Commutative Algebra

Fall Term

December 21, 2025

To all who find beauty in logic.

Syllabus

We are going to take a brief peek into the field of algebraic number theory in this ongoing seminar. Our ultimate goal is to master some basic tools and techniques, for example, the Dedekind domain and the ramification theory.

In the first part of our seminar, we will have a review on some rudiments from the ring theory and homological algebra. We shall simply follow Atiyah's *An Introduction to Commutative Algebra*.

In the second part, we will briefly discuss some basic concepts in algebraic number theory, like the ring $\mathcal{O}_K$, the Dedekind domains, primary decomposition and the ramification theory.

This project is maintained on GitHub at

https://github.com/AlohomoraPZX/Commutative-Algebra

under the MIT License.

Contents

Chapter 0

Rudiments

In this section, we briefly recall some basic concepts in abstract algebra and homological algebra (especially when things happen in R-Mod category).

0.1 Homological Algebra

0.1.1 Projective and Injective Objects

Recall that in homological algebra we already knew that functor $\operatorname{Hom}(M,-):\mathscr{A}\to\mathsf{Ab}$ is left exact for any $M\in\operatorname{Ob}(\mathscr{A})$, since $\operatorname{Hom}(M,-)$ preserves limits. A natural question is whether it is actually an exact functor or not. The following example shows that the functor can fail to be right exact.

Example 0.1.1. *Consider the following exact sequence:*

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

Let $M=\mathbb{Z}/2\mathbb{Z}$, the following sequence

$$\begin{tikzcd} \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}) \arrow[r, "\times 2"] & \operatorname{Hom}(\mathbb{Z}/2\mathbb{Z},\mathbb{Z}) \arrow[r, "\operatorname{mod} 2"] & \operatorname{End}(\mathbb{Z}/2\mathbb{Z}) \arrow[r] & 0 \end{tikzcd}$$

cannot be exact at all. Indeed, $\mathbb{Z}/2\mathbb{Z}$ is a torison module, but $\mathbb{Z}$ is torison-free, hence $\operatorname{Hom}(\mathbb{Z}/2\mathbb{Z},\mathbb{Z})$ could only be $\{0\}$. But $|\operatorname{End}(\mathbb{Z}/2\mathbb{Z})|$ has 2 elements, which is a contradiction.

So natually, it comes to us that when does $\operatorname{Hom}(M,-)$ be exact? The question leads to the definition of projective and injective objects.

Definition 0.1.1. *Let $\mathscr{A}$ be an abelian category, an object $M\in\operatorname{Ob}(\mathscr{A})$ is called **projective** (resp. **injective**), if $\operatorname{Hom}(M,-)$ (resp. $\operatorname{Hom}(-,M)$) is exact.*

The name actually comes from the following properties:

Proposition 0.1.1. *An object $M \in \mathrm{Ob}(\mathscr{A})$ is projective if and only if for any epimorphism $f : X \to Y$ and morphism $g : M \to Y$, there exists some $\varphi : M \to X$ such that the diagram*

$$\begin{tikzcd}
 & M \arrow[dl, "\varphi"'] \arrow[d, "g"] & \\
X \arrow[r, "f"] & Y \arrow[r] & 0
\end{tikzcd}$$

commutes.

Remark 0.1.1. *This property is often referred to as* ***the lifting property*** *of projective objects. Notice that the uniqueness of φ is not required.*

Proof. ($\Rightarrow$) $\mathrm{Hom}(M, -)$ preserves epimorphisms since it is right exact and preserves cokernels, hence we obtain

$$\begin{tikzcd}
\mathrm{Hom}(M, X) \arrow[r, "f_*"] & \mathrm{Hom}(M, Y) \arrow[r] & 0
\end{tikzcd}$$

Since $\mathrm{Hom}(M, X)$ and $\mathrm{Hom}(M, Y)$ are abelian groups, hence f_* is surjective. Therefore, for every $g \in \mathrm{Hom}(M, Y)$, there exists some $\varphi \in \mathrm{Hom}(M, X)$ such that $f \circ \varphi = f_*(\varphi) = g$, which shows the commutativity of the diagram.

($\Leftarrow$) Now suppose we have the sequence

$$\begin{tikzcd}
X \arrow[r, "f"] & Y \arrow[r, "g"] & Z \arrow[r] & 0
\end{tikzcd}$$

exact, it suffices to show the $\mathrm{Hom}(M, -)$ one is also exact.

The surjectiveness of g_* is a direct result of the lifting property. As for f_*, since $g_* \circ f_* = (g \circ f)_* = 0$, we obtain $\mathrm{Im}\, f_* \subset \mathrm{Ker}\, g_*$. It suffices to show $\mathrm{Ker}\, g_* \subset \mathrm{Im}\, f_*$. Suppose $\beta \in \mathrm{Hom}(M, Y)$ such that $g \circ \beta = 0$, consider the following diagram:

$$\begin{tikzcd}
 & & & M \arrow[dll, red, "\alpha"'] \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] \arrow[ddl, red, "\delta"] & & \\
 & X \arrow[r, "f"] \arrow[dl, two heads, "\pi"'] \arrow[d, two heads, "p"'] \arrow[dr, red, "\eta"] & Y \arrow[rr, "g"] & & Z \arrow[r] & 0 \\
\mathrm{Coim}\, f \arrow[r, hook, two heads, "\cong"] & \mathrm{Im}\, f \arrow[r, hook, two heads, "\cong"] \arrow[ur, "\kappa"] & \mathrm{Ker}\, g \arrow[u, hook, "\iota"] \arrow[rr, red] & & \color{red}{0} &
\end{tikzcd}$$

By the universal property of kernel, there is a unique $\delta : M \to \mathrm{Ker}\, g$ and $\eta : X \to \mathrm{Ker}\, g$ such that $\beta = \iota \circ \delta$ and $f = \iota \circ \eta$.

We claim that η is surjective. The exactness of the original sequence yields the cannonical morphism $\operatorname{Im} f \to \operatorname{Ker} g$ to be isomorphic, hence

$$f = \iota \circ \eta = \iota \circ (X \twoheadrightarrow \operatorname{Coim} f \xrightarrow{\cong} \operatorname{Ker} g) \Leftrightarrow \eta = (X \twoheadrightarrow \operatorname{Ker} g)$$

by the injectiveness of ι.

Now, the lifting property of M gives an $\alpha \in \operatorname{Hom}(M, X)$ which commutes the red diagram. Since $f \circ \alpha = (\iota \circ \eta) \circ \alpha = \iota \circ \delta = \beta$, we conclude that $\beta = f_*(\alpha) \in \operatorname{Im} f_*$, which in turn shows that $\operatorname{Ker} g_* \subset \operatorname{Im} f_*$ and completes the proof. □

The analogue to the result above is *the extension property* of injective objects, which can be stated as following:

Proposition 0.1.2. *An object $M \in \operatorname{Ob}(\mathscr{A})$ is injective if and only if for any monomorphism $f : X \to Y$ and morphism $g : X \to M$, there exists some $\varphi : Y \to M$ such that the diagram*

$$\begin{tikzcd}
0 \arrow[r] & X \arrow[r, "f"] \arrow[d, "g"] & Y \arrow[dl, "\varphi"] \\
 & M &
\end{tikzcd}$$

commutes. We say g is extended to φ by f.

An interesting fact is that projective and injective objects have close relationship with split exact sequences, hence are close with direct sums.

Proposition 0.1.3. *Suppose $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is an exact sequence in an abelian category $\mathscr{A}$, then the sequence splits if C (resp. A) is projective (resp. injective), hence we obtain $B \cong A \oplus C$.*

Proof. Suppose C be a projective object, then we obtain $\varphi : C \to B$ such that the diagram

$$\begin{tikzcd}
 & C \arrow[dl, "\varphi"'] \arrow[d, equal, "\mathrm{id}"] & \\
B \arrow[r, "g"] & C \arrow[r] & 0
\end{tikzcd}$$

commutes, meaning that $g \circ \varphi = \mathrm{id}_C$, which shows that the sequence splits.

As for the case of injective objects, the proof is a complete analogue. □

Talking about the direct sum, the following proposition shows that the direct summand of project objects is also projective.

Proposition 0.1.4. *Suppose I is an index set, $\{M_i\}_{i\in I}$ is a family of objects in an abelian category $\mathscr{A}$, then $\bigoplus_{i\in I} M_i$ is projective if and only if each M_i is projective.*

Proof. ($\Leftarrow$) Suppose each M_i is projective, we are going to show $N = \bigoplus_{i\in I} M_i$ is also projective. Let $f : X \to Y$ be an epimorphism, $\tilde{g} : \bigoplus_{i\in I} M_i \to Y$, which in fact gives a family of morphisms $g_i : M_i \to Y$ by setting $g_i = \tilde{g} \circ \iota_i$, where $\{\iota_i\}$ are cannonical morphisms. Now consider the diagram:

$$\begin{tikzcd}
& & X \arrow[d, two heads, dashed, "f"] & \\
& & Y \arrow[dd, dashed] & \\
M_i \arrow[uurr, "\varphi_i"] \arrow[urr, dashed, "g_i"] \arrow[r, "\iota_i"] & \bigoplus_{i\in I} M_i \arrow[uur, "\tilde{\varphi}"] \arrow[ur, dashed, "\tilde{g}"] & & M_j \arrow[uul, "\varphi_j"'] \arrow[ul, dashed, "g_j"'] \arrow[ll, "\iota_j"'] \\
& & 0 &
\end{tikzcd}$$

By the liftting property of each M_i, we obtain $\varphi_i : M \to X$ such that $g_i = f \circ \varphi_i$. Now, by the universal property of direct sum, we obtain a $\tilde{\varphi} : \bigoplus_{i\in I} M_i \to X$ such that $\varphi_i = \tilde{\varphi} \circ \iota_i$.

We aim to show the whole diagram commutes, which only requires $\tilde{g} = f \circ \tilde{\varphi}$. In fact, we have $(f \circ \tilde{\varphi}) \circ \iota_i = f \circ \varphi_i = g_i$ for each $i \in I$, thus by the universal property, we have $f \circ \tilde{\varphi} = \tilde{g}$, which completes the proof.

($\Rightarrow$) Now suppose $\bigoplus_{i\in I} M_i$ be projective, $g_i : M_i \to Y$. Our goal is to show the existence of some φ_i such that $g_i = f \circ \varphi_i$. Actually, set $g_j = 0$ for any $j \neq i$, which defines a unique $\tilde{g} : \bigoplus_{i\in I} M_i \to Y$ which commutes the diagram in the bottom surface. By the lifting property, we obtain a $\tilde{\varphi} : \bigoplus_{i\in I} M_i \to X$, which commutes the vertical diagram. Now notice that $f \circ (\tilde{\varphi} \circ \iota_i) = g_i$. We may set $\varphi_i = \tilde{\varphi} \circ \iota_i$, which completes the proof. □

Corollary 0.1.1. *Direct summands of a projective object are always projective.*

Now we state a much more general fact about projective and injective objects.

Proposition 0.1.5. *Let $\mathcal{F} : \mathscr{A} \to \mathscr{B}$ be a functor, where $\mathscr{A}, \mathscr{B}$ are both abelian categories. If $\mathcal{F}$ admits a right adjoint $\mathcal{G} : \mathscr{B} \to \mathscr{A}$ which preserves surjectiveness, then $\mathcal{F}$ preserves projectiveness.*

Proof. Suppose $M \in \mathrm{Ob}(\mathscr{A})$ be projective, we aim to show that $\mathcal{F}(M)$ is also projective. Let $f : X \twoheadrightarrow Y$ be an arbitrary epimorphism, where $X, Y \in \mathrm{Ob}(\mathscr{B})$, the adjunction suggests the diagram

$$\begin{tikzcd}
\mathrm{Hom}_{\mathscr{A}}(M, \mathcal{G}(X)) \arrow[r, "(\mathcal{G}(f))_*"] \arrow[d, hook, two heads, "\eta_X"'] & \mathrm{Hom}_{\mathscr{A}}(M, \mathcal{G}(Y)) \arrow[d, hook, two heads, "\eta_Y"] \\
\mathrm{Hom}_{\mathscr{B}}(\mathcal{F}(M), X) \arrow[r, "f_*"] & \mathrm{Hom}_{\mathscr{B}}(\mathcal{F}(M), Y)
\end{tikzcd}$$

commutes. Suppose $v : \mathcal{F}(M) \to Y$, we obtain a $\eta_Y^{-1} \circ v : M \to \mathcal{G}(Y)$. Since $\mathcal{G}(f)$ is still an epimorphism in $\mathscr{A}$, the liftting property of M gives some $u : M \to \mathcal{G}(X)$ such that the diagram

$$\begin{tikzcd}
 & M \arrow[dl, "u"'] \arrow[d, "\eta_Y^{-1}\circ v"] & \\
\mathcal{G}(X) \arrow[r, "\mathcal{G}(f)"] & \mathcal{G}(Y) \arrow[r] & 0
\end{tikzcd}$$

commutes. Let $\tilde{u} = \eta_X \circ u \in \mathrm{Hom}_{\mathscr{B}}(\mathcal{F}(M), X)$, the adjuction suggests

$$f_*(\tilde{u}) = f \circ \eta_X(u) = \eta_Y(\mathcal{G}(f) \circ u) = \eta_Y(\eta_Y^{-1} \circ v) = v,$$

which means that the following diagram

$$\begin{tikzcd}
 & \mathcal{F}(M) \arrow[dl, "\eta_X(u)"'] \arrow[d, "v"] & \\
X \arrow[r, "f"] & Y \arrow[r] & 0
\end{tikzcd}$$

commutes, which completes the proof. □

Remark 0.1.2. *Now let me simply explain how this derives the result that direct sum of projective objects is still projective. Consider the coproduct functor* $\mathcal{F} = \bigoplus_{i\in I}(-) : \mathscr{A}^I \to \mathscr{A}$ *defined by* $(M_i)_{i\in I} \mapsto \bigoplus_{i\in I} M_i$*, and the diagonal functor* $\Delta : \mathscr{A} \to \mathscr{A}^I$ *defined by* $M \mapsto (M)_{i\in I}$*. We aim to show that* Δ *is the right adjoint of* $\mathcal{F}$*.*

In fact, suppose $\mathscr{I} \in \mathscr{A}^I$*, the universal property of direct sum suggests that for each* $A \in \mathrm{Ob}(\mathscr{A})$*, we have*

$$\begin{aligned}
\mathrm{Hom}_{\mathscr{A}}(A, \mathcal{F}(\mathscr{I})) = \mathrm{Hom}_{\mathscr{A}}\left(A, \bigoplus_{i\in I} M_i\right) &\cong \bigoplus_{i\in I} \mathrm{Hom}_{\mathscr{A}}(A, M_i) \\
&\cong \mathrm{Hom}_{\mathscr{A}^I}(\Delta(A), \mathscr{I}),
\end{aligned}$$

which suggests adjunction. Now, Δ *preserves surjectiveness since epimorphisms in* $\mathscr{A}^I$ *are defined componentwise, which completes the proof.*

Now let's turn to some more specific category. Suppose R be a commutative ring, and $\mathscr{A} = R\text{-}\mathsf{Mod}$. We will see that projective modules are exactly the direct summands of free modules.

Proposition 0.1.6. *Let M be an R-module. Then M is projective if and only if there exists some free R-module N such that $N \cong M \oplus M'$.*

Proof. ($\Leftarrow$) Immediately from Proposition 0.1.4.

($\Rightarrow$) Take $M^I = F(M)$, where F is the free functor. Then we have a cannonical epimorphism $f : M^I \twoheadrightarrow M$. Consider the following exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \operatorname{Ker} f \arrow[r, "\iota"] & M^I \arrow[r, "f"] & M \arrow[r] & 0 \end{tikzcd}$$

Since M is projective, the sequence splits. Hence, we obtain $M^I \cong M \oplus \operatorname{Ker} f$. □

We have seen that submodules of a free module are still free if R is a PID. Hence, projective modules are exactly free modules. However, generally it is not true.

Example 0.1.2. *$\mathbb{Z}/6\mathbb{Z}$-module $\mathbb{Z}/2\mathbb{Z}$ is projective, but not free.*

Proof. By the Chinese Remainder Theorem we obtain $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ as $\mathbb{Z}$-module. Tensor product functor $(-) \otimes_{\mathbb{Z}} \mathbb{Z}/6\mathbb{Z}$ is additive, hence preserves direct sums. We obtain $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/6\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/6\mathbb{Z})$, which shows that $\mathbb{Z}/2\mathbb{Z}$ is projective as $\mathbb{Z}/6\mathbb{Z}$ module.

It is obvious that $\mathbb{Z}/2\mathbb{Z}$ is not free, since $2 \times [1] = 0$. □

Not every submodule of a free module is one of its direct summands, hence, not every submodule of a free module is projective. (But this is true if R is a PID)

Example 0.1.3. *$\mathbb{Z}/2\mathbb{Z}$ is not projective as $\mathbb{Z}/4\mathbb{Z}$-module, but is a submodule of the latter, which is free on itself.*

Proof. Suppose that there is some $\mathbb{Z}/4\mathbb{Z}$-module N such that $N = \mathbb{Z}/2\mathbb{Z} \oplus M$, consider the element $a = \overline{1} + 0$, we have $2a = 2 \times \overline{1} + 0 = 0$, which is a contradiction since it is a torison element. □

Even submodule of a free module may fails to be projective, not to mention the case of submodules of a projective module. So naturally a question arises: when do the submodules of a projective module still be projective? A common case is when R is a Dedekind domain.

Definition 0.1.2. *A ring R is called* ***left semi-hereditary*** *if every finite generated left ideal of R is projective. Moreover, if every left ideal of R is projective, then R is called* ***left hereditary****.*

The most important result of hereditary rings is the following theorem.

Theorem 0.1.1 (Kaplansky)**.** *Let R be a left hereditary ring, $F = \bigoplus_{i\in I} Re_i$ be a free module on R. Then any submodule P of F is isomorphic to a direct sum of left ideals of R, which shows that P is projective.*

Proof. The key is to use the fact that every set can be well-ordered. Now suppose we have a well order on I, let $F_{<\alpha} = \bigoplus_{\beta<\alpha} Re_\beta$, and $F_{\leq\alpha} = \bigoplus_{\beta\leq\alpha} Re_\beta$ for each $\alpha \in I$. Set $P_{<\alpha} = P \cap F_{<\alpha}$ and $P_{\leq\alpha} = P \cap F_{\leq\alpha}$.

We shall define a homomorphism $f_\alpha : P_{\leq\alpha} \to R$ by setting $f\left(\sum_{\beta\in I} r_\beta e_\beta\right) = r_\alpha$. It is trivial to verify that $\ker f_\alpha \cong P_{<\alpha}$, hence we obtain a exact sequence

$$\begin{tikzcd} 0 \arrow[r] & \ker f_\alpha \arrow[r] & P_{\leq\alpha} \arrow[r, "f_\alpha"] & \operatorname{im} f_\alpha \arrow[r] & 0 \end{tikzcd}$$

Since $\operatorname{im} f_\alpha$ is a left ideal of R, hence is projective. We obtain $P_{\leq\alpha} \cong P_{<\alpha} \oplus \operatorname{im} f_\alpha$ since the sequence splits. Let Q_α be the submodule of $P_{\leq\alpha}$ such that $f_\alpha|_{Q_\alpha} : Q_\alpha \to \operatorname{im} f_\alpha$ is an isomorphism.

We claim that $P \cong \bigoplus_{\alpha\in I} Q_\alpha$. Suppose there is some $x \in P$ such that $x \notin \sum_{\alpha\in I} Q_\alpha$. But since $x \in P \subset F$, we have $x = a_{\alpha_1}e_{\alpha_1} + \cdots + a_{\alpha_n}e_{\alpha_n}$, where $a_{\alpha_i} \in R$. Hence, there is a minimal $\beta = \alpha_n \in I$ such that $x \in P_{\leq\beta} = P_{<\beta} \oplus Q_\beta$. Hence, $x = y + z$ for some $y \in P_{<\beta}$ and $z \in Q_\beta$, which shows that $y \notin \sum_{\alpha\in I} Q_\alpha$, a contradiction with the minimality of β. Therefore, $P = \sum_{\alpha\in I} Q_\alpha$.

Now we only to verify that the sum is actually direct sum. Suppose there are some $a_{\alpha_i} \in Q_{\alpha_i}$ such that $a_{\alpha_1} + \cdots + a_{\alpha_n} = 0$. WLOG, assume $\alpha_1 < \cdots < \alpha_n$, we obtain

$$a_{\alpha_n} = -(a_{\alpha_1} + \cdots + a_{\alpha_{n-1}}) \in Q_{\alpha_n} \cap P_{<\alpha} = 0$$

By induction on n, we obtain $a_{\alpha_i} = 0$ for every $1 \leq i \leq n$, which completes the proof. □

For more specific properties of hereditary ring, see [**ringel_ext2_online**].

Corollary 0.1.2. *Let R be a left hereditary ring, P be a left R-module. Then P is projective if and only if P is a submodule of some free module.*

Corollary 0.1.3. *Let R be a ring, then TFAE:*

1. *R is left hereditary;*

2. *Any submodule of a free R-module is projective;*

3. *Any submodule of a projective R-module is projective.*

Proof. (1)⇒ (2), (2)⇒(3) are trivial. Assume (3), since R is free over itself, hence every submodule (i.e. left ideals) of R is projective. In other words, R is left hereditary. □

Definition 0.1.3. *A domain R is called a **Dedekind domain** if it is hereditary.*

So by the proposition, we know that a Dedekind domain R is a domain over which submodules of a projective module are still projective.

Remark 0.1.3. *You may hear that a Dedekind domain is a integral-closed Noetherian domain with Krull dimension* 1*. We will prove the equivalence of those two definitions later.*

0.1.2 Flat Modules

We have already seen in homological algebra that $- \otimes_R M \dashv \mathrm{Hom}(M, -)$ by the natural isomorphism

$$\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A \otimes_R M, B) \cong \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(A, \mathrm{Hom}(M, B))$$

given by the universal property of tensor products, that is: every bilinear transformation $\tau : A \times M \to B$ factors through $A \otimes_R M$. Hence, the tensor product functor is right exact. Similarly, we want to find out when would it be exact. Generally, it is not true.

Example 0.1.4. *Consider $f : \mathbb{Z} \to \mathbb{Z}$ defined by $x \mapsto 2x$, we have the sequence*

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, "f"] & \mathbb{Z} \arrow[r, "\pi"] & \mathbb{Z}/2\mathbb{Z} \arrow[r] & 0 \end{tikzcd}$$

exact. Now we tensor the sequence with $\mathbb{Z}/4\mathbb{Z}$, which cannot be exact since $f \otimes_{\mathbb{Z}} \mathbb{Z}/4\mathbb{Z} : x + 4\mathbb{Z} \mapsto 2x + 4\mathbb{Z}$ is no longer injective.

Definition 0.1.4. *Let R be a ring. An R-module M is called **flat** if functor $(-) \otimes_R M$ is exact.*

0.1.3 Derived Functors

0.2 Ring Theory

0.2.1 Radical of Ideals

Definition 0.2.1. *Let R be a commutative ring,and I an ideal of R.The* ***radical*** *of I,denoted $\sqrt{I}$,is defined as*

$$\sqrt{I} = \{r \in R \mid \exists n \in \mathbb{N} \ s.t. \ r^n \in I\}.$$

If $\sqrt{I} = I$,we say I is a ***radical ideal****. the* ***nilradical*** *of R is $\mathfrak{N} = \sqrt{(0)}$.*

Proposition 0.2.1 (Basic properties of radicals)**.** *Let I,J be ideals in a commutative ring R.Then:*

$$1.I \subseteq \sqrt{I}.$$

$$2.\sqrt{\sqrt{I}} = \sqrt{I}$$

$$3.\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

$$4.\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$$

$$5.\textit{If I is prime,then}\sqrt{I} = I$$

Proof. (1),(2)and(5) are trivial.For (3),$IJ \subseteq I \cap J \subseteq I, J \Longrightarrow \sqrt{IJ} \subseteq \sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.Conversely,if $x \in \sqrt{I} \cap \sqrt{J}$,then $\exists m, n$ such that $x^m \in I$ and $x^n \in J \Longrightarrow x^{m+n} \in IJ \Longrightarrow x \in \sqrt{IJ}$.For (4),$I + J \subseteq \sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$. □

The radical of an ideal palys a crucial role in algebraic geometry by Hilbert's Nullstellensatz.From a homological perspective,the quotient rings R/I and R/$\sqrt{I}$ are closely related.

Proposition 0.2.2. *There exists a surjective homomorphism:*

$$\pi : R/I \longrightarrow R/\sqrt{I}$$

$$r + I \longmapsto r + \sqrt{I}$$

Proof.
1.Well-definedness
Suppose $r_1 + I = r_2 + I$.Then $r_1 - r_2 \in I \subseteq \sqrt{I}$.

2.Ring homomorphism
For any $r_1, r_2 \in R$:

$$\pi((r_1{+}I){+}(r_2{+}I)) = \pi((r_1{+}r_2){+}I) = (r_1{+}r_2){+}\sqrt{I} = (r_1{+}\sqrt{I}){+}(r_2{+}\sqrt{I}) = \pi(r_1{+}I){+}\pi(r_2{+}I)$$

. Similarly for multiplicartion:

$$\pi((r_1{+}I)(r_2{+}I)) = \pi(r_1r_2{+}I) = r_1r_2{+}\sqrt{I} = (r_1{+}\sqrt{I})(r_2{+}\sqrt{I}) = \pi(r_1{+}I)\pi(r_2{+}I)$$

. 3.Surjectivity
For any $r + \sqrt{I} \in R/\sqrt{I}$,select $r + I \in R/I$.Then $\pi(r + I = r + \sqrt{I})$.So π is surjective. □

Moreover:

Corollary 0.2.1. *There exists an ring isomorphism:*

$$(R/I)/(\sqrt{I}/I) \cong R/\sqrt{I}$$

.

Proof.

$$\ker\pi = \{r + I \in R/I \mid \pi(r + I) = 0 + \sqrt{I}\} = \{r + I \mid r \in \sqrt{I}\} = \sqrt{I}/I$$

. By the First isomorphism Theorem for rings:

$$(R/I)/(\ker\pi) \cong \operatorname{Im}\pi$$

. Since π is surjective,Thus:

$$(R/I)/(\sqrt{I}/I) \cong r/\sqrt{I}$$

. □

Proposition 0.2.3. *Let R be a Noetherian ring, I an ideal. Then $\sqrt{I}$ is the intersection of all prime ideals containing I. In particular, the nilradical $\mathfrak{N}$ is the intersection of all prime ideals of R.*

Proof. Let $J = \bigcap_{\mathfrak{p}\supseteq I}\mathfrak{p}$.Clearly $\sqrt{I} \subseteq J$.For the reverse inclusion,suppose $x \notin \sqrt{I}$.Then the set $S = \{1, x, x^2, \cdots\}$ is disjoint from I. By Zorn's lemma,there exists an ideal $\mathfrak{p}$ maximal with respect to $I \subseteq \mathfrak{p}$ and $\mathfrak{p} \cap S = \varnothing$.Such $\mathfrak{p}$ is prime,so $x \notin J$. □

This intersection property is fundamental in the transition between algebra and geometry. It also leads to a homological observation:

Definition 0.2.2. *Let R be a commutative ring, and M an R-module. A prime ideal $\mathfrak{p}$ of R is called an* ***associated prime ideal*** *of M if there exists an element $x \in M$ such that $\mathfrak{p} = \mathrm{Ann}_R(x) = \{r \in R \mid rx = 0\}$. The set of associated prime ideals of M is denoted by $\mathrm{Ass}_R(M)$.*

Equivalently, $\mathfrak{p} \in \mathrm{Ass}_R(M) \iff M$ contains a submodule isomorphic to $R/\mathfrak{p}$. This characterization connects associated primes with the injective structure of the module category.

Proposition 0.2.4. *Let R be a Noetherian ring,I an ideal.Then the natural surjection $\pi : R/I \longrightarrow R/\sqrt{I}$induces an isomorphism on associated prime ideals: $\mathrm{Ass}_R(R/I) = \mathrm{Ass}_R(R/\sqrt{I})$. Moreover, for any R-module M, the induced map $\mathrm{Ext}^n_R(R/\sqrt{I}, M) \to \mathrm{Ext}^n_R(R/I, M)$ is injective for all $n \geq 0$.*

Proof. Consider the short exact sequence induced by the natural projection:

$$0 \longrightarrow \sqrt{I}/I \longrightarrow R/I \xrightarrow{\pi} R/\sqrt{I} \longrightarrow 0.$$

Note that $\sqrt{I}/I$ is a nilpotent submodule of R/I. Indeed, for any $x \in \sqrt{I}$, there exists $n \geq 1$ such that $x^n \in I$, so $x^n \equiv 0 \pmod{I}$. Hence, the image of x in $\sqrt{I}/I$ is nilpotent.

We prove the equality $\mathrm{Ass}_R(R/I) = \mathrm{Ass}_R(R/\sqrt{I})$ in two steps.

1.$\mathrm{Ass}_R(R/I) \subseteq \mathrm{Ass}_R(R/\sqrt{I})$.

Let $\mathfrak{p} \in \mathrm{Ass}_R(R/I)$. Then there exists a nonzero element $\bar{y} \in R/I$ such that $\mathfrak{p} = \mathrm{Ann}_R(\bar{y})$. Consider its image $\pi(\bar{y}) \in R/\sqrt{I}$.

Case 1: If $\pi(\bar{y}) \neq 0$, then we claim $\mathfrak{p} = \mathrm{Ann}_R(\pi(\bar{y}))$. Indeed, for $r \in R$, we have:

$$\begin{aligned} r \in \mathrm{Ann}_R(\pi(\bar{y})) &\iff r\pi(\bar{y}) = 0 \\ &\iff \pi(r\bar{y}) = 0 \\ &\iff r\bar{y} \in \ker(\pi) = \sqrt{I}/I. \end{aligned}$$

But since $\mathfrak{p} = \mathrm{Ann}_R(\bar{y})$, we have $r\bar{y} = 0$ if and only if $r \in \mathfrak{p}$. If $r\bar{y} \in \sqrt{I}/I$ but $r\bar{y} \neq 0$, then $r\bar{y}$ is nilpotent, so there exists $m \geq 1$ such that $(r\bar{y})^m = r^m\bar{y}^m = 0$. Since $\bar{y}^m \neq 0$ (otherwise $\bar{y}$ would be nilpotent, but $\mathfrak{p}$ is prime and contains $\mathrm{Ann}_R(\bar{y})$, so $\bar{y}$ cannot be nilpotent unless $\bar{y} = 0$), we have $r^m \in \mathrm{Ann}_R(\bar{y}^m) \subseteq \mathfrak{p}$

(the last inclusion follows because $\mathfrak{p}$ is a prime ideal containing $\mathrm{Ann}_R(\bar{y}^m)$). Hence $r \in \mathfrak{p}$. This shows $\mathrm{Ann}_R(\pi(\bar{y})) \subseteq \mathfrak{p}$. The reverse inclusion is clear: if $r \in \mathfrak{p}$, then $r\bar{y} = 0$, so $r\pi(\bar{y}) = 0$. Therefore $\mathfrak{p} = \mathrm{Ann}_R(\pi(\bar{y}))$, so $\mathfrak{p} \in \mathrm{Ass}_R(R/\sqrt{I})$.

Case 2: If $\pi(\bar{y}) = 0$, then $\bar{y} \in \sqrt{I}/I$. Since $\bar{y} \neq 0$ and $\sqrt{I}/I$ is nilpotent, there exists a smallest integer $k \geq 2$ such that $\bar{y}^k = 0$ but $\bar{y}^{k-1} \neq 0$. Let $\bar{z} = \bar{y}^{k-1}$. Then:

- $\bar{z} \neq 0$,
- $\mathfrak{p} = \mathrm{Ann}_R(\bar{y}) \subseteq \mathrm{Ann}_R(\bar{z})$,
- $\bar{z}$ is not in $\sqrt{I}/I$ because if it were, then $\bar{z}$ would be nilpotent, so $\bar{z}^m = 0$ for some m, which would imply $\bar{y}^{(k-1)m} = 0$, contradicting the minimality of k.

We show that $\mathrm{Ann}_R(\bar{z}) = \mathfrak{p}$. Let $r \in \mathrm{Ann}_R(\bar{z})$, i.e., $r\bar{z} = 0$. Then $r\bar{y}^{k-1} = 0$, so $r\bar{y} \in \mathrm{Ann}_R(\bar{y}^{k-2})$. Since $\mathfrak{p}$ is a maximal annihilator (by definition of associated primes in a Noetherian ring), we have $r\bar{y} \in \mathfrak{p}$. If $r \notin \mathfrak{p}$, then since $\mathfrak{p}$ is prime, we must have $\bar{y} \in \mathfrak{p}$. But $\mathfrak{p} = \mathrm{Ann}_R(\bar{y})$, so there exists $s \notin \mathfrak{p}$ such that $s\bar{y} = 0$, which contradicts $\bar{y} \in \mathfrak{p}$ (because then $s\bar{y} = 0$ implies $s \in \mathfrak{p}$). Hence $r \in \mathfrak{p}$, so $\mathrm{Ann}_R(\bar{z}) = \mathfrak{p}$.

Now consider $\pi(\bar{z}) \in R/\sqrt{I}$. Since $\bar{z} \notin \sqrt{I}/I$, we have $\pi(\bar{z}) \neq 0$, and by the same argument as in Case 1, $\mathfrak{p} = \mathrm{Ann}_R(\pi(\bar{z}))$. Therefore $\mathfrak{p} \in \mathrm{Ass}_R(R/\sqrt{I})$.//

2. $\mathrm{Ass}_R(R/\sqrt{I}) \subseteq \mathrm{Ass}_R(R/I)$.

Let $\mathfrak{p} \in \mathrm{Ass}_R(R/\sqrt{I})$. Then there exists $\bar{x} \in R/\sqrt{I}$ with $\bar{x} \neq 0$ such that $\mathfrak{p} = \mathrm{Ann}_R(\bar{x})$. Choose a lift $y \in R/I$ such that $\pi(y) = \bar{x}$. Clearly $y \neq 0$ (otherwise $\bar{x} = 0$). We claim $\mathfrak{p} = \mathrm{Ann}_R(y)$.

For any $r \in \mathfrak{p}$, we have $r\bar{x} = 0$, so $\pi(ry) = 0$, hence $ry \in \sqrt{I}/I$. Since $\sqrt{I}/I$ is nilpotent, there exists n such that $(ry)^n = r^n y^n = 0$. But $y^n \neq 0$ (otherwise y would be nilpotent, then $\bar{x} = \pi(y)$ would be nilpotent, but $\mathfrak{p}$ is prime and contains $\mathrm{Ann}_R(\bar{x})$, so $\bar{x}$ cannot be nilpotent unless $\bar{x} = 0$). Thus $r^n \in \mathrm{Ann}_R(y^n) \subseteq \mathfrak{p}$ (again because $\mathfrak{p}$ is prime and contains $\mathrm{Ann}_R(\bar{x})$ which is contained in $\mathrm{Ann}_R(y^n)$), so $r \in \mathfrak{p}$. This shows $\mathrm{Ann}_R(y) \subseteq \mathfrak{p}$.

Conversely, if $r \in \mathrm{Ann}_R(y)$, then $ry = 0$, so $r\bar{x} = 0$, hence $r \in \mathrm{Ann}_R(\bar{x}) = \mathfrak{p}$. Therefore $\mathfrak{p} = \mathrm{Ann}_R(y)$, and so $\mathfrak{p} \in \mathrm{Ass}_R(R/I)$.//

Combining both steps, we conclude $\mathrm{Ass}_R(R/I) = \mathrm{Ass}_R(R/\sqrt{I})$. □

Example 0.2.1. *Consider $R = \mathbb{Z}$ and $I = (12)$. Then $\sqrt{I} = (6)$, since $6^2 = 36 \in I$ and any element whose power is divisible by 12 must be divisible by 6. Note that $\mathbb{Z}/(12)$ and $\mathbb{Z}/(6)$ have different module structures, but their reduced rings* *(modulo nilpotents) are isomorphic. The nilradical of* $\mathbb{Z}/(12)$ *is* $(6)/(12)$*, which is nilpotent of index 2.*

Example 0.2.2. *Let* $R = k[x, y]/(x^2, xy)$ *where* k *is a field. The ideal* $I = (x)$ *satisfies* $I^2 = 0$*, so* $\sqrt{I} = I$*. However,* I *is not prime since* $y \cdot y = y^2 \notin I$ *but* $y \notin I$*. This shows that radical ideals need not be prime.*

0.2.2 Localization

0.2.3 Nakayama's Lemma

Chapter 1

Hilbert's Nullstellensatz

In this chapter, we introduce an important theorem in algebraic geometry: Hilbert's Nullstellensatz.

1.1 Zariski Topology