochain map between the injective coresolutions (lift is unique up to homotopy).*

Definition 14.1.10. Let $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ be additive functor between abelian categories, $\mathcal{F}$ either left or right exact. If $\mathcal{F}$ is right (resp. left) exact we define the **left (resp.**

right) derivative $L^n\mathcal{F}$(resp. $R^n\mathcal{F}$) : $\mathcal{C} \to \mathcal{D}$ as follows

Derivative		
$\mathcal{F}$	covariant	contravariant
right exact	$L^n\mathcal{F}(A) = H_n(\mathcal{F}P_*)$, and $P_* \to A$ projective resolutions of A.	$L^n\mathcal{F}(A) = H^n(\mathcal{F}E_*)$, and $A \to E_*$ injective coresolutions of A.
left exact	$R^n\mathcal{F}(A) = H^n(\mathcal{F}E_*)$, and $A \to E_*$ injective coresolutions of A.	$R^n\mathcal{F}(A) = H_n(\mathcal{F}P_*)$, and $P_* \to A$ projective resolutions of A.

More precisely, for F covariant right exact

- for any $A \in \mathcal{C}$, we have $L^n(\mathcal{F}(A)) = H_n(FP_*)$ where $\cdots \xrightarrow{dz} P_1 \xrightarrow{d_1} P_0 \longrightarrow A \longrightarrow 0$ is projective resolution, and FP_* is the $\mathcal{D}-$chain $\cdots \xrightarrow{\mathcal{F}dz} \mathcal{F}P_1 \xrightarrow{\mathcal{F}d_1} \mathcal{F}P_0$.
- For any $f \in \mathcal{C}(A, B)$, we have $L^n(\mathcal{F}(f)) = H_n(\mathcal{F}f_*)$ where f_* is a lift of f between projective resolution $P_* \to A$ and $P'_* \to B$ and $\mathcal{F}(f_*) = (\mathcal{F}f_n)_{n\geqslant 0}$ is the corresponding $\mathcal{D}-$chain morphism between $\mathcal{F}P_*$ and $\mathcal{F}P'_*$.

Remark 14.1.11. Derivatives are only defined if $\mathcal{C}$ has enough injective or projective (depending on the case).

Lemma 14.1.12. *Derivatives are well-defined up to $\mathcal{D}-$isomorphism and $L^0\mathcal{F} = \mathcal{F}$ for $\mathcal{F}$ right exact, and $R^0\mathcal{F} = \mathcal{F}$ for $\mathcal{F}$ left exact.*

Proof. For $\mathcal{F}$ covariant right exact,

- let $A \in \mathcal{C}$ and P_*, P'_* be projective resolution of A by previous theorem, $P_* \underset{h}{\simeq} P'_*$ for some homotopy h. Then $\mathcal{F}$ additive implies that $\mathcal{F}P_* \simeq \mathcal{F}P'_*$ implies $H_n(\mathcal{F}P_*) \simeq H_n(\mathcal{F}P'_*)$ (we have $f_*g_* \underset{h}{\simeq} \mathrm{Id}$ implies that $\mathcal{F}(f_*)\mathcal{F}(g_*) \underset{\mathcal{F}h}{\simeq} \mathrm{Id}$).
- For $f \in \mathcal{C}(A, B)$, let f_*, f'_* be lifts of f, by theorem $f_* \underset{h}{\simeq} f'_*$ we have $\mathcal{F}(f_*) \underset{\mathcal{F}h}{\simeq} \mathcal{F}(f'_*)$. This implies that $H_n(f_*) = H_n(f'_*)$.
- We have $L^0\mathcal{F}(A) = H_0(\mathcal{F}P_*)$ for $P_* \to A$ projective resolutions of A. Then $\mathcal{F}$ right exact and $P_* \to A \to 0$ exact which implies that $\mathcal{F}P_1 \xrightarrow{\mathcal{F}d_1} \mathcal{F}P_0 \xrightarrow{\mathcal{F}d_0} \mathcal{F}A \longrightarrow 0$ exact. Thus $\operatorname{coker}(\mathcal{F}d_1) = \mathcal{F}A$.

$\square$

14.2 Long Exact Sequences

Theorem 14.2.1 (Snake Lemma). *Let $\mathcal{C}$ be an additive category, suppose $\mathcal{C}-$diagram*

$$\begin{tikzcd}
 & A' \arrow[r] \arrow[d, "d'"] & A \arrow[r] \arrow[d, "d"] & A'' \arrow[r] \arrow[d, "d''"] & 0 \\
0 \arrow[r] & B' \arrow[r] & B \arrow[r] & B'' &
\end{tikzcd}$$

commutes and is row exact. Let $(K, q), (K', q'), (K'', q'')$ kernels of d, d', d'' and $(C, p), (C', p'), (C'', p'')$ cokernels, then there is $\alpha, \beta, \alpha', \beta', \delta$, such that

$$\begin{tikzcd}
K' \arrow[r, "\alpha"] \arrow[d] & K \arrow[r, "\beta"] \arrow[d] & K'' \arrow[d] \arrow[dddll, rounded corners, "\delta"] \\
A' \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A'' \arrow[d] \\
B' \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & B'' \arrow[d] \\
C' \arrow[r, "\alpha'"] & C \arrow[r, "\beta'"] & C''
\end{tikzcd}$$

(the diagram borrows from here) commutes and

$$K' \xrightarrow{\alpha} K \xrightarrow{\beta} K'' \xrightarrow{\delta} C' \xrightarrow{\alpha'} C \xrightarrow{\beta'} C''$$

is exact.

Theorem 14.2.2. *Let $\mathcal{C}$ be abelian category, if $0 \to A_* \to B_* \to C_* \to 0$ is exact sequence of $\mathcal{C}-$chains, then there exists $(\delta_n)_{n>0}$ such that*

$$\cdots \to H_n(A_*) \to H_n(B_*) \longrightarrow H_n(C_*) \xrightarrow{\delta_n} H_{n-1}(A_*) \to H_{n-1}(B_*) \to \cdots$$

is exact.

Lemma 14.2.3. *Alternative definition of $H_n(C_*)$ for C_* a $\mathcal{C}-$chain is*

$$\begin{tikzcd}
C_n \arrow[rr, "d_n"] \arrow[dr] & & C_{n-1} \arrow[r, "d_{n-1}"] & {} \\
 & \operatorname{coker}(d_{n+1}) \arrow[r, "\exists \overline{d_n}"] & \ker(d_{n-1}) \arrow[u] &
\end{tikzcd}$$

and $H_{n-1} = \operatorname{coker}(\overline{d_n})$ *(easy to see from definition of* H_n*). Also* $H_n = \ker(d_n)$ *(not obvious it coincide with definition of* H_n*).*

Example 14.2.4. Check this in $\mathcal{R} - \mathcal{Mod}$.

Proof of Theorem 14.2.2. Let $n > 0$, then

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d_n} & & \downarrow{\scriptstyle d_n} & & \\ 0 & \longrightarrow & A_{n-1} & \longrightarrow & B_{n-1} & \longrightarrow & C_{n-1} & \longrightarrow & 0 \end{array}$$

commutes and row exact. By snake lemma, we have

$$0 \longrightarrow \ker(d_n^A) \longrightarrow \ker(d_n^B) \longrightarrow \ker(d_n^C)$$

is exact and

$$\operatorname{coker}(d_n^A) \longrightarrow \operatorname{coker}(d_n^B) \longrightarrow \operatorname{coker}(d_n^C) \longrightarrow 0$$

is exact implies that

$$\begin{array}{ccccc} \operatorname{coker}(d_{n+1}^A) & \longrightarrow & \operatorname{coker}(d_{n+1}^B) & \longrightarrow & \operatorname{coker}(d_{n+1}^C) \\ \downarrow{\scriptstyle \overline{d_n}} & & \downarrow{\scriptstyle \overline{d_n}} & & \downarrow{\scriptstyle \overline{d_n}} \\ \ker(d_{n-1}^A) & \longrightarrow & \ker(d_{n-1}^B) & \longrightarrow & \ker(d_{n-1}^C) \end{array}$$

commutes. Hence snake goes through H_n:

$$H_n(A) \longrightarrow H_n(B) \longrightarrow H_n(C) \xrightarrow{\delta} H_{n-1}(A) \longrightarrow H_{n-1}(B) \longrightarrow H_n(C).$$

Same story for cohomology. $\square$

Theorem 14.2.5. *Let* $\mathcal{C}, \mathcal{D}$ *be abelian categories, let* $\mathcal{F} : \mathcal{C} \to \mathcal{D}$ *be left or right exact additive functors, let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be short exact in $\mathcal{C}$*, then there is long exact sequence in* $\mathcal{D}$*, such that*

- *for* $\mathcal{F}$ *covariant right exact*

$$\cdots \xrightarrow{\delta} L^1(\mathcal{F}A) \longrightarrow L^1\mathcal{F}B \longrightarrow L^1\mathcal{F}C \xrightarrow{\delta_1} \mathcal{F}A \xrightarrow{\mathcal{F}f} \mathcal{F}B \xrightarrow{\mathcal{F}g} \mathcal{F}C \longrightarrow 0$$

  exact.

- *For $\mathcal{F}$ covariant left exact,*

$$0 \longrightarrow \mathcal{F}A \longrightarrow \mathcal{F}B \longrightarrow \mathcal{F}C \xrightarrow{\delta} R^1\mathcal{F}A$$

  exact.

- *For $\mathcal{F}$ contravariant right exact,*

$$\cdots \longrightarrow L^1\mathcal{F}A \xrightarrow{\delta_1} \mathcal{F}C \longrightarrow \mathcal{F}B \longrightarrow \mathcal{F}A \longrightarrow 0$$

  exact.

Proof for $\mathcal{F}$ covariant right exact. Claim 1: there is projective resolutions $P'_* \to A, P_* \to B, P''_* \to C$ and chain maps f_*, g_* lifting f and g and such that

$$\cdots \to 0 \to P'_* \xrightarrow{f_*} P_* \xrightarrow{g_*} P''_* \to 0$$

is exact.

Claim 2: The sequence $0 \to \mathcal{F}P'_* \to \mathcal{F}P_* \to \mathcal{F}P''_* \to 0$ is exact. Then can apply the long exact sequence of homology on this $\mathcal{D}-$chain which gives the result. $\square$

Proof of Claim 1 (Horseshoe lemma). We have the diagram

$$\begin{tikzcd}
 & P'_1 \arrow[d, "d'_1"'] & & P''_1 \arrow[d, "d''_1"] & \\
 & P'_0 \arrow[d, "d'_0"'] & & P''_0 \arrow[d, "d''_0"] & \\
 {} \arrow[r, tail] & A \arrow[r, "f"'] & B \arrow[r, "g"'] & C \arrow[r] & 0
\end{tikzcd}.$$

Let $P'_n \to A$ be projective resolution of A and $P''_n \to C$ be projective resolution of C. Let $P_n = P'_n \oplus P''_n$. Let $p'_n : P_n \to P'_n, p''_n : P_n \to P''_n$ be projection: (P_n, p'_n, p''_n) is product of P'_n, P''_n via $\mathcal{C}$. Let $q'_n : P'_n \to P_n, q''_n : P''_n \to P_n$ be embedding: (P_n, q'_n, q''_n) is coproduct.

We can choose them such that $p'_n q'_n = \mathrm{Id}_{P'_n}, p''_n q'_n = 0, p'_n q''_n = 0, p''_n q''_n = \mathrm{Id}, q'_n p'_n + q''_n p''_n = \mathrm{Id}_{P_n}$. Then d_0 :

$$\begin{tikzcd}
P'_0 \arrow[r, "q'_0"] \arrow[d, two heads, "d'_0"'] \arrow[dr, "f d'_0"'] & P_0 \arrow[r, "p''_0"] \arrow[d, dotted, "d_0?"] & P''_0 \arrow[d, two heads, "d''_0"] \arrow[dl, "h"] \\
A \arrow[r, "f"'] & B \arrow[r, "g"'] & C
\end{tikzcd}$$

We have g epimorphism, p_0'' projective implies that there is $h, gh = d_0''$. Let $d_0 = fd_0'p_0' + hp_0''$. It commutes and d_0 is epimorphism (check).

How about d_1? We have d_0, d_0', d_0'' are epimorphism, then snake lemma implies

$$\begin{tikzcd}
0 \arrow[r] & \ker(d_0') \arrow[r] \arrow[d] & \ker(d_0) \arrow[r] \arrow[d] & \ker(d_0'') \arrow[r] \arrow[d] & 0 \\
& P_0' \arrow[r, "q_0'"'] & P_0 & P_0'' &
\end{tikzcd}$$

exact. Hence we have same situation as for d_0:

$$\begin{tikzcd}
0 \arrow[r] & P_1' \arrow[r] \arrow[d, two heads] & P_1 \arrow[r] \arrow[d, dotted, "?"] & P_1'' \arrow[r] \arrow[d, two heads] & 0 \\
& \ker(d_0') \arrow[r] & \ker(d_0) \arrow[r] & \ker(d_0'') &
\end{tikzcd}.$$

Then left for homework that $\mathcal{F}(P_n' \oplus P_n'') = \mathcal{F}(P_n') \oplus \mathcal{F}(P_n'')$ implies that

$$0 \longrightarrow \mathcal{F}P_n \longrightarrow \mathcal{F}P_n \longrightarrow \mathcal{F}P_n'' \longrightarrow 0$$

is exact. $\square$

14.3 Tor Functors

Definition 14.3.1. Let R be commutative ring, let A be $R-$module, let $\mathcal{F}_A = A\otimes - : \mathcal{R}-\mathcal{M}od \to \mathcal{R}-\mathcal{M}od$ defined by

$$\forall B \in \mathcal{R}-\mathcal{M}od, \mathcal{F}_A(B) = A \otimes B,$$

$$\forall f \in \mathcal{R}-\mathcal{M}od \text{ homomorphism}, \mathcal{F}_A(f) = \mathrm{Id}_A \otimes f.$$

Say $\mathcal{F}_A$ covariant additive functor, we have seen before that $\mathcal{F}_A$ is right exact, then

$$\mathrm{Tor}_n(A, B) = L^n\mathcal{F}_A(B) = H_n(A \otimes P_*)$$

where the last term is from $\mathcal{F}_A(P_*)$, where $P_* \to B \to 0$ is projective resolution for B. In other words, $\mathrm{Tor}_n(A, B) = \ker(\mathrm{Id}_A \otimes d_n^B)/\mathrm{Im}(\mathrm{Id}_A \otimes d_{n+1}^B)$ where $\cdots \to P_1 \xrightarrow{d_1} P_0 \to B \to 0$.

Example 14.3.2. Let $R = \mathbb{Z}$, A a $\mathbb{Z}-$module (additive group) and $B = \mathbb{Z}/n\mathbb{Z}$, then $\mathrm{Tor}_n(A, B) = \ker(\mathrm{Id}_A \otimes d_n)/\mathrm{Im}(\mathrm{Id}_A \otimes d_{n+1})$. Take P_* to be $0 \to \mathbb{Z} \xrightarrow{d_1} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \to 0$ where $d_1(x) = nx$. Then

$$\mathrm{Tor}_0(A\mathbb{Z}/n\mathbb{Z}) = \ker(0)/\mathrm{Im}(\mathrm{Id}_A \otimes d_1) = A \otimes \mathbb{Z}/A \otimes n\mathbb{Z} \simeq A/nA(\simeq A \otimes \mathbb{Z}/n\mathbb{Z}).$$

Also

$$\mathrm{Tor}_1(A, \mathbb{Z}/n\mathbb{Z}) = \ker(\mathrm{Id}_A \otimes d_1)/0 \simeq \ker(\widetilde{d}_1)$$

by $A \otimes \mathbb{Z} \simeq A = \{a \in A | na = 0\}$ where $\widetilde{d}_1 : A \to A$ by $x \mapsto nx$. Further,

$$\mathrm{Tor}_n(A, \mathbb{Z}/n\mathbb{Z}) = 0, \forall n > 0.$$

Proposition 14.3.3. *We have* $\mathrm{Tor}_n(A, B) \simeq \mathrm{Tor}_n(B, A)$.

14.4 Ext Functors

Definition 14.4.1. Let $\mathcal{C}$ be abelian category and let $A \in \mathcal{C}$, the functor $\mathcal{F} = \mathrm{Hom}_{\mathcal{C}}(A, -) : \mathcal{C} \to \mathcal{Ab}$ is covariant additive and left exact and

$$\forall B \in \mathcal{C}, \mathcal{F}(B) = \mathcal{C}(A, B),$$

$$\forall f \in \mathcal{C}(B, B'), \mathcal{F}(f) = f_{\#}$$

where $f_{\#}$ is

$$\mathcal{C}(A, B) \to \mathcal{C}(A, B')$$

$$g \mapsto fg.$$

Then $\mathrm{Ext}_n(A, B) = R^n\mathcal{F}(B) = H^n(\mathcal{C}(A, B_*))$ where the last term is from $\mathcal{F}(B_*)$ where $0 \to B \to B_*$ injective coresolution of B. Explicitly, take

$$\begin{tikzcd}
0 \arrow[r] & B \arrow[r] & B_0 \arrow[r] & B_1 \arrow[r] & \cdots \arrow[r, "d_n"] & B_n \arrow[r, "d_{n+1}"] & {} \\
 & & & & & A \arrow[u, "g"'] \arrow[ul, "h"] &
\end{tikzcd},$$

for any $n \geqslant 0$, we have

$$\mathrm{Ext}_n(A, B) = \ker(d_{n+1}\#)/\mathrm{Im}(d_n\#)$$

$$= \{g \in \mathcal{C}(A, B_n) | d_{n+1}g = 0\}/\{d_nh | h \in \mathcal{C}(A, B_{n-1})\}.$$

Remark 14.4.2. Let $B \in \mathcal{C}$, $\widetilde{F} = \mathrm{Hom}_{\mathcal{C}}(-,B) : \mathcal{C} \to \mathcal{Ab}$ contravariant left exact. By definition, $R^n\widetilde{F}(A) = H^n(\mathcal{C}(A_*, B))$ where $A_* \to A \to 0$ projective resolution of A. Explicitly we have

$$\begin{tikzcd} A_1 \arrow[r, "d_1"] & A_0 \arrow[r] & A \arrow[r] & \cdots \arrow[r, "d_{n+1}"] & A_n \arrow[r, "d_n"] \arrow[d] & {} \\ & & & & B & \end{tikzcd}$$

and $R^n\widetilde{F}(A) = \ker(\# d_{n+1})/\mathrm{Im}(\# d_n)$

$$= \{g \in \mathcal{C}(A_n, B) | g d_{n+1} = 0\}/\{h d_n | h \in \mathcal{C}(A_{n-1}, B)\}.$$

Theorem 14.4.3. *We have* $H_n(\mathcal{C}(A,B)) \simeq H^n(A_*, B)$ *so both give* $\mathrm{Ext}_n(A,B)$. *In fact, both are isomorphic to the additive group*

$$G_n = \{f_* : A^{(n)} \to B^{(n)} \textit{ chain map}\}/\textit{homotopy}$$

where

$$\begin{tikzcd} A^{(n)} = & A_{n+1} \arrow[r, "d^A_{n+1}"] & A_n \arrow[r] \arrow[d, "f_0"] & \cdots \arrow[r] \arrow[d] & A_0 \arrow[r] & A \arrow[r] & 0 \arrow[d, "0"] \\ B^{(n)} = & 0 \arrow[r] & B \arrow[r] & B_0 \arrow[r] & \cdots \arrow[r] & \cdots \arrow[r] & B_{n+1} \end{tikzcd}.$$

Sketch of Proof. Let $f_* : A^{(n)} \to B^{(n)}$ and $f_* = (b_i)_{0 \leqslant i \leqslant n+1}$ chain map. By definition of chain map $f_0 \in \ker(\# d^A_{n+1})$ and $f_{n+1} \in \ker(d^B_{n+1}\#)$. Moreover (to check) for any $f_0 \in \ker(\# d^A_{n+1})$, there is f_* lifting of f_0 to $A^{(n)} \to B^{(n)}$ and f_* is unique up to homotopy because $A^* \to A \to 0$ exact, and B_* injective. For any $f_{n+1} \in \ker(d^B_{n+1}\#)$ there is f_* lifting, unique up to homotopy. This gives surjective homomorphism

$$\phi : \ker(\# d^A_{n+1}) \longrightarrow G_n,$$

$$\psi : \ker(d_{n+1}\#) \longrightarrow G_n.$$

Moreover (check) $\ker\phi = \mathrm{Im}(\# d^A_n$ and $\ker\psi = \mathrm{Im}(d^B_n\#)$. Hence the isomorphism

$$\begin{tikzcd} {} \arrow[r] & A_n \arrow[r] & {} \arrow[dl] & {} \arrow[r] \arrow[dl] & {} \\ {} \arrow[r] & B \arrow[r] & {} \arrow[r] & {} \arrow[r] & {} \end{tikzcd}.$$

$\square$

Definition 14.4.4. Ext

$$\begin{tikzcd}
A_{n+1} \arrow[r, "d_{n+1}"] & A_n \arrow[r] \arrow[d, "f_0"'] & A_{n-1} \arrow[r] \arrow[d, "f_1"'] & \cdots \arrow[r] & A_0 \arrow[r, "d_0"] \arrow[d, "f_n"'] & A \arrow[r] \arrow[d, "f_{n+1}"'] \arrow[dllll, dashed] & 0 \\
0 \arrow[r] & B \arrow[r] & B_0 \arrow[r] & \cdots \arrow[r] & B_{n-1} \arrow[r] & B_n \arrow[r] & B_{n+1}
\end{tikzcd}.$$

Additional interpretation of Ext_n, for $n > 0$ let $\epsilon_n(A, B) = \{0 \to B \to C_1 \to \cdots \to C_n \to A \to 0$ exact sequence$\}/\sim$ where

$$0 \to B \to C_* \to A \to 0 \sim 0 \to B \to C'_* \to A \to 0$$

if there is $g_* : C_* \to C'_*$ chain map such that

$$\begin{tikzcd}
 & C_1 \arrow[r] \arrow[dd, "g_1"] & \cdots \arrow[r] & C_n \arrow[dd, "g_n"] \arrow[dr] & \\
A \arrow[ur] \arrow[dr] & & & & B \\
 & C'_1 \arrow[r] & \cdots \arrow[r] & C'_n \arrow[ur] &
\end{tikzcd}$$

commutes.

15

The Category R-Mod Has Enough Injective

Definition 15.0.1. For any

$$\begin{tikzcd}
\forall A \arrow[rr, tail, "\forall\alpha"] \arrow[dr, "\forall f"'] & & B \arrow[dl, dotted, "\exists\widetilde{f}"] \\
& E &
\end{tikzcd}$$

commutes, for any $\alpha : A \to B$ injective $R-$module homomorphism, for any $f : A \to E$ homomorphism, there is $\widetilde{f} : B \to E$ such that $f = \widetilde{f}\alpha$.

Lemma 15.0.2 (Baer's Criterion)**.** *A $R-$module E is injective if and only if for any $I \subseteq R$ ideal, for any $f : I \to E$, there is $\widetilde{f} : R \to E, f = \widetilde{f}\epsilon$ where $\epsilon : I \to R$ is the inclusion map.*

Proof. $(\Longrightarrow)$: Obvious ϵ is injective homomorphism.

$(\Longleftarrow)$: Suppose E satisfies this condition, let

$$\alpha : A \to \text{ injective homomorphism},$$

$$f : A \to E \text{ homomorphism}.$$

Want to show that there is $\widetilde{f} : B \to E$ such that $f = \widetilde{f}\alpha$. Let $\Omega = \{(X, h), X \subseteq B$ submodule and $h : B \to E, f = h\alpha\}$ ordered by $(X, h) \leqslant (X', h')$ if $X \subseteq X'$ and $h|'_X = h$.

By Zorn's Lemma, there is maximal element $(X, h) \in \Omega$. If $X = B$, suppose not, let $b \in B \backslash X$, let $I = \{r \in R | rb \in X\}$. This is ideal of R. By hypothesis (applied to $g : I \to E$ by $r \mapsto h(rb)$). There is $\overline{g} : R \to E$ such that $r \in I, \widetilde{g}(r) = h(rb)$. Define

$$X' = X + (b),$$

$$h' : X' \to E,$$
$$x + rb \mapsto h(X) + \widetilde{g}(r).$$

We see $(X, h) < (X', h')$ contradicting the maximality of (X, h). $\square$

Definition 15.0.3. Let R be a domain. A $R-$module M is **divisible** if $\forall x \in M, \forall d \in R, \exists y \in M$ such that $dy = x$.

Corollary 15.0.4. *If R is PID, then a $R-$module E is injective if and only if E is divisible.*

Proof. ($\Longleftarrow$): Let E be divisible, we use Baer's criterion to show E is injective. Let $I \subseteq R$ ideal, let $\epsilon : I \to R$ inclusion map, let $f : I \to E$ be $R-$module homomorphism. Then R PID implies that $I = (d)$. Let $x = f(d)$ and let y such that $dy = x$. We can define $\widetilde{f}(1) = y$ and $\widetilde{f}(r) = ry$ and check that $f = \widetilde{f}\epsilon$.

($\Longrightarrow$): Let E injective, let $x \in E$, let $d \in R$, let $f : (d) \to E$ such that $f(rd) = rx$. Then there is $\widetilde{f} : R \to E$ such that $f = \tilde{f}\epsilon$. Then $y = \tilde{f}(1)$ satisfies $dy = \tilde{f}(d) = f(d) = x$. $\square$

Example 15.0.5. The modules $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible $\mathbb{Z}-$modules, hence injective $\mathbb{Z}-$modules.

Theorem 15.0.6. *For any ring R, the category $\mathfrak{R} - \mathfrak{Mod}$ has enough injectives: for any M left $R-$module, there is E injective $R-$module and $M \rightarrowtail E$ injective $R-$module homomorphism (same holds for $\mathfrak{Mod} - \mathfrak{R}$ category of right $R-$modules).*

Definition 15.0.7. We call the **dual** of a left/right $R-$module is the right/left $R-$module. We write $M^\wedge = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$. If M is left $R-$module, the $R-$action is defined by $\forall r \in R, \forall f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ such that

$$(f \cdot r)(x) := f(rx).$$

This is a $R-$action ($(f \cdot r \cdot s)(x) = (f \cdot r)(sx) = f(rsx) = (f \cdot (rs))(x)$). If R is right $R-$module we define

$$(r \cdot f)(x) := f(xr).$$

Proposition 15.0.8. *If F is a free right $R-$module, then $F^\wedge$ is injecitve left $R-$module.*

Lemma 15.0.9. *In $\mathcal{C}$ abelian, we have E injective if and only if $\mathrm{Hom}_{\mathcal{C}}(-, E)$ is exact.*

Lemma 15.0.10. *In $\mathcal{C}$ abelian, for any i, we have if E_i injective then $\bigoplus_i E_i$ is injective.*

Proof. Homework. $\square$

Remark 15.0.11. For any A, B that are left $R-$modules, say $\mathrm{Hom}_R(A, B) = \{f \text{ left } R\text{−module homomorphism}\}$ is a right $R-$module with $R-$action defined by for any $r \in R, \forall f \in \mathrm{Hom}_R(A, B), (f \cdot r)(x) := f(rx)$ (this is a $R-$action since $f \cdot r \cdot s = f \cdot rs$).

Lemma 15.0.12. *For any A left $R-$module, we have $\mathrm{Hom}_R(A, R^\wedge) \simeq A^\wedge$ (isomorphism of right $R-$module) where R is considered as a right $R-$module and $R^\wedge = \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z})$ is a left $R-$module.*

Proof. Let A be a left $R-$module, for $f \in \mathrm{Hom}_R(A, R^\wedge), x \in A, r \in R$ we have

$$\mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) = R^\wedge \ni f(x)(r) = f(x)(1 \cdot r) = (r \cdot f(x))(1) = f(r \cdot x)(1)$$

by the definition of action in $R^\wedge$ and f homomorphism. Define

$$\tilde{f} : A \longrightarrow \mathbb{Q}/\mathbb{Z} \in A^\wedge,$$

$$x \longmapsto f(x)(1).$$

Above computation shows that $\phi : \mathrm{Hom}_R(A, R^\wedge) \to A^\wedge$ such that $f \mapsto \tilde{f}$ is an isomorphism of right $R-$modules. Then

- ϕ homomorphism since $(\widetilde{f \cdot r}(x)) = (fr)(x)(1) = f(rx)(1) = \tilde{f}(rx) = (\tilde{f} \cdot r)(x)$.
- ϕ injective since $f \in \mathrm{Hom}_R(A, R^\wedge)$ is determined by $f(y)(1), y \in A$,
- ϕ surjective since $g \in A^\wedge$ is $\tilde{f}$ for $f \in \mathrm{Hom}_R(A, R^\wedge)$ defined by $f(x)(r) := g(r \cdot x)$ (since $\tilde{f}(x) = f(x)(1) = g(x)$).

Hence the lemma. □

Proof of Proposition 15.0.8. We have

- $\mathbb{Q}/\mathbb{Z}$ is injective $\mathbb{Z}-$module, hence by Lemma 15.0.9 we have $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is exact.
- By Lemma 15.0.12, for any $A \in \mathfrak{R} - \mathfrak{Mod}$, we have $\mathrm{Hom}_R(A, R^\wedge) \simeq \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ in $\mathfrak{Mod} - \mathfrak{R}$. Hence $\mathrm{Hom}_R(-, R^\wedge)$ and $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z}) : \mathfrak{R} - \mathfrak{Mod} \to \mathfrak{Mod} - \mathfrak{R}$ are isomorphic functors. Hence $\mathrm{Hom}_R(-, R^\wedge)$ is exact. Therefore by Lemma 15.0.9, we have $R^\wedge$ is injective in $\mathfrak{R} - \mathfrak{Mod}$.
- Let F be free right $R-$module, then $F \simeq \bigoplus_{i \in I} R$ for some set I. Hence $F^\wedge \simeq \mathrm{Hom}_{\mathbb{Z}}(\bigoplus_{i \in I} R, \mathbb{Q}/\mathbb{Z}) \simeq \prod_{i \in I} \mathrm{Hom}_{\mathbb{Z}}(R, \mathbb{Q}/\mathbb{Z}) = \prod_{i \in I} R^\wedge$. By Lemma 15.0.10, we have $F^\wedge \simeq \prod R^\wedge$ is injective.

Hence the proposition. □

Proposition 15.0.13. *For any M left $R-$module, there is F free right $R-$module and an injective $R-$module homomorphism $M \rightarrowtail F^\wedge$.*

Proposition 15.0.8 and Proposition 15.0.13 together implies Theorem 15.0.6. That is, "$\mathscr{R}-\mathscr{Mod}$" has enough injectives.

Lemma 15.0.14. *For any M left $R-$module, there is injective $R-$module homomorphism $M \to M^{\wedge\wedge}$.*

Proof. For $x \in M$, let

$$\begin{aligned} \mathrm{ev}_x : M^{\wedge} &\longrightarrow \mathbb{Q}/\mathbb{Z}, \\ f &\longmapsto f(x) \end{aligned}$$

evaluation at x. Note that $\mathrm{ev}_x \in M^{\wedge\wedge}$ and

$$E_v : M \longrightarrow M^{\wedge\wedge},$$

$$x \longmapsto \mathrm{ev}_x.$$

Easy to check that E_v is a $R-$module homomorphism. Indeed, for any $r \in R, \forall x \in M, \forall f \in M^{\wedge}$, we have

$$\mathrm{ev}_{r\cdot x}(f) = f(rx) = (f \cdot r)(x) = \mathrm{ev}_x(f \cdot r) = (r \cdot \mathrm{ev}_x)(f)$$

where the last equality is because it is action in $M^{\wedge\wedge}$. Hence $E_v(rx) = rE_v(x)$. It remains to show that E_v is injective ($\Longrightarrow$ check $\ker(E_v) = 0$).

Let $x \in M\backslash\{0\}$, need to show that $\mathrm{ev}_x \neq 0$. Let $G := \{kx : k \in \mathbb{Z}\} \subseteq M$ additive subgroup of $(M, +)$ generated by x. Then G cyclic implies that $G \simeq \mathbb{Z}$ or $G \simeq \mathbb{Z}/n\mathbb{Z}$ with $n \geqslant 0$ ($x \neq 0$).

If $G \simeq \mathbb{Z}$, we let

$$\begin{aligned} f : G &\longrightarrow \mathbb{Q}/\mathbb{Z}, \\ kx &\longmapsto \frac{k}{z} + \mathbb{Z}. \end{aligned}$$

If $G \simeq \mathbb{Z}/n\mathbb{Z}$ we let

$$\begin{aligned} f : G &\longrightarrow \mathbb{Q}/\mathbb{Z}, \\ kx &\longmapsto \frac{k}{n} + \mathbb{Z}. \end{aligned}$$

In both cases, f is $\mathbb{Z}-$module homomorphism since $\mathbb{Q}/\mathbb{Z}$ injective, there exists $\tilde{f} \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z}) = M^{\wedge}$ such that

$$\begin{tikzcd} G \arrow[rr, hook] \arrow[dr, "f"'] & & M \arrow[dl, "\tilde{f}"] \\ & \mathbb{Q} & \end{tikzcd}$$

commutes. Observe that $f(x) \neq 0$ implies $\tilde{f}(x) \neq 0$. Hence $\mathrm{ev}_x(f) \neq 0$ implies that $\mathrm{ev}_x \neq 0$. $\square$

Proof of Proposition 15.0.13. The duality functor $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Q}/\mathbb{Z})$ is left exact (as any Hom functor) and additive. Let $M \in \mathcal{R} - \mathcal{Mod}$, in $\mathcal{Mod} - \mathcal{R}$, there is F free and $\beta : F \twoheadrightarrow M^\wedge$ surjective homomorphism. Since the duality functor is contravariant left exact, the image of epimorphism β is a monomorphism $\beta^\wedge : M^{\wedge\wedge} \rightarrowtail F^\wedge$. Hence we get $M \overset{E_v}{\rightarrowtail} M^{\wedge\wedge} \overset{\beta^\wedge}{\rightarrowtail} F^\wedge$ in $\mathcal{R} - \mathcal{Mod}$. $\square$

E-mail: hou@brandeis.edu