Homological Algebra

Keri Ann Sather-Wagstaff
(Notes by Shuai Wei)

September 18, 2023

Contents

Chapter 1

Introduction to Module Theory

Let R be a ring.

1.1 Basic Definitions and Examples

Definition 1.1. An *left R-module* is an additive abelian group M equipped with a scalar multiplication

$$\begin{aligned} u : R \times M &\to M \\ (r, m) &\to rm, \end{aligned}$$

where u satisfies that for all $r, s \in R$ and $m, n \in M$,

(a) $r(sm) = (rs)m$,

(b) $(r + s)m = rm + sm$,

(c) $r(m + n) = rm + rn$.

If R has multiplicative identity 1, then also assume $1 \cdot m = m$ for $m \in M$. ("*M is unital*".)

Remark. If R is commutative and M is a left R-module, we can make M into a right R-module by defining $mr = rm$ for $m \in M,\ r \in R$.

Example 1.2. Let F be a field.

(a) An F-module is a F-vector space and and vice versa.

(b) An $\mathbb{Z}$-module is an additive abelian group.

(c) The left ideal of R is a left *R-module*.

(d) $R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \,\middle|\, r_1, \ldots, r_n \in R \right\}$ is a left *R-module* by defining addition and multiplication componentwisely. If $R = F$, F^n is called *affine n-space* over F. We make F^n into a vector space by defining addition and scalar multiplication componentwisely.

Remark. Let M be an abelian group and write $\text{End}_{\text{grp}}(M)$ for the set of group homomorphisms from M to M. Then $\text{End}_{\text{grp}}(M)$ is a ring where $(f+g)(m) = f(m)+g(m)$ and $(f \circ g)(m) = f(g(m))$ for $f, g \in \text{End}_{\text{grp}}(M)$ and $m \in M$.

Now assume we have a ring homomorphism $\phi : R \to \text{End}_{\text{grp}}(M)$ that sends 1_R to the identity map in $\text{End}_{\text{grp}}(M)$. Set $rm = \phi(r)m$. Then this makes M into an R-module since M is abelian.

Conversely, now assume we are given an R-module M. We obtain a ring homomorphism $\phi : R \to \text{End}_{\text{grp}}(M)$ by setting $\phi(r)(m) = rm$.

Thus, we see an R-module is nothing more than an abelian group M along with a ring homomorphism $R \to \text{End}_{\text{grp}}(M)$.

1.2 Submodules

Let M be a left R-module.

Definition 1.3. A *submodule* of M is an additive subgroup $N \subseteq M$ such that scalar multiplication on M makes N into a left R-module, i.e., for $r \in R, n \in N$, we have $rn \in N$.

Remark. Submodules of M are therefore just subsets of M which are themselves modules under the restricted operations. Every R-module M has the two trivial submodules M and 0.

Example 1.4. $\mathbb{Q}$ is an $\mathbb{Z}$-module and $\mathbb{Q}[x]$ is an $\mathbb{Q}$-module.

Since $2 \cdot \frac{2}{3} \notin \mathbb{Z}$, and $1 \cdot x \notin \mathbb{Q}$, $\mathbb{Z}$ is not a $\mathbb{Q}$-module and $\mathbb{Q}$ is not a $\mathbb{Q}[x]$-module.

Example 1.5. Let F be an field.

(a) F can be considered as an 1-dimensional F-vector space over itself. A submodule of an F-module is a subspace of an F-vector space.

(b) A submodule of a left $\mathbb{Z}$-module is an additive abelian subgroup.

(c) The submodules of R are precisely the left ideals of R.

Proposition 1.6. Let $I \leqslant R$, then $IM = \{\sum_i^{\text{finite}} a_i m_i \mid a_i \in I, m_i \in M\} \leqslant M$.

Proof. Since $I, M \neq \emptyset$, there exists $a \in I$ and $m \in M$ such that $am \in IM$ and so $IM \neq \emptyset$. Also, $(a_1m_1 + \cdots + a_km_k) - (b_1n_1 + \cdots + b_ln_l) = a_1m_1 + \cdots + a_km_k - b_1n_1 - \cdots - \cdots b_ln_l \in IM$. So IM is a subgroup of M. Let $r \in R$ and $c = \sum_i^{\text{finite}} a_i m_i$ with $a_i \in I$ and $m_i \in M$, then since $ra_i \in I$ for each i, $rc = r\left(\sum_i^{\text{fintie}} a_i m_i\right) = \sum_i^{\text{finite}} (ra_i) m_i \in IM$. At last, the distributive law and associative law on IM are inherited from M. □

Proposition 1.7 (Submodule test)**.** Let $N \subseteq M$. The followings are equivalent.

(i) N is a submodule of M.

(ii) N is a left R-module via the additive and scalar multiplication on M.

(iii) N is and additive subgroup that absorbs scalar multiplication.

(iv) (Assume R has 1.) $N \neq \emptyset$ and for $r \in R$ and for $n, n' \in N$, we have $n + rn' \in N$.

Proof. "(i)$\Longrightarrow$(iv)". Assume N is a submodule of M. Since N is an abelian group, $N \neq \emptyset$. For $r \in R$ and for $n, n' \in N$, we have $rn' \in N$ and then $n + rn' \in N$.

"(iv)$\Longrightarrow$(i)". Assume (iv). Since $n - n' = n + (-1)n' \in N$, N is an additive abelian subgroup. Also, $rn' = 0_M + rn' \in N$. At last, the distributive law and associative law on N are inherited from M. $\square$

Proposition 1.8. (a) If $N_\lambda \leqslant M$ for $\lambda \in \Lambda$, then $\bigcap_{\lambda \in \Lambda} N_\lambda \leqslant M$.

(b) If $\mathcal{C}$ is a chain of submodules of M, $N = \bigcup_{L \in \mathcal{C}} L$ is also a submodule of M.

(c) If $N_1, \dots, N_t \leqslant M$, then $\sum_{i=1}^t N_i = N_1 + \cdots + N_t = \{n_1 + \cdots + n_t \mid n_i \in N_i, \forall i = 1, \dots, t\} \leqslant M$. This is the smallest submodule of M containing $\bigcup_{i=1}^t N_i$. For $L \leqslant M$, $\sum_{i=1}^t N_i \subseteq L$ if and only if $\bigcup_{i=1}^t N_i \subseteq L$.

(d) If $M_1, \dots, M_2$ are left R-modules, then so is $M_1 \times \cdots \times M_n$ with $r(m_1, \dots, m_n) = (rm_1, \dots, rm_n)$.

Proof. (b) Any $L \in \mathcal{C}$ is an additive subgroup, so $\bigcup_{L \in \mathcal{C}}$ is also an additive subgroup. Let $r \in R$ and $n \in N$, then there exists $L \in \mathcal{C}$ such that $n \in L \subseteq N$. So $rn \in L \subseteq N$. At last, the distributive law and associative law are inherited from M.

(c) Since $r(n_1 + \cdots + n_t) = (rn_1) + \cdots + (rn_t) \in N_1 + \cdots + N_t$, $\sum_{i=1}^t N_i \leqslant M$. Note $\sum_{i=1}^t N_i$ is an additive subgroup of M containing $\bigcup_{i=1}^t N_t$. For any additive subgroup G of M, $\sum_{i=1}^t N_i \subseteq G$ if and only if $\bigcup_{i=1}^t N_i \subseteq G$. L is an additive group for $L \leqslant M$. So $\sum_{i=1}^t N_i \subseteq L$ if and only if $\bigcup_{i=1}^t N_i \subseteq L$. Hence $\sum_{i=1}^t N_i$ smallest submodule containing $\bigcup_{i=1}^t N_i$. $\square$

Remark. Let G be an additive abelian group. There exists commutative ring with identity R such that G is a left R-module. If R is an arbitrary ring, G may or may not have an R-module structure.

1.3 Quotient and Homomorphism

Let M, N be left R-modules.

Definition 1.9. A function $f : M \to N$ is an *R-module homomorphism* if for all $m, n \in M$ and $r \in R$, $f(m + m') = f(m) + f(m')$ and $f(rm) = rf(m)$.

Remark. Note R is an R-module. However, R-module homomorphisms need not be ring homomorphisms and ring homomorphism need not be R-module homomorphisms. For example, the $\mathbb{Z}$-module homomorphism $\mathbb{Z} \to \mathbb{Z}$ given by $x \mapsto 2x$ is not a ring homomorphism.

Let F be a field. We have a ring homomorphism $\phi : F[x] \to F[x]$ given by $f(x) \mapsto f(x^2)$ with $(f + g)(x) \mapsto (f + g)(x^2) = f(x^2) + g(x^2)$ and $(fg)(x) \mapsto (fg)(x^2) = f(x^2)g(x^2)$. But it is not an $F[x]$-module homomorphism since $x^2 = \phi(x) = \phi(x \cdot 1) = x\phi(1) = x$, a contradiction.

Example 1.10. (a) Let F be a field, then an F-module homomorphism is a linear transform.

(b) Let R be commutative, M an R-module and $r \in R$, then $u_r : M \to M$ given by $m \mapsto rm$ is an R-module homomorphism (multiplicative map, "*homothety*") since for any $s \in R$ and any $m, m' \in M$, $u_r(m + m') = r \cdot (m + m') = r \cdot m + r \cdot m' = u_r(m) + u_r(m')$ and $u_r(sm) = r \cdot sm = s \cdot rm = s \cdot u_r(m)$.

(c) Let $R = \mathbb{Z}$. The action of ring elements (integers) on any $\mathbb{Z}$-module amounts to just adding and substracting within the additive abelian group structure of the module so that in this case the second condition of a homomorphism is implied by the first one. For example, $\phi(2x) = \phi(x + x) = \phi(x)+\phi(x) = 2\phi(x)$, etc. It follows that $\mathbb{Z}$-module homomorphisms are the same as additive abelian group homomorphism.

Definition 1.11. Define

$$\mathrm{Hom}_R(M, N) := \{R\text{-module homomorphisms } f : M \to N\}.$$

Proposition 1.12. Let $f, g \in \mathrm{Hom}_R(M, N)$ and $h \in \mathrm{Hom}_R(L, M)$.

(a) If $N \leqslant M$, then the natural map $N \to M$ is an R-module homomorphism.

(b) Define $f + g : M \to N$ by $(f + g)m \mapsto f(m) + g(m)$. Then $f + g \in \mathrm{Hom}_R(M, N)$.

(c) $f \circ h \in \mathrm{Hom}_R(L, N)$.

(d) If R is commutative and $r \in R$, then $rf : M \to N$ given by $(rf)(m) \mapsto r \cdot f(m) = f(rm)$ is an R-module homomorphism.

Proof. Let $r, s \in R$ and $m \in M$.

(b) $(f + g)(rm) = f(rm) + g(rm) = rf(m) + rg(m) = r(f(m) + g(m)) = r((f + g)m)$.

(d) $rf(sm) = r \cdot (s \cdot f(m)) = (rs) \cdot f(m) = (sr)f(m) = s \cdot (r \cdot f(m)) = s \cdot ((rf)(m))$. □

Proposition 1.13. (a) $\mathrm{Hom}_R(M, N)$ is an additive abelian group.

(b) If R is commutative, then $\mathrm{Hom}_R(M, N)$ is a (left) R-module.

Proof. (a) Note addition is well-defined on $\mathrm{Hom}_R(M, N)$ by Proposition 1.12 (b). Since N is an abelian group, $f + g = g + f$, for $g, f \in \mathrm{Hom}_R(M, N)$. Let $f \in \mathrm{Hom}_R(M, N)$, define $0 : M \to N$ by $m \mapsto 0$ and define $-f : M \to N$ by $(-f)(m) \mapsto -(f(m))$. Then $-f = 0 + (-f) \in \mathrm{Hom}_R(M, N)$ by Proposition 1.12 (b). Also, $(f + (-f))(m) = f(m) + (-f)(m) = f(m) - f(m) = 0(m) = 0$.

(b) By Proposition 1.12 (d), we can define $R \times \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_R(M, N)$ by $(r, f) \mapsto rf$. By Proposition 1.12 (d), for $r, s \in R$ and $f \in \mathrm{Hom}_R(M, N)$, we have $(rs)f,\ r(sf) \in \mathrm{Hom}_R(M, N)$. Then for $m \in M$, $(rs) \cdot f(m) = ((rs)f)(m) = (r(sf))(m) = r \cdot (sf)(m) = r \cdot (s \cdot f(m))$. So $(rs)f = r(sf)$, etc. □

Definition 1.14. Let R be a commutative ring with identity. An R-*algebra* is a ring A equipped with a ring homomorphism $\Psi : R \to A$ such that $\mathrm{Im}(\Psi) \subseteq Z(A)$.

Remark. If A is an R-algebra, then it is easy to check that A has a natural left and right (unital) R-module structure defined by $r \cdot a = a \cdot r = \Psi(r) \cdot a$. This tells me how to scalar multiply.

Example 1.15. Define $\Psi : \mathbb{Z} \to A$ by $n \mapsto n1_A$. For $a \in A$, we have $(n1_A)a = na = an = (an)1_A = a(n1_A)$. So $\Psi(\mathbb{Z}) \subseteq Z(A)$. So every ring A with 1_A is an $\mathbb{Z}$-algebra.

Example 1.16. (a) For any ring A with 1, if R is a subring of the center of A containing 1, then A is an R-algebra. In particular, a commutative ring with identity A is an R-algebra for any subring R of A containing 1. For example, the polynomial ring $R[x]$ with commutative ring with identity R is an R-algebra.

(b) If A is an R-algebra, then the R-module structure of A depends only on the subring $\Psi(R)$ contained in $Z(A)$. If we replace R by its image $\Psi(R)$, we see that "up to a ring homomorphism", every algebra A arises from a subring of the center of A that contains 1_A.

(c) A special case of the previous example occurs when $R = F$ is a field. In this case F is isomorphic to its image under $\Psi \neq 0$, so we can identify F itself as a subring of A. Hence, saying that A is an algebra over a field F is the same as saying that the ring A contains the field F in its center and the identity of A and of F are the same.

Example 1.17. Let F be a field and $n \geqslant 1$. Then $M_{n\times n}(F)$ is a ring with identity I_n. Note $M_{n\times n}$ is an F-algebra with $\Psi : F \to M_{n\times n}(F)$ given by $\lambda \mapsto \lambda \cdot I_n = \operatorname{diag}(\lambda, \ldots, \lambda)$. Then $\operatorname{Im}(\Psi) = Z\left(M_{n\times n}(F)\right)$. For $\lambda \in F$ and $A = (a_{ij}) \in M_{n\times n}(F)$, $\lambda(a_{ij}) := (\lambda a_{ij})$, i.e., $\lambda A = \Psi(\lambda)\cdot A = (\lambda I_n)\cdot A$.

Example 1.18. (a) $\operatorname{Hom}_R(M, M)$ is a ring with identity.

(b) If R is a commutative ring with identity, then $\operatorname{Hom}_R(M, M)$ is an R-algebra with $\Psi : R \to \operatorname{Hom}_R(M, M)$ given by $r \mapsto r \cdot \operatorname{id}_M := u_r = \cdot r$.

Proof. (a) We already showed it is an additive abelian group. Composite (multiplication) is well-defined and we have the associativity for composition. Note $\operatorname{id}_M \circ f = f = f \circ \operatorname{id}_M$. For $x \in M$,

$$(f + g) \circ h(x) = (f + g)\left(h(x)\right) = f(h(x)) + g(h(x)) = (f \circ h)(x) + (g \circ h)(x) = (f \circ h + g \circ h)(x).$$

Similarly, $h \circ (f + g) = h \circ f + h \circ g$.

(b) We have showed Ψ is well-defined. Let $r, s \in R$ and $x \in M$. Since $(rs)x = r\cdot(sx)$ and $(r+s)x = rx + sx$, i.e., $u_{rs} = u_r \circ u_s$ and $u_{r+s} = u_r + u_s$, we have $\Psi(rs) = \Psi(r)\Psi(s)$ and $\Psi(rs) = \Psi(r)\Psi(s)$. Also, $\Psi(1) = u_1 = \operatorname{id}_M$. So Ψ is a ring homomorphism. Let $f \in \operatorname{Hom}_R(M, M)$. Since f is R-linear, $u_r(f(x)) = rf(x) = f(rx) = f(u_r(x))$. So $u_r \circ f = f \circ u_r$. Hence $\operatorname{Im}(\Psi) \subseteq Z\left(\operatorname{Hom}_R(M, M)\right)$. □

Proposition 1.19. Let $N \leqslant M$. Then we can make the additive abelian group M/N an R-module by defining $r(m + N) = (rm) + N$, or $r\overline{m} = \overline{rm}$. The natural surjection $\pi : M \to M/N$ given by $m \mapsto m + N$ is an R-module homomorphism.

Proof. Let $m + N = m' + N$. Then $m - m' \in N$. Since $N \leqslant M$, $rm - rm' = r(m - m') \in N$. So $(rm) + N = (rm') + N$. Hence scalar multiplication is well-defined. Next, $(rs)(m + N) = ((rs)m) + N = r(sm) + N = r(sm + N) = r(s(m + N))$ and $\pi(rm) = rm + N = r(m + N) = r\cdot\pi(m)$, etc. □

Theorem 1.20 (Isomorphism theorem)**.** *Let $A, B \leqslant M$.*

(a) (The first isomorphism theorem). Let $\phi \in \operatorname{Hom}_R(M, N)$. Then $\operatorname{Ker}(\phi) \leqslant M$ and

$$\begin{aligned} \overline{\phi} : M/\operatorname{Ker}(\phi) &\cong \operatorname{Im}(\phi) \leqslant N. \\ \overline{m} &\mapsto \phi(m). \end{aligned}$$

Then $\overline{\phi}$ is an R-module isomorphism.

(b) (The second isomorphism theorem).

$$\begin{aligned} \alpha : \frac{A}{A \cap B} &\cong \frac{A + B}{B}. \\ \bar{a} &\mapsto \overline{a + 0}. \end{aligned}$$

(c) (The third isomorphism theorem). If $A \subseteq B$, then

$$\begin{aligned} \tau : M/A &\to M/B \\ m + A &\mapsto m + B. \end{aligned}$$

is a surjective abelian group homomorphism and τ is R-linear with $\mathrm{Ker}(\tau) = B/A$. So the first isomorphism theorem implies it is an R-module isomorphism.

$$\begin{aligned} \frac{M/A}{B/A} &\cong \frac{M}{B} \\ (m + A) + B/A &\mapsto m + B. \end{aligned}$$

(d) (The fourth isomorphism theorem).

$$\begin{aligned} \{T \leqslant M/A\} &\rightleftarrows \{U \leqslant M \mid A \subseteq U\} \\ T &\mapsto \pi^{-1}(T) \\ u/A &\leftarrow\!\shortmid u \\ \pi : u &\mapsto m/A \end{aligned}$$

Proof. All results are known for additive abelian group. So we just need to show all maps are R-linear. For (b), $\alpha(r\bar{a}) = \alpha(\overline{ra}) = \overline{ra + 0} = \overline{r(a + 0)} = r\overline{a + 0} = r\alpha(\bar{a})$. □

1.4 Generators, Direct sums and Free modules

Let R be a ring with identity and M be an R-module.

Definition 1.21. (a)

$$\langle A \rangle = RA = \bigcap_{N \leqslant M, A \subseteq N} N \leqslant M, \forall A \subseteq M.$$

If $N \leqslant M$ such that $N = RA$, then N is *(left) generated by* A and A is a *generating set* of N.

(b) Let $A = \{a_1, \ldots, a_n\} \subseteq M$,

$$RA = R\{a_1, \ldots, a_n\} = R(a_1, \ldots, a_n).$$

(c) If $N = R(a_1, \ldots, a_n) \leqslant M$ with $a_1, \ldots, a_n \in M$, then N is a *finitely generated R-module.*

(d) If $N \leqslant M$ such that there exists $a \in M$ such that $N = R(a)$, then N is *cyclic.*

Definition 1.22. Define the *restricted vectors* by

$$R^{\oplus \Lambda} = \{(x_\lambda) \mid x_\lambda \in R \text{ with } x_\lambda = 0 \text{ for almost all } \lambda \in \Lambda\}.$$

Fact 1.23. $R^{\oplus \Lambda}$ is a free module under componentwise addition and scalar multiplication with a standard basis which consists of the vectors e_μ whose λ^{th} component is the value of the *Kronecker delta function*, i.e.,

$$e_\mu := (\delta_{\mu\lambda}), \text{ where } \delta_{\mu\lambda} = \begin{cases} 1 & \text{if } \lambda = \mu \\ 0 & \text{if } \lambda \neq \mu \end{cases}.$$

Convention 1.24. If Λ has a finite number n of elements, then $R^{\oplus\Lambda}$ is often written R^n and called the *direct sum of n copies* of R.

Remark. The free module $R^{\oplus\Lambda}$ has the following UMP: given a module M and elements $m_\lambda \in M$ for $\lambda \in \Lambda$, there is a unique R-module homomorphism $\alpha : R^{\oplus\Lambda} \to M$ given by $e_\lambda \mapsto m_\lambda$, i.e., $(x_\lambda) = \sum x_\lambda e_\lambda \mapsto \sum x_\lambda m_\lambda$.

We have

(a) α is surjective if and only if the m_λ generate M.

(b) α is injective if and only if m_λ is linearly independent.

(c) α is an isomorphism if and only if the m_λ form a free basis.

Proposition 1.25. (a) For $A \subseteq M$, $RA = \left\{ \sum_{a\in A}^{\text{finite}} r_a a \;\middle|\; r_a \in R \right\} \leqslant M$.

If $A = \emptyset$, then $RA = \{0\}$.

(b) $R(a_1, \ldots, a_n) = \{\sum_{i=1}^n r_i a_i \mid r_i \in R\} = Ra_1 + \cdots + Ra_n$.

(c) For $A \subseteq M$, RA is the smallest submodule of M containing A.

For $N \leqslant M$, $RA \leqslant N$ if and only if $A \subseteq N$. Note it is not the same as ideals.

(d) For $a_1, \ldots, a_n \in M$ and $N \leqslant M$, $R(a_1, \ldots, a_n) \leqslant N$ if and only if $a_1, \ldots, a_n \in N$.

Remark. Let $N_1, \ldots, N_n \leqslant M$. $N_1 + \cdots + N_n = R(\cup_{i=1}^n N_n)$ and is the smallest submodule of M containing N_i for $i = 1, \ldots, n$.

If $N_i = RA_i$ for $i = 1, \ldots, n$, $N_1 + \cdots + N_n = R(\cup_{i=1}^n A_n)$.

Remark. A submodule N of M may have many different generating sets. If N is finitely generated, then there is a smallest nonnegative integer d such that N is generated by d elements. Any generating set consisting of d elements will be called a *minimal set of generators* for N. If N is not finitely generated, it need not have a minimal generating set.

The process of generating submodules of an R-module M by taking subsets A of M and forming all finite "R-linear combinations" of elements of A will be our primary way of producing submodules.

Submodules of a finitely generated module need not be finitely generated. For example, let $M = R := F[x_1, x_2, \cdots] = R(1)$ but $F(x_1, x_2, \cdots)$ is not finitely generated, where F is an field.

Example 1.26. Let $R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \;\middle|\; r_1, \ldots, r_n \in R \right\}$, and $e_i = \begin{bmatrix} 0 \\ \vdots \\ 1 \text{ (}i\text{th spot)} \\ \cdots \\ 0 \end{bmatrix}$ for $i = 1, \ldots, n$.

Since $1 \in R$, $R^n = R(e_1, \ldots, e_n) = Re_1 + \cdots + Re_n$. So R^n is finitely generated over R.

Proposition 1.27. Let $N \leqslant M$. If M is a finitely generated R-module, then so is M/N.

If M is cyclic, then so is M/N.

Proposition 1.28. Let R be a commutative ring with identity and $f \in R[x]$ be monic of degree $n \geqslant 1$. Then $M = \frac{R[x]}{(f)}$ is an $R[x]$-module and $M = R(\bar{1}, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{n-1})$.

Proposition 1.29. If $M = R\alpha_1 + \cdots + R\alpha_n$ for some $\alpha_1, \ldots, \alpha_n \in R$, then there exists $N \leqslant R^n$ such that $M \cong R^n/N$.

Proof. Define $\phi : R^n \to M$ by $(r_1, \ldots, r_n) \mapsto r_1\alpha_1 + \cdots + r_n\alpha_n$. Then ϕ is a surjective R-module homomorphism and so $M \cong R^n/\operatorname{Ker}(\phi)$. □

Proposition 1.30. Let $m \in M$. Then

(a) $\operatorname{Ann}_R(m) = \{r \in R \mid rm = 0\} = (0_R : m) \leqslant R$.

(b) Since $1 \in R$, $\frac{R}{\operatorname{Ann}_R(m)} \cong Rm$ by $\bar{r} \mapsto rm$.

(c) $\phi : R \to M$ give by $r \mapsto rm$ is a well-defined R-module homomorphism with $\operatorname{Im}(\phi) = Rm$ and $\operatorname{Ker}(\phi) = \operatorname{Ann}_R(m)$.

1.4.1 Direct Sum

Let M be a left R-module.

Definition 1.31. Let $N_1, \ldots, N_k$ be a collection of R-modules. The collection of k-tuples $(n_1, \ldots, n_k)$ where $n_i \in N_i$ for $i = 1, \ldots, k$ with addition and action of R defined componentwise is called the *direct product* of $N_1, \ldots, N_k$ denoted by $N_1 \times \cdots \times N_k$, which is also an R-module.

Theorem 1.32. *Define* $\pi : N_1 \times \cdots \times N_t \to N_1 + \cdots + N_t$ *by* $(n_1, \ldots, n_t) \mapsto n_1 + \cdots + n_t$. *Then* $N_1 + \cdots + N_t \cong \frac{N_1 \times \cdots \times N_t}{\operatorname{Ker}(\pi)}$.

Example 1.33. π usually not 1-1. Let $M = R := \mathbb{Z}$ and $\pi : 2\mathbb{Z} \times 3\mathbb{Z} \to 2\mathbb{Z} + 3\mathbb{Z} = (2,3)\mathbb{Z} = \mathbb{Z}$, we have $(6, -6) = (2 \cdot 3, 3 \cdot (-2)) \mapsto 6 + (-6) = 0$.

Proposition 1.34 (Set-up as in Theorem 1.32 with $t = 2$.)**.** Define $\delta : N_1 \cap N_2 \to N_1 \times N_2$ by $x \mapsto (x, -x)$. Then δ is R-module homomorphism and 1-1 and $N_1 \cap N_2 \cong \operatorname{Im}(\delta) = \operatorname{Ker}(\pi)$.

Proof. δ is a well-defined R-module homomorphism. Let $0 = \phi(x) = (x, -x)$, then $x, -x = 0$ and so ϕ is 1-1. Next,

$$\begin{aligned} \operatorname{Ker}(\pi) &= \{(x,y) \in N_1 \times N_2 \mid \pi(x,y) = 0\} = \{(x,y) \in N_1 \times N_2) \mid x + y = 0\} \\ &= \{(x,y) \in N_1 \times N_2) \mid y = -x\} = \{(x,-x) \in N_1 \times N_2) \mid x \in N_1, -x \in N_2\} \\ &= \{(x,-x) \in N_1 \times N_2) \mid x \in N_1 \cap N_2\} = \operatorname{Im}(\delta). \end{aligned}$$ □

Corollary 1.35 (same set up, $t = 2$)**.** $\pi : N_1 \times N_2 \to N_1 + N_2$ is an isomorphism if $N_1 \cap N_2 = 0$.

Corollary 1.36. We have an exact sequence $0 \to N_1 \cap N_2 \xrightarrow{\delta} N_1 \times N_2 \xrightarrow{\pi} N_1 + N_2 \to 0$.

Example 1.37 ("*Eilenberg Swindle*")**.** Assume $R \neq 0$, $M = \{(r_1, r_2, \cdots) \mid r_1, r_2, \cdots \in R\}$. Then $M \cap M = M \neq 0$. Note $M \times M \cong M + M = M$ given by $((r_1, r_2, \cdots), (s_1, s_2, \cdots)) \mapsto (r_1, s_1, r_2, s_2, \cdots)$.

Proposition 1.38 (same setup, $t \geqslant 2$)**.** The followings are equivalent.

(a) π is an isomorphism.

(b) $N_j \cap (N_1 + \cdots + N_{j-1} + N_{j+1} + \cdots + N_t) = 0$ for $j = 1, \ldots, t$.

(c) For $x \in N_1 + \cdots + N_t$, there exists unique $n_i \in N_i$ for $i = 1, \ldots, t$ such that $x = n_1 + \cdots + n_t$.

Proof. Let $K_j = \left\{(n_1, \ldots, n_t) \in N_1 \times \cdots \times N_t \mid n_j = -\sum_{i \neq j} n_i\right\}$ for $j = 1, \ldots, t$. Then $K_1 = \cdots = K_t = \operatorname{Ker}(\pi)$.

Let $\widetilde{K}_j = \left\{(n_1, \ldots, n_{j-1}, n_{j+1}, n_t) \in N_1 \cdots \times N_{j-1} \times N_{j+1} \cdots N_t \mid \sum_{i \neq j} n_i \in N_j\right\}$. Define $\delta_j : \widetilde{K}_j \to N_1 \times \cdots \times N_t$ by $(n_1, \ldots, n_{j-1}, n_{j+1}, \ldots, n_t) \mapsto (n_1, \ldots, n_{j-1}, -\sum_{i \neq j} n_i, n_{j+1}, \ldots, n_t)$ for $j = 1, \ldots, t$. Then $\operatorname{Im}(\delta_j) = \operatorname{Ker}(\pi)$ for $j = 1, \ldots, t$. ☐

Remark. If $N_1 \cap (N_2 + N_3) = 0$, $N_2 \cap (N_1 + N_3) = 0$ and $N_3 \cap (N_1 + N_2) = 0$, then $N_1 \cap N_2 \cap N_3 = 0$. However, $N_1 \cap N_2 \cap N_3 = 0$ does not imply $(N_1 + N_2) \cap N_3 = 0$ since we may have $N_3 = N_1 + N_2$.

Corollary 1.39. We have an exact sequence $\widetilde{K}_j \xrightarrow{\delta_j} N_1 \times \cdots \times N_t \xrightarrow{\pi} N_1 + \cdots + N_t \to 0, \forall j = 1, \ldots, t$.

Definition 1.40. Let $M = N_1 + \cdots + N_t$, where $N_1, \ldots, N_t$ are R-modules satisfying the equivalent conditions of the Proposition 1.38, then M is said to be the *(internal) direct sum* of $N_1, \ldots, N_t$, written $M = N_1 \oplus \cdots \oplus N_t = \bigoplus_{i=1}^t N_i$.

1.4.2 Free Modules

Assume R has an identity.

Definition 1.41. Let M be a left R-module and $A \subseteq M$.

(a) If whenver $r_1 a_1 + \cdots, r_n a_n = 0$ for $r_1, \ldots, r_t \in R$ and $a_1, \ldots, a_t \in A$, we have $r_1 = \cdots = r_n = 0$, then A is *free* or *linearly independent.*

(b) If for any $m \in M \setminus \{0\}$, there exist unique distinct $a_1, \ldots, a_t \in A$ and unique $r_1, \ldots, r_t \in R \setminus 0$ such that $m = r_1 a_1 + \cdots + r_t a_t$, i.e., A is free and A generates M, then A is an R-*basis* for M. Write $M = \bigoplus_{a \in A} Ra$.

M is *free* on R if it has an R-basis.

Example 1.42. R^n is free on R with standard basis $\{e_1, \ldots, e_n\}$.

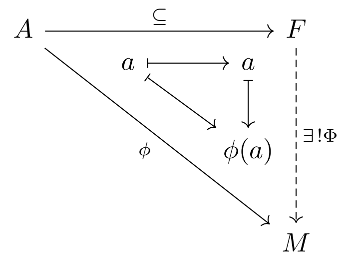
Example 1.43. Let F be a field and $R = F[X, Y]$ and $M = (X, Y)$. Then the ideal M is an R-module. Note $\{X, Y\}$ a generating set for M over R, but not linearly independent since $YX - XY = 0$ and $Y, X \in R$. M is a vector space over F with a basis $\{X^i Y^j \mid i, j \in \mathbb{Z}_{\geqslant 0}, i \text{ or } j > 0\}$.

Proposition 1.44. If R is commutative ring with identity and every R-module is free, then R is a field.

Proof. Let $\mathfrak{m} \leqslant R$ be maximal and $M = R/\mathfrak{m}$. Claim. $\mathfrak{m} = 0$. Suppose not. Since $R/\mathfrak{m}$ is an R-module and every R-module is free, $R/\mathfrak{m}$ has a basis A. Let $r + \mathfrak{m} \in A \subseteq R/\mathfrak{m}$ and $0 \neq x \in \mathfrak{m} \subseteq R$. Then in $R/\mathfrak{m}$, $0 \overset{\text{L.I.}}{\neq} x(r + \mathfrak{m}) = xr + \mathfrak{m} = \mathfrak{m} = 0$, a contradiction. ☐

Lemma 1.45. For any set A, there is a free R-module F with A as a basis. When A is the finite set $\{a_1, \ldots, a_n\}$, $F = Ra_1 \oplus \cdots \oplus Ra_n \cong R^n$.

Theorem 1.46 (UMP)**.** *Let F be free R-module with basis A. Then for any left R-module M and map $\phi : A \to M$, there exists a unique R-module homomorphism $\Phi : F \to M$ such that $\Phi(a) = \phi(a) := m_a$ for $a \in A$.*



Proof. Existence: Since A is a basis, for $x \in F$, $x = \sum_{a\in A}^{\text{finite}} r_a \cdot a$ for some $r_a \in A$ for any $a \in A$. Define $\Phi(x) = \sum_{a\in A}^{\text{finite}} r_a m_a$. Let $\sum_{a\in A}^{\text{finite}} r_a a = \sum_{a\in A}^{\text{finite}} s_a a$, then $r_a = s_a$ for any $a \in A$ since A is linearly independent. So Φ is well-defined. Note $\Phi(rx) = \phi(r \sum_{a\in A}^{\text{finite}} r_a \cdot a) = \Phi(\sum_{a\in A}^{\text{finite}} (rr_a)a) = \sum_{a\in A}^{\text{finite}} (rr_a)m_a = r\sum_{a\in A}^{\text{finite}} r_a m_a = r\Phi(x)$, etc.

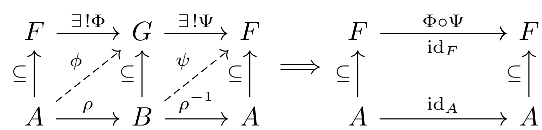
Uniqueness: Suppose $\widetilde{\Phi} : F \to M$ is another R-module homomorphism such that $\widetilde{\Phi}(a) = m_a$ for $a \in A$. Then $\widetilde{\Phi}(x) = \widetilde{\Phi}(\sum_{a\in A}^{\text{finite}} r_a \cdot a) = \sum_{a\in A}^{\text{finite}} r_a \widetilde{\Phi}(a) = \sum_{a\in A}^{\text{finite}} r_a m_a = \Phi(x)$. □

Corollary 1.47. Let F and G be a free R-modules with bases A and B.

(a) If $|A| = |B| \leqslant \infty$, then $F \cong G$.

(b) For any bijective function $\rho : A \to B$, there exists a unique isomorphism $\Phi : F \to G$ given by $a \mapsto \rho(a)$.

Proof. (b) Existence. Define $\phi : A \to G$ given by $a \mapsto \rho(a)$. Since ρ is bijection, there exists $\rho^{-1} : B \to A$. Define $\psi : B \to F$ by $b \mapsto \rho^{-1}(b)$.



By uniqueness, we have $\Psi \circ \Phi = \mathrm{id}_F$. Similarly, $\Phi \circ \Psi = \mathrm{id}_F$. So Φ is an isomorphism. Also, since the diagram commutes, $\Phi(a) = \phi(a) = \rho(a)$ for any $a \in A$.

The uniqueness follows from UMP.

(a) It follows from (b). □

Corollary 1.48. Let F be a free R-module with basis A and $|A| = n < \infty$, then $F \cong R^n$.

Proof. R^n has a basis of size n, then by Corollary 1.47(a), $F \cong R^n$. □

Theorem 1.49 (IBP: Invariant Basis property)**.** *Let R be a commutative ring with identity and $k, n \in \mathbb{Z}_{\geqslant 0}$. If $R^k \cong R^n$, then $k = n$.*

Proof. Let $\mathfrak{m} \leqslant R$ be maximal. Then $(R/\mathfrak{m})^k \overset{\text{hw}}{\cong} R^k/\mathfrak{m}R^k \cong R^n/\mathfrak{m}R^n \cong (R/\mathfrak{m})^n$. Since $R/\mathfrak{m}$ is a field, $(R/\mathfrak{m})^n$ is a vector space over $R/\mathfrak{m}$. □

Theorem 1.50. *Let R be a ring with identity. If F and G are free R-modules with bases A and B and $F \cong G$ and $|A| < \infty$, then $|A| = |B|$. (Hungerford, IV.2.6)*

Theorem 1.51. *For any set A, there exists an R-module F with basis B such that $|B| = |A|$.*

Proof. If $|A| = n < \infty$, let $F = R^n$ and $B = \{e_1, \ldots, e_n\}$.

In general, $F := \{\text{functions } f : A \to R : f(a) = 0\}$, where $f(a) = 0$ for all but finitly many $a \in A$, i.e., $f = 0$ almost everywhere. For example, let $A = \mathbb{Z}_{\geqslant 1}$, $f : \mathbb{Z}_{\geqslant 1} \to R$ represented by $(f(1), f(2), f(3), \cdots)$. Note

$$(f(1), f(2), \ldots, 0, 0, 0, \cdots) = f(1) \cdot (1, 0, 0, 0, \cdots) + f(2) \cdot (0, 1, 0, 0, \cdots) + \cdots = \sum_{i \in \mathbb{Z}_{\geqslant 1}}^{\text{finite}} f(i) \cdot \text{“}e_i\text{”}.$$

Operation on F are pointwise: for any $a \in A$, $(f \pm g)(a) = f(a) \pm g(a)$; $0(a) = 0$ and $(rf)(a) := r \cdot f(a)$. Check this makes F into an R-module. $f(a) = 0$ and $g(a) = 0$ almost everywhere implies $(f+g)(a) = 0$ almost everywhere and $0 + 0 = 0$ and $r \cdot 0 = 0$. So “+” and scalar multiplication “·” are well-defined. Then axioms follow from axioms of R.

For any $c \in A$, define $\chi_c : A \to R$ as $\chi_c(a) = \begin{cases} 1 & \text{if } a = c \\ 0 & \text{if } a \neq c \end{cases}$. For example, let $A = \mathbb{Z}_{\geqslant 1}$. Then χ_1 “=” $(1, 0, 0, 0, 0, \cdots) =$ “e_1” and χ_2 “=” $(0, 1, 0, 0, 0, \cdots) =$ “e_2”.

Need to show

(a) $\{\chi_c\}$ are linearly independent.

(b) $\{\chi_c\}$ are a generating set.

(c) $|A| = |\{\chi_a : a \in A\}| := \{B\}$.

(c) If $a \neq a'$, then $\chi_a(a) = 1 \neq 0 = \chi_{a'}(a)$ and so $\chi_a \neq \chi_{a'}$. Hence $A \to B$ given by $a \mapsto \chi_a$ is 1-1, and onto by definition of B.

(b) Let $f \in F$. Since $f = 0$ a.e., $r(f) = \{a \in A : f(a) \neq 0\}$ is a finite subset of A. Note $r(f)$ is the “support of f”. Claim. $f = \sum_{c \in r(f)} f(c) \cdot \chi_c$, which is finite sum and so well-defined. Note $\sum_{c \in r(f)} f(c) \cdot \chi_c : A \to R$. Need to show $\sum_{c \in r(f)} f(c) \cdot \chi_c(a) = f(a)$ for any $a \in A$.

(1) Case 1: Let $a \in r(f)$. Then $\sum_{c \in r(f)} f(c) \cdot \chi_c(a) = f(a) \cdot \chi_a(a) + \sum_{c \neq a,\ c \in r(f)} f(c) \cdot \chi_c(a) = f(a) \cdot 1 + \sum_{c \neq a,\ c \in r(f)} f(c) \cdot 0 = f(a)$.

(2) Case 2: Let $a \notin r(f)$. Then $\sum_{c \in r(f)} f(c) \cdot \chi_c(a) = 0 = f(a)$.

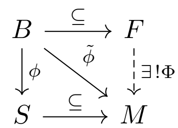
(a) Let $\sum_{c \in A}^{\text{finite}} r_c \chi_c = 0$. Then $0 = \sum_{c \in A}^{\text{finite}} r_c \chi_c(a) = r_a \chi_a(a) = r_a$ for any $a \in A$. □

Corollary 1.52. Let M be a left R-module.

(a) There exists a free R-module F and $N \leqslant F$ such that $M \cong F/N$.

(b) If M is finitely generated, then there exist $n \in \mathbb{Z}_{\geqslant 1}$ and $N \leqslant R^n$ such that $M \cong R^n/N$.

Proof. (a) Let $S \subseteq M$ be any generating set for M. Let F be a free R-module with basis B such that $|B| = |S|$. By the proof of previous theorem, there exists a 1-1 and onto function $\phi : B \to S \subseteq M$.



Let $m \in M$. Since S is generating set for M, $m = \sum_{s\in S}^{\text{finite}} r_s s = \sum_{b\in B}^{\text{finite}} r_{\phi(b)}\phi(b) = \sum_{b\in B}^{\text{finite}} r_{\phi(b)}\tilde{\phi}(b) = \sum_{b\in B}^{\text{finite}} r_{\phi(b)}\Phi(b) = \Phi(\sum_{b\in B}^{\text{finite}} r_{\phi(b)} b)$. So Φ is onto. By the first isomorphism theorem, there exists $N = \text{Ker}(\Phi) \leqslant F$ such that $M \cong F/N$.

(b) Choose S finite, say $S = \{s_1, \ldots, s_n\}$. Then use $F = R^n$. □

1.5 Noetherian Modules

Remark. In a d-dimensional vector space, every subspace is at most d-dimensional. However

(a) a submodule of a finitely generated module need not be finitely generated.

(b) Even if a submodule of a finitely generated module is finitely generated, the minimal number of generators of the submodule is not bounded above by the minimal number of generators of the original module.

Example 1.53. Let $R = F[X_1, X_2, \cdots]$, then $R = R(1)$, but $I = \langle X_1, X_2, \cdots \rangle$ is not finitely generated.

Example 1.54. Let R be the ring of entire functions on $\mathbb{C}$, i.e., R consists of power series with complex coefficients and infinite radius of convergence. It turns out that every finitely generated ideal in R is a principal ideal, but that does not mean all ideals in R are principal: one example of an ideal in R that is not finitely generated is the ideal of entire functions vanishing on all but finitely many indexes.

Example 1.55. The property of being finitely generated is not well-behaved on passage to submodules, so we will give a name to the modules in which every submodule is finitely generated. Emmy Noether was the first mathematician to make a systematic study of this property, so these modules are named after her.

Definition 1.56. Let R be a commutative ring. An R-module is called *Neotherian* if every submodule is finitely generated.

Example 1.57. A finite-dimensional F-vector space is a Noetherian F-module.

Theorem 1.58. *Every submodule of a Noetherian R-module is a Noetherian R-module.*

Proof. It follows from a submodule of a submodule is a submodule. □

Theorem 1.59. *If M is a Noetherian R-module, then for $N \leqslant M$, M/N is a Noetherian R-module.*

Proof. Every submodule of M/N has the form L/N, where $N \leqslant L \leqslant M$.
Since M is a Noetherian R-module, L is a finitely generated R-module and so L/N is a finitely generated R-module. □

Theorem 1.60. *Let M be an R-module and $N \leqslant M$. Then M is a Noetherian R-module if and only if N and M/N are Noetherian R-modules.*

Theorem 1.61. *If M and N are Noetherian R-modules, then $M \otimes N$ is a Noetherian R-module.*

Theorem 1.62. *If R is a PID, then every finitely generated R-module is a Noetherian R-module.*

Proof. Let $m_1, \ldots, m_k \in M$ such that $M = R(m_1, \ldots, m_k)$. Then there is a surjective R-linear map $f : R^k \twoheadrightarrow M$ given by $(c_1, \ldots, c_k) \mapsto c_1 m_1 + \cdots + c_k m_k$. So $M \cong R^k / \operatorname{Ker}(f)$. Since R is PID, R is a Noetherian R-module. So R^k is a Noetherian R-module and hence $R^k / \operatorname{Ker}(f)$ is a Noetherian R-module. □

Remark. When R is a PID. the number of generators in a finitely generated R-module behaves like vector spaces: if M is a module over a PID with n generators, then very submodule of M needs at most n generators.

1.5.1 Finitely Generated Modules over a Noetherian Ring

Theorem 1.63. *If R is a Noetherian ring , then an R-module is Noetherian if and only if it is finitely generated.*

Proof. "$\Longrightarrow$". By definition.
"$\Longleftarrow$". Suppose M is a finitely generated R-module. Then by the proof of the previous theorem, M is a quotient module of some R^k. Since R is a Noetherian R-module, R^k is a Noetherian R-module. So M is a Noetherian R-module. □

1.6 Tensor Product of Modules

Let R be a nonzero ring with identity.

Remark. Formation of the tensor product is a general construction that, loosely speaking, enables one to form another module in which one can take "products" mn with $m \in M$ and $n \in N$.

Remark. Let M be a left R-module. Note $\mu : R \times M \to M$ by $(r, m) \mapsto rm$ is not a R-module homomorphism since $\mu((r, m) + (s, n)) = \mu(r+s, m+n) = (r+s) \cdot (m+n) = rm + rn + sm + sn \neq rm + sn = \mu(r, m) + \mu(s, n)$. Tensor product "fix this", which gives you at minimum an abelian group $R \otimes M$ and additive group homomorphism $R \otimes M \xrightarrow{\hat{\mu}} M$. We may have the UMP

$$\begin{array}{ccc} R \times M & \xrightarrow{\rho} & R \otimes M \\ & \searrow^{\mu} & \downarrow{\hat{\mu}} \\ & & M \end{array}$$

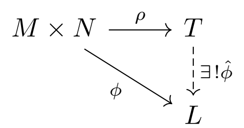
Notation 1.64. Write M_R if M is a right R-module and write ${}_R M$ if M is a left R-module.

Definition 1.65. Let M_R, ${}_RN$ and ${}_{\mathbb{Z}}L$. A function $f : M \times N \to L$ is *"middle linear" over R* or "*R-balanced*" if for all $r \in R$, $m_1, m_2 \in M$ and $n_1, n_2 \in N$, $f(m_1+m_2, n_1) = f(m_1, n_1)+f(m_2, n_1)$, $f(m_1, n_1 + n_2) = f(m_1, n_1) + f(m_1, n_2)$ and $f(m_1 r, n_1) = f(m_1, rn_1)$, where r can not be pulled out since L is not necessarily an R-module.

Example 1.66. (a) If ${}_RN$, we have the R-balanced multiplicative map $\mu : R \times N \to N$ given by $(r, x) \mapsto rx$.

(b) If M_R, we have the R-balanced multiplicative map $\mu : M \times R \to M$ given by $(a, r) \mapsto ar$.

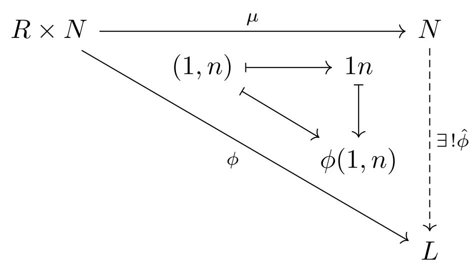
Definition 1.67. Let M_R and ${}_RN$. A *tensor product of M and N over R* is an additive abelian group T equipped with the R-balanced function $\rho : M \times N \to T$ such that for any R-balanced function $\phi : M \times N \to L$ with ${}_{\mathbb{Z}}L$, there exists a unique additive group homomorphism $\hat{\phi} : T \to L$ such that the diagram commutes, i.e., $\hat{\phi} \circ \rho = \phi$.



Write it as $T = M \otimes_R N$ after we define it.

Example 1.68. For any ${}_RN$, "$R \otimes_R N \cong N$ ". Then N is a tensor product of R and N over R using the middle-linear map $\mu : R \times N \to N$ by $(r, n) \mapsto r \cdot n$.

Proof. Let ${}_{\mathbb{Z}}L$ and $\phi : R \times N \to L$ be middle linear.

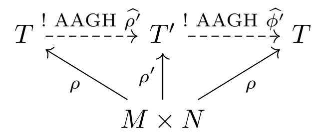


Define $\hat{\phi}(n) := \phi(1, n)$ for $n \in N$. Since ϕ is middle linear, $\hat{\phi}(x+y) = \phi(1, x+y) = \phi(1, x)+\phi(1, y) = \hat{\phi}(x) + \hat{\phi}(y)$ for $x, y \in N$. So $\hat{\phi}$ is an additive group homomorphism. Note $\hat{\phi}\,(\mu(r, n)) = \hat{\phi}(rn) = \phi(1, rn) = \phi(1 \cdot r, n) = \phi(r, n)$ for $r \in R$ and $n \in N$. So the diagram commutes. Let $\tilde{\phi} : N \to L$ be another additive group homomorphism such that $\tilde{\phi} \circ \mu = \phi$. Then $\tilde{\phi}(n) = \tilde{\phi}(1 \cdot n) = \tilde{\phi}\,(\mu(1, n)) = \phi(1, n) = \hat{\phi}(n)$ for $n \in N$. So it is unique. □

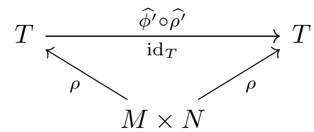
Corollary 1.69. If ${}_{\mathbb{Z}}G$, $\mathbb{Z} \otimes_{\mathbb{Z}} G = G$.

Theorem 1.70. *Let M_R and ${}_RN$. Then a tensor product of M and N over R is unique up to additive group isomorphism.*

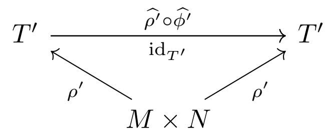
Proof. Assume T and T' are tensor products with universal middle-linear maps ρ and ρ'. Since ρ' and ρ are R-balanced functions,



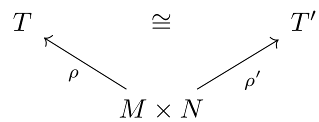
Then we have a UMP for T and ρ.



Similarly, we have a UMP for T' and ρ',



So $\widehat{\rho'}$ and $\widehat{\phi'}$ are the inverse isomorphisms. Thus, $T \cong T'$ as additive group isomorphism. Therefore, there exists an isomorphism

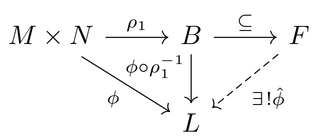


□

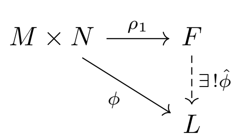
Theorem 1.71. *For any M_R and ${}_RN$, there exists a tensor product of M and N over R.*

Proof. By previous theorem, we can find a free ${}_{\mathbb{Z}}F$ with a basis $B = \{e_{a,x} \mid a \in M \text{ and } x \in N\}$, where $e_{a,x}$ should be selected carefully with $|B| = |M||N|$.

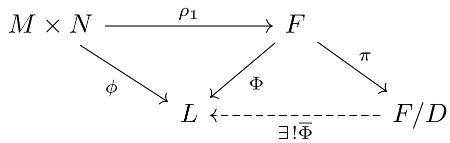
Let $D = \left\langle \begin{array}{c|c} e_{(a+b,x)} - e_{(a,x)} - e_{(b,x)} & \forall a, b \in M \\ e_{(a,x+y)} - e_{(a,x)} - e_{(a,y)} & \forall x, y \in N \\ e_{(ar,x)} - e_{(a,rx)}, e_{(ar,x)} - re_{(a,x)} & \forall r \in R \end{array} \right\rangle$ as $\mathbb{Z}$-module. Then F/D is an additive abelian group. Since ${}_{\mathbb{Z}}F$ is free on B, $\rho_1 : M \times N \to B \subseteq F$ given by $(a, x) \mapsto e_{(a,x)}$, is bijective. Let $\phi : M \times N \to L$ be an R-balanced function.



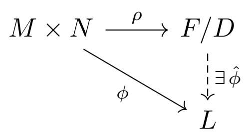
Since ${}_{\mathbb{Z}}F$ is free and ${}_{\mathbb{Z}}L$, by the UMP for free modules, there exists a unique $\mathbb{Z}$-module homomorphism $\hat{\phi}$ such that the right diagram commute. It is straightforward that the left diagram commutes. Then we have a UMP



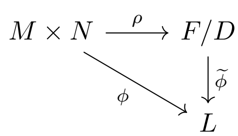
Let $\Phi := \hat{\phi}$. Then $\Phi(e_{(a,x)}) = \phi(a,x)$ for $e_{(a,x)} \in B$. Since $\hat{\phi}$ is an additive group homomorphism and ϕ is middle-linear, $\Phi\left(e_{(a,x+y)} - e_{(a,x)} - e_{(a,y)}\right) = \Phi\left(e_{(a,x+y)}\right) - \Phi\left(e_{(a,x)}\right) - \Phi\left(e_{(a,y)}\right) = \phi(a,x+y) - \phi(a,x) - \phi(a,y) = 0$. Similarly, for any other generator ξ of D, $\Phi(\xi) = 0$. So $D \subseteq \mathrm{Ker}(\Phi)$. Then there exists a unique additive abelian group homomorphism $\overline{\Phi}$ such that the right diagram commutes.



Let $\hat{\phi} := \overline{\Phi}$ and $\rho := \pi \circ \rho_1$, we have a UMP



Then $\hat{\phi}\left(\overline{e_{(a,x)}}\right) = \phi(a,x)$. Let $e_{(a+b,x)} - e_{(a,x)} - e_{(b,x)} \in D$, then $\rho(a+b,x) = \pi \circ \rho_1(a+b,x) = \pi(e_{(a+b,x)}) = \overline{e_{(a+b,x)}} = \overline{e_{(a,x)} + e_{(b,x)}} = \overline{e_{(a,x)}} + \overline{e_{(b,x)}} = \rho(a,x) + \rho(b,x)$, etc, we have ρ is R-balanced. Let $\widetilde{\phi} : F/D \to L$ be another additive abelian group homomorphism such that the diagram commutes. Then



Note $\hat{\phi}(\overline{e_{(a,x)}}) = \phi(a,x) = \widetilde{\phi}(\rho(a,x)) = \widetilde{\phi}(\overline{e_{(a,x)}})$ for $\overline{e_{(a,x)}} \in F/D$. Let $\beta \in F/D$, then $\beta = \overline{\sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} e_{(a,x)}} = \sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} \overline{e_{(a,x)}}$, where $m(a,x) \in \mathbb{Z}$. Since $\hat{\phi}$ and $\widetilde{\phi}$ are $\mathbb{Z}$-linear, $\hat{\phi}(\beta) = \hat{\phi}(\sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} \overline{e_{(a,x)}}) = \sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} \hat{\phi}(\overline{e_{(a,x)}}) = \sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} \widetilde{\phi}(\overline{e_{(a,x)}}) = \widetilde{\phi}(\sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} \overline{e_{(a,x)}}) = \widetilde{\phi}(\beta)$. □

Definition 1.72. The *tensor product of M and N* is defined by $M \otimes_R N := F/D$.

Definition 1.73. Let $a \in M, x \in N$, we have a *simple tensor* $a \otimes x := \rho(a,x) = \overline{e_{(a,x)}} \in T = M \otimes_R N$.

Remark. $\hat{\phi}\left(\overline{e_{(a,x)}}\right) = \hat{\phi}\left(\rho(a,x)\right) = \phi(a,x)$. For any $\beta \in M \otimes_R N$, $\beta = \sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)} (a \otimes x)$. Since $e_{(a+b,x)} - e_{(a,x)} - e_{(b,x)} \in D$, $(a+b) \otimes x = \overline{e_{(a+b,x)}} = \overline{e_{(a,x)} + e_{(b,x)}} = \overline{e_{(a,x)}} + \overline{e_{(b,x)}} = a \otimes x + b \otimes x$, etc.

Proposition 1.74. $M \otimes_R N = \langle a \otimes x \mid a \in M, x \in N \rangle$ as $\mathbb{Z}$-module. This is why linear maps on tensor products are in practice described only by their values on elementary tensors. It is similar to describing a linear map between finite free modules using a matrix. The matrix directly tells you only the values of the map on a particular basis, but this information is enough to determine the linear map everywhere.

Warning 1.75. (a) Arbitrary element of $M \otimes_R N$ is not ususally a simple tensor.

(b) Simple tensors not usually independent.

(c) Frequently, define $M \otimes_R N \xrightarrow{\psi} L$ by saying $\psi(a \otimes x) = \cdots$ since ψ is usually an AAGH and simple tensors are generators.

(d) $a \otimes x$ is not an arbitrary element of $M \otimes_R N$, but defining ψ on $a \otimes x$ and knowing that ψ is well-defined and linear respect linear combinations: $\psi(\xi) = \sum_{(a,x)}^{\text{finite}} m_{(a,x)} \psi(a \otimes x)$ for $\xi = \sum_{(a,x)\in M\times N}^{\text{finite}} m_{(a,x)}(a \otimes x)$.

Remark. Since each $m \otimes n$ represents a coset in some quotient group, we may have $m \otimes n = m' \otimes n'$ when $m \neq m'$ and $n \neq n'$. More generally, an element of $M \otimes N$ may be expressible in many different ways as a sum of simple tensors. In particular, care must be taken when defining maps from $M \otimes_R N$ to another group or module, since a map from $M \otimes N$ which is described on the generators $m \times n$ in term of m and n is not well-defined unless it is shown to be independent of the particular choice of $m \otimes n$ as a coset representative.

Theorem 1.76. *Restate UMP: for middle linear ρ and ϕ,*

$$\begin{array}{ccccc} M \times N & \xrightarrow{\rho} & M \otimes N & & a \otimes x \\ & \searrow^{\phi} & \downarrow{\scriptstyle \exists!\ AAGH} & & \downarrow \\ & & AAG & & \phi(a, x) \end{array}$$

Proposition 1.77. Let M_R and ${}_RN$. Then for all $a, b \in M$ and $x, y \in N$,

(a) $(a + b) \otimes x = a \otimes x + b \otimes x$, $a \otimes (x + y) = a \otimes x + a \otimes y$ and $(ar) \otimes x = a \otimes (rx)$. So $(\sum_{i=1}^{m} a_i) \otimes \left(\sum_{j=1}^{n} x_j\right) = \sum_{i=1}^{m} \sum_{j=1}^{n} (a_i \otimes x_j)$ for $a_1, \ldots, a_m \in M$ and $x_1, \ldots, x_n \in N$;

(b) $a \otimes (nx) = n(a \otimes x) = (na) \otimes x$ for $n \geqslant 0$;

(c) $0 \otimes x = 0 = a \otimes 0$;

(d) $a \otimes (-x) = -(a \otimes x) = (-a) \otimes x$;

(e) $\left(\sum^{\text{finite}} a\right) \otimes \left(\sum^{\text{finite}} x\right) = \sum^{\text{finite}} (a \otimes x)$.

Proof. (c) Since $0 \otimes x + 0 \otimes x = (0 + 0) \otimes x = 0 \otimes x = (0 \otimes x) + 0$, by the cancellation law of abelian group, we have $a \otimes 0 = 0$;

(d) Note $0 = (-a) \otimes x + a \otimes x$. □

Remark (Discussion)**.** Let M_R and ${}_RN$. $M \otimes N$ is AAG but the R-module structure has been lost in general. If R is not commutative, then $\text{Hom}_R(M, N)$ is "only" an AAG.

Definition 1.78. An *SR-bimodule* M is an AAG that is also a left S-module, a right R-module and is associative: $(sa)r = s(ar)$. Notation: ${}_SM_R$.

Example 1.79. (a) If M_R and ${}_RN$, then ${}_{\mathbb{Z}}M_R$ and ${}_RN_{\mathbb{Z}}$.

(b) ${}_RR_R$.

(c) If R is a commutative ring with identity and M_R and N_R, then ${}_RM_R$ and ${}_RN_R$.

Proof. (c) Since R is commutative, ${}_RM$ with $ra =: ar$ for $r \in R$ and $a \in M$. So $(ra)r' = r'(ra) = (r'r)a = (rr')a = r(r'a) = r(ar')$ for $r, r' \in R$ and $a \in M$, we have ${}_RM_R$. Similarly, ${}_RN_R$. ☐

Example 1.80. Let $R \xrightarrow{\varphi} S$ be homomorphism of commutative ring with identity's, ${}_SM$ and N_S. Since we can define $a \cdot r := \varphi(r) \cdot a$ and $r \cdot x := x \cdot \varphi(r)$ for $a \in M$ and $x \in N$, we have ${}_SM_R$ and ${}_RN_S$. Also, since ${}_SS_S$, we have ${}_SS_R$ and ${}_RS_S$.

Lemma 1.81. Let $\alpha : M_R \to M'_R$ be a right R-module homomorphism and $\beta : {}_RN \to {}_RN'$ be a left R-module homomorphism.

(a) There exists a unique AAGH, denoted by $\alpha \otimes \beta$, mapping $M \otimes_R N$ into $M' \otimes_R N'$, i.e., $\alpha \otimes \beta : M \otimes_R N \to M' \otimes_R N'$ given by $\sum_i a_i \otimes x_i \mapsto \sum_i \alpha(a_i) \otimes \beta(x_i)$ (or given by $a \otimes x \mapsto \alpha(a) \otimes \beta(x)$).

(b) There exists a well-defined AAGH $\alpha \otimes N : M \otimes N \to M' \otimes_R N$ given by $a \otimes x \mapsto \alpha(a) \otimes x$.

(c) There exists a well-defined AAGH $M \otimes \beta : M \otimes N \to M \otimes_R N'$ given by $a \otimes x \mapsto a \otimes \beta(x)$.

Proof. (a) Define $\alpha \times \beta : M \times N \to M' \to N'$ by $(a, x) \to (\alpha(a), \beta(x))$. Use UMP for $M \otimes_R N$.

$$\begin{array}{ccc} M \times N & \xrightarrow{\alpha \times \beta} & M' \times N' \\ & & \big\downarrow \rho' \\ & & M' \otimes_R N' \end{array}$$

Define $M \times N \underset{\rho' \circ (\alpha \times \beta)}{\xrightarrow{\phi}} M' \otimes N'$ by $(a, x) \mapsto \alpha(a) \otimes \beta(x)$. Note $\phi(a, x + y) = \alpha(a) \otimes \beta(x + y) = \alpha(a) \otimes (\beta(x) + \beta(y)) = \alpha(a) \otimes \beta(x) + \alpha(a) \otimes \beta(y) = \phi(a, x) + \phi(a, y)$, and $\phi(ar, x) = \alpha(ar) \otimes \beta(x) = (\alpha(a) \cdot r) \otimes \beta(x) = \alpha(a) \otimes (r \cdot \beta(x)) = \alpha(a) \otimes \beta(rx) = \phi(a, rx)$, etc, so ϕ is middle-linear. Hence

$$\begin{array}{ccc} M \times N & \xrightarrow{\rho} & M \otimes N \\ & \underset{\phi}{\searrow} & \big\downarrow \exists!\ \text{AAGH } \hat{\phi} \\ & & M' \otimes N' \end{array}$$

UMP implies $a \otimes \beta := \hat{\phi}$ and by the definition of ϕ, we have the definition for $\alpha \otimes \beta$.

(b) Special case of (a).

(c) Special case of (a). ☐

Theorem 1.82. *If $\lambda : M' \to M''$ and $\mu : N' \to N''$ are R-module homomorphisms, then $(\lambda \otimes \mu) \circ (\varphi \otimes \psi) = (\lambda \circ \varphi) \otimes (\mu \circ \psi)$.*

Proof. It follows from the uniqueness of UMP. ☐

Proposition 1.83. If ${}_SM_R$ and ${}_RN_T$, e.g. $S = \mathbb{Z}$ or $T = \mathbb{Z}$, then

(a) For any $s \in S$, there exists a well-defined AAGH $\mu_s : M \otimes_R N \to M \otimes N$ given by $a \otimes x \mapsto (sa) \otimes x$.

(b) For any $t \in T$, there exists a well-defined AAGH $\nu_t : M \otimes_R N \to M \otimes N$ given by $a \otimes x \mapsto a \otimes (xt)$.

Proof. (a) Since ${}_SM_R$, $\phi_s : M \to M$ given by $a \mapsto sa$ is a homomorphism of right R-modules. Then by lemma 1.81(b), $\mu_s := \phi_s \otimes N : M \otimes_R N \to M \otimes_R N$ is given by $a \otimes x \mapsto \phi_s(a) \otimes x = (sa) \otimes x$.

(b) Similarly. □

Example 1.84. $0 \otimes N \to 0$ given by $0 \otimes n \mapsto 0$ and $\sum 0 \otimes n \mapsto 0$.

Theorem 1.85. *Let ${}_SM_R$ and ${}_RN_T$. Then ${}_S(M \otimes_R N)_T$ such that $s(a \otimes x) := (sa) \otimes x$ and $(a \otimes x)t := a \otimes (xt)$.*

Proof. By Proposition 1.83, operations are well-defined. It is straightforward that ${}_S(M \otimes_R N)$ and $(M \otimes_R N)_T$, e.g., $((\sum_i a_i \otimes x_i)t)t' = (\sum_i a_i \otimes (x_i t))t' = \sum_i a_i \otimes ((x_i t)t') = \sum_i a_i \otimes (x_i(tt')) = (\sum_i a_i \otimes x_i)(tt')$ after distributive law is showed. Note $(s(\sum_i a_i \otimes x_i))t = (\sum_i s(a_i \otimes x_i)t) = \sum_i (sa_i) \otimes (x_i t) = \sum_i s(a_i \otimes (x_i t)) = s(\sum_i a_i \otimes (x_i t)) = s(\sum_i (a_i \otimes x_i)t) = s((\sum_i a_i \otimes x_i)t)$. □

Corollary 1.86. (a) $S = \mathbb{Z}$: If M_R and ${}_RN_T$, then $(M \otimes_R N)_T$.

(b) $T = \mathbb{Z}$: If ${}_SM_R$ and ${}_RN$ then ${}_S(M \otimes_R N)$.

Corollary 1.87. If R is a commutative ring with identity and M and N are left R-modules with canonical RR-bimodule structure, then ${}_R(M \otimes_R N)_R$ such that $r(a \otimes x) = (ra) \otimes x = ar \otimes x = a \otimes (rx) = a \otimes (xr) = (a \otimes x)r$ for $r \in R$ and $a \otimes x \in M \otimes_R N$.

Corollary 1.88 (extension of scalars)**.** Let $\varphi : R \to S$ be homomorphism of commutative ring with identity's and let ${}_RN$. Then ${}_S(S \otimes_R N)$.

Proof. Note ${}_SS_R$. Then it follows from Corollary 1.86 (b). □

Corollary 1.89. Let M_R and ${}_RN$. Then $R \otimes_R N \cong N$, which is an isomorphism of left R-module and $M \otimes_R R \cong M$, which is an isomorphism of right R-module.

Proof. We first show $\hat{\phi} : R \otimes_R N \to N$ given by $r \otimes n \mapsto rn$ is a well-defined isomorphism of AAG. Since $\phi : R \times N \to N$ given by $(r, n) \mapsto rn$ is middle-linear, we have the UMP:

$$\begin{array}{ccc} R \times N & \xrightarrow{\rho} & R \otimes_R N \\ & {\scriptstyle\phi}\searrow & \downarrow {\scriptstyle \exists!\ \text{AAGH}\ \hat{\phi}} \\ & & N \end{array}$$

Furthermore, since R has 1 and there is a AAGH $\psi : N \to R \otimes_R N$ given by $n \mapsto 1 \otimes n$. Since $(\psi \circ \hat{\phi})(r \otimes x) = \psi(rx) = 1 \otimes rx = r \otimes x$ and $(\hat{\phi} \circ \psi)(x) = \hat{\phi}(1 \otimes x) = 1 \cdot x = x$, $\hat{\phi}$ is a bijection and then an isomorphism. Note $\hat{\phi}(r\xi) = \hat{\phi}(r(\sum_i r_i \otimes x_i)) = \hat{\phi}(\sum_i r(r_i \otimes x_i)) = \hat{\phi}(\sum_i (rr_i) \otimes x_i) = \sum_i (rr_i)x_i = \sum_i r(r_i x_i) = r \sum_i r_i x_i = r\hat{\phi}(\sum_i r_i \otimes x_i) = r\hat{\phi}(\xi)$ for $r \in R$ and $\xi = \sum_i r_i \otimes x_i \in R \otimes_R N$. □

Theorem 1.90. *Let $\alpha : M_R \to M'_R$ be a right R-module homomorphism and $\beta : {}_RN \to {}_RN'$ be a left R-module homomorphism. If ${}_SM_R$, ${}_SM'_R$ and α is also an S-module homomorphism, then $\alpha \otimes \beta$ is a left S-module homomorphism. In particular, if R is commutative, then $\alpha \otimes \beta$ is always an R-module homomorphism.*

Proof. Since ${}_SM$ and ${}_SM'$, we have ${}_S(M \otimes N)$ and ${}_S(M' \otimes N')$. Since α is an S-module homomorphism, $(\alpha \otimes \beta)(s(m \otimes n)) = (\alpha \otimes \beta)(sm \otimes n) = \alpha(sm) \otimes \beta(n) = s\alpha(m) \otimes \beta(n) = s(\alpha(m) \otimes \beta(n)) = s(\alpha \otimes \beta)(m \otimes n)$ for $s \in S$ and $m \otimes n \in M \otimes_R N$. □

Proposition 1.91. Let R be a commutative ring with identity and ${}_RM$ and ${}_RN$ with canonical RR-bimodule structure. Let $B \subseteq M$ and $Y \subseteq N$ be a generating set over R, respectively. Let $\mathcal{S} = \{b \otimes y \in M \otimes_R N \mid b \in B, y \in Y\}$. Then $\mathcal{S}$ is a generating set for $M \otimes_R N$ as an R-module.

Proof. Set $H = \{a \otimes x \in M \otimes_R N \mid a \in M, x \in N\}$. We know $M \otimes_R N := {}_{\mathbb{Z}}H$, which means a generating set over $\mathbb{Z}$ by H. Since ${}_R(M \otimes_R N) \supseteq \mathcal{S}$, $M \otimes_R N \supseteq R\mathcal{S}$. Let $a \in M$ and $x \in N$, then $a = \sum_i r_i b_i$ with $r_i \in R, b_i \in B$ and $x = \sum_j s_j y_j$ with $s_j \in R, y_i \in Y$. Then $(a \otimes x) = (\sum_i r_i b_i) \otimes \left(\sum_j s_j y_j\right) = \sum_i \sum_j (r_i b_i) \otimes (s_i y_j) = \sum_i \sum_j r_i s_j b_i \otimes y_j \in R\mathcal{S}$. So $M \otimes_R N = {}_{\mathbb{Z}}H \subseteq {}_RH \subseteq R\mathcal{S}$. □

Corollary 1.92. Let R be commutative ring with identity and ${}_RM, {}_RN$ are both finitely generated over R. Then $M \otimes_R N$ is finitely generated over R.

Definition 1.93. Let ${}_SM_R$ and ${}_RN_T$ and ${}_SL_T$. A function $f : M \times N \to L$ is *ST-bilinear* if

(a) f is middle-linear.

(b) f respects S-module structure: $sf(a, x) = f(sa, x)$ for all $s \in S$, $a \in M$ and $x \in N$.

(c) f respects T-module structure: $f(a, x)t = f(a, xt)$ for all $t \in T$, $a \in M$ and $x \in N$.

Or it is *ST-bilinear* if

(a) $f(s_1a_1 + s_2a_2, n) = s_1f(a_1, x) + s_2f(a_2, x)$ for all $s_1, s_2 \in S$, $a_1, a_2 \in M$ and $n \in N$.

(b) $f(a, x_1t_1 + x_2t_2) = f(a, x_1)t_1 + f(a, x_2)t_2$ for all $t_1, t_2 \in T$, $x_1, x_2 \in N$ and $a \in M$.

Proposition 1.94. Let ${}_SM_R$ and ${}_RN_T$ and ${}_SL_T$.

(a) $\rho : M \times N \to M \otimes_R N$ is a ST-bilinear.

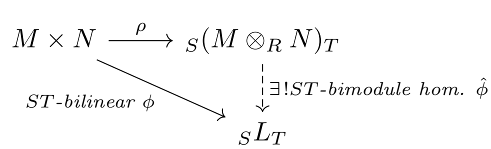
(b) $f : R \times N \to N$ given by $(r, x) \mapsto rx$ is RT-bilinear.

(c) $g : M \times R \to M$ given by $(a, r) \mapsto ar$ is SR-bilinear.

Proof. (a) The universal middle-linear is from definition of tensor product: $\rho(a, x) := a \otimes x$ for $(a, x) \in M \times N$. Since S_M, $s\rho(a, x) = s(a \otimes x) = (sa) \otimes x = \rho(sa, x)$, etc.

(b) Clearly, f is middle-linear. Note $r'f(r, x) = r'(rx) = (r'r)x = f(r'r, x)$, etc. □

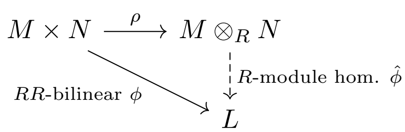
Theorem 1.95 (UMP for ST-bimodule)**.** *If ${}_SM_R$, ${}_RN_T$ and ${}_SL_T$, for any ST-bilinear map ϕ : $M \times N \to L$, there exists a unique ST-bimodule homomorphism $\hat{\phi}$ such that*



Proof. We need to show that $\hat{\phi}$ is an ST-bimodule. $\hat{\phi}(s(a \otimes x)) = \hat{\phi}((sa) \otimes x) = \hat{\phi}(\rho(sa, x)) = \phi(sa, x) = s\phi(a, x) = s\hat{\phi}(\rho(a, x)) = s\hat{\phi}(a \otimes x)$, then extend to $s\xi = s \sum a \otimes x \in M \times N$ using linearity. Similarly, for ξt.

The uniqueness follows from the original UMP. □

Corollary 1.96. Let R be a commutative ring with identity, ${}_RM$ and ${}_RN$, implying ρ is RR-linear, evoke a canonical RR-bimodule structures for any RR-bilinear map $\phi : M \times N \to L$, there exists a unique R-module homomorphism such that



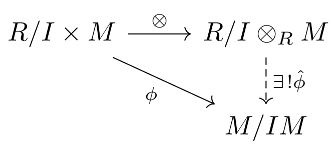
Example 1.97. Let $a \otimes b \in \mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/3\mathbb{Z}$. Since $3a = a$, $a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$. So $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z} = 0$. Thus, there are no nonzero bilinear maps from $\mathbb{Z}/2\mathbb{Z} \otimes \mathbb{Z}/3\mathbb{Z}$ to abelian groups.

Example 1.98. In general, $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$, where $d = (m, n)$.

Proof. Let $a \otimes b \in \mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z}$. Then $a \otimes b = (ab) \otimes 1 = ab(1 \otimes 1)$. So $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ is a cyclic group with $1 \otimes 1$ as generator. Since $m(1 \otimes 1) = m \otimes 1 = 0 \otimes 1 = 0$ and similarly $n(1 \otimes 1) = 1 \otimes n = 0$, we have $d(1 \otimes 1) = 0$. So the cyclic group has order dividing d. Since d divides both m and n, we have a well-defined map $\varphi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ given by $(a + m\mathbb{Z}, b + n\mathbb{Z}) \mapsto ab + d\mathbb{Z}$, which is clearly $\mathbb{Z}\mathbb{Z}$-bilinear. Then the induced map $\hat{\phi} : \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ maps $1 \otimes 1$ to $1 \in \mathbb{Z}/d\mathbb{Z}$, which is an element of order d. In particular, $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$ has order at least d. Hence $1 \otimes 1$ is an element of order d and $\hat{\phi}$ gives an isomorphism $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$. □

Example 1.99. Let $I \leqslant R$ and M be a left R-module, then there is a unique R-module isomorphism $(R/I) \otimes_R M \cong M/IM$ given by $\bar{r} \otimes m \mapsto \overline{rm}$. In particular, taking $I = (0)$, as R-module, $R \otimes_R M \cong M$ by $r \otimes m \mapsto rm$.

Proof. Start with $\phi : R/I \times M \to M/IM$ given by $(\bar{r}, m) \mapsto \overline{rm}$, which is well-defined and middle-linear. Then by UMP of tensor product, we get a unique AAGH map $\hat{\phi}$ making the following diagram commute, where $\hat{\phi} : R/I \otimes_R M \to M/IM$ is given by $\bar{r} \otimes m \mapsto \overline{rm}$.

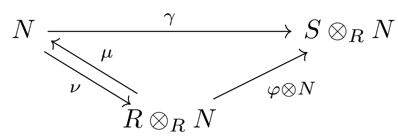


Define $\varphi : M \to R/I \otimes_R M$ by $m \mapsto \bar{1} \otimes m$, which is AAGH. Let $m = \sum_{i=1}^n a_i m_i \in IM$ with $a_i \in I$ and $m_i \in M$. Then $\varphi(m) = \bar{1} \otimes m = \bar{1} \otimes \sum_{i=1}^n a_i m_i = \sum_{i=1}^n \bar{1} \otimes a_i m_i = \sum_{i=1}^n \overline{a_i} \otimes m_i = \sum_{i=1}^n 0 \otimes m_i = 0$. So $IM \subseteq \operatorname{Ker}(\varphi)$. Similarly, $\operatorname{Ker}(\varphi) \subseteq IM$ by considering the R-generators $\{am \mid a \in I \text{ and } m \in M\}$ of IM. Then we get a AAGH $\overline{\varphi} : M/IM \to R/I \otimes_R M$ by $\overline{m} \mapsto \bar{1} \otimes m$. Let $\overline{m} \in M/IM$, then $\hat{\phi}(\overline{\varphi}(\overline{m})) = \hat{\phi}(\bar{1} \otimes m) = \overline{m}$. In $R/I \otimes_R M$, any simple tensor has the form $\bar{r} \otimes m = \bar{1} \otimes rm$, so sums of elementary tensors are $\bar{1} \otimes \sum_i m_i$. Note $\overline{\varphi}(\hat{\phi}(\bar{1} \otimes m)) = \overline{\phi}(\overline{m}) = \bar{1} \otimes m$. □

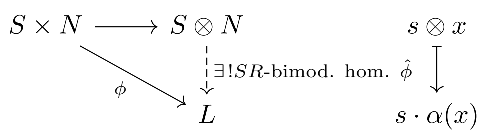
Theorem 1.100. *Let $\varphi : R \to S$ be a ring homomorphism of commutative ring with identity's and ${}_RN$ and ${}_SL$. Then we have an R-module isomorphism* $\operatorname{Hom}_S(S \otimes_R N, L) \cong \operatorname{Hom}_R(N, L)$.

Proof. Since $S \otimes_R N$ is an left S-module and S is commutative, $\mathrm{Hom}_S(S \otimes_R N, L)$ is an S-module. So $\mathrm{Hom}_S(S \otimes_R N, L)$ is an R-module by restriction of scalars. Also, L is an R-module by restriction of scalars. Define $r * s := \varphi(r)s$ and $r * l := \varphi(r)l$ for $r \in R, s \in S$ and $l \in L$.

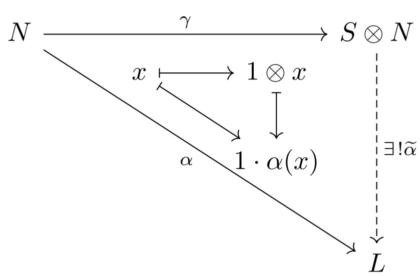
Let $f \in \mathrm{Hom}_R(N, L)$, then $(rf)(x) := rf(x) = f(rx)$. Let $r, r' \in R$. Since φ is a ring homomorphism, $\varphi(r+r') = \varphi(r)+\varphi(r')$. Also, since $\varphi(rr') = \varphi(r)\varphi(r') = r*\varphi(r')$, we have φ is an R-module homomorphism. Also, since R is commutative, $\varphi \otimes N$ is an R-module homomorphism. Claim. there exists an R-module homomorphism $\gamma : N \to S \otimes_R N$ compatible with the left R-module isomorphism $\nu : N \cong R \otimes_R N$ defined by $\nu(n) = 1 \otimes n$.



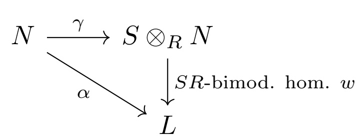
Define $\gamma := (\varphi \otimes N) \circ \nu$. Since ν and $\varphi \otimes N$ are R-module isomorphisms, γ is an R-module isomorphism. Let $\alpha \in \mathrm{Hom}_R(N, L)$ and define $\phi : S \times N \to L$ by $(s, r) \mapsto s \cdot \alpha(x)$. Since $\phi(ss', x) = (ss')\alpha(x) = s(s'\alpha(x)) = s\phi(s', x)$, etc, we have ϕ is SR-bilinear. By the UMP for SR-bimodule, there exists a unique SR-bimodule homomorphism $\hat{\phi} : S \otimes_R N \to L$ such that



commutes. Consider



So we can set $\widetilde{\alpha} = \hat{\phi}$. Suppose there is another SR-bimodule $w : S \otimes_R N \to L$ such that



commutes. Then $w(s \otimes x) = w(s \cdot (1 \otimes x)) = s \cdot w(1 \otimes x) = sw(\gamma(x)) = s \cdot \alpha(x) = \hat{\phi}(s \otimes x)$. Thus, there exists a unique S-module homomorphism $\widetilde{\alpha} : S \otimes_R N \to L$ such that

$$\begin{array}{ccc} N & \longrightarrow & S \otimes_R N \\ & \overset{\alpha}{\searrow} & \Big\downarrow \exists!\widetilde{\alpha} \\ & & L \end{array}$$

commutes. So we have a well-defined map

$$\begin{aligned} \operatorname{Hom}_S(S \otimes_R N, L) &\leftrightarrows \operatorname{Hom}_R(N, L) : \theta \\ \beta &\mapsto \beta \circ \gamma \\ \widetilde{\alpha} &\leftarrow\!\shortmid\, \alpha \end{aligned}$$

To show $\theta(r\alpha) = r\theta(\alpha)$, it is equivalent to show $\widetilde{r\alpha} = r \cdot \widetilde{\alpha}$. Let $s \otimes x \in S \otimes N$. Since $\widetilde{r\alpha}(s \otimes x) = s \cdot [(r\alpha)(x)] = s \cdot [r * \alpha(x)] = s[\varphi(r) \cdot \alpha(x)]$ and $(r \cdot \widetilde{\alpha})(s \otimes x) = r * [\widetilde{\alpha}(s \otimes x)] = r * [s \cdot \alpha(x)] = \varphi(r)[s \cdot \alpha(x)] = [\varphi(r) \cdot s] \cdot \alpha(x) = s[\varphi(r) \cdot \alpha(x)]$, we have $\widetilde{r\alpha} = r \cdot \widetilde{\alpha}$. Similarly, to show $\theta(\alpha + \alpha') = \theta(\alpha) + \theta(\alpha')$, it is equivalent to show $\widetilde{\alpha + \alpha'} = \widetilde{\alpha} + \widetilde{\alpha'}$. Assume $\theta(\alpha) = \theta(\alpha')$. Then $\widetilde{\alpha} = \widetilde{\alpha}'$. So $\alpha = \widetilde{\alpha} \circ \gamma = \widetilde{\alpha}' \circ \gamma = \alpha'$. Hence θ is 1-1. Let $\beta \in \operatorname{Hom}_S(S \otimes_R N, L)$. Since $S \otimes_R N$ is an S-module, $[\theta(\beta \circ \gamma)](s \otimes x) = \widetilde{\beta \circ \gamma}(s \otimes x) = s \cdot [\beta \circ \gamma(x)] = s \cdot [\beta(\gamma(x))] = s \cdot \beta(1 \otimes x) = \beta[s(1 \otimes x)] = \beta(s \otimes x)$. So $\theta(\beta \circ \gamma) = \beta$. Hence, θ is onto. □

Remark. This is a special case of "Hom-tensor adjoint".

$$\operatorname{Hom}_S(A \otimes_R B,\ C) \cong \operatorname{Hom}_R(B,\ \operatorname{Hom}_S(A, C)).$$

$$\langle \Phi(b), c \rangle = \langle b, \Phi^*(c) \rangle.$$

Let $A = S$, $B = N$ and $C = L$, then $\operatorname{Hom}_S(S \otimes_R N,\ L) \cong \operatorname{Hom}_R(N,\ \operatorname{Hom}_S(S, L)) \cong \operatorname{Hom}_R(N, L)$.

Let R, S, T, U be rings with 1.

Theorem 1.101. *Let ${}_SM_R$, ${}_RN_T$ and ${}_TP_U$. ${}_S({}_S(M \otimes_R N)_T \otimes_T P)_U$ and ${}_S(M \otimes_R {}_R(N \otimes_T P)_U)_U$ and we have an S-module isomorphism*

$$\begin{aligned} (M \otimes_R N) \otimes_T P &\xrightarrow{\cong} M \otimes (N \otimes P) \\ (a \otimes x) \otimes p &\underset{}{\overset{f}{\leftrightarrows}} a \otimes (x \otimes p) \end{aligned}$$

$$f(s\xi) = sf(\xi),$$

$$f(\xi u) = f(\xi)u.$$

Theorem 1.102. *Let M and M' be SR-bimodules. Let N and N' be RT-bimodules. Then*

$$\begin{aligned} {}_S(M \oplus M')_R \otimes_R {}_RN_T &\cong (M \otimes_R N) \oplus (M' \otimes_R N) \\ (a, a') \otimes x &\mapsto (a \otimes x, a' \otimes x) \\ (a, 0) \otimes x + (0, a') \otimes y &\leftarrow\!\shortmid\, (a \otimes x, a' \otimes y), \end{aligned}$$

Similarly, $M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N')$.

Remark. $\oplus$ and $\otimes$ behave like $+$ and $\cdot$ on ring. (element of class of modules.)

Corollary 1.103. If $\varphi : S \to R$ is homomorphism of commutative ring with identity's, then $S \otimes_R (R^n) \cong (S \otimes_R R)^n \cong S^n$.

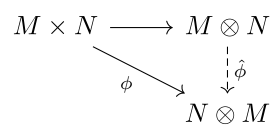
Proof. Note S_R and $R^n \cong R \oplus \cdots \oplus R$. □

Corollary 1.104. Let $R \neq 0$ be commutative ring with identity. Then $(R^m) \otimes_R (R^n) \cong (R \otimes_R (R^n))^m \cong (R^n)^m \cong R^{mn}$. A basis of R^m is $\{e_1, \ldots, e_m\}$ and a basis of R^n is $\{f_1, \ldots, f_n\}$. A basis of $R^m \otimes R^n$ is $\{e_i \otimes f_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$.

Theorem 1.105. *If R is commutative ring with identity and ${}_RM$ and ${}_RN$, then we have an R-module homomorphism $M \otimes_R N \cong N \otimes_R M$ given by*

$$a \otimes x \rightleftarrows x \otimes a$$

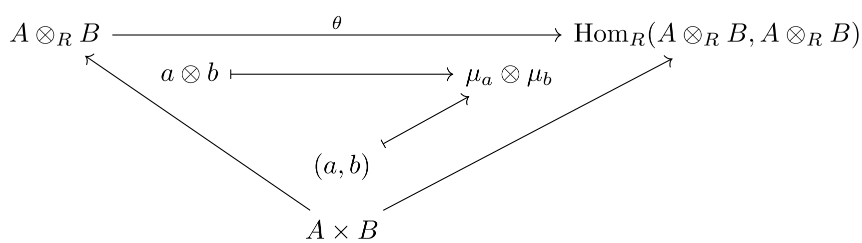
Proof. The map $\phi : M \times N \to N \otimes M$ defined by $\phi(m, n) = n \otimes m$ is R-balanced. Hence it induces a unique homomorphism $\hat{\phi}$ from $M \otimes N$ to $N \otimes M$ with $\hat{\phi}(m \otimes n) = n \otimes m$ for $m \otimes n \in M \otimes_R N$.



Similarly, we have a unique homomorphism $\hat{\varphi}$ from $N \otimes M$ to $M \otimes N$ with $\varphi(n \otimes m) = m \otimes n$ for $n \otimes m \in N \otimes M$, giving the inverse of f, and both maps are easily seen to be R-module isomorphism. □

Theorem 1.106. *Let R be a commutative ring with identity. Let A and B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') = aa' \otimes bb'$ is well-defined and makes $A \otimes_R B$ into an R-algebra.*

Proof. Define $\phi : R \to A \otimes_R B$ by $r \mapsto r \cdot (1 \otimes 1) = r \otimes 1 = 1 \otimes r = (1 \otimes 1)r$. So $\phi(R) \subseteq Z(A \otimes B)$. Let $a \in A, b \in B$ and define $\mu_a : A \to A$ by $\alpha \mapsto a\alpha$ and $\mu_b : B \to B$ by $\beta \mapsto b\beta$. Then $\mu_a \otimes \mu_b : A \otimes B \to A \otimes B$ is well-defined and R-linear. Let $\alpha \otimes \beta \in A \otimes_R B$, then $(\mu_a \otimes \mu_b)(\alpha \otimes \beta) = \mu_a(\alpha) \otimes \mu_b(\beta) = (a\alpha) \otimes (b\beta)$. So this is independent of representatives of $\alpha \otimes \beta$.



□

Let R be commutative ring with identity.

Definition 1.107. A subset $U \subseteq R$ is *multiplicatively closed* if it is closed under multiplication.

U is *multiplicatively closed*$_1$ if U is multiplicatively closed and $1 \in U$.

Example 1.108. (a) $R^\times \subseteq R$ is multiplicatively closed.

(b) $\mathrm{NZD}(R) = \{\text{non zero divisor of } R\} = \{r \in R \mid \forall s \in R : rs = 0 \Longrightarrow s = 0\}$ is multiplicatively closed$_1$ and $R^\times \subseteq \mathrm{NZD}(R)$.

(c) If U is strong multiplicatively closed, then U is multiplicatively closed and $U \subseteq \mathrm{NZD}(R)$.

(d) If $P \lneq R$ is prime, then $P \neq R$, $1 \notin P$ and for any $a, b \in R - P : ab \notin P$, i.e., $R - P$ is multiplicatively closed$_1$.

(e) If $\lambda \in \Lambda$, $U_\lambda \subseteq R$ is multiplicatively closed$_1$, then $\bigcap_{\lambda \in \Lambda} U_\lambda$ is also multiplicatively closed$_1$.

(f) If $P_\lambda \lneq R$ is prime for any $\lambda \in \Lambda$, then by De. Morgan law, $\bigcap_{\lambda\in\Lambda}(R - P_\lambda) = R - \bigcup_{\lambda\in\Lambda} P_\lambda$ is multiplicatively closed$_1$.

(g) If $U \subseteq R$ is multiplicatively closed, then $U \cup \{1\}$ is multiplicatively closed$_1$.

Remark. An ideal P of a commutative ring R is prime if and only if its complement $R - P$ is multiplicatively closed.

Let ${}_RN$ and $U \subseteq R$ be multiplicatively closed$_1$.

Definition 1.109 (Construction)**.** Define $\sim$ on $U \times N$ by $(u, x) \sim (v, y)$ if there exists $w \in U$ such that $w(uy - vx) = 0$.

Remark. If U is strongly multiplicatively closed$_1$, then this is the same relation as $uy - vx = 0$. Check this is an equivalence class.

Definition 1.110. $U^{-1}N := \frac{UN}{\sim} = \{\text{equiv classes under "}\sim\text{"}\}$, with elements $x/u = \frac{x}{u} = [(u, x)] \in U^{-1}N$, where $[(u, x)]$ is the equivalent class.

Example 1.111. Let $R = \frac{F[X,Y]}{(XY)}$ and let $x = \overline{X} \in R,\ y = \overline{Y} \in R$. By the third isomorphism theorem, $P = xR \leqslant R$ is prime. Let $y \in U := R - P$, then in $U^{-1}R$, $\frac{x}{1} = \frac{yx}{y} = \frac{0}{y} = \frac{0}{1} = 0$.

Example 1.112. Let $s \in R$ and $U = \{1, s, s^2, s^3, \cdots\}$, define $U^{-1}R =: R_s,\ U^{-1}N =: N_s$. Let $P \leqslant R$ prime and $U = R - P$, define $U^{-1}R =: R_P,\ U^{-1}N =: N_P$.

Theorem 1.113. *(a) $U^{-1}R$ is commutative ring with identity. With $r/u, s/v \in U^{-1}R$, we have $\frac{r}{u} + \frac{s}{v} = \frac{vr+us}{uv}$, $\frac{r}{u} \cdot \frac{s}{v} = \frac{rs}{uv}$, $0 = \frac{0}{1} = \frac{0}{u}$ and $1 = \frac{1}{1} = \frac{u}{u}$.*

(b) The function $\varphi : R \to U^{-1}R$ given by $r \mapsto r/1$ is a well defined homomorphism of commutative ring with identity's.

Proof. (a) Assume $\frac{r}{u} = \frac{r'}{u'}$ and $\frac{s}{v} = \frac{s'}{v'}$. Then there exist $w, w' \in U$ such that $w(ur' - u'r) = 0$ and $w'(vs' - v's) = 0$. WTS: $\frac{vr+us}{uv} = \frac{v'r'+u's'}{u'v'}$. It suffices to show $ww'\,[uv(v'r' + u's') - u'v'(vr + us)] = 0$. But LHS $= ww'uvv'r' - ww'u'v'vr + ww'uvu's' - ww'u'v'us = ww'vv'(ur' - u'r) + ww'uu'(vs' - v's) = 0 =$ RHS. So $+$ is well-defined. Similarly, we have $\cdot$ is well-defined. ☐

Theorem 1.114. *(a) $U^{-1}N$ is an R-module and a $U^{-1}R$-module. With $x/u, y/v \in U^{-1}N$ and $r/u, s/v \in U^{-1}R$, we have $\frac{x}{u} + \frac{y}{v} = \frac{vx+uy}{uv}$, $0 = \frac{0}{1} = \frac{0}{u}$, $r\frac{x}{u} = \frac{rx}{u}$ and $\frac{r}{u} \cdot \frac{s}{v} = \frac{rs}{uv}$.*

(b) $U^{-1}N$ has two R-module structures: (i) $r\frac{x}{u} = \frac{rx}{u}$. (ii) Restriction of scalar along $\varphi : R \to U^{-1}R$ defined by $\varphi(r) = r/1$, i.e., $r * \frac{x}{u}$. They are the same.

Proof. Note $r * \frac{x}{u} = \varphi(r) \cdot \frac{x}{u} = \frac{r}{1} \cdot \frac{x}{u} = r\frac{x}{u}$. Claim. $U^{-1}N = 0 \overset{(1)}{\Longleftarrow} 0 \in U \Longleftrightarrow U^{-1}R = 0$. If $0 \in U$, then $\frac{x}{u} = \frac{0 \cdot x}{0 \cdot u} = \frac{0}{0} \cdot \frac{x}{u} = 0\frac{x}{u} = \frac{0}{u} = \frac{0}{1} = 0$. If $U^{-1}R = 0$, then $\frac{1}{1} = 0 = \frac{0}{1}$. So there exists $w \in U$ such that $w = w(1 \cdot 1 - 1 \cdot 0) = 0$. Hence $0 = w \in U$. □

Remark. Converse for (1) fails in general. Let $R = \mathbb{Z}$ and $U = \{1, 7, 7^2, \cdots\}$ and $N = \mathbb{Z}/7\mathbb{Z}$. Then $7 \cdot N = 0$ and for $x \in N$ and $a \in \mathbb{Z}_{\geqslant 0}$, $U^{-1}N \ni \frac{x}{7^a} = \frac{7x}{7^{a+1}} = \frac{0}{7^{a+1}} = 0$.

Theorem 1.115.

$$
\begin{aligned}
(U^{-1}R) \otimes_R N &\overset{U^{-1}R,R}{\cong} U^{-1}N \\
\frac{r}{u} \otimes x &\mapsto \frac{rx}{u} \\
\frac{1}{u} \otimes x &\leftarrow\!\shortmid \frac{x}{u} = \frac{1 \cdot x}{u}
\end{aligned}
$$

Proof. By UMP, there exists $\Phi : (U^{-1}R) \otimes_R N \xrightarrow{\cong} U^{-1}N$ given by $\frac{r}{u} \otimes x \mapsto \frac{rx}{u}$, which is onto. Since R is commutative, Φ is an R-module homomorphism. We have shown in homework that the element of $(U^{-1}R) \otimes_R N$ is of the form $\frac{r}{u} \otimes x$. Suppose $\phi\left(\frac{r}{u} \otimes x\right) = 0$. Then $\frac{rx}{u} = 0 = \frac{0}{1}$. So there exists $v \in U$ such that $v \cdot rx = 0$. Then $\frac{r}{u} \otimes x = \frac{vr}{vu} \otimes x = \frac{1}{vu} \otimes vrx = \frac{1}{vu} \otimes 0 = 0$. So Φ is 1-1. Hence $\Phi^{-1}\left(\frac{x}{u}\right) = \frac{1}{u} \otimes x$. Since $\Phi\left(\frac{r}{u}\left(\frac{s}{v} \otimes x\right)\right) = \Phi\left(\left(\frac{r}{u} \cdot \frac{s}{v}\right) \otimes x\right) = \Phi\left(\frac{rs}{uv} \otimes x\right) = \frac{rsx}{uv} = \frac{r}{u}\frac{sx}{v} = \frac{r}{u}\Phi\left(\frac{s}{v} \otimes x\right)$, we have Φ is $U^{-1}R$ linear. □

Definition 1.116 ("Functor")**.** Let R and S be commutative ring with identity. "A functor from the category of R-modules" to the category of S-modules is a rule of assignment $\mathcal{F}$ such that for any R-module N, $\mathcal{F}(N)$ is an S-module and for any R-module homomorphism $\phi : M \to N$, $\mathcal{F}(\phi) : \mathcal{F}(M) \to \mathcal{F}(N)$ is an S-module and $\mathcal{F}(\phi \circ \psi) = \mathcal{F}(\phi) \circ \mathcal{F}(\psi)$ and $\mathcal{F}(id_N) = id_{\mathcal{F}(N)}$.

Example 1.117. If $\varphi : R \to S$ is a ring homomorphism, then

(a) $\left.\begin{array}{ll} \mathcal{F}(N): & S \otimes_R N \\ \mathcal{F}(\phi): & S \otimes \phi \end{array}\right\} \mathcal{F} = S \otimes_R -functor;$

(b) restriction of scalars gives from category of S-modules to category of R-modules. $\mathcal{G}(N) = U^{-1}N$ is a functor from category of R-mods to category of $U^{-1}R$-modules.

Chapter 2

Introduction to Homological Algebra

Let R is commutative ring with identity. When we say a homomorphism, we mean it is a R-module homomorphism.

2.1 Exact Sequences

How to understand R-modules ? "understand" $R^n = \left\{ \begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \middle| \, r_1, \ldots, r_n \in R \right\}$.

More generally, $R^{(\Lambda)}$ is a free R-module with a basis Λ. More generally, via generators and relations.

Example 2.1. Let $R = k[X,Y]/(X^2, Y^3)$ and $x = \overline{X}, y = \overline{Y} \in R$. Let $M = \langle x, y \rangle \leqslant R$. The generators are: $\{x, y\}$ and relations are: $x \cdot x = 0$, $y^2 \cdot y = 0$. These relations generate all the relations. Define $R^2 \xrightarrow{\tau} M$ by $e_1 \mapsto x$ and $e_2 \mapsto y$. There exists a unique τ such that $\tau(e_1) = x$ and $\tau(e_2) = y$ by UMP for free modules. τ is onto with $\mathrm{Ker}(\tau) = \langle xe_1, y^2e_2 \rangle$. So $M \cong R^2/\langle xe_1, y^2e_2 \rangle$. There exists more i, i.e., relations on the relations $x \cdot xe_1 = 0$, $y \cdot y^2e_2 = 0$. Note $\mathrm{Ker}(\tau) \cong R^2/\langle xf_1, yf_2 \rangle$, where $f_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $f_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Encode this, using homomorphism.

$$\mathrm{Im} \left(R^2 \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & y^2 \end{pmatrix}} R^2 \right) = \langle xe_1, y^2e_2 \rangle = \mathrm{Ker}(\tau) \subseteq R^2,$$

where image is span of columns. $\operatorname{Im}\left(R^2 \xrightarrow[\tau]{(x,y)} R\right) = \langle x, y\rangle = M \subseteq R$.

$$\operatorname{Ker}\left(R^2 \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & y^2 \end{pmatrix}} R^2\right) = \operatorname{Im}\left(R^2 \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}} R^2\right) = \langle xf_1, yf_2\rangle \subseteq R^2.$$

We see the sequence

$$R^2 \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}} R^2 \xrightarrow{\begin{pmatrix} x & 0 \\ 0 & y^2 \end{pmatrix}} R^2 \xrightarrow[\tau]{(x,y)} M \xrightarrow{0} 0.$$

In most of examples we began first with a given B and then determined some of its basic properties by constructing a homomorphism φ (often given implicity by the specification of $\operatorname{Ker}\varphi \subseteq B$) and examining both $\operatorname{Ker}\varphi$ and the resulting quotient $B/\operatorname{Ker}\varphi$.

We now consider in some greater detail the reverse situation, namely whether we may first specify the "smaller constiuents". More precisely, we consider whether, given two modules A and C, there exists a module B containing (an isomorphic copy of) A such that the resulting quotient module B/A is isomorphic to C in which case B is said to be an extension of C by A. It is then natural to ask how many such B exist for a given A and C, and the extent to which properties of B are determined by the corresponding properties of A and C.

To say that A is isomorphic to a submodule of B, is to say that there is an injective homomorphism $\psi : A \to B$, so then $A \cong \psi(A) \subseteq B$. To say that C is isomorphic to the resulting quotient is to say that there is a surjective homomorphism $\varphi : B \to C$ with $\operatorname{Ker}\varphi = \psi(A)$. In particular this gives us a pair of homomorphisms: $A \xrightarrow{\psi} B \xrightarrow{\varphi} C$ with $\operatorname{Im}(\psi) = \operatorname{Ker}\varphi$.

Definition 2.2. A sequence $A \xrightarrow{f} B \xrightarrow{g} C$ of R-module homomorphism is *exact* if $\operatorname{Im}(f) = \operatorname{Ker}(g)$.

More generally,

$$\cdots \xrightarrow{d_{i+1}} X_i \xrightarrow{d_i} X_{i-1} \xrightarrow{d_{i-1}} \cdots$$

sequence of R-module homomorphism is *exact* if $\operatorname{Im}(d_{i+1}) = \operatorname{Ker}(d_i)$ for $i \in \mathbb{Z}$.

Remark. $\operatorname{Im}(f) \subseteq \operatorname{Ker}(g)$ if and only if $g \circ f = 0$.

Example 2.3. If $A = B/C$, then

$$C \xrightarrow[i]{\subseteq} B \xrightarrow{\tau} A = B/C$$

is exact since $\operatorname{Ker}(\tau) = C = \operatorname{Im}(i)$. We have

$$0 \to C \xrightarrow[i]{\subseteq} B \xrightarrow{\tau} A = B/C \to 0$$

is also exact.

Example 2.4. If $\phi : X \to Y$ is an R-module homomorphism, then the sequence

$$0 \to \operatorname{Ker}(\phi) \xrightarrow[j]{\subseteq} X \xrightarrow{\phi} Y \xrightarrow[\pi]{\text{nat. proj.}} Y/\operatorname{Im}(\phi) \to 0$$

is exact, where $\operatorname{Coker}(\phi) = Y/\operatorname{Im}(\phi)$ is the cokernel of ϕ.

Proposition 2.5. (a) A sequence of R-module homomorphism $0 \to U \xrightarrow{\alpha} V$ is exact if and only if α is 1-1.

(b) $V \xrightarrow{\beta} W \to 0$ is exact if and only if β is onto.

(c) $0 \to U \xrightarrow{\alpha} V \xrightarrow{\beta} W \to 0$ is exact if and only if α is 1-1, β is onto and $\operatorname{Im}(\alpha) = \operatorname{Ker}(\beta)$.

Definition 2.6. A *short exact sequence (SES)* is an exact sequence of form

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

Remark. SES: extension of "W by U".

Remark. Any exact sequence can be written as a succession of short exact sequences since to say $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact at Y is the same as saying that the sequence

$$0 \to \alpha(X) \xrightarrow{\subseteq} Y \xrightarrow{\pi} Y/\operatorname{Ker}(\beta) \to 0$$

is a short exact sequence.

Example 2.7. Note

$$\begin{aligned} 0 \to U \xrightarrow{\epsilon} U \oplus W &\xrightarrow{\rho} W \to 0 \\ u \mapsto (u, 0)& \\ (u, w) &\mapsto w \end{aligned}$$

is a "trivial" SES. In particular, it follows that there always exists at least one extension of C by A.

A special case, consider two $\mathbb{Z}$-modules $U = \mathbb{Z}$ and $W = \mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{Z}$. Then

$$0 \to \mathbb{Z} \xrightarrow{\epsilon} \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \xrightarrow{\rho} \mathbb{Z}/n\mathbb{Z} \to 0$$

gives one extension of $\mathbb{Z}/n\mathbb{Z}$ by $\mathbb{Z}$.

Example 2.8. Another extension of $\mathbb{Z}/n\mathbb{Z}$ with $n \in \mathbb{Z}$ by $\mathbb{Z}$ is given by the SES

$$0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0,$$

$n(x) = nx$ for $x \in \mathbb{Z}$ and π is the natural projection.

Note $\mathbb{Z} \ncong \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ since in $\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, $(0, \bar{1})$ is annihilated by n, but $\mathbb{Z}$ has no such element.

Example 2.9. If $\varphi : B \to C$ is is a homomorphism, we may form an exact sequence

$$0 \to \operatorname{Ker}(\varphi) \xrightarrow{\subseteq} B \xrightarrow{\varphi} \operatorname{Im}(\varphi) \to 0.$$

If φ is onto, $0 \to \operatorname{Ker}(\varphi) \xrightarrow{\subseteq} B \xrightarrow{\varphi} C \to 0$ is a SES.

For a fixed A and C, in general there may be several extensions of C by A. To distinguish different extensions we define the notion of a homomorphism (and isomorphism) between two exact sequences.

Definition 2.10. A *homomorphism of SES's* is a triple α, β, γ of module homomorphism such that the following diagram commutes:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0
\end{array}$$

Furthermore, this homomorphism is an isomorphism if α, β, γ are all isomorphisms, in which case the extensions B and B' are said to be isomorphic extensions.

This is an equivalence of SES if $A = A'$, $C = C'$, $\alpha = \mathrm{id}_A$ and $\gamma = \mathrm{id}_C$. Note β must be an isomorphism by the following short five lemma. In this case the corresponding extensions B and B' are said to be equivalent extensions of C.

Example 2.11. (a) Let $k, n \in \mathbb{Z}$.

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{n} & \mathbb{Z} & \xrightarrow{\pi} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle =} & & \\
0 & \longrightarrow & \mathbb{Z}/k\mathbb{Z} & \xrightarrow{n} & \mathbb{Z}/nk\mathbb{Z} & \xrightarrow{\tau} & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0
\end{array}$$

where p, q are the natural projections, n below maps $(a \bmod k)$ to $(na \bmod nk)$, and τ is the natural projection of $\mathbb{Z}/nk\mathbb{Z}$ onto its quotient $(\mathbb{Z}/nk\mathbb{Z})/(n\mathbb{Z}/nk\mathbb{Z})$. One easily check that this is a homomorphism of short exact sequences but not isomorphic.

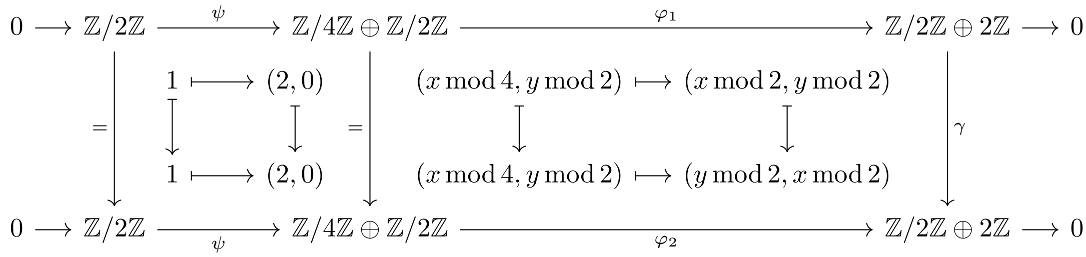
(b) Let $0 \to \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/n\mathbb{Z} \to 0$ be the short exact sequence of $\mathbb{Z}$-module. Map each module to itself by $x \mapsto -x$, then this triple of homomorphisms gives an isomorphism of the exact sequence with itself.

(c) Consider the maps

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow{\varphi} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\
 & & & x \longmapsto (x,0) & & (x,y) \longmapsto y & & & \\
 & & {\scriptstyle =}\downarrow & \downarrow \quad\quad \downarrow & \downarrow{\scriptstyle \beta} & \downarrow \quad\quad \downarrow & \downarrow{\scriptstyle =} & & \\
 & & & x \longmapsto (0,x) & & (y,x) \longmapsto y & & & \\
0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \xrightarrow[\phi']{} & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & \xrightarrow[\varphi']{} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0
\end{array}$$

Then this diagram is seen to commute, hence giving an equivalence of the two exact sequences.

(d) We exhibit two isomorphic but inequivalent $\mathbb{Z}$-module extensions.



Suppose it is an equivalent extension. Since $\varphi_1(0,1) = (0,1)$, any equivalence $=, \beta, =$ from the first sequence to the second must map $(0,1) \in \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ to either $(1,0)$ or $(3,0)$ in $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, since these are the two possible elements mapping to $(0,1)$ by φ_2. This is impossible, however, since the isomorphism β cannot send an element of order 2 to an element of order 4.

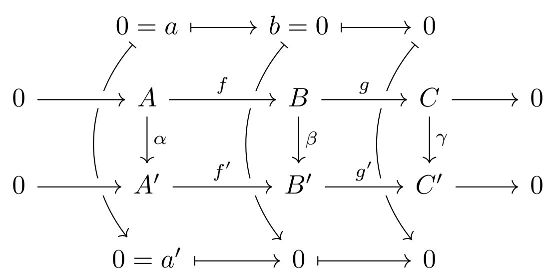
Theorem 2.12 (The short five lemma)**.** *Let α, β, γ be a homomorphism of short exact sequences.*

(a) If α and γ are 1-1, then β is 1-1.

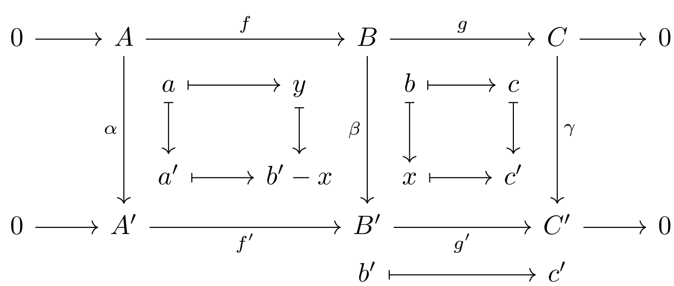
(b) If α and γ are onto, then β is onto.

(c) If α and γ are isomorphisms, then β is an isomorhism.

Proof. (b) Consider a homomorphism of SES. Start with $b = 0$.



Assume α and γ is onto. Start with $b' \in B'$.



Let $g'(b') = c'$. Since γ and g are onto, we can assume $\gamma(c) = c'$ and $g(b) = c$. Assume $\beta(b) = x$. Since the right diagram commutes, $g'(x) = c'$. Since g' is a homomorphism, $g'(b' - x) = c' - c' = 0$, i.e., $b' - x \in \operatorname{Ker}(g') = \operatorname{Im}(f')$. So there exists $a' \in A'$ such that $f'(a') = b' - x$. Since α and f are onto, we can assume $\alpha(a) = a' \in A'$ and $f(a) = y \in B$. Since the left diagram commutes, $\beta(y) = b' - x$. So $\beta(y + b) = \beta(y) + \beta(b) = b' - x + x = b'$. Thus, β is onto. ☐

Remark. It is an easy exercise to see that composition of homomorphisms of short exact sequence is also a homomorphism. Likewise, if the triple α, β, γ is an isomorphism (or equivalence) then $\alpha^{-1}, \beta^{-1}, \gamma^{-1}$ is an isomorphism (equivalence, respectively) in the reverse direction. It follows that "isomorphism" (or equivalence) is an equivalence relation on any set of short exact sequences.

Definition 2.13. A SES $L = (0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0)$ is *split* if and only if it is equivalent to $0 \to A \xrightarrow{\epsilon} A \oplus C \xrightarrow{\rho} C \to 0$, i.e., if and only if there exists a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {=}\downarrow\uparrow{=} & & \beta\downarrow\uparrow\beta^{-1} & & {=}\downarrow\uparrow{=} & & \\ 0 & \longrightarrow & A & \underset{\epsilon}{\overset{\rho'}{\leftrightarrows}} & A\oplus C & \underset{\rho}{\overset{\epsilon'}{\leftrightarrows}} & C & \longrightarrow & 0 \end{array}$$

So β is an isomorphism and then $B \cong A \oplus C$.

Theorem 2.14. *Given a SES $\zeta = (0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0)$. The followings are equivalent.*

(i) ζ splits.

(ii) ζ splits on the left, i.e., there exists a homomorphism $h : B \to A$ such that $h \circ f = \mathrm{id}_A$.

$$0 \longrightarrow A \underset{h}{\overset{f}{\rightleftarrows}} B$$

(iii) ζ splits on the right, i.e., there exists a homomorphism $k : C \to B$ such that $g \circ k = \mathrm{id}_C$.

$$B \underset{k}{\overset{g}{\rightleftarrows}} C \longrightarrow 0.$$

(iv) There exists a submodule $C' \subseteq B$ such that $B = f(A) \oplus C'$.

Proof. "(i)$\Longrightarrow$(ii)". Assume ζ splits. Then there exists a commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & {=}\downarrow\uparrow{=} & & \beta\downarrow\uparrow\beta^{-1} & & {=}\downarrow\uparrow{=} & & \\ 0 & \longrightarrow & A & \underset{\epsilon}{\overset{\rho'}{\leftrightarrows}} & A\oplus C & \underset{\rho}{\overset{\epsilon'}{\leftrightarrows}} & C & \longrightarrow & 0 \end{array}$$

Set $h = \rho' \circ \beta : B \to A$. Then $h \circ f = \rho' \circ \beta \circ f = \rho' \circ \epsilon = \mathrm{id}_A$.

"(i)$\Longrightarrow$(iii)". Similarly, use $k = \beta^{-1} \circ \epsilon'$.

"(iii)$\Longrightarrow$(i)". Assume there exists $k : C \to B$ such that $g \circ k = \mathrm{id}_C$. Define $\delta : A \oplus C \to B$ by $(a, c) \mapsto f(a) + k(c)$. By homework 6#1 from MATH8520, δ is a homomorphism and the following diagram commutes.

$$\begin{array}{ccccc} A & \xrightarrow{\epsilon} & A\oplus C & \xleftarrow{\epsilon'} & C \\ & {\scriptstyle f}\searrow & \downarrow{\scriptstyle\delta} & \swarrow{\scriptstyle k} & \\ & & B & & \end{array}$$

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & A & \xrightarrow{\quad f \quad} & B & \xrightarrow{\quad g \quad} & C & \longrightarrow & 0 \\
 & & \Big\uparrow {\scriptstyle =} & \begin{array}{ccc} a & \longmapsto & f(a) \\ \uparrow & & \uparrow \\ a & \longmapsto & (a,0) \end{array} & \Big\uparrow {\scriptstyle \delta} & \begin{array}{ccc} f(a)+k(c) & \longmapsto & c \\ \uparrow & & \uparrow \\ (a,c) & \longmapsto & c \end{array} & \Big\uparrow {\scriptstyle =} & & \\
0 & \longrightarrow & A & \xrightarrow[\quad \epsilon \quad]{} & A \oplus C & \xrightarrow[\quad \rho \quad]{} & C & \longrightarrow & 0
\end{array}
$$

Then by the short five lemma, δ is an isomorphism. Check: $\beta = \delta^{-1}$ makes the diagram in the definition of the splitting commute.

"(ii)$\Longrightarrow$(i)". Similarly. Define $\beta(b) = (h(b), g(b))$.

"(ii)$\Longrightarrow$(iv)". Assume there exists homomorphism $h : B \to A$ such that $h \circ f = \mathrm{id}_A$. Claim. $B = f(A) \oplus C'$. Let $x \in f(A) \cap \mathrm{Ker}(h)$. Then there exists $a \in A$ such that $x = f(a) \in \mathrm{Ker}(h)$. So $0 = h(x) = h(f(a)) = \mathrm{id}_A(a) = a$. Hence $x = f(a) = 0$. Next, let $b \in B$. Then $h(b - f(h(b))) = h(b) - (h \circ f)(h(b)) = h(b) - h(b) = 0$. So $b = f(h(b)) + c \in f(A) + \mathrm{Ker}(h)$ for some $c \in \mathrm{Ker}(h)$.

"(iv)$\Longrightarrow$(ii)". Assume $B = f(A) \oplus C'$ for some $C' \subseteq B$. Let $b \in B$. Since f is 1-1, there exists a unique $x \in f(A)$ and $c' \in C'$ such that $b = x + c'$. Since f is 1-1, there exists a unique $a \in A$ such that $f(a) = x$. Define $h(b) = h(f(a) + c') := a$. By construction, since $f(a) \in f(A)$ and $0 \in C$, $h(f(a)) = h(f(a) + 0) = a$. Hence $h \circ f = \mathrm{id}_A$. Let $h(b) = a$ and $h(b_1) = a_1$ with $b = f(a) + c'$ and $b_1 = f(a_1) + c'_1$. Then $b + b_1 = f(a) + f(a_1) + c' + c'_1 = f(a + a_1) + c' + c'_1$. So $h(b + b_1) = a + a_1 = h(b) + h(b_1)$. Let $r \in R$. Then $rb = f(ra) + rc'$. So $h(rb) = ra = r \cdot h(b)$. Hence h is a homomorphism. □

Example 2.15. $\zeta = (0 \to \mathbb{Z}/2\mathbb{Z} \xrightarrow{2} \mathbb{Z}/4\mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \to 0)$ is exact but not split since $\mathbb{Z}/4\mathbb{Z} \ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Set $M = \oplus_{i=1}^{\infty}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}) = \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \cdots \cong \mathbb{Z}_4 \oplus (\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \cdots) = \mathbb{Z}_4 \oplus M$. Then $\mathbb{Z}_2 \oplus M \cong M \cong \mathbb{Z}_4 \oplus M$. Consider

$$
\begin{array}{lllll}
0 \to \mathbb{Z}_2 & \xrightarrow{(2,0)} & \mathbb{Z}_4 \oplus M & \xrightarrow{\begin{pmatrix} \pi & 0 \\ 0 & 1 \end{pmatrix}} & \mathbb{Z}_2 \oplus M \to 0. \\
\quad a & \longrightarrow & (2a, 0) & & \\
 & & (b, c) & \longrightarrow & (\pi(b), c).
\end{array}
$$

Although $B := \mathbb{Z}_4 \oplus M \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \cdots \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \cdots \cong \mathbb{Z}_2 \oplus (\mathbb{Z}_2 \oplus M) =: A \oplus C$, we can check this is exact but not split. Suppose ζ split on the left, then there exists $h : \mathbb{Z}_4 \oplus M \to \mathbb{Z}_2$ such that $h \circ (2, 0) = \mathrm{id}_{\mathbb{Z}_2}$. By homework 6 Exercise #1, we have $h(a, b) = h_1(a) + h_2(b)$. Then $a = h((2, 0)(a)) = h(2a, 0) = h_1(2a) + h_2(0) = h_1(2a)$, a contradiction since we cannot find a homomorphism sending 2 to 1.

Theorem 2.16. *Let*

$$
\zeta = (0 \longrightarrow A \xrightarrow{\ f\ } B \underset{\overset{\curvearrowleft}{k}}{\xrightarrow{\ g\ }} C \longrightarrow 0)
$$

be a SES such that C is free with a basis Λ. Then ζ splits.

Proof. UMP for free modules $C \to B$ demonstrates right-splitting (where to send basis). Since g is onto, for $\lambda \in \Lambda$, there exists $b_\lambda \in B$ such that $g(b_\lambda) = \lambda$ for $\lambda \in \Lambda$. Define $k : C \to B$ to be the unique R-module homomorphism such that $k(\lambda) = b_\lambda$ for $\lambda \in \Lambda$. Let $\sum_{\lambda\in\Lambda}^{\text{finite}} a_\lambda \lambda \in C$. Since $g\left(k\left(\sum_{\lambda}^{\text{finite}} a_\lambda \lambda\right)\right) = \sum_{\lambda}^{\text{finite}} a_\lambda g\left(k(\lambda)\right) = \sum_{\lambda}^{\text{finite}} a_\lambda g(b_\lambda) = \sum_{\lambda}^{\text{finite}} a_\lambda \lambda$, we have $g \circ k = \mathrm{id}_C$. $\square$

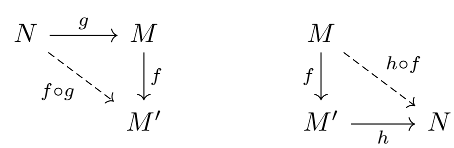
2.2 Functor

Let M, N be R-modules.

Theorem 2.17 (Functor)**.** *Let $f : M \to M'$ be an R-module homomorphism and N be an R-module. Then there exist R-module homomorphisms*

$$\begin{aligned} f_* = \mathrm{Hom}_R(N, f) : \mathrm{Hom}_R(N, M) &\to \mathrm{Hom}_R(N, M') \\ g &\mapsto f \circ g \end{aligned}$$

$$\begin{aligned} f^* = \mathrm{Hom}_R(f, N) : \mathrm{Hom}_R(M', N) &\to \mathrm{Hom}_R(M, N) \\ h &\mapsto h \circ f \end{aligned}$$



Example 2.18. Let M and N be R-modules and $r \in R$. Define $f : M \xrightarrow{r} M$ by $m \mapsto rm$. Note

$$\begin{aligned} f_* : \mathrm{Hom}_R(N, M) &\xrightarrow{r} \mathrm{Hom}_R(N, M') \\ g &\mapsto f \circ g = r \cdot g \end{aligned}$$

Then $f\left(g(x)\right) = r \cdot g(x) = (rg)(x)$ for $x \in N$. Note

$$\begin{aligned} f^* : \mathrm{Hom}_R(M', N) &\xrightarrow{r} \mathrm{Hom}_R(M, N) \\ h &\mapsto h \circ f = r \cdot h \end{aligned}$$

Then $h\left(f(x)\right) = h(rx) = r \cdot h(x) = (rh)(x)$ for $x \in M$.

Notation 2.19.

$$(-)_* : \text{preserves order.}$$

$$(-)^* : \text{reverses order.}$$

Theorem 2.20. *Let $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ be R-module homomorphism and N be an R-module. The operations $(-)_* = \mathrm{Hom}_R(N, -)$ and $(-)^* = \mathrm{Hom}_R(-, N)$ are functors, where input and output are R-module homomorphism, and respects to identities and compositions.*

$$\begin{aligned} (\beta \circ \alpha)_* &= \beta_* \circ \alpha_* : \text{“covariant”} \\ (\beta \circ \alpha)^* &= \alpha^* \circ \beta^* : \text{“contracovariant”} \end{aligned}$$

Proof. Note

$$\begin{aligned} \alpha^* : \mathrm{Hom}_R(B, N) &\to \mathrm{Hom}_R(A, N) \\ h &\mapsto h \circ \alpha \end{aligned}$$

Let $r \in R$ and $h, k \in \mathrm{Hom}_R(B, N)$. Then $\alpha^*(h+k) = (h+k)\circ\alpha = (h\circ\alpha)+(k\circ\alpha) = \alpha^*(h)+\alpha^*(k)$. To show $\alpha^*(rh) = r\alpha^*(h)$, we need to show: $(rh)\alpha = r(h\circ\alpha)$, it is obvious since $(rh)\alpha(x) = r \cdot h(\alpha(x))$. So α^* is an R-module homomorphism. Note $(\beta \circ \alpha)^*(h) = h \circ (\beta \circ \alpha) = (h \circ \beta) \circ \alpha = \alpha^*(h \circ \beta) = \alpha^*(\beta^*(h)) = (\alpha^* \circ \beta^*)(h)$. Diagrammatically, we have the following commutative diagrams

$$\begin{array}{ccc} A & \xrightarrow{\alpha} & B \\ & {}_{\gamma}\searrow & \downarrow{\scriptstyle \beta} \\ & & C \end{array}$$

$$(-)_* \qquad \begin{array}{ccc} \mathrm{Hom}_R(N, A) & \xrightarrow{\alpha_*} & \mathrm{Hom}_R(N, B) \\ & {}^{\gamma_*}\searrow & \downarrow{\scriptstyle \beta_*} \\ & & \mathrm{Hom}_R(N, C) \end{array}$$

$$(-)^* \qquad \begin{array}{ccc} \mathrm{Hom}_R(A, N) & \xleftarrow{\alpha^*} & \mathrm{Hom}_R(B, N) \\ & {}_{\gamma^*}\nwarrow & \uparrow{\scriptstyle \beta^*} \\ & & \mathrm{Hom}_R(C, N) \end{array}$$

□

Example 2.21. $\mathrm{Hom}_R(R, -) \cong (-)$. "natural isomorphism.", "isomorphism of functors", i.e., for an R-module A,

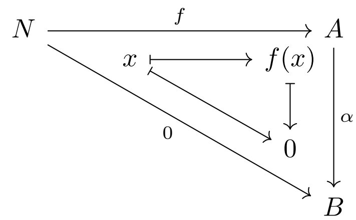
$$\begin{aligned} \mathrm{Hom}_R(R, A) &\cong A \\ \psi &\mapsto \psi(1) \end{aligned}$$

Let $\alpha : A \to B$.

$$\begin{array}{ccccc} \mathrm{Hom}_R(R, A) & & \xrightarrow{\quad\cong\quad} & & A \\ & \psi & \longmapsto & \psi(1) & \\ \alpha^* \Big\downarrow & \downarrow & & \downarrow & \Big\downarrow \alpha \\ & \alpha \circ \psi & \longmapsto & \alpha(\psi(1)) & \\ \mathrm{Hom}_R(R, B) & & \xrightarrow[\quad\cong\quad]{} & & B \end{array}$$

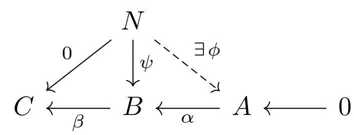
Theorem 2.22 (Left exactness of Hom., I)**.** *Given exact sequence* $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$. *Then the induced sequence* $0 \to \mathrm{Hom}(N, A) \xrightarrow{\alpha_*} \mathrm{Hom}(N, B) \xrightarrow{\beta_*} (N, C)$ *is exact.*

Proof. Let $f \in \mathrm{Ker}(\alpha_*)$. Then $\alpha_*(f) = \alpha \circ f = 0$. So from N to B, it is a 0 map by commutativity.



Since α is 1-1, we have $f(x) = 0$ for all $x \in N$, i.e., $f = 0$. Hence α^* is 1-1.

Since $\beta_* \circ \alpha_* = (\beta \circ \alpha)_* = 0_* = 0$, $\text{Im}(\alpha_*) \subseteq \text{Ker}(\beta_*)$. Let $\psi \in \text{Ker}(\beta_*)$. Then $0 = \beta_*(\psi) = \beta \circ \psi$, So $\text{Im}(\psi) \subseteq \text{Ker}(\beta) = \text{Im}(\alpha)$. Also, since α is 1-1, for $x \in N$, there exists a unique $a_x \in A$ such that $\alpha(a_x) = \psi(x)$. Define $\phi : N \to A$ by $\phi(x) = a_x$. Then $\alpha(\phi(x)) = \alpha(a_x) = \psi(x)$ for $x \in N$. So $\psi = \alpha \circ \phi = \alpha_*(\phi)$. Besides, we can show ϕ is a homomorphism using lifting argument as before. Hence $\psi \in \text{Im}(\alpha_*)$. Thus, $\text{Im}(\alpha_*) \supseteq \text{Ker}(\beta_*)$.



□

Example 2.23 (Hom. not short exact, I)**.** Let $\varphi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the natural projection. Use $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, -)$. Then $\varphi_* : \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) \to \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$. Let $\psi \in \text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z})$. Then $2\psi(1) = \psi(2 \cdot 1) = \psi(0) = 0$. Since $\mathbb{Z}$ is an integral domain, $\psi(1) = 0$. Hence $\psi = 0$. Moreover, since $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, φ_* is not onto.

Definition 2.24. Fix an element $r \in R$. Let $\mu_r^M : M \to M$ be given by $m \to rm$. Such a "multiplication-map" is a *homothety.*

Proposition 2.25. For $r, s \in R$,
$$\mu_r^M \otimes_R \mu_s^N = \mu_{rs}^{M \otimes_R N}.$$
In particular, $\mu_r^M \otimes_R N = \mu_r^{M \otimes_R N}$.

Proof. Let $m \otimes_R n \in M \otimes_R N$. Then
$$(\mu_r^M \otimes_R \mu_s^N)(m \otimes_R n) = \mu_r^M(m) \otimes_R \mu_s^N(n) = (rm) \otimes_R (sn) = (rs)(m \otimes_R n) = \mu_{rs}^{M \otimes_R N}(m \otimes_R n).$$
In particular,
$$\mu_r^M \otimes_R N = \mu_r^M \otimes_R \text{id}_N = \mu_r^M \otimes_R \mu_1^N = \mu_r^{M \otimes_R N}.$$
□

Example 2.26 (Hom. not short exact, I)**.** Let $\mu_2^{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}$ be a homothety. Use $(-) \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$. Then $\mu_2^{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = \mu_2^{\mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}} : \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z}$ is the zero map because $\mu_2^{\mathbb{Z}/2\mathbb{Z}} : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is the zero map.

Let $\text{Hom}(-, *)$ denote all R-module homomorphisms from $-$ to $*$.

Theorem 2.27. *Given the SES* $\zeta = \left(0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0\right)$, *then following are equivalent.*

(i) ζ *is split.*

(ii) For R-module N, the induced sequence $0 \to \operatorname{Hom}(N, A) \xrightarrow{\alpha_*} \operatorname{Hom}(N, B) \xrightarrow{\beta_*} \operatorname{Hom}(N, C) \to 0$ *is exact.*

(iii) The sequence $0 \to \operatorname{Hom}(C, A) \xrightarrow{\alpha_*} \operatorname{Hom}(C, B) \xrightarrow{\beta_*} \operatorname{Hom}(C, C) \to 0$ *is exact.*

(iv) For R-module N, $\beta_* : \operatorname{Hom}(N, B) \to \operatorname{Hom}(N, C)$ *is onto.*

(v) $\beta_* : \operatorname{Hom}(C, B) \to \operatorname{Hom}(C, C)$ *is onto.*

Proof. We have proved

$$\begin{array}{ccc} (ii) & \Longleftrightarrow & (iv) \\ \Downarrow & & \Downarrow \\ (iii) & \Longleftrightarrow & (v) \end{array}$$

"(i)$\Longrightarrow$(iv)". Assume ζ splits. Then there exists $\gamma : C \to B$ such that $\beta \circ \gamma = \mathrm{id}_C$.

$$\begin{array}{ccc} C & \xrightarrow{\gamma} & B \\ & \searrow^{\mathrm{id}_C} & \downarrow \beta \\ & & C \end{array}$$

Use $\operatorname{Hom}(N, -)$.

$$\begin{array}{ccc} \operatorname{Hom}(N, C) & \xrightarrow{\gamma_*} & \operatorname{Hom}(N, B) \\ \delta & \longmapsto & \gamma_*(\delta) \\ & \searrow^{\mathrm{id}} & \downarrow \beta_* \\ & & \delta \\ & & \operatorname{Hom}(N, C) \end{array}$$

Note $\beta_*\left(\gamma_*(\delta)\right) = (\beta \circ \gamma)_*(\delta) = \mathrm{id}_*(\delta) = \mathrm{id} \circ \delta = \delta$ for $\delta \in \operatorname{Hom}(N, C)$. So β_* is onto.

"$(v) \Longrightarrow (i)$". Assume β_* is onto. Then there exists $\delta \in \operatorname{Hom}(C, B)$ such that $\mathrm{id}_C = \beta_*(\delta) = \beta \circ \delta$. So ζ splits on the right, and hence splits. $\square$

Theorem 2.28 (left exactness of Hom. II)**.** *Let* $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ *be exact. Then the induced sequence* $0 \to \operatorname{Hom}(C, N) \xrightarrow{\beta^*} \operatorname{Hom}(B, N) \xrightarrow{\alpha^*} \operatorname{Hom}(A, N)$ *is exact.*

Example 2.29 (Hom. not short exact, II)**.** Since α^* is not necessarily onto, we have

$$0 \to \operatorname{Hom}(C, N) \xrightarrow{\beta^*} \operatorname{Hom}(B, N) \xrightarrow{\alpha^*} \operatorname{Hom}(A, N) \to 0$$

may not be a SES.

Theorem 2.30. *Given the SES* $\zeta = \left(0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0\right)$*, then the following are equivalent.*

(a) ζ is split.

(b) For R-module N, the induced sequence $0 \to \mathrm{Hom}(C,N) \xrightarrow{\beta^*} \mathrm{Hom}(B,N) \xrightarrow{\alpha^*} \mathrm{Hom}(A,N) \to 0$ *is exact.*

(c) The sequence $0 \to \mathrm{Hom}(C,C) \xrightarrow{\beta^*} \mathrm{Hom}(B,C) \xrightarrow{\alpha^*} \mathrm{Hom}(A,C) \to 0$ *is exact.*

(d) For R-module N, $\alpha^* : \mathrm{Hom}(B,N) \to \mathrm{Hom}(A,N)$ *is onto.*

(e) $\alpha^* : \mathrm{Hom}(B,C) \to \mathrm{Hom}(A,C)$ *is onto.*

Proof. It is similar. □

Theorem 2.31. *Let $_RN$. The followings are equivalent.*

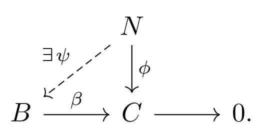
(i) $\mathrm{Hom}_R(N,-)$ *transforms epimorphisms into epimorphisms.*

(ii) $\mathrm{Hom}_R(N,-)$ *transforms SES's into SES's.*

(iii) $\mathrm{Hom}_R(N,-)$ *transforms exact sequences into exact sequences.*

(iv) Every SES $0 \to A \to B \to N \to 0$ *splits.*

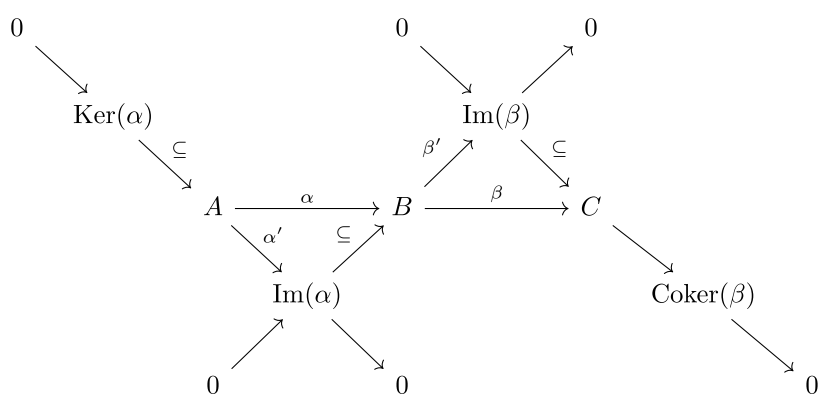
(v) For R-modules B and C, if $B \xrightarrow{\beta} C \to 0$ *is exact, then every R-module homomorphism from N to C lifts to an R-module homomorphism into B, i.e., give* $\phi \in \mathrm{Hom}_R(N,C)$*, there is a lift* $\psi \in \mathrm{Hom}_R(N,B)$ *making the following diagram commute:*



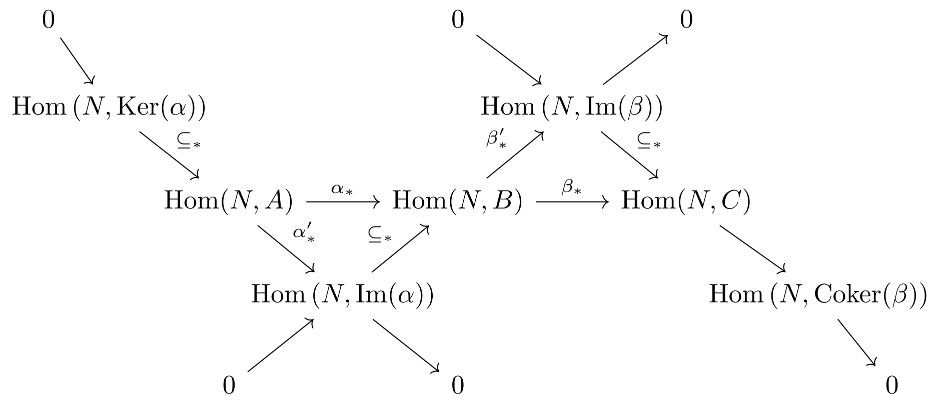
(vi) There exists an $_RN'$ such that $N \oplus N'$ is free, i.e., N is a summand of a free R-module.

Proof. (i)⟹(ii) Let $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ be a SES. By left exactness of Hom., I, we have $0 \to \mathrm{Hom}(N,A) \xrightarrow{\alpha_*} \mathrm{Hom}(N,B) \xrightarrow{\beta_*} \mathrm{Hom}(N,C)$ is exact. Also, by assumption, we have $\mathrm{Hom}(N,B) \xrightarrow{\beta_*} \mathrm{Hom}(N,C)$ is onto.

(ii)⟹(iii) Consider the exact sequence $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$.



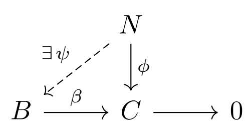
The Δ's commute and the diagonal sequences are SES's. Apply $\mathrm{Hom}(N,-)$.



Since $\beta_*\circ\alpha_* = (\beta\circ\alpha)_* = 0_* = 0$, $\mathrm{Im}(\alpha_*) \subseteq \mathrm{Ker}(\beta_*)$. Let $r \in \mathrm{Ker}(\beta_*)$. Then $\beta'_*(r) = \beta_*(r) = \beta\circ r = 0$. Since $\subseteq_*$ is actually $\subseteq$ w.r.t. new subsets, $r \in \mathrm{Hom}(N, \mathrm{Im}(\alpha))$. So there exists $a \in \mathrm{Hom}(N, A)$ such that $\alpha_*(a) = \alpha'_*(a) = r$. Hence $\mathrm{Im}(\alpha_*) \supseteq \mathrm{Ker}(\beta_*)$.

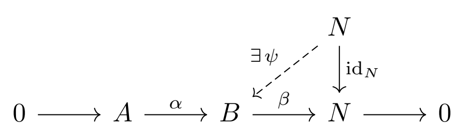
(iii)$\Longrightarrow$(i) Done.

(i)$\Longrightarrow$(v) Since $\beta : B \to C$ is onto, $\beta_* : \mathrm{Hom}(N, B) \to \mathrm{Hom}(N, C)$ is onto. Let $\phi \in \mathrm{Hom}(N, C)$. Then there exists $\psi \in \mathrm{Hom}(N, B)$ such that $\phi = \beta_*(\psi) = \beta\circ\psi$.

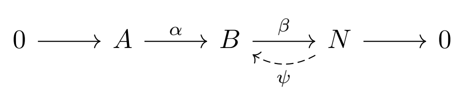


(v)$\Longrightarrow$(i) (v) says that $\mathrm{Hom}(N, B) \to \mathrm{Hom}(N, C)$ is onto.

(v)$\Longrightarrow$(iv) Let $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} N \to 0$ be exact. Then



Hence



Thus, it splits on the right and hence splits.

(iv)$\Longrightarrow$(vi) Fact: every R-module N is homomorphic image of a free R-module, i.e., there exists a free R-module F and epimorphism $\tau : F \to N$ such that

$$0 \longrightarrow \mathrm{Ker}(\tau) \xrightarrow{\subseteq} F \xrightarrow{\tau} N \longrightarrow 0$$

is a SES. So by assumption, $F \cong N \oplus \mathrm{Ker}(\tau)$.

(vi)$\Longrightarrow$(v)

$$\begin{array}{ccccc} & & N & & \\ & & \big\downarrow{\scriptstyle i} & & \\ & & F := N \oplus N' & & \\ & \swarrow{\scriptstyle \zeta} & \big\downarrow{\scriptstyle \rho} & & \\ & & N & & \\ & & \big\downarrow{\scriptstyle \phi} & & \\ B & \xrightarrow{\beta} & C & \longrightarrow & 0 \end{array}$$

Let X be the basis of F. Since β is onto, for $x \in X$, there exists $b_x \in B$ such that $\beta(b_x) = \phi(\rho(x))$. By UMP, there exists a unique homomorphism $\zeta : F \to B$ such that $\zeta(x) = b_x$ for $x \in X$. Define $\psi := \zeta \circ i$. Then

$$\begin{array}{ccccc} & & N & & \\ & \swarrow{\scriptstyle \psi} & \big\downarrow{\scriptstyle \phi\circ\rho\circ i=\phi} & & \\ B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

□

Theorem 2.32 (Long exact sequence)**.** *Given an exact sequence* $0 \to M_1 \xrightarrow{\alpha} M_2 \xrightarrow{\beta} M_3 (\to 0)$, *there exists an exact sequence*

$$0 \longrightarrow \mathrm{Hom}(N, M_1) \longrightarrow \mathrm{Hom}(N, M_2) \longrightarrow \mathrm{Hom}(N, M_3) \longrightarrow$$
$$\mathrm{Ext}^1(N, M_1) \longrightarrow \mathrm{Ext}^1(N, M_2) \longrightarrow \mathrm{Ext}^1(N, M_3) \longrightarrow$$
$$\mathrm{Ext}^2(N, M_1) \longrightarrow \cdots$$

$$0 \longrightarrow \mathrm{Hom}(M_3, N) \xrightarrow{\partial_1^*} \mathrm{Hom}(M_2, N) \xrightarrow{\partial_2^*} \mathrm{Hom}(M_1, N) \longrightarrow$$
$$\mathrm{Ext}^1(M_3, N) \xrightarrow{\delta_1^*} \mathrm{Ext}^1(M_2, N) \longrightarrow \mathrm{Ext}^1(M_1, N) \longrightarrow$$
$$\mathrm{Ext}^2(M_3, N) \longrightarrow \cdots$$

Then

$$\mathrm{Ext}^1(M_3, N) = \frac{\mathrm{Ker}(\partial_2^*)}{\mathrm{Im}(\partial_1^*)},$$

$$\mathrm{Ext}^2(M_2, N) = \frac{\mathrm{Ker}(\delta_1^*)}{\mathrm{Im}(\partial_2^*)}.$$

Remark. $\mathrm{Ext}^1_R(M_3, N)$ is the first measure of failure of the second sequence to be exact on the right−in fact it can be extended to a short exact sequence on the right if and only if the connecting homomorphism ∂_2^* is the zero homomorphism. In particular, if $\mathrm{Ext}^1_R(M_3, N) = 0$ for all R-modules M_3, then it will be exact on the right for every exact sequence. Then this implies the R-module N is injective.

Remark. Slogan: Ext measures the lack of right exactness of Hom..

Remark. It is hard to calculate the cokernel without prior complete understanding. Sometimes you can calculate $\mathrm{Ext}^1(N, M_1)$ or $\mathrm{Ext}^1(M_3, N)$ without understanding anything about α_* or β_*.

Definition 2.33. ${}_RN$ is *projective* if it satisfies any of the equivalent conditions of Theorem 2.31.

Remark. In the proof of (iv)$\Longrightarrow$(v) in Theorem 2.31, we have free modules are projective.

Theorem 2.34. *An R-module N is projective if and only if* $\mathrm{Ext}^n_R(N, -) = 0$ *for* $n \geqslant 1$.

Theorem 2.35. *An R-module N is injective if and only if* $\mathrm{Ext}^n_R(-, N) = 0$ *for* $n \geqslant 1$.

Example 2.36. Assume R_1 and R_2 are commutative rings with identity such that $R = R_1 \times R_2$, $N_1 = R_1 \times 0$ and $N_2 = 0 \times R_2$. Then $N_1 \oplus N_2 \cong R$. So N_1 and N_2 are both projective. If $R_1, R_2 \neq 0$, then N_1, N_2 are not free R-modules since $(0,1)(1,0) = 0$. So projectiveness does not imply freeness.

Definition 2.37. Given R-module N, there exists a projective R-module P and an R-linear surjection $\tau : P \to N$

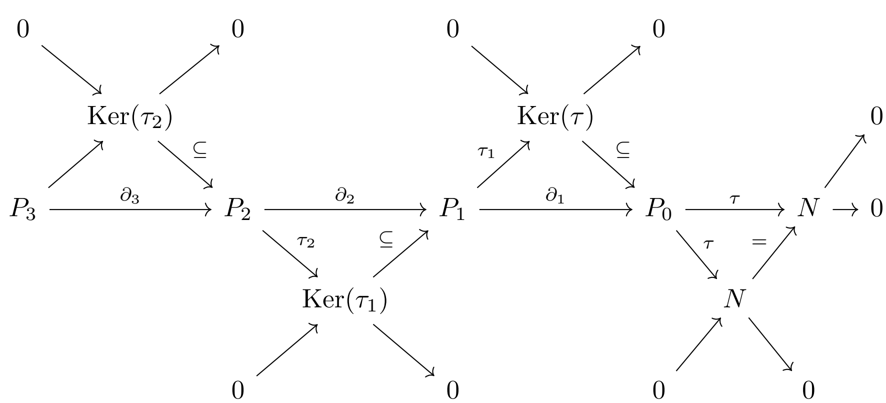
Remark. Slogan: Every R-module is a homomorphic image of a projective R-module.
free = nice! projective = pretty nice!

Lemma 2.38. For every set Λ, there exists free module R with basis B such that $|B| = |\Lambda|$. Frequently denoted $R^{(\Lambda)}$ with basis vectors denoted $e_\lambda, \forall \lambda \in \Lambda$.

Lemma 2.39. P is projective if and only if there exists P' such that $P \oplus P' \cong R^{(\Lambda)}$ for some Λ.

Example 2.40. A $\mathbb{Z}$-module is projective if and only if it is free. So $\mathbb{Z}/2\mathbb{Z}$ is not projective.

Remark. $P \xrightarrow{\tau} N \to 0$ can be thought of as approximating N by the projective module P. Error approximation is $\mathrm{Ker}(\tau)$. $0 \to \mathrm{Ker}(\tau) \xrightarrow{\subseteq} P \xrightarrow{\tau} N \to 0$ is exact. Since $\mathrm{Ker}(\tau)$ is an R-module, there exists a projective R-module P_1 such that $P_1 \to \mathrm{Ker}(\tau)$. Note $\mathrm{Ker}(\tau) \xrightarrow{\subseteq} P_0 := P$ is an R-module homomorphism. Let $\partial_1 = \tau_1$. Then $\mathrm{Im}(\partial_1) = \mathrm{Im}(\tau_1) = \mathrm{Ker}(\tau)$. Repeat this process, we have



Definition 2.41. An *augmented free* (resp. *projective*) *resolution* of M is an exact sequence

$$P_\bullet^+ := \cdots \xrightarrow{\partial_{i+2}} P_{i+1} \xrightarrow{\partial_{i+1}} P_i \xrightarrow{\partial_i} \cdots P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \xrightarrow{\tau} M \to 0,$$

of R-modules and R-module homomorphism such that P_i is free (resp. projective) as a R-module for $i \geqslant 0$.

Lemma 2.42. Every R-module M has a projective resolution over R.

Construction 2.43. We use the fact that every module is a homomorphic image of a free module to construct free resolution of the R-module M. Take F_0 to be a free module that maps onto M, and we have non-isomorphic choices there; for example, choose F_0 to be the free R-module generated by the elements of M, we then take F_1 to be a free module that maps onto $\operatorname{Ker}(F_0 \to M)$, giving an exact sequence $F_1 \to F_0 \to M \to 0$; after which we may take F_2 to be a free module that maps onto $\operatorname{Ker}(F_1 \to F_0)$, etc.

Definition 2.44. The *associated (truncated) projective resolution* of M is a complex

$$P_\bullet := \left(\cdots \xrightarrow{\partial_{i+2}} P_{i+1} \xrightarrow{\partial_{i+1}} P_i \xrightarrow{\partial_i} \cdots P_2 \xrightarrow{\partial_2} P_1 \xrightarrow{\partial_1} P_0 \to 0 \right),$$

where ∂_i are the differentials of the resolution. Let

$$P_\bullet^* = \operatorname{Hom}(P_\bullet, N) := \left(0 \longrightarrow P_0^* \xrightarrow{\partial_1^*} P_1^* \xrightarrow{\partial_2^*} \cdots P_{i-1}^* \xrightarrow{\partial_i^*} P_i^* \xrightarrow{\partial_{i+1}^*} \cdots \right),$$

which is usually not exact, where $P_i^* = \operatorname{Hom}_R(P_i, N)$ for $i \geqslant 0$ and $\partial_i^* = \operatorname{Hom}_R(\partial_i, N)$ for $i \geqslant 1$. Also,

$$\operatorname{Hom}(P_\bullet^+, N) := \left(0 \to \operatorname{Hom}_R(M, N) \to P_0^* \xrightarrow{\partial_1^*} P_1^* \xrightarrow{\partial_2^*} \cdots P_{i-1}^* \xrightarrow{\partial_i^*} P_i^* \xrightarrow{\partial_{i+1}^*} \cdots \right)$$

Let $P_\bullet$ be projective resolution of M.

Theorem 2.45. *Since* $\partial_{i+1}^* \circ \partial_i^* = (\partial_i \circ \partial_{i+1})^* = 0^* = 0$, *we have* $\operatorname{Im}(\partial_i^*) \subseteq \operatorname{Ker}\left(\partial_{i+1}^*\right)$.

Definition 2.46. For $i \geqslant 1$, define

$$\operatorname{Ext}_R^i(M, N) := \frac{\operatorname{Ker}\left(\partial_{i+1}^*\right)}{\operatorname{Im}\left(\partial_i^*\right)}.$$

Theorem 2.47. $\operatorname{Ext}_R^0(M, N) := \frac{\operatorname{Ker}(\partial_1^*)}{0} \cong \operatorname{Ker}(\partial_1^*)$.

Lemma 2.48. $0 \to A \xrightarrow{\alpha} B \to 0$ is exact if and only if α is an isomorphism.
$0 \to C \to 0$ is exact if and only if $C = 0$.

Theorem 2.49 (Hom. cancellation)**.** *Let R be commutative ring with identity, then*

$$\begin{aligned} \operatorname{Hom}_R(R, N) &\cong N \\ \Phi : \phi &\mapsto \phi(1) \\ \cdot x =: \phi_x &\leftarrow x \end{aligned}$$

Proof. Let $\phi \in \operatorname{Ker}(\Phi)$. Then $\phi(1) = 0$. Since $\phi \in \operatorname{Hom}_R(R, N)$, we have $\phi = 0$. So Φ is 1-1. Let $x \in N$. Define $\phi \in \operatorname{Hom}_R(R, N)$ by $\phi(1) = x$. Then Φ is onto. □

Theorem 2.50.

$$\operatorname{Hom}_R(R/I, N) \cong (0 :_N I)$$
$$\phi \mapsto \phi(\bar{1})$$

Proof. Let $\phi \in \operatorname{Hom}_R(R/I, N)$. For any $x \in I$, we have $\phi(\bar{1})x = \phi(\bar{x}) = \phi(0) = 0$. So it is well-defined. The rest is similar. □

Theorem 2.51.

$$\operatorname{Ext}^i_R(R, N) \cong \begin{cases} N, & \textit{if } i = 0 \\ 0, & \textit{if } i \geqslant 1 \end{cases}.$$

Proof. Note R is projective. The augmented projective resolution of R is

$$P_\bullet^+ = \left(0 \xrightarrow{\partial} R \xrightarrow{\text{id}} R \to 0\right),$$

where $P_0 = R$ and $M = R$. The associated projective resolution of R is

$$P_\bullet = \left(0 \xrightarrow{\partial_1} R \to 0\right).$$

Since $P_i = 0$ for $i \geqslant 1$, we have $P_i^* = \operatorname{Hom}_R(P_i, N) = 0$ for $i \geqslant 1$. So

$$P_\bullet^* = \left(0 \to P_0^* = \operatorname{Hom}_R(R, N) \xrightarrow{\partial_1^*} 0 \to 0 \to 0 \cdots\right).$$

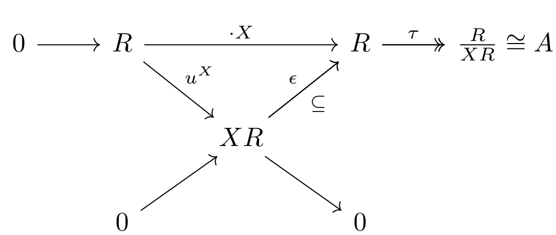
So $\operatorname{Ext}^0_R(R, N) \cong \operatorname{Ker}(\partial_1^*) = \operatorname{Hom}_R(R, N) \cong N$. When $i \geqslant 0$, $\operatorname{Ext}^i_R(R, N) := \frac{\operatorname{Ker}(\partial_{i+1}^*)}{\operatorname{Im}(\partial_i^*)} = 0$. □

Example 2.52. Let A be a nonzero commutative ring with identity and $R = A[X]$. Let $\mathfrak{a} = (X)R$. Then $R/\mathfrak{a} = \frac{A[X]}{(X)R} \cong A$. So A is an R-module. Then

$$\operatorname{Ext}^i_R(A, R) = \begin{cases} A, & \text{if } i = 1 \\ 0 & \text{if } i \neq 1 \end{cases}.$$

$$\operatorname{Ext}^i_R(A, A) = \begin{cases} A, & \text{if } i = 0, 1 \\ 0 & \text{if } i \geqslant 2 \end{cases}.$$

Proof. Note



where $u^X(r) = rX$ for $r \in R$. Since $R \overset{\tau}{\twoheadrightarrow} \frac{R}{XR} \cong A$, we have

$$P_\bullet^+ = \left(\cdots 0 \to 0 \to R \xrightarrow{\cdot X} R \to A \to 0 \right),$$

$$P_\bullet = \left(\cdots 0 \to 0 \to R \xrightarrow{\cdot X} R \to 0 \right).$$

$$P_\bullet^* = \quad \begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Hom}_R(R,R) & \xrightarrow{(\cdot X)^*} & \operatorname{Hom}_R(R,R) & \longrightarrow & 0 & \longrightarrow & \cdots \\ \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & R & \xrightarrow{\cdot X} & R & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & & & & & & & \\ & & P_0 & & P_1 & & P_2 & & \cdots \end{array}$$

When $i \geqslant 2$, $\operatorname{Ext}_R^i(A,R) = 0$. Since X is NZD, $\operatorname{Ext}_R^0(A,R) \cong \operatorname{Ker}(R \xrightarrow{\cdot X} R) = 0$. Also, $\operatorname{Ext}_R^1(A,R) = \frac{\operatorname{Ker}(R \to 0)}{\operatorname{Im}(R \xrightarrow{\cdot X} R)} = \frac{R}{XR} \cong A$.

Similarly, apply $\operatorname{Hom}_R(-,A)$,

$$P_\bullet^* \cong \left(0 \to A \xrightarrow{\cdot X} A \to 0 \to 0 \to \cdots \right).$$

Let $r + XR \in \frac{R}{XR} = A$. Since $X(r + XR) = (Xr) + XR = 0 + XR = XR$, we have $(\cdot X) = 0$. When $i \geqslant 2$, $\operatorname{Ext}_R^i(A,A) = 0$. Also, $\operatorname{Ext}_R^0(A,A) \cong \operatorname{Ker}(A \xrightarrow{0} A) = A$ and $\operatorname{Ext}_R^1(A,A) = \frac{\operatorname{Ker}(A \to 0)}{\operatorname{Im}(A \xrightarrow{0} A)} = \frac{A}{0} \cong A$. □

Proposition 2.53. $\operatorname{Ext}_R^0(M,N) \cong \operatorname{Hom}_R(M,N)$.

Proof. Let

$$P_\bullet^+ = \left(\cdots \xrightarrow{\partial 2} P_1 \xrightarrow{\partial 1} P_0 \xrightarrow{\tau} M \to 0 \right).$$

Since Hom. is left exact,

$$0 \longrightarrow \operatorname{Hom}_R(M,N) \xrightarrow{\tau^*} \operatorname{Hom}_R(P_0,N) \xrightarrow{\partial_1^*} \operatorname{Hom}_R(P_1,N),$$

is exact. So $\operatorname{Ext}_R^0(M,N) \cong \operatorname{Ker}(\partial_1^*) = \operatorname{Im}(\tau^*) \cong \frac{\operatorname{Hom}_R(M,N)}{\operatorname{Ker}(\tau^*)} = \frac{\operatorname{Hom}_R(M,N)}{0} \cong \operatorname{Hom}_R(M,N)$. □

Question 2.54. (a) Is Ext well-defined? i.e., is it independent of the choice of $P_\bullet^+$?

(b) How to build the long exact seque?

2.3 Depth

Remark. It is good for induction.

Definition 2.55. Let M be an R-module. An element $x \in R$ is a *non-zero divisor* (NZD) on M if

$$0 \longrightarrow M \xrightarrow{\cdot x} M$$

is exact.

Remark. $x \in R$ is a NZD on M, meaning for $m \in M$, if $xm = 0$, then $m = 0$.

Definition 2.56. x is *M-regular* if x is NZD on M and $xM \neq M$.

Definition 2.57. A sequence $x = x_1, \dots, x_n \in R$ is *M-regular* if x_1 is M-regular and x_i is $\frac{M}{(x_1,\dots,x_{i-1})M}$-regular, for $i = 2, \dots, n$.

Theorem 2.58.

$$\frac{M/(x_1,\dots,x_{i-1})}{x_i \cdot M/(x_1,\dots,x_{i-1})M} = \frac{M/(x_1,\dots,x_{i-1})M}{(x_1,\dots,x_i)M/(x_1,\cdots x_{i-1})M} \cong \frac{M}{(x_1,\dots,x_i)M}.$$

Lemma 2.59. If R is Noetherian and $\mathfrak{a} \leqslant R$ such that $\mathfrak{a}M \neq M$, then there exists a maximal M-regular sequence in $\mathfrak{a}$, i.e., an M-regular sequence $\underset{\sim}{x} = x_1, \dots, x_n \in \mathfrak{a}$ such that for $y \in \mathfrak{a}$, the sequence $x_1, \dots, x_n, y$ is not M-regular.

Definition 2.60. Let $\mathfrak{a} \leqslant R$ such that $\mathfrak{a}M \neq M$. The length n of a maximal M-regular sequence in $\mathfrak{a}$, is called the *depth* of $\mathfrak{a}$ on M, denoted $n = \operatorname{depth}(\mathfrak{a}; M)$. If R is local, write $n = \operatorname{depth}(M)$.

The *depth* of a ring means the depth of R as an R-module.

Question 2.61. Is the depth independent of the choice of maximal M-regular sequence? Answer: Yes, if M is finitely generated.

Proof. Use Ext. All the $\operatorname{Ext}^0_R(R/\mathfrak{a}, M)$, $\operatorname{Ext}^1_R(R/\mathfrak{a}, M)$, $\operatorname{Ext}^2_R(R/\mathfrak{a}, M)$, $\cdots$, $\operatorname{Ext}^{n-1}_R(R/\mathfrak{a}, M)$ are 0 and $\operatorname{Ext}^n_R(R/\mathfrak{a}, M)$ is not 0. Then $\operatorname{depth}(\mathfrak{a}; M) = \min\left\{i \geqslant 0 \mid \operatorname{Ext}^i_R(R/\mathfrak{a}, M) \neq 0\right\} = n$. □

2.4 Localization problem for regular local rings

Assume $(R, \mathfrak{m}, K)$ is a local Noetherian, i.e., R has a unique maximal ideal $\mathfrak{m}$ and $K = R/\mathfrak{m}$.

Definition 2.62 (*Krull dimension*)**.**

$$\dim(R) = \sup\{n \geqslant 0 \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}_2 \subsetneq \cdots \mathfrak{p}_n \subsetneq R \text{ s.t. } \mathfrak{p}_i \in \operatorname{Spec}(R), \forall i = 1, \dots, n\},$$

which measures the size of R.

Lemma 2.63. If R is local Noetherian, then $\dim(R) < \infty$.

Definition 2.64 (*Embedding dimension*)**.**

$$\operatorname{edim}_R := \dim_K(\mathfrak{m}/\mathfrak{m}^2) < \infty.$$

Proof. $\mathfrak{m}/\mathfrak{m}^2$ is an R-module such that $\mathfrak{m} \cdot (\mathfrak{m}/\mathfrak{m}^2) = 0$. So it is $R/\mathfrak{m}$-module, i.e., it is K-vector space. Hence it is a finite dimensional vector space over K. □

Remark. (a) The Krull dimension is the supremum of the lengths of chains of prime ideals of R.

(b) The embedded dimension may also be described as the least number of generators of the maximal ideal $\mathfrak{m}$.

Theorem 2.65. $\operatorname{depth}_R(\mathfrak{m}; R) \leqslant \dim(\mathfrak{m}; R) \leqslant \operatorname{edim}(R)$.

Definition 2.66. A local ring $(R, \mathfrak{m}; K)$ is *regular* (RLR) if $\dim(R) = \operatorname{edim}(R)$.
$(R, \mathfrak{m}; K)$ is *Cohen-Macaulay* (CM) if $\operatorname{depth}_R(\mathfrak{m}; R) = \dim(R)$.

Theorem 2.67. *If $(R, \mathfrak{m}, K)$ is RLR, then it is CM.*

Example 2.68. Assume that R is local Noetherian with unique maximal ideal $\mathfrak{m} = (X_1, \ldots, X_n)R$. $R = K[X_1, \ldots, X_n]_{(X_1,\ldots,X_n)}$. Geometrically, R represents K^n, e.g., $\mathbb{R}^n$ or $\mathbb{C}^n$. $\dim(R) = n = \operatorname{edim}(R)$. So R is RLR.

Example 2.69. Let $R = \mathbb{R}[X, Y]/(Y^2 - X^2(X + 1))$. Let $V = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^2(x + 1)\}$. Let $p = (a, b) \in V$ and $\mathfrak{m}_p = (X - a, Y - b)R$. $(R)_{\mathfrak{m}_p}$ is a local ring. If p is smooth on the curve, $(R)_{\mathfrak{m}_p}$ is RLR. Note all rings $(R)_{\mathfrak{m}_p}$ has Krull dimension 1 because it is a curve. Since $\operatorname{edim}((R)_{\mathfrak{m}_p}) = \dim(\text{tangent space through } p)$, we have $\operatorname{edim}((R)_{\mathfrak{m}_0}) = 2$, $(R)_{\mathfrak{m}_0}$ is not regular.

Remark. Localization: "zoom in" on some neighborhood of your points. Localization should make the singularity not worse. nonsingular $\to$ singular.

Remark. If R is RLR and $\mathfrak{p} \lneq R$ prime. Must $R_\mathfrak{p}$ also be RLR? A: Yes. (Can usually control $\dim(R_\mathfrak{p})$ vs $\dim(R)$, but $\operatorname{edim}(R_\mathfrak{p})$ is $\dim(R)$?) hard. (Is it for $\mathfrak{p}$ in $K[x, y, z]_{(x,y,z)}$ or $K[x, y, z]$.)

Theorem 2.70 (Auslander-Buchsbaum and Serre)**.** *R is RLR if and only if for all R-modules M and N, $\operatorname{Ext}^i_R(M, N) = 0$ for $i > \dim(R)$ if and only if $\operatorname{Ext}^{\dim(R)+1}_R(K, K) = 0$ if and only if there exists $d \geqslant 0$ such that $\operatorname{Ext}^d_R(K, K) = 0$.*

Corollary 2.71. Let R be RLR and $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $R_\mathfrak{p}$ is RLR.

Proof. It is enough to show $\operatorname{Ext}^d_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) = 0$ for some $d \geqslant 0$. The ring $R_\mathfrak{p}$ is local with residue field $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p}$. Since R is RLR, $\operatorname{Ext}^d_R(R/\mathfrak{p}, R/\mathfrak{p}) = 0$ for $d > \dim(R)$.

$$\operatorname{Ext}^d_{R_\mathfrak{p}}(R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}, R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}) \cong \operatorname{Ext}^d_\mathfrak{p}((R/\mathfrak{p})_\mathfrak{p}, (R/\mathfrak{p})_\mathfrak{p}) \cong \operatorname{Ext}^d_R(R/\mathfrak{p}, R/\mathfrak{p})_\mathfrak{p} = 0, \forall d > \dim(R).$$

So $R_\mathfrak{p}$ is RLR. $\square$

Chapter 3

Localization

Let R be a nonzero commutative ring with identity and M, N be an R-modules.

Definition 3.1. A subset $U \subseteq R$ is *multiplicatively closed* if $1 \in U$ and $uv \in U$ for $u, v \in U$.

Example 3.2. If $s \in R$, then $S = \{1, s, s^2, \cdots\} \subseteq R$ is multiplicative closed.

Example 3.3. If $\mathfrak{p} \leqslant R$ is prime, then $R \smallsetminus \mathfrak{p}$ is multiplicative closed.

Let $U \subseteq R$ be multiplicative closed.

Definition 3.4. The *equivalent relation* on $M \times U$: $(m, u) \sim (n, v)$ if there exists $w \in U$ such that $w(vm - un) = 0$.

Remark. Want to define $U^{-1}M = \{\frac{m}{u} \mid m \in M, u \in U\}$. Note $\frac{m}{u} = \frac{vm}{vu}$ is ok because $u(vm) = (vu)m$.

Definition 3.5.

$$U^{-1}M = \{\text{equivalent classes from } M \times U \text{ under } \sim\}.$$

Denote the *equivalent class* of (m, u) as $\frac{m}{u}$ or m/u.

Remark. If $0 \in U$, then $U^{-1}M = 0$ since we can always take $w = 0$ in the definition.

Example 3.6. $U^{-1}R$ is a commutative ring with identity. $\frac{m}{u} + \frac{n}{v} = \frac{vm+un}{uv}$, $\frac{m}{u} \cdot \frac{n}{v} = \frac{mn}{uv}$, $0_{U^{-1}R} = \frac{0_R}{u} = \frac{0_R}{1_R}$ and $1_{U^{-1}R} = \frac{u}{u} = \frac{1_R}{1_R}$. There exists a ring homomorphism

$$\begin{aligned} \psi : R &\to U^{-1}R \\ r &\mapsto \frac{r}{1} = \frac{ur}{u}. \end{aligned}$$

UMP for ψ: Given any ring homomorphism $\phi : R \to S$ such that for $u \in U$, $\phi(u) \in S^\times$. Then there exists a unique ring homomorphism $\widetilde{\phi} : U^{-1}R \to S$ such that the following diagram commutes

$$\begin{array}{ccc} R & \xrightarrow{\psi} & U^{-1}R \\ & {\scriptstyle \phi}\searrow & \downarrow {\scriptstyle \exists!\, \widetilde{\phi}} \\ & & S \end{array}$$

Note $\psi(u) = \frac{u}{1} \in (U^{-1}R)^\times$ and $(\frac{u}{1})^{-1} = \frac{1}{u}$ for $u \in U$.

Theorem 3.7. *In general, $U^{-1}M$ is*

(a) an additive abelian group $\frac{m}{u} + \frac{n}{v} = \frac{vm+un}{uv}$ and $0_{U^{-1}M} = \frac{0_U}{1_R} = \frac{0_U}{u}$;

(b) an R-module. $r \cdot \frac{m}{u} = \frac{rm}{u}$;

(c) a $U^{-1}R$-module. $\frac{r}{v} \cdot \frac{m}{u} = \frac{rm}{vu}$.

Example 3.8. Let R be an integral domain. Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $U = R \setminus \mathfrak{p}$ is multiplicative closed and $(R \setminus \{0\})^{-1}R$ is field of fractions of R. $(R \setminus \{0\})^{-1}M$ is a vector space over field of fractions since it is a $(R \setminus 0)^{-1}R$-module.

Definition 3.9. Let $f : M \to N$ be a homomorphism, then

$$\begin{aligned} U^{-1}f : U^{-1}M &\to U^{-1}N \\ \frac{m}{u} &\mapsto \frac{f(m)}{u} \end{aligned}$$

is a well-defined $U^{-1}R$-module homomorphism.

Proof. Let $\frac{m}{u} = \frac{m'}{u'}$. Then there exists $v \in U$ such that $vu'm = vum'$. So $f(vu'm) = f(vum')$. Since U is multiplicative closed and M is an R-module, $vu'f(m) = vuf(m')$. So by definition, $\frac{f(m)}{u} = \frac{f(m')}{u'}$. Thus, $U^{-1}f$ is well-defined. Since $(U^{-1}f)(\frac{m}{u} + \frac{x}{w}) = (U^{-1}f)(\frac{wm+ux}{uw}) = \frac{wf(m)+uf(x)}{uw} = \frac{f(m)}{u} + \frac{f(x)}{w} = U^{-1}f(\frac{m}{u}) + U^{-1}f(\frac{x}{w})$ and $U^{-1}f(\frac{r}{u} \cdot \frac{x}{v}) = \frac{rf(x)}{uv} = \frac{r}{u}\frac{f(x)}{v}$, $U^{-1}f$ is a $U^{-1}R$-module homomorphism. $\square$

Definition 3.10 (Notation)**.** If $s \in R$ and $S = \{1, s, s^2, \cdots\}$, then $M_s := S^{-1}M$. If $\mathfrak{p} \in \operatorname{Spec}(R)$ and $U = R \setminus \mathfrak{p}$, then we have the localization $M_\mathfrak{p} = U^{-1}M = (R \setminus \mathfrak{p})^{-1}M$.

Remark. U^{-1} eats modules or homomorphisms, it's a covariant functor (respect the order of arrows).

Theorem 3.11. *Let $f : M \to N$, $g : N \to P$ be R-module homomorphisms. Then $U^{-1}(g \circ f) = (U^{-1}g) \circ (U^{-1}f)$, i.e.,*

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ & \searrow^{g\circ f} & \downarrow g \\ & & P \end{array} \qquad \begin{array}{ccc} U^{-1}M & \xrightarrow{U^{-1}f} & U^{-1}N \\ & \searrow^{U^{-1}(g\circ f)} & \downarrow U^{-1}g \\ & & U^{-1}P \end{array}$$

commute and $U^{-1}(\mathrm{id}_M) = \mathrm{id}_{U^{-1}M}$.

Theorem 3.12. *$U^{-1}(-)$ is exact, i.e., $U^{-1}(-)$ respects short exact sequences.*

Proof. Let $0 \to M \xrightarrow{f} N \xrightarrow{g} P \to 0$ be exact. Consider

$$0 \to U^{-1}M \xrightarrow{U^{-1}f} U^{-1}N \xrightarrow{U^{-1}g} U^{-1}P \to U^{-1}(0) = 0.$$

Since $(U^{-1}g)\circ(U^{-1}f)=U^{-1}(g\circ f)=U^{-1}(0)=0$, $\mathrm{Im}(U^{-1}f)\subseteq \mathrm{Ker}(U^{-1}g)$. Let $\frac{n}{u}\in\mathrm{Ker}(U^{-1}g)$. Then $0=(U^{-1}g)(\frac{n}{u})=\frac{g(n)}{u}$. So there exists $v\in U$ such that $0=v\cdot g(n)=g(vn)$. Since $\mathrm{Ker}(g)\subseteq \mathrm{Im}(f)$, then there exists $m\in M$ such that $f(m)=vn$. Since $\frac{m}{uv}\in U^{-1}M$ and $(U^{-1}f)(\frac{m}{uv})=\frac{f(m)}{uv}=\frac{vn}{uv}=\frac{n}{u}$, we have $\frac{u}{u}\in\mathrm{Im}(U^{-1}g)$. So $\mathrm{Ker}(U^{-1}g)\subseteq\mathrm{Im}(U^{-1}f)$. Hence $\mathrm{Im}(U^{-1}f)=\mathrm{Ker}(U^{-1}g)$.

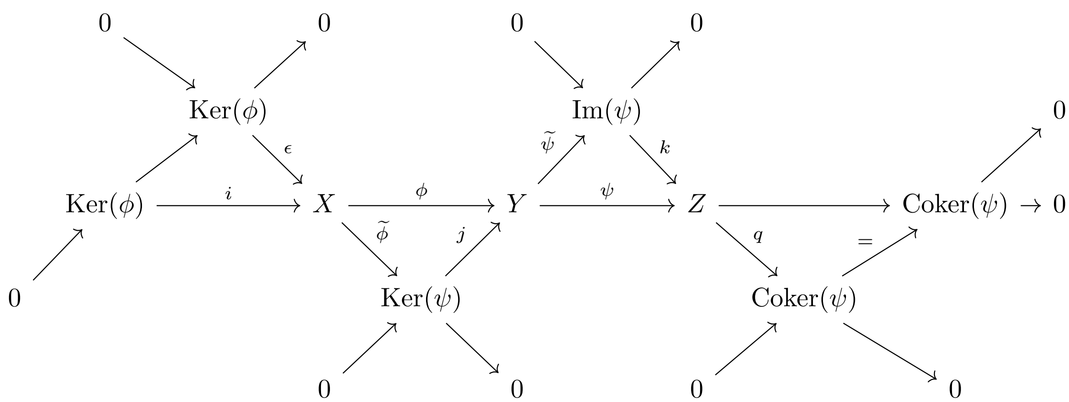
Let $\frac{m}{u}\in U^{-1}M$. Then $\frac{m}{u}\in\mathrm{Ker}(U^{-1}f)$ if and only if $\frac{0}{1}=0=(U^{-1}f)(\frac{m}{u})=\frac{f(m)}{u}$ if and only if there exists v such that $v\cdot 1\cdot f(m)=0=f(vm)$ if and only if $vm=0$ since f is 1-1 if and only if $\frac{m}{u}=\frac{vm}{vu}=\frac{0}{vu}=0$. So $U^{-1}f$ is 1-1.

Let $\frac{p}{u}\in U^{-1}P$. Since g is onto, then there exists $n\in N$ such that $p=g(n)$. Since $(U^{-1}g)(\frac{n}{v})=\frac{g(n)}{v}=\frac{p}{u}$, $U^{-1}g$ is onto. □

Theorem 3.13 (Graphical proof)**.** *Consider an arbitrary exact sequence $X\xrightarrow{\phi}Y\xrightarrow{\psi}Z$. Want an exact sequence*

$$U^{-1}X\xrightarrow{U^{-1}\phi}U^{-1}Y\xrightarrow{U^{-1}\psi}U^{-1}Z.$$

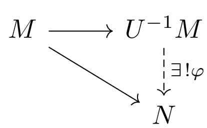
Proof. Since $\psi\circ\phi=0$, we have $U^{-1}\psi\circ U^{-1}\phi=U^{-1}(\psi\circ\phi)=U^{-1}0$. So $\mathrm{Im}(U^{-1}\phi)\subseteq\mathrm{Ker}(U^{-1}\psi)$.



Then we have a graph with the same structure and $U^{-1}()$ putting on each map.

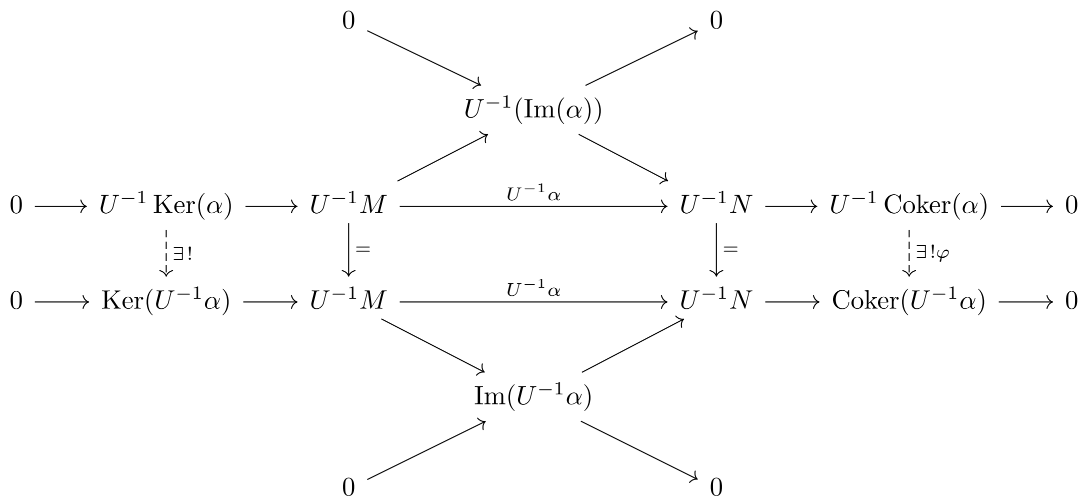
Let $\frac{y}{u}\in\mathrm{Ker}(U^{-1}\psi)$. Since $U^{-1}(-)$ respects SES, $U^{-1}(\widetilde{\phi})$ is onto and $U^{-1}j$ is 1-1. Note that $\widetilde{(U^{-1}\psi)}(\frac{y}{u}=0$. Then there exists $\frac{a}{v}\in U^{-1}\mathrm{Ker}(\psi)$ such that $U^{-1}j(\frac{a}{v})=\frac{y}{v}$, etc. By the commutativity of the lower left diagram, there exists $\frac{x}{w}\in U^{-1}X$ such that $\frac{y}{u}=(U^{-1}\phi)(\frac{x}{w})$. So $\mathrm{Ker}(U^{-1}\psi)\subseteq\mathrm{Im}(U^{-1}(\phi))$. □

Theorem 3.14 (UMP for localization of modules)**.** *Given an R-module homomorphism $f:M\to N$ on which the elements of U act by multiplication as automorphism, there is a unique R-module homomorphism $U^{-1}M\to N$ such that the following diagram commutes:*

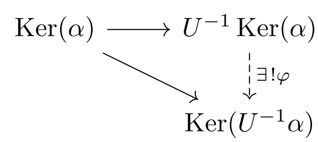


Theorem 3.15. *For R-module homomorphisms $\alpha:M\to N$, $U^{-1}(\mathrm{Ker}(\alpha))\cong\mathrm{Ker}(U^{-1}\alpha)$, we have $U^{-1}(\mathrm{Coker}(\alpha))\cong\mathrm{Coker}(U^{-1}\alpha)$ and $U^{-1}(\mathrm{Im}(\alpha))\cong\mathrm{Im}(U^{-1}\alpha)$.*

Proof. Consider



We have a ring homomorphism $f : \operatorname{Ker}(\alpha) \to \operatorname{Ker}(U^{-1}\alpha)$ given by $a \mapsto \frac{a}{1}$. We claim that $\operatorname{Ker}(U^{-1}M) \xrightarrow{\cdot u} \operatorname{Ker}(U^{-1}M)$ is a well-defined automorphism for any $u \in U$. Let $m/v \in \operatorname{Ker}(U^{-1}M)$, then $U^{-1}\alpha(m/v) = 0$, $m/v = u(m/uv)$ and $U^{-1}\alpha(m/uv) = (1/u)\alpha(m/v) = 0$, so it is onto. Assume $u(m/v) = 0$, then there exists w such that $(wu)m = 0$, implying $m/v = 0$, and hence it is 1-1. Then by UMP for localization of modules, we have the following commutative diagram:



It is straightforward to check that the middle left diagram commutes. So φ is 1-1. It is onto since the first horizontal sequence is exact. We have $U^{-1}(\operatorname{Im}(\alpha)) \to \operatorname{Im}(U^{-1}\alpha)$ is 1-1 since $U^{-1}\operatorname{Im}(\alpha) \to U^{-1}B$ and $\operatorname{Im}(U^{-1}\alpha) \to U^{-1}B$ is 1-1. Similarly, it is onto. $\square$

Theorem 3.16 (Prime correspondence under localization)**.**

$$\{\textit{prime ideals of } U^{-1}R\} \rightleftarrows \{\textit{prime ideal } \mathfrak{q} \leqslant R \ \mid \mathfrak{q} \cap U = \emptyset\}$$
$$Q \mapsto \psi^{-1}(Q) = \{x \in R \mid \psi(x) \in Q\}$$
$$\langle x/1 \mid x \in \mathfrak{q}\rangle U^{-1}R = \mathfrak{q}(U^{-1}R) \leftarrow\!\shortmid \mathfrak{q}.$$

Theorem 3.17.

$$U^{-1}R/(\mathfrak{q} \cdot U^{-1}R) \cong U^{-1}(R/\mathfrak{q})$$
$$(U^{-1}R)_{\mathfrak{q} \cdot U^{-1}R} \cong R_{\mathfrak{q}}$$
$$\frac{r/1}{z/1} \leftarrow\!\shortmid \frac{r}{z}$$
$$\frac{r/u}{z/v} \mapsto \frac{vr}{uz}.$$

Example 3.18. Let $U = R \setminus \mathfrak{p}$.

$$\begin{aligned} \operatorname{Spec}(R_\mathfrak{p}) &\rightleftarrows \{\mathfrak{q} \in \operatorname{Spec}(R)\} \mid \mathfrak{q} \subseteq \mathfrak{p}\} \\ R_\mathfrak{p}/\mathfrak{q}R_\mathfrak{p} &\cong (R/\mathfrak{q})_\mathfrak{p} \\ (R_\mathfrak{p})_{\mathfrak{q}R_\mathfrak{p}} &\cong R_\mathfrak{q}. \end{aligned}$$

So $R_\mathfrak{p}$ has a unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$. Note $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p}$, which is the field of fractions of the integral domain $R/\mathfrak{p}$.

Remark. As we have seen, one way to "simplify" the study of ideals in a ring R is to pass to a quotient ring R/I: this has the effect of "cutting" off the bottom of the ideal lattice by keeping only ideals $J \supseteq I$.

The localization effects the opposite kind of simplification: given $\mathfrak{p} \leqslant R$ and the canonical map $\varphi : R \to R_\mathfrak{p}$, $\varphi^* : \operatorname{Spec}(R_\mathfrak{p}) \to \operatorname{Spec}(R)$ is 1-1 with $\operatorname{Im}(\varphi) = \{\mathfrak{q} \in \operatorname{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\}$.

Theorem 3.19.

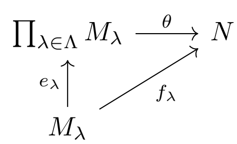
$$\operatorname{Hom}_R\left(\prod_{\lambda\in\Lambda} M_\lambda, N\right) \cong \prod_{\lambda\in\Lambda} \operatorname{Hom}_R(M_\lambda, N).$$

Proof. Define

$$\begin{aligned} \varphi : \operatorname{Hom}_R\left(\prod_{\lambda\in\Lambda} M_\lambda, N\right) &\to \prod_{\lambda\in\Lambda} \operatorname{Hom}_R(M_\lambda, N) \\ f &\mapsto (fe_\lambda) = (e_\lambda^*(f)), \end{aligned}$$

where $e_\lambda : M_\lambda \to \prod_{\lambda\in\Lambda} M_\lambda$ are the natural injections. Then φ is an R-module homomorphism.

Let $(f_\lambda) \in \prod_{\lambda\in\Lambda} \operatorname{Hom}_R(M_\lambda, N)$. Define an R-module homomorphism $\theta : \prod_{\lambda\in\Lambda} M_\lambda \to N$ by $\theta(\underline{a}) = \sum_{\lambda\in\Lambda} f_\lambda(a_\lambda)$. Then $\varphi(\theta) = (\theta e_\lambda) = (f_\lambda)$. So φ is surjective.



Let $f \in \operatorname{Hom}_R(\prod_{\lambda\in\Lambda} M_\lambda, N)$. Claim. If $fe_\lambda = 0$ for each $\lambda \in \Lambda$, then $f = 0$. Suppose $f \neq 0$. Then $f(\underline{a}) \neq 0$ for some $\underline{a} \in \prod_{\lambda\in\Lambda} M_\lambda$. Then $0 = \sum_{\lambda\in\Lambda} 0(a_\lambda) = \sum_{\lambda\in\Lambda} fe_\lambda(a_\lambda) = f \sum_{\lambda\in\Lambda} e_\lambda(a_\lambda) = f(\underline{a}) \neq 0$, a contradiction. So $\operatorname{Ker}(\varphi) = \{f \in \operatorname{Hom}_R(\prod_{\lambda\in\Lambda} M_\lambda, N) \mid (fe_\lambda) = 0\} = \{0\}$. Thus, φ is injective. ☐

Theorem 3.20.

$$\operatorname{Hom}_R\left(M, \prod_{\lambda\in\Lambda} N_\lambda\right) \cong \prod_{\lambda\in\Lambda} \operatorname{Hom}_R(M, N_\lambda).$$

Proof. Define

$$\begin{aligned} \varphi : \operatorname{Hom}_R\left(M, \prod_{\lambda\in\Lambda} N_\lambda\right) &\to \prod_{\lambda\in\Lambda} \operatorname{Hom}_R(M, N_\lambda) \\ f &\mapsto (p_\lambda f) = (p_{\lambda *}(f)), \end{aligned}$$

where $p_\lambda : \prod_{\lambda\in\Lambda} N_\lambda \to N_\lambda$ are the natural projection. Then φ is an R-module homomorphism.

Let $(f_\lambda) \in \prod_{\lambda\in\Lambda} \mathrm{Hom}_R(M, N_\lambda)$. Define an R-module homomorphism $\theta : M \to \prod_{\lambda\in\Lambda} N_\lambda$ by $\theta(a) = (f_\lambda(a))$. Then $\varphi(\theta) = (p_\lambda\theta) = (f_\lambda)$. So φ is surjective.

$$\begin{array}{ccc} \prod_{\lambda\in\Lambda} N_\lambda & \xleftarrow{\ \theta\ } & M \\ {\scriptstyle p_\lambda}\downarrow & \swarrow {\scriptstyle f_\lambda} & \\ N_\lambda & & \end{array}$$

Let $f \in \mathrm{Hom}_R(M, \prod_{\lambda\in\Lambda} N_\lambda)$. Claim. If $p_\lambda f = 0$ for each $\lambda \in \Lambda$, then $f = 0$. Suppose $f \neq 0$. Then $(b_\lambda) := f(a) \neq 0$ for some $a \in M$ and so $b_\lambda \neq 0$ for some $\lambda \in \Lambda$. Hence $0 = 0(a) = p_\lambda f(a) = b_\lambda \neq 0$, a contradiction. So $\mathrm{Ker}(\varphi) = \{f \in \mathrm{Hom}_R(M, \prod_{\lambda\in\Lambda} N_\lambda) \mid (p_\lambda f) = 0\} = \{0\}$. Thus, φ is injective. □

Corollary 3.21. $w : \mathrm{Hom}_R(M \oplus M', N) \xrightarrow{\cong} \mathrm{Hom}_R(M, N) \oplus \mathrm{Hom}_R(M', N)$.

Proof. Let

$$\begin{array}{ccccc} M & \underset{\tau}{\overset{\epsilon}{\rightleftarrows}} & M \oplus M' & \underset{\tau'}{\overset{\epsilon'}{\leftrightarrows}} & M' \\ & & \downarrow {\scriptstyle \psi} & & \\ & & N & & \end{array}$$

Let $w(\psi) = (\psi \circ \epsilon, \psi \circ \epsilon') = (\epsilon^*(\psi), \epsilon'^*(\psi))$ for $\psi \in \mathrm{Hom}_R(M \oplus M', N)$.

$$0 \longrightarrow M \underset{\tau}{\overset{\epsilon}{\rightleftarrows}} M \oplus M' \underset{\epsilon'}{\overset{\tau'}{\rightleftarrows}} M' \longrightarrow 0$$

Note $\tau \circ \epsilon = \mathrm{id}_M$ and $\tau' \circ \epsilon' = \mathrm{id}_{M'}$.

Method 1. Since the above sequence splits, ϵ^* is onto. So $\mathrm{Hom}_R(M \oplus M', N) \cong \mathrm{Hom}_R(M, N) \oplus \mathrm{Hom}_R(M', N)$.

Method 2. Since $\epsilon^* \circ \tau^* = (\tau \circ \epsilon)^* = (\mathrm{id}_M)^* = \mathrm{id}_{\mathrm{Hom}_R(M,N)}$, ϵ^* is surjective since it has right inverse and thus the above sequence is a SES. (The other way around is also a SES). So $\mathrm{Hom}_R(M \oplus M', N) \cong \mathrm{Hom}_R(M, N) \oplus \mathrm{Hom}_R(M', N)$.

$$0 \longrightarrow \mathrm{Hom}_R(M', N) \underset{\epsilon'^*}{\overset{\tau'^*}{\rightleftarrows}} \mathrm{Hom}_R(M \oplus M', N) \underset{\tau^*}{\overset{\epsilon^*}{\rightleftarrows}} \mathrm{Hom}_R(M, N) \longrightarrow 0$$

Method 3. Check w is a well-defined homomorphism since ϵ^* and ϵ'^* are well-defined homomorphisms.

$$\begin{array}{ccccccccc} 0 \longrightarrow & \mathrm{Hom}_R(M', N) & \xrightarrow{\tau'^*} & \mathrm{Hom}_R(M \oplus M', N') & & \xrightarrow{\epsilon^*} & & \mathrm{Hom}_R(M, N) & \longrightarrow 0 \\ & & \alpha \longmapsto \alpha \circ \tau' & & \psi & \longmapsto & \psi \circ \epsilon & & \\ & {\scriptstyle =}\downarrow & \downarrow \quad\quad \downarrow & \downarrow {\scriptstyle w} & \downarrow & & \downarrow & \downarrow{\scriptstyle =} & \\ & & \alpha \longmapsto (0, \alpha) & & (\psi \circ \epsilon, \psi \circ \epsilon') & \longmapsto & \psi \circ \epsilon & & \\ 0 \longrightarrow & \mathrm{Hom}_R(M', N) & \xrightarrow{E'} & \mathrm{Hom}_R(M \oplus M', N') & & \xrightarrow{T} & & \mathrm{Hom}_R(M, N) & \longrightarrow 0 \end{array}$$

since $(0,\alpha) = (\alpha \circ \tau' \circ \epsilon, \alpha \circ \tau' \circ \epsilon') = w(\alpha \circ \tau')$. So the squares commutes. Thus, by short 5-lemma or snake lemma or diagram chase, we have w is an isomorphism. $\square$

Corollary 3.22.

$$\begin{aligned} w_n : \operatorname{Hom}_R\left(\bigoplus_{i=1}^{n} M_i, N\right) &\to \bigoplus_{i=1}^{n} \operatorname{Hom}_R(M_i, N) \\ \psi &\mapsto \begin{bmatrix} \epsilon_1^*(\psi) \\ \vdots \\ \epsilon_n^*(\psi) \end{bmatrix} \end{aligned}$$

where

$$\begin{aligned} \epsilon_j : M_j &\to \bigoplus_{j=1}^{n} M_i \\ m_j &\mapsto \begin{bmatrix} 0 \\ \vdots \\ m_j \\ \vdots \\ 0 \end{bmatrix} \end{aligned}$$

Example 3.23.

$$\begin{aligned} w_n : \operatorname{Hom}_R(R^n, R) &\to R^n \\ \psi &\mapsto \begin{bmatrix} \psi(\vec{e}_1) \\ \vdots \\ \psi(\vec{e}_n) \end{bmatrix} \end{aligned}$$

where $\vec{e}_1, \dots, \vec{e}_n$ is standard basis on $\mathbb{R}^n$. It is a special case. of previous corollary. Or we can prove it by induction. If $n = 1$, $\operatorname{Hom}_R(R, R) \xrightarrow{\cong} R$ given by $\psi \mapsto \psi(1)$

Example 3.24. Let $R^n \xrightarrow{\phi} R^m$ be an R-module homomorphism. Let $A \in \operatorname{Mat}_{m\times n}$. For $j = 1, \dots, n$, let the j^{th} column of A be $\phi(\vec{v}_j)$, where $\{\vec{v}_j\}$ is the standard basis of R^n. Then $Ax = [\phi(x)]_{\{v_j\}}$ or $\sum_{j=1}^{n} (Ax)_j = \phi(x)$ for $x \in R^n$. Apply $\operatorname{Hom}_R(-, R)$,

$$\begin{array}{ccccc} \operatorname{Hom}_R(R^m, R) & & \xrightarrow[A^*]{\phi^*} & & \operatorname{Hom}_R(R^n, R) \\ & \vec{e}_i^* & \longmapsto & \vec{e}_i^* \circ \phi & \\ \cong \Big\downarrow w_m & \Big\downarrow & & \Big\downarrow & \cong \Big\downarrow w_n \\ & \vec{e}_i & \longmapsto & (A^T)_i & \\ R^m & & \xrightarrow[A^T]{} & & R^n \end{array}$$

Note $\operatorname{Hom}_R(R^m, R) \cong R^m$ and $\operatorname{Hom}_R(R^m, R)$ is free with dual basis $\vec{e}_1^*, \ldots, \vec{e}_m^*$, where $\vec{e}_i^*(\vec{e}_j) = \delta_{ij}$ for $1 \leqslant i, j \leqslant m$. Let's check commutativity on generators (basis). Note $w_m(\vec{e}_i^*) = \begin{bmatrix} \vec{e}_i^*(\vec{e}_1) \\ \vdots \\ \vec{e}_i^*(\vec{e}_m) \end{bmatrix} = \vec{e}_i$ for $i = 1, \ldots, m$. Note for $i = 1, \ldots, m$ and $j = 1, \ldots, n$,

$$(\vec{e}_i^* \circ \phi)(\vec{v}_j) = \vec{e}_i^*(\phi(\vec{v}_j)) = \vec{e}_i^*(j^{\text{th}} \text{ col. of } A) = \vec{e}_i^*\left(\sum_{k=1}^{m} a_{kj}\vec{e}_k\right) = a_{ij} = j^{\text{th}} \text{ entry of } i^{\text{th}} \text{ col. of } A^T.$$

So $w_n(\vec{e}_i^* \circ \phi) = \begin{bmatrix} (\vec{e}_i^* \circ \phi)(\vec{v}_1) \\ \vdots \\ (\vec{e}_i^* \circ \phi)(\vec{v}_n) \end{bmatrix}$ is the i^{th} column of A^T, i.e., the i^{th} row of A.

Remark. When R on right was changed to N, the similar conclusion also holds.

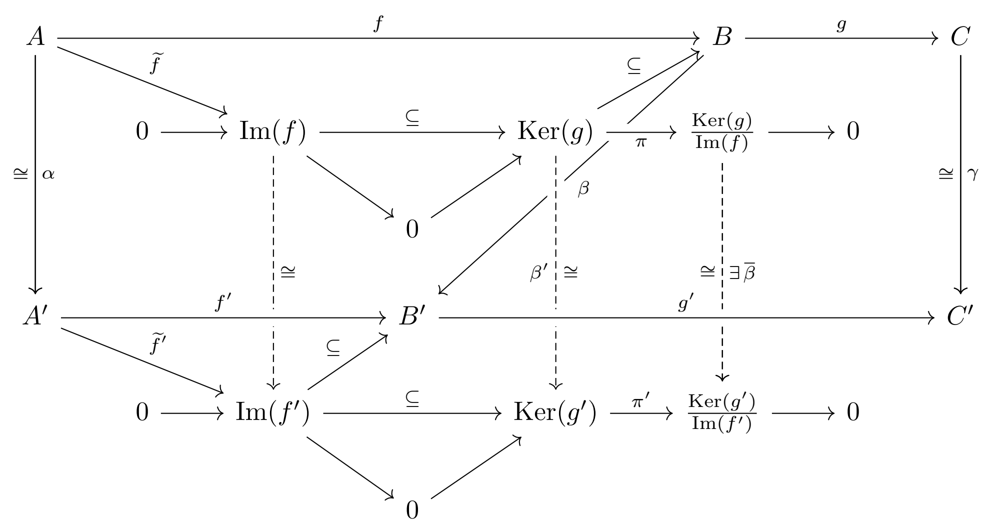
Lemma 3.25. Consider commutative diagram of R-modules and R-module homomorphism.

$$\begin{array}{ccccc} A & \xrightarrow{f} & B & \xrightarrow{g} & C \\ \cong\downarrow\alpha & & \downarrow\beta & & \cong\downarrow\gamma \\ A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' \end{array}$$

Assume $g \circ f = 0$, so $g' \circ f' = 0$. Then there exists a well-defined isomorphism.

$$\begin{aligned} \overline{\beta} : \frac{\operatorname{Ker}(g)}{\operatorname{Im}(f)} &\xrightarrow{\cong} \frac{\operatorname{Ker}(g')}{\operatorname{Im}(f')} \\ b + \operatorname{Im}(f) &\mapsto \beta(b) + \operatorname{Im}(f') \\ \textit{or } \bar{b} &\mapsto \overline{\beta(b)}. \end{aligned}$$

Proof. Sketch:



∎

Theorem 3.26.

$$\begin{aligned}\gamma:\ U^{-1}(M\oplus M') &\xrightarrow{\cong} U^{-1}M\oplus U^{-1}M'\\ \frac{(m,m')}{u} &\mapsto \left(\frac{m}{u},\frac{m'}{u}\right)\\ \frac{(u'm,um')}{uu'} &\leftarrow\!\shortmid \left(\frac{u'm}{uu'},\frac{um'}{uu'}\right)=\left(\frac{m}{u},\frac{m'}{u'}\right)\end{aligned}$$

Theorem 3.27.

$$\begin{aligned}U^{-1}\left(\bigoplus_{i=1}^{n}M_i\right) &\xrightarrow{\cong} \bigoplus_{i=1}^{n}U^{-1}M_i\\ \begin{pmatrix}m_1\\ \vdots\\ m_n\end{pmatrix}\Big/ u &\mapsto \begin{pmatrix}\frac{m_1}{u}\\ \vdots\\ \frac{m_n}{u}\end{pmatrix}\end{aligned}$$

Remark. The two above isomorphisms are R-linear and $U^{-1}R$-linear.

Remark. Since $U^{-1}(R^n)\cong(U^{-1}R)^n$, there is no ambiguity to write $U^{-1}R^n$.

Theorem 3.28. *Let $R^m \xrightarrow{(a_{ij})} R^n$. Then we have the following commutative diagram.*

$$\begin{array}{ccc}U^{-1}R^m & \xrightarrow{U^{-1}(a_{ij})} & U^{-1}R^n\\ \downarrow\cong & & \downarrow\cong\\ (U^{-1}R)^m & \xrightarrow[\cdot(a_{ij})]{(\frac{a_{ij}}{1})} & (U^{-1}R)^n\end{array}$$

3.1 homomorphism and localization

Theorem 3.29. *(a) For $\frac{\phi}{u}\in U^{-1}\operatorname{Hom}_R(M,N)$, the map*

$$\begin{aligned}\phi_u: U^{-1}M &\to U^{-1}N\\ \frac{m}{v} &\mapsto \frac{\phi(m)}{uv}\end{aligned}$$

is a well-defined $U^{-1}R$-module homomorphism.

(b) The function

$$\begin{aligned}\Theta_{U,M,N}: U^{-1}\operatorname{Hom}_R(M,N) &\to \operatorname{Hom}_{U^{-1}R}(U^{-1}M,U^{-1}N)\\ \frac{\phi}{u} &\mapsto \phi_u\end{aligned}$$

is a well-defined $U^{-1}R$ module homomorphism.

(c) If M is finitely presented, i.e., there exists an exact sequence $R^m\xrightarrow{f}R^n\xrightarrow{g}M\to 0$, then $\Theta_{U,M,N}$ is an isomorphism.

(d) If R is noetherian and M is finitely generated, then

$$\Theta_{U,M,N} : U^{-1}\operatorname{Hom}_R(M,N) \xrightarrow{\cong} \operatorname{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N).$$

Proof. (a) Step 1: for $u \in U$ and $\phi \in \operatorname{Hom}_R(M,N)$, we have $\phi_u(\frac{m}{v}) = \frac{\phi(m)}{uv} = \frac{1}{u}(U^{-1}\phi)(\frac{m}{v}) = ((\text{mult. } \circ \text{ by } \frac{1}{u}) \circ (U^{-1}\phi))(\frac{m}{v})$, where multiplication $\circ$ by $\frac{1}{u}$ and $U^{-1}\phi$ is a well-defined $U^{-1}R$-module homomorphism and so the composition is a well-defined $U^{-1}R$-module homomorphism.

Step2: Let $\frac{\phi}{u} = \frac{\phi'}{u'}$. Then $\exists u'' \in U$ such that $uu''\phi' = u'u''\phi$. So $(uu''\phi')(m) = (u'u''\phi)(m)$. Then $uu'' \cdot \phi'(m) = u'u'' \cdot \phi(m)$. So $\phi_u(\frac{m}{v}) = \frac{\phi(m)}{uv} = \frac{u'u''\phi(m)}{u'u''uv} = \frac{uu''\phi'(m)}{u'u''uv} = \frac{\phi'(m)}{u'v} = \phi'_{u'}(\frac{m}{v})$. Hence $\phi_u = \phi'_{u'}$.

(b) Part (a) implies $\Theta_{U,M,N}$ is well-defined. Note $\Theta_{U,M,N}$ respects addition. $\Theta_{U,M,N}(\frac{r}{t} \cdot \frac{\phi}{u}) = \Theta_{U,M,N}(\frac{r\phi}{tu}) = (r\phi)_{tu}$ and $\frac{r}{t}\Theta_{U,M,N}(\frac{\phi}{u}) = \frac{r}{t} \cdot \phi_u$. Since ϕ_u is an $U^{-1}R$-module homomorphism, $(r\phi)_{tu}(\frac{m}{v}) = \frac{r\phi(m)}{tuv} = \frac{r \cdot \phi(m)}{tuv}$ and $(\frac{r}{t} \cdot \phi_u)(\frac{m}{v}) = \frac{r}{t} \cdot \phi_u(\frac{m}{v}) = \frac{r}{t} \cdot \frac{\phi(m)}{uv}$, we have $\Theta_{U,M,N}(\frac{r}{t} \cdot \frac{\phi}{u}) = (r\phi)_{tu} = \frac{r}{t} \cdot \phi_u = \frac{r}{t}\Theta_{U,M,N}(\frac{\phi}{u})$.

(c) Step 1. $\Theta_{U,M\oplus M',N}$ is an isomorphism if and only if $\Theta_{U,M,N}$ and $\Theta_{U,M',N}$ are both isomorphisms. NTS: $\Theta_{U,M\oplus M',N}$ is an isomorphism if and only if $\Theta_{U,M,N} \oplus \Theta_{U,M',N}$ is an isomorphism. NTS: the following diagram commutes.

$$\begin{array}{ccc}
U^{-1}\operatorname{Hom}_R(M\oplus M', N) & \xrightarrow{\Theta_{U,M\oplus M',N}} & \operatorname{Hom}_{U^{-1}R}(U^{-1}(M\oplus M'), U^{-1}N) \\
{\scriptstyle U^{-1}w}\big\downarrow{\scriptstyle \cong} & & \big\downarrow{\scriptstyle \gamma^{-1*}} \\
U^{-1}(\operatorname{Hom}_R(M,N)\oplus \operatorname{Hom}_R(M',N)) & & \operatorname{Hom}_{U^{-1}R}((U^{-1}M)\oplus(U^{-1}M'), U^{-1}N) \\
{\scriptstyle \cong}\big\downarrow{\scriptstyle \Gamma} & & {\scriptstyle \cong}\big\downarrow{\scriptstyle \Omega} \\
U^{-1}\operatorname{Hom}_R(M,N)\oplus U^{-1}\operatorname{Hom}_R(M',N) & \xrightarrow{\Theta_{U,M,N}\oplus\Theta_{U,M',N}} & \operatorname{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N)\oplus \\
& & \operatorname{Hom}_{U^{-1}R}(U^{-1}M', U^{-1}N)
\end{array}$$

The corresponding map is

$$\begin{array}{ccc}
\frac{\psi}{u} & \longmapsto & \phi_u \\
\big\downarrow & & \big\downarrow \\
\frac{w(\psi)}{u} = \frac{(\psi\circ\epsilon, \psi\circ\epsilon')}{u} & & \psi_u \circ \gamma^{-1} \\
\big\downarrow & & \big\downarrow \\
(\frac{\psi\circ\epsilon}{u}, \frac{\psi\circ\epsilon'}{u}) & & (\psi_u\circ\gamma^{-1}\circ j, \psi_u\circ\gamma^{-1}\circ j') \\
& \searrow & \\
& & (\Theta_{U,M,N}(\frac{\phi\circ\epsilon}{u}), \Theta_{U,M',N}(\frac{\psi\circ\epsilon'}{u})) \\
& & \| \\
& & ((\psi\circ\epsilon)_u, (\psi\circ\epsilon')_u)
\end{array}$$

where $U^{-1}M \xrightarrow{j} (U^{-1}M) \oplus (U^{-1}M') \xrightarrow{j'} U^{-1}M'$. Recall the definitions

$$M \xrightarrow{\epsilon} M \oplus M' \xrightarrow{\epsilon'} M'.$$

$$\begin{array}{rcl} \gamma:\ U^{-1}(M \oplus M') & \xrightarrow{\cong} & U^{-1}M \oplus U^{-1}M' \ \ : \gamma^{-1} \\ \dfrac{(m,m')}{u} & \mapsto & \left(\dfrac{m}{u}, \dfrac{m'}{u}\right) \\ \dfrac{(u'm, um')}{uu'} & \leftarrow\!\shortmid & \left(\dfrac{u'm}{uu'}, \dfrac{um'}{uu'}\right) = \left(\dfrac{m}{u}, \dfrac{m'}{u'}\right) \end{array}$$

Note $(\psi \circ \epsilon)_u(\frac{m}{v}) = \frac{(\psi\circ\epsilon)(m)}{uv} = \frac{\psi(\epsilon(m))}{uv} = \frac{\psi(m,0)}{uv}$, $(\psi_u \circ \gamma^{-1} \circ j)(\frac{m}{v}) = \phi_u(\gamma^{-1}(j(\frac{m}{v}))) = \psi_u(\gamma^{-1}(\frac{m}{v}, 0)) = \phi_u(\gamma^{-1}(\frac{m}{v}, \frac{0}{v})) = \phi_u(\frac{(m,0)}{v}) = \frac{\psi(m,0)}{uv'}$. So $(\psi \circ \epsilon)_u = \psi_u \circ \gamma^{-1} \circ j$.

Step 2: $\Theta_U, \oplus_{i=1}^n M_i, N$ is an isomorphism if and only if $\Theta_{U,M_i,N}$ is an isomorphism$\forall i = 1, \ldots, n$. Check this by inducting on n and using step 1 several times.

Step 3: $\Theta_{U,R^n,N}$ is an isomorphism. By step 2, it suffices to show $\Theta_{U,R,N}$ is an isomorphism.

$$\begin{array}{ccc} U^{-1}\operatorname{Hom}_R(R,N) & \xrightarrow{\Theta_{U,R,N}} & \operatorname{Hom}_{U^{-1}R}(U^{-1}R, N) \\ {\scriptstyle U^{-1}f}\downarrow\cong & \Phi(1) \leftarrow\!\shortmid \Phi & \swarrow F \\ U^{-1}N & & \end{array}$$

where $f : \operatorname{Hom}_R(R,N) \xrightarrow{\cong} N$ given by $\psi \mapsto \psi(1)$.

Step 4: Assume $(\ddagger :) R^m \xrightarrow{f} R^n \xrightarrow{g} M \to 0$ is exact. Then

$$\operatorname{Hom}_R(\ddagger, N):\ 0 \to \operatorname{Hom}_R(M,N) \xrightarrow{g^*} \operatorname{Hom}_R(R^n,N) \xrightarrow{f^*} \operatorname{Hom}_R(R^m,N)$$

is exact. Since $U^{-1}(-)$ is exact,

$$U^{-1}\operatorname{Hom}_R(\ddagger, N):\ 0 \to U^{-1}\operatorname{Hom}_R(M,N) \xrightarrow{U^{-1}g^*} U^{-1}\operatorname{Hom}_R(R^n,N) \xrightarrow{U^{-1}f^*} U^{-1}\operatorname{Hom}_R(R^m,N)$$

and $\operatorname{Hom} U_R^{-1}(U^{-1}(\ddagger), U^{-1}(N))$:

$$0 \to \operatorname{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N) \to U^{-1}\operatorname{Hom}_{U^{-1}R}(U^{-1}R^n, U^{-1}N) \to \operatorname{Hom}_{U^{-1}R}(U^{-1}R^m, U^{-1}N)$$

are exact.

$$\begin{array}{ccccccc} 0 \longrightarrow & U^{-1}\operatorname{Hom}_R(M,N) & \xrightarrow{U^{-1}g^*} & U^{-1}\operatorname{Hom}_R(R^n,N) & \xrightarrow{U^{-1}f^*} & U^{-1}\operatorname{Hom}_R(R^m,N) \\ & \downarrow{\scriptstyle\Theta_{U,M,N}} & & \cong\downarrow{\scriptstyle\Theta_{U,R^n,N}} & & {\scriptstyle\Theta_{U,R^m,N}}\downarrow\cong \\ 0 \to & \operatorname{Hom}_{U^{-1}R}(U^{-1}M, U^{-1}N) & \to & \operatorname{Hom}_{U^{-1}R}(U^{-1}R^n, U^{-1}N) & \to & \operatorname{Hom}_{U^{-1}R}(U^{-1}R^m, U^{-1}N) \end{array}$$

As before, it implies $\Theta_{U,M,N}$ is an isomorphism. $(-)^+ := \text{Hom}_{U^{-1}R}(-, U^{-1}N)$.

(d) If R is noetherian and M is f.g., then exercise implies there exists an exact sequence

$$\cdots \to R^b \to R^q \to R^m \to R^n \to M \to 0.$$

So $R^m \to R^n \to M \to 0$ is exact and then M is finitely presented. Thus, by part (c), $\Theta_{U,M,N}$ is an isomorphism.

□

Chapter 4

Associated Primes and Support of Modules

Let R be nonzero commutative ring with identity, M, N, M' be R-modules and $I \leqslant R$.

Definition 4.1. The *prime spectrum* of R is

$$\operatorname{Spec}(R) = \{\text{prime ideals of } R\}.$$

$$\operatorname{V}(I) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}.$$

$$\operatorname{rad}(I) = \{x \in R \mid \exists n \geqslant 1 \text{ s.t. } x^n \in I\},$$

which is the *radical* of I.

Notation 4.2. $\operatorname{rad}(I) = r(I) = \sqrt{I}$.

Example 4.3. Let R be a PID, then a UFD. For non-unit $x \in R \smallsetminus \{0\}$ (if exists), there exists prime element $p_1, \ldots, p_n \in R$ and $e_1, \ldots, e_n \geqslant 1$ such that $x = p_1^{e_1} \cdots p_n^{e_n}$, where $p_i R \neq p_j R$ for $1 \leqslant i, j \leqslant n$ with $i \neq j$. Let $I = xR$. Then $\operatorname{V}(I) = \{p_1 R, \ldots, p_n R\}$, essentially because for a prime $p \in R$, we have $p \mid x$ if and only if $p \sim p_i$ for some $i \in \{1, \ldots, n\}$ (i.e., $pR = p_i R$). Then $\operatorname{rad}(I) = \operatorname{rad}(p_1^{e_1} \cdots p_n^{e_n} R) = p_1 \cdots p_n R$.

"$\supseteq$". Let $e = \max\{e_1, \ldots, e_n\}$. Then $(p_1 \cdots p_n)^e = p_1^e \cdots p_n^e \in p_1^{e_1} \cdots p_n^{e_n} R$. So $p_1 \cdots p_n \in \operatorname{rad}(I)$. Since $\operatorname{rad}(I)$ is an ideal, $p_1 \cdots p_n R \subseteq \operatorname{rad}(I)$.

"$\subseteq$". Let $y \in \operatorname{rad}(I)$. Then $y^n \in I$ for some $n \geqslant 1$. So $x \mid y^n$. Hence $p_1 \cdots p_n \mid y$.

Example 4.4. Let $x = 2^5 13^{17} 19 \in \mathbb{Z}$. Then $\operatorname{V}(2^5 13^{17} 19\mathbb{Z}) = \{2\mathbb{Z}, 3\mathbb{Z}, 19\mathbb{Z}\}$ and $\operatorname{rad}(2^5 13^{17} 19\mathbb{Z}) = 2 \cdot 13 \cdot 19\mathbb{Z}$.

Remark. Let $I \leqslant R$.

(a) $\operatorname{rad}(I) \leqslant R$.

(b) If $J \leqslant R$ such that $J \subseteq I$, then $\operatorname{rad}(J) \subseteq \operatorname{rad}(I)$.

(c) $\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$.

Theorem 4.5. $\operatorname{rad}(I) = \bigcap_{\mathfrak{p}\in \mathrm{V}(I)} \mathfrak{p}$.

Proof. Note $\mathrm{V}(I) = \emptyset$ if and only if $I = R$.

"$\subseteq$". If $x \in \operatorname{rad}(I)$, then $x^n \in I$ for some n. Let $\mathfrak{p} \in \mathrm{V}(I)$. Then $x^n \in I \subseteq \mathfrak{p}$. So $x \in \mathfrak{p}$. Hence $\operatorname{rad}(I) \subseteq \mathfrak{p}$.

"$\supseteq$". Let $x \in R \setminus \operatorname{rad}(I)$. Let $S = \{1, x, x^2, \cdots\}$ be multiplicative closed. Since $x \notin \operatorname{rad}(I)$, we have $S \cap \operatorname{rad}(I) = \emptyset$. So $S^{-1}\operatorname{rad}(I) \lneq S^{-1}R$. Then $S^{-1}R$ has a maximal ideal $S^{-1}\mathfrak{m}$ containing $S^{-1}\operatorname{rad}(I)$. Hence $\mathfrak{m} \in \operatorname{Spec}(R)$ satisfying $\mathfrak{m} \cap S = \emptyset$ and $\operatorname{rad}(I) \subseteq \mathfrak{m}$. So $\mathfrak{m} \in \mathrm{V}(\operatorname{rad}(I)) = \mathrm{V}(I)$. Since $\mathfrak{m} \cap S = \emptyset$, we have $x \notin \mathfrak{m}$. Thus, $x \notin \bigcap_{\mathfrak{p}\in \mathrm{V}(I)} \mathfrak{p}$. □

Definition 4.6. Let $m \in M$, the *annihilator* of m is

$$\operatorname{Ann}_R(m) = \{r \in R \mid rm = 0\}.$$

Definition 4.7. The *annihilator* of M is

$$\operatorname{Ann}_R(M) = \{r \in R \mid rM = 0\} = \{r \in R \mid rm = 0, \forall m \in M\} = \bigcap_{m\in M} \operatorname{Ann}_R(m).$$

Definition 4.8. The *support* of M is

$$\operatorname{Supp}_R(M) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\} \subseteq \operatorname{Spec}(R).$$

Remark. (a) Let $U \subseteq R$ be multiplicatively closed. For $m \in M$, we have $\frac{0}{1} = 0 = \frac{m}{1} \in U^{-1}M$ if and only if there exists $u \in U$ such that $um = 0$ if and only if $U \cap \operatorname{Ann}_R(m) \neq \emptyset$.

(b) Assume M is finitely generated. Then $U^{-1}M = 0$ if and only if there exists $u \in U$ such that $uM = 0$ if and only if $U \cap \operatorname{Ann}_R(M) \neq \emptyset$.

Proof. (b) If $u \in U$ such that $uM = 0$, then $um = 0$ for $m \in M$. Then in $U^{-1}M$, $\frac{m}{v} = \frac{um}{uv} = \frac{0}{uv} = 0$ for $\frac{m}{v} \in U^{-1}M$. So $U^{-1}M = 0$. Assume $M = \langle m_1, \ldots, m_n\rangle$ for $m_1, \ldots, m_n \in M$ and $U^{-1}M = 0$. Since $\frac{m_i}{1} \in U^{-1}M = 0$, by (a), there exists $u_i \in U$ such that $u_i m_i = 0$ for $i = 1, \ldots, n$. So $u := u_1 \cdots u_n \in U$ satisfying $um_i = 0$ for $i = 1, \ldots, n$. Thus, $uM = 0$. □

Theorem 4.9. $\operatorname{Ann}_R(m)$, $\operatorname{Ann}_R(M) \leqslant R$.

Theorem 4.10. $\operatorname{Supp}_R(R) = \operatorname{Spec}(R)$.

Proof. "$\subseteq$". By definition.

"$\supseteq$". Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Since $1 \notin \mathfrak{p}$, $0 \neq \frac{1}{1} \in R_{\mathfrak{p}}$. So $R_{\mathfrak{p}} \neq 0$. Hence $\mathfrak{p} \in \operatorname{Supp}_R(R)$. □

Theorem 4.11. $\operatorname{Supp}_R(R/I) = \mathrm{V}(I)$.

Proof. Let $\mathfrak{p} \in \operatorname{Spec}(R) = \operatorname{Supp}_R(R)$. Then $R_{\mathfrak{p}} \neq 0$. Note $I_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}$ if and only if $I \cap (R \setminus \mathfrak{p}) = \emptyset$ if and only if $\mathfrak{p} \supseteq I$ if and only if $\mathfrak{p} \in \mathrm{V}(I)$. Since $0 \to I \to R \to R/I \to 0$ is exact and localization is exact, we have $0 \to I_{\mathfrak{p}} \to R_{\mathfrak{p}} \to (R/I)_{\mathfrak{p}} \to 0$ is also exact. So $(R/I)_{\mathfrak{p}} \cong R_{\mathfrak{p}}/I_{\mathfrak{p}}$. Thus, $\mathfrak{p} \in \operatorname{Supp}_R(R/I)$ if and only if $(R/I)_{\mathfrak{p}} \neq 0$ if and only if $R_{\mathfrak{p}}/I_{\mathfrak{p}} \neq 0$ if and only if $I_{\mathfrak{p}} \subsetneq R_{\mathfrak{p}}$ if and only if $\mathfrak{p} \in \mathrm{V}(I)$. □

Remark. $\operatorname{Supp}_R(R/I) = \mathrm{V}(I) = \mathrm{V}(\operatorname{rad}(I)) = \operatorname{Supp}_R(R/\operatorname{rad}(I))$.

Theorem 4.12. *If M is finitely generated, then* $\operatorname{Supp}_R(M) = \mathrm{V}(\operatorname{Ann}_R(M))$.

Proof. Since M is finitely generated, $0 = M_{\mathfrak{p}} = (R \smallsetminus \mathfrak{p})^{-1}M$ if and only if $(R \smallsetminus \mathfrak{p}) \cap \mathrm{Ann}_R(M) \neq \emptyset$. Then $\mathfrak{p} \in \mathrm{Supp}_R(M)$ if and only if $M_{\mathfrak{p}} \neq 0$ if and only if $(R \smallsetminus \mathfrak{p}) \cap \mathrm{Ann}_R(M) = \emptyset$ if and only if $\mathfrak{p} \in \mathrm{V}(\mathrm{Ann}_R(M))$. □

Example 4.13. Let k be a field and $R = k[X, Y]$.

(a) Let $f \in R$, then $\mathrm{Supp}_R(R/fR) = \mathrm{V}(fR) = \{\mathfrak{p} \in \mathrm{Spec}(R) \mid f \in \mathfrak{p}\}$.

(b) Let $m, n \in \mathbb{N}$. Then $\mathrm{Supp}_R(R/(X^m, Y^n)R) = \{(X, Y)R\} = \mathrm{Supp}_R(R/((X, Y)R)^m)$.

(c) $\mathrm{Supp}_R(R/(X^2, XY)R) = \mathrm{V}(XR) = \mathrm{Supp}_R(R/XR)$ and $\mathrm{rad}((X^2, XY)R) = XR$.

Proof. (b) For the first equality, it suffices to show $\mathrm{V}((X^m, Y^n)R) = \{(X, Y)R\}$. Let $\mathfrak{p} \in \mathrm{Spec}(R)$. Then $\mathfrak{p} \in \mathrm{V}((X^m, Y^n)R)$ if and only if $(X^m, Y^n)R \subseteq \mathfrak{p}$ if and only if $X^m, Y^n \in \mathfrak{p}$ if and only if $X, Y \in \mathfrak{p}$ if and only if $(X, Y)R \subseteq \mathfrak{p} \subsetneq R$ if and only if $(X, Y)R = \mathfrak{p}$ since $(X, Y)R \in \text{m-Spec}(R)$. □

Remark. Let k be a field and $R = k[X, Y]$. Then $(X^m, Y^n)R := \{(a, b) \mid a \geqslant X^m, b \geqslant Y^n\}$. By binomial theorem,

$$((X, Y)R)^m = (X^m, X^{m-1}Y, \ldots, Y^m)R = X^mR + (X^{m-1}Y)R + \cdots + Y^mR.$$

Definition 4.14. $\mathfrak{p} \in \mathrm{Spec}(R)$ is *associated* to M if there exists $m \in M$ such that $\mathfrak{p} = \mathrm{Ann}_R(m)$.

$$\begin{aligned}\mathrm{Ass}_R(M) &= \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \text{ is a associated to } M\} \\ &= \{\mathrm{Ann}_R(m) \leqslant R \mid m \in M\} \cap \mathrm{Spec}(R) \\ &= \{\mathrm{Ann}_R(m) \leqslant R \mid m \in M \text{ and } \mathrm{Ann}_R(m) \in \mathrm{Spec}(R)\}.\end{aligned}$$

Example 4.15. Let $\mathfrak{p} \in \mathrm{Spec}(R)$ and $r + \mathfrak{p} \in R/\mathfrak{p}$ with $r \in R$. Then $\mathrm{Ann}_R(r + \mathfrak{p}) = \begin{cases} R & \text{if } r \in \mathfrak{p} \\ \mathfrak{p} & \text{if } r \notin \mathfrak{p} \end{cases}$ since $R/\mathfrak{p}$ is an integral domain with $0_{R/\mathfrak{p}} = \mathfrak{p}$ and $\bar{r} \neq 0_{R/\mathfrak{p}}$. So $\mathrm{Ann}_R(R/\mathfrak{p}) = \bigcap_{r \in R} \mathrm{Ann}(\bar{r}) = \{\mathfrak{p}\}$ and $\mathrm{Ass}_R(R/\mathfrak{p}) = \mathfrak{p}$.

Example 4.16. Assume R is UFD and $I = xR$.

(a) If $x \in R^\times$, then $xR = R$ and $R/xR = 0$. So $\mathrm{Ass}_R(R/xR) = \mathrm{Ass}_R(0) = \emptyset$.

(b) If $x = 0$, then $xR = 0$ and $R/xR = R$. Since R is an integral domain, $\mathrm{Ass}_R(R/xR) = \mathrm{Ass}_R(R) = \{0\}$.

(c) Let $x \in R \smallsetminus \{R^\times \cup 0\}$. Let $x = p_1^{e_1} \cdots p_n^{e_n}$ such that $p_1, \ldots, p_n$ are distinct primes and $e_1, \ldots, e_n \geqslant 1$. Claim $\mathrm{Ass}(R/xR) = \{p_1R, \ldots, p_nR\}$. "$\supseteq$". Let $x' = p_1^{e_1-1}p_2^{e_2} \cdots p_n^{e_n}$. Since R is a UFD, $p_1R = \{r \in R \mid rx' \in xR\} = \{r \in R \mid r(x' + xR) = 0_{R/xR}\} = \mathrm{Ann}_R(x' + xR)$. So $p_1R \in \mathrm{Ass}(R/xR)$. By symmetry, $p_iR \in \mathrm{Ass}_R(R/xR)$ for $i = 1, \ldots, n$. "$\subseteq$". Let $\mathfrak{p} \in \mathrm{Ass}(R/xR)$. Then there exists $\bar{y} \in R/xR$ with $y \in R$ such that $\mathfrak{p} = \mathrm{Ann}_R(\bar{y}) \in \mathrm{Spec}(R)$. Also, since R is UFD, $\mathrm{Ann}_R(\bar{y}) = \{r \in R \mid ry \in xR\} = p_iR$ for some $i \in \{1, \ldots, n\}$.

Remark. Let k be a field and $R = k[X, Y]$.

(a) Claim. $\mathrm{Ass}_R(R/(X^m, Y^n)R) \supseteq \{(X, Y)R\}$, where we have actually equal sign by later theorem. Since $X, Y \in \mathrm{Ann}_R(X^{m-1}Y^{n-1} + (X^m, Y^n)R)$ and $1 \notin \mathrm{Ann}_R(X^{m-1}Y^{n-1} + (X^m, Y^n)R)$, we have $\mathrm{Ann}_R(X^{m-1}Y^{n-1} + (X^m, Y^n)R) = (X, Y)R$.

(b) $\text{Ass}_R(R/((X,Y)R)^3) \supseteq \{(X,Y)R\}$ since $\text{Ann}_R(XY + ((X,Y)R)^3) = (X,Y)R$,

(c) $\text{Ass}_R(R/(X^2,XY)R) \supseteq \{XR, (X,Y)R\}$ since $\text{Ann}_R(Y + (X^2,XY)R) = XR$ and $\text{Ann}_R(X + (X^2,XY)R) = (X,Y)R$.

Remark.

Proposition 4.17. We have $\mathfrak{p} \in \text{Ass}_R(M)$ if and only if there exists $R/\mathfrak{p} \hookrightarrow M$.

Proof. Let $\mathfrak{p} \in \text{Ass}_R(M)$. Then there exists $m \in M$ such that $\mathfrak{p} = \text{Ann}_R(m)$. Note $\mu_m : R \to M$ given by $r \mapsto rm$ is a well-defined R-module homomorphism. By the 1IT, there exists a 1-1 R-module homomorphism $\overline{\mu}_m = R/\mathfrak{p} \hookrightarrow M$. Conversely, if $\varphi : R/\mathfrak{p} \hookrightarrow M$ is a 1-1 R-module homomorphism, then $\varphi(\overline{1}) =: m$ satisfies $\text{Ann}_R(m) = \mathfrak{p}$. ☐

Theorem 4.18. *(c)* $\text{Ass}_R(M) \subseteq \text{Supp}_R(M)$.
Assume R is noetherian and $M \neq 0$.

(a) $\text{Ass}_R(M) \neq \emptyset$.

(b) $\text{ZD}_R(M) := \{$*zero divisors on M in R*$\} = \bigcup_{\mathfrak{p} \in \text{Ass}_R(M)} \mathfrak{p}$.

Proof. (c) Let $\mathfrak{p} \in \text{Ass}_R(M)$. Then there exists 1-1 R-module homomorphism $R/\mathfrak{p} \hookrightarrow M$. So $(R/\mathfrak{p})_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$. Then since $(R/\mathfrak{p})_\mathfrak{p} \cong R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong Q(R/\mathfrak{p})$ is a field, $0 \neq Q(R/\mathfrak{p})$. So $M_\mathfrak{p}$ contains a non-zero submodule. Then $M_\mathfrak{p} \neq 0$. So $\mathfrak{p} \in \text{Supp}_R(M)$.

(b) Let $A_R(M) := \{\text{Ann}_R(m) \mid m \in M \smallsetminus \{0\}\}$ be a set of ideals of R. Then $\text{ZD}_R(M) = \bigcup_{J \in A_R(M)} J$. Since $0_R \cdot m = 0_m$ for $m \in M$, $A_R(M) \neq \emptyset$. Since R is noetherian, $A_R(M)$ has a maximal element $I := \text{Ann}_R(m)$ for some $m \in M \smallsetminus \{0\}$. Since $M \neq 0$, $I \neq R$. Let $a, b \in R$ such that $ab \in I$. Assume $a \notin I$. Then $am \neq 0$. So $I = \text{Ann}_R(m) \subseteq \text{Ann}_R(am) \in A_R(M)$. Since I is an maximal element, $I = \text{Ann}_R(m) = \text{Ann}_R(am) \in A_R(M)$. Also, since $ab \in I$, $abm = 0$. So $b \in \text{Ann}_R(am) = I$. Thus, $I \in \text{Spec}(R)$. ☐

Remark. (a) implies every element of $A_R(M)$ is contained in an associated prime of M. So for $0 \neq m \in M$, there exists $\mathfrak{p} \in \text{Ass}_R(M)$ such that $\text{Ann}_R(m) \subseteq \mathfrak{p}$.

Theorem 4.19. *Let k be a field and $R := \prod_{i=1}^\infty k = \{(a_1, a_2, \cdots) \mid a_i \in k\}$. Then R is commutative ring with identity under componentwise operations and $1_R = (1,1,1,\cdots)$. Let $I := \bigoplus_{i=1}^\infty k = \{(a_1,a_2,\cdots) \in \prod_{i=1}^\infty k \mid a_i = 0, \forall i >> 0\}$. Then $I \subsetneq R$. Let $m_i = \{(a_1,a_2,\cdots)R \mid a_i = 0\} \in$ m-Spec(R) since $\varphi_i : R \to k$ given by $(a_1, a_2, \ldots,) \mapsto a_i$ is a ring epimorphism and $\text{Ker}(\varphi_i) = m_i$ for $i = 1, \ldots, m$. Note $I \not\subseteq m_i$ for $i \geqslant 1$. Also, since $I \neq R$, there exists $M \in$ m-Spec(R) such that $I \subseteq M \neq m_i$ for $i \geqslant 1$.*

Question 4.20. Describe M explicitly.

Remark. (a) Since I is not finitely generated, R is not Noetherian.

(b) $\text{Ass}_R(R/I) = \emptyset$ even if $R/I \neq 0$.
Moral: Previous theorem says if R is noetherian, then $\text{Ass}_R(R/I) \neq \emptyset$. Also, if $M = 0$, then $\text{Ass}_R(M) = \emptyset$.

Proof. If $\mathfrak{p} \in \text{Ass}_R(M)$, then $0 \neq R/\mathfrak{p} \hookrightarrow M$. So $M \neq 0$. ☐

Example 4.21 (Exer)**.** If R is not necessarily noetherian, but M is noetherian over R, then if $M \neq 0$, then $\operatorname{Ass}_R(M) = \emptyset$ since $R/\operatorname{Ann}_R(M)$ is noetherian given M is noetherian.

Remark (Goal)**.** If R is noetherian and M is finitely generated, then $|\operatorname{Ass}_R(M)| < \infty$. (Usually, $|\operatorname{Supp}_R(M)| = \infty$.)

Theorem 4.22. *Consider a SES* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$.

(a) $\operatorname{Supp}_R(M) = \operatorname{Supp}_R(M') \cup \operatorname{Supp}_R(M'')$.

(b) $\operatorname{Ass}_R(M) \subseteq \operatorname{Ass}_R(M') \cup \operatorname{Ass}_R(M'')$.

Proof. (a) Fact: if $0 \to A' \to A \to A'' \to 0$ is exact, then $A = 0$ if and only if $A' = 0 = A''$, and $A \neq 0$ if and only if $A' \neq 0$ or $A'' \neq 0$. Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to M''_\mathfrak{p} \to 0$ is exact. Note $\mathfrak{p} \in \operatorname{Supp}_R(M)$ if and only if $M_\mathfrak{p} \neq 0$ if and only if $M'_\mathfrak{p} \neq 0$ or $M'_\mathfrak{p} \neq 0$ if and only if $\mathfrak{p} \in \operatorname{Supp}_R(M')$ or $\mathfrak{p} \in \operatorname{Supp}_R(M'')$ if and only if $\mathfrak{p} \in \operatorname{Supp}_R(M') \cup \operatorname{Supp}_R(M'')$.

(b) Let $\mathfrak{p} \in \operatorname{Ass}_R(M')$. Then there exists $R/\mathfrak{p} \hookrightarrow M' \overset{f}{\hookrightarrow} M$. So there exists $R/\mathfrak{p} \hookrightarrow M$. Hence $\mathfrak{p} \in \operatorname{Ass}_R(M)$.

Let $\mathfrak{q} \in \operatorname{Ass}_R(M)$. Then there exists $N \subseteq M$ such that $R/\mathfrak{q} \cong N$. Let $\alpha \in R/\mathfrak{q} \cong N$ such that $\alpha \neq 0_{R/\mathfrak{q}}$. Then $\operatorname{Ann}_R(\alpha) = \mathfrak{q}$.

Case 1: Assume $N \cap \operatorname{Im}(f) \neq \{0\}$. Then then there exists $\alpha \in N \cap \operatorname{Im}(f)$. So $f(\beta) = \alpha \neq 0$ for some $\beta \in M'$. Since f is monomorphism, $\operatorname{Ann}_R(\beta) = \operatorname{Ann}_R(\alpha) = \mathfrak{q}$. Since $\beta \in M'$, $\mathfrak{q} \in \operatorname{Ass}_R(M')$.

Case 2: Assume $N \cap \operatorname{Im}(f) = \{0\}$. Then $\operatorname{Ker}(g|_N : N \to M'') = N \cap \operatorname{Ker}(g) = N \cap \operatorname{Im}(f) = \{0\}$. So $g|_N$ is 1-1. Hence $R/\mathfrak{q} \cong N \cong g(N) \subseteq M''$. So $\mathfrak{q} \in \operatorname{Ass}_R(M'')$. ☐

Lemma 4.23. Assume there exists a finite filtration $0 = M_0 \subseteq M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$. Then

(a) $\operatorname{Supp}_R(M) = \bigcup_{i=1}^n \operatorname{Supp}_R(M_i/M_{i-1})$.

(b) $\operatorname{Ass}_R(M_i) \subseteq \operatorname{Ass}_R(M) \subseteq \bigcup_{i=1}^n \operatorname{Ass}_R(M_i/M_{i-1})$.

Proof. (a) Induct on n. Base case: $n = 0, 1$, trivial. Assume $n \geqslant 2$ and result holds for any module with filtration of length $n-1$. Since M_{n-1} has filtration of length $n-1$: $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1}$, inductive hypothesis implies $\operatorname{Supp}_R(M) = \bigcup_{i=1}^{n-1} \operatorname{Supp}_R(M_i/M_{i-1})$. Since $0 \to M_{n-1} \to M_n \to M_n/M_{n-1} \to 0$ is exact, by previous Theorem, $\operatorname{Supp}_R(M) = \operatorname{Supp}_R(M_n) = \operatorname{Supp}_R(M_{n-1}) \cup \operatorname{Supp}_R(M_n/M_{n-1}) = \bigcup_{i=1}^{n-1} \operatorname{Supp}_R(M_i/M_{i-1}) \cup \operatorname{Supp}_R(M_n/M_{n-1}) = \bigcup_{i=1}^{n} \operatorname{Supp}_R(M_i/M_{i-1})$.

(b) Similarly. ☐

Corollary 4.24. If $M' \hookrightarrow M$, then $\operatorname{Ass}_R(M') \subseteq \operatorname{Ass}_R(M)$.

Lemma 4.25. Let $M = \coprod_{i=1}^n M_i = \bigoplus_{i=1}^n M_i$. Then

(a) $\operatorname{Supp}_R(M) = \bigcup_{i=1}^n \operatorname{Supp}_R(M_i)$.

(b) $\operatorname{Ass}_R(M) = \bigcup_{i=1}^n \operatorname{Ass}_R(M_i)$.

Proof. (b) Note there exists a finite filtration $0 =: M_0 \subseteq \coprod_{i=1}^{1} M_1 \subseteq \cdots \subseteq \coprod_{i=1}^{n-1} M_i \subseteq \coprod_{i=1}^{n} M_i = M$. By the 1IT, $\frac{\coprod_{i=1}^{j} M_i}{\coprod_{i=1}^{j-1} M_i} \cong M_j$ for $j = 1, \ldots, n$. So $\mathrm{Ass}_R(M) \subseteq \bigcup_{j=1}^{n} \mathrm{Ass}_R\left(\frac{\coprod_{i=1}^{j} M_i}{\coprod_{i=1}^{j-1} M_i}\right) = \bigcup_{j=1}^{n} \mathrm{Ass}_R(M_j)$. For $j = 1, \ldots, n$, define $M_j \hookrightarrow \coprod_{j=1}^{n} M_j = M$ by $m_j \to (0, \ldots, 0, m_j, 0, \ldots, 0)$. By the previous corollary, $\mathrm{Ass}_R(M_j) \subseteq \mathrm{Ass}_R(M)$. So $\bigcup_{j=1}^{n} \mathrm{Ass}_R(M_j) \subseteq \mathrm{Ass}_R(M)$.

(a) It is similar. □

Chapter 5

Prime Filtration

Let R be commutative ring with identity.

Theorem 5.1. *Assume R is Noetherian and M is finitely generated over R. Then there exists finite (prime) filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ such that there exists $\mathfrak{p}_i \in \operatorname{Spec}(R)$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $i = 1, \ldots, n$.*

Proof. If $M = 0$, use $n = 0$ (empty filtration). Assume now $M \neq 0$. Then there exists $\mathfrak{p}_1 \in \operatorname{Ass}_R(M)$. So there exists submodule $M_1 \subseteq M$ such that $M_1/M_0 \cong M_1 \cong R/\mathfrak{p}_1$. If $M_1 = M$, then stop and $n = 1$. If $M_1 \neq M$, then $M/M_1 \neq 0$ and so there exists $\mathfrak{p}_2 \in \operatorname{Ass}_R(M/M_1)$. So there exists submodule $M_1 \subseteq M_2 \subseteq M$ such that $M_2/M_1 \cong R/\mathfrak{p}_2$. If $M_2 = M$, stop and $n = 2$. Otherwise, continue the process. Process terminates in finite number of steps since M is Noetherian given R is Noetherian and M is finitely generated. □

Theorem 5.2. *Assume M has a prime filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ such that there exists $\mathfrak{p}_i \in \operatorname{Spec}(R)$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $i = 1, \ldots, n$. Then*

(a) $\operatorname{Ass}_R(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Supp}_R(M)$. *So* $|\operatorname{Ass}_R(M)| < \infty$.

(b) Let $\mathfrak{p} \in \operatorname{Spec}(R)$. Then $\mathfrak{p} \in \operatorname{Supp}_R(M)$ if and only if there exists $i \in \{1, \ldots, n\}$ such that $\mathfrak{p}_i \subseteq \mathfrak{p}$, i.e., $\operatorname{Supp}_R(M) = \bigcup_{i=1}^n \operatorname{V}(\mathfrak{p}_i)$.

Proof. (a) Note $\operatorname{Ass}_R(M) \subseteq \bigcup_{i=1}^n \operatorname{Ass}_R(M_i/M_{i-1}) = \bigcup_{i=1}^n \operatorname{Ass}_R(R/\mathfrak{p}_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Note for $i = 1, \ldots, n$, $0 \neq (R/\mathfrak{p}_i)_{\mathfrak{p}_i} \cong (M_i/M_{i-1})_{\mathfrak{p}_i} \cong \frac{(M_i)_{\mathfrak{p}_i}}{(M_{i-1})_{\mathfrak{p}_i}}$, so $0 \neq (M_i)_{\mathfrak{p}_i} \subseteq M_{\mathfrak{p}_i}$, hence $M_{\mathfrak{p}_i} \neq 0$ and thus $\mathfrak{p}_i \in \operatorname{Supp}_R(M)$.

(b) $\operatorname{Supp}_R(M) = \bigcup_{i=1}^n \operatorname{Supp}_R(M_i/M_{i-1}) = \bigcup_{i=1}^n \operatorname{Supp}_R(R/\mathfrak{p}_i) = \bigcup_{i=1}^n \operatorname{V}(\mathfrak{p}_i)$. □

Corollary 5.3. Let R be Noetherian and M be finitely generated, then $|\operatorname{Ass}_R(M)| < \infty$.

Remark. M must be finitely generated for this to hold. Fact: Let k be a field and $R = k[X]$ or $R = \mathbb{Z}$. Let $M = \bigoplus_{i=1}^\infty R/\mathfrak{p}_i$ such that $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \in \operatorname{Spec}(R)$ are distinct. Then $\operatorname{Ass}_R(M) \supseteq \{\mathfrak{p}_1, \mathfrak{p}_2, \cdots\}$.

Example 5.4. Let R be UFD and $x \in R \setminus \{R^\times \cup 0\}$. Let $x = p_1 \cdots p_n$ such that p_i is prime in R for $i = 1, \ldots, n$. Then $\operatorname{Ass}_R(R/xR) = \{p_1R, \ldots, p_nR\}$.

Proof. "$\subseteq$". Method 1. Note $(0) = (p_1 \cdots p_n)R/xR \subsetneq (p_1 \cdots p_{n-1}R)/xR \subsetneq \cdots \subsetneq p_1R/xR \subsetneq R/xR$ is a prime filtration of R/xR since for $i = 1, \ldots, n-1$,

$$\frac{p_1 \cdots p_i R/xR}{(p_1 \cdots p_{i+1}R)/xR} \cong \frac{p_1 \cdots p_i R}{p_1 \cdots p_{i+1} R} \cong \frac{R}{p_{i+1}R}$$
$$\overline{p_1 \cdots p_i x} \leftarrow\!\shortmid \bar{x}.$$

So by previous theorem, $\mathrm{Ass}_R(R/rR) \subseteq \{p_1R, \ldots, p_nR\}$.

Method 2. Claim.

$$0 \hookrightarrow \frac{R}{p_1R} \hookrightarrow \cdots \hookrightarrow \frac{R}{p_1 \cdots p_{n-2}R} \overset{\phi_2}{\hookrightarrow} \frac{R}{p_1 \cdots p_{n-1}R} \overset{\phi_1}{\hookrightarrow} \frac{R}{p_1, \ldots, p_nR} = \frac{R}{xR}$$
$$\bar{r} \mapsto \overline{p_n r}$$

is a prime filtration of R/xR. Since $\mathrm{Im}(\phi_1) = \langle \bar{p}_n \rangle$ and ϕ_1 is 1-1, $\frac{R/p_1 \cdots p_n R}{R/p_1 \cdots p_{n-1}R} \cong \frac{R/p_1 \cdots p_n R}{\bar{p}_n R/p_1 \cdots p_n R} \cong \frac{R/p_1 \cdots p_n R}{p_n R/p_1 \cdots p_n R} \cong R/p_nR$. Similarly, $\frac{R/p_1 \cdots p_i R}{\mathrm{Im}(\phi_{n-i+1})} \cong R/p_iR$ for $i = 1, \ldots, n$. So $\mathrm{Ass}_R(R/xR) \subseteq \{p_1R, \ldots, p_nR\}$.

"$\supseteq$". For $i = 1, \ldots, n$, set $p_i' = x/p_i$ and define $R/p_iR \to R/xR$ by $\bar{r} \mapsto \overline{p_i' r}$. This is a well-defined monomorphism. So $\mathrm{Ass}_R(R/rR) \supseteq \{p_1R, \ldots, p_nR\}$. □

Example 5.5. Let k be a field and $R = k[X,Y]$. Then $\mathrm{Ass}_R(R/(X^m, Y^n)R) = \{(X,Y)R\} = \mathrm{Ass}_R(R/((X,Y)R)^n)$ for $m, n \geqslant 1$.

Proof. Method1. Since $\mathfrak{q} := (X^m, Y^n)R$ is a primary ideal and $\mathrm{rad}(\mathfrak{q}) = (X,Y)R$, we have that $\mathrm{Ass}_R(R/(X^m, Y^n)R) = \{(X,Y)R\}$. □

Proof. Note that

$$0 \subseteq (X^{m-1}Y^{n-1})R/(X^m, Y^n)R \subseteq \overline{\langle X^{m-1}Y^{n-2} \rangle} \subseteq \overline{\langle X^{m-2}Y^{n-3} \rangle} \subseteq \cdots \subseteq \langle \overline{X^{m-1}Y^{n-2}}, \overline{X^{m-2}Y^{n-1}} \rangle.$$

Define $R \xrightarrow{\tau_1} \overline{\langle X^{m-1}Y^{n-1} \rangle}$ by $r \mapsto \overline{rX^{m-1}Y^{n-1}}$. Since $\overline{\langle X^{m-1}Y^{n-1} \rangle} \neq 0$, $(X,Y)R \subseteq \mathrm{Ker}(\tau_1) \subsetneq R$. Also, since $(X,Y)R \in$ m-Spec(R) , $(X,Y)R = \mathrm{Ker}(\tau_1) \subsetneq R$. Moreover, τ_1 is onto, by the 1IT, $0 \neq R/(X,Y)R \underset{\cong}{\xrightarrow{\overline{\tau_1}}} \overline{X^{m-1}Y^{n-1}}$ given by $\bar{r} \mapsto \overline{rX^{m-1}Y^{n-1}}$. Simiarly, $0 \neq \frac{\overline{\langle X^{m-1}Y^{n-2} \rangle}}{\overline{\langle X^{m-1}Y^{n-1} \rangle}} \underset{\cong}{\xrightarrow{\text{"}\tau\text{"}}} \frac{R}{(X,Y)R}$. As before, $R \xrightarrow{\tau_2} \overline{\langle X^{m-1}Y^{n-2} \rangle}$ given by $r \mapsto rX^{m-1}Y^{n-2}$ with $\mathrm{Ker}(\tau_2) = (X,Y)R$. Continue with back filtration and use induction on m to show $R/(X^mY^n)$ has filtration with m, n terms and each quotient in the filtration is isomorphic tp $R/(X,Y)R$. Since $\frac{\langle \overline{X^{m-1}Y^{n-2}}, \overline{X^{m-2}Y^{n-1}} \rangle}{\overline{\langle X^{m-1}Y^{n-2} \rangle}}$ is cyclic and $\overline{X^{m-2}Y^{n-1}} \notin \langle X^{m-1}Y^{n-2} \rangle$, we have this generator is not 0. Note $R \xrightarrow{\phi} \frac{\langle \overline{X^{m-1}Y^{n-2}}, \overline{X^{m-2}Y^{n-1}} \rangle}{\overline{\langle X^{m-1}Y^{n-2} \rangle}}$ given by $r \mapsto \overline{rX^{m-1}Y^{n-2}}$ is onto b/c generators and $\mathrm{Ker}(\varphi) = (X,Y)R$. □

Remark. In general, if $I \subseteq k[X,Y] = R$ and I is generated by some monomials X^iY^j with $i, j \geqslant 1$ and $X^m, Y^n \in I$ for some $m, n \geqslant 1$, then basis for R/I as k-vector space is finite and the number of basis vector is the area of A under graph representation. Also, you can use the diagram to build a prime filtration of R/I with A terms such that each subsequent quotient is isomorphic to $R/(X,Y)R$.

Proof. By induction on A. Assume $I \neq R$, then $\mathrm{Ass}_R(R/I) = \{(X,Y)R\}$. Let $J := (X^2, XY)R \subseteq R = k[X,Y]$. Since $(X,Y)R = \mathrm{Ann}_R(X+J)$ and $XR = \mathrm{Ann}_R(Y+J)$, $(X,Y)R, XR \in \mathrm{Ass}_R(R/J)$. The prime filtration $0 \subseteq \langle X+J\rangle \subseteq R/J$. As before, $\langle X+J\rangle \cong R/(X,Y)R$. By 1IT, $\frac{R/J}{\langle X+J\rangle} \cong R/XR$. Prime filtration with $\mathfrak{p}_1 = (X,Y)R$ and $\mathfrak{p}_2 = XR$. So $\mathrm{Ass}_R(R/J) \subseteq \{(X,Y)R, XR\}$. Hence $\mathrm{Ass}_R(R/J) = \{(X,Y)R, XR\}$. Note for $n \geqslant 1$, $\mathrm{Ann}_R(Y^n + J) = XR$. Note $0 \overset{*}{\subseteq} \langle Y^n + J\rangle \subseteq \langle Y^{n-1} + J\rangle \subseteq \cdots \subseteq \langle Y + J\rangle \subseteq \langle X+J, Y+J\rangle \subseteq \langle 1+J\rangle = R/J$ has $n+2$ terms, and $n+1$ of the subsequent quotients are isomorphic to $R/(X,Y)R$ and 1 of the subsequent quotients is isomorphic to R/XR (*). □

Theorem 5.6. *Let $R \neq 0$, M is an R-module and $U \subseteq R$ is multiplicatively closed.*

(a) $\mathrm{Supp}_{U^{-1}R}(U^{-1}M) = \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Supp}_R(M)$ *and* $\mathfrak{p} \cap U = \emptyset\}$.

(b) $\mathrm{Ass}_{U^{-1}R}(U^{-1}M) \supseteq \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_R(M)$ *and* $\mathfrak{p} \cap U = \emptyset\}$.

(c) If R is Noetherian, then $\mathrm{Ass}_{U^{-1}R}(U^{-1}M) = \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Ass}_R(M)$ *and* $\mathfrak{p} \cap U = \emptyset\}$.

Proof. (a) Note $\mathrm{Spec}(U^{-1}R) = \{U^{-1}\mathfrak{p} \mid \mathfrak{p} \in \mathrm{Spec}(R)$ and $U \cap \mathfrak{p} = \emptyset\}$. Since $(U^{-1}M)_{U^{-1}\mathfrak{p}} \cong M_{\mathfrak{p}}$, we have $(U^{-1}M)_{U^{-1}\mathfrak{p}} \neq 0$ if and only if $M_{\mathfrak{p}} \neq 0$ if and only if $\mathfrak{p} \in \mathrm{Supp}_R(M)$.

(b) Let $\mathfrak{p} \in \mathrm{Ass}_R(M)$ and $U \cap \mathfrak{p} \neq \emptyset$. Then $R/\mathfrak{p} \hookrightarrow M$. So $\frac{U^{-1}R}{U^{-1}\mathfrak{p}} \cong U^{-1}(R/\mathfrak{p}) \hookrightarrow U^{-1}M$. Thus, $U^{-1}\mathfrak{p} \in \mathrm{Ass}_R(U^{-1}M)$.

(c) Assume R is Noetherian and let $U^{-1}\mathfrak{p} \in \mathrm{Ass}_{U^{-1}R}(U^{-1}M)$. Since R is Noetherian, $\mathfrak{p}$ is finitely generated. Let $\mathfrak{p} = (x_1, \ldots, x_n)R$ for some $x_1, \ldots, x_n \in \mathfrak{p}$. Let $m/u \in U^{-1}M$ such that $x_i/1 \in U^{-1}\mathfrak{p} = \mathrm{Ann}_{U^{-1}R}(m/u)$ for $i = 1, \ldots, n$. Then $\frac{x_i}{1} \cdot \frac{m}{u} = 0$ for $i = 1, \ldots, n$. So there exists $u_i \in U$ such that $u_i x_i m = 0$ for $i = 1, \ldots, n$. Let $u' = u_1 \cdots u_n$. Then $x_i u' m = 0$ for $i = 1, \ldots, n$. So $R/\mathfrak{p} \overset{\alpha}{\to} M$ given by $r + \mathfrak{p} \mapsto ru'm$ is well-defined. Note we have a commutative diagram:

$$\begin{array}{ccc} R/\mathfrak{p} & \xrightarrow{\ \alpha\ } & M \\ \big\downarrow{\scriptstyle \beta} & & \big\downarrow{\scriptstyle \gamma} \\ U^{-1}(R/\mathfrak{p}) & \xrightarrow{U^{-1}\alpha} & U^{-1}M \end{array}$$

Note $U^{-1}\mathfrak{p} = \mathrm{Ann}_{U^{-1}R}(m/u) = \mathrm{Ann}_{U^{-1}R}(u'm/1)$ since $\frac{u'm}{1} = \frac{uu'}{1}\frac{m}{u}$ and $\frac{uu'}{1} \in (U^{-1}R)^{\times}$. Since β and $U^{-1}\alpha$ is 1-1, we have $\gamma \circ \alpha = (U^{-1}\alpha) \circ \beta$ is also 1-1. So α is 1-1. Thus, $\mathfrak{p} \in \mathrm{Ass}_R(M)$. □

Remark. Ideals generated by one variable or one linear factor is always prime.

Definition 5.7.

$$\mathrm{Min}(\mathrm{Ass}_R(M)) := \text{sets of minimals of } \mathrm{Ass}_R(M).$$

Example 5.8. Let $R = \mathbb{C}[X]$. Then R is UFD. Let $M = \frac{\mathbb{C}[X]}{X(X-1)(X-2)(X-3)}$. By previous example, $\mathrm{Ass}_R(M) = \{XR, (X-1)R, (X-2)R, (X-3)R\}$. Since $(X-i)R \not\subseteq (X-j)R$ for $0 \leqslant i, j \leqslant 3$ with $i \neq j$, we have $\mathrm{Min}(\mathrm{Ass}_R(M)) = \mathrm{Ass}_R(M)$.

Example 5.9. Let k be a field, $R = k[X,Y]$ and $M = R/(X^2, XY)R$. Then $\mathrm{Ass}_R(M) = \{XR, (X,Y)R\}$. So $\mathrm{Min}(\mathrm{Ass}_R(M)) = \{XR\}$.

Corollary 5.10. Let $\mathfrak{q} \in \operatorname{Spec}(R)$. Then

(a) $\operatorname{Supp}_{R_\mathfrak{q}}(M_\mathfrak{q}) = \{\mathfrak{p}_\mathfrak{q} \mid \mathfrak{p} \in \operatorname{Supp}_R(M) \text{ and } \mathfrak{p} \subseteq \mathfrak{q}\}$.

(b) $\operatorname{Ass}_{R_\mathfrak{q}}(M_\mathfrak{q}) \supseteq \{\mathfrak{p}_\mathfrak{q} \mid \mathfrak{p} \in \operatorname{Ass}_R(M) \text{ and } \mathfrak{p} \subseteq \mathfrak{q}\}$.

(c) If R is Noetherian, then $\operatorname{Ass}_{R_\mathfrak{q}}(M_\mathfrak{q}) = \{\mathfrak{p}_\mathfrak{q} \mid \mathfrak{p} \in \operatorname{Ass}_R(M) \text{ and } \mathfrak{p} \subseteq \mathfrak{q}\}$.

Proof. Let $U = R \setminus \mathfrak{q}$. Then $X_\mathfrak{q} = (R \setminus \mathfrak{q})^{-1}X = U^{-1}X$. Then $\mathfrak{p} \cap (R \setminus \mathfrak{q}) = \emptyset$ if and only if $\mathfrak{p} \subseteq \mathfrak{q}$. □

Theorem 5.11. *Let $0 \neq R$ be Noetherian and $0 \neq M$ is a finitely generated R-module with prime filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ and $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $i = 1, \ldots, n$.*

(a) $\operatorname{Min}(\operatorname{Ass}_R(M)) = \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \operatorname{Min}(\operatorname{Supp}_R(M))$. *(Note the equality* $\operatorname{Min}(\operatorname{Ass}_R(M)) = \operatorname{Min}(\operatorname{Supp}_R(M))$ *does not need the prime filtration condition.)*

(b) For $\mathfrak{p} \in \operatorname{Supp}_R(M)$, there exists $\mathfrak{p}' \in \operatorname{Min}(\operatorname{Supp}_R(M))$ such that $\mathfrak{p}' \subseteq \mathfrak{p}$ and $|\operatorname{Min}(\operatorname{Supp}_R(M))| < \infty$.

(c) For $\mathfrak{p} \in \operatorname{Spec}(R)$, there exists $\mathfrak{p}' \in \operatorname{Min}(\operatorname{Spec}(R))$ such that $\mathfrak{p}' \subseteq \mathfrak{p}$ and $|\operatorname{Min}(\operatorname{Spec}(R))| < \infty$.

Proof. (a) Assume $\mathfrak{p} \in \operatorname{Min}(\operatorname{Supp}_R(M))$. Then $\mathfrak{p} \in \operatorname{Supp}_R(M)$ and so $M_\mathfrak{p} \neq 0$. Also, there exists $\mathfrak{q} \in \operatorname{Ass}_R(M)$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. Since R is Noetherian, $R_\mathfrak{p}$ is also Noetherian. So $\operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p}) \neq \emptyset$. Then $\mathfrak{q}_\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}}(M_\mathfrak{p})$. Note $\mathfrak{q} \in \operatorname{Ass}_R(M) \subseteq \operatorname{Supp}_R(M)$. By the minimality of $\mathfrak{p}$ in $\operatorname{Suppp}_R(M)$ and $\mathfrak{q} \subseteq \mathfrak{p}$ and $\mathfrak{q} \in \operatorname{Suppp}_R(M)$, we have $\mathfrak{p} = \mathfrak{q} \in \operatorname{Ass}_R(M)$. Claim. $\mathfrak{p} \in \operatorname{Min}(\operatorname{Ass}_R(M))$.

Since R is Noetherian and M is finitely generated, we have $|\operatorname{Ass}_R(M)| < \infty$. Then there exists $\mathfrak{p}' \in \operatorname{Min}(\operatorname{Ass}_R(M))$ such that $\mathfrak{p}' \subseteq \mathfrak{p}$. Note $\mathfrak{p}' \in \operatorname{Supp}_R(M)$. By the minimality of $\mathfrak{p}$ in $\operatorname{Min}(\operatorname{Supp}_R(M))$ again, we have $\mathfrak{p} = \mathfrak{p}' \in \operatorname{Min}(\operatorname{Ass}_R(M))$. Thus, we have our first conclusion that $\operatorname{Min}(\operatorname{Supp}_R(M)) \subseteq \operatorname{Min}(\operatorname{Ass}_R(M))$. Claim. $\operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Min}(\operatorname{Supp}_R(M))$.

Let $\mathfrak{p}_i \in \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Supp}_R(M)$ since we have shown in previous proof that $M_{\mathfrak{p}_i} \neq 0$ for $i = 1, \ldots, n$. Suppose $\mathfrak{p}' \in \operatorname{Supp}_R(M)$ such that $\mathfrak{p}' \subseteq \mathfrak{p}_i$. By theorem 5.2, we have there exists $\mathfrak{p}_j \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ such that $\mathfrak{p}_j \subseteq \mathfrak{p}' \subseteq \mathfrak{p}_i$. By the minimality of $\mathfrak{p}_i$, we have $\mathfrak{p}_i \subseteq \mathfrak{p}_j \subseteq \mathfrak{p}' \subseteq \mathfrak{p}_i$. So $\mathfrak{p}' = \mathfrak{p}_i = \mathfrak{p}_j$. Thus, $\mathfrak{p}_i \in \operatorname{Min}(\operatorname{Supp}_R(M))$. Claim. $\operatorname{Min}(\operatorname{Ass}_R(M)) \subseteq \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Let $\mathfrak{p}_i \in \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By just previous argument, we have $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Then $\mathfrak{p} = \mathfrak{p}_i$ for some $i \in \{1, \ldots, n\}$. Since $|\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}| < \infty$, we have there exists $\mathfrak{p}_j \in \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ such that $\mathfrak{p}_j \subseteq \mathfrak{p}_i = \mathfrak{p}$. By what we have shown, we have $\mathfrak{p}_i \in \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \operatorname{Min}(\operatorname{Supp}_R(M)) \subseteq \operatorname{Min}(\operatorname{Ass}_R(M)) \ni \mathfrak{p}$, i.e., $\mathfrak{p}_i, \mathfrak{p} \in \operatorname{Min}(\operatorname{Ass}_R(M))$. By the minimality of $\mathfrak{p}$, we have $\mathfrak{p}_j = \mathfrak{p}_i = \mathfrak{p}$.

(b) Let $\mathfrak{p} \in \operatorname{Supp}_R(M)$, by theorem 5.2, we have there exists $\mathfrak{p}_i \subseteq \mathfrak{p}$ for some $i \in \{1, \ldots, n\}$. Since $\operatorname{Min}(\operatorname{Supp}_R(M)) = \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, we have there exists $\mathfrak{p}_j$ for some $j \in \{1, \ldots, n\}$ such that $\mathfrak{p}' := \mathfrak{p}_j \subseteq \mathfrak{p}_i \subseteq \mathfrak{p}$. So $|\operatorname{Min}(\operatorname{Supp}_R(M))| = |\operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}| \leqslant n < \infty$.

(c) Take $M = R$. □

Definition 5.12. Let $0 \neq R$ be Noetherian and $0 \neq M$ is a finitely generated R-module with prime filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ and $M_i/M_{i-1} \cong R/\mathfrak{p}_i$ for $i = 1, \ldots, n$. Let $\operatorname{Min}_R(M) := \operatorname{Min}(\operatorname{Ass}_R(M))$. Then $\mathfrak{p} \in \operatorname{Min}_R(M)$ is a *minimal prime* of M or an *associated prime* of M. If $\mathfrak{q} \in \operatorname{Ass}_R(M) \setminus \operatorname{Min}_R(M)$, then $\mathfrak{q}$ is an *embedded prime* of M. Fact: If $\mathfrak{p} \subseteq \mathfrak{q}$, then $\operatorname{V}(\mathfrak{q}) \subseteq \operatorname{V}(\mathfrak{p})$. So $\operatorname{Supp}_R(M) = \bigcup_{i=1}^n \operatorname{V}(\mathfrak{p}_i) = \bigcup_{\mathfrak{p}_i \in \operatorname{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}} \operatorname{V}(\mathfrak{p}_i) = \bigcup_{\mathfrak{p}_i \in \operatorname{Min}(\operatorname{Supp}_R(M))} \operatorname{V}(\mathfrak{p}_i)$.

Chapter 6

Prime Avoidance and Nakayama's Lemma

Let R be a nonzero commutative ring with identity.

Lemma 6.1 (Prime avoidance)**.** Let $I_1, \dots, I_n, J \leqslant R$. Assume one of the followings:

(a) R contains an infinite field as a subring;

(b) The ideals $I_1, \dots, I_{n-2} \in \mathrm{Spec}(R)$.

Then if $J \subseteq \bigcup_{i=1}^n I_i$, then $J \subseteq I_i$ for some $i \in \{1, \dots, n\}$, i.e., if $J \nsubseteq I_i$ for $i = 1, \dots, n$, then $J \nsubseteq \bigcup_{i=1}^n I_i$.

Corollary 6.2. Let R be Noetherian and $0 \neq M$ a finitely generated R-module. If $J \leqslant R$ such that $J \subseteq \mathrm{ZD}(M)$, then there exists $\mathfrak{p} \in \mathrm{Ass}_R(M)$ such that $J \subseteq \mathfrak{p}$.

Proof. Since R is Noetherian and M is finitely generated, $\emptyset \neq \mathrm{Ass}_R(M) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$ for some $\mathfrak{p}_1, \dots, \mathfrak{p}_n \in \mathrm{Spec}(R)$. Then $J \subseteq \mathrm{ZD}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \mathfrak{p} = \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n$. So by Prime avoidance, $J \subseteq \mathfrak{p}_i$ for some $i \in \{1, \dots, n\}$. $\square$

Corollary 6.3. Let R be Noetherian and $0 \neq M$ be finite R-module. Then $\mathfrak{m} \in \text{m-Spec}(R)$ contains a non-zero divisor on M if and only if $\mathfrak{m} \notin \mathrm{Ass}_R(M)$, i.e., $\mathfrak{m}$ consists entirely of zero-divisors on M, i.e., $\mathfrak{m} \subseteq \mathrm{ZD}(M)$) if and only if $\mathfrak{m} \in \mathrm{Ass}_R(M)$.

Proof. "$\Longrightarrow$". Assume $\mathfrak{m} \subseteq \mathrm{ZD}(M)$. Then by previous corollary, there exists $\mathfrak{p} \in \mathrm{Ass}_R(M)$ such that $\mathfrak{m} \subseteq \mathfrak{p}$. Since $\mathfrak{m} \in \text{m-Spec}(R)$, $\mathfrak{m} = \mathfrak{p}$.

"$\Longleftarrow$". Assume $\mathfrak{m} \in \mathrm{Ass}_R(M)$, then $\mathfrak{m} = \mathrm{Ann}_R(m)$ for some $0 \neq m \in M$, so $\mathfrak{m} \subseteq \mathrm{ZD}(M)$. $\square$

Example 6.4. For $I \leqslant R$, there exists $M \neq 0$ such that $I \subseteq \mathrm{ZD}(M)$. For example, $M = R/I$.

Definition 6.5. Let $I \leqslant R$ and M is an R-module. Then the submodule of M

$$IM = \{im \in M \mid i \in I \text{ and } m \in M\} = \left\{ \sum_j^{\text{finite}} i_j m_j \;\middle|\; i_j \in I, m_j \in M \right\}.$$

Fact 6.6. M/IM is an R/I-module. $(r+I)(m+IM) = (rm)+IM$ or $\bar{r}\cdot\overline{m} = \overline{rm}$.

Definition 6.7. R is *local* if it has a unique maximal ideal $\mathfrak{m}$, "$(R,\mathfrak{m})$ is a local ring".

Fact 6.8. R is local if and only if $R\smallsetminus R^\times \leqslant R$. If this is true, then $\mathfrak{m} = R\smallsetminus R^\times$. So if R is local, then for $x\in\mathfrak{m}$, $1-x, 1+x\in R^\times$ since if $x\in\mathfrak{m}$ and $1\notin\mathfrak{m}$, then $1\pm x\notin\mathfrak{m}$.

Lemma 6.9 (Nakayama's lemma, N.K.A.)**.** Assume $(R,\mathfrak{m})$ is local and M is a finitely generated R-module. Then TFAE.

(i) $M=0$.

(ii) $M=\mathfrak{m}M$.

(iii) $M/\mathfrak{m}M=0$.

Proof. "(i)$\Longrightarrow$(iii)$\Longrightarrow$(ii)" is straightforward.

"(ii)$\Longrightarrow$(i)". Assume $M=\mathfrak{m}M$. Since M is finitely generated, $\mathfrak{m}M = M = \mathfrak{m}(m_1,\dots,m_n)$ for some $m_1,\dots,m_n\in M$. Suppose no proper subsequence of $m_1,\dots,m_n$ generates M. Since $m_1\in M$, there exist $r_1,\dots,r_n\in\mathfrak{m}$ such that $m_1=\sum_{i=1}^n r_im_i$, i.e., $(1-r_1)m_1=\sum_{i=2}^n r_im_i\in\langle m_2,\dots,m_n\rangle$. Since $1-r_1\in R^\times$, we have $m_1\in\langle m_2,\cdots,m_n\rangle$. So $M=\langle m_1,\dots,m_n\rangle\subseteq\langle m_2,\dots,m_n\rangle\subseteq M$. Thus, $M=\langle m_2,\cdots m_n\rangle$, which is contradicted by the minimality of generating sequence $m_1,\dots,m_n$. □

Example 6.10. Let K be a field and set $R=K\times K$. Define $R=K\times K\xrightarrow{\varphi_2}K$ by $(a,b)\mapsto b$. Then φ_2 is an epimorphism. Note $\mathfrak{m}=\operatorname{Ker}(\varphi_2)=K\times 0$ is a maximal ideal of R. Let $M=0\times K$ be a cyclic R-module generated by $(0,1)$. Note $\mathfrak{m}M=(K\times 0)\cdot(0\times K)=\{(0,0)\}=0$. Let $\mathfrak{n}=M$. Then $\mathfrak{n}M=(0\times K)\cdot(0\times K)=0\times K=M$, but $M\neq 0$, so in order to use a maximal ideal in N.A.K., R must be local.

Fact 6.11. If A is a ring and $\mathfrak{p}\in\operatorname{Spec}(A)$, then $A_\mathfrak{p}$ is local with unique maximal ideal $\mathfrak{p}_\mathfrak{p}$. Also, if A is an integral domain and $U\subseteq A$ is multiplicatively closed such that $0\notin U$, then $U^{-1}A$ is an integral domain; moreover, $U^{-1}A\subseteq Q(A)$ a field of fraction.

Example 6.12. Let R be an integral domain, local but not a field. For example, $\mathbb{Z}_{\langle p\rangle}$ or $K[X]_{\langle X\rangle}$.

Let $M=Q(R)$. Since R is not a field, $\mathfrak{m}\neq 0$. So $\mathfrak{m}\cdot Q(R)=Q(R)$, but $Q(R)\neq 0$. So in order to use a maximal ideal in N.A.K., M must be finitely generated.

Corollary 6.13. If $(R,\mathfrak{m})$ is local, Noetherian and not a field, then $\mathfrak{m}^2\subsetneq\mathfrak{m}$.

Proof. Since R is Noetherian, $\mathfrak{m}$ is finitely generated. If $\mathfrak{m}^2=\mathfrak{m}$, then $\mathfrak{m}=0$ by N.K.A., a contradiction since R is not a field. □

Corollary 6.14. Assume R is Noetherian and $0\neq M$ is a finitely generated R-module.

(a) If R is local and not a field with maximal ideal $\mathfrak{m}$ and $\mathfrak{m}\notin\operatorname{Ass}_R(M)$, then $\mathfrak{m}\smallsetminus\mathfrak{m}^2$ containsa a non-zero divisor on M.

(b) $\mathfrak{m}\in\text{m-Spec}(R)$ such that $\mathfrak{m}^2\neq\mathfrak{m}$ and $\mathfrak{m}\notin\operatorname{Ass}_R(M)$, then $\mathfrak{m}\smallsetminus\mathfrak{m}^2$ contains a non-zero divisor on M.

Proof. (b) Since R is Noetherian and $0 \neq M$ is a finitely generated R-module, $\emptyset \neq \mathrm{Ass}_R(M) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ for some $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \mathrm{Spec}(R)$. Prime avoidance: $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{m}^2$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are primes and $\mathfrak{m}^2$ is not prime. Since $\mathfrak{m} \notin \mathrm{Ass}_R(M)$, $\mathfrak{m} \not\subseteq \mathfrak{p}_i$ for $i = 1, \ldots, n$. Also, since $\mathfrak{m} \neq \mathfrak{m}^2$, $\mathfrak{m} \not\subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n \cup \mathfrak{m}^2$ by N.K.A.. So there exists $x \in \mathfrak{m} \smallsetminus \mathfrak{m}$ such that $x \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n = \mathrm{ZD}(M)$ since R is Noetherian and $M \neq 0$.

(a) It follows from part (b). □

Corollary 6.15. Let $(R, \mathfrak{m})$ be local and M be an R-module. Let $N \subseteq M$ be a submodule such that M/N is finitely generated over R. If $M = N + \mathfrak{m}M$, then $M = N$.

Proof. Note $\mathfrak{m} \cdot \frac{M}{N} = \frac{\mathfrak{m}M+N}{N} = \frac{M}{N}$. By N.A.K., $M/N = 0$. So $M = N$. □

Definition 6.16. Let M be a finitely R-module. A *minimal generating sequence* for M is a generating sequence $m_1, \ldots, m_n$ such that no proper subsequence generates M.

Example 6.17. Let $R = K[X, Y]$, then $\{X, Y\}$ is mininal generating sequence for $\langle X, Y \rangle$.

Corollary 6.18. Let $(R, \mathfrak{m})$ be local and $K = R/\mathfrak{m}$. Let M be a finitely generated R-module and $m_1, \ldots, m_n \in M$.

(a) $M/\mathfrak{m}M$ is a finitely generated vector space over K via scalar multiplication $(r+\mathfrak{m})(m+\mathfrak{m}M) = (rm) + \mathfrak{m}M$, i.e., $\bar{r} \cdot \overline{m} = \overline{rm}$.

(b) $M = R(m_1, \ldots, m_n)$ if and only if $\overline{m}_1, \ldots, \overline{m}_n \in M/\mathfrak{m}M$ spans $M/\mathfrak{m}M$ as a K-vector space.

(c) $m_1, \ldots, m_n \in M$ is a minimal generating sequence for M if and only if $\overline{m}_1, \ldots, \overline{m}_n \in M/\mathfrak{m}M$ is a basis for $M/\mathfrak{m}M$ over K. In particular, every minimal generating sequence for M has the same number of elements, namely, $\dim_K(M/\mathfrak{m}M)$.

Proof. (a) Check scalar multiplication is well-defined. Then K-vector space axioms follow directly from R-module. For example, $\bar{r}(\bar{s} \cdot \overline{m}) = \bar{r} \cdot \overline{sm} = \overline{r(sm)} = \overline{(rs)m} = \overline{rs} \cdot \overline{m} = (\bar{r} \cdot \bar{s})\overline{m}$. Let $M = R(m_1', \ldots, m_n')$ for some $m_1', \ldots, m_n' \in M$. Then $\overline{m}_1', \ldots, \overline{m}_n'$ spans $M/\mathfrak{m}M$ over K clearly.

(b) "$\Longrightarrow$". Done by (a).

"$\Longleftarrow$". Assume $\overline{m}_1, \ldots, \overline{m}_n$ spans $M/\mathfrak{m}M$. Claim $M = R(m_1, \ldots, m_n) + \mathfrak{m}M$. "$\supseteq$". It is clear. "$\subseteq$". Let $m \in M$. Then there exists $\bar{r}_1, \cdots \bar{r}_n \in K$ such that $\overline{m} = \sum_{i=1}^n \bar{r}_i \cdot \overline{m}_i = \overline{\sum_{i=1}^n r_i m_i}$ in $M/\mathfrak{m}M$. So $m - \sum_{i=1}^n r_i m_i \in \mathfrak{m}M$. Then $m \in R(m_1, \ldots, m_n) + \mathfrak{m}M$. So $M \subseteq R(m_1, \ldots, m_n) + \mathfrak{m}M$. Thus, $M = R(m_1, \ldots, m_n) + \mathfrak{m}M = R(m_1, \ldots, m_n)$.

(c) "$\Longrightarrow$". Assume $m_1, \ldots, m_n$ is a minimal generating sequence for M. By (b), $\overline{m}_1, \ldots, \overline{m}_n$ is a spanning set for $M/\mathfrak{m}M$ over K. Suppose $\overline{m}_1, \ldots, \overline{m}_n$ is not a basis. We can rearrange m_i's if necessary to assume $\overline{m}_1, \ldots, \overline{m}_{n-1}$ also spans $M/\mathfrak{m}M$. By (b) again, we have $m_1, \ldots, m_{n-1}$ generate M over R, which is contradicted by the minimality of the original generating sequence.

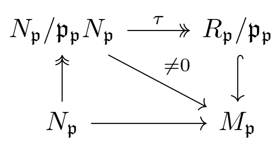
"$\Longleftarrow$". Similarly, apply (b) twice. □

Corollary 6.19. Let $(R, \mathfrak{m})$ be local and P is a finitely generated projective R-module. Then P is free and $P \cong R^n$, where $n := \dim_K(P/\mathfrak{m}P)$.

Proof. Let $K = R/\mathfrak{m}$. Then $P/\mathfrak{m}P$ is a n-dimensional vector space over K. So by previous corollary, there exist $p_1, \ldots, p_n \in P$ such that it is a minimal generating sequence for P. Note $P/\mathfrak{m}P \cong K^n$. Define $\tau : R^n \to P$ by $e_i \mapsto p_i$ for $i = 1, \ldots, n$ and $\sum_{i=1}^n r_i e_i \mapsto \sum_{i=1}^n r_i p_i$. Then τ is a well-defined R-module epimorphism with $\operatorname{Ker}(\tau) =: H$. So the sequence $0 \to H \xrightarrow{\subseteq} R^n \xrightarrow{\tau} P \to 0$ is exact. It suffices to show $H = 0$. Since P is projective, the sequence splits. So $R^n \cong H \oplus P \xrightarrow{\pi} H$, where π is the natural surjection. Since R^n is a free R-module, H is finitely generated over R. Then $(R/\mathfrak{m})^n \cong R^n/\mathfrak{m}R^n \cong (H \oplus P)/\mathfrak{m}(H \oplus P) \cong H/\mathfrak{m}H \oplus P/\mathfrak{m}P \cong H/\mathfrak{m}H \oplus K^n$. Since isomorphic vector spaces have the same vector space dimension, we have $n = \dim_K(H/\mathfrak{m}H) + n$. So $\dim_K(H/\mathfrak{m}H) = 0$. Hence $H/\mathfrak{m}H = 0$. Thus, $H = \mathfrak{m}H$. Since $(R, \mathfrak{m})$ is local and H is finitely generated R-module, by N.A.K., we have $H = 0$. □

Lemma 6.20. Let R be Noetherian, $0 \neq M, N$ be finitely generated R-modules and $I \leqslant R$ such that $\operatorname{Supp}_R(N) = \operatorname{V}(I)$. If $I \subseteq \operatorname{ZD}(M)$, then $\operatorname{Hom}_R(N, M) \neq 0$.

Proof. Since $I \subseteq \operatorname{ZD}(M)$, there exists $\mathfrak{p} \in \operatorname{Ass}_R(M)$ such that $I \subseteq \mathfrak{p}$ by previous Corollary. Claim $\operatorname{Hom}_{R_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p}) \neq 0$. Since $\mathfrak{p} \in \operatorname{Ass}_R(M)$, there exists $R/\mathfrak{p} \hookrightarrow M$. So $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} \cong (R/\mathfrak{p})_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$. Since $I \subseteq \mathfrak{p}$, $\mathfrak{p} \in \operatorname{V}(I) = \operatorname{Supp}_R(N)$. So $N_\mathfrak{p} \neq 0$. Since N is finitely generated over R, we have $0 \neq N_\mathfrak{p}$ is a finitely generated $R_\mathfrak{p}$-module. Since $(R_\mathfrak{p}, \mathfrak{p}_\mathfrak{p})$ is local, $0 \neq N_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}N_\mathfrak{p}$ is a vector space over $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p}$. So there exists surjection τ such that



commutes. So $0 \neq \operatorname{Hom}_{R_\mathfrak{p}}(N_\mathfrak{p}, M_\mathfrak{p}) \cong \operatorname{Hom}_R(N, M)$. Thus, $\operatorname{Hom}_R(N, M) \neq 0$. □

Corollary 6.21. Let R be Noetherian and $0 \neq M$ be a finitely generated R-module and $I \leqslant R$. If $\operatorname{depth}(I; M) = 0$, then $\operatorname{Hom}_R(R/I, M) \neq 0$.

Proof. Since $\operatorname{depth}(I; M) = 0$, $I \subseteq \operatorname{ZD}(M)$. Since $M = 0$, $I \neq R$. $N = R/I \neq 0$ is finitely generated. Also, $\operatorname{Supp}_R(N) = \operatorname{Supp}_R(R/I) = \operatorname{V}(I)$. So $\operatorname{Hom}_R(N, M) \neq 0$. □

Lemma 6.22. Let M, N be finitely generated R-modules, then $\operatorname{Ass}_R(\operatorname{Hom}_R(M, N)) = \operatorname{Supp}_R(M) \cap \operatorname{Ass}_R(N)$.

Proof. If $M = 0$, then $\operatorname{Hom}_R(M, N) = 0$. So $\operatorname{Ass}_R(\operatorname{Hom}_R(M, N)) = \emptyset = \emptyset \cap \operatorname{Ass}_R(N) = \operatorname{Supp}_R(M) \cap \operatorname{Ass}_R(M)$. Similarly, if $N = 0$, then done. Assume now $M, N \neq 0$.

"$\subseteq$". Let $\mathfrak{p} \in \operatorname{Spec}(R)$. If $\mathfrak{p} \notin \operatorname{Supp}_R(M)$, then $M_\mathfrak{p} = 0$. So $(\operatorname{Hom}_R(M, N))_\mathfrak{p} \overset{\Theta}{\cong} \operatorname{Hom}_{R_\mathfrak{p}}(M_\mathfrak{p}, N_\mathfrak{p}) = 0$. Then $\mathfrak{p} \notin \operatorname{Supp}_R(\operatorname{Hom}_R(M, N))$. So $\mathfrak{p} \notin \operatorname{Ass}_R(\operatorname{Hom}_R(M, N))$. Thus, if $\mathfrak{p} \in \operatorname{Ass}_R(\operatorname{Hom}_R(M, N))$, then $\mathfrak{p} \in \operatorname{Supp}_R(M)$. Since M is finitely generated, there exists $t \geqslant 1$ such that $R^t \twoheadrightarrow M$. Then $\operatorname{Hom}_R(M, N) \hookrightarrow \operatorname{Hom}_R(R^t, N) \cong N^t$ Thus, $\operatorname{Ass}_R(\operatorname{Hom}_R(M, N)) \subseteq \operatorname{Ass}_R(N^t) = \operatorname{Ass}_R(N)$.

"$\supseteq$". Let $\mathfrak{p} \in \operatorname{Supp}_R(M) \cap \operatorname{Ass}_R(N)$. Claim 1: $\operatorname{Hom}_R(M, R/\mathfrak{p}) \neq 0$. Since M is finitely generated, $\mathfrak{p} \in \operatorname{Supp}_R(M) = \operatorname{V}(\operatorname{Ann}_R(M))$. So $\operatorname{Ann}_R(M) \subseteq \mathfrak{p}$. Then $\operatorname{Ann}_R(M) \cdot R/\mathfrak{p} = 0$. So $\operatorname{Ann}_R(M) \subseteq \operatorname{ZD}(R/\mathfrak{p})$. Thus, $\operatorname{Hom}_R(M, R/\mathfrak{p}) \neq 0$. Claim 2. Let $0 \neq \alpha \in \operatorname{Hom}_R(M, R/\mathfrak{p})$, then $\operatorname{Ann}_R(\alpha) = \mathfrak{p}$. "$\supseteq$". $x \in \mathfrak{p}$ if and only if $x \cdot R/\mathfrak{p} = 0$ if and only if $x \cdot \alpha(m) = 0$ for $m \in M$ if and only if $(x\alpha)(m) = 0$ for $m \in M$ if and only if $x\alpha = 0$, i.e., $x \in \operatorname{Ann}_R(\alpha)$. "$\subseteq$". Let $y \in \operatorname{Ann}_R(\alpha$. Since $\alpha \neq 0$, $\exists m \in M$ such that $0_{R/\mathfrak{p}} \neq \alpha(m) \in R/\mathfrak{p}$. Then $x \cdot \alpha(m) = 0, \forall x \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, (no other $r \in R \smallsetminus \mathfrak{p}$ such that $r \cdot \alpha(m) = 0$) $\mathrm{Ann}_R(\alpha(m)) = \mathfrak{p}$. Since $y \cdot \alpha = 0$, we have $(y \cdot \alpha)(m) = 0$, i.e., $y \cdot \alpha(m) = 0$. So $y \in \mathrm{Ann}_R(\alpha(m)) = \mathfrak{p}$. Next, let $0 \neq \alpha \in \mathrm{Hom}_R(M, R/\mathfrak{p})$. Define $R \xrightarrow{\phi} \mathrm{Hom}_R(M, R/\mathfrak{p})$ by $r \mapsto r\alpha$. Then $\mathrm{Ker}(\phi) = \mathrm{Ann}_R(\alpha) = \mathfrak{p}$. By the 1IT, $R/\mathfrak{p} \hookrightarrow \mathrm{Hom}_R(M, R/\mathfrak{p})$ by $\bar{r} \mapsto r\alpha$. Since $\mathfrak{p} \in \mathrm{Ass}_R(N)$, there exists $R/\mathfrak{p} \hookrightarrow N$. So

$$\begin{array}{ccc} \mathrm{Hom}_R(M, R/\mathfrak{p}) & \hookrightarrow & \mathrm{Hom}_R(M, N) \\ \uparrow & \nearrow_{\exists} & \\ R/\mathfrak{p} & & \end{array}$$

Thus, $\mathfrak{p} \in \mathrm{Ass}_R(\mathrm{Hom}_R(M, N))$. □

Example 6.23. Let K be a field, then

	Supp_R	Ass_R
$R = K[X, Y]$	$\mathrm{Spec}(R)$	$\{0\}$
$A = R/(X, Y)^n$	$\{(X, Y)\}$	$\{(X, Y)\}$
$B = R/(X^n, Y^l)$	$\{(X, Y)\}$	$\{(X, Y)\}$
$C = R/(X^2, XY)$	$\mathrm{V}(XR)$	$\{XR, (X, Y)\}$

Regard sets as elements in big sets, we have $\{(X, Y)\} \cap \{0\} = \emptyset$. Then $\mathrm{Ass}_R(\mathrm{Hom}_R(A, R)) = \mathrm{Supp}_R(A) \cap \mathrm{Ass}_R(R) = \{(X, Y)\} \cap \{0\} = \emptyset$. Claim $\mathrm{Hom}_R(A, R) = 0$. Let $\beta \in \mathrm{Hom}_R(A, R)$. Note $(X, Y)^n \cdot A = 0$ and $(X, Y)^n \cdot R \neq 0$. Assume $\beta \neq 0$. Then there exists $a \in A$ such that $\beta(a) = r \in \mathbb{R} \smallsetminus 0$. So $0 \neq (X, Y)^n \cdot r = (X, Y)^n \cdot \beta(a) = \beta((X, Y)^n \cdot a) = \beta(0) = 0$, a contradiction. Thus, $\beta = 0$. Next, $\mathrm{Ass}_R(\mathrm{Hom}_R(B, C)) = \mathrm{Supp}_R(B) \cap \mathrm{Ass}_R(C) = \{(X, Y)R\} \cap \{XR, (X, Y)R\} = \{(X, Y)R\} \neq \emptyset$.

Chapter 7

Regular Sequences and Ext

Let R be a nonzero commutative ring with identity.

Definition 7.1. Let M be an R-module. Then $x \in R$ is *M-regular* if

(a) $x \in \mathrm{NZD}(M)$,

(b) $xM \neq M$.

Remark. (a) is understood in terms of $\mathrm{Ass}_R(M)$.

Remark. Observe if $(R, \mathfrak{m})$ is local, $x \in \mathfrak{m}$ and $M \neq 0$ is finitely generated, then by N.A.K, we have $xM \neq M$.

Definition 7.2. Let $I \leqslant R$. Then a sequence $a_1, \ldots, a_n \in I$ is *M-regular* if

(a) $a_1 \in \mathrm{NZD}(M)$,

(b) $a_i \in \mathrm{NZD}(M/(a_1, \ldots, a_{i-1})M)$ for $i = 2, \ldots, n$,

(c) $(a_1, \ldots, a_n)M \neq M$.

An R-regular sequence is called simply a *regular sequence.*

Remark. If $IM \neq M$, then $(a_1, \ldots, a_n)M \subseteq IM \subsetneq M$, and then (c) is automatic. For example, if $(R, \mathfrak{m})$ is local and M finitely generated and $M \neq 0$ and $I \subseteq \mathfrak{m} \lneq R$, then by N.A.K., $IM \subseteq \mathfrak{m}M \subsetneq M$, and then (c) is automatic.

Remark (Reasoning)**.** Note for $i = 2, \ldots, n$, we have $\frac{M/(a_1,\ldots,a_{i-1})}{a_i \cdot M/(a_1,\ldots,a_{i-1})M} = \frac{M/(a_1,\ldots,a_{i-1})M}{(a_1,\ldots,a_i)M/(a_1,\cdots a_{i-1})M} \cong \frac{M}{(a_1,\ldots,a_i)M}$.

Example 7.3. $X, Y(1-X), Z(1-X)$ is a regular sequence in $\mathbb{C}[X, Y, Z]$ while $Y(1-X), Z(1-X), X$ is not a regular sequence.

Definition 7.4. Let $I \leqslant R$. Then $a_1, \ldots, a_n \in I$ is a *maximal M-regular sequence* in I if $a_1, \ldots, a_n$ is a M-regular sequence such that for $b \in I$, $a_1, \ldots, a_n, b$ is not a M-regular sequence.

Example 7.5. Let k be a field. Then $X_1, \ldots, X_n$ is $k[X_1, \ldots, X_n]$-regular (actually only need k be a nonzero commutative ring with identity).

Proof. Note $X_1 \in k[X_1, \ldots, X_n]$ is a NZD and $\frac{k[X_1,\ldots,X_n]}{(X_1)} \cong k[X_2, \ldots, X_n] \neq 0$. Induct on n and note $(X_1, \ldots, X_n)k[X_1, \ldots, X_n] \neq k[X_1, \ldots, X_n]$. □

Example 7.6. Let $R = \mathbb{Z}$ and $n \geqslant 2$, then n is $\mathbb{Z}$-regular. Note n is non-zero, non-unit in the integral domain $\mathbb{Z}$. Note $\mathbb{Z}$ does not have any regular sequences of length 2.

Proof. Suppose m, n is $\mathbb{Z}$-regular with $m \in \mathbb{Z}$. Then m is non-zero and non-unit. If $\gcd(m, n) = 1$, then since $n\mathbb{Z} + m\mathbb{Z} = \gcd(m, n)\mathbb{Z} = \mathbb{Z}$, we have $n \cdot \mathbb{Z}/m\mathbb{Z} = (m, n)\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m\mathbb{Z}$. So n is not $\mathbb{Z}/m\mathbb{Z}$-regular. If $\gcd(m, n) = d \geqslant 2$, then $\frac{m}{d}, \frac{n}{d} \in \mathbb{Z}$. Since $n \cdot (\frac{m}{d} + m\mathbb{Z}) = m \cdot \frac{n}{d} + m\mathbb{Z} = 0_{\mathbb{Z}/m\mathbb{Z}}$, we have $n \in \mathrm{ZD}(\mathbb{Z}/m\mathbb{Z})$. So n is not $\mathbb{Z}/m\mathbb{Z}$-regular. □

Example 7.7. A field k has no regular sequence since $a \in k$ is either 0 or a unit.

Example 7.8. Let $R = k[X]/(X^2)$. If $a, b \in k$ with $b \neq 0$, then $(a\overline{X} + \bar{b})(\overline{X} + \overline{\frac{1}{b}}) = \bar{1}$. So non-units of $k[X]/(X^2)$ are $a\overline{X}, a \in k$. Note $a\overline{X} \cdot \overline{X} = 0$. So $a\overline{X} \in \mathrm{ZD}(k[X]/(X^2))$. Thus R has no regular sequences.

Theorem 7.9. *If R is noethrian and M is any R-module, then M has a maximal regular sequence. Moreover, every M-regular sequence in I extends to maximal M-regular sequence in I.*

Proof. Suppose $(a_1)M \subsetneq (a_1, a_2)M \subsetneq (a_1, a_2, a_3)M \subsetneq \cdots$. Then we have $(a_1)R \subsetneq (a_1, a_2)R \subsetneq (a_1, a_2, a_3)R \subsetneq \cdots$, contradicting that R is noetherian. □

Remark (Algorithm)**.** Let R be noetherian and local with maximal ideal $\mathfrak{m}$ and $0 \neq M$ is a finitely generated R-module. Find a maximal M-regular sequence in $\mathfrak{m}$. Note (c) is automatic.

(a) If $\mathfrak{m} \in \mathrm{Ass}_R(M)$, then $\mathfrak{m} \subseteq \mathrm{ZD}(M)$, so $\emptyset$ is maximal M-regular sequence and we stop.

(b) Assume $\mathfrak{m} \notin \mathrm{Ass}_R(M)$. Since $\mathfrak{m}$ is the unique maximal ideal, $\mathrm{ZD}(M) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}_R(M)} \subsetneq \mathfrak{m}$. So there exists $x_1 \in \mathfrak{m} \smallsetminus \mathrm{ZD}(M)$. Then $x_1 \in \mathfrak{m} \smallsetminus \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Ass}_R(M)$.

(c) Repeat with the module M/x_1M. If $\mathfrak{m} \in \mathrm{Ass}_R(M/x_1M)$, then $\mathfrak{m} \subseteq \mathrm{ZD}(M/x_1M)$. So x_1 is maximal M-regular sequence and we stop. If $\mathfrak{m} \in \mathrm{Ass}_R(M/x_1M)$, find $x_2 \in \mathfrak{m} \smallsetminus \mathfrak{p}$ for $\mathfrak{p} \in \mathrm{Ass}_R(M)$.

(d) Repeat with $M/(x_1, x_2)M$.

Since R is noetherian, I contains a maximal M-regular sequence. So process terminates in finite number of steps.

Lemma 7.10. Let R be noetherian and $I \leqslant R$. Then

(a) $\mathrm{rad}(I) = \bigcap_{\mathfrak{p} \in \mathrm{V}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Ass}_R(R/I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Min}_R(R/I)} \mathfrak{p}$.

(b) If $I = \bigcap_{i=1}^n \mathfrak{p}_i$ for some $n \in \mathbb{N}$ and $\mathfrak{p}_i \in \mathrm{Spec}(R)$ for $i = 1, \ldots, n$, then $\mathrm{Ass}_R(R/I) = \mathrm{Min}_R(R/I) = \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

(c) If I is an intersection of prime ideals, then it is an intersection of a finite number of prime ideals.

Proof. (a) By definition, $\mathrm{Min}_R(R/I) = \mathrm{Min}(\mathrm{Ass}_R(R/I))$. Claim. $\mathfrak{p} \in \mathrm{Supp}_R(R/I)$ if and only if there exists $\mathfrak{q} \in \mathrm{Min}_R(R/I)$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. Since R is noetherian, R is a R-module and then R is finitely generated. So $M := R/I$ is finitely generated. Hence there exists prime filtration $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ such that for $i = 1, \ldots, n$, there exists $\mathfrak{p}_i \in \mathrm{Spec}(R)$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$. Then by theorem 5.11, $\mathrm{Min}_R(R/I) = \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \mathrm{Min}_R(\mathrm{Supp}_R(R/I))$, $\mathfrak{p} \in \mathrm{Supp}_R(R/I)$ if and only if there exists $\mathfrak{q} \in \mathrm{Min}_R(R/I)$ such that $\mathfrak{q} \subseteq \mathfrak{p}$. Thus, $\mathrm{rad}(I) = \bigcap_{\mathfrak{p} \in \mathrm{V}(I)} \mathfrak{p} = \bigcap_{\mathfrak{p} \in \mathrm{Supp}_R(R/I)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Ass}_R(R/I)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Min}_R(R/I)} \mathfrak{p} \subseteq \bigcap_{\mathfrak{p} \in \mathrm{Supp}_R(R/I)} \mathfrak{p}$.

(b) Reorder the $\mathfrak{p}_i$'s if necessary to assume that $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_j\} = \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. So $I = \bigcap_{i=1}^{j} \mathfrak{p}_i$. By theorem 5.11(a), $\mathfrak{p}_1, \ldots, \mathfrak{p}_j \in \mathrm{Min}_R(R/I) = \mathrm{Min}(\mathrm{Supp}_R(R/I)) = \mathrm{Min}(\mathrm{V}(I))$. It suffices to show $\mathfrak{p}_i \in \mathrm{Min}(\mathrm{V}(I))$ for $i = 1, \ldots, j$. Since $I = \bigcap_{k=1}^{n} \mathfrak{p}_k \subseteq \mathfrak{p}_i$, we have $\mathfrak{p}_i \in \mathrm{V}(I)$. Suppose $\mathfrak{p} \in \mathrm{V}(I)$ and $\mathfrak{p} \subseteq \mathfrak{p}_i$. By the definition of prime ideal, $\mathfrak{p}_1 \cdots \mathfrak{p}_j \subseteq \bigcap_{k=1}^{j} \mathfrak{p}_k = I \subseteq \mathfrak{p}$. So there exists $k \in \{1, \ldots, j\}$ such that $\mathfrak{p}_k \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$. Since $\mathfrak{p}_i \in \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, we have $\mathfrak{p}_i \subseteq \mathfrak{p}_k \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$. So $\mathfrak{p}_k = \mathfrak{p}_i$. Hence $\mathfrak{p} = \mathfrak{p}_i$. Thus, $\mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_j\} \subseteq \mathrm{Min}_R(R/I)$. Claim. $\mathrm{Ass}_R(R/I) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_j\}$, then done with (b) since we will have $\mathrm{Min}_R(R/I) \subseteq \mathrm{Ass}_R(R/I) \subseteq \mathrm{Min}\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subseteq \mathrm{Min}_R(R/I)$. Let $\mathfrak{p} \in \mathrm{Ass}_R(R/I)$. Then there exists $0 \neq \overline{x} \in R/I$ such that $\mathfrak{p} = \mathrm{Ann}_R(\overline{x})$. Then $x \in R \smallsetminus I$, $\mathfrak{p} \cdot x \subseteq I = \bigcap_{i=1}^{j} \mathfrak{p}_i$. Since $x \notin \bigcap_{i=1}^{j} \mathfrak{p}_i$, we have there exists $k \in \{1, \ldots, j\}$ such that $x \notin \mathfrak{p}_k$. Then $\mathfrak{p} \cdot x \subseteq \bigcap_{j=1}^{j} \mathfrak{p}_i \subseteq \mathfrak{p}_k$. Since $x \notin \mathfrak{p}_k$, $\mathfrak{p} \subseteq \mathfrak{p}_k$. Subclaim. $\mathfrak{p}_k \in \mathrm{Ass}_R(R/\bigcap_{i=1}^{n} \mathfrak{p}_i)$ for $k = 1, \ldots, n$. Let (existence?) $x \in \bigcap_{i \neq k} \mathfrak{p}_i$ but $x \notin \mathfrak{p}_k$. Then $x \notin \bigcap_{i=1}^{n} \mathfrak{p}_i$. So $\mathfrak{p}_k \cdot x \subseteq \mathfrak{p}_k \cap (\bigcap_{i \neq k} \mathfrak{p}_i) = \bigcap_{i=1}^{n} \mathfrak{p}_i$. Note $\mathfrak{p}_k \bigcap_{i=1}^{n} \mathfrak{p}_i \subseteq \bigcap_{i=1}^{n} \mathfrak{p}_i$. Hence $\mathfrak{p}_k(x + \bigcap_{i=1}^{n} \mathfrak{p}_i) = \mathfrak{p}_k \cdot x + \mathfrak{p}_k \bigcap_{i=1}^{n} \mathfrak{p}_i = 0$. Thus, $\mathfrak{p}_k \in \mathrm{Ass}_R(R/\bigcap_{i=1}^{n} \mathfrak{p}_i)$ for $k = 1, \ldots, n$. Since $\mathfrak{p}, \mathfrak{p}_k \in \mathrm{Ass}_R(R/I)$ and $\mathfrak{p}_k \in \mathrm{Min}((\mathrm{V}(I))$, we have $\mathfrak{p} = \mathfrak{p}_k$.

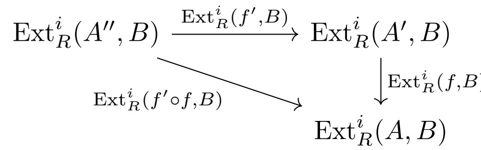
(c) Since I is an intersection of prime ideals, then by (a), $I = \mathrm{rad}(I) = \bigcap_{\mathfrak{p} \in \mathrm{Min}_R(R/I)} \mathfrak{p}$. $\square$

Example 7.11. Let k be a field, and $R = K[X,Y]_{(X,Y)}$ is local with $\mathfrak{m} = (X,Y)R$. Let $M = R/(XY)R$. Since $(X,Y)R = (XR) \cap (YR)$ and $\mathrm{Min}\{xR, yR\} = \{xR, yR\}$ by previous lemma, we have $\mathrm{Ass}_R(M) = \{xR, yR\}$. Need $a_1 \in (x,y)R \smallsetminus (xR \cup yR)$, e.g. $a_1 = fx + gy$ such that $x \nmid a_1$ and $y \nmid a_1$. e.g. $a_1 = x - y$. Then $M/a_1M = \frac{R/(xy)R}{(x-y) \cdot R/(xy)R} \cong \frac{R}{(x-y, xy)R} \cong \frac{R/(x-y)R}{xy \cdot R/(x-y)R}$. Note $R/(x-y)R = \frac{K[x,y]_{(x,y)}}{(x-y) \cdot K[x,y]_{(x,y)}} \cong K[x]_{(x)}$, i.e., killing $x - y$ is the same as setting $y = x$. Also, $xy \cdot R/(x-y)R \cong (x^2)K[x]_{(x)}$. So $M/(x-y)M \cong \frac{R/(x-y)R}{xy \cdot R/(x-y)R} \cong \frac{K[x]_{(x)}}{(x^2)K[x]_{(x)}}$. Note $\mathfrak{m} \in \mathrm{Ass}_R(M/(x-y)M)$. Claim. $\mathrm{Ann}_R(\overline{x} \in M/(x-y)M) = (x,y)R = \mathfrak{m}$. "$\supseteq$". $x \cdot \overline{x} = \overline{x^2} = 0$ in $\frac{K[x]_{(x)}}{(x^2)K[x]_{(x)}}$. Also, $x\overline{y} = x\overline{x} = 0$? "$\subseteq$". Since $x \notin x^2K[x,y]$, we have $0 \neq \overline{x} \in K[x]_{(x)}/(x^2)K[x]_{(x)}$. So $\mathrm{Ann}_R(\overline{x}) \neq R$. But since max'l $\mathfrak{m} \subseteq \mathrm{Ann}_R(\overline{x}) \subsetneq R$, $\mathfrak{m} = \mathrm{Ann}_R(\overline{x})$. Thus, $(x - y)$ is a maximal M-regular sequence in $\mathfrak{m}$.

Fact 7.12. Let $f : A \to A'$ and $g : A \to B'$ be R-module homomorphism. Then for $i \geqslant 0$, there exists R-module homomorphism $\mathrm{Ext}_R^i(A, g) : \mathrm{Ext}_R^i(A, B) \to \mathrm{Ext}_R^i(A, B')$ and $\mathrm{Ext}_R^i(f, B) : \mathrm{Ext}_R^i(A', B) \to \mathrm{Ext}_R^i(A, B)$. If $f' : A' \to A''$ and $g' : B' \to B''$ are also R-module homomorphism, then the following diagram commutes.

$$\begin{array}{ccc}
\mathrm{Ext}_R^i(A,B) & \xrightarrow{\mathrm{Ext}_R^i(A,g)} & \mathrm{Ext}_R^i(A,B') \\
& \searrow^{\mathrm{Ext}_R^i(A,g'\circ g)} & \downarrow{\scriptstyle \mathrm{Ext}_R^i(A,g')} \\
& & \mathrm{Ext}_R^i(A,B'')
\end{array}$$

So $\operatorname{Ext}^i_R(A, g' \circ g) = \operatorname{Ext}^i_R(A, g') \circ \operatorname{Ext}^i_R(A, g)$. Also

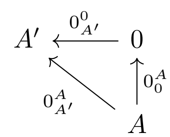


So $\operatorname{Ext}^i_R(f' \circ f, B) = \operatorname{Ext}^i_R(f, B) \circ \operatorname{Ext}^i_R(f', B)$. Also, the following diagram commutes.

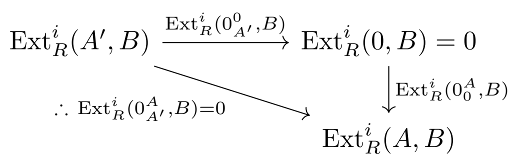
Thus, $\operatorname{Ext}^i_R(A, -)$ and $\operatorname{Ext}^i_R(-, B)$ respect composition.

Fact 7.13. When f and g are 0 maps, i.e., $f = 0^A_{A'}$ and $g = 0^B_{B'}$, we have $\operatorname{Ext}^i_R(A, 0^B_{B'}) = 0 = \operatorname{Ext}^i_R(0^A_{A'}, B)$.

Proof. Since $0^A_{A'} = 0^0_{A'} \circ 0^A_0$, we have



commutes. So $\operatorname{Ext}^i_R(0^A_{A'}, B) = \operatorname{Ext}^i_R(0^A_0, B) \circ \operatorname{Ext}^i_R(0^0_{A'}, B) = 0$. Our byproduct is that the following diagram commutes.



□

Fact 7.14. Let $a \in R$. Then $\mu^B_a : B \xrightarrow{a\cdot} B$ given by $b \mapsto ab$ is an R-module homormophism. Since $\operatorname{Ext}^i_R(A, \mu^B_a) : \operatorname{Ext}^i_R(A, B) \xrightarrow{a\cdot} \operatorname{Ext}^i_R(A, B)$, we have $\operatorname{Ext}^i_R(A, \mu^B_a) = \mu_a^{\operatorname{Ext}^i_R(A,B)}$. Since $\operatorname{Ext}^i_R(\mu^A_a, B) : \operatorname{Ext}^i_R(A, B) \xrightarrow{a\cdot} \operatorname{Ext}^i_R(A, B)$, we have $\operatorname{Ext}^i_R(\mu^A_a, B) = \mu_a^{\operatorname{Ext}^i_R(A,B)}$.

Fact 7.15. Let $1 \in R$ and $\operatorname{id}_A : A \to A$ and $\operatorname{id}_B : B \to B$. Then $\operatorname{Ext}^i_R(\operatorname{id}_A, B) = \operatorname{Ext}^i_R(\mu^A_1, B) = \mu_1^{\operatorname{Ext}^i_R(A,B)} = \operatorname{id}_{\operatorname{Ext}^i_R(A,B)}$ and $\operatorname{Ext}^i_R(A, \operatorname{id}_B) = \operatorname{Ext}^i_R(A, \mu^B_1) = \mu_1^{\operatorname{Ext}^i_R(A,B)} = \operatorname{id}_{\operatorname{Ext}^i_R(A,B)}$.

Lemma 7.16. Let M and N be R-module Then $\operatorname{Ann}_R(M) \cup \operatorname{Ann}_R(N) \subseteq \operatorname{Ann}_R(\operatorname{Ext}^i_R(M, N))$ for $i \geqslant 0$, i.e., if $x \in R$ such that $xM = 0$ or $xN = 0$, then $x \cdot \operatorname{Ext}^i_R(M, N) = 0$ for $i \geqslant 0$.

Proof. Let $x \in R$. Assume $xM = 0$. Then $\mu^M_x = 0^M_M$. Note $\mu_x^{\operatorname{Ext}^i_R(M,N)} = \operatorname{Ext}^i_R(\mu^M_x, N) = \operatorname{Ext}^i_R(0^M_M, N) = 0$. Assume $xN = 0$. Then $\mu^N_x = 0^N_N$. Note $\mu_x^{\operatorname{Ext}^i_R(M,N)} = \operatorname{Ext}^i_R(M, \mu^N_x) = \operatorname{Ext}^i_R(M, 0^N_N) = 0$. □

Example 7.17 (Previously)**.** Let $d = \gcd(m, n)$. Since $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}) \cup \mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = m\mathbb{Z} \cup n\mathbb{Z}$, we have $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/d\mathbb{Z}$.

Remark. $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N) \subseteq \mathrm{Ann}_R(\mathrm{Ext}^i_R(M, N))$ for $i \geqslant 0$. Note in general, it is $\subsetneq$. For example, since $\mathrm{Ext}^2_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = 0$, we have $\mathrm{Ann}_{\mathbb{Z}}(\mathrm{Ext}^2_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z})) = \mathbb{Z}$. But in general, $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}) + \mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}) = m\mathbb{Z} + n\mathbb{Z} = \gcd(m, n)\mathbb{Z} \neq \mathbb{Z}$. So $\mathrm{Ann}_R(M) + \mathrm{Ann}_R(N) \subseteq \bigcap_{i=0}^{\infty} \mathrm{Ann}_R(\mathrm{Ext}^i_R(M, N))$.

Theorem 7.18. *Assume R noetherian and $I \leqslant R$ and M f.g. R-mod. such that $IM \neq M$. Let $n \in \mathbb{N}_0$. Then the followings are equivalent.*

(a) $\mathrm{Ext}^i_R(N, M) = 0$ *for $i < n$ for finitely generated R-module N such that* $\mathrm{Supp}_R(N) \subseteq \mathrm{V}(I)$.

(b) $\mathrm{Ext}^i_R(R/I, M) = 0$ *for $i < n$.*

(c) $\mathrm{Ext}^i_R(N, M) = 0$ *for $i < n$ for some finitely generated R-module N such that* $\mathrm{Supp}_R(N) = \mathrm{V}(I)$.

(d) Every M-regular sequence in I of length $\leqslant n$ can be extended into an M-regular sequence in I of length n.

(e) M has a regular sequence of length n in I.

Proof. "(i)$\Longrightarrow$(ii)$\Longrightarrow$(iii)" since $\mathrm{Supp}_R(R/I) = \mathrm{V}(I)$.

"(iii)$\Longrightarrow$(iv)". Assume N is f.g. R-mod. with $\mathrm{Supp}_R(N) = \mathrm{V}(I)$ such that $\mathrm{Ext}^i_R(N, M) = 0$ for $i < n$. If $n = 0$, results are trivial. Assume $n \geqslant 1$. Since $\mathrm{Ext}^0_R(N, M) = 0$, we have $\mathrm{Hom}_R(N, M) = 0$. By lemma **??**, there exists $a_1 \in \mathrm{NZD}(M)$. Now induct on $n \in \mathbb{N}$. If $n = 1$, then done since start with a M-regular sequence of length 0 or 1 can be extended to a M-regular sequence of length 1. Inductive step: Assume $n \geqslant 2$ and result holds for any finitely generated N' such that $\mathrm{Ext}^i_R(N', M) = 0$ for $i < n-1$. Start with a M-regular sequence $a_1, \dots, a_k \in I$ such that $k \leqslant n$. If $k = n$, then done. If $k = 0$, then by previous argument, there exists M-regular $a_1 \in I$. Assume $1 \leqslant k \leqslant n-1$. Since $0 \to M \xrightarrow{a_1 \cdot} M \to M/a_1M \to 0$ is exact, the long exact sequence in $\mathrm{Ext}^i_R(N, -)$ is

$$0 \longrightarrow \mathrm{Hom}_R(N, M) \xrightarrow{a_1 \cdot} \mathrm{Hom}_R(N, M) \longrightarrow \mathrm{Hom}_R(N, M/a_1M) \longrightarrow \mathrm{Ext}^1_R(N, M) \longrightarrow \cdots$$

$$0 = \mathrm{Ext}^i_R(N, M) \longrightarrow \mathrm{Ext}^i_R(N, M/a_1M) \longrightarrow 0 = \mathrm{Ext}^{i+1}_R(N, M) \longrightarrow \cdots$$

where $i < n-1 < n$. So $i + 1 < n$. Hence $\mathrm{Ext}^i_R(N, M/a_1M) = 0$ for $i < n-1$. Since $a_2, \dots, a_k$ is a M/a_1M-regular sequence in I of length $k - 1 < n - 1$, by inductive hypothesis, we can extend it into a M-regular sequence $a_2, \dots, a_k, \dots, a_n$ of length $n-1$. Thus, $a_1, \dots, a_k, \cdots a_n \in I$ is a M-regular sequence of length n. (Check: if $IM \neq M$ and $a_1 \in I$, then $I \cdot M/a_1M \neq M/a_1M$.)

"(iv)$\Longrightarrow$(v)". Assume (iv). Then the empty sequence can be extended to an M-regular sequence in I of length I.

"(iv)$\Longrightarrow$(v)". Assume M has a regular sequence $a_1, \ldots, a_n \in I$. Let N be a finitely generated R-module such that $\mathrm{Supp}_R(N) \subseteq \mathrm{V}(I)$. NTS $\mathrm{Ext}_R^i(N, M) = 0$ for $i < n$. By induct on n. Base case: $n = 1$. NTS $\mathrm{Hom}_R(N, M) = 0$. Since N is finitely generated, $\mathrm{V}(\mathrm{Ann}_R(N)) = \mathrm{Supp}_R(N) \subseteq \mathrm{V}(I)$. So $I \subseteq \mathrm{Ann}_R(N)j$. Since $a_1 \in I$, $a_1^t \in I^t \subseteq I \subseteq \mathrm{Ann}_R(N)$ for $t \geqslant 1$. So $a_1^t N = 0$ for $t \geqslant 1$. Since $0 \to M \xrightarrow{a_1\cdot} M \to M/a_1M \to 0$ is exact, we have $0 \to \mathrm{Hom}_R(N, M) \xrightarrow{a_1\cdot} \mathrm{Hom}_R(N, M)$ and for $t \geqslant 1$, $0 \to \mathrm{Hom}_R(N, M) \xrightarrow{a_1^t\cdot} \mathrm{Hom}_R(N, M)$ are exact. Since $a_1^t N = 0$ for $t \geqslant 1$, we have $\mathrm{Hom}_R(N, M) = 0$. Inductive step: Assume $n \geqslant 2$ and I contains a M-regular sequence $a_1, \ldots, a_{n-1}$ of length $n-1$. By inductive hypothesis, $\mathrm{Ext}_R^i(N, M) = 0$ for $i < n-1$, and I contains a M/a_1M-regular sequence $a_2, \ldots, a_n$ of length $n-1$. Then by inductive hypothesis, $\mathrm{Ext}_R^i(N, M/a_1M) = 0$ for $i < n-1$. NTS $\mathrm{Ext}_R^{n-1}(N, M) = 0$. Since $0 \to M \xrightarrow{a_1\cdot} M \to M/a_1M \to 0$ is exact, the long exact sequence in $\mathrm{Ext}_R^i(N, -)$ is

$$0 \longrightarrow \mathrm{Hom}_R(N, M) \xrightarrow{a_1\cdot} \mathrm{Hom}_R(N, M) \longrightarrow \mathrm{Hom}_R(N, M/a_1M) \longrightarrow \mathrm{Ext}_R^1(N, M) \longrightarrow \cdots$$

$$\cdots \longrightarrow 0 = \mathrm{Ext}_R^{n-2}(N, M/a_1M) \longrightarrow \mathrm{Ext}_R^{n-1}(N, M) \xrightarrow{a_1\cdot} \mathrm{Ext}_R^{n-1}(N, M)$$

Thus, $\mathrm{Ext}_R^{n-1}(N, M) = 0$. $\square$

Chapter 8

Homology

8.1 Chain complexes and homology

Definition 8.1. A *chain complex* of R-modules and R-module homorphisms (R-complex, R-cplx, R-cx or R-cpx) is a sequence

$$(M_\bullet, \partial_\bullet^M) = \cdots \xrightarrow{\partial_{i+2}^M} M_{i+1} \xrightarrow{\partial_{i+1}^M} M_i \xrightarrow{\partial_i^M} M_{i-1} \xrightarrow{\partial_{i-1}^M} \cdots$$

of R-modules and R-module homorphisms such that $\partial_n^M \circ \partial_{n+1}^M = 0$ for $n \in \mathbb{Z}$, where the dot differentiates the complex from a module, and $\partial_\bullet$ denotes the collection of all the ∂_i's.

Let $(M_\bullet, \partial_\bullet^M)$ be a chain complex.

Definition 8.2. ∂_i^M is the i^{th} *differential* of the chain complex. $\partial_\bullet^M$ is called the *differential* of the complex.

Definition 8.3. $M_\bullet$ is *bounded below* if $M_i = 0$ for all sufficiently small (megative) i; a complex is *bounded above* if $M_i = 0$ for all sufficiently large (positive) i; a complex is *bounded* if $M_i = 0$ for all sufficiently large $|i|$.

For complexes bounded below we abbreviate "$0 \to 0 \to 0 \to 0 \to \cdots$" to one zero module, and similarly for complexes bounded above.

Definition 8.4. Define the i^{th} *homology module* by

$$\mathrm{H}_i(M_\bullet) = \frac{\mathrm{Ker}(\partial_i^M)}{\mathrm{Im}(\partial_{i+1}^M)}, \forall i \in \mathbb{Z},$$

which is the i^{th} homology module of M.

Lemma 8.5. $\mathrm{H}_i(M_\bullet)$ measures how far $M_\bullet$ is from being exact at M_i.

Definition 8.6. $M_\bullet$ is *exact at the i^{th} place* if $\mathrm{H}_i(M_\bullet) = 0$. $M_\bullet$ is exact if and only if $\mathrm{H}_i(M_\bullet) = 0$ for all $i \in \mathbb{Z}$.

Remark. If $M_\bullet$ is exact, then it decomposes into short exact sequences

$$\begin{array}{ccccccccccccc} & & & & & & 0 \longrightarrow \mathrm{Ker}(\partial_{i-1}^M) \longrightarrow M_{i-1} \longrightarrow \mathrm{Im}(\partial_{i-1}^M) \longrightarrow 0 \\ & & & & & & \| \\ & & & 0 \longrightarrow \mathrm{Ker}(\partial_i^M) \longrightarrow M_i \longrightarrow \mathrm{Im}(\partial_i^M) \longrightarrow 0 \\ & & & \| \\ 0 \longrightarrow \mathrm{Ker}(\partial_{i+1}^M) \longrightarrow M_{i+1} \longrightarrow \mathrm{Im}(\partial_{i+1}^M) \longrightarrow 0 \end{array}$$

etc.

Definition 8.7. $M_\bullet$ is *free* (resp. *flat, projective, injective*) if all the M_i's are free (resp, flat, projective, injective).

Remark. Free, projective, flat resolution are not uniquely determined, in the sense that free modules and the homomorphisms are not uniquely defined, not even up to isomorphisms.

Example 8.8. Let M be R-module. Let $P_\bullet^+ = \cdots \xrightarrow{\partial_3^P} P_2 \xrightarrow{\partial_2^P} P_1 \xrightarrow{\partial_1^P} P_0 \xrightarrow{\tau} M \to 0$ be an augmented projective resolution of M. Then $P_\bullet^+$ is a chain complex with $\mathrm{H}_i(P_\bullet^+) = 0$ for $i \in \mathbb{Z}$. Note $P_\bullet = \cdots \xrightarrow{\partial_3^P} P_2 \xrightarrow{\partial_2^P} P_1 \xrightarrow{\partial_1^P} P_0 \to 0$ is also a chain complex since $\partial_i^P \circ \partial_{i+1}^P = 0$ for $i \geqslant 1$, $\partial_0^P \circ \partial_1^P = 0 \circ \partial_1^P = 0$ and $\partial_i^P \circ \partial_{i+1}^P = 0 \cdot \partial_{i+1}^P = 0$ for $i \in \mathbb{Z}^{<0}$. So $\mathrm{H}_i(P_\bullet) = 0$ for $i \in \mathbb{Z} \setminus \{0\}$ and $\mathrm{H}_0(P_\bullet) = \frac{\mathrm{Ker}(P_0 \to 0)}{\mathrm{Im}(P_1 \to P_1)} = \frac{P_0}{\mathrm{Im}(\partial_1^P)} = \frac{P_0}{\mathrm{Ker}(\tau)} \cong \mathrm{Im}(\tau) = M$.

Theorem 8.9. *If the complex* $Q_\bullet = \cdots \xrightarrow{\partial_3^Q} Q_2 \xrightarrow{\partial_2^Q} Q_1 \xrightarrow{\partial_1^Q} Q_0 \to 0$ *is projective and* $\mathrm{H}_i(Q_\bullet) = 0$ *for* $i \in \mathbb{Z} \setminus \{0\}$, *then* $Q_\bullet$ *is a projective resolution of* $\mathrm{H}_0(Q_\bullet)$.

Proof. Note $\mathrm{H}_0(Q_\bullet) = \frac{\mathrm{Ker}(Q_0 \to 0)}{\mathrm{Im}(\partial_1^Q)} = \frac{Q_0}{\mathrm{Im}(\partial_1^Q)}$. Let $\pi : Q_0 \to Q_0 / \mathrm{Im}(\partial_1^P)$ be the natural projection. Then $Q_\bullet^+ : \cdot \xrightarrow{\partial_3^Q} Q_2 \xrightarrow{\partial_2^Q} Q_1 \xrightarrow{\partial_1^Q} Q_0 \xrightarrow{\pi} \frac{Q_0}{\mathrm{Im}(\partial_1^Q)} \to 0$ is exact. □

Remark. A complex might be naturally numbered in the opposite order:

$$(M^\bullet, \partial^\bullet) = \cdots \xrightarrow{\partial^{i-2}} M^{i-1} \xrightarrow{\partial^{i-1}} M^i \xrightarrow{\partial^i} \cdots,$$

we call it *co-complex.* The i^{th} *cohomology module* is

$$\mathrm{H}^i(M^\bullet) = \frac{\mathrm{Ker}(\partial^i)}{\mathrm{Im}(\partial^{i-1})}, \forall i \in \mathbb{Z}.$$

If $(M^\bullet, \partial^\bullet)$ is a co-complex, then

$$\cdots M^{-2} \xrightarrow{\partial^{-2}} M^{-1} \xrightarrow{\partial^{-1}} M^0 \xrightarrow{\partial^0} M^1 \xrightarrow{\partial^1} M^2 \xrightarrow{\partial^2} M_3 \xrightarrow{\partial^3} \cdots.$$

After renaming $N_n = M^{-n}$ and $d_n = \partial^{-n}$, we convert the co-complex into the complex:

$$\cdots N^2 \xrightarrow{d^2} N^1 \xrightarrow{d^1} N^0 \xrightarrow{d^0} N^{-1} \xrightarrow{d^{-1}} N^{-2} \xrightarrow{d^{-2}} N_{-3} \xrightarrow{d^{-3}} \cdots.$$

The naming can be even shifted: $F_n = M^{-n+2}$ and $e_n = \partial^{-n+2}$ converts the co-complex into the following complex:

$$\cdots F^2(= N^0) \xrightarrow{e^2=d^0} F^1(= N^{-1}) \xrightarrow{e^1} F^0 \xrightarrow{e^0} F^{-1} \xrightarrow{e^{-1}} F^{-2} \xrightarrow{e^{-2}} F_{-3} \xrightarrow{e^{-3}} \cdots .$$

Similarly, any complex can be converted into a co-complex, possibly with shifting.

Definition 8.10. Let N be an R-module.

(a)

$$\mathrm{Hom}_R(N, M_\bullet) = \cdots \xrightarrow{\mathrm{Hom}_R(N,\partial^M_{i+2})} \mathrm{Hom}_R(N, M_{i+1}) \xrightarrow{\mathrm{Hom}_R(N,\partial^M_{i+1})} \mathrm{Hom}_R(N, M_i) \xrightarrow{\mathrm{Hom}_R(N,\partial^M_i)} \cdots ,$$

or denote it as

$$M_{\bullet *} = \cdots \xrightarrow{(\partial^M_{i+2})_*} M_{i+1_*} \xrightarrow{\partial^M_{i+1_*}} M_{i*} \xrightarrow{\partial^M_{i\ *}} \cdots .$$

(b)

$$\mathrm{Hom}_R(M_\bullet, N) = \cdots \xrightarrow{\mathrm{Hom}_R(\partial^M_{i-1},N)} \mathrm{Hom}_R(M_{i-1}, N) \xrightarrow{\mathrm{Hom}_R(\partial^M_i,N)} \mathrm{Hom}_R(M_i, N) \xrightarrow{\mathrm{Hom}_R(\partial^M_{i+1},N)} \cdots ,$$

or denote it as

$$M^*_\bullet = \cdots \xrightarrow{\partial^M_{i-1}{}^*} (M_{i-1})^* \xrightarrow{\partial^{M*}_i} M^*_i \xrightarrow{\partial^M_{i+1}{}^*} \cdots .$$

Theorem 8.11. *$M_{\bullet *}$ and $M^*_\bullet$ are R-cpx.*

Proof. $\partial^M_{i\ *} \circ \partial^M_{i+1_*} = (\partial^M_i \circ \partial^M_{i+1})_* = 0_* = 0$ for $i \in \mathbb{Z}$ and $\partial^{M^*}_i \circ \partial^M_{i-1}{}^* = (\partial^M_{i-1} \circ \partial^M_i)^* = 0^* = 0$ for $i \in \mathbb{Z}$. ☐

Notation 8.12. (a) Let $(M_*)_i = M_{i*}$. Then $\partial^M_{i\ *} : M_{i*} \to M_{i-1*}$, which is $\partial^{M_*}_i : (M_*)_i \to M_{*i-1}$. So $\partial^{M_*}_i = \partial^M_{i\ *}$.

(b) Let $(M^*)_n = M_{-n}{}^*$. Then $\partial^M_{-n+1}{}^* : M_{-n}{}^* \to M_{-n+1}{}^*$. Also, $\partial^{M^*}_n : (M^*)_n \to (M^*)_{n-1}$. So $\partial^{M^*}_n = \partial^M_{-n+1}{}^*$.

Theorem 8.13. *Let M be an R-cx and N an R-module*

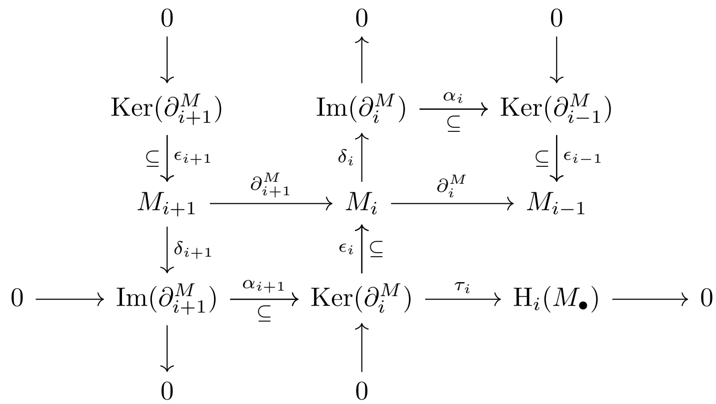
(c) If N is projective, then $\mathrm{H}_i(\mathrm{Hom}_R(N, M_\bullet)) \cong \mathrm{Hom}_R(N, \mathrm{H}_i(M_\bullet))$.

Slogan: Homming with projection in 1^{st} slot commutes with taking homology.

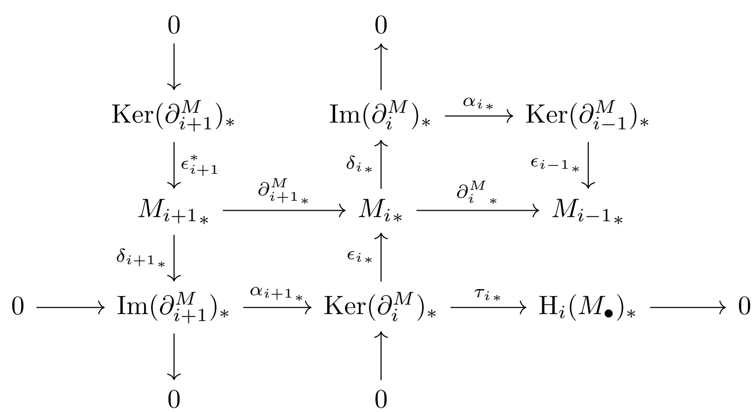
(d) If N is injective, then $\mathrm{H}_i(\mathrm{Hom}_R(M_\bullet, N)) \cong \mathrm{Hom}_R(\mathrm{H}_{-i}(M_\bullet), N)$.

Slogan: Homming with injection in 2^{nd} slot commutes with taking homology, as long as you are careful with the indices.

Proof. (c) . Let $i \in \mathbb{Z}$. Consider the following diagram



Note τ_i is canonical surjection and let δ_i be induced by ∂_i^M, i.e., $\delta_i(m) = \partial_i^M(m)$ for $m \in M_i$. All the three vertical sequences are exact, as is the lower horizontal sequence. Also, the above diagram commutes. (Hint: lower horizontal sequence in part (d) is $0 \to \mathrm{Im}(\partial_{-i+1}^M) \xrightarrow[\subseteq]{\alpha_{-i+1}} \mathrm{Ker}(\partial_{-i}^M) \xrightarrow{\tau_{-i}} \mathrm{H}_{-i}(M_\bullet) \to 0$.) Consider the following diagram



By the left exactness of homorphism, $(-)_*$ transforms monomorphism into monomorphism. Since N is projective, $(-)_*$ also transforms epimorphims into epimorphism. So all the three vertical sequences are exact, as is the lower horizontal sequence. Similarly, since α_i is a monomorphism, we have α_{i*} is a monomorphism. Also, the diagram above commutes. Claim 1. $\mathrm{Ker}(\delta_{i*}) = \mathrm{Ker}(\partial_i^M{}_*)$. Let $x \in \mathrm{Ker}(\delta_{i*})$. Then $\delta_{i*}(x) = 0$. Since α_{i*} and ϵ_{i-1_*} are monomorphisms, we have $\epsilon_{i-1_*} \circ \alpha_{i*}$ is also a monomorphsim. Since the above diagram on the right commutes, $\partial_i^M{}_*(x) = \epsilon_{i-1_*} \circ \alpha_{i*} \circ \delta_{i*}(x) = \epsilon_{i-1_*} \circ \alpha_{i*}(\delta_{i*}(x)) = \epsilon_{i-1_*} \circ \alpha_{i*}(0) = 0$. So $x \in \mathrm{Ker}(\partial_i^M{}_*)$. Hence $\mathrm{Ker}(\delta_{i*}) \subseteq \mathrm{Ker}(\partial_i^M{}_*)$. Let $y \in \mathrm{Ker}(\partial_i^M{}_*)$. Assume $\delta_{i*}(y) = z$. Since the above diagram on the right commutes, we have $0 = \partial_i^M{}_*(y) = \epsilon_{i-1_*} \circ \alpha_{i*} \circ \delta_{i*}(y) = \epsilon_{i-1_*} \circ \alpha_{i*}(z)$. Since $\epsilon_{i-1_*} \circ \alpha_{i*}$ is a monomorphism, $z = 0$. Then $y \in \mathrm{Ker}(\partial_{i*})$. Hence $\mathrm{Ker}(\delta_{i*}) \supseteq \mathrm{Ker}(\partial_i^M{}_*)$. Thus, $\mathrm{Ker}(\delta_{i*}) = \mathrm{Ker}(\partial_i^M{}_*)$. Claim 2. $\mathrm{Im}(\partial_{i+1}^M)_* \cong \mathrm{Im}(\partial_{i+1_*}^M)$. Since the above diagram on the left commutes, $\epsilon_{i*} \circ \alpha_{i+1_*} \circ \delta_{i+1_*} \equiv \partial_{i+1_*}^M$. Since α_{i+1_*} and ϵ_{i*} are monomorphisms and δ_{i+1_*} is an epimorphism, $\mathrm{Im}(\partial_{i+1}^M)_* = \mathrm{Im}(\delta_{i+1_*}) \cong \mathrm{Im}(\partial_{i+1_*}^M)$. We need to show $\mathrm{H}_i(M_{\bullet *}) \cong \mathrm{H}_i(M_\bullet)_*$. Consider the following diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Im}(\partial^M_{i+1})_* & \xrightarrow[\subseteq]{\alpha_{i+1*}} & \mathrm{Ker}(\partial^M_i)_* & \xrightarrow{\tau_{i*}} & \mathrm{H}_i(M_\bullet)_* & \longrightarrow & 0 \\
 & & \cong\big\downarrow\beta & & \cong\big\downarrow\gamma & & \cong\big\downarrow\exists\theta & & \\
0 & \longrightarrow & \mathrm{Im}(\partial^M_{i+1*}) & \xrightarrow{\subseteq} & \mathrm{Ker}(\partial^M_{i\ *}) & \longrightarrow & \mathrm{H}_i(M_{\bullet *}) & \longrightarrow & 0 \\
 & & =\big\uparrow & & =\big\uparrow & & =\big\uparrow & & \\
0 & \longrightarrow & \mathrm{Im}(\partial^{M_*}_{i+1}) & \xrightarrow{\subseteq} & \mathrm{Ker}(\partial^{M_*}_i) & \longrightarrow & \mathrm{H}_i((M_*)_\bullet) & \longrightarrow & 0
\end{array}$$

Since N is projective, we have $(-)_*$ transforms SES into SES. So the first horizontal sequence in the above diagram is exact. Since $M_{\bullet *} = \cdots \xrightarrow{\partial^M_{i+2*}} M_{i+1*} \xrightarrow{\partial^M_{i+1*}} M_{i*} \xrightarrow{\partial^M_{i\ *}} \cdots$, we have $\mathrm{H}_i(M_{\bullet *}) = \mathrm{Ker}(\partial^M_{i\ *})/\mathrm{Im}(\partial^M_{i+1*})$. So the second horizontal sequence in the above diagram is exact. Let $\gamma(x) := \epsilon_{i*}(x)$ for $x \in \mathrm{Ker}(\partial^M_i)_*$. Since $\mathrm{Ker}(\delta_{i*}) = \mathrm{Ker}(\partial^M_{i\ *})$, we have $\mathrm{Im}(\gamma) = \mathrm{Im}(\epsilon_{i*}) = \mathrm{Ker}(\delta_{i*}) = \mathrm{Ker}(\partial^M_{i\ *})$. So $\gamma : \mathrm{Ker}(\partial^M_i)_* \to \mathrm{Ker}(\partial^M_{i\ *})$ is a well-defined epimorphism. Also, ϵ_{i*} is a monomorphism, so γ is an isomorphism. Let β be defined as the isomorphism $\beta : \mathrm{Im}(\partial^M_{i+1})_* \cong \mathrm{Im}(\partial^M_{i+1*})$. By one of our homework, $\mathrm{H}_i(M_\bullet)_* \cong \mathrm{H}_i(M_{\bullet *})$. □

8.2 Ext modules

Theorem 8.14. *Let M and N be R-modules and $P_\bullet$ is a projective resolution of M. Then* $\mathrm{Ext}^i_R(M,N) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, N)) = \mathrm{H}_{-i}(P^*_\bullet)$ *for* $i \in \mathbb{Z}$.

Proof. $P^+_\bullet : 0 \to P^*_0 \to P^*_1 \to P^*_2 \to \cdots \to P^*_i \to \cdots$ is exact and has degree $1 \to 0 \to -1 \to -2 \to \cdots - i \to \cdots$ and $(P^*_\bullet)_i = P^*_{-i}$. □

Theorem 8.15 (Slogan: $\mathrm{Ext}(M,N)$ is independent of choice of proj. resol.). *If $P_\bullet$ and $Q_\bullet$ are proj. resol. of M, then* $\mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, N)) \cong \mathrm{H}_{-i}(\mathrm{Hom}_R(Q_\bullet, N))$.

Theorem 8.16. *(a)* $\mathrm{Ext}^i_R(M,N) = 0$ *for* $i < 0$.

(b) $\mathrm{Ext}^i_R(M,0) = 0$ *for* $i \in \mathbb{Z}$.

(c) $\mathrm{Ext}^i_R(0,N) = 0$ *for* $i \in \mathbb{Z}$.

Proof. (a) Since $(P^*_\bullet)_{-i} = 0$ for $-i > 0$, we have $\mathrm{Ext}^i_R(M,N) = \mathrm{H}_{-i}(P^*_\bullet) = 0$ for $i < 0$.

(b) Since $\mathrm{Hom}_R(P_\bullet, 0)_{-i} = \mathrm{Hom}_R(P_i, 0) = 0$ for $i \in \mathbb{Z}$, have $\mathrm{Ext}^i_R(M,0) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, 0)) = \mathrm{Hom}_R(P_\bullet, 0)_{-i} = 0$ for $i \in \mathbb{Z}$.

(c) The projective resolution of $M = 0$ is $P^+_\bullet = \cdots \to 0 \to 0 \to 0 \to 0$. Then $P_\bullet = 0 = P^+_\bullet$, $\mathrm{Hom}_R(P_\bullet, N) = \mathrm{Hom}_R(0, N) = 0$, $\mathrm{Ext}^i_R(M,0) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, N)) = \mathrm{H}_{-i}(0_\bullet) = 0$ for $i \in \mathbb{Z}$. □

Theorem 8.17. $\mathrm{Ext}^0_R = \mathrm{Hom}_R(M,N)$.

Proof. By left-exactness of Hom- proved earlier. □

Theorem 8.18. *(a) If M is projective, then* $\mathrm{Ext}^i_R(M,N) = 0$ *for* $i \geqslant 1$.

(b) If N is injective, then $\mathrm{Ext}^i_R(M,N) = 0$ *for* $i \geqslant 1$.

Proof. (a) Since M is projective, the projective resolution of M is $P_\bullet^+ = \cdots \to 0 \to 0 \to M \xrightarrow{\text{id}} M \to 0 \to \cdots$ which has degree $\cdots \to 2 \to 1 \to 0 \to -1 \to -2 \to \cdots$. Note $P_\bullet = \cdots \to 0 \to 0 \to M \to 0 \to \cdots$. Then $P_\bullet^* = \cdots \to 0 \to 0 \to M^* \to 0 \to \cdots$, where M_* corresponds to first M. Since the stuff after M^* is 0, $\mathrm{Ext}_R^i(M,N) = \mathrm{H}_{-i}(P_\bullet^*) = 0$ for $i \geqslant 1$.

(b) Since $\mathrm{H}_i(P_\bullet) = 0$ for $i \geqslant 1$ and $\mathrm{H}_0(P_\bullet) \cong M$, we have $\mathrm{Ext}_R^i(M,N) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, N)) \cong \mathrm{Hom}_R(\mathrm{H}_i(P_\bullet), N) \cong \mathrm{Hom}_R(0,N) = 0$ for $i \geqslant 1$. □

Theorem 8.19. *Assume R is noetherian and M, N are both finitely generated R-modules, then $\mathrm{Ext}_R^i(M,N)$ are finitely generated for any i.*

Proof. Since R is noetherian and M is finitely generated, M has projective resolution of form $P_\bullet = \cdots \to R^{\beta_2} \to R^{\beta_1} \to R^{\beta_2} \to 0$ with $\beta_i \in \mathbb{Z}^{\geqslant 0}$. Note $\mathrm{Hom}_R(R^{\beta_i}, N) \cong \mathrm{Hom}_R(R,N)^{\beta_i} \cong N^{\beta_i}$. Since N is finitely generated R-module, N^{β_i} is also finitely generated R-module. Then since R is noetherian, N^{β_i} is also noetherian. Since $\mathrm{Ker}({\partial_{i+1}^P}^*) \subseteq N^{\beta_i}$, we have $\mathrm{Ext}_R^i(M,N) = \mathrm{H}_{-i}(P_\bullet^*) = \frac{\mathrm{Ker}({\partial_{i+1}^P}^*)}{\mathrm{Im}(\partial_i^{P^*})}$. (Actually, ${\partial_{i+1}^P}^* = \partial_{-i}^{P^*}$ and $\partial_i^{P^*} = \partial_{-i+1}^{P^*}$.) □

Chapter 9

Chain maps

Definition 9.1. Let $M_\bullet$ and $N_\bullet$ be R-cxs. *Chain maps* are commutative ladder diagram $F_\bullet = M_\bullet \to N_\bullet$, i.e.,

$$\begin{array}{ccccccc}
M_\bullet & & \cdots M_i & \xrightarrow{\partial_i^M} & M_{i-1} & \longrightarrow & \cdots \\
\downarrow{\scriptstyle F_\bullet} & & \downarrow{\scriptstyle F_i} & & \downarrow{\scriptstyle F_{i-1}} & & \\
N_\bullet & & \cdots N_i & \xrightarrow{\partial_i^N} & N_{i-1} & \longrightarrow & \cdots
\end{array}$$

commutes, i.e., a sequence $\{F_i : M_i \to N_i | i \in \mathbb{Z}\}$ of R-modules making the above diagram commute. (An isomorphism from $M_\bullet \to N_\bullet$ is a chain map $F; M_\bullet \to N_\bullet$ such that each F_i is an isomorphism.) Then there exists induced map (R-mod. hom.) on homology, $\mathrm{H}_i(F_\bullet) : \mathrm{H}_i(M_\bullet) \to \mathrm{H}_i(N_\bullet)\overline{m} = \overline{F_i(m)}$ for $m \in \mathrm{Ker}(\partial_i^M)$.

Theorem 9.2. *Let $F_\bullet : M_\bullet \to N_\bullet$ be a chain map.*

(a) $F_i(\mathrm{Ker}(\partial_i^M)) \subseteq \mathrm{Ker}(\partial_i^N)$.

(b) $F_i(\mathrm{Im}(\partial_{i+1}^M) \subseteq \mathrm{Im}(\partial_{i+1}^N)$.

(c) F_i induces a well-defined R-module homomorphism $\mathrm{H}_i(F_\bullet) : \mathrm{H}_i(M_\bullet) \to \mathrm{H}_i(N_\bullet)$ *given by* $\overline{m} \mapsto \overline{F_i(m)}$, *i.e.,* $m + \mathrm{Im}(\partial_{i+1}^M) \mapsto F_i(m) + \mathrm{Im}(\partial_{i+1}^N)$.

Proof. (a) and (b) is from the community of F_i. Note

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathrm{Im}(\partial_{i+1}^M) & \xrightarrow{\subseteq} & \mathrm{Ker}(\partial_i^M) & \longrightarrow & \mathrm{H}_i(M_\bullet) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_i} & & \downarrow{\scriptstyle \beta_i} & & \downarrow{\scriptstyle \exists!\, \mathrm{H}_i(F_\bullet)} & & \\
0 & \longrightarrow & \mathrm{Im}(\partial_{i+1}^N) & \xrightarrow{\subseteq} & \mathrm{Ker}(\partial_i^N) & \longrightarrow & \mathrm{H}_i(N_\bullet) & \longrightarrow & 0
\end{array}$$

where α_i is induced by F_i by (b) and β_i is induced by F_i by (a). □

Example 9.3. Let $R = \mathbb{Z}/12\mathbb{Z}$. Consider

$$\begin{array}{ccccccccc}
M_\bullet & \cdots & \xrightarrow{6} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{4} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{6} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{4} \cdots \\
\downarrow F_\bullet & & & \downarrow 2 & & \downarrow 3 & & \downarrow 2 & \\
N_\bullet & \cdots & \xrightarrow{4} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{6} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{4} & \mathbb{Z}/12\mathbb{Z} & \xrightarrow{6} \cdots
\end{array}$$

Since

$$\begin{array}{ccc}
 & \longrightarrow & \\
\downarrow & & \downarrow \cdot 12 \\
 & \xrightarrow{\cdot 12} & 0
\end{array}$$

we have each diagram commutes. So $F_\bullet$ is a chain map. Let the degree of the middle module $\mathbb{Z}/12\mathbb{Z}$ be 0. Then $\mathrm{H}_0(M_\bullet) = \frac{\mathrm{Ker}(\mathbb{Z}_{12} \xrightarrow{6} \mathbb{Z}_{12})}{\mathrm{Im}(\mathbb{Z}_{12} \xrightarrow{4} \mathbb{Z}_{12})}. = \frac{2\mathbb{Z}_{12}}{4\mathbb{Z}_{12}} \cong \frac{2\mathbb{Z}}{4\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$ and $\mathrm{H}_0(N_\bullet) = \frac{\mathrm{Ker}(\mathbb{Z}_{12} \xrightarrow{4} \mathbb{Z}_{12})}{\mathrm{Im}(\mathbb{Z}_{12} \xrightarrow{6} \mathbb{Z}_{12})}. = \frac{4\mathbb{Z}_{12}}{6\mathbb{Z}_{12}} \cong\cong \frac{6\mathbb{Z}}{12\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$. Let

$$\begin{aligned}
\mathrm{H}_0(F_\bullet) : \mathrm{H}_0(M_\bullet) &\to \mathrm{H}_0(N_\bullet) \\
\frac{2\mathbb{Z}_{12}}{4\mathbb{Z}_{12}} &\xrightarrow{\cdot 3} \frac{3\mathbb{Z}_{12}}{6\mathbb{Z}_{12}} \\
\overline{2n} &\mapsto \overline{3 \cdot 2n} = \overline{6n} = 0.
\end{aligned}$$

So $\mathrm{H}_0(F_\bullet) = 0$. Let

$$\begin{aligned}
\mathrm{H}_1(F_\bullet) : \mathrm{H}_1(M_\bullet) &\to \mathrm{H}_1(N_\bullet) \\
\frac{3\mathbb{Z}_{12}}{6\mathbb{Z}_{12}} &\xrightarrow{\cdot 2} \frac{2\mathbb{Z}_{12}}{4\mathbb{Z}_{12}} \\
\overline{3k} &\mapsto \overline{2 \cdot 3n} = \overline{6k} \\
\bar{0} = \overline{0k} &\mapsto \overline{0k} = 0 \\
\bar{3} &\mapsto \bar{6} = \bar{2}
\end{aligned}$$

So $\mathrm{H}_0(F_\bullet) = 0$. Since $\bar{3}$ is gen. for $\mathrm{H}_1(M_\bullet)$ and $\bar{2}$ is gen. for $\mathrm{H}_1(N_\bullet)$, we have $\mathrm{H}_1(F_\bullet)$ is an isomorphism.

Remark. Review

(a) There exists induced maps on Ext.

(b) Maps induced by multiplicative maps are themselves multiplication maps.

(c) L.E.S's.

Remark. Let $f : M \to M'$ and $g : N \to N'$ and $\mathrm{Ext}^i_R(M,N) \xrightarrow{\mathrm{Ext}^i_R(M,g)} \mathrm{Ext}^i_R(M,N')$, and $\mathrm{Ext}^i_R(M,N) \xrightarrow{\mathrm{Ext}^i_R(f,N)} \mathrm{Ext}^i_R(M',N)$. These will come from chain maps on corresponding CXS used to define the Ext. $\mathrm{Hom}_R(P_\bullet, N) \xrightarrow{\mathrm{Hom}_R(P_\bullet, g)} \mathrm{Hom}_R(P_\bullet, N')$ and $\mathrm{Hom}_R(P'_\bullet, N) \xrightarrow{\mathrm{Hom}_R(F_\bullet, N)} \mathrm{Hom}_R(P_\bullet, N)$, where $F_\bullet$ is not f, $P_\bullet$ is a projection resolution of M and $P'_\bullet$ is a projetive resolution of M', and $F_\bullet : P_\bullet \to P'_\bullet$ is a "lift" of f, i.e.,

$$\begin{array}{ccccccccc}
P_\bullet^+ = \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle F_1} & & \Big\downarrow{\scriptstyle F_0} & & \Big\downarrow{\scriptstyle f} & & \\
(P'_\bullet)^+ = \cdots & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & M' & \longrightarrow & 0
\end{array}$$

commutes, i.e., $F_\bullet$ is a chain map such that

$$\mathrm{H}_0(F_\bullet): \qquad \begin{array}{ccc}
\mathrm{H}_0(P_\bullet) & \xrightarrow{\mathrm{H}_0(F_\bullet)} & \mathrm{H}_0(P'_\bullet) \\
\Big\downarrow{\scriptstyle \cong} & & \Big\downarrow{\scriptstyle \cong} \\
M & \xrightarrow{\quad f \quad} & M'
\end{array}$$

Note

$$\begin{array}{ccccccc}
P_\bullet = \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & 0 \\
 & & \Big\downarrow{\scriptstyle F_1} & & \Big\downarrow{\scriptstyle F_0} & & \\
P'_\bullet = \cdots & \longrightarrow & P'_1 & \longrightarrow & P'_0 & \longrightarrow & 0
\end{array}$$

also commutes. Need to show $\mathrm{Hom}_R(P_\bullet, g)$ and $\mathrm{Hom}_R(F_\bullet, N)$ are chain maps.

$$\begin{array}{cccccccccc}
\mathrm{Hom}_R(P_\bullet, N): 0 & \longrightarrow & P_0^* & \xrightarrow{\partial_1^{P\,*}} & P_1^* & \longrightarrow \cdots \longrightarrow & P_i^* & \xrightarrow{\partial_{i+1}^{P}{}^*} & P_{i+1}^* & \longrightarrow \cdots \\
 & & \Big\downarrow & & \Big\downarrow{\scriptstyle g^*} & & \Big\downarrow{\scriptstyle g^*} & & \Big\downarrow{\scriptstyle g^*} & \\
\mathrm{Hom}_R(P_\bullet, N'): 0 & \longrightarrow & P_0^* & \xrightarrow{\partial_1^{P\,*}} & P_1^* & \longrightarrow \cdots \longrightarrow & P_i^* & \xrightarrow{\partial_{i+1}^{P}{}^*} & P_{i+1}^* & \longrightarrow \cdots
\end{array}$$

where $P_i^* \xrightarrow{g^*} P_i^*$ is actually $\mathrm{Hom}_R(P_i, N) \xrightarrow{\mathrm{Hom}_R(P_i, g)} \mathrm{Hom}_R(P_i, N')$. Let $\phi \in P_i^*$. Then

$$\begin{array}{ccc}
\phi & \longmapsto & \phi \circ \partial_{i+1}^P \\
\Big\downarrow & & \Big\downarrow \\
g \circ \phi & \longmapsto & (g \circ \phi) \circ \partial_{i+1}^P = g \circ (\phi \circ \partial_{i+1}^P)
\end{array}$$

$\mathrm{Ext}_R^i(M, g) = \mathrm{H}_{-i}(\mathrm{Hom}_R(P_\bullet, g))$ and $\mathrm{Ext}_R^i(M, g)(\bar{\phi}) = \overline{\mathrm{Hom}_R(P_\bullet, g)_{-i}(\phi)} = \overline{\mathrm{Hom}_R(P_i, g)(\phi)} = \overline{g \circ \phi}$. Next, consider $\mathrm{Ext}_R^i(f, N)$. $\mathrm{Hom}_R(F_\bullet, N): \mathrm{Hom}_R(P'_\bullet, N) \to \mathrm{Hom}_R(P_\bullet, N)$.

$$\begin{array}{cccccccccc}
\mathrm{Hom}_R(P'_\bullet, N): 0 & \longrightarrow & P_0'^* & \xrightarrow{\partial_1^{P'\,*}} & P_1'^* & \longrightarrow \cdots \longrightarrow & P_i'^* & \xrightarrow{\partial_{i+1}^{P'}{}^*} & P_{i+1}'^* & \longrightarrow \cdots \\
 & & \Big\downarrow & & \Big\downarrow{\scriptstyle F_0^*} & & \Big\downarrow{\scriptstyle F_i^*} & & \Big\downarrow{\scriptstyle F_{i+1}^*} & \\
\mathrm{Hom}_R(P_\bullet, N): 0 & \longrightarrow & P_0^* & \xrightarrow{\partial_1^{P\,*}} & P_1^* & \longrightarrow \cdots \longrightarrow & P_i^* & \xrightarrow{\partial_{i+1}^{P}{}^*} & P_{i+1}^* & \longrightarrow \cdots
\end{array}$$

where $P_i^* \xrightarrow{F_i^*} P_i^*$ is actually $\mathrm{Hom}_R(P'_i, N) \xrightarrow{\mathrm{Hom}_R(F_i, N)} \mathrm{Hom}_R(P_i, N)$. Let $\psi \in P_i'^*$.

$$\begin{array}{ccc}
\psi & \longmapsto & \psi \circ \partial_{i+1}^{P'} \\
\Big\downarrow & & \Big\downarrow \\
\psi \circ F_i & \longmapsto & (\psi \circ F_i) \circ \partial_{i+1}^P = (\psi \circ \partial_{i+1}^{P'}) \circ F_{i+1}
\end{array}$$

since $F_\bullet$ is a chain map and then by the community of the following diagram,

$$\begin{array}{ccccccc} \cdots & \longrightarrow & P_{i+1} & \xrightarrow{\partial_{i+1}} & P_i & \longrightarrow & \cdots \\ & & \downarrow F_{i+1} & & \downarrow F_i & & \\ \cdots & \longrightarrow & P'_{i+1} & \xrightarrow{\partial'_{i+1}} & P'_i & \longrightarrow & \cdots \end{array}$$

NTS these are independent of choices of $P_\bullet, P'_\bullet$ and $F_\bullet$. The existence of $F_\bullet$ is already been showed. $\mathrm{Ext}^i_R(f,N)(\overline{\psi}) = \overline{\mathrm{Hom}_R(F_\bullet,N)_{-i}(\psi)} = \overline{\psi \circ F_i}$. Review of goal 1. Yes. Review of goal 2. Let $r \in R$. $\mu^{M,r} : M \xrightarrow{r\cdot} M$. If $L_\bullet$ is an R-cx, note that

$$\begin{array}{ccccccc} L_\bullet = \cdots & \longrightarrow & L_i & \xrightarrow{\partial^L_i} & L_{i-1} & \longrightarrow & \cdots \\ & & \downarrow \mu^{L_i,r} & & \downarrow \mu^{L_{i-1},r} & & \\ L_\bullet = \cdots & \longrightarrow & L_i & \xrightarrow{\partial^L_i} & L_{i-1} & \longrightarrow & \cdots \end{array}$$

Let $l \in L_i$. Then

$$\begin{array}{ccc} l & \longmapsto & \partial^L_i(l) \\ \downarrow & & \downarrow \\ rl & \longmapsto & \partial^L_i(rl) = r \cdot \partial^L_i(l) \end{array}$$

since ∂^L_i is an R-module homomorphism. So $\mu^{L_\bullet,r}$ is a chain map. Furthermore, $\mathrm{H}_i(\mu^{L_\bullet,r}) = \mu^{\mathrm{H}_i(L_\bullet),r}$ since $\mathrm{H}_i(\mu^{L_\bullet,r})(\bar{l}) = \overline{\mu^{L_i,r}(l)} = \overline{rl} = r\bar{l} = \mu^{\mathrm{H}_i(L_\bullet),r}(\bar{l})$. Claim. $\mathrm{Ext}^i_R(\mu^{M,r},N) = \mu^{\mathrm{Ext}^i_R(M,N),r} = \mathrm{Ext}^i_R(M,\mu^{N,r})$. Since $\mu^{N,r}(\phi(x)) = r \cdot \phi(x) = (r\phi)(x)$, we have $\mu^{N,r} \circ \phi = r\phi$. $\mathrm{Ext}^i_R(M,\mu^{N,r})(\bar{\phi}) = \overline{\mu^{N,r} \circ \phi} = \overline{r\phi} = r\bar{\phi} = \mu^{\mathrm{Ext}^i_R(M,N),r}(\bar{\phi})$. For $\mathrm{Ext}^i_R(\mu^{M,r},N)$, need to find F.

$$\begin{array}{ccccccccc} P^+_\bullet = \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ \downarrow \mu^{P^+_\bullet,r} & & \downarrow \mu^{P_1,r} & & \downarrow \mu^{P_0,r} & & \downarrow \mu^{M,r} & & \\ P^+_\bullet = \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

commutes, where $F_i := \mu^{P_i,r}$. So $\mathrm{Ext}^i_R(\mu^{M,r},N)(\overline{\psi}) = \overline{\psi \circ \mu^{P_i,r}} = \overline{r\psi} = r \cdot \overline{\psi} = \mu^{\mathrm{Ext}^i_R(M,N),r}(\overline{\psi})$.

9.1 Liftings of resolutions

Lemma 9.4. Consider diag. with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & P & \xrightarrow{\gamma} & M & \longrightarrow & 0 \\ & & & & & & \downarrow f & & \\ 0 & \longrightarrow & N' & \xrightarrow{\delta} & Q & \xrightarrow{\sigma} & N & \longrightarrow & 0 \end{array}$$

such that P is projective and f is an R-module homomorphism. Then there exists commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{\alpha} & P & \xrightarrow{\gamma} & M & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle f'} & & \Big\downarrow{\scriptstyle F} & & \Big\downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & N' & \xrightarrow{\delta} & Q & \xrightarrow{\sigma} & N & \longrightarrow & 0 \end{array}$$

Proof. $\exists F$. version 1:

$$\begin{array}{ccccc} & & P & & \\ & \swarrow{\scriptstyle \exists F} & \Big\downarrow{\scriptstyle f\circ\gamma} & & \\ Q & \xrightarrow{\sigma} & N & \longrightarrow & 0 \end{array}$$

$\exists F$. version 2: since P is projective, $\mathrm{Hom}_R(P,-)$ is exact. Then $0 \to \mathrm{Hom}_R(P,N') \to \mathrm{Hom}_R(P,Q) \xrightarrow{\mathrm{Hom}_R(P,\sigma)=\sigma_*} \mathrm{Hom}_R(P,N) \to 0$ is exact. So σ_* is onto. Thus, there exists $F \in \mathrm{Hom}_R(P,Q)$ such that $f\circ\gamma = \sigma_*(F) = \sigma\circ F$.

$\exists f'$. Let $m' \in M'$. Then $\sigma(F(\alpha(m'))) = f(\gamma(\alpha(m'))) = f(0) = 0$. So $F(\alpha(M')) \subseteq \mathrm{Ker}(\sigma) = \mathrm{Im}(\delta)$ ($\cong N'$). Since δ is 1-1, for $m' \in M'$, there exists a unique $n' \in N'$ such that $F(\alpha(m')) = \delta(n')$. Then define $f'(m') = n'$, which is well-defined. Check f' is an R-module homomorphism. Let $m' \in M'$ and $r \in R$. Then there exists $n' \in N'$ such that $F(\alpha(m')) = \delta(n')$. So $\delta(rn') = r\cdot\delta(n') = rF(\alpha(m')) = F(\alpha(rm'))$, i.e., $rm' \longleftrightarrow rn'$. Hence $f'(rm') = rn' = rf'(m')$. The additive of f' is verified similarly. □

Theorem 9.5. *Let $P_\bullet^+$ be a proj. resol. of M and $Q_\bullet^+$ be "a lift resolution of N", i.e., $Q_\bullet^+ = \cdots \to Q_1 \to Q_0 \to N \to 0$ is exact but Q_i may or may or be projective. Then for any R-module homomorphism $f : M \to N$, there exists commutative diagram*

$$\begin{array}{cccccccccc} P_\bullet^+ \cdots & \longrightarrow & P_1 & \longrightarrow & P_0 & \longrightarrow & M & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle F_1} & & \Big\downarrow{\scriptstyle F_0} & & \Big\downarrow{\scriptstyle f} & & \\ Q_\bullet^+ \cdots & \longrightarrow & Q_1 & \xrightarrow{\delta} & Q_0 & \xrightarrow{\sigma} & N & \longrightarrow & 0 \end{array}$$

Proof. Proof using the previous lemma.

□

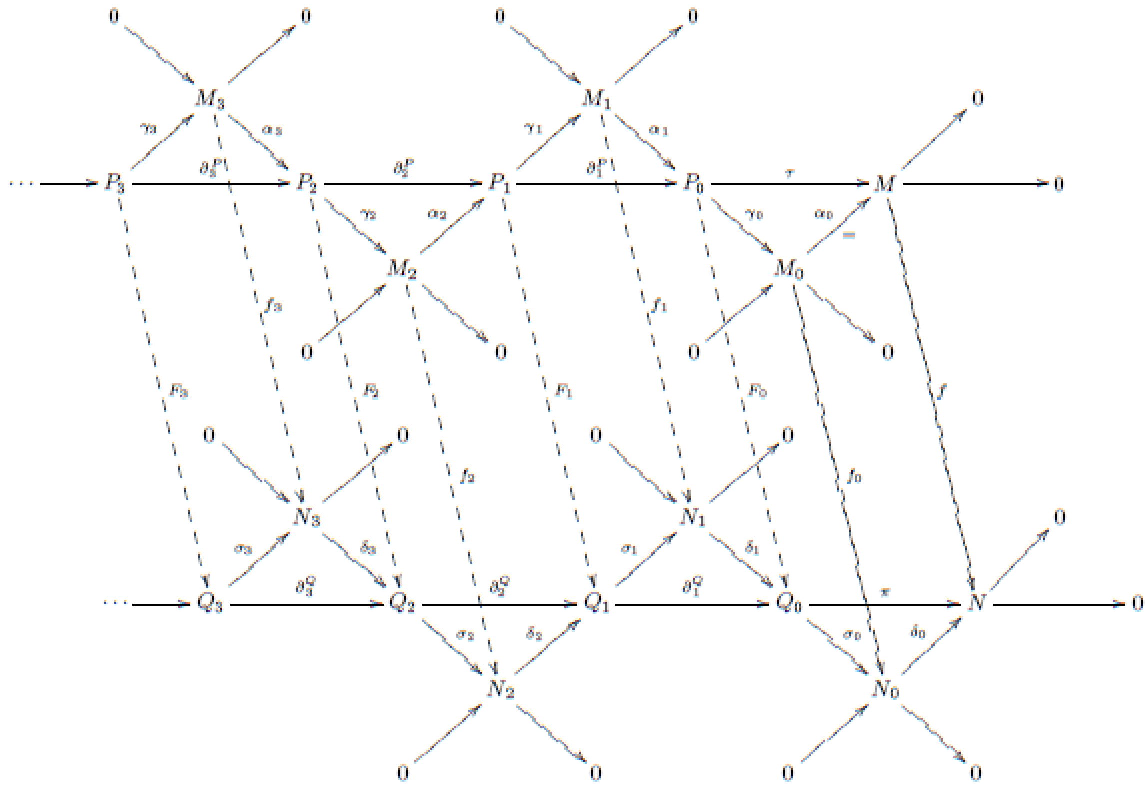
Example 9.6. Let $R = \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$, and $M = \mathbb{Z}_6$, $M' = \mathbb{Z}_3$.

$$\begin{array}{cccccccccccccc} P_\bullet^+ \cdots & \xrightarrow{2} & \mathbb{Z}_{12} & \xrightarrow{6} & \mathbb{Z}_{12} & \xrightarrow{2} & \mathbb{Z}_{12} & \xrightarrow{6} & \mathbb{Z}_{12} & \xrightarrow{\tau} & \mathbb{Z}_6 & \longrightarrow & 0 \\ & & \Big\downarrow{\scriptstyle 2} & & \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle 2} & & \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle \rho} & & \\ Q_\bullet^+ \cdots & \xrightarrow{4} & \mathbb{Z}_{12} & \xrightarrow{3} & \mathbb{Z}_{12} & \xrightarrow{4} & \mathbb{Z}_{12} & \xrightarrow{3} & \mathbb{Z}_{12} & \xrightarrow{\pi} & \mathbb{Z}_3 & \longrightarrow & 0 \end{array}$$

where τ, ρ, π are natural surjections $\overline{\alpha} \to \overline{\alpha}$.

$$\begin{array}{cccccccccccc} P_\bullet & \cdots & \xrightarrow{2} & \mathbb{Z}_{12} & \xrightarrow{6} & \mathbb{Z}_{12} & \xrightarrow{2} & \mathbb{Z}_{12} & \xrightarrow{6} & \mathbb{Z}_{12} & \longrightarrow & 0 \\ \Big\downarrow{\scriptstyle F_\bullet} & & & \Big\downarrow{\scriptstyle 2} & & \Big\downarrow{\scriptstyle 1} & & \Big\downarrow{\scriptstyle 2} & & \Big\downarrow{\scriptstyle 1} & & \\ Q_\bullet & \cdots & \xrightarrow{4} & \mathbb{Z}_{12} & \xrightarrow{3} & \mathbb{Z}_{12} & \xrightarrow{4} & \mathbb{Z}_{12} & \xrightarrow{3} & \mathbb{Z}_{12} & \longrightarrow & 0 \end{array}$$

Compute induced map $\mathrm{Ext}_{\mathbb{Z}_{12}}(-,\mathbb{Z}_{12})$. Note



$$
\begin{array}{ccccc}
\mathrm{Ext}^i_{\mathbb{Z}_{12}}(\rho,\mathbb{Z}_{12}): & & \mathrm{Ext}^i_{\mathbb{Z}_{12}}(\mathbb{Z}_3,\mathbb{Z}_{12}) & \longrightarrow & \mathrm{Ext}^i_{\mathbb{Z}_{12}}(\mathbb{Z}_6,\mathbb{Z}_{12}) \\
\big\downarrow = & & \big\downarrow = & & \big\downarrow = \\
\mathrm{H}_{-i}(\mathrm{Hom}_{\mathbb{Z}_{12}}(F_\bullet,\mathbb{Z}_{12})): & & \mathrm{H}_i(\mathrm{Hom}_{\mathbb{Z}_{12}}(Q_\bullet,\mathbb{Z}_{12})) & \longrightarrow & \mathrm{H}_{-i}(\mathrm{Hom}_{\mathbb{Z}_{12}}(\rho,\mathbb{Z}_{12})) \\
\big\downarrow = & & \big\downarrow = & & \big\downarrow = \\
\mathrm{H}_{-i}(F^*_\bullet) & & \mathrm{H}_{-i}(Q^*_\bullet) & & \mathrm{H}_{-i}(P^*_\bullet)
\end{array}
$$

$\mathrm{H}_{-i}(\mathrm{Hom}_{\mathbb{Z}_{12}}(F_\bullet,\mathbb{Z}_{12})(\overline{\phi}) = \overline{\phi \circ F_i}$, where

$$
\begin{array}{ccc}
Q_i & \xrightarrow{\phi} & \mathbb{Z}_{12} \\
{\scriptstyle F_i}\big\uparrow & & \\
P_i & &
\end{array}
$$

Note

$$\begin{array}{lccccccccc}
P_\bullet^* & 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{6} & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{2} & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{6} & \cdots \\
& & & {\scriptstyle 1}\uparrow & & {\scriptstyle 2}\uparrow & & {\scriptstyle 1}\uparrow & & \\
Q_\bullet^* & 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{3} & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{4} & \mathrm{Hom}_{\mathbb{Z}_{12}}(\mathbb{Z}_{12},\mathbb{Z}_{12}) & \xrightarrow{3} & \cdots
\end{array}$$

which is

$$\begin{array}{lccccccccc}
P_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_{12} & \xrightarrow{6} & \mathbb{Z}_{12} & \xrightarrow{2} & \mathbb{Z}_{12} & \xrightarrow{6} & \cdots \\
& & & {\scriptstyle 1}\uparrow & & {\scriptstyle 2}\uparrow & & {\scriptstyle 1}\uparrow & & \\
Q_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_{12} & \xrightarrow{3} & \mathbb{Z}_{12} & \xrightarrow{4} & \mathbb{Z}_{12} & \xrightarrow{3} & \cdots
\end{array}$$

Since $6 \cdot 2 = 12$ and $3 \cdot 4 = 12$, we have $\mathrm{H}_{-i}(P_\bullet^*) = 0 = \mathrm{H}_{-i}(Q_\bullet^*)$ for $i \geqslant 1$. So $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_6,\mathbb{Z}_{12}) = 0 = \mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_{12})$ for $i \in\geqslant 1$. Hence $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\rho,\mathbb{Z}_{12}) = 0$ for $i \geqslant 1$. Claim. $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_2) = 0 = \mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_4)$ for $i \geqslant 1$ since $(3,2) = 1 = (3,4)$. Since $2 \cdot \mathbb{Z} = 0 = 3\mathbb{Z}_3$, we have $2 \cdot \mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_2) = 0 = 3 \cdot \mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_2)$. Since $1 = 3 - 2$ also kills $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_2)$, we have $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_2) = 0$. Similarly, we have $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\mathbb{Z}_3,\mathbb{Z}_4) = 0$.

Example 9.7. Let $R = \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$, $M = \mathbb{Z}_6$ and $M' = \mathbb{Z}_3$.

$$\begin{array}{lcccccccccccc}
P_\bullet^+ \cdots & \xrightarrow{2} & \mathbb{Z}_6 & \xrightarrow{6=0} & \mathbb{Z}_6 & \xrightarrow{2} & \mathbb{Z}_6 & \xrightarrow{6=0} & \mathbb{Z}_6 & \xrightarrow{\tau} & \mathbb{Z}_6 & \longrightarrow & 0 \\
& & \downarrow{\scriptstyle 2} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 2} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \rho} & & \\
Q_\bullet^+ \cdots & \xrightarrow{4} & \mathbb{Z}_6 & \xrightarrow{3} & \mathbb{Z}_6 & \xrightarrow{4} & \mathbb{Z}_6 & \xrightarrow{3} & \mathbb{Z}_6 & \xrightarrow{\pi} & \mathbb{Z}_3 & \longrightarrow & 0
\end{array}$$

Similarly,

$$\begin{array}{lccccccccc}
P_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_6 & \xrightarrow{6=0} & \mathbb{Z}_6 & \xrightarrow{2} & \mathbb{Z}_6 & \xrightarrow{6=0} & \cdots \\
& & & {\scriptstyle 1}\uparrow & & {\scriptstyle 2}\uparrow & & {\scriptstyle 1}\uparrow & & \\
Q_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_6 & \xrightarrow{3} & \mathbb{Z}_6 & \xrightarrow{4} & \mathbb{Z}_6 & \xrightarrow{3} & \cdots
\end{array}$$

Note $\mathrm{H}_0(P_\bullet^*) = \frac{\mathrm{Ker}(\mathbb{Z}_6 \xrightarrow{0} \mathbb{Z}_6)}{\mathrm{Im}(0 \to \mathbb{Z}_6)} = \frac{\mathbb{Z}_6}{0} \cong \mathbb{Z}_6$, $\mathrm{H}_0(Q_\bullet^*) = \frac{\mathrm{Ker}(\mathbb{Z}_6 \xrightarrow{3} \mathbb{Z}_6)}{\mathrm{Im}(0 \to \mathbb{Z}_6)} \cong \frac{2 \cdot \mathbb{Z}_6}{0} \cong 2 \cdot \mathbb{Z}_6 \cong \mathbb{Z}_3$. Then

$$\begin{array}{ccc}
\mathrm{H}_0(P_\bullet^*) & \xrightarrow{\cong} & \mathbb{Z}_6 \\
{\scriptstyle \cdot 1}\uparrow & & {\scriptstyle \subseteq}\uparrow \\
\mathrm{H}_0(Q_\bullet^*) & \xrightarrow{\cong} & 2\mathbb{Z}_6
\end{array}$$

So $\mathrm{Ext}_{\mathbb{Z}_{12}}^0(\rho,\mathbb{Z}_{12}) = \mathrm{H}_0(F_\bullet^*) = \mathrm{H}_0(\mathrm{Hom}_{\mathbb{Z}_{12}}(F_\bullet,\mathbb{Z}_6)) : \mathrm{H}_0(Q_\bullet^*) \to \mathrm{H}_0(P_\bullet^*)$ is non-zero 1-1 but not onto. Note $\mathrm{H}_{-1}(P_\bullet^*) = \frac{\mathrm{Ker}(\mathbb{Z}_6 \xrightarrow{2} \mathbb{Z}_6)}{\mathrm{Im}(\mathbb{Z}_6 \xrightarrow{0} \mathbb{Z}_6)} = \frac{3\mathbb{Z}_6}{0}3 \cong \mathbb{Z}_6 \cong \mathbb{Z}_2$ and $\mathrm{H}_{-1}(Q_\bullet^*) = \frac{\mathrm{Ker}(\mathbb{Z}_6 \xrightarrow{4=-2} \mathbb{Z}_6)}{\mathrm{Im}(\mathbb{Z}_6 \xrightarrow{3} \mathbb{Z}_6)} \cong \frac{3 \cdot \mathbb{Z}_6}{3 \cdot \mathbb{Z}_6} \cong 0$. So $\mathrm{Ext}_{\mathbb{Z}_{12}}^1(\rho,\mathbb{Z}_6) = \mathrm{H}_{-1}(F_\bullet^*) = 0$. Periodicity implies $\mathrm{Ext}_R^{2k+1}(\rho,\mathbb{Z}_6) = 0$ for $k \geqslant 1$. Note $\mathrm{H}_{-1}(Q_\bullet^*) = \frac{\mathrm{Ker}(\mathbb{Z}_6 \xrightarrow{3} \mathbb{Z}_6)}{\mathrm{Im}(\mathbb{Z}_6 \xrightarrow{4=-2} \mathbb{Z}_6)} \cong \frac{2 \cdot \mathbb{Z}_6}{2 \cdot \mathbb{Z}_6} \cong 0$. So $\mathrm{Ext}_{\mathbb{Z}_{12}}^2(\rho,\mathbb{Z}_6) = \mathrm{H}_{-2}(F_\bullet^*) = 0$. Periodicity implies $\mathrm{Ext}_{\mathbb{Z}_{12}}^{2k}(\rho,\mathbb{Z}_6) = 0$ for $k \in \mathbb{N}$. Thus, $\mathrm{Ext}_{\mathbb{Z}_{12}}^i(\rho,\mathbb{Z}_6) = 0$ for $i \geqslant 1$.

Example 9.8. Let $R = \mathbb{Z}/12\mathbb{Z} = \mathbb{Z}_{12}$, $M = \mathbb{Z}_3$ and $M' = \mathbb{Z}_3$.

$$
\begin{array}{lcccccccccccc}
P_\bullet^+ \cdots & \xrightarrow{2=-1} & \mathbb{Z}_3 & \xrightarrow{6=0} & \mathbb{Z}_3 & \xrightarrow{2=-1} & \mathbb{Z}_3 & \xrightarrow{6=0} & \mathbb{Z}_3 & \xrightarrow{\tau} & \mathbb{Z}_3 & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle 2=-1} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle 2=-1} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \rho} & & \\
Q_\bullet^+ \cdots & \xrightarrow{4=1} & \mathbb{Z}_3 & \xrightarrow{3=0} & \mathbb{Z}_3 & \xrightarrow{4=1} & \mathbb{Z}_3 & \xrightarrow{3=0} & \mathbb{Z}_3 & \xrightarrow{\pi} & \mathbb{Z}_3 & \longrightarrow & 0
\end{array}
$$

Similarly,

$$
\begin{array}{lccccccccc}
P_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_3 & \xrightarrow{6=0} & \mathbb{Z}_3 & \xrightarrow{2=-1} & \mathbb{Z}_3 & \xrightarrow{6=0} & \cdots \\
 & & & {\scriptstyle 1}\uparrow & & {\scriptstyle 2=-1}\uparrow & & {\scriptstyle 1}\uparrow & & \\
Q_\bullet^* & 0 & \longrightarrow & \mathbb{Z}_3 & \xrightarrow{3=0} & \mathbb{Z}_3 & \xrightarrow{4=1} & \mathbb{Z}_3 & \xrightarrow{3=0} & \cdots
\end{array}
$$

Similarly, we can show $\operatorname{Ext}^i_{\mathbb{Z}_{12}}(\rho, \mathbb{Z}_3) = 0$ for $i \geqslant 1$.

Chapter 10

Long Exact sequence

Definition 10.1. A short exact sequence of *chain complexes* is a diagram

$$0 \to M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \to 0,$$

where $f_\bullet$ and $g_\bullet$ are chain maps, each row

$$0 \to M'_i \xrightarrow{f_i} M_i \xrightarrow{g_i} M''_i \to 0$$

is exact and each square in the following diagram commutes.

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_i & \xrightarrow{f_i} & M_i & \xrightarrow{g_i} & M''_i & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'_{i-1} & \xrightarrow{f_{i-1}} & M_{i-1} & \xrightarrow{g_{i-1}} & M''_{i-1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Let $m'_i \in M'_i$. Then

$$\begin{array}{ccccc}
 & & m_i & \longmapsto & m''_i \\
 & & \downarrow & & \downarrow \\
m'_{i-1} & \longmapsto & \partial^M_i(m_i) & \longmapsto & 0
\end{array}$$

Theorem 10.2. *Given a S.E.S. of R-cxs* $0 \to M'_\bullet \xrightarrow{f_\bullet} M_\bullet \xrightarrow{g_\bullet} M''_\bullet \to 0$*. For any* $i \in \mathbb{Z}$*, there exists R-module homomorphism* $\eth_i : \mathrm{H}_i(M''_\bullet) \to \mathrm{H}_{i-1}(M'_\bullet)$*, making the following long exact sequence*

$$\cdots \xrightarrow{\eth_{i+1}} \mathrm{H}_i(M'_\bullet) \xrightarrow{\mathrm{H}_i(f_\bullet)} \mathrm{H}_i(M_\bullet) \xrightarrow{\mathrm{H}_i(g_\bullet)} \mathrm{H}_i(M''_\bullet) \xrightarrow{\eth_i} \mathrm{H}_{i-1}(M'_\bullet) \xrightarrow{\mathrm{H}_{i-1}(f_\bullet)} \cdots,$$

with $\eth_i$ *being the "connecting homomorphisms" and* $\eth_i(\overline{m''_i}) = \overline{m'_{i-1}}$.

Proof. (a) Claim. $m'_{i-1} \in \mathrm{Ker}(\partial^{M'}_{i-1})$. Let $m''_i \in \mathrm{Ker}(\partial^{M''}_i) \subseteq M''_i$. Since $m''_i \in \mathrm{Ker}(\partial^{M''}_i)$, we have $\partial^{M''}_i(m''_i) = 0$. Since g_i is onto, there exists $m_i \in M_i$ such that $g_i(m_i) = m''_i$. Let $m_{i-1} := \partial^M_i(m_i)$. Since $\mathrm{Ker}(g_{i-1}) = \mathrm{Im}(f_{i-1})$, there exists $m'_{i-1} \in M'_{i-1}$ such that $f_{i-1}(m'_{i-1}) = m_{i-1}$. Since the columns are chain complexes, $\partial^M_{i-1}(m_{i-1}) = 0$. Let $\partial^{M'}_{i-1}(m'_{i-1}) =: *$. Since the diagram commutes $f_{i-2}(*) = 0$. Since f_{i-2} is 1-1, $* = 0$. So $m'_{i-1} \in \mathrm{Ker}(\partial^M_{i-1})$. Hence $\overline{m'_{i-1}}$ makes sense as an element of $\mathrm{H}_{i-1}(M\bullet') = \frac{\mathrm{Ker}(\partial^{M'}_{i-1})}{\mathrm{Im}(\partial^{M'}_i)}$.

(b) Claim. $\eth_i$ is well-defined, i.e., independent of choices pf m_i and $\overline{m'_{i-1}}$. Let $m''_i, n''_i \in \mathrm{Ker}(\eth^{M'}_i)$ such that $\overline{m''_i} = \overline{n''_i}$ in $\mathrm{H}_i(M''_\bullet)$. NTS: $\overline{m'_{i-1}} = \overline{n'_{i-1}}$ in $\mathrm{H}_i(M'_\bullet)$, i.e., $\overline{m'_{i-1}} - \overline{n'_{i-1}} = \overline{m'_{i-1} - n'_{i-1}} = \bar{0} = 0$, i.e., $m'_{i-1} - n'_{i-1} \in \mathrm{Im}(\partial^{M'}_{i+1})$. Note $m''_i - n''_i \in \mathrm{Im}(\partial^{M''}_{i+1})$. Then there exists $x''_{i+1} \in M''_{i+1}$ such that $\partial^{M''}_{i+1}(x''_{i+1}) = m''_i - n''_i$. Since g_i is onto, there exists $x_i \in M_i$ such that $g_i(x_i) = m''_i - n''_i = g_i(m_i) - g_i(n_i) = g_i(m_i - n_i)$. Then $(m_i - n_i) - x_i \in \mathrm{Ker}(g_i) = \mathrm{Im}(f_i)$. So there exists $y'_i \in M'_i$ such that $f'_i(y'_i) = m_i - n_i - x_i$. Since diagrams on the left side commute and

$$
\begin{array}{ccc}
x_{i+1} & \longmapsto & x''_{i+1} \\
\downarrow & & \downarrow \\
x_i & \longmapsto & m''_i - n''_i \\
\downarrow & & \\
0 & &
\end{array}
$$

we have $f_{i-1}(\partial^{M'}_i(y'_i)) = \partial^M_i(f_i(y'_i)) = \partial^M_i(m_i - n_i - x_i) = m_{i-1} - n_{i-1} - 0 = f_{i-1}(m'_{i-1} - n'_{i-1})$. Since f_{i-1} is 1-1, $m'_{i-1} - n'_{i-1} = \partial^{M'}_i(y'_i) \in \mathrm{Im}(\partial^{M'}_i)$.

(c) Claim. $\eth_i$ is an R-module homomorphism. Let $r \in R$ and $\overline{m''_i}$, $\overline{p''_i} \in \mathrm{H}_i(M'')$. Use the symbol from part (a). Then $g_i(m_i + p_i) = g_i(m_i) + g_i(p_i) = m''_i + p'_i$. $g_i(rm_i) = r \cdot g_i(m_i) = rm''_i$. So $\eth_i(\overline{m''_i} + \overline{p''_i}) = \eth_i(\overline{m''_i + p''_i}) = \overline{m'_{i-1} + p'_{i-1}} = \overline{m'_{i-1}} + \overline{p'_{i-1}} = \eth_i(\overline{m''_i}) + \eth_i(\overline{p''_i})$ and $\eth_i(r\overline{m''_i}) = \eth_i(\overline{rm''_i}) = \overline{rm'_{i-1}} = r\overline{m'_{i-1}} = r\eth_i(\overline{m''_i})$.

(d) Claim. $\mathrm{H}_i(g_\bullet) \circ \mathrm{H}_i(f_\bullet) = 0$. $\mathrm{H}_i(g_\bullet)(\mathrm{H}_i(f_\bullet)(\overline{m'_i})) = \mathrm{H}_i(g_\bullet)(\overline{f_i(m''_i)}) = \overline{g_i(f_i(m''_i))} = \overline{g_i \circ f_i(m''_i)} = \bar{0}$. Quick proof. Since $\mathrm{H}_i(g_\bullet \circ f_\bullet) = g_i \circ f_i = 0$, we have $\mathrm{H}_i(g_\bullet) \circ \mathrm{H}_i(f_\bullet) = \mathrm{H}_i(g_\bullet \circ f_\bullet) = 0$.

(e) Claim. $\eth_i \circ \mathrm{H}_i(g_\bullet) = 0$. Let $\overline{m_i} \in \mathrm{H}_i(M_\bullet)$. Since f_{i-1} is 1-1,

$$
\begin{array}{ccc}
 & m_i & \longmapsto \ m''_i \\
 & \downarrow & \\
0'_{i-1} = 0 \longmapsto & 0 &
\end{array}
$$

So $\eth_i(\mathrm{H}_i(g_\bullet)(\overline{m_i})) = \eth_i(\overline{g_i(m_i)}) = \eth_i(\overline{m''_i}) = \overline{0'_{i-1}} = 0$.

(f) Claim. $\mathrm{H}_{i-1}(f_\bullet) \circ \eth_i = 0$. Since $\partial^M_i \in \mathrm{Im}(\partial^M_i)$, we have $\mathrm{H}_{i-1}(f_\bullet)(\eth_i(\overline{m''_i})) = \mathrm{H}_{i-1}(f_\bullet)(\overline{m'_{i-1}}) = \overline{f_{i-1}(m'_{i-1})} = \overline{m_{i-1}} = \overline{\partial^M_i(m_i)} = 0$.

(g) Claim. $\mathrm{Ker}(\mathrm{H}_i(g_\bullet)) \subseteq \mathrm{Im}(\mathrm{H}_i(f_\bullet))$. Let

$$\begin{array}{ccccc} \mathrm{H}_i(M'_\bullet) & \xrightarrow{\mathrm{H}_i(f_\bullet)} & \mathrm{H}_i(M_\bullet) & \xrightarrow{\mathrm{H}_i(g_\bullet)} & \mathrm{H}_i(M''_\bullet) \\ & & \overline{m_i} \mapsto 0 & & \end{array}$$

Then $\overline{m_i} \in \mathrm{Ker}(\mathrm{H}_i(g_\bullet)) \subseteq \mathrm{H}_i(M_\bullet)$. So $0 = \mathrm{H}_i(g_\bullet)(\overline{m_i}) = \overline{g_i(m_i)}$ in $\mathrm{H}_i(M''_\bullet)$. Hence $m''_i := g_i(m_i) \in \mathrm{Im}(\partial^{M''}_{i+1})$. Then there exists $m''_{i+1} \in M''_{i+1}$ such that $\partial^{M''}_{i+1}(m''_{i+1}) = m''_i$. Since g_{i+1} is onto, there exists $z_{i+1} \in M_{i+1}$ such that $g_{i+1}(z_{i+1}) = m''_{i+1}$. Then $z_i := \partial^M_{i+1}(z_{i+1}) \in \mathrm{Im}(\partial^M_{i+1})$. We have

$$\begin{array}{ccc} z_{i+1} & \longmapsto & m''_{i+1} \\ \downarrow & & \downarrow \\ z_i & \longmapsto & m''_i \end{array}$$

Let $m'_i \in M'_i$ such that $f_i(m'_i) = m_i - z_i$. Then $\mathrm{H}_i(f_\bullet)(\overline{m'_i}) = \overline{f_i(m'_i)} = \overline{m_i - z_i} = \overline{m_i} - \overline{z_i} = \overline{m_i} - 0 = \overline{m_i}$ in $\mathrm{H}_i(M_\bullet)$. So $\overline{m_i} \in \mathrm{Im}(\mathrm{H}_i(f_\bullet)$.

(h) Claim. $\mathrm{Ker}(\eth_i) \subseteq \mathrm{Im}(\mathrm{H}_i(g_\bullet))$. Let $\overline{m''_i} \in \mathrm{Ker}(\eth_i)$. Then $m''_i \in \mathrm{Ker}(\partial^{M''}_i)$ such that $\overline{m'_{i-1}} := \eth_i(\overline{m''_i}) = 0$ in $\mathrm{H}_{i-1}(M'_\bullet)$. So $m'_{i-1} \in \mathrm{Im}(\partial^{M'}_i)$. Then there exists $x'_1 \in M'_i$ such that $\partial^{M'}_i(x'_i) = m'_{i-1}$. We have

$$\begin{array}{ccccc} x'_i & & m_i & \longmapsto & m''_i \\ \downarrow & & \downarrow & & \downarrow \\ m'_{i-1} & \longmapsto & m_{i-1} & \longmapsto & 0 \end{array}$$

Let $x_i := f_i(x'_i)$. Then $\partial^M_i(m_i - x_i) = \partial^M_i(m_i) - \partial^M_i(x_i) = \partial^M_i(m_i) - \partial^M_i(f_i(x'_i)) = \partial^M_i(m_i) - f_{i-1}(\partial^{M'}_i(x'_i)) = \partial^M_i(m_i) - f_{i-1}(m'_{i-1}) = \partial^M_i(m_i) - \partial^M_i(m_i) = 0$. So $m_i - x_i \in \mathrm{Ker}(\partial^M_i)$. Hence $\overline{m_i - x_i} \in \mathrm{H}_i(M_\bullet)$. Also, since $g_i(m_i - x_i) = g_i(m_i) - g_i(x_i) = m''_i - g_i(f_i(x'_i)) = m''_i$, we have $\mathrm{H}_i(g_\bullet)(\overline{m_i - x_i}) = \overline{g_i(m_i - x_i)} = \overline{m''_i}$. So $\overline{m''_i} \in \mathrm{Im}(\mathrm{H}_i(g_\bullet))$.

(i) Claim. $\mathrm{Ker}(\mathrm{H}_{i-1}(f_\bullet)) \subseteq \mathrm{Im}(\eth_i)$. Let $\overline{m'_{i-1}} \in \mathrm{Ker}(\mathrm{H}_{i-1}(f_\bullet)) \subseteq \mathrm{H}_{i-1}(M'_\bullet)$. Then $0 = \mathrm{H}_{i-1}(f_\bullet)(\overline{m'_{i-1}}) = \overline{f_{i-1}(m'_{i-1})}$ in $\mathrm{H}_{i-1}(M_\bullet)$. So $f_{i-1}(m'_{i-1}) \in \mathrm{Im}(\partial^M_i)$. Let $m_{i-1} := f_{i-1}(m'_{i-1})$. Then there exists $m_i \in M_i$ such that $\partial^M_i(m_i) = m_{i-1}$. Also note $g_{i-1}(m_{i-1}) = 0$. Let $m''_i := g_i(m_i)$. We have

$$\begin{array}{ccccc} & & m_i & \longmapsto & m''_i \\ & & \downarrow & & \downarrow \\ m'_{i-1} & \longmapsto & m_{i-1} & \longmapsto & 0 \end{array}$$

Since the diagram commutes, $\partial^{M''}_i(m''_i) = 0$. So $m''_i \in \mathrm{Ker}(\partial^{M''}_i)$. Then $\overline{m''_i} \in \mathrm{H}_i(M'_\bullet)$ satisfying $\eth_i(\overline{m''_i}) = \overline{m'_{i-1}}$. So $\overline{m'_{i-1}} \in \mathrm{Im}(\eth_i)$. □

Corollary 10.3 (Snake Lemma)**.** Consider a commutative diagram with exact rows.

$$\begin{CD}
0 @>>> M_1' @>{f_1}>> M_1 @>{g_1}>> M_1'' @>>> 0\\
@. @VV{\partial_1'}V @VV{\partial_1}V @VV{\partial_1''}V @.\\
0 @>>> M_0' @>{f_0}>> M_0 @>{g_0}>> M_0'' @>>> 0
\end{CD}$$

Then there exists exact sequence

$$0 \longrightarrow \operatorname{Ker}(\partial_1') \longrightarrow \operatorname{Ker}(\partial_1) \longrightarrow \operatorname{Ker}(\partial_1'') \longrightarrow \operatorname{Coker}(\partial_1') \longrightarrow \operatorname{Coker}(\partial_1) \longrightarrow \operatorname{Coker}(\partial_1'') \longrightarrow 0$$

Proof. The given commutative diagram extends to the following short exact sequence of chain maps: $0 \to M_\bullet' \xrightarrow{F_\bullet} M_\bullet \xrightarrow{G_\bullet} M_\bullet'' \to 0$, where

$$\begin{CD}
@. 0 @. 0 @. 0 @.\\
@. @VVV @VVV @VVV @.\\
0 @>>> M_1' @>{f_1}>> M_1 @>{g_1}>> M_1'' @>>> 0\\
@. @VV{\partial_1'}V @VV{\partial_1}V @VV{\partial_1''}V @.\\
0 @>>> M_0' @>{f_0}>> M_0 @>{g_0}>> M_0'' @>>> 0\\
@. @VVV @VVV @VVV @.\\
@. 0 @. 0 @. 0 @.
\end{CD}$$

The long exact sequence is

$$0 \longrightarrow \mathrm{H}_1(M_\bullet') \longrightarrow \mathrm{H}_1(M_\bullet) \longrightarrow \mathrm{H}_1(M_\bullet'') \longrightarrow \mathrm{H}_0(M_\bullet') \longrightarrow \mathrm{H}_0(M_\bullet) \longrightarrow \mathrm{H}_0(M_\bullet'') \longrightarrow 0 \longrightarrow 0$$

The desired exact sequence of kernels and cokernels is precisely the long exact sequence guaranteed by previous theorem. For instance, $\mathrm{H}_1(M_\bullet) = \frac{\operatorname{Ker}(M_1 \xrightarrow{\partial_1} M_0)}{\operatorname{Im}(0 \to M_1)} = \frac{\operatorname{Ker}(\partial_1)}{0} \cong \operatorname{Ker}(\partial_1)$ and $\mathrm{H}_0(M_\bullet) = \frac{\operatorname{Ker}(M_0 \to 0)}{\operatorname{Im}(M_1 \xrightarrow{\partial_1} M_0)} = \frac{M_0}{\operatorname{Im}(\partial_1)} = \operatorname{Coker}(\partial_1)$. ☐

Remark. If ∂_1'' is 1-1, then ∂_1 is 1-1 if and only if ∂_1' is 1-1. In terms of Long exact sequence, if $0 \to \operatorname{Ker}(\partial_1') \to \operatorname{Ker}(\partial_1) \to \operatorname{Ker}(\partial_1'') = 0$, then $\operatorname{Ker}(\partial_1') = 0$ if and only if $\operatorname{Ker}(\partial_1) = 0$. Similarly, if ∂_1' is onto, then ∂_1 is onto if and only if ∂_1'' is onto.

10.1 LES in Ext

Theorem 10.4. *Let L be an R-module and let $0 \to N' \xrightarrow{\alpha} N \xrightarrow{\beta} N'' \to 0$ be a S.E.S. of R-modules. Then there exists L.E.S. associated to $\operatorname{Ext}^i_R(L,-)$.*

$$\begin{array}{l}
0 \longrightarrow \operatorname{Hom}_R(L,N') \longrightarrow \operatorname{Hom}_R(L,N) \longrightarrow \operatorname{Hom}_{\mathrm{R}}(L,N'') \\
\hookrightarrow \operatorname{Ext}^1_R(L,N') \longrightarrow \operatorname{Ext}^1_R(L,N) \longrightarrow \operatorname{Ext}^1_R(L,N'') \\
\hookrightarrow \cdots \longrightarrow \cdots \longrightarrow \operatorname{Ext}^{i-1}_R(L,N'') \\
\hookrightarrow \operatorname{Ext}^i_R(L,N') \longrightarrow \operatorname{Ext}^i_R(L,N) \longrightarrow \operatorname{Ext}^i_R(L,N'') \\
\hookrightarrow \operatorname{Ext}^{i+1}_R(L,N') \longrightarrow \cdots
\end{array}$$

where

$$\operatorname{Ext}^i_R(L,N') \xrightarrow{\operatorname{Ext}^i_R(L,\alpha)} \operatorname{Ext}^i_R(L,N) \xrightarrow{\operatorname{Ext}^i_R(L,\beta)} \operatorname{Ext}^i_R(L,N'').$$

Proof. Let $P_\bullet$ be a projective resolution for L. Then $\operatorname{Hom}_R(P_\bullet,N')$ is an R-cx and so are $\operatorname{Hom}_R(P_\bullet,N)$ and $\operatorname{Hom}_R(P_\bullet,N'')$. Since

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \operatorname{Hom}_R(P_0,N') & \xrightarrow{\alpha^*} & \operatorname{Hom}_R(P_0,N) & \xrightarrow{\beta^*} & \operatorname{Hom}_R(P_0,N'') & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_1^{P*}} & & \downarrow{\scriptstyle \partial_1^{P*}} & & \downarrow{\scriptstyle \partial_1^{P*}} & & \\
0 & \longrightarrow & \operatorname{Hom}_R(P_1,N') & \xrightarrow{\alpha^*} & \operatorname{Hom}_R(P_1,N) & \xrightarrow{\beta^*} & \operatorname{Hom}_R(P_1,N'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & & \\
0 & \longrightarrow & \operatorname{Hom}_R(P_i,N') & \xrightarrow{\alpha^*} & \operatorname{Hom}_R(P_i,N) & \xrightarrow{\beta^*} & \operatorname{Hom}_R(P_i,N'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

have exact rows and commute by associated of composition, we have

$$\operatorname{Hom}_R(P_\bullet,-):\ 0 \to \operatorname{Hom}_R(P_\bullet,N') \to \operatorname{Hom}_R(P_\bullet,N) \to \operatorname{Hom}_R(P_\bullet,N'') \to 0,$$

is a SES of R-cxs. Since the associated LES has this "sneak" shape and $\mathrm{H}_{-i}(\operatorname{Hom}_R(P_\bullet,N') = \operatorname{Ext}^i_R(L,N')$, we have the result. $\square$

Theorem 10.5. *What about* $\operatorname{Ext}^i_R(-,L)$ *LES?*

$$
\begin{array}{l}
0 \longrightarrow \operatorname{Hom}_R(N'',L) \longrightarrow \operatorname{Hom}_R(N,L) \longrightarrow \operatorname{Hom}_R(N',L) \\
\hookrightarrow \operatorname{Ext}^1_R(N'',L) \longrightarrow \operatorname{Ext}^1_R(N,L) \longrightarrow \operatorname{Ext}^1_R(N',L) \\
\hookrightarrow \cdots \longrightarrow \cdots \longrightarrow \operatorname{Ext}^{i-1}_R(N',L) \\
\hookrightarrow \operatorname{Ext}^i_R(N'',L) \longrightarrow \operatorname{Ext}^i_R(N,L) \longrightarrow \operatorname{Ext}^i_R(N',L) \\
\hookrightarrow \operatorname{Ext}^{i+1}_R(N',L) \longrightarrow \cdots
\end{array}
$$

Let $Q''_\bullet, Q_\bullet, Q'_\bullet$ *be a projective resolution of* N'', N, N'*, respectively, then*

$$\operatorname{Ext}^i_R(N'',L) = \operatorname{H}_{-i}(\operatorname{Hom}_R(Q''_\bullet, L)),$$

$$\operatorname{Ext}^i_R(N,L) = \operatorname{H}_{-i}(\operatorname{Hom}_R(Q_\bullet, L)),$$

$$\operatorname{Ext}^i_R(N',L) = \operatorname{H}_{-i}(\operatorname{Hom}_R(Q'_\bullet, L)).$$

Need a S.E.S. of R-cxs

$$0 \to \operatorname{Hom}_R(Q''_\bullet, L) \to \operatorname{Hom}_R(Q_\bullet, L) \to \operatorname{Hom}_R(Q_\bullet, L) \to \operatorname{Hom}_R(Q'_\bullet, L) \to 0.$$

i.e., want a S.E.S of R-cxs $0 \to Q'_\bullet \to Q_\bullet \to Q''_\bullet \to 0$ $(*)$ *such that* $\operatorname{Hom}_R(-,L)$ *is exact. Note if there exists S.E.S of R-cxs (*), then* $\operatorname{Hom}_R(-,L)$ *is automatically exact.*

Proof. The i^{th} row of (*) is $(*_i)_\bullet :\ 0 \to Q'_i \to Q_i \to Q''_i \to 0$. Since Q''_i is projective, this sequence split, then $\operatorname{Hom}_R(*_i, L)$ is split exact, and so exact. Need: given SES $0 \to N' \to N \to N'' \to 0$, construct S.E.S. of projective resolution $0 \to Q'_\bullet \to Q_\bullet \to Q''_\bullet \to 0$. Recall. Lifting lemma can lift α to chain map $Q'_\bullet \xrightarrow{A} Q_\bullet$, and lift β to chain map $Q_\bullet \xrightarrow{B} Q''_\bullet$. Bad news: the sequence $0 \to Q'_\bullet \xrightarrow{A} Q_\bullet \xrightarrow{B} Q''_\bullet \to 0$ will not be exact in general. For remaining L.E.S. in Ext., need the following lemma. □

Lemma 10.6. Given a S.E.S. of R-module $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$, and given projective resolutions $P'_\bullet$ and $P''_\bullet$ for M' and M'', respectively, there exists projective resolution for M and exists S.E.S. of R-cx $0 \to P'_\bullet \xrightarrow{F_\bullet} P_\bullet \xrightarrow{G_\bullet} P''_\bullet \to 0$ such that the following diagram commutes.

$$
\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_1' & \longrightarrow & P_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_0' & \longrightarrow & P_0 & \longrightarrow & P_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Proof. Proved later. □

Example 10.7. Let p be prime and $R = \mathbb{Z}$. Let $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \to 0$ be a S.E.S. of R-module. Then $P'_\bullet = (0 \to \mathbb{Z} \to 0) = P_\bullet$ and $P''_\bullet = (0 \to \mathbb{Z} \xrightarrow{P} \mathbb{Z} \to 0)$. So $0 \to P'_\bullet \to P_\bullet \to P''_\bullet \to 0$ is

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

But the exact rows are not possible. To get horseshoe diagram in this example, use given $P'_\bullet$ and $P''_\bullet$

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot 1} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \cdot p} & & \\
0 & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{Z}^2 & \xrightarrow{(0\ 1)} & \mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \cdot 1} & & \downarrow{\scriptstyle \pi=(p\ 1)} & & \downarrow{\scriptstyle \tau} & & \\
0 & \longrightarrow & \mathbb{Z} & \xrightarrow{\cdot p} & \mathbb{Z} & \xrightarrow{\tau} & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Note

$$\begin{array}{ccc} \vec{e}_2 & \longmapsto & 1 \\ \downarrow & & \downarrow \\ 1 & \longmapsto & \bar{1} \end{array}$$

So π is onto. It is easy to see $\mathrm{Ker}(\pi) = \left\langle \begin{pmatrix} -1 \\ p \end{pmatrix} \right\rangle \subseteq \mathbb{Z}^2$. Note $\mathbb{Z} \xrightarrow{\cong} \mathrm{Ker}(\pi)$ given by $a \mapsto a \begin{pmatrix} -1 \\ p \end{pmatrix}$.

Example 10.8. Let $R = \mathbb{Z}_4$. Let $0 \to \mathbb{Z}_2 \xrightarrow{f=\cdot 2} \mathbb{Z}_4 \xrightarrow{\tau} \mathbb{Z}_2 \to 0$ be S.E.S. of R-module with $f(\bar{0}) = \bar{0}$, $f(\bar{1}) = \bar{2}$ and $\tau(\bar{a}) = \bar{a}$. Consider

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \downarrow{\scriptstyle 2} & & \downarrow & & \downarrow{\scriptstyle 2} & & \\ 0 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 2} & & \downarrow & & \downarrow{\scriptstyle 2} & & \\ 0 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 2} & & \downarrow & & \downarrow{\scriptstyle 2} & & \\ 0 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \tau} & & \downarrow & & \downarrow{\scriptstyle \tau} & & \\ 0 & \longrightarrow & \mathbb{Z}_2 & \xrightarrow{2} & \mathbb{Z}_4 & \xrightarrow{\tau} & \mathbb{Z}_2 & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

But the exact rows are not possible.

Lemma 10.9. Given a diagram of R-mod. homs.

$$\begin{array}{ccccccccc} & & P' & & & & P'' & & \\ & & \downarrow{\scriptstyle \tau'} & & & & \downarrow{\scriptstyle \tau''} & & \\ 0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ & & 0 & & & & 0 & & \end{array}$$

with exact rows and exact columns such that P'' is projective, then there exists R-module homomorphism $P' \oplus P'' \xrightarrow{\tau} M$ making the next diagram commute.

$$
\begin{array}{ccccccccc}
0 & \longrightarrow & P' & \xrightarrow{\begin{pmatrix} 1 \\ 0 \end{pmatrix}} & P' \oplus P'' & \xrightarrow{(0\ 1)} & P'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau''} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Moreover, the middle column is also exact.

Proof. We have

$$
\begin{array}{ccccc}
 & & P'' & & \\
 & \swarrow{\scriptstyle \alpha} & \downarrow{\scriptstyle \tau''} & & \\
M & \xrightarrow{g} & M' & \longrightarrow & 0
\end{array}
$$

with $\alpha = g \circ \tau''$. Define $\tau : P' \oplus P'' \to M$ by $\begin{pmatrix} x' \\ x'' \end{pmatrix} \mapsto f(\tau'(x')) + \alpha(x'')$. So τ is actually $(f \circ \tau',\ \alpha)$. Check τ is an R-module homomorphism. It is easy to verify the diagram commutes. By Sneak lemma, τ' and τ'' surjection implies τ is also surjective. So middle column is exact.

□

Lemma 10.10. Given a S.E.S. of R-module $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ and given projective resolutions $P'_\bullet$ and $P''_\bullet$ for M' and M'', respectively, there exists projective resolution for M and exists S.E.S. of R-cx $0 \to P'_\bullet \xrightarrow{F_\bullet} P_\bullet \xrightarrow{G_\bullet} P''_\bullet \to 0$ such that the following diagram commutes.

$$
\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'_1 & \longrightarrow & P_1 & \longrightarrow & P_1 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P'_0 & \longrightarrow & P_0 & \longrightarrow & P_0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Proof. We have

$$\begin{array}{ccccccccc}
 & & P_0' & & & & P_0'' & & \\
 & & \downarrow{\scriptstyle \tau'} & & & & \downarrow{\scriptstyle \tau''} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
 & & 0 & & & & 0 & &
\end{array}$$

By previous lemma,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_0' & \xrightarrow{F_0} & P_0' \oplus P_0'' & \xrightarrow{G_0} & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau''} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

with $F_0 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $G_0 = (0,\ 1)$. The Snake Lemma shows that the following commutative diagram has exact rows and exact columns.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Ker}(\tau') & \xrightarrow{f_1} & \mathrm{Ker}(\tau) & \xrightarrow{g_1} & \mathrm{Ker}(\tau'') & \longrightarrow & 0 \\
 & & \subseteq\downarrow{\scriptstyle \epsilon_1'} & & \subseteq\downarrow{\scriptstyle \epsilon_1} & & \subseteq\downarrow{\scriptstyle \epsilon_1''} & & \\
0 & \longrightarrow & P_0' & \xrightarrow{F_0} & P_0' \oplus P_0'' & \xrightarrow{G_0} & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau''} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where f_1 is the restriction of F_0 and g_1 is the restriction of G_0. We have

$$\begin{array}{ccccccccc}
 & & P_1' & & & & P_1'' & & \\
 & & \downarrow{\scriptstyle \tau_1'} & & & & \downarrow{\scriptstyle \tau_2''} & & \\
0 & \longrightarrow & \mathrm{Ker}(\tau') & \xrightarrow{f_1} & \mathrm{Ker}(\tau) & \xrightarrow{g_1} & \mathrm{Ker}(\tau'') & \longrightarrow & 0 \\
 & & \downarrow & & & & \downarrow & & \\
 & & 0 & & & & 0 & &
\end{array}$$

where τ_1' is the restriction of $\partial_1^{P'}$ and τ_1'' is the restriction of $\partial_1^{P''}$ and note $\mathrm{Im}(\partial_1^{P'}) = \mathrm{Ker}(\tau')$ and $\mathrm{Im}(\partial_1^{P''}) = \mathrm{Ker}(\tau'')$. By previous lemma,

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_1' & \xrightarrow{F_1} & P_1' \oplus P_1'' & \xrightarrow{G_1} & P_1'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau_1'} & & \downarrow{\scriptstyle \tau_1} & & \downarrow{\scriptstyle \tau_1''} & & \\
0 & \longrightarrow & \mathrm{Ker}(\tau') & \xrightarrow{f} & \mathrm{Ker}(\tau) & \xrightarrow{g} & \mathrm{Ker}(\tau'') & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

with $F_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $G_1 = (0,\ 1)$. Splice these two diagrams above together to obtain the next commutative diagram with exact rows and exact columns

$$\begin{array}{ccccccccc}
0 & \longrightarrow & P_1' & \xrightarrow{F_1} & P_1' \oplus P_1'' & \xrightarrow{G_1} & P_1'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_1^{P'}} & & \downarrow{\scriptstyle \partial_1^{P} = \epsilon_1 \circ \tau_1} & & \downarrow{\scriptstyle \partial_1^{P''}} & & \\
0 & \longrightarrow & P_0' & \xrightarrow{F_0} & P_0' \oplus P_0'' & \xrightarrow{G_0} & P_0'' & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \tau'} & & \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \tau''} & & \\
0 & \longrightarrow & M' & \xrightarrow{f} & M & \xrightarrow{g} & M'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

with $\mathrm{Ker}(\partial_1^{P'}) = \mathrm{Ker}(\tau_1')$. Similarly, for ∂_1^P and $\partial_1^{P''}$. Continue inductively to build the desired diagram one floor per level at a time. The middle column is exact since we build it using our algorithm for constructing projective resolution.

surjective projective; take kernel; surjective projective; take kernel; $\cdots$.

Recall: direct sum of projective modules is projective. □