Algebra

June 18, 2017

1 Commutative Algebra

1.1 ED, PID and UFD (week 9)

We shall consider R to be an integral domain below.

Def 1. A function $N : R \to \mathbb{N}$ with $N(0) = 0$ is called a norm on R.

Def 2. R is called a Euclidean domain if exists a norm N on R satisfying

$$\forall\, a, b \in R,\ \exists\, q, r \in R \text{ s.t. } a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b)$$

Eg 1.1.1.

- $\mathbb{Z}$ is a ED with $N(n) = |n|$.
- $K[x]$ is a ED with $N(f) = \deg f$, $\forall\, f \in K[x]$.

Def 3. A_d is defined to be the ring of integers in the quadratic field $\mathbb{Q}(\sqrt{d})$ with $d \neq 1$ and d is square-free. That is,

$$A_d \triangleq \{\alpha \in \mathbb{Q}(\sqrt{d}) \mid \alpha \text{ is integral over } \mathbb{Z}\}$$

Theorem 1.

- If $d \equiv 1 \pmod 4$, then
$$A_d = \left\{a + b\frac{1+\sqrt{d}}{2} : a, b \in \mathbb{Z}\right\}$$
- Else, $d \equiv 2, 3 \pmod 4$, then
$$A_d = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

Proof. Let $\alpha = p + q\sqrt{d} \in A_d$ for $p, q \in \mathbb{Q}$ with $q \neq 0$. We have $\alpha - p = q\sqrt{d}$, then $(\alpha - p)^2 = q^2 d$ and thus $\alpha^2 - 2p\alpha + (p^2 - q^2 d) = 0$. Let $g(x) \triangleq x^2 - 2px + (p^2 - q^2 d)$. Assume $f(x) \in \mathbb{Z}[x]$ with f monic and $f(\alpha) = 0$, then we could write $f(x) = q(x)g(x) + (ax + b)$. Since α is not rational, $a\alpha + b = 0 \implies a = b = 0$, so $f(x) = q(x)g(x)$ in $\mathbb{Q}[x]$. By gauss lemma, $g(x) \in \mathbb{Z}[x]$, so $2p \in \mathbb{Z}$ and $p^2 - q^2 d \in \mathbb{Z}$.

If $2p$ is even, then $p \in \mathbb{Z}$, and $p^2 - q^2 d \in \mathbb{Z}$ implies q is also an integer since d is square free.

If $2p$ is odd, say $2p = 2m + 1$, then $(2p)^2 \equiv (2m + 1)^2 \equiv 1 \pmod 4$. Also, $4(p^2 - q^2 d) \equiv 0 \pmod 4$, so $4q^2 d \equiv 4p^2 \equiv 1 \pmod 4$. Since d is square free, so $4 \nmid d$, thus q has to be of the form $q = (2n + 1)/2$. Plug in the equation we get $d \equiv 1 \pmod 4$. Thus in this case, p, q are half integer and $d \equiv 1 \pmod 4$. $\square$

Theorem 2. A_d is a ED if $d = 2, 3, 5, -1, -2, -3, -7, -11$. Hence A_d is also PID and UFD for these value.

Proof. Let $N'(p + q\sqrt{d}) = (p + q\sqrt{d})(p - q\sqrt{d}) = p^2 - q^2 d$. Define $N(\alpha) \triangleq |N'(\alpha)|$ which is positive since $p^2 - q^2 d = 0 \iff p = q = 0$. Notice also N is multiplicative.

Now, for $\alpha, \beta \in A_d$, write $\alpha/\beta = x + y\sqrt{d}$. If we could find $\lambda = a + b\sqrt{d}$ such that $|\alpha/\beta - \lambda| < 1$, then $\alpha = \beta\lambda + \gamma$ with $N(\gamma) < N(\beta)$ which proves that A_d is an ED.

- $d = 2, 3, -2, -1$: Choose $a, b \in \mathbb{Z}$ such that $|x - a|, |y - b| \leq 1/2$. Then $N \triangleq N(\alpha/\beta - \lambda) = |(x - a)^2 - (y - b)^2 d|$.

  - If $d = 2, 3$, then $N \le \max(|(x-a)^2|, |(y-b)^2 d|) \le \max(1/4, d/4) < 1$.
  - If $d = -2, -1$, then $N \le |(x-a)^2| + |(y-b)^2 d| \le 1/4 + |d|/4 < 1$.

- $d = 5, -3, -7, -11$: Similarly, but now $d \equiv 1 \pmod 4$, so we could choose $\lambda = a + b(1 + \sqrt{d})/2 = (a + b/2) + b/2\sqrt{d}$. Thus let b be the one such that $|2y - b| \le 1/2$, and then choose a so that $x - a - b/2 \le 1/2$. We have $N(\alpha/\beta - \lambda) = |(x-a-b/2)^2 - d(y-b/2)^2| \le 1/4 + d/16 < 1$.

$\square$

Eg 1.1.2. A_{-5} is not a ED.

Proof. Consider $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Notice that $1 + \sqrt{-5}$ is irreducible, since if $1 + \sqrt{-5} = \alpha\beta$, then $6 = N(1 + \sqrt{-5}) = N(\alpha)N(\beta)$. But this implies $a^2 + 5b^2 = 2$ or 3 which has no integer solution. Also $1 + \sqrt{-5} \nmid 2, 3$. Since if $(1 + \sqrt{-5})\alpha = 2$, then $N(1 + \sqrt{-5})N(\alpha) = N(2) = 4$, but $N(1 + \sqrt{-5}) = 6$. Similarly $1 + \sqrt{-5} \nmid 3$. So A_{-5} is not an UFD thus not an ED. $\square$

1.1.1 A_{-1} and A_{-3}

Def 4. If p is odd and $a \not\equiv 0 \pmod p$, then

- If $x^2 \equiv a \pmod p$ is solvable, then define $\left(\frac{a}{p}\right) = 1$.
- Else $x^2 \equiv a \pmod p$ is not solvable and define $\left(\frac{a}{p}\right) = -1$.

Prop 1.1.1.

- $a \equiv b \pmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- $\left(\frac{a}{p}\right) = a^{(p-1)/2}$:

  Proof. Consider the sequence:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & (\mathbb{F}_p^\times)^2 & \longrightarrow & \mathbb{F}_p^\times & \xrightarrow{\varphi} & \{\pm 1\} & \longrightarrow & 1 \\ & & y^2 & \longmapsto & y^2 = x & \longmapsto & (-1)^{(p-1)/2} & \longmapsto & 1 \end{array}$$

  which is exact since $y^2 \mapsto y^2 \mapsto y^{2(p-1)/2} \equiv 1$. And since $\mathbb{F}_p^\times$ is cyclic with even elements, $\left[\mathbb{F}_p^\times : (\mathbb{F}_p^\times)^2\right] = 2$, and $(\mathbb{F}_p^\times)^2 = \ker\varphi$. $\square$

- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
- Let $t_k \equiv ka \pmod p$ with $0 \le t_k < p$, for $1 \le k \le (p-1)/2$. Assume that $n = \#\{t_i \mid t_i > p/2\}$, then $\left(\frac{a}{p}\right) = (-1)^n$.

  Proof. Define

$$|t_i| = \begin{cases} t_j & \text{If } 1 \le t_j < p/2 \quad (t_j \equiv |t_j|) \\ p - t_j & \text{If } p/2 < t_j < p \quad (t_j \equiv -|t_j|) \end{cases}$$

  Notice that $|t_i|$ takes value between 1 and $(p-1)/2$, and $|ra| \equiv |sa| \pmod p \implies ra \equiv \pm sa \pmod p \implies r \equiv \pm s \pmod p$ since $\gcd(a, p) = 1$. So $|t_k|$ would have distinct value for $1 \le k \le (p-1)/2$. Thus

$$\prod t_k \equiv \frac{p-1}{2}! a^{(p-1)/2} \equiv (-1)^n \frac{p-1}{2}! \implies a^{(p-1)/2} \equiv (-1)^n$$

$\square$

- If p, q are odd primes, then we have:

$$\left(\frac{q}{p}\right) = (-1)^{\left(\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor\right)}$$

Proof. Write $kq = g_k p + t_k$ with $0 \le t_k < p$ consistent with the previous definition. Then we have $\lfloor kq/p \rfloor = g_k$, and

$$\begin{array}{lll} \text{if } |t_k| = t_k & \rightsquigarrow qk = g_k p + |t_k| & \rightsquigarrow k \equiv g_k + |t_k| \pmod 2 \\ \text{if } |t_k| = p - t_k & \rightsquigarrow qk = (g_k+1)p - |t_k| & \rightsquigarrow k \equiv g_k + 1 + |t_k| \pmod 2 \end{array}$$

So

$$\sum_{i=1}^{(p-1)/2} k \equiv n + \sum_{i=1}^{(p-1)/2} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{k=1}^{(p-1)/2} |t_k| \pmod 2$$

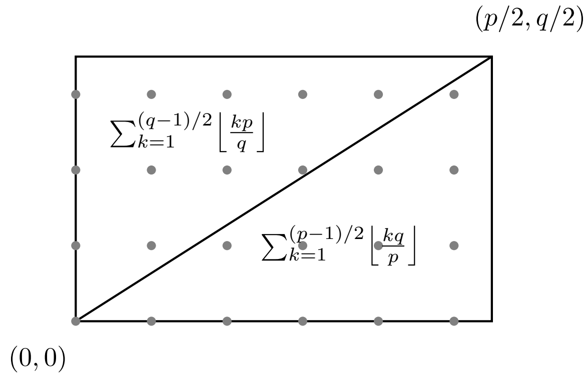
As in the previous proof, $\sum k = \sum |t_k|$, so $n \equiv \sum \lfloor qk/p \rfloor \pmod 2$, which proves the statement. ☐

- $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

By above,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\sum_{k=1}^{(p-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor\right)} (-1)^{\left(\sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor\right)}$$

Which is the number of integer points in the rectangle:



And we know that there are $\frac{p-1}{2}\frac{q-1}{2}$ points in the rectangle.

Prop 1.1.2.

- α is a unit $\iff N(\alpha) = 1$.

Proof. "$\Rightarrow$": If $\alpha\beta = 1$, $N(\alpha)N(\beta) = 1$ so $N(\alpha) = 1$.

"$\Leftarrow$": Immediately by $\alpha\bar{\alpha} = N(\alpha) = 1$. ☐

- If α is a prime in A_d, then $N(\alpha) = p$ or p^2 for some prime integer p. Also $N(\alpha) = p^2 \implies \alpha \sim p$.

Proof. $\alpha\bar{\alpha} = N(\alpha) = p_1 \cdots p_n$ where p_i are primes in $\mathbb{Z}$. Continue using the fact that "If α is a prime and $\alpha \mid xy$, then $\alpha \mid x$ or $\alpha \mid y$", we will get $\alpha \mid p_i$ for an i. Say $\alpha\beta = p_i$, then $\bar{\alpha}\bar{\beta} = \bar{p}_i = p_i$, so $N(\alpha)N(\beta) = p_i^2$ which means that $N(\alpha) = p_i$ or p_i^2. Also, if $N(\alpha) = p_i^2$, then $N(\beta) = 1 \implies \beta$ is a unit . $\square$

By the proposition above we identify the unit in A_{-1}, A_{-3}.

- A_{-1}: $\pm 1, \pm \mathrm{i}$.
- A_{-3}: $\pm 1, \pm\omega, \pm\omega^2$.

Now, notice that $2 = (1+\sqrt{-1})(1-\sqrt{-1})$, $3 = (1-\omega)(1-\omega^2)$, so $2, 3$ are not prime in A_{-1}, A_{-3} respectively.

Let p be a prime in $\mathbb{Z}$.

- In A_{-1}:

$$
\begin{aligned}
& p \text{ is a prime in } \mathbb{Z}[\sqrt{-1}] \\
\iff & \langle p \rangle \text{ is maximal ideal} \\
\iff & \frac{\mathbb{Z}[\sqrt{-1}]}{\langle p \rangle} \cong \frac{\mathbb{Z}[x]}{\langle p, x^2+1 \rangle} \cong \frac{\mathbb{Z}[x]/\langle p \rangle}{\langle p, x^2+1 \rangle/\langle p \rangle} \cong \frac{\mathbb{F}_p[x]}{\langle x^2+1 \rangle} \text{ is a field} \\
\iff & x^2+1 \text{ irreducible in } \mathbb{F}_p[x] \\
\iff & x^2 \equiv -1 \pmod p \text{ is not solvable} \\
\iff & \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} \neq 1 \\
\iff & p \not\equiv 1 \pmod 4
\end{aligned}
$$

  So p is **not** a prime in $A_{-1} \iff p \equiv 1 \pmod 4$.

- In A_{-3}: If a prime $p \neq 3$ in $\mathbb{Z}$ is not a prime in $\mathbb{Z}[\omega]$, then it has a nontrivial factor $\alpha \mid p$. But $N(p) = p^2$, so we must have $N(\alpha) = p$, i.e. $\alpha\bar{\alpha} = p$. Let $\alpha = a + b\omega$, then $p = \alpha\bar{\alpha} = a^2 + b^2 - ab \implies 4p = (2a-b)^2 + 3b^2$, so $p \equiv (2a-b)^2 \equiv 1 \pmod 3$. ($p \not\equiv 0$ since $p \neq 3$)

  Conversely, if $p \equiv 1 \pmod 3$, then

$$
\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1
$$

  So exists $a \in \mathbb{Z}$ such that $a^2 \equiv -3 \pmod p$, say $pb = a^2 + 3 = (a+\sqrt{-3})(a-\sqrt{-3}) = (a+1+2\omega)(a-1-2\omega)$.

  If p is a prime in $\mathbb{Z}[\omega]$, then $p \mid (a+1+2\omega)$ or $p \mod (a-1-2\omega)$, which implies that $p \mid 2$ (since $p \in \mathbb{Z}$, $p \mid a + b\omega \implies p \mid a, p \mid b$), which leads to a contradiction, thus p is not a prime.

  Hence $p \neq 3$ is not a prime in $A_{-3} \iff p \equiv 1 \pmod 3$.

1.2 Primary decomposition

Def 5.

- The radical of an ideal I is defined by $\sqrt{I} = \{a \in R \mid a^n \in I \text{ for some } n \in \mathbb{N}\}$.
- I is radical if $\sqrt{I} = I$.

Def 6. The **nilradical** is defined as $\sqrt{\langle 0\rangle} \triangleq \{a \in R \mid a^n = 0 \text{ for some } n \in \mathbb{N}\}$. Elements in it are called nilpotent.

Prop 1.2.1. $\sqrt{\langle 0\rangle} = \bigcap_{P \in \operatorname{Spec} R} P$, where $\operatorname{Spec} R$ is the set of prime ideals in R.

Proof. "$\subset$": Notice that $a^n = 0 \in P$ for any prime ideal P. By the definition of prime ideal, either $a \in P$ or $a^{n-1} \in P$. No matter which, eventually we would get $a \in P$.

"$\supset$": Let $\mathcal{S} \triangleq \{I : \text{ ideal in } R \,|\, a^n \notin I, \forall\, n \in \mathbb{N}\}$. By the routine argument of Zorn's lemma, exists maximal element Q in $\mathcal{S}$. We claim that Q is a prime ideal.

For each $x, y \notin Q$, we have $Q + Rx \supsetneq Q$ and $Q + Ry \supsetneq Q$. By the maximality of Q, these two ideals are not in $\mathcal{S}$. So exists n, m such that $a^n \in Q + Rx$, $a^m \in Q + Ry$ which implies $a^{n+m} \in Q + Rxy$, so $Q + Rxy \notin \mathcal{S}$, thus $xy \notin Q$, hence Q is prime. □

Coro 1.2.1.

$$\sqrt{I} = \bigcap_{\substack{P \supset I \\ P \in \operatorname{Spec} R}} P$$

Proof. Notice that $\operatorname{Spec} R/I = \{P \in \operatorname{Spec} R \mid R \subset I\}$. By the proposition above,

$$\sqrt{\langle \bar{0}\rangle} = \bigcap_{\bar{P} \in \operatorname{Spec} R/I} \bar{P} \implies \sqrt{I} = \bigcap_{\substack{P \supset I \\ P \in \operatorname{Spec} R}} P$$

□

Def 7. An ideal q of R is called primary if $q \neq R$ and "$xy \in q$ and $x \notin q$" implies $y^n \in q$ for some $n \in \mathbb{N}$.

Prop 1.2.2.

- prime $\implies$ primary.
- $\sqrt{\text{primary}} \implies$ prime. Also, if q is primary, then $p = \sqrt{q}$ is the smallest prime ideal containing q, we say q is p-primary.

Proof. The first one is obvious.

If q is primary and $\sqrt{q} = p$. For any $xy \in p$ and $x \notin p$, there exists n so that $x^n y^n \in q$, and for this n, $x^n \notin q$. Thus $(y^n)^m \in q$ for some m, hence $y \in p$. We conclude that p is a prime ideal.

Finally, by corollary 1.2.1,

$$p = \sqrt{q} = \bigcap_{\substack{P \supset q \\ P \in \operatorname{Spec} R}} P \subset P, \quad \forall\, P \text{ prime },$$

thus p is indeed the smallest. □

Eg 1.2.1. The primary ideals in $\mathbb{Z}$ are $\langle 0\rangle$ and $\langle p^m\rangle$ where p is a prime.

Proof. If $q = \langle a\rangle$ is primary, then $\sqrt{q} = \langle p\rangle$ is prime, and $p^n \in \langle a\rangle$. So $ab = p^n$ which implies $a = p^m$ for some m. □

Def 8. An ideal I is said to be **irreducible** if $I = q_1 \cap q_2 \implies I = q_1 \vee I = q_2$.

Def 9. Define $(I : x) = \{a \in R \mid ax \in I\}$.

Theorem 3. In a Noetherian ring R, every irreducible ideal I is primary.

Proof. Let $xy \in I$ and $x \notin I$. Consider $(I : y) \subseteq (I : y^2) \subseteq \cdots$. Since R is Noetherian, exists n such that $(I : y^n) = (I : y^m)$ for any $m \geq n$.

We claim that $I = (I + Ry^n) \cap (I + Rx)$.

- "$\subset$": Obvious.
- "$\supset$": For any $b \in (I + Ry^n) \cap (I + Rx)$, write $b = a_1 + r_1 y^n = a_2 + r_2 x$. Then $r_1 y^{n+1} = a_2 y - a_1 y + r_2 xy \in I$ since $a_1, a_2, xy \in I$. So $r_1 \in (I : y^{n+1}) = (I : y^n) \implies r_1 y^n \in I$. Thus $b = a_1 + r_1 y^n \in I$.

Now by the fact that I is irreducible and $I \neq I + Rx$ since $x \notin I$, thus $I = I + Ry^n \implies y^n \in I$. $\square$

Theorem 4. In a Noetherian ring R, every ideal is a finite intersection of irreducible ideals.

Proof. If not, let $\mathcal{I} \triangleq \{I :\ \text{ideal in } R \mid I \text{ is not a finite intersection of irreducible ideals }\}$ and $\mathcal{I}$ is not an empty set. Since R is Noetherian, the set has a maximal element I_0. Then I_0 is not irreducible (or else it is an intersection of itself, which is irreducible). Write $I_0 = I_1 \cap I_2$, with $I_1, I_2 \neq I_0$. Then $I_1, I_2 \notin \mathcal{I}$, so these two ideals could be written as a finite intersection of irreducible ideals, implying that I_0 could also be written as a finite intersection of irreducible ideals, which is a contradiction. $\square$

Prop 1.2.3. Let q be a p-primary ideal and $x \in R$.

1. If $x \in q$, then $(q : x) = R$.

   Proof. In this case $1 \in (q : x)$, thus $(q : x) = R$. $\square$

2. If $x \notin q$, then $(q : x)$ is p-primary.

   Proof. For any $y \in (q : x)$, $xy \in q$ but $x \notin q$, thus $y^n \in q \implies y \in p$. Hence

   $$q \subset (q : x) \subset p \implies p = \sqrt{q} \subset \sqrt{(q : x)} \subset \sqrt{p} = p$$

   and thus $(q : x)$ is p-primary.

   For any y, z with $yz \in (q : x)$ but $y \notin (q : x)$, which is equivalent to $xyz \in q$ but $xy \notin q$. Since q primary, $z^n \in q \subset (q : x)$. $\square$

3. If $x \notin p$, then $(q : x) = q$.

   Proof.

   $$\begin{cases} y \in (q : x) \\ x \notin p \end{cases} \implies \begin{cases} xy \in (q : x) \\ x^n \notin q,\ \forall\, n \in \mathbb{N} \end{cases} \implies y \in q$$ $\square$

Prop 1.2.4. If each q_i are p-primary, then $q \triangleq \cap_{i=1}^n q_i$ is p-primary.

Proof. We check that $\sqrt{q} = \bigcap_{i=1}^n \sqrt{q_i} = \bigcap_{i=1}^n p = p$.

Also, if $xy \in q$ with $x \notin q$, then $x \notin q_k$ for some k. But $xy \in q_k$, thus $y^n \in q_k$. But $q_k \subseteq \sqrt{q_k} = p = \sqrt{q}$, so $(y^n)^{m'} = y^m \in q$, thus q is p-primary. $\square$

Def 10. A **primary decomposition** of $I = q_1 \cap \cdots \cap q_n$ is **minimal** if $\sqrt{q_1}, \ldots, \sqrt{q_n}$ are distinct and $q_i \not\supseteq \bigcap_{j \neq i} q_j$.

A minimal primary decomposition of an ideal always exists in Noetherian ring since by theorem 4, the ideal could be written as a finite intersection of irreducible ideals, and then by theorem 3, these ideals are primary. Now If $\sqrt{q_i} = \sqrt{q_j}$ happen in these ideals, we could remove these two ideals and add $q' = \sqrt{q_i} \cap \sqrt{q_j}$. By proposition 1.2.4, q' is also primary. And if $q_i \supseteq \bigcap_{j \neq i} q_j$, we could simply remove q_i.

Theorem 5 (Uniqueness of primary decomposition)**.** Let $I = \cap_{i=1}^n q_i$ be a minimal decomposition of I. If $p_i = \sqrt{q_i}$, $\forall\, i$, then we have

$$\{p_i\} = \left\{ \sqrt{(I : x)} \,\middle|\, x \in R \wedge \sqrt{(I : x)} \in \operatorname{Spec} R \right\}$$

which is independent of the decomposition.

Proof. "$\supset$": Let $x \in R \setminus I$, then $(I : x) = \left(\bigcap_{i=1}^n q_i : x\right) = \bigcap_{i=1}^n (q_i : x)$. By proposition 1.2.3, we have $\sqrt{(I : x)} = \bigcap \sqrt{(q_i : x)} = \bigcap_{x \notin q_i} p_i$.

Now, we have the following observation. "If $p \in \operatorname{Spec} R$ with $p = \bigcap_{i=1}^n J_i$, then $p = J_j$ for some j." If not, then $J_i \not\subset p$ for all i, so we could pick $x_i \in J_i \setminus p$. But then $x_1 x_2 \cdots x_n \in \cap J_i = p$ since J_i are ideals, which leads to a contradiction since p is prime.

So if $\sqrt{(I : x)}$ is a prime, then it is equal to some p_i.

"$\subset$": By assumption, $q_i \not\supseteq \bigcap_{j \neq i} q_j$ for each i, thus we could pick $x \in \bigcap_{j \neq i} q_j \setminus q_i$, then $\sqrt{(I : x)} = \bigcap_j \sqrt{(q_j : x)} = \sqrt{(q_i : x)} = p_i$. $\square$

Def 11. If $\{p_i\}$ is the unique prime ideals from the minimal primary decomposition of I.

- $\{p_i\}$ is said to be associated with I or to belong to I.
- The minimal elements in $\{p_i\}$ are called isolated primes.
- The other are called embedded primes.

Eg 1.2.2. Let $R = k[x, y]$ and $I = \langle x^2, xy \rangle$. If $P_1 = \langle x \rangle, P_2 = \langle x, y \rangle$, then $I = P_1 \cap P_2^2$. P_1 is isolated, while P_2 is embedded.

1.3 The equivalence of algebra and geometry (week 10)

In the following, k will be an algebraically closed field.

Def 12. The category of affine algebraic sets $\mathcal{G}$ and its objects and morphisms are defined as following:

objects: The objects are affine algebraic sets in k^n.

An **affine algebraic set** is the common zero set of $\{F_i\}_{i\in\Lambda} \subset k[x_1, \ldots, x_n]$ in k^n. We denote it by $V = \mathcal{V}(\{F_i\}_{i\in\Lambda}) \subset k^n$. (In fact, $I = \langle F_i : i \in \Lambda\rangle$ is Noetherian, so $I = \langle F_1, \ldots, F_n\rangle$ and $V = \mathcal{V}(I)$.)

morphisms: The morphisms are the polynomial map from k^n to k^m.

A **polynomial map** is a mapping as following:

$$\begin{aligned} k^n &\longrightarrow k^m \\ \alpha &\longmapsto (F_1(\alpha), \ldots, F_m(\alpha)) \end{aligned}$$

where each F_i is a polynomial in $K[x_1, \ldots, x_n]$.

Given two affine algebraic sets $V \subset k^n$ and $W \subset k^m$, if a map $F : V \to W$ is the restriction of a polynomial map from k^n to k^m, then F is a morphism from V to W.

Moreover, if $F : V \to W$ and $G : W \to V$ satisfy $F \circ G = \mathrm{Id}$ and $G \circ F = \mathrm{Id}$, then we say $V \cong W$.

Def 13. The category of finitely generated reduced k-algebra $\mathcal{A}$ and its objects and morphisms are defined as following:

objects: The objects are the reduced finitely generated k-algebra R.

A finitely generated k-algebra R is reduced if R has no non-zero nilpotent elements.

morphisms: The morphisms are the k-algebra homomorphisms.

Eg 1.3.1. It is easy to see that $\mathcal{V}(0) = k^n$ and $\mathcal{V}(1) = \varnothing$.

1.3.1 One-one correspondence between affine algebraic sets and radical ideals

Def 14. Define $\mathcal{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(\alpha) = 0, \forall\, \alpha \in V\}$.

The one-one correspondence is given by

$$\begin{aligned} \{\text{affine algebraic sets in } \mathbb{A}^n_k\} &\longleftrightarrow \{\text{ radical ideals in } k[x_1, \ldots, x_n]\} \\ V &\longmapsto \mathcal{I}(V) \\ \mathcal{V}(I) &\longleftarrow I \end{aligned}$$

Prop 1.3.1.

- $\sqrt{\mathcal{I}(V)} = \mathcal{I}(V)$.

  Proof. For all $f^n \in \mathcal{I}(V)$, $f^n(\alpha) = 0, \forall\, \alpha \in V \implies f(\alpha) = 0, \forall\, \alpha \in V$. Thus $f \in \mathcal{I}(V)$. □

- If V is an affine set, then $\mathcal{V}(\mathcal{I}(V)) = V$.

  Proof. "$\supset$": $\forall\, \alpha \in V$, $f \in \mathcal{I}(V)$, $f(\alpha) = 0 \implies \alpha \in \mathcal{V}(\mathcal{I}(V))$.

  "$\subset$": Since V is an affine set, $V = \mathcal{V}(I)$, then $I \subset \mathcal{I}(V)$, so $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(I) = V$. □

Lemma 1. Given $T/S/R$, a tower of rings. If R is Noetherian, T/S is module finite and T/R is ring finite, then S/R is ring finite.

Proof. Let $T = R[a_1, \dots, a_n] = Sw_1 + \cdots + Sw_m$. Then $a_i = \sum r_{i,j} w_j$ for some $r_{i,j}$ and $w_i w_j = \sum t_{i,j,k} w_k$ for some $t_{i,j,k}$.

Let $S' = R\big[\{r_{i,j}\}, \{t_{i,j,k}\}\big] \subseteq S$, which is Noetherian by the Hilbert basis theorem (R Notherian $\implies$ $R[x]$ Notherian). Thus $T = S'\omega_1 + \cdots + S'\omega_m$ is a Noetherian S'-module by the fact that finitely generated module over a Noetherian ring is a Noetherian module.

Since $S \subset T$, S is a finitely generated S' submodule, so

$$S = S'v_1 + \cdots + S'v_r = R\big[\{r_{i,k}\}, \{t_{i,j,k}\}, \{v_i\}\big].$$ □

Lemma 2. If $S = k(z_1, \dots, z_p)$, $p > 0$ with each z_i transcendental, then S/k is not ring finite.

Proof. If not, say $S = k[f_1, \dots, f_n]$ with $f_i = g_i/h_i$, $g_i, h_i \in k[z_1, \dots, z_p]$. Then for any irreducible polynomial p such that $p \nmid h_i$ for each h_i (This polynomial exists since for each h_i there are only finite degree 1 factors). Then $1/p \notin k[f_1, \dots, f_n]$ by checking the divisibility of the denominator under addition and multiplication, which leads to a contradiction. □

Lemma 3. If A/k is an extension of fields and ring finite, then A/k is algebraic.

Proof. If A/k is transcendental and let $\{z_1, \dots, z_t\}$ be a transcendental base. Then $A/k(z_1, \dots, z_t)$ is algebraic, thus module finite (note that A/k is ring finite). By lemma 1, $k(z_1, \dots, z_t)$ is ring finite, which contradicts with lemma 2. □

Theorem 6 (Weak form of Hilbert Nullstellensatz)**.**

$$I \subsetneq k[x_1, \dots, x_n] \implies v(I) \neq \varnothing$$

Proof. Since I proper, by lemma **??**, there exists a maximal ideal M such that $I \subseteq M$. Consider $K \triangleq k[x_1, \dots, x_n]/M = k[\bar{x}_1, \dots, \bar{x}_n]$. By proposition **??**, K is a field, and by lemma 3, K/k is algebraic. Since k is already algebraically closed, $K = k$ and hence each $\bar{x}_i \in k$. Let $\alpha \triangleq (\bar{x}_1, \dots, \bar{x}_n) \in A_k^n$, then for any $f \in M$, $f(\alpha) = f(\bar{x}_1, \dots, \bar{x}_n) = \bar{f} = 0$, thus $\alpha \in \mathcal{V}(M) \subseteq \mathcal{V}(I)$. □

Theorem 7 (Strong form of Hilbert Nullstellensatz)**.** $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$

Proof. "$\supset$": $f \in \sqrt{I} \implies f^n \in I$, then $f^n(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I) \implies f(\alpha) = 0, \forall\, \alpha \in \mathcal{V}(I)$, thus $f \in \mathcal{I}(\mathcal{V}(I))$.

"$\subset$": If $\mathcal{I}(\mathcal{V}(I)) = 0$, then $I \subseteq \sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I)) = 0$, thus $I = 0$.

Otherwise, exists $0 \neq f \in \mathcal{I}(\mathcal{V}(I))$, Let $J = \langle I, ft - 1\rangle \subset k[x_1, \dots, x_n, t]$. If $(a_1, \dots, a_n, t_0)$ is a zero of J, then $ft - 1 \in J \implies -1 = f(a_1, \dots, a_n)t_0 - 1 = 0$, which is a contradiction, so by theorem 6, $J = k[x_1, \dots, x_n, t]$.

Write $1 = \sum h_i f_i + s(ft - 1)$, where each $f_i \in I$ and $h_i, s \in k[x_1, \dots, x_n, t]$. This is a equation of variables, so if we set $t = 1/f$, the equation still holds. Now each h_i would be the form $\sum p_i/f^{k_i}$, so we could multiply each side by a suitable f^ρ and get $f^\rho = \sum c_i f_i$ with each $c_i \in k[x_1, \dots, x_n]$. This implies $f^\rho \in I$, thus $f \in \sqrt{I}$. □

Def 15. Let $V \in \mathcal{G}$, the coordinate ring of V is $k[V] \triangleq k[x_1, \dots, x_n]/\mathcal{I}(V)$.

1.3.2 Equivalence of $\mathcal{G}$ and $\mathcal{A}$

We define a functor F from $\mathcal{G}$ to $\mathcal{A}$ by

$$\begin{aligned} F: \quad \mathcal{G} &\longrightarrow \mathcal{A} \\ V &\longmapsto k[V] \end{aligned}$$

And For a polynomial map $f : V \to W$, define

$$\begin{aligned} F(f) = f^* : \quad k[W] &\longrightarrow k[V] \\ g &\longmapsto g \circ f \end{aligned}$$

Conversely, define a functor G by

$$\begin{aligned} G: \qquad \mathcal{A} &\longrightarrow \mathcal{G} \\ k[x_1, \ldots, x_n]/I &\longmapsto \mathcal{V}(I) \end{aligned}$$

Then if

$$\begin{aligned} \varphi : \quad k[\ldots]/I &\longrightarrow k[\ldots]/J \\ \bar{x}_i &\longmapsto \bar{f}_i \end{aligned}$$

Define

$$\begin{aligned} G(\varphi) = \psi : \qquad \mathcal{V}(J) &\longrightarrow \mathcal{V}(I) \\ \alpha = (a_1, \ldots, a_m) &\longmapsto (f_1(\alpha), \ldots, f_n(\alpha)) \end{aligned}$$

1.4 Gröbner basis (week 11)

1.4.1 Division algorithm in $K[X_1, \dots, X_n]$

Eg 1.4.1. $I = \langle xy-1, y^2-1 \rangle \subseteq K[x,y]$, $f_1 = xy-1$ an d $f_2 = y^2 - 1$ $G = \{f_1, f_2\}$. Does $f = x^2y + xy^2 + y^2 \in I$?

- Choose a lexicographic monomial ordering: $x > y$
- The multidegree $\partial(f) = (2,1)$, $\partial(f_1) = (1,1)$, $\partial(f_2) = (0,2)$
- The leading term $\mathrm{LT}(f) = x^2y$, $\mathrm{LT}(f_1) = xy$, $\mathrm{LT}(f_2) = y^2$
- $\mathrm{LT}(f) = x\,\mathrm{LT}(f_1) \Rightarrow f = xf_1 + xy^2 + y^2 + x \Rightarrow f = \underbrace{(x+y)}_{h_1}f_1 + \underbrace{(1)}_{h_2}f_2 + \underbrace{(x+y+1)}_{\bar{f}^G}$ or $f = \underbrace{x}_{h_1}f_1 + \underbrace{(x+1)}_{h_2}f_2 + \underbrace{(2x+1)}_{\bar{f}^G}$.

Note: Divisor h_1, h_2 and remainder $\bar{f}^G$ are not unique!!

Def 16. Fix a monomial ordering and let I be an ideal of $K[X_1, \dots, X_n]$. The ideal of leading terms in I is defined to be $\mathrm{LT}(I) = \langle\, \mathrm{LT}(f) \mid f \in I\, \rangle$.

Remark 1. Let $I = \langle f_1, \dots, f_n \rangle$. In general, $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_n) \rangle \subsetneq \mathrm{LT}(I)$.

Eg 1.4.2. Let $f_1 = xy^2 + y$, $f_2 = x^2y$. And, $xf_1 - yf_2 = xy \in \langle f_1, f_2 \rangle$ but $xy \notin \langle xy^2, x^2y \rangle$.

Def 17. $G = \{g_1, \dots, g_m\}$ is called a Gröbner basis of I if $I = \langle g_1, \dots, g_m \rangle$ and $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m) \rangle$.

Prop 1.4.1. Let $g_1, \dots, g_m \in I$, then $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m) \rangle \implies I = \langle g_1, \dots, g_m \rangle$.

Proof. $\forall\, f \in I$, do the division process. Then $f = \sum_{i=1}^{m} h_i g_i + r$, either $r = 0$ or $\underline{\bigstar = \text{no term of } r \text{ is divisible by any of } \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m)}$. Assume $r \neq 0$, then $r = f - \sum_{i=1}^{m} h_i g_i \in I \Rightarrow \mathrm{LT}(r) \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m) \rangle$, which is a contradiction. Hence, $r = 0$ (i.e. $f \in \langle g_1, \dots, g_m \rangle$). □

Theorem 8. Each ideal I has a Gröbner basis.

Proof. By Hilbert basis thm, $\mathrm{LT}(I) = \langle f_1, \dots, f_m \rangle$ for some f_i's. Write $f_i = \sum_{j=1}^{m_i} h_{ij}\,\mathrm{LT}(g_{ij})$ with $h_{ij} \in K[X_1, \dots, X_n]$, $g_{ij} \in I$. Then $\mathrm{LT}(I) = \langle\, \mathrm{LT}(g_{ij}) | i = 1, \dots, m,\ j = 1, \dots, m_i\, \rangle$. By prop 1.4.1, This is Gröbner basis. □

Theorem 9. Let $G = \{g_1, \dots, g_m\}$ be a Gröbner basis of I, then

- $\forall\, f \in K[X_1, \dots, X_n]$, $f = f_I + r$ where $f_I \in I, r = \bigstar$ are unique.

  Proof. By division algorithm, $f = f_I + \underset{\bigstar}{r} = f'_I + \underset{\bigstar}{r'}$, then $r \underset{\bigstar}{-} r' = f_I - f'_I$. But if $r - r' \neq 0$, then $\mathrm{LT}(r - r') \in \mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_m) \rangle$, which is a contradiction. Hence, $r - r' = 0 \Rightarrow f_I = f'_I$. □

- $f \in I \iff r = 0$.

  Proof. Suppose $f \in I$, then $f = f_I + \underset{\bigstar}{r}$, and if $r \neq 0$, $\underset{\bigstar}{r} = f - f_I \in I$, which is a contradiction. Hence, $r = 0$. Conversly, if $r = 0$, $f = f_I \in I$. □

1.4.2 Buchberger's algorithm

Def 18. Let $f, g \in K[x_1, \dots, x_n]$ and M be the monic least common multiple of $\mathrm{LT}(f)$ and $\mathrm{LT}(g)$. $S(f,g) = \frac{M}{\mathrm{LT}(f)} f - \frac{M}{\mathrm{LT}(g)} g$ is called an S-polynomial of f, g.

Let $I = \langle g_1, \dots, g_m \rangle$ and $G = \{g_1, \dots, g_m\}$. A Gröbner basis of I can be constructed by the following algorithm:

1. Initially let $G_0 \leftarrow G$.
2. Repeatly construct $G_{i+1} \leftarrow G_i \cup \left(\{S(f,g) \mod G_i \mid f, g \in G_i\} \setminus \{0\}\right)$, until once $G_{i+1} = G_i$, then G_i is a Gröbner basis of I.

Lemma 4. Let $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ with $a_1, \dots, a_m \in K$ satisfying $\partial(f_1) = \partial(f_2) = \dots = \partial(f_m) = \alpha$ and $h = \sum_{i=1}^m a_i f_i$ with $\partial(h) < \alpha$. Then $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$ for some $b_i \in K$.

Proof. Write $f_i = c_i f_i'$ with $c_i \in K$ and f_i' being monic of multidegree α. Note: $S(f_i, f_j) = f_i' - f_j'$ since all multidegree are equal. Then,

$$\begin{aligned}
h &= \sum_{i=1}^m \left(a_i c_i f_i'\right) \\
&= a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \dots + (a_1 c_1 + \dots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') \\
&+ (a_1 c_1 + \dots + a_m c_m) f_m' \\
&= \sum_{i=2}^m b_i S(f_{i-1}, f_i) + b_{m+1} f_m' \text{ with } b_i = \sum_{j=1}^{i-1} a_j c_j.
\end{aligned}$$

Also, in this equality, f_m' is the only term that has multidegree α (other terms have multidegree less than α). So $b_{m+1} = 0$ must hold. Then, we have $h = \sum_{i=2}^m b_i S(f_{i-1}, f_i)$. □

Theorem 10 (Buchberger's criterion)**.** Assume $I = \langle g_1, \dots, g_m \rangle$, then $G = \{g_1, \dots, g_m\}$ is a Gröbner basis of $I \iff S(g_i, g_j) \equiv 0 \pmod G$ for each i, j.

Proof.

- Suppose G is a Gröbner basis of I. $S(g_i, g_j) \in I \Rightarrow S(g_i, g_j) = 0$ by thm 9.
- Converely, suppose $S(g_i, g_j) \equiv 0 \pmod G \forall\, i, j$. For $f \in I$, $f \underset{\textit{not division}}{=} \sum\limits_{i=1}^m h_i g_i$ for some $h_i \in K[x_1, \dots, x_n]$. Define $\alpha = \max\{\partial(h_1 g_1), \dots, \partial(h_m g_m)\}$. We have $\partial(f) \leq \alpha$ and we can select an expression $f = \sum\limits_{i=1}^m h_i g_i$ for f s.t α is minimal.
- Claim: $\partial(f) = \alpha$.
- (pf) If not, we rewrite f

$$\begin{aligned}
f &= \sum_{i=1}^m h_i g_i \\
&= \sum_{\partial(h_i g_i) = \alpha} h_i g_i + \sum_{\partial(h_i g_i) < \alpha} h_i g_i \qquad \text{(the first term} \neq 0 \text{ since } \alpha \text{ is minimal.)} \\
&= \sum_{\partial(h_i g_i) = \alpha} \mathrm{LT}(h_i) g_i + \sum_{\partial(h_i g_i) = \alpha} (h_i - \mathrm{LT}(h_i) g_i) + \sum_{\partial(h_i g_i) < \alpha} h_i g_i
\end{aligned}$$

Let $\mathrm{LT}(h_i) = a_i h_i^0$ with h_i^0 being a monic monomial. Comparing the multidegree on both side, $\partial\left(\sum\limits_{\partial(h_i g_i) = \alpha} a_i h_i^0 g_i\right) < \alpha$ By lemma 4, $\sum\limits_{\partial(h_i g_i) = \alpha} \left(a_i h_i^0 g_i\right) = c_{12} S(h_{i_1}^0 g_{i_1}, h_{i_2}^0 g_{i_2}) + \dots$ (finite) where $\partial(h_{i_1}g_{i_1}) = \partial(h_{i_2}g_{i_2}) = \cdots = \alpha$. By def, if we set $M_{st} = X_{st}^{\beta}$ = the monic LCM of $\mathrm{LT}(g_{i_s}), \mathrm{LT}(g_{i_t})$, then

$$\begin{aligned}
S(h_{i_s}^0 g_{i_s}, h_{i_t}^0 g_{i_t}) &= \frac{X^\alpha}{\mathrm{LT}(h_{i_s}^0 g_{i_s})} h_{i_s}^0 g_{i_s} - \frac{X^\alpha}{\mathrm{LT}(h_{i_t} g_{i_t})} h_{i_t}^0 g_{i_t} \\
&= X^{\alpha-\beta_{st}} \left(\frac{X^{\beta_{st}}}{\cancel{h_{i_s}^0}\,\mathrm{LT}(g_{i_s})} \cancel{h_{i_s}^0} g_{is} - \frac{X^{\beta_{st}}}{\cancel{h_{i_t}^0}\,\mathrm{LT}(g_{i_t})} \cancel{h_{i_t}^0} g_{i_t} \right) \\
&= X^{\alpha-\beta_{st}} S\left(g_{i_s}, g_{i_t}\right) \\
&= X^{\alpha-\beta_{st}} \sum_{j=1}^{m} l_j g_j \text{ (by division)}
\end{aligned}$$

- Then, $\partial(l_j g_j) < \beta_{st} \implies$ we found an expression with multidegree less than α, which is a contradiction. Therefore, $\partial(f) = \alpha \implies \mathrm{LT}(f) = \sum\limits_{\partial(h_i g_i)=\alpha} \mathrm{LT}(h_i)\,\mathrm{LT}(g_i) \implies \mathrm{LT}(f) \in \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle$.

$\square$

Theorem 11. The Buchberger's algorithm will terminate

Proof. .

- $\langle \mathrm{LT}(G_i) \rangle \subsetneq \langle \mathrm{LT}(G_{i+1}) \rangle$ if $G_i \neq G_{i+1}$

$$G_i \neq G_{i+1} \implies \exists\, f, g \in G_i \text{ s.t. } S(f,g) \not\equiv 0 \pmod{G} \implies \mathrm{LT}(S(s,g)) \notin \langle \mathrm{LT}(G_i) \rangle$$

- $\langle \mathrm{LT}(G_0) \rangle \subsetneq \langle \mathrm{LT}(G_1) \rangle \subsetneq \cdots$ is not possible since $K[x_1, \ldots, x_n]$ is a Noetherian ring. (Noetherian ACC condition).

$\square$

1.5 Applications of Gröbner basis

Def 19. Let $I \subseteq K[x_1, \ldots, x_n]$ and $x_1 > x_2 > \cdots > x_n$. $I_i \triangleq I \cap K[x_{i+1}, \ldots, x_n]$ is called the i-th elimination ideal of I.

Theorem 12 (Elimination theorem)**.** Let $G = \{g_1, \ldots, g_m\}$ be a Gröbner basis of $I \neq 0$ with ordering $x_1 > \cdots > x_n$. Then $G_i \triangleq G \cap K[x_{i+1}, \ldots, x_n]$ is a Gröbner basis of I_i (i.e., $\langle \mathrm{LT}(G_i) \rangle = \mathrm{LT}(I_i)$).

Proof. "$\subseteq$": Obvious.

"$\supseteq$": Let $f \in I_i$. Write

$$\mathrm{LT}(f) = \sum h_i \,\mathrm{LT}(g_i) = \sum a_k x^{\alpha_k}\,\mathrm{LT}(g_{i_k})$$

Since $\mathrm{LT}(f)$ involves only the variables $x_{i+1}, \ldots, x_n$, and each terms of $x^{\alpha_k}\,\mathrm{LT}(g_{i_k})$ which uses variables x_k with $k \leq i$ must sum to zero. Remove those term we could write $\mathrm{LT}(f)$ as a combination of $\mathrm{LT}(g_i)$ with $\mathrm{LT}(g_i) \in K[x_{i+1}, \ldots, x_n]$. But by the definition of leading term and the ordering $x_1 > \cdots > x_n$, we have $g_i \in K[x_{i+1}, \ldots, x_n] \implies g_i \in G_i$. Thus $\mathrm{LT}(f) \in \langle \mathrm{LT}(G_i) \rangle$. $\square$

Eg 1.5.1. Find $V = \mathcal{V}(x + y - z, x^2 + y^2 - z^3, x^3 + y^3 - z^5)$.
We compute a Gröbner basis of $I = \langle f_1, \ldots, f_3 \rangle$ with respect to the ordering $x > y > z$. The Gröbner basis is $\{x + y - z, 2y^2 - 2yz - z^3 + z^2, 2z^5 - 3z^4 + z^3\}$.

Eg 1.5.2.

$$\begin{aligned} f: \quad \mathbb{A}^1 &\longrightarrow \mathbb{A}^3 \\ t &\longmapsto (t^4, t^3, t^2) \end{aligned}$$

We compute a Gröbner basis of $I = \langle t^4 - x, t^3 - y, t^2 - z \rangle$ with respect to $t > x > y > z$. The Gröbner basis is $\{-t^2 + z, ty - z^2, tz - y, x - z^2, y^2 - z^3\}$.

Eg 1.5.3.

$$\begin{aligned} f: \quad V = \mathcal{V}(x^3 - x^2 z - y^z) &\longrightarrow \mathbb{A}^3 \\ (x, y, z) &\longmapsto (x^2 z - y^2 z, 2xyz, -z^3) \end{aligned}$$

The ideal is $\langle x^3 - x^2 z - y^2 z, u - x^2 z + y^2 z, v - 2xyz, w + z^3 \rangle$ has a Gröbner basis $\langle \dots, u^2 + v^2 - w^2 \rangle$.

Theorem 13. Let I, J be two ideals of $K[x_1, \dots, x_n]$, then $I \cap J = (t\tilde{I} + (1-t)\tilde{J}) \cap K[x_1, \dots, x_n]$, where $\tilde{I} \triangleq K[x_1, \dots, x_n, t]I$.

Proof. "$\subseteq$": If $f \in I \cap J$, then $f = tf + (1-t)f \in \text{RHS}$.
"$\supseteq$": If $f \in \text{RHS}$, then $f = t\tilde{f}_1 + (1-t)\tilde{f}_2$. with $\tilde{f}_1 \in \tilde{I}$, $\tilde{f}_2 \in \tilde{J}$. Write

$$\tilde{f}_1 = \sum (h_i t + r_i) f_i, \quad \tilde{f}_2 = \sum (h'_j t + r'_j) f_j$$

with each $r_i, r'_j \in K[x_1, \dots, x_n]$, $h_i, h'_j \in K[t, x_1, \dots, x_n]$. Take $t = 0$, $f = \sum r'_j f_j \in J$. Then take $t = 1$, $f = \sum (h_i(1, x_1, \dots, x_n) + r_i) f_i \in J$. Thus $f \in I \cap J$. $\square$

Eg 1.5.4. $I = \langle y^2, x - yz \rangle$, $J = \langle x, z \rangle$. We shall find $I \cap J$.
$tI + (1-t)J = \langle tx - tyz, ty^2, (1-t)x, (1-t)z \rangle$ has a Gröbner basis $\{f_1, f_2, f_3, f_4, xy, x - yz\}$, so $I \cap J = \langle xy, x - yz \rangle$.

Theorem 14. Let $L = \langle f_1, \dots, f_s \rangle \subsetneq K[x_1, \dots, x_n]$, then $f \in \sqrt{I} \iff \langle f_1, \dots, f_s, 1 - tf \rangle = K[x_1, \dots, x_n, t]$.

Proof. "$\Leftarrow$": By theorem 6, $\langle f_1, \dots, f_s, 1 - tf \rangle = K[x_1, \dots, x_n, t]$ if and only if $\mathcal{V}(f_1, \dots, f_s, 1 - tf) = \varnothing$. Notice that $1 - tf$ has no zero if $f = 0$, which means that If $\boldsymbol{x}$ is a common zero of $f_1, \dots, f_s$, then $f(\boldsymbol{x}) = 0$. So $f \in \mathcal{I}(\mathcal{V}(I)) \implies f \in \sqrt{I}$ by theorem 7.
"$\Rightarrow$": $f^m \in I \implies 1 = t^m f^m + 1 - t^m f^m = t^m f^m + (1 - tf)(1 + tf + \cdots + t^{m-1} f^{m-1}) \in \langle f_1, \dots, f_s, 1 - tf \rangle$. $\square$

Eg 1.5.5. Let $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$, and we want to determine $f = y - x^2 + 1$ is in $\sqrt{I}$ or not.

Prop 1.5.1. An affine algebraic set V in $\mathbb{A}^n_k$ has a unique minimal decomposition. $V = V_1 \cup V_2 \cup \cdots \cup V_m$ with V_i irreducible and $V_i \not\subset V_j$.

Proof.

Existence: If not, then $V = V_1 \cup V'_1$, and one of V_1, V'_1, say $V_1 = V_2 \cup V'_2$, ... So we would find

$$V \supsetneq V_1 \supsetneq V_2 \subsetneq \cdots \implies \mathcal{I}(V) \subsetneq \mathcal{I}(V_1) \subsetneq \mathcal{I}(V_2) \subsetneq \text{ in } k[x_1, \dots, x_n],$$

which contradicts that $k[x_1, \dots, x_n]$ is Noetherian.

- Uniqueness: If
$$V = V_1 \cup \cdots \cup V_m = V_1' \cup \cdots \cup V_m'$$
then $V_i = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_m')$. But V_i irreducible, so $V_i = V_i \cap V_j' \implies V_i \subset V_j'$. By symmetry we would find $V_j' \subset V_k$, then $V_i \subset V_j' \subset V_k \implies V_i = V_k$. Thus these two decompositions are equal.

□

Theorem 15 (Decomposition)**.** Assume $\sqrt{I} = I$ and $I \subset J$, then $\mathcal{V}(I : J) = \mathcal{V}(\mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J)))$. and $\mathcal{V}(I) = \mathcal{V}(J) \cup \mathcal{V}(I : J)$.

Proof. Let $f \in \mathcal{I}(\mathcal{V}(I) \setminus \mathcal{V}(J))$ and $g \in J$, then $fg = \mathcal{I}(\mathcal{V}(I)) = \sqrt{I} = I$ since $f(\alpha) = 0$ for each $\alpha \in \mathcal{V}(I) \setminus \mathcal{I}(J)$ and $g(\alpha) = 0$ for each $\alpha \in \mathcal{V}(J)$. Thus $f \in (I : J)$. □

Eg 1.5.6. Let $I = \langle xz - y^2, x^3 - yz \rangle$ and $V = \mathcal{V}(I)$.

Notice that $\langle xz - y^2, x^3 - yz \rangle \subseteq \langle x, y \rangle = J$, so $(I : J) = (I : \langle x \rangle) \cap (I : \langle y \rangle)$.

First we calculate $(I : x)$. Notice that we know how to calculate $I \cap \langle x \rangle$ now. After a calculation, $I \cap \langle x \rangle = \{x^2z - xy^2, x^4 - xyz, x^3y - xz^2\}$, so $(I : x) = \langle f_1/x, f_2/x, f_3/x \rangle = I + \langle x^2y - z^3 \rangle$. Simarly one could find that $(I : y) = (I : x)$, thus $(I : J) = (I : x)$.

Hence $V = \mathcal{V}(x, y) \cap \mathcal{V}(xz - y^2, x^3 - yz, x^2y - z^2)$.

Prop 1.5.2. Let $f : V \to W$, then $\overline{f(V)} = \mathcal{V}(\ker f^*)$ where $f^* : k[W] \to k[V]$.

Proof. We claim that $\ker f^* = \mathcal{I}(f(V))$, since

$$\bar{g} \in \mathcal{I}(f(V)) \iff \bar{g}(f(\alpha)) = 0, \forall\, \alpha \in V \iff \bar{g} \circ f \in \mathcal{I}(V) \iff f^*(\bar{g}) = \overline{g \circ f} = \bar{0} \iff \bar{g} \in \ker f^*$$

Thus $\mathcal{V}(\ker f^*) = \mathcal{V}(\mathcal{I}(f(V))) = \overline{f(V)}$. □

Remark 2. In general, if $W \subseteq \mathbb{A}_k^n$ is an affine algebraic set defined by $x_i = f_i(t_1, \ldots, t_m)$, then W is irreducible.

Proof. $f : \mathbb{A}_k^m \twoheadrightarrow W$ is onto, so $\overline{f(\mathbb{A}_k^m)} = W = \mathcal{V}(0)$. By the previous proposition, $\ker f^* = 0$, thus $f^* : K[W] \cong k[x_1, \ldots, x_n]/\mathcal{I}(W) \hookrightarrow k[t_1, \ldots, t_m]$. But $k[t_1, \ldots, t_m]$ is an integral domain, so $\mathcal{I}(W)$ is a prime ideal, thus W is irreducible. □

1.6 Local Rings (week 12)

From now on, R is a commutative ring with 1.

We list some facts about localization.

Prop 1.6.1. Let p be a prime ideal in R, R_p be the localization about p.

- Extension and contraction gives a bijective correspondence between $\{$ prime ideal $q \subset p\}$ and $\{$ prime ideal in $R_p\}$.
- Extension and contraction gives a bijective correspondence between $\{p$-primary ideal $q\}$ and $\{$ primary ideal in $R_p\}$.
- Localization commutes with intersection.
- Localization preserves exact sequence.
- If R is Noetherian (Artinian), then R_p is Noetherian (Artinian).

Def 20. R is called a local ring if it has a unique maximal ideal.

Prop 1.6.2. TFAE

(1) R is a local ring.

(2) The set of non-units forms an ideal.

(3) $\exists\, M \in \operatorname{Max} R$ s.t. $1 + m$ is a unit $\forall\, m \in M$.

Proof.

(1) ⇒ (2): Let M be the unique maximal ideal of R. Then M couldn't contain any unit. For each non-unit x, $\langle x\rangle \neq R$ and is contained in a maximal ideal by lemma **??**, thus $x \in M$. Hence $M = \{\text{non-units}\}$.

(2) ⇒ (3): This ideal must be a maximal ideal M since it can't be extended. Now, $1 \notin M \rightsquigarrow 1 + m \notin M$. So $1 + m$ is a unit.

(3) ⇒ (1): If there exists another maximal ideal N, then $M + N = R$. Say $m \in M, n \in N$ s.t. $m + n = 1$, then $n = 1 - m$ is a unit $\implies N = R$, which is a contradiction. □

Eg 1.6.1. $k[[x]]$ is a local ring with the unique maximal ideal $\langle x\rangle$.

Proof. For each $f = \sum a_n x^n \in k[[x]]$, one could see that f is an unit if and only if $a_n \neq 0$, and the leftovers form an ideal $\langle x\rangle$. □

Eg 1.6.2. Let $P \in \operatorname{Spec} R$. If $S = R \setminus P$, then S is a multiplicatively closed set with $1 \in S$ and $R_P \triangleq R_S$ is a local ring.

Proof. S is a multiplicatively closed set simply follow from the definition of prime ideal. One could then easily see that $P_P \triangleq \left\{ \frac{x}{s} \mid x \in P, s \in S \right\}$ contains all non-unit, thus R_P is local. □

Prop 1.6.3. The following sets are correspondent (k is algebraically closed):

(1) $\mathbb{A}_k^n$

(2) $\operatorname{Max} k[x_1, \ldots, x_n]$

(3) $\operatorname{Hom}_k(k[x_1, \ldots, x_n], k)$

Proof. (1) $\Rightarrow$ (2): For any $(a_1,\dots,a_n)\in\mathbb{A}_k^n$, $k[x_1,\dots,x_n]/\langle x_1-a_1,\dots,x_n-a_n\rangle\cong k$ is a field, hence $\langle x_1-a_1,\dots,x_n-a_n\rangle$ is a maximal ideal.

(2) $\Rightarrow$ (1): Let $M\in\operatorname{Max}k[x_1,\dots,x_n]$, by theorem 6, $\mathcal{V}(M)\neq\varnothing$, so exists $(a_1,\dots,a_n)\in\mathcal{V}(M)$. Now $M=\sqrt{M}=\mathcal{I}(\mathcal{V}(M))\subseteq\mathcal{I}((a_1,\dots,a_n))=\langle\dots,x_i-a_i,\dots\rangle$ which is maximal, We conclude that $(a_1,\dots,a_n)$ is the only element in $\mathcal{V}(M)$ and $M=\langle\dots,x_i-a_i,\dots\rangle$.

(1) $\Rightarrow$ (3): For each $(a_1,\dots,a_n)$, define $\varphi\in\operatorname{Hom}_k(\cdots)$ by evaluation:

$$\begin{aligned}\varphi:\quad k[x_1,\dots,x_n]&\longrightarrow k\\ x_i&\longmapsto a_i\end{aligned}$$

(3) $\Rightarrow$ (1): Similarly, for each $\varphi\in\operatorname{Hom}_k(\cdots)$, recover $(a_1,\dots,a_n)$ by $(\varphi(x_1),\dots,\varphi(x_n))$. □

Remark 3. Inspired by the correspondence,

Def 21. A property of an R-module M is said to be a local property if

$$M \text{ has this property } \iff M_P \text{ (as an } R_P\text{-module) has this property } \forall\, P\in\operatorname{Spec}R$$

Prop 1.6.4. TFAE

(1) $M=0$

(2) $M_P=0\quad\forall\, P\in\operatorname{Spec}R$

(3) $M_Q=0\quad\forall\, Q\in\operatorname{Max}R$

Proof. (1) $\Rightarrow$ (2) and (2) $\Rightarrow$ (3) are clear.

(3) $\Rightarrow$ (1): If $M\neq0$, let $x\in M$ such that $x\neq0$, then $\operatorname{Ann}(x)\subsetneq R$ since $1\notin\operatorname{Ann}(x)$. Let $\operatorname{Ann}(x)\subset Q\in\operatorname{Max}R$. By assumption, $M_Q=0$ implies $\frac{x}{1}=\frac{0}{1}$. By the definition of equal in localization, $\exists\, r\notin Q$ such that $rx=0$, thus $r\in\operatorname{Ann}(x)$ which leads to a contradiction. □

Coro 1.6.1. Let $N\subseteq M$, TFAE (consider M/N)

(1) $N=M$

(2) $N_P=M_P\quad\forall\, P\in\operatorname{Spec}R$

(3) $N_Q=M_Q\quad\forall\, Q\in\operatorname{Max}R$

Prop 1.6.5. TFAE

(1) $0\to M\xrightarrow{\phi}N\xrightarrow{\psi}L\to0$ exact

(2) $0\to M_P\xrightarrow{\phi_P}N_P\xrightarrow{\psi_P}L\to0$ exact $\forall\, P\in\operatorname{Spec}R$

(3) $0\to M_Q\xrightarrow{\phi_Q}N_Q\xrightarrow{\psi_Q}L\to0$ exact $\forall\, Q\in\operatorname{Max}R$

Proof. (1) $\Rightarrow$ (2): By the fact that localization preserves exact sequence.

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

(3) $\Rightarrow$ (1): Let $K=\ker\phi$, then $0\to K\to M\to N$ exact. Since we just proved (1) $\Rightarrow$ (3), $0\to K_Q\to M_Q\to N_Q$ exact, but $K_Q=0$, by proposition 1.6.4, $K=0$.

We could prove the other half similarly by letting K to be the cokernel. □

Def 22.

- Let $R \subseteq S$. $\bar{R} = \{x \in S \mid x \text{ is integral over } R\}$ is called the integral closure of R in S.
- R is integrally closed in S if $R = \bar{R}$.
- An integral domain R is called normal if R is integrally closed in its field of fractions.

Theorem 16. UFD is normal.

Proof. Let R be a UFD and K be its field of fractions. If $a \in K$ is integral over R and $a^n + r_1 a^{n-1} + \cdots + r_n = 0$. Write $a = u/s$ with $\gcd(u, s) = 1$. Then $u^n + r_1 s u^{n-1} + \cdots + r_n s^n = 0$. Now if s is a non-unit, says $p \mid s$ with p is a prime. Then $p \mid u$ obviously $\rightsquigarrow p \mid \gcd(u, s) = 1$, which is a contradiction. So s is a unit $\implies a \in R$. $\square$

Prop 1.6.6.

- Let S/R is an integral extension and $T \subset R$ be a m.c. set with $1 \in T$. Then S_T is also integral over R_T.

  Proof. Let $a/t \in S_T$ with $a^n + r_1 a^{n-1} + \cdots + r_n = 0$, then we have
  $$\left(\frac{a}{t}\right)^n + \frac{r_1}{t}\left(\frac{a}{t}\right)^{n-1} + \cdots + \frac{r_n}{t^n} = 0.$$
  Thus a/t is integral over R_T. $\square$

- Let S/R be an arbitrary extension and $T \subset R$ be m.c. with $1 \in T$. Then $(\bar{R})_T = \overline{(R_T)}$ in S_T.

  Proof. By 1., $(\overline{R})_T$ is integral over R_T. If $a/t \in S_T$ is integral over R_T, say
  $$\left(\frac{a}{t}\right)^n + \frac{r_1}{t_1}\left(\frac{a}{t}\right)^{n-1} + \cdots + \frac{r_n}{t_n} = 0.$$
  Then we let $v = t_1 t_2 \cdots t_n$, multiply the equation by $(tv)^n$, we get
  $$(va)^n + (r_1 t t_2 \cdots t_n)(va)^{n-1} + \cdots = 0 \implies va \in \overline{R}$$
  So $a/t = va/(vt) \in \overline{R}_T$. $\square$

Prop 1.6.7. "Being normal" is a local property. TFAE

(1) R is normal

(2) R_P is normal $\forall\, P \in \operatorname{Spec} R$

(3) R_Q is normal $\forall\, Q \in \operatorname{Max} R$

Proof. The key is to realize that if K is the field of fraction of R, then K is also the field of fraction of any R_P. Then by lemma 1.6.5,
$$0 \to R \to \overline{R} \to 0 \iff 0 \to R_P \to (\overline{R})_P \to 0, \forall\, P$$
By the previous proposition, $(\overline{R})_P = \overline{R_P}$ in S_P, this proves all. $\square$

Def 23. An R-module F is flat if the functor $- \otimes_R M$ is exact (i.e., it preserves exact sequence).

Prop 1.6.8. Given an homomorphism $R_1 \to R_2$. If M is a flat R_1-module, then $R_2 \otimes_{R_1} M$ is a flat R_2 module.

Proof. Notice that $N \otimes_{R_1} M \cong N \otimes_{R_2} (R_2 \otimes_{R_1} M)$, so

$$\begin{aligned} 0 \to N \to N' \text{ exact } &\implies 0 \to N \otimes_{R_1} M \to N' \otimes_{R_1} M \text{ exact} \\ &\implies 0 \to N \otimes_{R_2} (R_2 \otimes_{R_1} M) \to N' \otimes_{R_2} (R_2 \otimes_{R_1} M) \text{ exact} \end{aligned}$$

Which is to say that $R_2 \otimes_{R_1} M$ flat. □

Prop 1.6.9. TFAE

(1) M is a flat R-module

(2) M_P is a flat R-module $\forall\, P \in \operatorname{Spec} R$

(3) M_Q is a flat R-module $\forall\, Q \in \operatorname{Max} R$

Proof. (1) $\Rightarrow$ (2): By the previous proposition combined with the property of localization, $M_P \cong R_P \otimes_R M$ is a flat module.

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

(3) $\Rightarrow$ (1): If $0 \to N \to N'$ exact, then by prop 1.6.5, $0 \to N_Q \to N'_Q$ exact, so

$$0 \to N_Q \otimes_{R_Q} M_Q \to N'_Q \otimes_{R_Q} M_Q$$

is also exact. By the property of localization, $N_Q \otimes_{R_Q} M_Q \cong (N \otimes_R M)_Q$. Using prop 1.6.5, $0 \to N \otimes_R M \to N' \otimes_R M$ exact. □

1.7 Krull dimension

Def 24.

- The Krull dimension of a topological space X is the supremum of the lengths n of all chains $X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n$, where X_i are closed irreducible subset of X.
- The Krull dimension of a commutative ring R with 1 is the supremum of the lengths n of all chains $P_0 \subsetneq \cdots \subsetneq P_n$ where $P_i \in \operatorname{Spec} R$.

Prop 1.7.1. Let $R \subseteq S$ be two integral domains and S/R be integral. Then S is a field if and only if R is a field.

Proof. "$\Rightarrow$": For each $a \neq 0$ in R, $a^{-1} \in S$, so we could write

$$(a^{-1})^n + r_1(a^{-1})^{n-1} + \cdots + r_n = 0,\ r_i \in R$$

Which implies

$$a^{-1} = -(r_1 + \cdots + r_n a^{n-1}) \in R$$

"$\Leftarrow$": For each $a \neq 0$ is S, write

$$a^n + r_1 a^{n-1} + \cdots + r_n = 0,\ r_i \in R$$

Notice that we could assume $r_n \neq 0$, or else $a(a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-1}) = 0$ and hence $a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-1} = 0$ because R is an integral domain. Then

$$a^{-1} = -r_n^{-1}(a^{n-1} + r_1 a^{n-2} + \cdots + r_{n-2})$$

□

Prop 1.7.2. Let S/R be integral.

1. If $q \in \operatorname{Spec} S$ and $p = q \cap R \in \operatorname{Spec} R$, then $q \in \operatorname{Max} S \iff p \in \operatorname{Max} R$.

   Proof. It is easy to see that S/q is integral over R/p by the identification

   $$\begin{aligned} R/p &\hookrightarrow S/q \\ r+p &\longmapsto r+q \end{aligned}$$

   So

   $$q \in \operatorname{Max} S \iff S/q \text{ is a field} \iff R/p \text{ is a field} \iff p \in \operatorname{Max} R$$

   ☐

2. If $q, q' \in \operatorname{Spec} S$ with $q \subseteq q'$ and $q \cap R = p = q' \cap R$. Then $q = q'$.

   Proof. We know that $S_p \triangleq S_{R\setminus p}$ is integral over R_p. Since $q_p \subseteq q'_p$ and both $q_p \cap R_p$ and $q'_p \cap R_p$ equal p_p is maximal in R_p. Using 1., q_p, q'_p are maximal in S_p, but $q_p \subseteq q'_p \implies q_p = q'_p$. By corollary 1.6.1, $q = q'$. ☐

Theorem 17 (Going-up theorem)**.** Let S/R be integral, then

- If $p \in \operatorname{Spec} R$, then $\exists\, q \in \operatorname{Spec} S$ such that $q \cap R = p$.

  Proof. We have the diagram:

  $$\begin{tikzcd} p \arrow[r, rightsquigarrow] & R \arrow[r, hook] \arrow[d] & S \arrow[d] \\ p_p \arrow[r, rightsquigarrow] & R_p \arrow[r, hook] & S_p \end{tikzcd}$$

  Pick $q_p = N \in \operatorname{Max} S_p$, then $N \cap R_p \in \operatorname{Max} R_p = \{p_p\}$ by 1. of proposition 1.7.2, so $N \cap R_p = p_p$, and $(q \cap R)_p = q_p \cap R_p = p_p$, thus $q \cap R = p$. ☐

- If $p_1 \subset p_2$ in $\operatorname{Spec} R$ and $q_1 \in \operatorname{Spec} S$ with $q_1 \cap R = p_1$, then $\exists\, q_2 \in \operatorname{Spec} S$ with $q_1 \subset q_2$ and $q_2 \cap R = p_2$.

  Proof. Let $R' = R/p_1$ and $S' = S/q_1$. Then again, S'/R' is integral. By the previous statement, exists $q_2/q_1 \in \operatorname{Spec} S'$ so that $q_2/q_1 \cap R' = p_2/p_1$, thus $q_2 \cap R = p_2$ and $q_2 \supseteq q_1$. ☐

Theorem 18. If S/R is integral, then $\dim S = \dim R$.

Proof. For any chain $q_0 \subsetneq q_1 \subsetneq \cdots \subsetneq q_n$ in $\operatorname{Spec} S$, by prop 2., $q_0 \cap R \subsetneq q_1 \cap R \subsetneq \cdots \subsetneq a_n \cap R$.

Conversely, given $p_0 \subsetneq p_1 \subsetneq \cdots \subsetneq p_n$ in $\operatorname{Spec} R$, there is $q_0 \subsetneq q_1 \subsetneq \cdots \subsetneq q_n$ by the going up theorem (17). ☐

Prop 1.7.3. Let S, R be integral domains and S/R be integral, assume R is normal with the field of fractions K. If $a \in S$ is integral over $I \subseteq R$, then $f = m_{\alpha,K} = x^n + r_1 x^{n-1} + \cdots + r_n$ with $r_i \in \sqrt{I}$.

Proof. Assume $\deg f = n$ and $a_1, \ldots, a_n \in \overline{K}$ are the zeros of f. By assumption, $a^m + t_1 a^{m-1} + \cdots + t_m = 0$ with $t_i \in I \subset R \subset K$. For each i, exists $\varphi \in \operatorname{Aut}(\overline{K}/K)$ such that $\varphi(a) = a_i$. Then $0 = \varphi(a^m + t_1 a^{m-1} + \cdots + t_m) = a_i^m + t_1 a_i^{m-1} + \cdots + t_m$, so a_i is integral over I. Moveover, the coefficients of f are the elementary symmetry symmetric polynomial of a_i, hence they are integral over I and lie in $\sqrt{I\overline{R}} = \sqrt{IR} = \sqrt{I}$. ☐

Theorem 19 (Going-down theorem)**.** Let S, R be integral domains and S/R be integral, assume R is normal with the field of fractions K. If $p_1 \supset p_2$ in $\operatorname{Spec} R$ and $q_1 \in \operatorname{Spec} S$ with $q_1 \cap R = p_1$, then $\exists\, q_2 \in \operatorname{Spec} S$ such that $q_1 \supset q_2$ and $q_2 \cap R = p_2$.

Proof. First we claim that $p_2 S_{q_1} \cap R = p_2$.

"$\supseteq$": Obvious.

"$\subseteq$": For $b/t \in p_2 S_{q_1} \cap R$, $b \in p_2 S \subset \sqrt{p_2 S} = \sqrt{\overline{p_2 R}}$, which means that b is integral over p_2 and $t \in S \setminus q_1$. By proposition 1.7.3, if $m_{b,K} = x^l + r_1 x^{l-1} + \cdots + r_l$, then $r_i \in \sqrt{p_2} = p_2$.

Now, $a = b/t \in R$, so $t = b/a \in S_{R\setminus\{0\}} = SK$, so

$$\left(\frac{b}{a}\right)^l + \left(\frac{r_1}{a}\right)\left(\frac{b}{a}\right)^{l-1} + \cdots + \left(\frac{r_l}{a^l}\right) \leftrightarrow b^l + r_1 b^{l-1} + \cdots + r_l = 0$$

is a correspondence. Thus we know that $m_{t,K} = x^l + (r_1/a)x^{l-1} + \cdots + (r_l/a^l)$.

Again by proposition 1.7.3, since t is integral over R, $u_i \triangleq r_i/a^i \in R$, and $u_i a^i = r_i$ for each i.

If $a \notin p_2$, then $u_i a^i = r_i \in p_2$, so $u_i \in p_2$. But with $m_{t,K}$ we will find that $t^l \in p_2 S \subseteq p_1 S \subseteq q_1$, so $t \in q_1$, which leads to a contradiction. Thus $a \in p_2$.

Now we've proved $p_2 S_{q_1} \cap R = p_2$, by exercise 12.4, $p_2 = Q \cap R$ for some $Q \in S_{q_1}$. Letting $q = Q \cap S$ and we're done. $\square$

Theorem 20. All maximal chain in $\operatorname{Spec} K[x_1, \ldots, x_n]$ have the same length n, and thus

$$\dim K[x_1, \ldots, x_n] = n.$$

Proof. Let $P_0 \subset P_1 \subset \cdots \subset P_m$ in $\operatorname{Spec} K[x_1, \ldots, x_n]$ We shall use induction on n to prove $m = n$.

$n = 0$: Then $\langle 0 \rangle$ is a max chain in $\operatorname{Spec} K$, so $m = 0 = n$.

$n > 0$: Let $K[y_1, \ldots, y_n] \hookrightarrow K[x_1, \ldots, x_n]$ be a strong Noether normalization with $P_1 \cap K[y_1, \ldots, y_n] = \langle y_{d+1}, \ldots, y_n \rangle$, then $h(P_1) = 1 \implies h(P_1 \cap K[y_1, \ldots, y_n]) = 1$ by the going down theorem (19). Then we can say $P_1 \cap K[y_1, \ldots, y_n] = \langle y_n \rangle$. Then we can consider $K[x_1, \ldots, x_n]/P_1$ and $K[y_1, \ldots, y_n]/\langle y_n \rangle \cong K[y_1, \ldots, y_{n-1}]$. $\square$

1.8 Artinian rings and DVR (week 13)

1.8.1 Artinian rings

Def 25. R is called an Artinian ring if one of the followings holds:

- any non-empty set of ideals has a minimal element.
- any descending chain of ideals is stationary (DCC).

Goal:

1. $R \cong R_1 \times \cdots \times R_l$ where R_i is an Artinian local rings.
2. Artinian $\iff$ Noetherian $+ \dim = 0$.

Prop 1.8.1.

- $\sqrt{\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}} = \sqrt{\sqrt{\mathfrak{m}_i^{n_i}} + \sqrt{\mathfrak{m}_j^{n_j}}}$

  Proof.
  "$\subseteq$": Obvious.

  "$\supseteq$" $\forall\, a \in$ RHS, that is, $a^n = b + c$ with $b^k \in \mathfrak{m}_i^{n_i}$ and $c^t \in \mathfrak{m}_j^{n_j}$. Then $(a^n)^{k+t} = (b+c)^{k+t} = b^{k+t} + \cdots + \binom{k+t}{t} b^k c^t + \cdots + c^{k+t}$. Every term is in either $\mathfrak{m}_i^{n_i}$ or $\mathfrak{m}_j^{n_j}$, then $(a^n)^{k+t} = c + d$ with $c \in \mathfrak{m}_i^{n_i}$, $d \in \mathfrak{m}_j^{n_j} \Rightarrow a \in$ LHS ☐

- If m is prime, $\sqrt{m^n} = m$

  Proof.
  "$\subseteq$": If $a \in$ LHS, then $a^k \in m^n \subset m$ and m is prime. $\Rightarrow a \in m$.

  "$\supseteq$": If $a \in$ RHS, then $a^n \in m^n \implies a^n \in$ LHS. ☐

- If m, $m_i, i = 1, \cdots, n$ are prime and $m \supseteq m_1 \cap \cdots \cap m_n$, then $m \supseteq m_i$ for some i.

  Proof.
  Suppose not, then we pick $a_i \in m_i \backslash m$. Then $b \triangleq a_1 \cdots a_n \in m_i$, $\forall\, i$. So $b \in m_1 \cap \cdots \cap m_n \subseteq m$. But m is prime, so exist $a_i \in m$, which is a contradiction. ☐

Prop 1.8.2. Let R be an Artinian ring

(1) If $I \subseteq R$, then R/I is also Artinian.

(2) If R is an integral domain, then R is a field.

  Proof. $\forall\, a \neq 0 \in R, \langle a \rangle \supseteq \langle a^2 \rangle \supseteq \cdots$ is a descending chain of ideals $\implies \langle a^l \rangle = \langle a^{l+1} \rangle = \cdots$ for some $l \in \mathbb{N} \implies a^l = ba^{l+1} \implies a^l(1 - ab) = 0 \implies ab = 1$ since cancellation works in integral domain. ☐

(3) $\operatorname{Spec} R = \operatorname{Max} R$. ($\implies \dim R = 0$)

  Proof. $\forall\, p \in \operatorname{Spec} R, R/p$ is an integral domain $\implies R/p$ is a field $\implies p \in \operatorname{Max} R$. ☐

(4) $|\operatorname{Max} R| < \infty$.

Proof. Consider the set $\left\{ \bigcap_{\text{finite}} \mathfrak{m} \,\middle|\, \mathfrak{m} \in \operatorname{Max} R \right\} \neq \varnothing$. So there exists a minimal element in this set since R is Artinian, say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$. Now, for $\mathfrak{m} \in \operatorname{Max} R$, we have $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k$ since the latter is minimal, so $\mathfrak{m} \supseteq \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \implies \mathfrak{m} \supseteq \mathfrak{m}_i$ for some i, by 3. of proposition 1.8.1. Then $\mathfrak{m} = \mathfrak{m}_i$, since $\mathfrak{m}_i$ is max. So $\operatorname{Max} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_k\}$. □

(5) $\exists\, n_1, \ldots, n_k \in \mathbb{N}$ s.t. $\langle 0 \rangle = \mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} = \mathfrak{m}_1^{n_1} \cap \mathfrak{m}_2^{n_2} \cap \cdots \cap \mathfrak{m}_k^{n_k}$.

Proof. First we claim that $\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} = \mathfrak{m}_1^{n_1} \cap \mathfrak{m}_2^{n_2} \cap \cdots \cap \mathfrak{m}_k^{n_k}$. Recall that if I_i, I_j are coprime for $i \neq j$, then $\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$. By Prop 1.8.1

$$\sqrt{\mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j}} = \sqrt{\sqrt{\mathfrak{m}_i^{n_i}} + \sqrt{\mathfrak{m}_j^{n_j}}} = \sqrt{\mathfrak{m}_i + \mathfrak{m}_j} = \sqrt{R} = R \implies \mathfrak{m}_i^{n_i} + \mathfrak{m}_j^{n_j} = R.$$

Now, let n_i be the one so that $\mathfrak{m}_i^{n_i} = \mathfrak{m}_{i+1}^{n_{i+1}}$. We claim that $\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} = \langle 0 \rangle$.
If not, let $\mathcal{S} = \{J \subseteq R \mid J \mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0\} \neq \varnothing$ since $\mathfrak{m}_i \in S$. By the fact that R is Artinian, there exists a minimal element $J_0 \in \mathcal{S}$. By definition of $\mathcal{S}$, Exists $x \in J_0$ so that $x \mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq 0$. Then $\langle x \rangle \in \mathcal{S}$ $\langle x \rangle \subseteq J_0$ which by the minimality we must have $\langle x \rangle = J_0$.

Also, $x \mathfrak{m}_1^{n_1+1} \mathfrak{m}_2^{n_2+1} \cdots \mathfrak{m}_k^{n_k+1} = x \mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \neq \langle 0 \rangle$, so $I = x \mathfrak{m}_1 \ldots \mathfrak{m}_k \in S$ and $I \subseteq xR = J_0 \implies I = xR$. Then we have $\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_k = \operatorname{Jac} R$ with $\operatorname{Jac} R(xR) = xR$ since $\operatorname{Max} R = \operatorname{Spec} R$. By Nakayama's lemma, $xR = 0 \implies x = 0$ which leads to an contradiction. □

(6) The nilradical $\mathfrak{n}_R$ of R is nilpotent.

Proof. Again, $\mathfrak{n}_R = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k = \operatorname{Jac} R$. Let $n = \max\{n_1, \ldots, n_k\}$ in (5), then $\mathfrak{n}_R^n = (\mathfrak{m}_1 \mathfrak{m}_2 \cdots \mathfrak{m}_k)^n = 0$. □

Theorem 21. If R is an Artinian ring, then $R \cong R_1 \times \cdots \times R_k$ where each R_i is Artinian local ring.

Proof. By Chinese Remainder theorem,

$$R \cong R/\langle 0 \rangle = R/\mathfrak{m}_1^{n_1} \mathfrak{m}_2^{n_2} \cdots \mathfrak{m}_k^{n_k} \cong R/\mathfrak{m}_1^{n_1} \times R/\mathfrak{m}_2^{n_2} \times \cdots \times R/\mathfrak{m}_k^{n_k}$$

Let $R_i = R/\mathfrak{m}_i^{n_i}$, which is Artinian since it is the quotient of an Artinian ring. Since quotient preserves maximality, $\bar{\mathfrak{m}} \in \operatorname{Max} R_i \iff \mathfrak{m} \in \operatorname{Max} R$. But then $\mathfrak{m} \supset \mathfrak{m}_i^{n_i} \implies \mathfrak{m} = \mathfrak{m}_i$. Since $\mathfrak{m}_i = \sqrt{\mathfrak{m}_i^{n_i}}$ is the smallest prime containing $\mathfrak{m}_i^{n_i}$ by proposition 1.2.2. So $\operatorname{Max} R_i = \{\bar{\mathfrak{m}}_i\} \implies R_i$ is a local ring. □

Lemma 5. Let V be a K-vector space, TFAE

(1) $\dim_k V < \infty$

(2) V has DCC on subspaces.

(3) V has ACC on subspaces.

Proof.
Fact : If $V_1 \subseteq V_2$ is finite dimensional vector space over K, then $V_1 = V_2 \iff \dim_k V_1 = \dim_k V_2$. Otherwise, $\dim_k V_1 < \dim_k V_2$.

(1) $\Leftrightarrow$ (3)
" $\Rightarrow$ " Suppose there exists a chain in vector space V with strictly increasing and infinite length,

$$V_1 \subset V_2 \subset \cdots \subseteq V \Rightarrow \dim_k V_1 < \dim_k V_2 < \cdots \leq \dim_k V$$

Then, $\dim_k V$ must be infinite.
" $\Leftarrow$ " If $\dim_k V$ is infinite, let S $= \{b_1, b_2, \dots\}$ be basis of V.

$$\langle b_1 \rangle_K \subset \langle b_1, b_2 \rangle_K \subset \cdots$$

is a infinite ascending chain.
Similarily, (1) $\Leftrightarrow$ (2). $\square$

Lemma 6. If R is Northerian and $\dim R = 0$, then there exist $\mathfrak{m}_i, n_i$ so that $\mathfrak{m}_1^{n_1}\mathfrak{m}_2^{n_2}\cdots\mathfrak{m}_k^{n_k} = \langle 0 \rangle$.

Proof. By primary decomposition, $\langle 0 \rangle = \bigcap_{i=1}^k q_i$ for some primary ideals q_i. Let $\mathfrak{m}_i = \sqrt{q_i}$, since $\mathfrak{m}_i$ finitely generated, say $\mathfrak{m}_i = \langle x_1, \dots, x_k \rangle$. Since $\mathfrak{m}_i = \sqrt{q_i}$, for each x_i, exists r_i so that $x_i^{r_i} \in q_i$. Let $n_i = \max\{r_i\}$ and one could easily see that $\mathfrak{m}_i^{n_i} \subset q_i$. Thus

$$\mathfrak{m}_1^{n_1}\mathfrak{m}_2^{n_2}\cdots\mathfrak{m}_k^{n_k} = \mathfrak{m}_1^{n_1} \cap \mathfrak{m}_2^{n_2} \cap \cdots \cap \mathfrak{m}_k^{n_k} \subseteq q_1 \cap q_2 \cap \cdots \cap q_k = \langle 0 \rangle$$

$\square$

Theorem 22. R is Artinian $\iff$ R is Noetherian with dimension 0.

Proof. In both case we could find maximal ideals $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ not necessarily different in R such that $\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = 0$. So we shall prove tha this implies Artinian $\iff$ Noetherian.

Observe that we have a chain of ideals in R: $R \supset \mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots \supset \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = 0$. Let $M_i = \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{i-1}/\mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_i$ which could be see as an R-module. Moreover, notice that $\mathfrak{m}_i M_i = 0$, so we M_i could be regard as $R/\mathfrak{m}_i$-module. But $R/\mathfrak{m}_i$ is a field, so M_i can be further regarded as a vector space. Hence we could use lemma 5 now:

$$M_i \text{ is Artinian} \iff M_i \text{ is Noetherian.}$$

By definition,

$$0 \to \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_i \to \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_{i-1} \to M_i \to 0$$

exact. By exercise, given $0 \to K \to M \to L$ exact, then M Noetherian (Artinian) $\iff$ K, M Noetherian (Artinian). Thus

$$\begin{aligned}
\mathfrak{m}_0 = R \text{ Artinian} &\iff \mathfrak{m}_1, M_1 \text{ Artinian} \\
&\iff \mathfrak{m}_1\mathfrak{m}_2, M_1, M_2 \text{ Artinian} \\
&\quad \vdots \\
&\iff \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = \langle 0 \rangle,\ M_1, \dots, M_n \text{ Artinian} \\
&\iff \mathfrak{m}_1\mathfrak{m}_2\cdots\mathfrak{m}_n = \langle 0 \rangle,\ M_1, \dots, M_n \text{ Noetherian} \\
&\quad \vdots \\
&\iff \mathfrak{m}_1\mathfrak{m}_2, M_1, M_2 \text{ Noetherian} \\
&\iff \mathfrak{m}_1, M_1 \text{ Noetherian} \iff \mathfrak{m}_0 = R \text{ Noetherian}
\end{aligned}$$

$\square$

1.8.2 DVR (Discrete Valuation Ring)

Def 26.

(1) Let K be a field. A discrete valuation of K is $\nu : K^{\times} \twoheadrightarrow \mathbb{Z}$ ($\nu(0) = \infty$) s.t.

- $\nu(xy) = \nu(x) + \nu(y)$.
- $\nu(x \pm y) = \min\{\nu(x), \nu(y)\}$.

(2) The valuation ring of ν is $R = \{x \in K \mid \nu(x) \geq 0\}$, called a DVR.

Prop 1.8.3.

1. $\nu(1) = 0$:

   Proof. $\nu(1) = \nu(1) + \nu(1) \implies \nu(1) = 0$ ☐

2. $\nu(x) = -\nu(x^{-1})$:

   Proof. $0 = \nu(xx^{-1}) = \nu(x) + \nu(x^{-1})$ ☐

3. $\nu(x) = 0 \iff x$ is a unit, so $\mathfrak{m} = \{x \in R \mid \nu(x) > 0\}$ is the unique maximal ideal

   Proof. "$\Rightarrow$": $\nu(x) = 0 \implies \nu(x^{-1}) = 0 \implies x^{-1} \in R$
   "$\Leftarrow$": Then $\nu(x^{-1}), \nu(x) \geq 0.$, so $\nu(x) = -\nu(x) \leq 0 \implies \nu(x) = 0$. ☐

4. Let $t \in R$ with $\nu(t) = 1$, then $\mathfrak{m} = \langle t \rangle$. More over, each element $x \in \mathfrak{m}$ could be uniquely written as $x = t^k u$ where u is an unit.

   Proof. $\forall\, x \in \mathfrak{m}, \nu(x) = k > 0$, so $\nu\big(x(t^k)^{-1}\big) = \nu(x) - k\nu(t) = 0 \implies x = t^k u$, where u is unit in R. ☐

5. Let $I \subseteq \mathfrak{m}$ and define $m = \min\{l \in \mathbb{N} \mid x = t^l u, \forall\, x \in I\}$. Then $I = \langle t^m \rangle$.

   Proof. "$\subseteq$": Immediately by the previous statement. "$\supseteq$": Let $x = t^m u$ be the one letting $l = m$, then $t^m = xu'$ for some u' since where u is a unit. ☐

Prop 1.8.4. *R is a DVR $\iff$ R is 1-dimensional normal, Noetherian local integral domain.*

Proof.

"$\Rightarrow$":
$$\begin{tikzcd} \text{DVR} \arrow[r, Rightarrow] & \text{PID} \arrow[r, Rightarrow] \arrow[dr, Rightarrow] & \text{UFD} \arrow[r, Rightarrow] & \text{normal} \\ & & \text{Noetherian} & \end{tikzcd}$$
Where UFD $\implies$ normal by theorem 16.

Now if P is a prime ideal in R, then by 5. of proposition 1.8.3, $P = \langle t^k \rangle = \mathfrak{m}^k$ where $\mathfrak{m}$ is the maximal ideal. Then $P = \sqrt{P} = \sqrt{\mathfrak{m}^k} = \mathfrak{m}$ since $\mathfrak{m}$ maximal. Thus the only prime ideals are $\{0, \mathfrak{m}\}$ and thus R has dimension 1.

" $\Leftarrow$ ": Let $\mathfrak{m}$ be the unique maximal ideal. Then $\operatorname{Spec} R = \{0, \mathfrak{m}\}$. If $\mathfrak{m} = \mathfrak{m}^2$ then since $\operatorname{Jac} R = \mathfrak{m}$, $\mathfrak{m} = 0$ by Nakayama's lemma, so $\mathfrak{m}^2 \neq \mathfrak{m}$. Pick $t \in \mathfrak{m}^2 \setminus \mathfrak{m}$. We claim that $\langle t \rangle = \mathfrak{m}$. If not, then $M \triangleq \mathfrak{m}/\langle t \rangle \neq 0$. See M as an R-module and consider $S \triangleq \{\operatorname{Ann}(\bar{x}) \mid \bar{x} \neq 0 \in M\}$. Since R Noetherian, there is a maximal element, say $I = \operatorname{Ann}(\bar{x})$.

We shall prove that I is prime. If not, then there are $ab \in I$ but $a, b \notin I$, which is to say that $ab\bar{x} = 0$ but $b\bar{x} \neq 0$. Notice the obvious fact $\operatorname{Ann}(\bar{x}) \subseteq \operatorname{Ann}(b\bar{x})$, but $b\bar{x} \neq 0$ and by the maximality of $\operatorname{Ann}(\bar{x})$, $\operatorname{Ann}(\bar{x}) = \operatorname{Ann}(b\bar{x})$, then $a \in \operatorname{Ann}(b\bar{x}) = \operatorname{Ann}(\bar{x}) \implies ax = 0$, which is a contradiction, thus I is prime.

So, if $M \neq 0$, then we could pick $\bar{x}$ such that $\operatorname{Ann}(\bar{x})$ is a prime, and thus $\operatorname{Ann}(\bar{x}) = \mathfrak{m}$. Now, $x\mathfrak{m} \subset \langle t \rangle = tR$, so $J \triangleq (x/t)\mathfrak{m} \subset R$ in the field of fraction.

- If $J = R$, then there exists $y \in \mathfrak{m}$ so that $xy/t = 1 \implies t = xy \in M^2$, which is a contradiction the definition of t.
- If $J \neq R$, then J is contained in the maximal ideal $\mathfrak{m}$, so $(x/t)\mathfrak{m} = \mathfrak{m}$. Since $\mathfrak{m}$ finitely generated, $\mathfrak{m} = \langle y_1, \ldots, y_k \rangle$. Then $(x/t)y_i = \sum a_{i,j} y_j$. Using the routine determinant trick, $f(x/t)m = 0, \forall\, m \in M \implies f(x/t) = 0$ for some monic polynomial $f \in R[x]$. Then x/t is integral over R. But then $x/t \in R$ since R normal, and thus $x \in Rt$, which contradict how we picked x.

Thus $\mathfrak{m} = \langle t \rangle$ is principle. Now, by exercise problem, $\bigcap_{n=0}^{\infty} \mathfrak{m}^n = 0$, so for each $x \in R$, exists an unique k so $x \in \mathfrak{m}^k$ but $x \notin \mathfrak{m}^{k+1}$. Write $x = t^k u$, then $u \notin \mathfrak{m}$ implies that u is an unit. One could easily see that this representation is actually unique.

Finally, define $\nu(x) = k$, one could easily checked that this definition extends well to the field of fraction, so R is a DVR. □

1.8.3 Dedekind domains

Def 27. A Dedekind domain is a Noetherian normal domain of dim 1.

Def 28. Let R be an integral domain and $K = \operatorname{Frac}(R)$. A nonzero R-submodule I of K is called a fractional ideal of R if $\exists\, 0 \neq a \in R$ s.t. $aI \subset R$.

Eg 1.8.1. If $I = \langle f_1, \ldots, f_n \rangle_R$, a finitely generated R-module with $f_i = \frac{a_i}{b_i} \in K$, then $a = b_1 b_2 \cdots b_n$ and $aI \subset R \implies I$ is fractional.

In general, if R is a Noetherian, then every fractional ideal I of R is finitely generated.

Def 29. A fractional ideal I of R is invertible if $\exists\, J$: a fractional ideal of R s.t. $IJ = R$.

Prop 1.8.5.

1. If I is invertible, then $J = I^{-1}$ is unique and equals $J = (R : I) \triangleq \{a \in K \mid aI \subset R\}$.

   Proof. $J \subseteq (R : I) \subseteq (R : I)R \subseteq (R : I)IJ \subseteq RJ = J \implies J = (R : I)$ □

2. If I is invertible, then I is a finitely generated R-module.

   Proof. If $I(R : I) = R$ then $1 = \sum_{i=0}^{k} x_i y_i$, for some $x_i \in I$ and $y_i \in (R : I)$. Then, $\forall\, x \in I$, $x = \sum_{i=0}^{k} \underbrace{(xy_i)}_{\in R} x_i$ Thus $I = \langle x_0, \ldots, x_k \rangle_R$. □

Prop 1.8.6. Let R be a local domain but not a field, $K = \operatorname{Frac}(R)$. Then R is a DVR $\iff$ every nonzero fractional ideal I of R is invertible.

Proof. " $\Rightarrow$ ": Let I be fractional ideal of R, then $\exists\, a \in R$ s.t. $aI \subseteq R$. Since R is a DVR which is not a field, the maximal ideal $\mathfrak{m} = \langle t \rangle$ for some $t \neq 0$. We know from proposition 1.8.3 that $a = t^k u$ where u is a unit in R.

- If $aI = R$, then let $J \triangleq \langle a \rangle_R$ and $JI = R$.
- If $aI \neq R$, then $aI = \langle t^l \rangle$ again since R is DVR. Then $I = \langle t^{l-k} \rangle$, let $J = \langle t^{k-l} \rangle$ and we have $IJ = R$.

" $\Leftarrow$ ": First, for any $I \subset R$, which is obvious a fractional ideal, so I is invertible, and hence by proposition 1.8.5, I is finitely generated, thus R is Noetherian.

Let $\mathfrak{m}$ be the unique maximal ideal, then if $\mathfrak{m}^2 = \mathfrak{m}$, since R Noetherian, by Nakayama's lemma, $\mathfrak{m} = 0$, which contradicts the fact that R is not a field.

Thus pick $t \in \mathfrak{m} \setminus \mathfrak{m}^2$. Consider $t\mathfrak{m}^{-1}$ which is in R since $t \in \mathfrak{m}$. If $t\mathfrak{m}^{-1} \subseteq \mathfrak{m}$, then $t\mathfrak{m}^{-1}\mathfrak{m} = tR \subseteq \mathfrak{m}^2 \implies t \in \mathfrak{m}^2$, which is a contradiction. So $t\mathfrak{m}^{-1} = R \implies tR = \mathfrak{m}$. Using the same construction ν in proposition 1.8.4, R is a DVR. □

Theorem 23. Let R be an integral domain and $K = \mathrm{Frac}(R)$. TFAE

(a) R is a Dedekind domain.

(b) R is Noetherian and R_P is a DVR for all $P \in \operatorname{Spec} R$.

(c) Every nonzero fractional ideal of R is invertible.

(d) Every nonzero proper ideal of R can be written (uniquely) as a product of powers of prime ideals.

Proof.

(a)$\Leftrightarrow$(b): Recall that R is a Dedekind domain if R is (1) Noetherian, (2) normal, (3) integral domain with (4) Dimension 1. And R_p is a DVR if it is a local Dedekind domain. All of these are guaranteed by proposition 1.6.1, where (4) is by the correspondence of prime ideals.

(b)$\Leftrightarrow$(c): We need a small lemma:

Lemma 7. If I is finitely generated, then $(R_P : I_P) = (R : I)_P$.

Proof. Notice that I_P is then a finitely generated R_P-module, and thus by example 1.8.1 $(R_P : I_P)$ is a fractional ideal. Then $(R : I)_P = \{x \mid xI \subset R\}_P = \{x \mid xI_P \subset R_P\} = (R_P : I_P)$. □

Now,

$$\forall\, P \in \operatorname{Spec} R,\ R_P = I_P(R_P : I_P) = I_P(R : I)_P = (I(R : I))_P \iff I(R : I) = R$$

by corollary 1.6.1.

(a)(b)(c)$\Rightarrow$(d):

Existence: Since R is Noetherian, $I = q_1 \cap \cdots \cap q_n = q_1 q_2 \cdots q_n$ Where the intersection equals product is because if we let $P_i \triangleq \sqrt{q_i}$, then $P_i \in \operatorname{Spec} R$, and $P_i \neq 0$ is always maximal, so $P_i + P_j = R$, which implies $q_i + q_j = R$ (as in proposition 1.8.1).

Now, we shall prove that $q_i = P_i^{k_i}$ for some k_i. By (b), each R_{P_i} is a DVR, which has primary ideals of the form $\{\mathfrak{m}^k\}$. By proposition 1.6.1, primary ideals are correspondent in localization, so $(q_i)_{P_i} = \mathfrak{m}^k \iff q_i = P_i^k$. Thus $k_i = k$ is what we want. Then we could write $I = P_1^{k_1} \cdots P_n^{k_n}$.

Uniqueness: Actually, the factorization into product of invertible prime ideal is unique in any integral domain.

If $P_1 P_2 \cdots P_k = Q_1 Q_2 \cdots Q_r$, then $P_1 P_2 \cdots P_k = P_1 \cap \cdots \cap P_k \in Q_1$, so there is one, say $P_1 \subset Q_1$. Assume Q_1 is the minimal among Q_i. Similarly we could find $Q_i \subset P_1$. But then

$Q_i \subseteq Q_1$. Since Q_i minimal, $Q_i = Q_1$. Now, since these ideals are invertible, $P_2P_3\cdots P_k = Q_2Q_3\cdots Q_r$. By induction, the proof is completed.

(d)⇒(c):

Lemma 8. Let P_i be fractional ideals. If $P_1P_2\cdots P_n = \langle a\rangle$ is principle, then P_i are invertible.

Proof. P_i^{-1} is actually $a^{-1}P_1P_2\cdots P_{i-1}P_{i+1}\cdots P_n$. □

First we prove that p is maximal if p is prime and invertible.

If not, let $p + aR = P_1\cdots P_k$ and $p + a^2R = Q_1\cdots Q_r$ with $a \notin p$. Since $P_i, Q_j \subset p$, passing to the quotient R/p, we have $\bar{a} = P_1\cdots P_k$, $\bar{a}^2 = Q_1\cdots Q_r$. Using the uniqueness of factorization, which only requires R/p to be an integral domain (which is the case) and P_i, Q_j be invertible (by lemma above), by $\bar{a}^2 = P_1^2\cdots P_k^2 = Q_1\cdots Q_r$, we have $2k = r$ and we could assume $Q_{2i-1} = Q_{2i} = P_i$. This shows that $p + a^2R = (p + aR)^2 \subseteq p^2 + aR$. So $p \subseteq p+a^2R \subseteq p^2+aR$. Now, if $x \in p$, $x = y+az$ for some $y \in p^2, z \in R$. Then $az = x-y \in p$ but $a \notin p$, so $z \in p$. Thus we could refine the relation to $p \subseteq p^2+ap$. But then $p \subseteq p(p+aR)$, since p invertible, $R \subseteq p + aR$ which implies that $p + aR = R$. Thus p is maximal.

Now, we show that every prime ideal p is invertible. By assumption, let $a \in p$, then $Ra = P_1\cdots P_k$, so by the lemma above, each P_i is invertible and thus maximal by the previous paragraph. Then $P_1\cdots P_k \subset p$, so again $P_i \subset p$, which implies $P_i = p$. Thus p is invertible.

Finally, since each ideal is the product of prime ideals, and we've just prove that priome ideals are invertible, any ideal are invertible. For a fractional ideal I, $aI \subseteq R \implies \exists\, J$, $aIJ = R \implies I(aJ) = R$, which is to say that I is invertible.

□

2 Introduction to Homological Algebra

2.1 Projective, Injective and Flat modules (week 14)

Def 30.

- $M \in \mathbf{Mod}_R$ is **projective** if $\mathrm{Hom}(M, \cdot)$ preserves the *right* exactness.
- $N \in \mathbf{Mod}_R$ is **injective** if $\mathrm{Hom}(\cdot, N)$ preserves the *right* exactness.
- $M \in \mathbf{Mod}_R$ is **flat** if $M \otimes \cdot$ preserves the *left* exactness.

Fact 2.1.1.

- M is projective $\iff$ $$\begin{tikzcd} & M \arrow[dl, "\exists\, \tilde{f}"'] \arrow[d, "f"] & \\ M_2 \arrow[r] & M_3 \arrow[r] & 0 \end{tikzcd}$$
- N is injective $\iff$ $$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] \arrow[d, "g"'] & M_2 \arrow[dl, "\exists\, \tilde{g}"] \\ & N & \end{tikzcd}$$
- free $\implies$ projective: If $X = \{x_i \mid i \in \Lambda\}$ and $f : x_i \mapsto a_i$. Since β onto, exists b_i so that $\beta(b_i) = a_i$. we can then set $\tilde{f} : x_i \mapsto b_i$ by the universal property of free module.
$$\begin{tikzcd} & F(X) \arrow[dl, "\exists\, \tilde{f}"'] \arrow[d, "f"] & \\ M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$
- free $\implies$ flat: Let $F \cong R^{\oplus\Lambda}$ be a free module, and M_1, M_2 be two modules such that $0 \to M_1 \to M_2$. Since $R \otimes_R M \cong M$, we have
$$\begin{aligned} & 0 \to M_1 \to M_2 && \text{exact} \\ \implies & 0 \to R \otimes M_1 \to R \otimes M_2 && \text{exact} \\ \implies & 0 \to \bigoplus_{i\in\Lambda} R \otimes M_1 \to \bigoplus_{i\in\Lambda} R \otimes M_2 && \text{exact} \\ \overset{(a)}{\implies} & 0 \to R^{\oplus\Lambda} \otimes M_1 \to R^{\oplus\Lambda} \otimes M_2 && \text{exact} \\ \implies & 0 \to F \otimes M_1 \to F \otimes M_2 && \text{exact} \end{aligned}$$
Where (a) is by the fact that $(A \oplus B) \otimes C \cong (A \otimes C) \oplus (B \otimes C)$. Thus F flat.
- If S is a multiplication closed set in R with $1 \in S$, then
$$0 \to M \to N \to L \to 0 \implies 0 \to M_S \to N_S \to L_S \to 0.$$
We know that $M_S \cong R_S \otimes_R M$. So R_S is a flat R-module. e.g. $\mathbb{Q}$ is a flat $\mathbb{Z}$-module.

For any $M \in \mathbf{Mod}_R$, a projective module N such that $N \to M \to 0$ could be easily found: Simply let $N = F$, a free module on the generating set of M.

Now we shall ask for any module M, does there exist $N \in \mathbf{Mod}_R$ such that N is injective and $0 \to M \to N$?

Theorem 24 (Baer's criterion)**.** N is injective $\iff$ $\forall\, I \subset R$, and a homomorphism f, there exists a homomorphism h such that the following diagram commutes:

$$\begin{tikzcd} 0 \arrow[r] & I \arrow[r] \arrow[d, "f"'] & R \arrow[dl, dashed, "\exists\, h"] \\ & N & \end{tikzcd}$$

Proof. "$\Rightarrow$": See I as an R module, then it is obivous by the definition of injective module.

"$\Leftarrow$: Consider the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r] \arrow[d, "g"] & M_2 \\ & N & \end{tikzcd}$$

Let $S \triangleq \{(M, \rho) \mid M_1 \subseteq M \subseteq M_2 \text{ and } \rho : M \to N \text{ extends } g\} \neq \varnothing$ since $(M_1, g) \in S$.

By the routinely proof using Zorn's lemma, exists a maximal element $(M^*, \mu) \in S$.

We claim that $M^* = M_2$. If not, pick $a \in M_2 \setminus M^*$ and let $M' \triangleq M^* + Ra \supsetneq M^*$, $I \triangleq \{r \in R \mid ra \in M^*\}$. Define $f : I \to N$ with $r \mapsto \mu(ra)$. Then we have an extension $h : R \to N$ of f.

Now, let $\mu' : M' \to N = x + ra \mapsto \mu(x) + h(r)$. We shall prove that this map is well-defined: If $x_1 + r_1 a = x_2 + r_2 a$, then $(r_1 - r_2)a = x_2 - x_1 \in M \implies r_1 - r_2 \in I$. So $h(r_1) - h(r_2) = f(r_1 - r_2) = \mu((r_1 - r_2)a) = \mu(x_2) - \mu(x_1)$, which prove μ' is well defined, and the existence of μ' contradicts the fact that (M^*, μ) is maximal. □

Def 31. M is **divisible** if $\forall x \in M, r \in R \setminus \{0\}$, there exists $y \in M$ such that $x = ry$, i.e. $rM = M \quad \forall r \in R \setminus \{0\}$.

Prop 2.1.1.

1. Every injective module N over an integral domain is divisible.

   Proof. For any $x_0 \in N$ and $r_0 \in R \setminus \{0\}$. Let $I = \langle r_0 \rangle \subset R$. As long as R is an integral domain, $I \cong R$ as an R-module, so the R-module homomorphism $f : I \to N = rr_0 \mapsto rx_0$ is well-defined. Since N injective, this map extends to $h : R \to N$. Let $y_0 \triangleq h(1)$, then $r_0 y_0 = r_0 h(1) = h(r_0) = x_0$. Thus N injective. □

2. Every divisible module N over an PID is injective.

   Proof. For any $I \subseteq R$ and a homomorphism $f : I \to N$, if $I = 0$ then $h = x \mapsto 0$ is always an extension of f. So assume $I \neq 0$. Since R is a PID, $I = \langle r_0 \rangle$ for some $r_0 \neq 0 \in R$. By the fact that N divisible, exists $y_0 \in N$ such that $r_0 y_0 = x_0 \triangleq f(r_0)$.

   Now we could define $h : R \to N$ by $1 \mapsto y_0$. Then $h(r_0) = r_0 h(1) = r_0 y_0 = x_0$, thus h is an extension of f and N injective. □

3. If R is a PID, then any quotient N of a injective R-module M is injective.

   Proof. By 2., $rM = M$ for any $r \neq 0$, thus $rN = N$ for any $r \neq 0$, and hence N injective. □

Theorem 25. For any $M \in \mathbf{Mod}_R$, there exists an injective module N containing M.

Proof.

Case 1: $R = \mathbb{Z}$.

Let $X = \{x_i\}_{i \in \Lambda}$ be a generating set for M and F is free on X. Let f be the natural map from F to M. then $M \cong F/\ker f$.

Define $F' = \bigoplus_{i \in \Lambda} \mathbb{Q} e_i \supset F$, which is obviously a divisible $\mathbb{Z}$-module. Then $M \subseteq F'/\ker f \triangleq M'$, where M' is injective by proposition 2.1.1.

Case 2: R arbitrary.

We can regard any M as a $\mathbb{Z}$-module, then there exists an injective module $N_0 \supset M$. Now, we have an R-module $N \triangleq \mathrm{Hom}_{\mathbb{Z}}(R, N_0)$ with multiplication $rf \triangleq x \mapsto f(xr)$.

We claim that N is injective. For any $f : M_1 \to N$, and a homomorphism $\alpha : M_1 \to M_2$, first we can regard α as a $\mathbb{Z}$-module homomorphism, then we define $f' : M_1 \to N_0$ as $x \mapsto f(x)(1)$. Since N_0 injective (in $\mathbf{Mod}_{\mathbb{Z}}$), there exists a $\mathbb{Z}$-module homomorphism h' from M_2 to N_0.

$$
\begin{tikzcd}
 & x \arrow[dddd, bend right, mapsto] \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] & & \\
 & {} & & \\
0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[d, "f"] & M_2 \arrow[dl, dashed, "\exists\, h(?)"] & \\
 & N \arrow[r, phantom, "\cong"] \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & \mathrm{Hom}_{\mathbb{Z}}(R, N_0) & \\
 & f(x) & &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & x \arrow[dddd, bend right, mapsto] \arrow[d, phantom, "\rotatebox{-90}{$\in$}"] & \\
 & {} & \\
0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[d, "f'"] & M_2 \arrow[dl, "\exists\, h'"] \\
 & N_0 \arrow[d, phantom, "\rotatebox{90}{$\in$}"] & \\
 & f(x)(1) &
\end{tikzcd}
$$

Now, define

$$
\begin{aligned}
h : M_2 &\longrightarrow N \\
y &\longmapsto h(y) : R \longrightarrow N_0 \\
&\qquad\qquad\quad 1 \longmapsto h'(y) \\
&\qquad\qquad\quad r \longmapsto h'(ry)
\end{aligned}
$$

We check that h is well-defined.

- $h(y) \in \mathrm{Hom}_{\mathbb{Z}}(R, N_0)$

$$h(y)(r_1 + r_2) = h'((r_1 + r_2)y) = h'(r_1 y + r_2 y) = h'(r_1 y) + h'(r_2 y) = h(y)(r_1) + h(y)(r_1)$$

- $h \in \mathrm{Hom}_R(M_2, N)$

$$
\begin{aligned}
h(r_1 y_1 + y_2)(r) &= h'(r(r_1 y_1 + y_2)) = h'(r r_1 y_1 + r y_2) \\
&= h'(r r_1 y_1) + h'(r y_2) \\
&= h(y)(r r_1) + h(y_2)(r) \\
&= (r_1 h(y))(r) + h(y_2)(r)
\end{aligned}
$$

- Show diagram commute $f = h \circ \alpha$. Fix $y \in M_1$, then $\forall\, r \in R$:

$$
\begin{aligned}
(h \circ \alpha)(y)(r) = h(\alpha(y))(r) &= h'(r\alpha(y)) \\
&= h'(\alpha(ry)) = f'(ry) \\
&= f(ry)(1) = rf(y)(1) \\
&= f(y)(r)
\end{aligned}
$$

Thus N injective.

Now, notice that $\mathrm{Hom}_{\mathbb{Z}}(R, \cdot)$ is a left exact functor, so $M \hookrightarrow N_0$ implies $\mathrm{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, N_0)$, thus $M \cong \mathrm{Hom}_R(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, M) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}}(R, N_0) = N$. $\square$

Prop 2.1.2. TFAE

1. M is projective.
2. Every exact sequence $0 \to M_1 \to M_2 \to M \to 0$ split.

3. $\exists\, M'$ s.t. $M \oplus M' \cong F$: free.

Proof.
(1) $\Rightarrow$ (2) : Since M projective, the map λ with $\beta \circ \lambda = \mathrm{Id}$ exists in the following diagram:

$$\begin{tikzcd} & M \arrow[dl, "\exists\,\lambda"'] \arrow[d, "\mathrm{Id}"] & \\ M_2 \arrow[r, "\beta"] & M \arrow[r] & 0 \end{tikzcd}$$

Then λ is a lifting, so $M_2 \cong M_1 \oplus M$ and $0 \to M_1 \to M_2 \to M \to 0$ split.

(2) $\Rightarrow$ (3): Let F be a free module on a generating set of M, and $\beta :: F \to M$ be the natural map, then $0 \to \ker\beta \to F \to M \to 0$ split, so $F \cong \ker\beta \oplus M$.

(3) $\Rightarrow$ (1): For any $M_2 \to M_3 \to 0$, since $M' \oplus M$ free and thus projective, λ' exists in the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] & M' \oplus M \arrow[r, shift right, "\pi"'] \arrow[d, "\exists\,\lambda'"] & M \arrow[l, shift right, "\mu"'] \arrow[r] \arrow[d, "f"] & 0 \\ & & M_2 \arrow[r, "\beta"] & M_3 \arrow[r] & 0 \end{tikzcd}$$

Define $\lambda = \lambda' \circ \mu$. Then $\beta \circ \lambda = \beta \circ \lambda' \circ \mu = f \circ \pi \circ \mu = f$. $\square$

Prop 2.1.3. TFAE

1. M is injective.
2. Each exact sequence $0 \to M \to M_2 \to M_3 \to 0$ split.

Proof. (1) $\Rightarrow$ (2): Similar to the projective case, μ exists in the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\alpha"] \arrow[d, "\mathrm{Id}"] & M_2 \arrow[dl, dashed, "\exists\,\mu"] \\ & M & \end{tikzcd}$$

So $M_2 = M \oplus M_3$.

(2) $\Rightarrow$ (1): By theorem 25, there is a module $N \subset M$ so that N is injective.

Consider $\begin{tikzcd} 0 \arrow[r] & M \arrow[r, shift left, "i"] & N \arrow[l, shift left, "\exists\,\mu"] \arrow[r] & \operatorname{coker} i \arrow[r] & 0 \end{tikzcd}$ split exact and $\mu \circ i = \mathrm{Id}_M$. Since N injective, h' exists in the following diagram:

$$\begin{tikzcd} 0 \arrow[r] & M_1 \arrow[r, "\alpha"] \arrow[d, "f"] \arrow[dd, bend right=60, "i \circ f"'] & M_2 \arrow[ddl, "\exists\,h'"] \\ & M \arrow[d, shift right, "i"'] & \\ & N \arrow[u, shift right, "\mu"'] & \end{tikzcd}$$

Let $h = \mu \circ h'$, then $h \circ \alpha = \mu \circ h' \circ \alpha = \mu \circ i \circ f = f$. $\square$

Prop 2.1.4. projective $\implies$ flat.

Proof. Observe that $\bigoplus_{i\in\Lambda} M_i$ is flat if and only if M_i is flat for each i, since if $0 \to N_1 \xrightarrow{\alpha} N_2$ exact, then

$$\begin{tikzcd}
0 \arrow[r] & (\bigoplus M_i) \otimes N_1 \arrow[r, "1\otimes\alpha"] \arrow[d, equal] & (\bigoplus M_i) \otimes N_2 \arrow[d, equal] \\
0 \arrow[r] & \bigoplus(M_i \otimes N_1) \arrow[r, "\oplus(1\otimes\alpha)"] \arrow[d, Leftrightarrow] & \bigoplus(M_i \otimes N_2) \\
0 \arrow[r] & M_i \otimes N_1 \arrow[r, "1\otimes\alpha"] & M_i \otimes N_2 & \forall\, i \in \Lambda
\end{tikzcd}$$

If M is projective, then by proposition 2.1.2 $\exists\, M'$ such that $M \oplus M' \cong F$ is free. Since free implies flat, by above, M is flat. □

Def 32.

- A chain complex $C_\bullet$ of R-modules is a sequence and maps:

$$C_\bullet : \cdots \to C_{n+1} \xrightarrow{d_{n+1}} C_n \xrightarrow{d_n} C_{n-1} \to \cdots \to C_1 \xrightarrow{d_1} C_0 \to 0$$

  with $d_n \circ d_{n+1} = 0, \quad \forall\, n$. (i.e. $\operatorname{Im} d_{n+1} \subseteq \ker d_n$)

  Then define

  - $Z_n(C_\bullet) \triangleq \ker d_n$ is the n-cycle.
  - $B_n(C_\bullet) \triangleq \operatorname{Im} d_{n+1}$ is the n-boundary.
  - $H_n(C_\bullet) \triangleq Z_n(C_\bullet)/B_n(C_\bullet)$ is called the n-th homology.

- A cochain complex $C^\bullet$ of R-modules is a sequence and maps:

$$C^\bullet : 0 \to C^0 \xrightarrow{d^1} C^1 \to \cdots \to C^{n-1} \xrightarrow{d^n} C^n \xrightarrow{d^{n+1}} C^{n+1} \to \cdots$$

  with $d^{n+1} \circ d^n = 0, \quad \forall\, n$. (i.e. $\operatorname{Im} d^n \subseteq \ker d^{n+1}$)

  Then define

  - $Z^n(C^\bullet) \triangleq \ker d^{n+1}$ is the n-cocycle.
  - $B^n(C^\bullet) \triangleq \operatorname{Im} d^n$ is the n-coboundary.
  - $H^n(C^\bullet) \triangleq Z^n(C^\bullet)/B^n(C^\bullet)$ is called the n-th cohomology.

- $\varphi : C_\bullet \to \tilde{C}_\bullet$ is a chain map if the following diagram commutes:

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "\varphi_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[d, "\varphi_n"] & C_{n-1} \arrow[r] \arrow[d, "\varphi_{n-1}"] & \cdots \\
\cdots \arrow[r] & \tilde{C}_{n+1} \arrow[r, "\tilde{d}_{n+1}"] & \tilde{C}_n \arrow[r, "\tilde{d}_n"] & \tilde{C}_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

  Observe that $\varphi_n(\ker d_n) \subseteq \ker \tilde{d}_n$ and $\varphi_n(\operatorname{Im} d_{n+1}) \subseteq \operatorname{Im} \tilde{d}_{n+1}$. This will induce the following maps:

$$\begin{aligned} \varphi_* : \quad H_n(C_\bullet) \quad &\to \quad H_n(\tilde{C}_\bullet) \\ x + B_n(C_\bullet) &\mapsto \varphi_n(x) + B_n(\tilde{C}_\bullet) \end{aligned}$$

- $f : C_\bullet \to \tilde{C}_\bullet$ is null homotopic if $\exists\, s_n : C_n \to \tilde{C}_{n+1}$ s.t. $f_n = \tilde{d}_{n+1} \circ s_n + s_{n-1} \circ d_n, \quad \forall\, n$.

$$\begin{tikzcd}
\cdots \arrow[r] & C_{n+1} \arrow[r, "d_{n+1}"] \arrow[d, "f_{n+1}"] & C_n \arrow[r, "d_n"] \arrow[d, "f_n"] \arrow[dl, red, "s_n"] & C_{n-1} \arrow[r] \arrow[d, "f_{n-1}"] \arrow[dl, red, "s_{n-1}"] & \cdots \\
\cdots \arrow[r] & \tilde{C}_{n+1} \arrow[r, "d_{n+1}"] & \tilde{C}_n \arrow[r, "d_n"] & \tilde{C}_{n-1} \arrow[r] & \cdots
\end{tikzcd}$$

Prop 2.1.5. If f is null homotopic, then $f_* = 0$.

Proof. $f_*(x) = \tilde{d}_{n+1}s_n(x) + s_{n-1}d_n(x) = \tilde{d}_{n+1}s_n(x) \in B_n(\tilde{C}_\bullet) \implies f_*(\bar{x}) = 0$. □

- Two chain map $f, g : C_\bullet \to \tilde{C}_\bullet$ are homotopic if $f - g$ is null homotopic. ($f_* = g_*$)
- Let $M \in \mathbf{Mod}_R$. A projection resolution of M is an exact sequence:

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\alpha} M \to 0$$

where P_i is projective for all i.

For any M, projection resolution always exists. Let P_0 be a free module on the generators of M. We get $P_0 \xrightarrow{\alpha} M \to 0$. Similarly, let P_1 be free on $\ker\alpha$, then we could extend the map to $P_1 \to P_0 \to M \to 0$. Continue the process we would get a diagram as below, where K_i are the kernels:

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[rr] \arrow[dr] & & P_1 \arrow[rr] \arrow[dr] & & P_0 \arrow[r] & M \arrow[r] & 0 \\
& & K_1 \arrow[ur] \arrow[dr] & & K_0 \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

Theorem 26 (Comparison theorem)**.** Given two chain as following:

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, dashed, "\exists f_2"] & P_1 \arrow[r, "d_1"] \arrow[d, dashed, "\exists f_1"] & P_0 \arrow[r, "\alpha"] \arrow[d, dashed, "\exists f_0"] & M \arrow[r] \arrow[d, "f"] & 0 & \text{(projective resolution)} \\
\cdots \arrow[r] & \tilde{C}_2 \arrow[r, "d'_2"] & \tilde{C}_1 \arrow[r, "d'_1"] & \tilde{C}_0 \arrow[r, "\alpha'"] & N \arrow[r] & 0 & \text{(exact sequence)}
\end{tikzcd}$$

Then $\exists\, f_i : P_i \to C_i$ s.t. $\{f_i\}$ forms a chain map making the completed diagram commutes. And any two such chain maps are homotopic.

Proof. Using induction on n.

For $n = 0$, the existence of f_0 is guaranteed by the definition of projective module.

$$\begin{tikzcd}
& P_0 \arrow[dl, dashed, "\exists f_0"'] \arrow[d, "f \circ \alpha"] & \\
C_0 \arrow[r] & N \arrow[r] & 0
\end{tikzcd}$$

For $n > 0$, we claim that $f_{n-1}d_n(P_n) \subseteq \operatorname{Im} d'_n$, since $d'_{n-1}f_{n-1}d_n(x) = f_{n-2}d_{n-1}d_n(x) = 0$ and by the fact that C is exact, $f_{n-1}d_n(x) \in \ker d'_{n-1} = \operatorname{Im} d'_n$. So using the diagram and again by the definition of projective module, f_n exists.

$$\begin{tikzcd}
& P_n \arrow[dl, dashed, "\exists f_n"'] \arrow[d, "f_{n-1} \circ d_n"] & \\
C_n \arrow[r] & \operatorname{Im} d'_n \arrow[r] & 0
\end{tikzcd}$$

Now, for another chain map $\{g_i : P_i \to C_i\}$, we shall construct suitable $\{s_n\}$ to prove they are homotopic. For $s_{-1} : M \to C_0$ we could simply pick the zero map. Again, if we could prove that $\operatorname{Im}(g_n - f_n - s_{n-1}d_n) \subset \ker d'_n$, then by the definition of projective module, we would obtain s_n with

$$d_{n+1}s_n = g_n - f_n - s_{n-1}d_n \implies g_n - f_n = d_{n+1}s_n + s_{n-1}d_n$$

immediately. For this we calculate $d'_n(g_n - f_n - s_{n-1}d_n) = g_{n-1}d_n - f_{n-1}d_n - d'_n s_{n-1}d_n$. Notice that $d'_n s_{n-1} = g_{n-1} - f_{n-1} - s_{n-2}d_{n-1}$, and with $d_{n-1}d_n = 0$, we get $d'_n(g_n - f_n - s_{n-1}d_n) = 0$. $\square$

Def 33. Let $M \in \mathbf{Mod}_R$ and $\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\alpha} M \to 0$ be a projective resolution of M. Fix $N \in \mathbf{Mod}_R$. Applying $\mathrm{Hom}_R(\cdot, N)$ will get a complex:

$$0 \to \mathrm{Hom}_R(M,N) \xrightarrow{\bar{\alpha}} \mathrm{Hom}_R(P_0,N) \xrightarrow{\bar{d}_1} \mathrm{Hom}_R(P_1,N) \to \cdots$$

Define

- $\mathrm{Ext}^0_R(M,N) = \ker \bar{d}_1 = \mathrm{Im}\,\bar{\alpha} \cong \mathrm{Hom}_R(M,N)$.
- $\mathrm{Ext}^n_R(M,N) = H^n(\mathrm{Hom}(P_\bullet, N)), \quad \forall\, n \geq 1$.

Theorem 27 (Indenpedency of the choice of projective resolutions)**.** $\mathrm{Ext}^n(M,N)$ is independent of the choice of the projective resolution used.

Proof. First, consider two projective resolutions of $M, \tilde{M}$, and map $f : M \to \tilde{M}$, and two liftings $\{f_i\}, \{g_i\}$. Use $\bar{\cdot}$ to denote the natural transformation from $X \to Y$ to $\mathrm{Hom}(Y,N) \to \mathrm{Hom}(X,N)$ by $\bar{f} \triangleq g \mapsto g \circ f$. Then we shall prove that $\bar{f_\bullet}^* = \bar{g_\bullet}^*$, which is to say $\bar{f_\bullet}^*$ is independent of the lifting used.

By comparison theorem (26), $\{f_i\}, \{g_i\}$ are homotopic, and we could write down the diagram below:

$$\begin{tikzcd}
\cdots \arrow[r] & P_2 \arrow[r, "d_2"] \arrow[d, shift right, "f_2"'] \arrow[d, shift left, "g_2"] & P_1 \arrow[r, "d_1"] \arrow[d, shift right, "f_1"'] \arrow[d, shift left, "g_1"] \arrow[dl, "s_1"'] & P_0 \arrow[r, "\alpha"] \arrow[d, shift right, "f_0"'] \arrow[d, shift left, "g_0"] \arrow[dl, "s_0"'] & M \arrow[r] \arrow[d, "f"] & 0 \\
\cdots \arrow[r] & \tilde{P}_2 \arrow[r, "\tilde{d}_2"] & \tilde{P}_1 \arrow[r, "\tilde{d}_1"] & \tilde{P}_0 \arrow[r, "\tilde{\alpha}"] & \tilde{M} \arrow[r] & 0
\end{tikzcd}$$

Notice that $\bar{\cdot}$ act linearly, that is, $\overline{f+g} = \bar{f} + \bar{g}$, and $\overline{fg} = \bar{g}\bar{f}$. So we have

$$g_n - f_n = s_{n-1}d_n + \tilde{d}_{n+1}s_n \implies \bar{g}_n - \bar{f}_n = \bar{d}_n\bar{s}_{n-1} + \bar{s}_n\bar{d}_{n+1}$$

and $\bar{f}_n, \bar{g}_n$ are homotopic. Thus by proposition 2.1.5, $\bar{f}^*_\bullet = \bar{g}^*_\bullet$.

Now, let $P_\bullet, P'_\bullet$ be two projective resolutions. Consider the diagram:

$$\begin{tikzcd}
\cdots \arrow[r] & P_1 \arrow[r] \arrow[d, "f_1"] \arrow[dd, bend right, "\mathrm{Id}"'] & P_0 \arrow[r] \arrow[d, "f_0"] \arrow[dd, bend right, "\mathrm{Id}"'] & M \arrow[r] \arrow[d, "\mathrm{Id}"] & 0 \\
\cdots \arrow[r] & P'_1 \arrow[r] \arrow[d, "g_1"] & P'_0 \arrow[r] \arrow[d, "g_0"] & M \arrow[r] \arrow[d, "\mathrm{Id}"] & 0 \\
\cdots \arrow[r] & P_1 \arrow[r] & P_0 \arrow[r] & M \arrow[r] & 0
\end{tikzcd}$$

Then $g_i \circ f_i$ and Id are two liftings, and thus by previous we have $\bar{g}_i^* \circ \bar{f}_i^* = \mathrm{Id}^*$. By symmetry, $\bar{f}_i^* \circ \bar{g}_i^* = \mathrm{Id}^*$, which means that the homology calculated using different resolution are isomorphic.

$\square$

Theorem 28 (Horseshoe Lemma)**.** Given $0 \to L \to M \to N \to 0$ and projective resolutions $P_\bullet \to L \to 0$, $\tilde{P}_\bullet \to N \to 0$. Then there is a projective resolution for M such that the following diagram commutes:

$$\begin{tikzcd}
 & \vdots \arrow[d] & \vdots \arrow[d] & \vdots \arrow[d] & \\
0 \arrow[r] & P_1 \arrow[r] \arrow[d] & \bar{P}_1 \arrow[r] \arrow[d] & \tilde{P}_1 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & P_0 \arrow[r] \arrow[d] & \bar{P}_0 \arrow[r] \arrow[d] & \tilde{P}_0 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & L \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

Proof. Let $\bar{P}_n \triangleq P_n \oplus \tilde{P}_n$. $\bar{P}_n$ is projective by the fact that direct sum of projective modules are projective. Also $0 \to P_n \to P_n \oplus \tilde{P}_n \to \tilde{P}_n \to 0$ by injection and projection. It remains to show that the maps in the middle column exists.

Consider the following diagram:

$$\begin{tikzcd}
 & \vdots \arrow[d] & & \vdots \arrow[d] & \\
0 \arrow[r] & P_0 \arrow[r] \arrow[d, "\alpha"] & P_0 \oplus \tilde{P}_0 \arrow[r] \arrow[d, dashed, "\bar{\alpha}"] & \tilde{P}_0 \arrow[r] \arrow[d, "\tilde{\alpha}"] \arrow[dl, "\exists\, \sigma"] & 0 \\
0 \arrow[r] & L \arrow[r, "f"'] \arrow[d] & M \arrow[r, "g"'] \arrow[d] & N \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

σ exists because $\tilde{P}_0$ is projective. Define

$$\begin{aligned}
\bar{\alpha} : P_0 \oplus \tilde{P}_0 &\longrightarrow M \\
(z, y) &\longmapsto f \circ \alpha(z) + \sigma(y)
\end{aligned}$$

It easy to see that $\bar{\alpha}$ let the diagram commutes. So we show that $P_0 \oplus \tilde{P}_0 \xrightarrow{\bar{\alpha}} M \to 0$:

For any $x \in M$, consider $g(x) \in N$. Since $\tilde{P}_0 \xrightarrow{\tilde{\alpha}} N \to 0$, there exists $y \in \tilde{P}_0$ such that $\tilde{\alpha}(y) = g(x) \implies g \circ \sigma(y) = g(x)$. Then $x - \sigma(y) = \ker g = \operatorname{Im} f$, so there exists $w \in L$ such that $f(w) + \sigma(y) = x$. Now, since $P_0 \xrightarrow{\alpha} L \to 0$, there exists $z \in P_0$ such that $\alpha(z) = w$. Then we have $\bar{\alpha}(z, y) = x$. So $P_0 \oplus \tilde{P}_0 \xrightarrow{\bar{\alpha}} M \to 0$.

By induction on n, but we use $\ker d_{n-1}, \ker \bar{d}_{n-1}, \ker \tilde{d}_{n-1}$ to replace L, M, N ($d_{-1} = \alpha$ and so on). Then we are done. $\square$

Theorem 29 (Long exact sequence for Ext)**.** If $0 \to L \to M \to N \to 0$ exact, then there is a long exact sequence:

$$\begin{aligned}
0 \to \operatorname{Hom}(N, K) \to \operatorname{Hom}(M, K) \to \operatorname{Hom}(L, K)& \\
\to \operatorname{Ext}^1(N, K) \to \operatorname{Ext}^1(M, K) \to \operatorname{Ext}^1(L, K) \to \operatorname{Ext}^2(N, K) \to \dots&
\end{aligned}$$

Proof. Taking $\mathrm{Hom}(-,K)$ in the diagram of Horseshoe' lemma (28) and delete the first row, we get

$$\begin{tikzcd}
 & \vdots & \vdots & \vdots & \\
0 & \mathrm{Hom}(P_1,K) \arrow[l] \arrow[u] & \mathrm{Hom}(\bar{P}_1,K) \arrow[l] \arrow[u] & \mathrm{Hom}(\tilde{P}_1,K) \arrow[l] \arrow[u] & 0 \arrow[l] \\
0 & \mathrm{Hom}(P_0,K) \arrow[l] \arrow[u] & \mathrm{Hom}(\bar{P}_0,K) \arrow[l] \arrow[u] & \mathrm{Hom}(\tilde{P}_0,K) \arrow[l] \arrow[u] & 0 \arrow[l] \\
 & 0 \arrow[u] & 0 \arrow[u] & 0 \arrow[u] &
\end{tikzcd}$$

Notice that $\mathrm{Hom}(M \oplus N, K) \cong \mathrm{Hom}(M,K) \oplus \mathrm{Hom}(N,K)$, so each row is indeed exact.

By exercise 14.7, the long exact sequence in the statement exists. (one can check the kernels of the first row are indeed $\mathrm{Hom}(N,K), \mathrm{Hom}(M,K), \mathrm{Hom}(L,K)$.) $\square$

2.2 Ext and Tor (week 15)

Given $M, N \in \mathbf{Mod}_R$, there are two ways to define $\operatorname{Ext}^n(M, N)$:

Def 34 (Ext functor)**.**

- Find any projective resolution $P_\bullet \xrightarrow{\alpha} M \to 0$, and let $P_M : P_\bullet \to 0$ (called a *deleted resolution*). We can define $\operatorname{Ext}^n_{\text{proj}}(M, N) = H^n(\operatorname{Hom}(P_M, N))$.
- Find any injective resolution $0 \xrightarrow{\alpha} N \to E^\bullet$, and let $E_N : 0 \to E^\bullet$. We can define $\operatorname{Ext}^n_{\text{inj}}(M, N) = H^n(\operatorname{Hom}(M, E_N))$.

Prop 2.2.1. $\operatorname{Ext}^0_{\text{proj}}(M, N) \cong \operatorname{Ext}^0_{\text{inj}}(M, N) \cong \operatorname{Hom}(M, N)$.

Proof.

$$\operatorname{Hom}(P_M, N) : 0 \xrightarrow{\overline{d_0}} \operatorname{Hom}(P_0, N) \xrightarrow{\overline{d_1}} \operatorname{Hom}(P_1, N) \to \cdots$$

so $\operatorname{Ext}^0_{\text{proj}}(M, N) = \ker \overline{d_1} / \operatorname{im} \overline{d_0} = \ker \overline{d_1} = \operatorname{im} \alpha = \operatorname{Hom}(M, N)$. $\square$

Similarly, $\operatorname{Ext}^0_{\text{inj}}(M, N) = \operatorname{Hom}(M, N)$.

Lemma 9.

- If M is projective, then $\operatorname{Ext}^n_{\text{proj}}(M, N) = 0$ for all $n > 0, N \in \mathbf{Mod}_R$.
- If N is injective, then $\operatorname{Ext}^n_{\text{inj}}(M, N) = 0$ for all $n > 0, M \in \mathbf{Mod}_R$.

Proof. If M is projective, then $0 \to M \xrightarrow{\mathbf{1}_M} M \to 0$ is a projective resolution of M. Its deleted resolution is then $P_M : 0 \to M \to 0$. Hence for $n > 0$, $\operatorname{Ext}^n_{\text{proj}}(M, N) = H^n(\operatorname{Hom}(P_M, N)) = 0$.

The argument applies similarly to injective case. $\square$

Theorem 30 (Equivalence of $\operatorname{Ext}_{\text{proj}}$ and $\operatorname{Ext}_{\text{inj}}$)**.**

$$\operatorname{Ext}^n_{\text{proj}}(M, N) \cong \operatorname{Ext}^n_{\text{inj}}(M, N).$$

Proof. Let $P_\bullet \to M \to 0$ and $0 \to N \to E^\bullet$ be projective and injective resolutions, then we have $0 \to K_0 \to P_0 \to M \to 0$ and $0 \to N \to E^0 \to L^1 \to 0$ exact.

$$\begin{tikzcd}
\cdots \to P_2 \arrow[rr] \arrow[dr] & & P_1 \arrow[rr] \arrow[dr] & & P_0 \to M \to 0 \\
& K_1 \arrow[ur] \arrow[dr] & & K_0 \arrow[ur] \arrow[dr] & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0
\end{tikzcd}
\qquad
\begin{tikzcd}
0 \to N \to E^0 \arrow[rr] \arrow[dr] & & E^1 \arrow[rr] \arrow[dr] & & E^2 \to \cdots \\
& L^1 \arrow[ur] \arrow[dr] & & L^2 \arrow[ur] \arrow[dr] & \\
0 \arrow[ur] & & 0 \arrow[ur] & & 0
\end{tikzcd}$$

We can construct long exact sequences of homology of $\operatorname{Hom}(\cdot, E_N)$:

$$0 \to \operatorname{Hom}(M, N) \to \operatorname{Hom}(M, E^0) \to \operatorname{Hom}(M, L^1) \to \operatorname{Ext}^1_{\text{inj}}(M, N) \to \operatorname{Ext}^1_{\text{inj}}(M, E^0) = 0$$

$$0 \to \operatorname{Hom}(P_0, N) \to \operatorname{Hom}(P_0, E^0) \to \operatorname{Hom}(P_0, L^1) \to 0$$

$$0 \to \operatorname{Hom}(K_0, N) \to \operatorname{Hom}(K_0, E^0) \to \operatorname{Hom}(K_0, L^1) \to \operatorname{Ext}^1_{\text{inj}}(K_0, N) \to \operatorname{Ext}^1_{\text{inj}}(K_0, E^0) = 0$$

The second sequence is short because P_0 is projective (so $\operatorname{Hom}(P_0, \cdot)$ preserves exactness).

Similarly, for $\operatorname{Hom}(P_M, \cdot)$ we have:

$$0 \to \operatorname{Hom}(M, N) \to \operatorname{Hom}(P_0, N) \to \operatorname{Hom}(K_0, N) \to \operatorname{Ext}^1_{\text{proj}}(M, N) \to \operatorname{Ext}^1_{\text{proj}}(P_0, N) = 0$$

$$0 \to \mathrm{Hom}(M, E^0) \to \mathrm{Hom}(P_0, E^0) \to \mathrm{Hom}(K_0, E^0) \to 0$$

$$0 \to \mathrm{Hom}(M, L^1) \to \mathrm{Hom}(P_0, L^1) \to \mathrm{Hom}(K_0, L^1) \to \mathrm{Ext}^1_{\mathrm{proj}}(M, L^1) \to \mathrm{Ext}^1_{\mathrm{proj}}(P_0, L^1) = 0$$

Combining these sequences together, we got the following 2D diagram:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & & \\
0 \arrow[r] & \mathrm{Hom}(M,N) \arrow[r] \arrow[d] & \mathrm{Hom}(M,E^0) \arrow[r, "\phi"] \arrow[d] & \mathrm{Hom}(M,L^1) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\mathrm{inj}}(M,N) \arrow[r] & 0 \\
0 \arrow[r] & \mathrm{Hom}(P_0,N) \arrow[r] \arrow[d, "\alpha"] & \mathrm{Hom}(P_0,E^0) \arrow[r, "\sigma"] \arrow[d, "\beta"] & \mathrm{Hom}(P_0,L^1) \arrow[rr] \arrow[d, "\gamma"] & & 0 \\
0 \arrow[r] & \mathrm{Hom}(K_0,N) \arrow[r] \arrow[d] & \mathrm{Hom}(K_0,E^0) \arrow[r, "\tau"] \arrow[d] & \mathrm{Hom}(K_0,L^1) \arrow[r] \arrow[d] & \mathrm{Ext}^1_{\mathrm{inj}}(K_0,N) \arrow[r] & 0 \\
 & \mathrm{Ext}^1_{\mathrm{proj}}(M,N) \arrow[d] & 0 & \mathrm{Ext}^1_{\mathrm{proj}}(M,L^1) \arrow[d] & & \\
 & 0 & & 0 & &
\end{tikzcd}$$

By Snake lemma, there is an exact sequence

$$(\ker \alpha \to) \ker \beta \to \ker \gamma \to \operatorname{coker} \alpha \to \operatorname{coker} \beta (\to \operatorname{coker} \gamma)$$

and this reads

$$\mathrm{Hom}(M, E^0) \xrightarrow{\phi} \mathrm{Hom}(M, L^1) \to \mathrm{Ext}^1_{\mathrm{proj}}(M, N) \to 0$$

Thus $\mathrm{Ext}^1_{\mathrm{proj}}(M, N) \cong \operatorname{coker} \phi \cong \mathrm{Ext}^1_{\mathrm{inj}}(M, N)$.
(From now on, we don't need to distinguish proj/inj for Ext^1 !)

Since σ is onto, $\operatorname{im} \gamma = \operatorname{im}(\gamma \circ \sigma)$. Similarly, $\operatorname{im} \tau = \operatorname{im}(\tau \circ \beta)$.

By the commutativity of the diagram, $\operatorname{im} \gamma = \operatorname{im} \tau$, so

$$\mathrm{Ext}^1(K_0, N) \cong \operatorname{coker} \gamma = \mathrm{Hom}(K_0, L^1)/\operatorname{im} \gamma \cong \operatorname{coker} \tau \cong \mathrm{Ext}^1(M, L^1).$$

Write $K_{-1} := M, L^0 := N$, then $\mathrm{Ext}^1(K_0, L^0) = \mathrm{Ext}^1(K_{-1}, L^1)$ $(\star)$.

Similarly, from the exact sequences

$$0 \to K_j \to P_j \to K_{j-1} \to 0$$

$$0 \to L^i \to E^i \to L^{i+1} \to 0$$

, we can obtain $\mathrm{Ext}^1(K_j, L^i) \cong \mathrm{Ext}^1(K_{j-1}, L^{i+1})$ for $i, j \geq 0$.

Now, observe that

$$0 \to L^{n-1} \to E^{n-1} \xrightarrow{d_{n-1}} E^n \xrightarrow{d_n} \cdots$$

is an injective resolution of L^{n-1}, and $\mathrm{Ext}^1(M, L^{n-1}) \cong \ker \overline{d_n} / \operatorname{im} \overline{d_{n-1}} \cong \mathrm{Ext}^n_{\mathrm{inj}}(M, N)$.

Similarly, for projective resolution we have $\mathrm{Ext}^1(K_{n-2}, N) \cong \mathrm{Ext}^n_{\mathrm{proj}}(M, N)$.

Finally, by $(\star)$,

$$\mathrm{Ext}^n_{\mathrm{inj}}(M, N) \cong \mathrm{Ext}^1(K_{-1}, L^{n-1}) \cong \mathrm{Ext}^1(K_0, L^{n-2}) \cong \cdots \cong \mathrm{Ext}^1(K_{n-2}, L^0) \cong \mathrm{Ext}^n_{\mathrm{proj}}(M, N).$$

$\square$

Def 35 (Tor functor)**.** Let $M, N \in \mathbf{Mod}_R$, and $P_\bullet \to M \to 0$ be a projective resolution of M, similar to the Ext case, for $n \geq 0$ we can define

$$\mathrm{Tor}_n(M, N) = H_n(P_M \otimes N).$$

Fact 2.2.1. By Horseshoe lemma, short exact sequence $0 \to M_1 \to M_2 \to M_3 \to 0$ induces a long exact sequence:

$$\cdots \to \mathrm{Tor}_1(M_1, N) \to \mathrm{Tor}_1(M_2, N) \to \mathrm{Tor}_1(M_3, N) \to M_1 \otimes N \to M_2 \otimes N \to M_3 \otimes N \to 0$$

Prop 2.2.2. If M is flat, then $\mathrm{Tor}_n(M, N) = 0$ for $n > 0, N \in \mathbf{Mod}_R$.

Proof. M is flat $\implies$ $M \otimes \cdot$ is an exact functor. If $Q_\bullet \to N \to 0$ is a projective resolution of N, then $\cdots \to M \otimes Q_1 \to M \otimes Q_0 \to M \otimes N \to 0$ is also exact. By Exercise 15-1, we have

$$\mathrm{Tor}_n(M, N) \cong H_n(M \otimes Q_N) = 0. \qquad \square$$

Theorem 31 (Tor for flat resolutions)**.** Let $U_\bullet \to M \to 0$ be a flat resolution of M, then for $n \geq 0$,

$$\mathrm{Tor}_n(M, N) \cong H_n(U_M \otimes N).$$

Proof.

$$\begin{tikzcd}
\cdots \arrow[r] & U_2 \arrow[rr] \arrow[dr] & & U_1 \arrow[rr] \arrow[dr] & & U_0 \arrow[r] & M \arrow[r] & 0 \\
& & W_1 \arrow[ur] \arrow[dr] & & W_0 \arrow[ur] \arrow[dr] & & & \\
& 0 \arrow[ur] & & 0 \arrow[ur] & & 0 & &
\end{tikzcd}$$

$$H_\bullet(U_M \otimes N) : \cdots \to U_2 \otimes N \xrightarrow{d_2 \otimes \mathbf{1}} U_1 \otimes N \xrightarrow{d_1 \otimes \mathbf{1}} U_0 \otimes N \to 0$$

- $n = 0$:
  Since tensor is right exact, $U_1 \otimes N \xrightarrow{d_1 \otimes \mathbf{1}} U_0 \otimes N \xrightarrow{\alpha \otimes \mathbf{1}} M \otimes N \to 0$ is exact. Hence

  $$H_0(U_M \otimes N) = (U_0 \otimes N)/\operatorname{im}(d_1 \otimes \mathbf{1}) = (U_0 \otimes N)/\ker(\alpha \otimes \mathbf{1}) \cong M \otimes N$$

  Any projective resolution also has this property, so $\mathrm{Tor}_0(M, N) = H_0(U_M \otimes N)$.

- $n = 1$:
  $0 \to W_0 \to U_0 \to M \to 0$ induces a long exact sequence:

  $$\cdots \to \mathrm{Tor}_1(W_0, N) \to 0 \to \mathrm{Tor}_1(M, N) \to W_0 \otimes N \xrightarrow{i \otimes 1} U_0 \otimes N \to M \otimes N \to 0$$

  where $\mathrm{Tor}_1(U_0, N) = 0$ because U_0 is flat. We can see that $\mathrm{Tor}_1(M, N) \cong \ker(i \otimes 1)$.

  $$\begin{tikzcd}
  U_2 \otimes N \arrow[rr, "d_2 \otimes 1"] \arrow[dr, "\beta' \otimes 1"'] & & U_1 \otimes N \arrow[rr, "d_1 \otimes 1"] \arrow[dr, "\alpha' \otimes 1"'] & & U_0 \otimes N \\
  & W_1 \otimes N \arrow[ur, "j \otimes 1"'] \arrow[dr] & & W_0 \otimes N \arrow[ur, "i \otimes 1"'] \arrow[dr] & \\
  & & 0 & & 0
  \end{tikzcd}$$

  Since $\alpha' \otimes 1$ is onto, $W_0 \otimes N \cong (U_1 \otimes N)/\ker(\alpha' \otimes 1)$. Also, $x \in \ker(d_1 \otimes 1) \iff (d_1 \otimes 1)(x) = 0 \iff (\alpha' \otimes 1)(x) \in \ker(i \otimes 1)$, so $\ker(i \otimes 1) = (\alpha' \otimes 1)(\ker(d_1 \otimes 1)) \cong \ker(d_1 \otimes 1)/\ker(\alpha' \otimes 1)$. ($\alpha' \otimes 1$ can be considered a quotient map, then $\ker(d_1 \otimes 1)$ descends to $\ker(d_1 \otimes 1)/\ker(\alpha' \otimes 1)$.)

Now, in the diagram $W_1 \otimes N \to U_1 \otimes N \to W_0 \otimes N \to 0$ exact, so $\ker(\alpha' \otimes 1) = \mathrm{im}(j \otimes 1)$. But $\beta' \otimes 1$ is onto, thus $\mathrm{im}(j \otimes 1) = \mathrm{im}(d_2 \otimes 1)$.

Finally,

$$\mathrm{Tor}_1(M, N) \cong \ker(i \otimes 1) \cong \ker(d_1 \otimes 1)/\ker(\alpha' \otimes 1) = \ker(d_1 \otimes 1)/\mathrm{im}(d_2 \otimes 1) = H_1(U_M \otimes N).$$

- $n \geq 2$:
  Let's see further in the previous long exact sequences:

  $$\cdots \to \mathrm{Tor}_2(W_0, N) \to 0 \to \mathrm{Tor}_2(M, N) \xrightarrow{\sim} \mathrm{Tor}_1(W_0, N) \to 0 \to \mathrm{Tor}_1(M, N) \to \cdots$$

  we can see that $\mathrm{Tor}_n(M, N) \cong \mathrm{Tor}_{n-1}(W_0, N)$ for $n \geq 2$.

  Now,

  $$\cdots U_3 \xrightarrow{d_3} U_2 \xrightarrow{d_2} U_1 \to W_0 \to 0$$

  is a flat resolution of W_0, and its homology is $H_{n-1}(U_{W_0} \otimes N) = \ker(d_n \otimes 1)/\mathrm{im}(d_{n-1} \otimes 1) = H_n(U_M \otimes N)$.

  By induction, assume it's true for $n - 1$, then

  $$H_n(U_M \otimes N) = H_{n-1}(U_{W_0} \otimes N) \cong \mathrm{Tor}_{n-1}(W_0, N) \cong \mathrm{Tor}_n(M, N).$$

$\square$

Eg 2.2.1. $R = \mathbb{Z}, M = \mathbb{Z}/m\mathbb{Z}$ with $m \geq 2$. Then

$$P : 0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \xrightarrow{/m\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \to 0$$

is a projective resolution of $\mathbb{Z}/m\mathbb{Z}$. So for any $N \in \mathbf{Mod}_{\mathbb{Z}}$,

$$H^n(\mathrm{Hom}_{\mathbb{Z}}(P_{\mathbb{Z}/m\mathbb{Z}}, N)) : 0 \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \xrightarrow{\overline{m}} \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, N) \to 0,$$

$$\begin{aligned}
\mathrm{Ext}^0_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) \cong {}_mN := \{a \in N \mid ma = 0\} \\
\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) &\cong N/mN \\
\mathrm{Ext}^n_{\mathbb{Z}}(\mathbb{Z}/m\mathbb{Z}, N) &= 0 \quad (\text{for } n \geq 2)
\end{aligned}$$

Eg 2.2.2. $\mathbb{Q} = \mathbb{Z}_{\langle 0 \rangle}$ is a localization, thus a flat $\mathbb{Z}$ module. Then

$$U : 0 \to \mathbb{Z} \xrightarrow{i} \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

is a flat resolution of $\mathbb{Q}/\mathbb{Z}$. For $G \in \mathbf{Mod}_{\mathbb{Z}}$ (i.e. an abelian group),

$$H_n(G \otimes U_{\mathbb{Q}/\mathbb{Z}}) : 0 \to G \otimes \mathbb{Z} \xrightarrow{\mathbf{1} \otimes i} G \otimes \mathbb{Q} \to 0$$

$$\begin{aligned}
\mathrm{Tor}_0(G, \mathbb{Q}/\mathbb{Z}) &\cong G \otimes \mathbb{Q}/\mathbb{Z} \\
\mathrm{Tor}_1(G, \mathbb{Q}/\mathbb{Z}) &= \ker(\mathbf{1} \otimes i) \cong t(G) := \{a \in G \mid ma = 0 \text{ for some } m \in \mathbb{N}\} \\
\mathrm{Tor}_n(G, \mathbb{Q}/\mathbb{Z}) &= 0 \quad (\text{for } n \geq 2)
\end{aligned}$$

Def 36. Let M be a left R-module, then define $M^* := \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ as a right R-module by

$$\begin{aligned}
fr : M &\to \mathbb{Q}/\mathbb{Z} \\
x &\mapsto f(rx)
\end{aligned}$$

Fact 2.2.2.

1. $\mathbb{Q}/\mathbb{Z}$ is injective.
2. $A = 0 \iff A^* = 0$.
3. $B \hookrightarrow C \iff C^* \twoheadrightarrow B^*$.

Proof.

1. For $m \in \mathbb{Z} \setminus \{0\}$, $m(\mathbb{Q}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}$ by $m(\frac{a}{mb} + \mathbb{Z}) \leftarrow\!\shortmid \frac{a}{b} + \mathbb{Z}$, so $\mathbb{Q}/\mathbb{Z}$ is divisible. But $\mathbb{Z}$ is a PID, so $\mathbb{Q}/\mathbb{Z}$ is injective.
2. ($\Rightarrow$) $A^* = \mathrm{Hom}_{\mathbb{Z}}(0, \mathbb{Q}/\mathbb{Z}) = 0$.

   ($\Leftarrow$) If $A \neq 0$, then $\exists\, a \in A, a \neq 0$, so $0 \to \mathbb{Z}a \xrightarrow{i} A$ is an inclusion.

   Since $\mathbb{Z}a$ is a cyclic abelian group, there is a nonzero $g : \mathbb{Z}a \to \mathbb{Q}/\mathbb{Z}$. (If $\mathbb{Z}a \cong \mathbb{Z}/m\mathbb{Z}$, let $g : a \mapsto \frac{1}{m}$; if $\mathbb{Z}a \cong \mathbb{Z}$, let $g : a \mapsto \frac{1}{2}$.)

   But $\mathbb{Q}/\mathbb{Z}$ is injective, so $\exists\, f : A \to \mathbb{Q}/\mathbb{Z}$ (i.e. $f \in A^*$), and $f \circ i = g \neq 0$ so $f \neq 0$, thus $A^* \neq 0$.

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z}a \arrow[r, "i"] \arrow[d, "g"] & A \arrow[dl, "\exists\, f"] \\
& \mathbb{Q}/\mathbb{Z} &
\end{tikzcd}$$

3. Since $\mathbb{Q}/\mathbb{Z}$ is injective, $\mathrm{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$ is exact. Let $0 \to \ker f \to B \xrightarrow{f} C$ exact, applying $\mathrm{Hom}(\cdot, \mathbb{Q}/\mathbb{Z})$ results in $C^* \xrightarrow{f^*} B^* \to (\ker f)^* \to 0$ exact. Thus $\operatorname{coker} f^* = (\ker f)^*$.

   By 2., $B \hookrightarrow C \iff \ker f = 0 \iff (\ker f)^* = 0 \iff \operatorname{coker} f^* = 0 \iff C^* \twoheadrightarrow B^*$.

$\square$

Prop 2.2.3. Let M be an R-module, then TFAE

1. M is flat.
2. M^* is injective (as a R-module).
3. $\mathrm{Tor}_1(R/I, M) = 0$ for all ideal $I \subseteq R$.
4. $I \otimes_R M \cong IM$ for all ideal $I \subseteq R$.

Proof.

- 3. $\iff$ 4.
  For any ideal $I \subseteq R$, $0 \to I \xrightarrow{i} R \xrightarrow{q} R/I \to 0$ is exact. This induces a long exact sequence:

  $$\mathrm{Tor}_1(R, M) \to \mathrm{Tor}_1(R/I, M) \to I \otimes_R M \xrightarrow{i \otimes \mathbf{1}} R \otimes_R M \xrightarrow{q \otimes \mathbf{1}} R/I \otimes_R M \to 0$$

  - $\mathrm{Tor}_1(R, M) = 0$ since R is a flat R-module.
  - $R \otimes_R M \cong M$.
  - $R/I \otimes_R M \cong M/IM$ by $(r + I) \otimes a \mapsto (ra + IM)$.

  So we have

  $$0 \to \mathrm{Tor}_1(R/I, M) \to I \otimes_R M \xrightarrow{i'} M \xrightarrow{q'} M/IM \to 0$$

  exact, with $q' : M \to M/IM$ being exactly the quotient map (one can check that $q \otimes \mathbf{1} \cong q'$).

  Now it's clear that $\mathrm{Tor}_1(R/I, M) = 0 \iff I \otimes_R M \cong \ker(q') \cong IM$.

  (The reverse direction requires $I \otimes_R M \cong IM$ being the natural isomorphism $r \otimes b \mapsto rb$, so $i' : IM \to M$ can then be the natural inclusion.)

- 1. $\iff$ 2.
  Let $0 \to N' \xrightarrow{f} N$, then $\mathrm{Hom}_R(N, M^*) \xrightarrow{\overline{f}} \mathrm{Hom}_R(N', M^*)$.

  By the adjoint relation,

  $$\mathrm{Hom}_R(N, M^*) = \mathrm{Hom}_R(N, \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})) \cong \mathrm{Hom}_{\mathbb{Z}}(N \otimes_R M, \mathbb{Q}/\mathbb{Z}) = (N \otimes_R M)^*,$$

  we have another map $(N \otimes_R M)^* \xrightarrow{(f\otimes\mathbf{1})^*} (N' \otimes_R M)^*$ isomorphic to the previous one, with its unstarred map $N' \otimes_R M \xrightarrow{f\otimes\mathbf{1}} N \otimes_R M$.

  Now, M^* is injective $\iff$ $\overline{f}$ is surjective $\forall\, N, N'$ $\iff$ $(f \otimes \mathbf{1})^*$ is surjective $\forall\, N, N'$ $\iff$ $f \otimes \mathbf{1}$ is injective $\forall\, N, N'$ $\iff$ M is flat.
- 2. $\iff$ 4.
  Similar to the previous section, by Baer's criterion,

  $$\begin{aligned} M^* \text{ is injective} \quad &\iff \quad \mathrm{Hom}_R(R, M^*) \twoheadrightarrow \mathrm{Hom}_R(I, M^*), \forall\, I \subseteq R \\ &\iff \quad (R \otimes_R M)^* \twoheadrightarrow (I \otimes_R M)^*, \forall\, I \subseteq R \\ &\iff \quad I \otimes_R M \hookrightarrow R \otimes_R M \cong M, \forall\, I \subseteq R \\ &\iff \quad I \otimes_R M \cong IM, \forall\, I \subseteq R. \end{aligned}$$

  Similarly, this requires the isomorphism of $I \otimes_R M \cong IM$ be natural (the following f).

  The map $\begin{aligned} f : I \otimes_R M &\to IM \\ r \otimes a &\mapsto ra \end{aligned}$ is always onto, but may not be 1-1. If it is, $I \otimes_R M \cong IM$.

□

Prop 2.2.4. For $I, J \subseteq R$ being ideals, then $\mathrm{Tor}_1(R/I, R/J) \cong (I \cap J)/IJ$.

Proof. $0 \to I \xrightarrow{i} R \to R/I \to 0$ induces a long exact sequence

$$0 \to \mathrm{Tor}_1(R/I, R/J) \to I \otimes_R R/J \xrightarrow{i\otimes 1} R \otimes_R R/J \to R/I \otimes_R R/J \to 0,$$

where $\mathrm{Tor}_1(R, R/J) = 0$ since R is flat.

Also $I \otimes_R R/J \cong I/IJ, R \otimes_R R/J \cong R/J$, so we have $I/IJ \xrightarrow{i'} R/J$ with $\mathrm{Tor}_1(R/I, R/J) \cong \ker(i \otimes 1) \cong \ker i'$.

But $\begin{aligned} i' : \ I/IJ &\to R/J \\ x + IJ &\mapsto x + J \end{aligned}$, so $\overline{x} \in \ker i' \iff x \in I$ and $x \in J \iff x \in I \cap J$, hence $\ker i' \cong (I \cap J)/IJ$. □

2.3 Koszul complex (week 16)

In this section, we assume that R is commutative with 1.

Def 37. Let $L \in \mathbf{Mod}_R$, with $f : L \to R$ an R-linear map, define

$$\begin{array}{rcl} \mathrm{d}_f : \quad \Lambda^n L & \to & \Lambda^{n-1} L \\ x_1 \wedge \cdots \wedge x_n & \mapsto & \sum_{i=1}^{n} (-1)^{i+1} f(x_i) x_1 \wedge \cdots \wedge \hat{x}_i \wedge \cdots \wedge x_n \end{array}$$

where $\Lambda^n L$ is the n-th exterior power of L, and $\hat{x}_i$ means omitting x_i.

Then we can define a chain complex called **Koszul complex**:

$$K_\bullet(f) : \cdots \to \Lambda^n L \xrightarrow{\mathrm{d}_f} \Lambda^{n-1} L \to \cdots \to \Lambda^2 L \xrightarrow{\mathrm{d}_f} L \xrightarrow{f} R$$

Also, d_f can be considered as a graded R-homomorphism of degree -1:

$$\begin{array}{rcl} \mathrm{d}_f : \ \Lambda L & \to & \Lambda L \\ x \wedge y & \mapsto & \mathrm{d}_f(x) \wedge y + (-1)^{\deg x} \cdot x \wedge \mathrm{d}_f(y) \end{array}$$

where ΛL is the exterior algebra of L, and x, y are any homogeneous elements of ΛL.

Def 38. Let $(C_\bullet, d), (C'_\bullet, d')$ be chain complexes of R-modules, define their *tensor product* to be a chain complex $C_\bullet \otimes C'_\bullet$ with

$$(C_\bullet \otimes C'_\bullet)_n = \bigoplus_{i=0}^{n} \left(C_i \otimes_R C'_{n-i} \right)$$

with the boundary maps being

$$\begin{array}{rcl} d \otimes d' : \ (C_\bullet \otimes C'_\bullet)_n & \to & (C_\bullet \otimes C'_\bullet)_{n-1} \\ \sum_{i=0}^{n} x_i \otimes y_{n-i} & \mapsto & \sum_{i=0}^{n} \left(d(x_i) \otimes y_{n-i} + (-1)^i \cdot x_i \otimes d'(y_{n-i}) \right) \end{array}$$

One can verify that

$$\begin{aligned} (d \otimes d') \circ (d \otimes d')(x \otimes y) &= (d \otimes d')(d(x) \otimes y + (-1)^{\deg x} \cdot x \otimes d'(y)) \\ &= d \circ d(x) \otimes y + (-1)^{\deg x - 1} \cdot d(x) \otimes d'(y) \\ &\quad + (-1)^{\deg x} \cdot d(x) \otimes d'(y) + x \otimes d' \circ d'(y) \\ &= 0 \end{aligned}$$

Prop 2.3.1. Let $L_1, L_2 \in \mathbf{Mod}_R, f_1 \in \mathrm{Hom}_R(L_1, R), f_2 \in \mathrm{Hom}_R(L_2, R)$. Define

$$\begin{array}{rcl} f = f_1 + f_2 : L_1 \oplus L_2 & \to & R \\ (x, y) & \mapsto & f_1(x) + f_2(y) \end{array},$$

then

$$\begin{array}{rcl} K_\bullet(f_1) \otimes K_\bullet(f_2) & \cong & K_\bullet(f) \\ \bigoplus_{i=0}^{n} \left(\Lambda^i L_1 \otimes_R \Lambda^{n-i} L_2 \right) & \cong & \Lambda^n (L_1 \oplus L_2) \end{array}$$

with $\mathrm{d}_{f_1} \otimes \mathrm{d}_{f_2} = \mathrm{d}_f$.

Proof. Exercise 16-1(2). $\square$

Def 39. Let $L = \bigoplus_{i=1}^{n} Re_i$ be a free R-module, and $\mathbf{x} = (x_1, \cdots, x_n)$ with $x_i \in R$, define

$$K_\bullet(\mathbf{x}) := K_\bullet(f), \text{with } \begin{array}{c} f : L \to R \\ e_i \mapsto x_i \end{array}.$$

Coro 2.3.1. $K_\bullet(\mathbf{x}) \cong K_\bullet(x_1) \otimes \cdots \otimes K_\bullet(x_n)$ with $K_\bullet(x_i) : 0 \to R \xrightarrow{x_i} R$.

Prop 2.3.2. Let $x \in R$ and $(C_\bullet, \partial)$ be a chain complex of R-modules, then there exist ρ, π s.t.

$$0 \to C_\bullet \xrightarrow{\rho} C_\bullet \otimes K_\bullet(x) \xrightarrow{\pi} C_\bullet(-1) \to 0$$

is exact, where $(C_\bullet(-1))_n = C_{n-1}$.

Proof. Since $K_\bullet(x) : 0 \to R \xrightarrow{x} R$, so

$$(C_\bullet \otimes K_\bullet(x))_n = (C_i \otimes_R R) \oplus (C_{i-1} \otimes_R R),$$

and the boundary map is

$$\begin{array}{rcl} \mathrm{d} : (C_i \otimes_R R) \oplus (C_{i-1} \otimes_R R) \to & & (C_{i-1} \otimes_R R) \oplus (C_{i-2} \otimes_R R) \\ (z_1 \otimes r_1, z_2 \otimes r_2) & \mapsto & \big(\partial z_1 \otimes r_1 + (-1)^{i-1} z_2 \otimes x r_2, \partial z_2 \otimes r_2\big) \end{array}.$$

Under the isomorphism $C_i \otimes_r R \cong C_i$, the boundary map become

$$\begin{array}{rcl} \mathrm{d} : C_i \oplus C_{i-1} \to & & C_{i-1} \oplus C_{i-2} \\ \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} & \mapsto & \begin{pmatrix} \partial & (-1)^{i-1} x \\ 0 & \partial \end{pmatrix} \begin{pmatrix} r_1 z_1 \\ r_2 z_2 \end{pmatrix} \end{array}$$

Let

$$\begin{array}{rcl} \rho_i : C_i & \to & C_i \oplus C_{i-1} \\ z_1 & \mapsto & (z_1, 0) \end{array} \quad \text{and} \quad \begin{array}{rcl} \pi_i : C_i \oplus C_{i-1} & \to & C_{i-1} \\ (z_1, z_2) & \mapsto & z_2 \end{array}$$

then

$$\begin{tikzcd} 0 \arrow[r] & C_i \arrow[r, "\rho_i"] \arrow[d, "\partial"] & C_i \oplus C_{i-1} \arrow[r, "\pi_i"] \arrow[d, "\mathrm{d}"] & C_{i-1} \arrow[r] \arrow[d, "\partial"] & 0 \\ 0 \arrow[r] & C_{i-1} \arrow[r, "\rho_{i-1}"] & C_{i-1} \oplus C_{i-2} \arrow[r, "\pi_{i-1}"] & C_{i-2} \arrow[r] & 0 \end{tikzcd}$$

commutes and exact:

- $\mathrm{d} \circ \rho(z_1) = \mathrm{d}(z_1, 0) = (\partial z_1, 0)$
- $\rho \circ \partial(z_1) = \rho(\partial z_1) = (\partial z_1, 0)$
- $\partial \circ \pi(z_1, z_2) = \partial(z_2) = \partial z_2$
- $\pi \circ \mathrm{d}(z_1, z_2) = \pi(\partial z_1 + (-1)^{i-1} x z_2, \partial z_2) = \partial z_2$

□

Coro 2.3.2. This induces a long exact sequence

$$\cdots \to H_i(C_\bullet) \xrightarrow{\rho_*} H_i(C_\bullet \otimes K_\bullet(x)) \xrightarrow{\pi_*} H_i(C_\bullet(-1)) \xrightarrow{\pm x} H_{i-1}(C_\bullet) \to \cdots.$$

Proof. We only need to show the connection homomorphism is indeed $\pm x$.

Given $z \in C_{i-1}$ with $\partial z = 0$,

$$z \xmapsto{\pi^{-1}} (0, z) \xmapsto{d} \big((-1)^{i-1} x z, 0\big) \xmapsto{\rho^{-1}} (-1)^{i-1} x z.$$

□

Def 40. We call x to be $C_\bullet$-regular, if x is not a zero divisor of C_i and $C_i/xC_i \neq 0$, for all $i \geq 0$.

Prop 2.3.3. If x is $C_\bullet$-regular, then $H_i(C_\bullet \otimes K_\bullet(x)) \cong H_i(C_\bullet/xC_\bullet)$ for all $i \geq 0$.

Proof. Let

$$\begin{array}{rcl} \phi_i : C_i \oplus C_{i-1} & \to & C_i/xC_i \\ (z_1, z_2) & \mapsto & \overline{z_1} \end{array},$$

then

$$\begin{tikzcd} C_i \oplus C_{i-1} \arrow[r, "\phi_i"] \arrow[d, "\mathrm{d}_i"] & C_i/xC_i \arrow[d, "\overline{\partial}_i"] \\ C_{i-1} \oplus C_{i-2} \arrow[r, "\phi_{i-1}"] & C_{i-1}/xC_{i-1} \end{tikzcd}$$

commutes.

- $\overline{\partial} \circ \phi_i(z_1, z_2) = \overline{\partial}(z_1) = \overline{\partial z_1}$.
- $\phi_{i-1} \circ \mathrm{d}(z_1, z_2) = \phi_{i-1}(\partial z_1 + (-1)^{i-1}xz_2, \partial z_2) = \overline{\partial z_1}$, since $xz_2 \in xC_{i-1}$.

Now we need to show the induced maps

$$\begin{array}{rcl} \phi_{*i} : \ker \mathrm{d}_i / \operatorname{im} \mathrm{d}_{i+1} & \to & \ker \overline{\partial}_i / \operatorname{im} \overline{\partial}_{i+1} \\ \overline{(z_1, z_2)} & \mapsto & \overline{\overline{z_1}} = \overline{z_1} + \operatorname{im} \overline{\partial}_{i+1} \end{array}$$

are isomorphisms.

- Onto:
  For $\overline{z} \in \ker \overline{\partial}_i$ with $\partial z = xz' \in xC_{i-1}$, $z' \in C_{i-1}$. Then $\phi_i(z, (-1)^i z') = \overline{z}$, and $\mathrm{d}(z, (-1)^i z') = (\partial z - xz', (-1)^i \partial z') = (0, 0)$, so $(z, (-1)^i z') \in \ker \mathrm{d}_i$. (Since $x\partial z' = \partial(xz') = \partial^2 z = 0$, and x is not a zero divisor of C_i, so $\partial z' = 0$.)

  Now, $\phi_{*i}\left(\overline{(z, (-1)^i z')}\right) = \overline{\overline{z}}$, so ϕ_{*i} is onto.
- 1-1:
  Let $(z, z') \in \ker \mathrm{d}_i$ with $\phi_i(z, z') = \overline{z} \in \operatorname{im} \overline{\partial}_{i+1}$, i.e. $\overline{z} = \partial \overline{z''}$ with $z'' \in C_{i+1}$. This means $z - \partial z'' = xz'''$ with $z''' \in C_i$, so $\partial(z - \partial z'') = \partial z = x\partial z'''$.

  On the other hand, $\mathrm{d}(z, z') = (\partial z + (-1)^{i-1}xz', \partial z') = (0, 0)$, so $\partial z = (-1)^i xz', \partial z' = 0$.

  So $\mathrm{d}(z'', (-1)^i z''') = (\partial z'' + (-1)^{2i}xz'''), (-1)^i \partial z''') = (z, z')$, i.e. $(z, z') \in \operatorname{im} d_{i+1}$. ($\partial z = x\partial z''' = (-1)^i xz'$, since x is not a zero divisor, so $\partial z''' = (-1)^i z'$.)

  Hence, $\phi_{*i}\left(\overline{(z_1, z_2)}\right) = \overline{0}$ implies $\overline{(z_1, z_2)} = \overline{0}$, so ϕ_{*i} is 1-1.

□

Def 41. Let $M \in \mathbf{Mod}_R$. A sequence $\{a_1, \cdots, a_m\}, m \geq 0$ is said to be M-regular if

- $M/\langle a_1, \cdots, a_m \rangle M \neq 0$.
- a_{i+1} is not a zero divisor of $M/\langle a_1, \cdots, a_i \rangle M$ for $0 \leq i \leq m - 1$.

Theorem 32. If $\mathbf{x} = (x_1, \cdots, x_n)$ is an R-regular sequence, then $K_\bullet(\mathbf{x}) \to R/\langle x_1, \cdots, x_n \rangle \to 0$ is a free resolution of $R/\langle x_1, \cdots, x_n \rangle$.

Proof. Since its modules are $K_i(\mathbf{x}) = \Lambda^i R^n \cong R^{\binom{n}{i}}$, i.e. free R-modules, so we only need to show the exactness.

By induction on n,

- $n = 1$: $K_\bullet(x_1) : 0 \to R \xrightarrow{x_1} R \to R/\langle x_1 \rangle \to 0$ exact.

- $n > 1$: Assume that $\mathbf{x}' = (x_1, \cdots, x_{n-1})$ and $K_\bullet(\mathbf{x}') \to R/\langle x_1, \cdots, x_{n-1}\rangle \to 0$ exact, i.e. $H_i(K_\bullet(\mathbf{x}')) = 0$ for $i > 0$.

  Since we have $K_\bullet(\mathbf{x}) \cong K_\bullet(\mathbf{x}') \otimes K_\bullet(x_n)$ and a long exact sequence
  $$\cdots \to H_i(K_\bullet(\mathbf{x}')) \to H_i(K_\bullet(\mathbf{x})) \to H_i(K_\bullet(\mathbf{x}')(-1)) \xrightarrow{\pm x_n} H_{i-1}(K_\bullet(\mathbf{x}')) \to \cdots$$
  where $H_i(K_\bullet(\mathbf{x}')(-1)) = H_{i-1}(K_\bullet(\mathbf{x}'))$.

  For $i > 1$, the sequence becomes
  $$\cdots \to 0 \to H_i(K_\bullet(\mathbf{x})) \to 0 \xrightarrow{\pm x_n} \cdots,$$
  so $H_i(K_\bullet(\mathbf{x})) = 0$.

  For $i = 1$, we have $H_0(K_\bullet(\mathbf{x}')) \cong R/\langle x_1, \cdots, x_{n-1}\rangle$, so
  $$0 \to H_1(K_\bullet(\mathbf{x})) \to R/\langle x_1, \cdots, x_{n-1}\rangle \xrightarrow{\pm x_n} R/\langle x_1, \cdots, x_{n-1}\rangle$$
  But x_n is not a zero divisor of $R/\langle x_1, \cdots, x_{n-1}\rangle$, so the map $\pm x_n$ is 1-1, then $H_1(K_\bullet(\mathbf{x})) \cong \ker(\pm x_n) = 0$.

$\square$

Eg 2.3.1. Let $\mathbf{x} = (x_1, x_2)$, then
$$K_\bullet(\mathbf{x}) : 0 \to R \xrightarrow{\alpha} R^2 \xrightarrow{\beta} R \xrightarrow{q} R/\langle x_1, x_2\rangle \to 0$$
with $\alpha : r \mapsto (-x_2 r, x_1 r)$ and $\beta : (r_1, r_2) \mapsto x_1 r_1 + x_2 r_2$.

Coro 2.3.3. Let $I = \langle x_1, \cdots, x_n\rangle \subset R$ be an ideal with $\{x_1, \cdots, x_n\}$ be R-regular, then R/I has *projective dimension* $\mathrm{pd}(R/I) = n$, i.e. the shortest projective resolution of R/I has length n.

Proof. $K_\bullet(\mathbf{x})$ is already a projective resolution of length N, so we only need to show that there's no shorter ones.

The left side of $K_\bullet(\mathbf{x})$ reads
$$0 \to \Lambda^n R^n \xrightarrow{d_n} \Lambda^{n-1} R^n \to \cdots$$
But
$$\Lambda^n R^n = R(e_1 \wedge \cdots \wedge e_n) \cong R, \quad \Lambda^{n-1} R^n = \bigoplus_{i=1}^{n} R(e_1 \wedge \cdots \wedge \hat{e_i} \wedge \cdots \wedge e^n) \cong R^n$$
so
$$\begin{aligned} d_n : R \to &\ R^n \\ r \mapsto &\ (x_1 r, -x_2 r, \cdots, (-1)^{n-1} x_n r) \end{aligned}$$
Taking tensor with R/I, we get
$$0 \to R \otimes_R R/I \xrightarrow{d_n \otimes \mathbf{1}} R^n \otimes_R R/I \to \cdots$$
but $R \otimes_R R/I \cong R/I, R^n \otimes_R R/I \cong (R/I)^n$, so
$$\begin{aligned} d_n \otimes \mathbf{1} : R/I \to &\ (R/I)^n \\ \overline{r} \mapsto &\ (\overline{x_1 r}, \overline{-x_2 r}, \cdots, \overline{(-1)^{n-1} x_n r}) \end{aligned}$$
Now,
$$\mathrm{Tor}_n(R/I, R/I) = H_n(K_\bullet(\mathbf{x}) \otimes R/I) = \ker(d_n \otimes \mathbf{1}) = \mathrm{Ann}_{R/I}\, I = \{\overline{r} \in R/I \mid rI = I\} = R/I \neq 0.$$
($R/I \neq 0$ is because $\{x_1, \cdots, x_n\}$ is R-regular.) Thus, any projective resolution can't have length shorter than n since that will imply $\mathrm{Tor}_n(R/I, R/I) = 0$. $\square$

Remark 4. Let $I = \langle x_1, \cdots, x_n \rangle$ generated by R-regular sequence $\{x_1, \cdots, x_n\}$, then

- $\mathrm{Tor}_n(R/I, M) \cong \mathrm{Ann}_M I$.
- $\mathrm{Ext}^n(R/I, M) \cong M/IM$.

2.4 Derived category

Def 42.

- $\mathcal{C}$ is a pre-additive category if $\mathrm{Hom}_{\mathcal{C}}(X, Y)$ is an abelian group $\forall\, X, Y \in \mathcal{C}$ s.t.

$$X \xrightarrow{u} Y \overset{f}{\underset{g}{\rightrightarrows}} Z \xrightarrow{v} T$$

  with $(f+g)u = fu + gu$ and $v(f+g) = vf + vg$.
- addivitve category: a pre-additive category $\mathcal{C}$ s.t.
  - There exists a zero object 0 s.t. $\forall\, X$, $\mathrm{Hom}_{\mathcal{C}}(0, X) = \{0\} = \mathrm{Hom}_{\mathcal{C}}(X, 0)$.
  - Finite sum and finite products exist.

Def 43.

- $f \in \mathrm{Hom}(B, C)$ is called a monomorphism if $\forall\, X \xrightarrow{g} B \xrightarrow{f} C$ with $f \circ g = 0 \implies g = 0$.
- $f \in \mathrm{Hom}(B, C)$ is called a epimorphism if $\forall\, B \xrightarrow{f} C \xrightarrow{h} D$ with $h \circ f = 0 \implies h = 0$.
- a kernel of $f \in \mathrm{Hom}(B, C)$ is a morphism $i : A \to B$ s.t. $f \circ i = 0$ and $\forall\, g : X \to B$ with $f \circ g = 0$, we have

$$\begin{tikzcd} A \arrow[r, "i"] & B \arrow[r, "f"] & C \\ & X \arrow[ul, dashed, "\exists!"] \arrow[u, "g"] \arrow[ur, "0"'] & \end{tikzcd}$$

- a cokernel of $f \in \mathrm{Hom}(B, C)$ is a morphism $p : C \to D$ s.t. $p \circ f = 0$ and $\forall\, h : C \to Y$ with $h \circ f = 0$, we have

$$\begin{tikzcd} B \arrow[r, "f"] \arrow[dr, "0"'] & C \arrow[r, "p"] \arrow[d, "h"] & D \arrow[dl, dashed, "\exists!"] \\ & Y & \end{tikzcd}$$

Remark 5.

- If i is a kernel of f, then i is a monomorphism.
- If p is a cokernel of f, then p is a epimorphism.

Remark 6. An epimorphism may not be a cokernel. Consider $\mathbb{Z} \xrightarrow{\times 3} \mathbb{Z}$ which is an epimorphism in the category of f.g. free $\mathbb{Z}$-modules. If $\mathbb{Z} \xrightarrow{\times 3} \mathbb{Z}$ is the cokernel of $G \xrightarrow{f} \mathbb{Z}$, then

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[dr, "0"'] & \mathbb{Z} \arrow[r, "\times 3"] \arrow[d, "\times 2"] & \mathbb{Z} \arrow[dl, dashed, "\exists!\, \tilde{f}"] \\ & \mathbb{Z} & \end{tikzcd}$$

This implies $\tilde{f} : 1 \mapsto \frac{2}{3}$, which is impossible.

Def 44. $\mathcal{A}$ is an **abelian category** if it is an additive category s.t.

- kernels and cokernels always exist in $\mathcal{A}$.
- every monomorphism is a kernel and every epimorphism is a cokernel.

Fact 2.4.1. If $\mathcal{A}$ is an abelian category, then:

- every morphism is expressible as the composite of an epimorphism and a monomorphism. Given $f : B \to C$, we have

$$\begin{tikzcd} B \arrow[rr, "f"] \arrow[dr, two heads] & & C \\ & \operatorname{Im} f \arrow[ur, hook] & \end{tikzcd}$$

  where $\operatorname{Im} f$ is unique up to isomorphism.

  Proof. Consider the following diagram:

$$\begin{tikzcd} \ker f \arrow[r, hook, "i"] & B \arrow[r, "f"] \arrow[d, two heads, "p'"] \arrow[dr, dashed, "\exists \mu"] & C \arrow[r, two heads, "p"] & \operatorname{coker} f \\ & \operatorname{coker} i \arrow[r, dashed, "\exists ! \sigma"'] \arrow[ur, dashed, "\exists \nu"] & \ker p \arrow[u, hook, "i'"'] & \end{tikzcd}$$

  where μ, ν exist because i', p' are kernel and cokernel. Now, $i'\mu i = fi = 0$, and since i' is a monomorphism, $\mu i = 0$. Moreover, since p' is the cokernel of i, there exists a unique σ letting the diagram commute.

  By exercise, σ is both a monomorphism and epimorphism. In an abelian category, this implies that σ is actually an isomorphism (i.e., σ^{-1} exists). $\square$

- $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact if f is monomorphism, g is epimorphism and $\operatorname{Im} f = \ker g$.

Theorem 33 (Freyd-Mitchell theorem)**.** A small abelian category is equivalent to a full subcategory of a category of R-modules.

Def 45.

- $I \in \operatorname{Obj} \mathcal{A}$ is injective if the functor $\operatorname{Hom}(-, I)$ is exact.
- An abelian category is said to be **enough injectives** if for any $A \in \operatorname{Obj} \mathcal{A}$, there exists an injective object I such that $A \hookrightarrow I$.

Def 46. Given a functor $F : \mathcal{A} \to \mathcal{B}$ satisfy:

1. F is additive, which is to say F is a group homomorphism $\operatorname{Hom}(A, A') \to \operatorname{Hom}(FA, FA')$.
2. F is left exact. If $0 \to A' \to A \to A'' \to 0$, then $0 \to FA' \to FA \to FA''$.

Then the derived functor $R^i F : \mathcal{A} \to \mathcal{B}$ is defined as

$$R^i F(A) = \begin{cases} F(A), & \text{if } i = 0 \\ H^i(F(I^\bullet)), & \text{else} \end{cases}$$

Our goal is to construct the derived category $D^+(\mathcal{A})$ and $D^+(\mathcal{B})$ letting RF be a exact functor.

Def 47. Let $\mathcal{A}$ be an abelian category.

- $\operatorname{Kom}(\mathcal{A})$ is the category of complexes over $\mathcal{A}$.

- $K(\mathcal{A})$ is the homotopy category of $\mathcal{A}$, defined by $\mathrm{Obj}(K(\mathcal{A})) = \mathrm{Obj}(\mathrm{Kom}(\mathcal{A}))$ and

$$\mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, B^\bullet) = \mathrm{Hom}_{\mathrm{Kom}(\mathcal{A})}(A^\bullet, B^\bullet)/\sim,$$

where $\sim$ indicates homotopy equivalences.

Remark 7.

- $\mathrm{Hom}_{K(\mathcal{A})}(I_A^\bullet, I_B^\bullet) \cong \mathrm{Hom}_{\mathcal{A}}(A, B)$ by comparison theorem (26).
- It could be shown that $K(\mathcal{A})$ is additive but may not be abelian.

Def 48. $f \in \mathrm{Hom}_{K(\mathcal{A})}(A^\bullet, B^\bullet)$ is called a quasi-isomorphism if $H^n(f)$ is an isomorphism between $H^n(A^\bullet)$ and $H^n(B^\bullet)$ for each n.

Eg 2.4.1.

- A quasi-isomorphism is often not invertible. For example:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "\times 2"] \arrow[d] & \mathbb{Z} \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \cdots \\ 0 \arrow[r] & 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \arrow[r] & \cdots \end{tikzcd}$$

- Given $0 \to A \to I^\bullet$,

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & 0 \arrow[r] \arrow[d] & \cdots \\ 0 \arrow[r] & I^0 \arrow[r] & I^1 \arrow[r] & I^2 \arrow[r] & \cdots \end{tikzcd}$$

are two quasi-isomorphic complexes.

Def 49. Let $\mathcal{B}$ be a category. A class of morphism $S \subset \mathrm{Mor}(\mathcal{B})$ is said to be **localizing** if

1. S is closed under composition with $\mathrm{Id}_X \in S$ for each object X in $\mathcal{B}$.
2. Extension condition holds: For each $f \in \mathrm{Mor}\,\mathcal{B}$, $s \in S$ as in the following diagram, exists $g \in \mathrm{Mor}\,\mathcal{B}$, $t \in S$ such that $ft = sg$. The dual version should hold as well.

$$\begin{tikzcd} A \arrow[r, "g"] \arrow[d, "t"] & B \arrow[d, "s"] \\ C \arrow[r, "f"] & D \end{tikzcd}$$

3. For any $f, g \in \mathrm{Hom}(X, Y)$,

$$\exists\, s \in S \text{ s.t. } sf = sg \iff \exists\, t \in S \text{ s.t. } ft = gt.$$

Theorem 34. If S is localizing, then there exists a category $\mathcal{B}[S^{-1}]$ with a functor $Q : \mathcal{B} \to \mathcal{B}[S^{-1}]$ such that

1. $Q(s)$ is an isomorphism for each $s \in S$.
2. Given another functor $F : \mathcal{B} \to \mathcal{B}'$ satisfy condition 1, there exists a unique functor $G : \mathcal{B}[S^{-1}] \to \mathcal{B}'$ such that $F = G \circ Q$.

Proof. Define a roof to be a pair (s, t) with

$$\begin{tikzcd} & X' \arrow[dl, "S \ni s"'] \arrow[dr, "t"] & \\ X & & Y \end{tikzcd}$$

Also, define $(s,f) \sim (t,g)$ if there exists Z such that

$$\begin{tikzcd}
 & X' \arrow[dl, "s"'] \arrow[dr, "f"] & \\
X & Z \arrow[u, "p"] \arrow[d, "q"] & Y \\
 & X'' \arrow[ul, "t"] \arrow[ur, "g"'] &
\end{tikzcd}$$

with $sp = tq \in S$ and $fp = gq$.

First we check that "$\sim$" is indeed an equivalence relation. $(s,f) \sim (s,f)$ and $(s,f) \sim (t,g) \implies (t,g) \sim (s,f)$ are trivial. If $(s,f) \sim (t,g)$ and $(t,g) \sim (u,h)$, then we have the following diagram:

$$\begin{tikzcd}
 & X' \arrow[ddl, "s"'] \arrow[ddr, "f"] & & & \\
 & Z \arrow[u, "p"] \arrow[d, "q"] & & & \\
A & X'' \arrow[l, "t"] \arrow[r, "g"] & B & R \arrow[ull, "\exists\, z"'] \arrow[dll, "\exists\, a"] & T \arrow[l, "\exists\, w"] \\
 & W \arrow[u, "r"] \arrow[d, "v"] & & & \\
 & X''' \arrow[uul, "u"] \arrow[uur, "h"'] & & &
\end{tikzcd}$$

Using definition 2. on $tr \in S$ and sp, there are morphism z, a with $z \in S$ and $spz = tra$. Moreover, $tqz = spz = tra$, if we let $b = qz, c = ra$, then by 3., morphism $w \in S$ exists with $bw = cw$. Define $x = pzw, y = vaw$, we have $sx = spzw = tqzw = tbw = tcw = traw = uvaw = uy$ and $sx \in S$ since $sx = spzw$ and sp, z, w are all in S. Similarly, $fx = hy$, thus $(s,f) \sim (u,h)$. Hence we've just proved that $\sim$ is an equivalence relation.

Now we could construct the localized category as following: The objects are $\mathrm{Obj}(\mathcal{B}[S^{-1}]) = \mathcal{B}$ and $\mathrm{Mor}(\mathcal{B}[S^{-1}]) = \{$ equivalence classes under $\sim \}$. $[(t,g)] \circ [(s,f)] = [(su, gh)]$ could be defined as in the following diagram:

$$\begin{tikzcd}
 & & \exists\, U \quad \text{by 2.} \arrow[dl, "S \ni u"'] \arrow[dr, "h"] & & \\
 & X \arrow[dl, "s"'] \arrow[dr, "f"] & & Y \arrow[dl, "t"'] \arrow[dr, "g"] & \\
A & & B & & C
\end{tikzcd}$$

$\square$

Finally, define functor Q by $Q(X) = X, \forall\, X \in \mathrm{Obj}(\mathcal{B})$ and $Q(f) = [(\mathrm{Id}_X, f)]$. For the universal property, if F is another functor making every morphism in S be invertible, then the functor G exists uniquely by $G([(s,f)]) = F(f)F(s)^{-1}$. By induction hypothesis, we can say $m - 1 = n - 1$. Done.

Def 50. The mapping cone of a chain map f between two chain $X^\bullet \xrightarrow{f} Y^\bullet$ is defined as a chain with $\text{cone}(f)^n = X^{n+1} \oplus Y^n$, and the chain map is defined as

$$\begin{aligned} d_{\text{cone}(f)} : \text{cone}(f)^n = X^{n+1} \oplus Y^n &\longrightarrow \text{cone}(f)^{n+1} = X^{n+2} \oplus Y^{n+1} \\ (x_{n+1}, y_n) &\xmapsto[\begin{pmatrix} -d_X & 0 \\ f & d_Y \end{pmatrix}]{} \big(- d_X(x^{n+1}), f(x^{n+1}) + d_Y(y_n)\big) \end{aligned}$$

It is easy to see that $d^2_{\text{cone}(f)} = 0$.

Prop 2.4.1. Suppose that $f : X^\bullet \to Y^\bullet$ is a chain map, then there is a short exact sequence

$$\begin{aligned} 0 \longrightarrow Y \longrightarrow \text{cone}(f) &\longrightarrow X[+1] \longrightarrow 0 \\ y \longmapsto (0, y)& \\ (x, y) &\longmapsto x \end{aligned}$$

Proof. It is easy to see that the rows are exact. Tracing the diagram shows that the diagram commutes. ☐

Coro 2.4.1. There exists a long exact sequence of homology:

$$\cdots \to H^m(Y^\bullet) \to H^m(\text{cone}(f)) \to H^{m+1}(X^\bullet) \xrightarrow{\delta} H^{m+1}(Y^\bullet) \to H^{m+1}(\text{cone}(f)) \to \cdots$$

Where the connecting homomorphism $\delta = f^*$.

Proof. Tracing the diagram below as in the snake lemma,

$$\begin{tikzcd} & X^m \oplus Y^{m-1} \arrow[r] \arrow[d] & X^m \arrow[d] \\ Y^m \arrow[r] & X^{m+1} \oplus Y^m \arrow[r] & X^{m+1} \end{tikzcd}$$

Suppose $\bar{x} \in H^m(X^\bullet)$, then $d_X(x) = 0$, so $d(x, 0) = (-d_X(x), f(x)) = (0, f(x))$, which implies $f(x) :: Y^m \mapsto d(x, 0) :: X^{m+1} \oplus Y^m$, then $\delta(\bar{x}) = \overline{f(x)}$, so $\delta = f^*$. ☐

Coro 2.4.2. $\text{cone}(f)$ acyclic (exact) $\iff$ f quasi-isomorphic.

Proof. Directly by the exact sequence

$$H^{m-1}(\text{cone}(f)) \to H^m(X^\bullet) \to H^m(Y^\bullet) \to H^m(\text{cone}(f))$$

☐

Notice that $X[-k]$ is defined as $X[-k]^n = X^{n-k}$ with $d_{X[-k]} = (-1)^k d_X$ below.

Theorem 35. Let $\mathcal{A}$ be an abelian category and $K(\mathcal{A})$ be the homotopy category. Then the class of quasi-isomorphisms are localizing.

Proof. We check that:

1. It is closed under composition: If f, g are quasi-isomorphic, then $(fg)^* = f^* g^*$ is a isomorphism since both f^*, g^* are, thus fg is quasi-isomorphic.

2. The diagram could be completed:

$$\begin{tikzcd} \exists\, W^\bullet \arrow[r, dashed] \arrow[d, dashed] & Z^\bullet \arrow[d, "g\text{: q-iso}"] \\ X^\bullet \arrow[r, "f"] & Y^\bullet \end{tikzcd}$$

Consider the following diagram:

$$\begin{tikzcd} \mathrm{cone}(\pi f)[-1] \arrow[r, "k", "(x_n,z_n,y_{n-1})\mapsto x_n"'] \arrow[d, "(x_n,z_n,y_{n-1})\mapsto z_n"', "h{[-1]}"] & X^\bullet \arrow[r, "\pi f"] \arrow[d, "f"] & \mathrm{cone}(g) \arrow[d, equal] \\ Z^\bullet \arrow[r, "k", "z_n\mapsto g(z_n)"'] & Y^\bullet \arrow[r, "\pi", "y_n\mapsto(0,y_n)"'] & \mathrm{cone}(g) \end{tikzcd}$$

Where $\mathrm{cone}(\pi f)^n \cong X^{n+1} \oplus \mathrm{cone}(g)^n \cong X^{n+1}Z^{n+1}Y^n$.

We claim that $fk \simeq gh[-1]$. Since $(fk - gh[-1])(x_n, z_n, y_{n-1}) = f(x_n) + g(z_n)$. Define

$$\begin{aligned} \varphi : \mathrm{cone}(\pi f)[-1]^n = \mathrm{cone}(\pi f)^{n-1} &\longrightarrow Y^{n-1} \\ (x_n, z_n, y_{n-1}) &\longmapsto -y_{n-1} \end{aligned}$$

Then

$$\begin{aligned} \varphi d_{C(\pi f)[-1]}(x_n, (z_n, y_{n-1})) &= \varphi(d(x_n), -\pi f(x_n) - d(z_n, y_{n-1})) \\ &= \varphi(d(x_n), -(0, f(x_n)) - (d(z_n), g(z_n) + d(y_{n-1}))) \\ &= \varphi(d(x_n), -d(z_n), -f(x_n) - g(z_n) - d(y_{n-1})) \\ &= f(x_n) + g(z_n) + d(y_{n-1}) \end{aligned}$$

and $d_Y\varphi(x_n, z_n, y_{n-1}) = -d(y_{n-1})$, so $\varphi d_{C(\pi f)[-1]} + d_Y\varphi = fk - gh[-1]$, thus $fk \simeq gh[-1]$.

3. Let $f : X^\bullet \to Y^\bullet$ in $K(\mathcal{A})$. We shall prove that

$$\exists\, s : Y^\bullet \to Z^\bullet \text{ s.t. } sf = 0 \iff \exists\, t : W^\bullet \to X^\bullet \text{ s.t. } ft = 0$$

Let $h^i : X^i \to Z^{i-1}$ be a homotopy bewteen sf and 0. Consider the diagram:

$$\begin{tikzcd} \mathrm{cone}(s)[-1] \arrow[d, equal] & X^\bullet \arrow[l, "g"', "(f(x_n),-h(x_n))\leftarrow\!\shortmid x_n"] \arrow[d, "f"] & \mathrm{cone}(g)[-1] = W^\bullet \arrow[l, "t"'] & \\ \mathrm{cone}(s)[-1] \arrow[r, "p{[-1]}"] & Y^\bullet \arrow[r, "s"] & Z^\bullet \arrow[r, "\pi"] & \mathrm{cone}(s) \end{tikzcd}$$

One can easily check that g is a chain map, which congruent with the boundary map (because of h^i). Now, we have $ft = p[-1]gt$, but $gt \simeq 0$ by

$$\begin{aligned} k_n : \qquad W^n = X^n \oplus Y^{n-1} \oplus Z^{n-2} &\longrightarrow C(s)[-1]^{n-1} = Y^{n-1} \oplus Z^{n-2} \\ (x_n, y_{n-1}, z_{n-2}) &\longmapsto (y_{n-1}, z_{n-2}) \end{aligned}$$

since

$$\begin{aligned} kd(x_n, y_{n-1}, z_{n-2}) &= k(-(dx_n, g(x_n) + d(y_{n-1}, z_{n-2}))) \\ &= k(-dx_n, -(f(x_n), -h(x_n)) + (-dy_{n-1}, g(y_{n-1}) + dz_{n-2})) \\ &= (-f(x_n) - dy_{n-1}, h(x_n) + g(y_{n-1}) + dz_{n-2}) \end{aligned}$$

and $dk(x_n, y_{n-1}, z_{n-2}) = d(y_{n-1}, z_{n-2}) = (dy_{n-1}, -g(y_{n-1}) - dz_{n-2})$. Thus $dk + kd = -gt \implies gt \simeq 0$.

Now, since s is quasi-isomorphic, by corollary 2.4.2, cone(s) is acyclic, and thus t is quasi-isomorphic. Hence we've find t so that $ft \simeq 0$.

We could then define the derived category as $D(\mathcal{A}) = K(\mathcal{A})[S^{-1}]$ now. $\square$

Prop 2.4.2. The derived category is additive.

Proof. Let $\varphi, \varphi' : X \to Y$ in $D(\mathcal{A})$ with $\varphi = [(s,f)], \varphi' = [(s', f')]$, that is, we have the following two diagram

$$\begin{tikzcd} & Z \arrow[dl, "s"'] \arrow[dr, "f"] & \\ X & & Y \end{tikzcd} \qquad \begin{tikzcd} & Z' \arrow[dl, "s'"'] \arrow[dr, "f'"] & \\ X & & Y \end{tikzcd}$$

using 2. in the definition of localizing, exists U so that

$$\begin{tikzcd} \exists\, U \arrow[r, "r'"] \arrow[d, "r"] & Z' \arrow[d, "s'"] \\ Z \arrow[r, "s"] & X \end{tikzcd}$$

with one of r, r' is guaranteed to be quasi-isomorphic, say r. But then $H^n(U) \cong H^n(Z) \cong H^n(X) \cong H^n(Z')$ since r, s, s' are all quasi-isomorphic. This implies r' is also quasi-isomorphic, so we'll have the new roof for φ

$$\begin{tikzcd} & & U \arrow[dl, "r"'] \arrow[dd, "g"] \arrow[ddll, bend right] \\ & Z \arrow[dl, "s"'] \arrow[dr, "f"] & \\ X & & Y \end{tikzcd}$$

Similarly, this applies to φ'. Since $rs = r's'$, we could define $\varphi + \varphi' = [(rs, g + g')]$. $\square$

Def 51. Let $\mathcal{A}, \mathcal{B}$ be abelian categories, $F : \mathcal{A} \to \mathcal{B}$ be an additive functor.

- Define $D^+(\mathcal{A})$ as a subcategory of $D(\mathcal{A})$ consist of all the objects (chains) $X^\bullet$ in $D(\mathcal{A})$ such that $X^i = 0$ for all $i \leq i_0(X^\bullet)$. $K^+(\mathcal{A})$ is defined similarly.
- Assume that F act on complexes component wise. $K^+(F) : K^+(\mathcal{A}) \to K^+(\mathcal{B})$.
- A triangle in $K^+(\mathcal{A})$ is a diagram of the form $\triangle : X^\bullet \to Y^\bullet \to Z^\bullet \to X^\bullet[1]$
- $\triangle$ is said to be distinguished if

$$\begin{tikzcd} X^\bullet \arrow[r, "f"] \arrow[d, "\wr"] & Y^\bullet \arrow[r] \arrow[d, "\wr"] & Z^\bullet \arrow[r] \arrow[d, "\wr"] & X^\bullet[1] \arrow[d, "\wr"] \\ \bar{X}^\bullet \arrow[r, "\bar{f}"] & \bar{Y}^\bullet \arrow[r] & \operatorname{cone}(\bar{f}) \arrow[r] & \bar{X}^\bullet[1] \end{tikzcd}$$

  In this case, we denote it as $\triangle\!\!\!\!\cdot\;$.

Recall that $\bar{Y}^\bullet \to \operatorname{cone}(\bar{f}) \to \bar{X}^\bullet$ induces a long exact sequence

$$\cdots \to H^i(\bar{Y}) \to H^i(\operatorname{cone}(\bar{f})) \to H^i(\bar{X}[1]) \to H^{i+1}(\bar{Y}) \to \cdots$$

Prop 2.4.3. Let $F : \mathcal{A} \to \mathcal{B}$ be an exact functor, then

1. The exact functor $D^+(F) : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ exists.

2. $D^+(F)$ preserves distinguished triangle, (i.e., $\triangle \mapsto \triangle$.)

Proof. First, we have the following observation:

- F sends acyclic chain to acyclic chain: If $X^\bullet$ acyclic, then $X^\bullet$ could be decomposed to many short exact sequence:
$$0 \to \ker d_X^i \to X^i \to \ker d_X^{i+1} \to 0$$
Apply F we would then get
$$0 \to F(\ker d_X^i) \to F(X^i) \to \ker d_X^{i+1} \to 0$$
which we could connect them and get the desired exact sequence
$$\cdots \to F(X^{i-1}) \to F(X^i) \to F(X^{i+1}) \to \cdots$$

- If $f : X^\bullet \to Y^\bullet$, then $F(f) : F(X)^\bullet \to F(Y)^\bullet$, and we have $F(\mathrm{cone}(f)) \cong \mathrm{cone}(F(f))$, since $F(\mathrm{cone}(f))^n = F(X^{n+1} \oplus Y^n) \cong F(X^{n+1}) \oplus F(Y^n) = \mathrm{cone}(F(f))^n$ because F is additive. Moreover, the boundary map $d_{\mathrm{cone}(F(f))}$ is
$$\begin{pmatrix} -F(d_X) & 0 \\ F(f) & F(d_Y) \end{pmatrix} = F \begin{pmatrix} d_X & 0 \\ f & d_Y \end{pmatrix} = d_{F(\mathrm{cone}(f))}$$
Since F transform the object and morphisms consistently, thus $F(\mathrm{cone}(f)) \cong \mathrm{cone}(F(f))$. Similarly we have $F(\mathrm{cyl}(f)) \cong \mathrm{cyl}(F(f))$.

Now, return to our proof:

1. If f quasi-isomorphic, then $\mathrm{cone}(f)$ acyclic by corollary 2.4.2, and $F(\mathrm{cone}(f)) \cong \mathrm{cone}(F(f))$ acyclic by the discussion above, and finally $F(f)$ acyclic by the same corollary. Thus F preserves quasi-isomorphisms.

   Moreover, we could complete the following diagram
$$\begin{tikzcd} K^+(\mathcal{A}) \arrow[r, "K^+(F)"] \arrow[d, "Q_A"] & K^+(\mathcal{B}) \arrow[d, "Q_B"] \\ K^+(\mathcal{A})[S_A^{-1}] \arrow[r, "\exists ! D^+(F)"] & K^+(\mathcal{B})[S_B^{-1}] \end{tikzcd}$$
   since F send quasi-isomorphisms to quasi-isomorphism and by the universal property of the localized category. Thus $D^+(f)$ exists.

2. Apply $D^+(F)$ to the diagram
$$\begin{tikzcd} X^\bullet \arrow[r, "f"] \arrow[d, "\wr"] & Y^\bullet \arrow[r] \arrow[d, "\wr"] & Z^\bullet \arrow[r] \arrow[d, "\wr"] & X^\bullet[1] \arrow[d, "\wr"] \\ \bar{X}^\bullet \arrow[r, "\bar{f}"] & \bar{Y}^\bullet \arrow[r] & \mathrm{cone}(\bar{f}) \arrow[r] & \bar{X}^\bullet[1] \end{tikzcd}$$
   We get
$$\begin{tikzcd} FX^\bullet \arrow[r, "Ff"] \arrow[d, "\wr"] & FY^\bullet \arrow[r] \arrow[d, "\wr"] & FZ^\bullet \arrow[r] \arrow[d, "\wr"] & FX^\bullet[1] \arrow[d, "\wr"] \\ F\bar{X}^\bullet \arrow[r, "F\bar{f}"] & F\bar{Y}^\bullet \arrow[r] & F\,\mathrm{cone}(\bar{f}) \arrow[r] & F\bar{X}^\bullet[1] \end{tikzcd}$$
   Where the quasi-isomorphisms are preserved by the discussion above.

$\square$

Def 52. A class R of objects in $\operatorname{Obj}\mathcal{A}$ is said to be adapted to a left exact functor F if

1. It is stable under finite direct sums
2. F sends acyclic chain in $\operatorname{Kom}^+(R)$ to acyclic chain (in $\operatorname{Kom}^+(\mathcal{B})$).
3. For each $X \in \operatorname{Obj}\mathcal{A}$, exists $I \in R$ such that $0 \to X \to I$.

Theorem 36. Let F be a left exact functor, R be a class of objects adpated to F. Define S_R to be the class of quasi-isomorphisms on $K^+(R)$ which is localizing since it is stable with the construction of mapping cones. Then $D^+(\mathcal{A}) \cong K^+(R)[S_R^{-1}]$.

Proof. First we claim that for all $C^\bullet \in D^+(\mathcal{A})$ (which we assume $C^i = 0, \forall\, i < 0$), There exists $I^\bullet \in K^+(R)$ such that $C^\bullet \cong I^\bullet$.

We shall construct quasi-isomorphism $t^n : C^n \to I^n$. Using induction on n:

$n = 0$: By the definition of adapting class we have $0 \to C^0 \xrightarrow{t^0} I^0$ for some I^0. Consider the following diagram:

$$\begin{tikzcd}
& 0 \arrow[d] & & \\
0 \arrow[r] & C^0 \arrow[r, "d_C"] \arrow[d, "t^0"] & C^1 \arrow[r, "t^1=ca"] \arrow[d, "a"] & I^1 \\
& I^0 \arrow[r, "b"'] \arrow[urr, "d_I"] & I^0 \amalg_{C^0} C^1 \arrow[ur, "c"'] & \\
& 0 \arrow[ur] & &
\end{tikzcd}$$

Where $I^0 \amalg_{C^0} C^1 \triangleq (I^0 \oplus C^1)/\{(t^0(x), -d_C(x)) \mid x \in C^0\}$.

We shall prove that t^0 is an isomorphism between $H^0(C^\bullet) = \ker d_C^1$ and $H^0(I^\bullet) = \ker d_I^1$. It is obviously 1-1 since $0 \to C^0 \xrightarrow{t^0} I^0$, so we need to check it is onto. For any $y \in \ker d_I^1 = \ker b$ since c is monomorphism. Then $b(y) = 0 \implies (y, 0) = (t^0(x), -d_C^1(x))$ for some $x \in C^0$. So $y = t^0(x)$ with $d_C^1(x) = 0 \implies x \in \ker d_C^1$.

$n = 1$: Consider the diagram now:

$$\begin{tikzcd}
& & C^1 \arrow[r, "d_C^2"] \arrow[dl, "t^1"'] \arrow[d] & C^2 \arrow[r, "t^2"] \arrow[d, "a'"] & I^2 \\
I^0 \arrow[r, "d_I^1"] & I^1 \arrow[r, "f"'] \arrow[urrr, "d_I^2"] & \operatorname{coker} d_I^1 \arrow[r, "b'"] & \operatorname{coker} d_I^1 \amalg_{C^1} C^2 \arrow[ur, "c'"'] & \\
& & 0 \arrow[ur] & &
\end{tikzcd}$$

Similarly, we shall prove that

$$H^1(t) : \frac{\ker d_C^2}{\operatorname{Im} d_C^1} \xrightarrow{\sim} \frac{\ker d_I^2}{\operatorname{Im} d_I^1}$$

is an isomorphism.

- 1-1: Let $t^1(x) \in \operatorname{Im} d_I^1$. Since $t^1 = ca$ and $d_I^1 = cb$, there is y such that $ca(x) = cb(y)$. Since c 1-1, $a(x) = b(y) \implies (0, x) = (y, 0)$. in the pushout, so $(y, -x) = (t^0(z), -d_C^1(z))$ for some $z \in C^0$. Thus $x = d_c^1(z) \in \operatorname{Im} d_C^1$.
- onto: For each $y \in \ker d_I^2 = \ker b'p$ since c' 1-1. Then

  $$b'p(y) = 0 \implies (y + \operatorname{Im} d_I^1, 0) = (t'(x) + \operatorname{Im} d_I^1, -d_C^2(x)) \text{ for some } x \in C^1$$

  in the pushout, so we have $y - t'(x) \in \operatorname{Im} d_I^1$ and $x \in \ker d_C^2$ and thus $H^1(t)(\bar{x}) = \bar{y}$.

$n > 1$: Similar as $n = 1$.

After proving this claim, we shall show that $\mathrm{Hom}_{K^+(R)[S_R^{-1}]}(X^\bullet, Y^\bullet) \cong \mathrm{Hom}_{K^+(\mathcal{A})[S_\mathcal{A}^{-1}]}(X^\bullet, Y^\bullet)$. **We will use left roofs instead of right roofs defined before here.**

- 1-1: If $(f, s) \cong (g, t)$ in $K^+(\mathcal{A})[S_\mathcal{A}^{-1}]$, then

$$
\begin{tikzcd}
 & P \arrow[d] & & \\
X \arrow[ur] \arrow[dr] & T \in \mathcal{A} \arrow[rr, bend left, "\exists\, u", "\sim"'] & Y \arrow[ul, "\sim"'] \arrow[dl, "\sim"] & Z \in R \\
 & Q \arrow[u] & &
\end{tikzcd}
$$

  where u exists by the previous claim.

- onto: Given a roof in $\mathcal{A}$

$$
\begin{tikzcd}
 & Z \in R & \\
 & X' \in \mathcal{A} \arrow[u, "\wr"] & \\
X \arrow[ur, "f"] & & Y \arrow[ul, "s"']
\end{tikzcd}
$$

  We could find a roof in R which is equivalent to it again by the previous claim.

$\square$

Finally, if $F : \mathcal{A} \to \mathcal{B}$ is an additive left exact functor, then we will have $K^+(F) : K^+(\mathcal{A}) \to K^+(\mathcal{B})$ which sends acyclic chain in $K^+(R)$ to acyclic chain in $K^+(\mathcal{B})$. This implies that $K^+(F)$ sends quasi-isomorphism in $K^+(R)$ to quasi-isomorphism in $K^+(\mathcal{B})$. So we have the following diagram:

$$
\begin{tikzcd}
K^+(R) \arrow[r, "K^+(F)"] \arrow[d, "Q_R"] & K^+(\mathcal{B}) \arrow[d, "Q_\mathcal{B}"] \\
I^\bullet \in K^+(R)[S_R^{-1}] \arrow[r, "\exists\, !\bar{F}"] & D^+(\mathcal{B}) \\
D^+(\mathcal{A}) \arrow[u, "\wr"] \arrow[ur, "RF"'] &
\end{tikzcd}
$$

Where $\bar{F}$ exists by the universal property of localization. Then the derived functor RF could be defined with $R^iF(C^\bullet) = H^i(RF(C^\bullet))$.

The universal property of RF is as following: $RF : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ is exact and the diagram commutes:

$$
\begin{tikzcd}
 & D^+(\mathcal{A}) \arrow[dr, "RF"] & \\
K^+(\mathcal{A}) \arrow[ur, "Q_\mathcal{A}"] \arrow[dr, "K^+(F)"'] & & D^+(\mathcal{B}) \\
 & K^+(\mathcal{B}) \arrow[ur, "Q_\mathcal{B}"'] &
\end{tikzcd}
$$

with $\epsilon_F : Q_\mathcal{B} \circ K^+(F) \to RF \circ Q_\mathcal{A}$ being a morphism of functors (???).
Moreover, if $G : D^+(\mathcal{A}) \to D^+(\mathcal{B})$ is another exact functor with $\epsilon_G : Q_\mathcal{B} \circ K^+(F) \to G \circ Q_\mathcal{A}$, then

there is an unique $y : RF \to G$ such that

$$\begin{tikzcd}
 & Q_{\mathcal{B}} \circ K^+(F) \arrow[dl, "\epsilon_F"'] \arrow[dr, "\epsilon_G"] & \\
RF \circ Q_{\mathcal{A}} \arrow[rr, "y \circ Q_{\mathcal{A}}"] & & G \circ Q_{\mathcal{A}}
\end{tikzcd}$$

Now, one may ask that whether $RG \circ RF \cong R(G \circ F)$, the answer is no in generally, but there are spectral sequences so that ... Which is another story then...

Index