March 25, 2020

Contents

0.1 Intro To the Course

In this course, all rings are commutative and unital (has multiplicative identity), unless you find it is not commutative.

Definition 0.1.1.

1. Textbook: Intro to Commutative Algebra by AM.
2. Office hours: Tuesday $2 - 3$.
3. See paper.

Chapter 1

Modules

Algebra is the offer made by the devil to the mathematician...All you need to do, is give me your soul: give up geometry

Michael Atiyah

1.1 Intro

Definition 1.1.1. Fix a ring A, an A-module is an abelian group $(M, +)$ eqvipped with a function $\mu : A \times M \to M$ such that, if we write ax for $\mu(a, x)$,

1. $a(x + y) = ax + ay$,
2. $(a + b)x = ax + bx$,
3. $(ab)x = a(bx)$,
4. $1x = x$.

Remark 1.1.2. Axiom 1 says that for each fixed $a \in A$, $\mu(a, x) : M \to M$ is a group homomorphism/endomorphism. In particular, $a0 = 0$ and $a(-x) = -ax$. Thus, we have a function $\alpha : A \to End(M)$ given by $a \mapsto \mu(a, x)$, where $End(M)$ has a ring structure with addition and composition.

Axiom $2, 3, 4$ says α is a ring homomorphism. In particular, we get $(-1)x = -x$. It follows the converse is also true: Given an abelian group M and a ring homomorphism $\alpha : A \to End(M)$, we obtain, canonically, an A-module where $\mu(a, x) := \alpha(a)(x)$.

The point is that the category of A modules is just the category of abelian groups with a ring homomorphism $\alpha : A \to End(M)$. I.e., an A-module is an abelian group with an action of A on it.

Example 1.1.3.

1. If A is a field, then the modules are just A-vector spaces.
2. If $A = \mathbb{Z}$, then from abelian group M there is a unique ring homomorphism $\mathbb{Z} \to End(M)$, given by $nx = \sum_{i=1}^{n} x$ for all $n \geq 0$. Viz, $\mathbb{Z}$-modules are just abelian groups with no additional structure.
3. Suppose $A = k[X]$, the polynomials over a field k. Given any k-vector space V and a linear map $T : V \to V$, we get a $k[X]$-module structure on V by

$$p(X)v := p(T)(v)$$

   Exercise: The converse is also true: every $k[X]$-module arises this way.
4. Let A be any ring, every ideal $I \leq A$ is an A-module, by $\mu(a, x) = ax$.
5. Let A be a ring, then A^n is an A-module with component-wise addition and multiplication is defined as $a \cdot (a_1, ..., a_n) = (aa_1, ..., aa_n)$.

Definition 1.1.4. If M, N are A-modules ,then an A-module homomorphism (or A-linear map) $f : M \to N$ is a group homomorphism such that $f(ax) = af(x)$. Via, f is a group homomorphism pervers the action of the ring A.

Example 1.1.5. When $A = \mathbb{Z}$, an $\mathbb{Z}$-linear map is just a group homomorphism.

Example 1.1.6. Note $Hom_A(M, N)$ is an A-module where $(f+g)(x) = f(x)+g(x)$ and $(af)(x) = af(x)$.

Definition 1.1.7. An A-linear map is an ***isomorphism*** if it is bijective. We say M is ***isomorphic*** to N if there exists an isomorphism between N and M and write $N \cong M$.

Example 1.1.8. We have $Hom_A(A, M) \cong M$ via $f \mapsto f(1)$.

Definition 1.1.9. Let M be an A-module, an ***A-submodule*** of M is a subgroup $N \leq M$ such that $rn \in N$ for all $r \in R$ and $n \in N$.

Example 1.1.10.

1. Let $A = \mathbb{Z}$, then submodules are subgroups.
2. Let $A = k$ a field, then submodules are subspaces.
3. Let $A = k[X]$ be the polynomial field, then submodules are T-invariant subspaces.
4. Let A be any ring and $M \subseteq A$ be an ideal. Then submodules are ideals of A containing M.

Definition 1.1.11. If $N \leq M$ is an A-submodule, then the ***quotient module*** M/N is the group M/N with the action $r(m + N) \mapsto rm + N$. We need to check this action is well-defined.

Theorem 1.1.12 (Correspondence Theorem)**.** *Let N be a submodule of an A-module M. Let $\pi : M \to M/N$ be the quotient map $x \mapsto x + N$. Then π induces a containment preserving bijection between the submodules of M that contains N and the submodules of M/N via the mapping $M' \mapsto M'/N$.*

Proof. Exercise: take the Correspondence Theorem for groups and restrict to submodules. ♡

Remark 1.1.13. Let $f : M \to N$ be A-linear map, then $Ker(f)$ and $Im(f)$ are submodules.

Theorem 1.1.14 (Universal Property of Quotients)**.** *Suppose $f : M \to N$ and $g : M \to L$ are A-linear. Consider the following diagram:*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[dr, "q"'] & N \arrow[d, dashed, "h"] \\ & L \end{tikzcd}$$

There exists a homomorphism $h : B \to C$ such that $q = h \circ f$ iff $Ker(f) \subseteq Ker(q)$

Proof. Exercise. ♡

Remark 1.1.15. Note $Im(\phi) = Im(f)$ as π is surjective and $Ker(\phi) = Ker(f)/M'$. In particular, apply the universal property to $M' = Ker(f)$ yields the first isomorphism theorem.

Theorem 1.1.16. *If $f : M \to N$ is A-linear, then $M/Ker(f) \cong Im(f)$.*

Definition 1.1.17. Let M_1, M_2 be submodules of an A-module, then $M_1 + M_2 := \{x_1 + x_2 : x_i \in M_i\}$ is an A-submodule of M.

Remark 1.1.18. $M_1 + M_2$ is the smallest submodule of M that containing M_1, M_2.

We also note $M_1 \cap M_2$ is an A-submodule and it is the largest submodule of M contained in both M_1 and M_2.

Definition 1.1.19. Given a sequence $\{M_i : i \in I\}$ of submodules of M, we can take the sum

$$\sum_{i \in I} M_i = \{\sum_{i \in I} a_i : a_i \in M_i, \text{and all but finite many are } 0\}$$

Remark 1.1.20. The sum is the smallest submodule that contains each M_i.

1.2 Intro II

Definition 1.2.1. Let M be an A-module and $\Lambda \subseteq M$. The ***submodule generated by*** Λ is

$$\langle \Lambda \rangle = \{\sum_{i=1}^{n} a_i \lambda_i : n \geq 0, a_1, ..., a_n \in A, \lambda_1, ..., \lambda_n \in \Lambda\}$$

Remark 1.2.2. This is a submodule and it is the smallest submodule that contains Λ.

Definition 1.2.3. We say M is ***generated by*** Λ if $\langle \lambda \rangle = M$. In addition, we say M is ***finitely generated*** (f.g.) if $M = \langle \Lambda \rangle$ where $|\Lambda| < \infty$, i.e. it is finite.

Proposition 1.2.4. *M be finitely generated if and only if $M \cong A^n/N$ for some $n \geq 0$ and $N \leq A^n$ a submodule.*

Proof. Suppose $N \cong A^n/N$. Note that being finitely generated is preserved under automorphism.

Note A^n is generated by $\Lambda := \{(1, ..., 0), ..., (0, ..., 1)\}$. Also, note if Λ generates M and $N \leq M$, then $\Lambda + N := \{\lambda + N : \lambda \in \Lambda\}$ generates M/N.

Thus, A^n/N is indeed finitely generated.

Conversely, say $M = \langle \Lambda \rangle$ with $\Lambda = \{v_1, ..., v_n\}$. Consider the mapping $\phi : A^n \to M$ given by

$$\phi(a_1, ..., a_n) = a_1\lambda_1 + ... + a_n\lambda_n$$

One should check that ϕ is an A-linear map of modules. Then, since $M = \langle \Lambda \rangle$, we have ϕ is surjective and so $A^k/Ker(\phi) \cong Im(\phi) = M$ as desired. ♡

Proposition 1.2.5 (Cayley-Hamilton for module)**.** *Let M be finitely generated A-module. Let $\phi : M \to M$ be A-linear, then there exists $n > 0$, $a_0, ..., a_{n-1} \in A$ such that*

$$\phi^n + a_{n-1}\phi^{n-1} + ... + a_1\phi + a_0 = 0$$

in the ring $End_A(M) := Hom_A(M, M)$.

Proof. Fix generators $x_1, ..., x_n \in M$ for M. Then $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$ for some $a_{ij} \in A$. Thus,

$$(a_{ij}) \in Mat_n(A) =: R$$

is the analogy of the matrix of a linear operator with a basis, where $Mat_n(R)$ is n by n matrices with coefficients in R.

Consider

$$P := \begin{bmatrix} a_{11} - \phi & a_{12} & ... & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & ... & a_{nn} - \phi \end{bmatrix} \in Mat_n(End_A(M))$$

where a_{ij} is viewed as an endomorphism by scalar multiplication.

Now, note $Mat_n(End_A(M))$ acts naturally on M^n via the matrix multiplication

$$\begin{bmatrix} f_{11} & ... & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n1} & ... & f_{nn} \end{bmatrix} \cdot \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} \sum_{i=1}^n f_{1i}(y_i) \\ \vdots \\ \sum_{i=1}^n f_{ni}(y_i) \end{bmatrix}$$

Thus, the ith entry of $P \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ is

$$\sum_{\substack{i=1 \\ i \neq j}}^{n} a_{ij}x_i + (a_{ii} - \phi)(x_i) = \sum_{j=1}^{n} a_{ij}x_j - \phi(x_i) = 0$$

Thus $P \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0$.

Then, let $\tilde{P} \in Mat_n(End_A(M))$ be the classical adjoint of P, i.e. $\tilde{P}_{ij}$ is the (j,i)-cofactor of P. Then, we have a fact that $\tilde{P} \cdot P = diag(det(P), ..., det(P))$, where $det(P) \in End_A(M)$.

Thus, we must have

$$(\tilde{P}) \left(P \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \right) = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} = (\tilde{P}P) \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

Thus, we have

$$\begin{bmatrix} det(P) & ... & 0 \\ \vdots & \ddots & \vdots \\ 0 & ... & det(P) \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

and therefore, $det(P)(x_i) = 0$ for $i = 1, ..., n$ and so one should check if an A-linear map vanishes on the generators then it vanishes on the whole module. Therefore, $det(P)$ vanishes all elements of M, i.e. $det(P) = 0$ where $det(P)$ is a polynomial in ϕ with leading coefficient to be ± 1. Thus the proof follows. ♡

Remark 1.2.6. Actually, we learn a lot more from this proof about coefficients $a_0, ..., a_{n-1}$.

Proposition 1.2.7. *Let M be f.g. A module, $I \leq A$ be an ideal. Let $\phi : M \to M$ be A-linear such that $\phi(M) \subseteq IM := \{\sum_{i=1}^{n} b_i x_i : n \geq 0, b_i \in I, x_i \in M\}$. Then, there are $a_0, ..., a_{n-1} \in I$ such that $\phi^n + a_{n-1}\phi^{n-1} + ... + a_0 = 0$.*

Proof. Same proof as 1.2.5, just observe a_{ij}'s are in I. ♡

Corollary 1.2.7.1 (Nakayama's Lemma)**.** *Suppose M is f.g. A-module, $I \leq A$, and $IM = M$. Then there is $a \in A$ such that*

$$a \equiv 1 \pmod I$$

and $aM = 0$.

Proof. Apply 1.2.7 to $\phi = Id$. ♡

1.3 Exact Sequences

Definition 1.3.1. A sequence of R modules and R homomorphisms

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

is said to be ***exact at*** M_i if $Im(f_i) = Ker(f_{i+1})$. The sequence is exact if it is exact at each M_i.

Definition 1.3.2. A ***short exact sequence*** is a sequence of the form

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

Proposition 1.3.3.

1. *$0 \to M' \xrightarrow{f} M$ is exact if and only if f is injective*
2. *$M \xrightarrow{g} M' \to 0$ is exact if and only if g is surjective*
3. *$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ is exact if and only if f is injective, g is surjective, and g induces an isomorphism between $Coker(f) = M/f(M')$ and M''. In particular, the isomorphism is $m'' \mapsto g(m) + Im(f)$.*
   Equivalently, we say that M is an extension of M'' by M'.

Proof. Trivial. ♡

Example 1.3.4. Consider

$$0 \longrightarrow M \xrightarrow{i} M \oplus N \xrightarrow{\pi} N \longrightarrow 0$$

where $i(m) = (m, 0)$ is inclusion and $\pi(m, n) = n$ is exclusion. This is exact.

Consider

$$0 \longrightarrow \mathbb{Z} \xrightarrow{4} \mathbb{Z} \xrightarrow{q} \mathbb{Z}/4\mathbb{Z} \longrightarrow 0$$

where $4(n) = 4n$ and $q(n) = n + 4\mathbb{Z}$. This is also exact.

Definition 1.3.5. A short exact sequence

$$0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$$

is ***split*** iff there is an isomorphic $\alpha : M_2 \to M_1 \oplus M_3$ such that

$$\begin{tikzcd}
 & & M_1 \oplus M_3 \arrow[dr, "\pi"] & & \\
0 \arrow[r] & M_1 \arrow[ur, "i"] \arrow[dr, "f"'] & & M_3 \arrow[r] & 0 \\
 & & M_2 \arrow[uu, "\alpha"] \arrow[ur, "g"'] & &
\end{tikzcd}$$

commutes.

Theorem 1.3.6. *The following are equivalent:*

1. $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ *is split and short exact,*
2. f *has a left inverse: there exists* $f' : M_2 \to M_1$ *such that* $f' \circ f = Id$,
3. g *has a right inverse: there exists* $g' \in M_3 \to M_2$ *such that* $g \circ g' = Id$.

Proof. $(1) \Rightarrow (2), (3)$ is clear: let f' be projection onto the first factor (M_1) and g' be the inclusion into second factor (M_2).

$(2) \Rightarrow (1)$: Define $\alpha : M_2 \to M_1 \oplus M_3$ by $\alpha(m_2) = (f'(m_2), g(m_2))$. It clearly suffices to show that α is an isomorphism.

Say $\alpha(m_2) = 0$, then $f'(m_2) = 0$ and $g(m_2) = 0$, hence $m_2 = f(m_1)$ by $g(m_2) = 0$ for some $m_1 \in M$. Thus $0 = m_1$ and so $m_2 = f(m_1) = 0$. This shows injective.

Let $(m_1, m_3) \in M_1 \oplus M_3$. Choose $m \in M_2$ such that $g(m) = m_3$, let $m_2 = f(m_1 - f'(m)) + m$. Then

$$\begin{aligned} \alpha(m_2) &= (f'(f(m_1 - f'(m)) + m), g(f(m_1 - f'(m)) + m)) \\ &= (m_1 - f'(m) + f'(m), g(m)) \\ &= (m_1, m_3) \end{aligned}$$

$(3) \Rightarrow (1)$: Assume g' is the right inverse. Define $\alpha : M_1 \oplus M_3 \to M_2$ by $\alpha(m_1, m_3) = f(m_1) + g'(m_3)$.

To see injectivity, let $(m_1, m_3) \in Ker(\alpha)$, then

$$g(f(m_1) + g'(m_3)) = g(0) = 0 \Rightarrow 0 + gg'(m_3) = 0 \Rightarrow m_3 = 0$$

Thus $f(m_1) = 0$ as $g'(m_3) = g'(0) = 0$, and by injectivity of f, we must have $m_1 = 0$. Therefore $(m_1, m_3) = (0, 0)$ and hence α is injective.

Next we show surjectivity. Say $m_2 \in M_2$, let $m_3 = g(m_2)$. Define $m = m_2 - g'(g(m_2))$, we have $g(m) = g(m_2) - g(m_2) = 0$, so $m \in Ker(g) = Im(f)$, i.e. there exists m_1 such that $f(m_1) = m =$. Viz, $m_2 = f(m_1) + g'(m_3) = \alpha(m_1, m_2)$ and so α is indeed surjective. ♡

Example 1.3.7. By Theorem 1.3.6, we have

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\ 4\ } \mathbb{Z} \xrightarrow{\ q\ } \mathbb{Z}/4\mathbb{Z} \longrightarrow 0$$

does not split.

Remark 1.3.8. If A is a field, then every short exact sequence of finitely generated A-modules splits. Indeed, if A is a field, then this is linear algebra, and so we must have

$$0 \longrightarrow A^n \longrightarrow A^{m+n} \longrightarrow A^m \longrightarrow 0$$

where A^{m+n} is exactly $A^n \oplus A^m$.

Definition 1.3.9. Let A be a ring and M, M', N, N' be R modules. Then, let $u \in Hom_A(M, M'), v \in Hom_A(N, N')$, we obtain two induced (module) homomorphisms

$$u^* : Hom(M, N) \to Hom(M', N), \quad \text{with } \overline{u}(f) = f \circ u$$

$$v_* : Hom(M, N) \to Hom(M, N'), \quad \text{with } \overline{v}(f) = v \circ f$$

Definition 1.3.10. $Hom(-, N)$ is ***contravariant*** (as it reverse arrows).

$Hom(N, -)$ is ***covariant*** (if it is not contravariant).

Theorem 1.3.11. *$Hom(M, -)$ is left exact and $Hom(-, N)$ is right exact. That is,*

1. $0 \to N_1 \xrightarrow{f} N_2 \xrightarrow{g} N_3$ *is exact iff for all A modules M, the following sequence is exact*
$$0 \to Hom(M, N_1) \xrightarrow{f_*} Hom(M, N_2) \xrightarrow{g_*} Hom(M, N_3)$$
2. *Similarly,* $0 \to M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3$ *is exact iff for all A-module N, the following sequence is exact*
$$0 \to Hom(M_3, N) \xrightarrow{g^*} Hom(M_2, N) \xrightarrow{f^*} Hom(M_1, N)$$

Proof. (1): Exactness at $Hom(M, N_1)$: this is just the injectivity of f_*. In particular,

$$f_*(\alpha) = 0 \Leftrightarrow \forall m, (f \circ \alpha)(m) = 0 \Leftrightarrow \forall m, f(\alpha(m)) = 0 \Leftrightarrow \alpha = 0$$

Exactness at $Hom(M, N_2)$: We need to show $Im(f_*) = Ker(g_*)$. If $\alpha_2 \in Im(f_*)$, then $\alpha_2 = f \circ \alpha_1$ for some α_1. Then $g \circ \alpha = g \circ f \circ \alpha_1 = 0$. Next, if $\alpha_2 \in Ker(g_*)$, then $g_*(\alpha_2) = 0$, so $g \circ \alpha_2 = 0$, so $Im(\alpha_2) \subseteq Ker(g) = Im(F)$ and so $\alpha_2 = f_*(F^{-1} \circ \alpha_2)$ where $F : N_1 \to Im(f)$ is the restriction of f by codomain. The proof follows.

Next we show (2).

We first show g^* is injective. Say $g^*(\alpha_3) = 0$, then $\alpha_3 \circ g = 0$ so $Im(g) \subseteq Ker(\alpha_3)$. But g is surjective, so $M_3 \subseteq Ker(\alpha_3)$, i.e. $\alpha_3 = 0$.

To show exactness at $Hom(M_2, N)$, we need to show $Im(g^*) = Ker(f^*)$. Let $\alpha_2 \in Im(g^*)$, then $\alpha_2 = g^*(\alpha_3) = \alpha_3 \circ g$ so $f^*(\alpha_2) = \alpha_2 \circ f = \alpha_3 \circ g \circ f = 0$ by exactness of the original sequence. Thus $Im(g^*) \subseteq Ker(f)$.

Next, let $\alpha_2 \in Ker(f^*)$, then $\alpha_2 \circ f = 0$. So $Im(f) \subseteq Ker(\alpha_2)$ and hence $Ker(g) \subseteq Ker(\alpha_2)$. In particular, observe the diagram

$$\begin{tikzcd} M_2 \arrow[r, "g"] \arrow[dr, "\alpha_2"'] & M_3 \arrow[d, dashed, "\alpha_3"] \\ & N \end{tikzcd}$$

We want to find $\alpha_3 : M_3 \to N$ such that $\alpha_2 = \alpha_3 \circ g$. However, by universal property of quotient, we are done. ♡

1.4 Operations On Modules

Definition 1.4.1. Let M, N be two R modules, then $M \otimes_A N$, the tensor products of M and N, is an A-module (that follows the same construction as the tensor product of vector spaces).

Remark 1.4.2. We give a explicit construction of $M \otimes_A N$. Consider B be the free A-module on $M \times N$, i.e. it is the module generated by all elements of $M \times N$. Let $R \leq B$ be the A-submodule generated by elements of the following forms:

$$(m_1 + m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1 + n_2) - (m, n_1) - (m, n_2)$$

$$(am, n) - a(m, n)$$

$$(m, an) - a(m, n)$$

for all $a \in A, m, m_1, m_2 \in M, n, n_1, n_2 \in N$. Then we define $M \otimes_A N := B/R$ be the quotient module.

Example 1.4.3.

1. We have $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z} = \{\sum_{i=1}^{k} a_i \otimes b_i : a_i, b_i \in \mathbb{Z}, i \in \mathbb{Z}_{\geq 1}\}$. In particular, $\sum a_i \otimes b_i = \sum a_i b_i (1 \otimes 1) = (\sum a_i b_i)(1 \otimes 1)$ and this is isomorphic to $\mathbb{Z}$.
2. We have $\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Z}[y] \cong \mathbb{Z}[x, y]$.
3. Consider $(\mathbb{Z}/3\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/5\mathbb{Z})$. Let $\sum a_i \otimes b_i = \sum 3(a_i \otimes 2b_i) = \sum (3a_i \otimes 2b_i) = \sum 0 \otimes 2b_i = 0$.
4. We have $\mathbb{Z}[x] \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}[x]$.

Definition 1.4.4. Suppose $\{M_i\}_{i \in I}$ is a sequence of A-modules where I is an index set. We define the ***direct sum*** to be the A-module $\bigoplus_{i \in I} M_i$ whose elements are I-sequences $(x_i : i \in I)$ where for each $i \in I$ we have $x_i \in M_i$ and there are all but finitely many x_i are zero. When we drop the condition that all but finitely many x_i are zero, we get the ***direct product*** $\prod_{i \in I} M_i$.

In particular, we define $(x_i : i \in I) + (y_i : i \in I) = (x_i + y_i : i \in I)$ and $a(x_i : i \in I) = (ax_i : i \in I)$ to be the operations that makes $\bigoplus_{i \in I} M_i$ an A-module (also makes $\prod_{i \in I} M_i$ an A-module).

Example 1.4.5. When all $M_i = A$, we have $A^I := \bigoplus_{i \in I} A$ is the set of all functions from I to A with finite support. When I is finite, we write $A^n := A^{\{1,\dots,n\}}$.

Definition 1.4.6. An A-module M is ***free*** if it is isomorphic to A^I for some I.

Example 1.4.7. Consider M an A-module, $N_1, N_2 \leq M$ be submodules. Then, consider $N_1 \oplus N_2$ and the A-homomorphism $\phi : N_1 \oplus N_2 \to M$ given by $(n_1, n_2) \mapsto n_1 + n_2$, note this map is canonical. In particular, we note this canonical map is isomorphic if and only if $M = N_1 + N_2$ and $N_1 \cap N_2$ is trivial(try to show this!).

To abuse notations, when $N_1, N_2 \leq M$ such that $N_1 + N_2 = M$ and $N_1 \cap N_2 = \{0\}$, we write $M = N_1 \oplus N_2$, i.e. ϕ as above is an isomorphism.

We should try to show this can be generalized to $\{N_i : i \in I\}$ and $N_i \leq M$.

1.5 Classification of Finitely Generated Modules Over PIDs

Definition 1.5.1. Let M be an A-module and $X \subseteq M$. We say X is A-***linearly independent*** if whenever $x_1, ..., x_n \in X$ are distinct, $a_1, ..., a_n \in A$ such that $\sum_{i=1}^n a_i x_i = 0$, then $\forall 1 \le i \le n, a_i = 0$.

Definition 1.5.2. We say X is a basis of M if X is linearly independent and generates M.

Lemma 1.5.3. *M has a basis if and only if it is free.*

Proof. Suppose M is free, i.e. $\phi : M \to A^I$ is an A-isomorphism. For each $i \in I$, let $e_i \in A^I$ be the function $e_i(j) = \delta_{ij}$. Then, it is not hard to see $\{e_i : i \in I\}$ is a basis for A^I and it is called standard basis. Hence, $X := \{\phi^{-1}(e_i) : i \in I\}$ is a basis for M as we note the pullback of a basis under isomorphism is a basis.

Next, suppose $X \subseteq M$ is a basis for M. Consider A^X and define $\phi : A^X \to M$ by $(a_x : x \in X) \mapsto \sum_{x \in X} a_x \cdot x$. ♡

Definition 1.5.4. Let A be an integral domain, the ***rank*** of an A-module M is the supremum of the size of A-linearly independent subset. This is denoted as $rk(M) = rank(A)$.

Remark 1.5.5. Note if $X \subseteq M$ is A-lienar independent, then $Y \subseteq X$ imply Y is linear independent. Therefore, $rank(M) \le d$ if and only if M has no linear independent subset of size $d + 1$.

Lemma 1.5.6. *Say A is an integral domain, then*

1. *$N \le M$ then $rank(N) \le rank(M)$,*
2. *Let $f : M \to N$ be an A-homomorphism, then $rank(f(M)) \le rank(M)$.*
3. *For all $m \ge 0$, $rank(A^m) = m$.*

Proof. The first one is easy.

(2): Assume $rank(M) < \infty$, suppose $m = rank(M)$, let $y_1, ..., y_{m+1} \in f(M)$ be distinct. Let $x_1, ..., x_{m+1} \in M$ be such that $f(x_i) = y_i$. Since $rank(M) = m$, $\{x_1, ..., x_{m+1}\}$ is linear dependent. Now, suppose $\sum a_i x_i = 0$ with not all a_i's are zero, then $f(\sum a_i x_i) = f(0) = 0 \Rightarrow \sum a_i f(x_i) = \sum a_i y_i = 0$. Therefore, we get $y_1, ..., y_{m+1}$ are not linear independent, i.e. it's rank cannot be $m + 1$ and therefore is at most m. The proof follows.

(3): Let $F = Frac(A)$ be the fraction field. Then A^m is a additive subgroup of F^m, where F^m is a m-dimensional F-vector space. If $x_1, ..., x_{m+1} \in A^m \le F^m$, then there exists $a_1, ..., a_{m+1} \in F$, not all zero and such that $\sum a_i x_i = 0$. Next, clean the denominator, we get $\sum b_i x_i = 0$ where $b_i \in A$ and not all of b_i are zero. Viz, $rank(A^m) \le m$.

On the other hand, $(1,0,...,0),(0,1,...,0),...,(0,...,1) \in A^m$ are A linear independent and so $rank(A^m) \geq m$. ♡

Corollary 1.5.6.1. *Every f.g. A-module has finite rank if A is an integral domain.*

Proof. We see every f.g. module M is isomorphic to A^m/N with $rank(A^m/N) \leq rank(A^m) = m$ and hence finite. ♡

Definition 1.5.7. Let M be an A-module, $x \in M$ is ***torsion*** if there exists $0 \neq a \in A$ such that $ax = 0$.

Definition 1.5.8. A submodule $N \leq M$ is ***torsion*** if every element of N is torsion. A submodule $N \leq M$ is ***torsion free*** if no nonzero element in N is torsion.

Lemma 1.5.9. *Let A be an integral domain,*

1. *M is torsion iff $rank(M) = 0$,*
2. *Free modules are torsion free.*

Proof. (1): We have M is torsion iff $\forall x \in M, \exists a \in A, a \neq 0, ax = 0$ iff $\forall x \in M$, $\{x\}$ is linear dependent iff $rank(M) \leq 1 - 1 = 0$, i.e. $rank(M) = 0$.

(2): Note torsion is preserved by isomorphism, we assume $M = A^I$, let $x \in M$ and $x \neq 0$. Say $x = (a_i : i \in I)$ where $a_i \in A$ are not all zero. Let $0 \neq a \in A$ be arbitrary, then $ax = (aa_i : i \in I)$ and it cannot be zero as A is an integral domain. Thus $ax \neq 0$. ♡

Remark 1.5.10. The first step in the classification is that we want to show, if A is a PID, we want to show, a submodule of a free finite rank A-module is free.

Proposition 1.5.11. *Let A be a PID, let M be free A-module and $N \leq M$ be a submodule. Then, there exists $0 \neq y \in M$, $0 \neq a \in A$ and $K \leq M$ such that*

1. *$M = \langle y \rangle \oplus K$,*
2. *$N = (ay) \oplus (K \cap N)$,*
3. *$\langle a \rangle$ is maximal in $\Sigma := \{\phi(N) : \phi \in Hom_A(M, A)\}$, i.e. $\langle a \rangle \subseteq \phi(N)$ then $\langle a \rangle = \phi(N)$.*

Proof. We will obtain our a first, i.e. we show (3) first.

To get this a, we use Zorn's lemma on $(\Sigma, \subseteq)$. Let $\mathcal{C}$ be a chain in this poset, take the union of all elements in $\mathcal{C}$, say it is I, since A is PID, we have $I = \langle b \rangle$ where $b \in I_j$ for some $j \in I$ and hence $I = I_j$, i.e. $I \in \Sigma$. Thus, by Zorn's lemma, we have Σ has a maximal element, say $\langle a \rangle$.

Next, we let $\theta : M \to A$ be linear such that $\theta(N) = \langle a \rangle$. Let $\gamma \in N$ be such that $\theta(\gamma) = a$.

Claim: For all $\phi \in Hom(M, A)$, we have $a \mid \phi(\gamma)$.

Consider $\langle a, \phi(\gamma)\rangle = \langle d\rangle$ for some $d \in A$, write $d = r_1 a + r_2\phi(\gamma)$ for some $r_1, r_2 \in A$. Let $\psi := r_1\theta + r_2\phi \in Hom(M, A)$. We have $\psi(\gamma) = r_1\theta(\gamma) + r_2\phi(\gamma) = r_1 a + r_2\phi(\gamma) = d$, i.e. $d \in \psi(N)$. Therefore, $\theta(N) = \langle a\rangle \subseteq \langle d\rangle \subseteq \psi(N)$ and so we must have $\theta(N) = \langle a\rangle = \langle d\rangle = \psi(N)$ as $\langle a\rangle$ is maximal. Therefore, we have $\phi(\gamma) \in \langle a\rangle$ and so $a \mid \phi(\gamma)$. This finishes the claim.

End of Claim

Fix a basis X for M. Every element of M is written uniquely as an A-linear combination of elements in X. So each $x \in X$ gives a linear projection $\pi_x : M \to A$ to be $\pi_x(m)$ to be the coefficient of x when you write m as linear combination of the basis X. In particular, we have $\gamma = \sum_{i=1}^{l} c_i x_i = \sum_{i=1}^{l} \pi_{x_i}(\gamma)x_i$.

From above, we recall $\forall \phi \in Hom(M, A)$ we have $a \mid \phi(\gamma)$ and so $a \mid \pi_{x_i}(\gamma)$ for each $1 \leq i \leq l$ and thus $\pi_{x_i}(\gamma) = ab_i$ for some $b_i \in A$. Viz

$$\gamma = ab_1x_1 + ... + ab_lx_l = a(\sum_{i=1}^{l} b_i x_i)$$

Let $y = \sum_{i=1}^{l} b_i x_i$ and we have $y \neq 0$ as $\gamma \neq 0$. We have $\gamma = ay$.

Note we have $\theta(y) = 1$. This is because, $a = \theta(\gamma) = \theta(ay) = a\theta(y)$ and so $\theta(y) = 1$ as $a \neq 0$ and A is an integral domain.

Note we have $M = \langle y\rangle + Ker(\theta)$. Indeed, let $x \in M$, consider $x - \theta(x)y \in M$, and we have

$$\theta(x - \theta(x)y) = \theta(x) - \theta(x)\theta(y) = \theta(x) - \theta(x) = 0$$

Therefore, $x - \theta(x)y \in Ker(\theta)$ and hence $x \in \langle y\rangle + Ker(\theta)$ as desired.

Let $K = Ker(\theta)$.

We claim $\langle y\rangle \cap K = \langle 0\rangle$. Let $x \in \langle x\rangle \cap K$, so $x = by$ for some $b \in A$ and $\theta(x) = 0$. Thus $0 = \theta(x) = \theta(by) = b\theta(y) = b$, i.e. $x = 0y = 0$. This finishes the claim and so $M = \langle y\rangle \oplus K$, which is the first assertion in our proposition.

We claim $N = \langle ay\rangle + (N \cap K)$. Indeed, we have $ay = \gamma \in N$ so $\langle ay\rangle + (N \cap K) \subseteq N$. Now, let $x \in N$, and consider $\theta(x) \in \theta(N) = \langle a\rangle$. Thus, say $\theta(x) = ba$ for some $b \in A$ and observe $x - bay = x - b\gamma \in N$. Then,

$$\theta(x - bay) = \theta(x) - ba\theta(y) = ba - ba = 0$$

where $\theta(x) - ba\theta(y) = ba - ba$ as $\theta(y) = 1$. Hence $x - bay \in Ker(\theta) \cap N = N \cap K$ and so $x \in \langle ay\rangle + N \cap K$. This finishes the claim.

Finally, we claim $\langle ay\rangle \cap (N \cap K) = \langle 0\rangle$. Note $\langle ay\rangle \subseteq \langle y\rangle$, $N \cap K \subseteq K$ and so $\langle ay\rangle \cap (N \cap K) \subseteq \langle y\rangle \cap K = 0$ and hence $N = \langle ay\rangle \oplus (N \cap K)$. This proofs our second assertion. ♡

Proposition 1.5.12. *Let A be a PID, M be free of finite rank k. Let $N \leq M$, then N is free.*

Proof. Note $rank(N) \leq rank(M) < \infty$, so we proceed by induction on $rank(N)$. When $rank(N) = 0$, then N is torsion. However, M is free so it has no non-zero torsion elements, i.e. N must be zero and so it is free.

Now, suppose $rank(N) > 0$, in particular, suppose $N \neq 0$. Apply Proposition 1.5.11, and so there exists $0 \neq y \in M$, $0 \neq a \in A$ and $K \leq M$ so $M = \langle y \rangle \oplus K, N = \langle ay \rangle \oplus N \cap K$.

We claim $rank(N) \geq rank(N \cap K) + 1$.

Let $x_1, ..., x_l \in N \cap K$ be A-linear independent. We will show $\{x_1, ..., x_l, ay\}$ is linear independent. Suppose $\sum_{i=1}^{l} b_i x_i + cay = 0$ where $b_i \in A$ and $c \in A$. Therefore, we have

$$cay = -(\sum_{i=1}^{l} b_i x_i) \in \langle ay \rangle \cap (N \cap K) \Rightarrow cay = 0$$

However, $a \neq 0$, y is not torsion as $y \in M$ and M is torsion free. Hence, $c = 0$ and so we get

$$\sum_{i=1}^{l} b_i x_i = 0 \Rightarrow b_1 = ... = b_l = 0$$

This finishes the claim.

In particular, we get $rank(N \cap K) < rank(N)$ and $N \cap K \leq M$ and so we can apply induction hypothesis. Therefore, $N \cap K \cong A^l$ for some $l \geq 0$.

However, note the map $\phi : A \to \langle ay \rangle$ given by $b \mapsto bay$ is an isomorphism. Indeed, $b \in Ker(\phi)$ then $bay = 0$ where $0 \neq a$ and y is not torsion so $b = 0$.

Hence, we get $N = \langle ay \rangle \oplus (N \cap K)$ and so $N \cong \langle ay \rangle \oplus (N \cap K)$ where the second direct sum is external. Hence $N \cong \langle ay \rangle \oplus (N \cap K) \cong A \oplus A^l \cong A^{l+1}$. The proof follows. ♡

Example 1.5.13. Note if A is not PID, then the above proposition is false. Consider $A = k[x, y]$ where k is a field, then A as A-module is free, but only the principle ideals are free submodules.

Proposition 1.5.14. *Let A be PID, M be free and finite rank. Let N be a submodule. Then there exists a basis $y_1, ..., y_m$ of M and $a_1, ..., a_n \in A$ such that*

1. *$\{a_1 y_1, ..., a_n y_n\}$ is a basis of N for some $n \leq m$,*
2. *$a_1 \mid a_2 \mid a_3 \mid ... \mid a_n$ in A.*

Proof. We use induction on $rank(M)$. If $rank(M) = 0$ then we are done.

Then, assume $rank(M) > 0$, apply Proposition 1.5.11, we have $0 \neq y_1 \in M, 0 \neq a_1 \in A$ and $K \leq M$ such that $M = \langle y_1 \rangle \oplus K$ and $N = \langle a_1 y_1 \rangle \oplus (N \cap K)$ and $\langle a_1 \rangle$ is maximal in $\{\phi(N) : \phi \in Hom(M, A)\}$.

By Proposition 1.5.12, K is free. Hence, as in the proof of 1.5.12, we get $rank(M) \geq rank(K) + 1$ and so $rank(K) < rank(M)$.

Thus, using induction hypothesis, there is $\{y_2, ..., y_m\}$ a basis for K and $a_1 \mid a_3 \mid ... \mid a_n$ for $n \leq m$ such that $\{a_2 y_2, ..., a_n y_n\}$ is a basis of $N \cap K$.

From $M = \langle y_1 \rangle \oplus K$, we see that $\{y_1, ..., y_m\}$ is a basis of M and $\{a_1 y_1, ..., a_n y_n\}$ is a basis for $N \cap K$, we need to show $a_1 \mid a_2$. Consider $\phi : M \to A$ given by $y_1 \mapsto 1$, $y_2 \mapsto 1$ and $y_i \mapsto 0$ for $i \geq 3$. Note this determines ϕ and $\phi \in Hom(M, A)$ and $\phi(a_1 y_1) = a_1 \phi(y_1) = a_1$ and so $a_1 \in \phi(N) \Rightarrow \langle a_1 \rangle \subseteq \phi(N) \Rightarrow \langle a_1 \rangle = \phi(N)$ and so $\phi(a_2 y_2) = a_2 \phi(y_2) = a_2$ and so $a_2 \in \phi(N) = \langle a_1 \rangle$, i.e. $a_1 \mid a_2$. ♡

Theorem 1.5.15 (FTFGMPID, Invariant Factor Form, Existence)**.** *Let A be a PID, M be a finitely generated A-module, then*

$$M \cong A^r \oplus \bigoplus_{i=1}^{m} A/\langle a_i \rangle$$

for some $r \geq 0$, some non-zero, non-units $a_1 \mid a_2 \mid ... \mid a_m$.

Proof. Let $\{x_1, ..., x_n\}$ generates M. Consider $\pi : A^n \to M$ given by $\pi(b_1, ..., b_n) = b_1 x_1 + ... + b_n x_n$ and so $M \cong A^n / Ker(\pi)$. Apply the proposition 1.5.14 above to $Ker(\pi) \leq A^n$ and we get a basis $\{y_1, ..., y_n\}$ of A^n and non-zero $a_1 \mid ... \mid a_m$ where $m \leq n$ such that $Ker(\pi) = \langle a_1 y_1, ..., a_m y_m \rangle$.

Now, consider $f : A^n \to \bigoplus_{i=1}^{m} A/\langle a_i \rangle \oplus A^{n-m}$ given as follows: $x \in A^n$, write $x = \alpha_1 y_1 + ... + \alpha_n y_n$ with $\alpha_i \in A$, then we define

$$f(x) := (\alpha_1 + \langle a_1 \rangle, \alpha_2 + \langle a_2 \rangle, ..., \alpha_m + \langle a_m \rangle, \alpha_{m+1}, ..., \alpha_n)$$

To show f is linear, it suffice to observe that each coordinate function of f is linear.

Also, we note f is surjective as well. Now, we consider the kernel of f. Note

$$Ker(f) = \{x = \alpha_1 y_1 + ... + \alpha_m y_m : \alpha_i \in \langle a_i \rangle\} = \langle a_1 y_1 \rangle + ... + \langle a_m y_m \rangle = Ker(\pi)$$

Hence, we have

$$M \cong A^n / Ker(\pi) \cong A^{n-m} \oplus A/\langle a_1 \rangle \oplus ... \oplus A/\langle a_m \rangle$$

Throw away those a_i's that are units in A then we are done. ♡

Remark 1.5.16.

1. Note each factor on the RHS of FTFGMPID, invariant factor form, is a cyclic A-module, so we split every f.g. module into a direct sum of cyclic modules (note every cyclic A-module is of the form A/I).
2. Each factor of the form A is free and each $A/\langle a_i \rangle$ is torsion. We split M into a free part and a torsion part.

Definition 1.5.17. We define $Tor(M) = \{x \in M : \exists 0 \neq a \in A, ax = 0\}$. This is a submodule.

Proposition 1.5.18. *Let A be a PID, M be f.g. A-module, then*

1. *In FTFGMPID, $Tor(M) = A/\langle a_1 \rangle \oplus ... \oplus A/\langle a_m \rangle$,*
2. *It follows that M is free if and only if M is torsion free.*
3. *If r is as in FTFGMPID, then $rank(M) = r$.*

Proof. (1): If $x := (\alpha_1 + \langle a_1 \rangle, ..., \alpha_m + \langle a_m \rangle) \in A/\langle a_1 \rangle \oplus ... \oplus A/\langle a_m \rangle$.

Then $a_1 a_2 ... a_m x = 0$. Hence $Tor(M) \supseteq \bigoplus A/\langle a_i \rangle$.

Let $x \in M$ be torsion, then by FTFGMPID, we have $x = (\alpha_1, ..., \alpha_r, \alpha_{r+1} + \langle a_1 \rangle, ..., \alpha_{r+m} + \langle a_m \rangle)$. Let $0 \neq a$ be so $ax = 0$, then $a\alpha_1 = ... = a\alpha_r = 0$ and so $\alpha_1 = ... = \alpha_r = 0$. Hence $x \in \bigoplus_{i=1}^n A/\langle a_i \rangle$.

(2): Trivial.

(3): Note $rank(M) = rank(A^r) + rank(Tor(M)) = r$ and the proof follows. ♡

Remark 1.5.19. Recall if A is UFD, and $a \in A$, we can write a "uniquely" as

$$a = u p_1^{n_1} p_2^{n_2} ... p_k^{n_k}$$

where $p_1, ..., p_k$ are non-associative primes in A, $n_i \geq 1$ and u is a unit.

Now suppose A is PID with $i \neq j$. Say $\langle p_i^{n_i} \rangle + \langle p_j^{n_j} \rangle = \langle d \rangle$ for some $d \in A$. Then $d \mid p_i^{n_i}$ and $d \mid p_j^{n_j}$. Therefore, d is a unit as p_i, p_j are non-associative. Thus $\langle p_i^{n_i} \rangle + \langle p_j^{n_j} \rangle = A$.

Also, by unique factorization, we have $\langle p_1^{n_i} \rangle \cap ... \cap \langle p_k^{n_k} \rangle = \langle a \rangle$ and by Chinese Remainder Theorem, we get

$$A/\langle a \rangle \cong A/\langle p_1^{n_1} \rangle \oplus ... \oplus A/\langle p_k^{n_k} \rangle$$

Then, we plugging this into FTFGMPID, invariant form, for each $A/\langle a_i \rangle$, we get FTFGMPID, elementray factor form, Existence.

Theorem 1.5.20 (FTFGMPID, Elementray Divisor Form, Existence). *Keep the same notation as Theorem 1.5.15, we also get*

$$M \cong A^r \oplus A/\langle p_1^{n_1} \rangle \oplus ... \oplus A/\langle p_t^{n_t} \rangle$$

where $p_1, ..., p_t$ are (not necessary distinct) primes in A and $n_1, ..., n_t > 0$ are positive integers.

Proof. We are done. ♡

Example 1.5.21. One should try to use elementray factor form to prove the invariant factor form.

Theorem 1.5.22 (FTFGMPID, Uniqueness)**.** *For Theorem 1.5.15, r and m are unique and $a_1, ..., a_m$ are unique upto multiplication by units.*

For Theorem 1.5.20, r and t are unique, and $p_1, ..., p_t$ are unique upto re-ordering and associative, and $n_1, ..., n_t$ are unique.

Proof. We are not going to proof. ♡

Remark 1.5.23. Note FTFGMPID is a generalization of classification of finitely generated abelian groups when $A = \mathbb{Z}$.

Example 1.5.24. Now let $A = F[x]$ where F is a field.

Suppose I is proper non-trivial ideal in $F[x]$, so $I = \langle p(x) \rangle$ where we may assume $p(x)$ is monic and non-constant. Suppose $p(x) = x^k + b_{k-1}x^{k-1} + ... + b_0$ with $b_0, ..., b_{k-1} \in F$. Then, we have $F[x]/I$, this is a finite dimensional vector space with basis $B = \{1 + \langle p(x) \rangle, x + \langle p(x) \rangle, ..., x^{k-1} + \langle p(x) \rangle\}$, i.e. it's dimension over F is k. Let this denote the first way to form a basis.

In particular, multiplication by x is an F-linear transformation $T : F[x]/I \mapsto F[x]/I$ where

$$[T]_B = \begin{bmatrix} 0 & 0 & ... & 0 & -b_0 \\ 1 & 0 & ... & 0 & -b_1 \\ 0 & 1 & ... & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & ...1 & -b_{k-1} & \end{bmatrix}$$

which is the companion matrix of $p(x)$.

Now assume that $p(x) = (x - \lambda)^k$ for some $k > 0$ and $\lambda \in F$. Then there is another natural F-basis for $F[x]/\langle p(x) \rangle$, which is $E = \{1 + I, (x - \lambda) + I, ..., (x - \lambda)^{k-1} + I\}$. Let's denote this as the second method to form a basis. Now, what is $[T]_E$?

Note $T(1 + I) = x + I = ((x - \lambda) + I) + (\lambda \cdot 1 + I)$ and $T(x - \lambda + I) = x^2 - \lambda x + I = ((x - \lambda)^2 + I) + (\lambda(x - \lambda) + I)$ and so on. Viz

$$[T]_E = \begin{bmatrix} \lambda & 0 & 0 & ... & 0 \\ 1 & \lambda & 0 & ... & 0 \\ 0 & 1 & \lambda & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & ... & \lambda \end{bmatrix} =: J_\lambda^k$$

Now, fix a finite dimensional F vector space V with a linear operator T. Then this makes V a A-module where x acts as T. So V is in particular a f.g. A-module.

Hence, apply FTFGMPID, invariant form, we get

$$V \cong F[x]^r \oplus F[x]/\langle a_1(x) \rangle \oplus ... \oplus F[x]/\langle a_m(x) \rangle$$

where $a_1 \mid a_2 \mid ... \mid a_m$ are non-constant polynomials (and we may assume they are monic) in $Fx]$. We also remark $a_m(x)$ is the minimal polynomial of T.

Now, sicne V is finite dimensional and $F[x]$ is infinite dimensional, we must have $F[x]^r = F[x]^0$, i.e. r must be 0. Therefore,

$$V \cong F[x]/\langle a_1(x)\rangle \oplus ... \oplus F[x]/\langle a_m(x)\rangle$$

For each $F[x]/\langle a_i(x)\rangle$, let B_i be the basis of $F[x]/\langle a_i(x)\rangle$ obtained by method one. Then, let $B = (B_1, B_2, ..., B_m)$ and we get

$$[T]_B = diag(C_{a_1(x)}, ..., C_{a_m(x)})$$

where $C_{a_i(x)}$ is the companion matrix of $a_i(x)$. This is called the ***rational canonical form***.

Now, using FTFGMPID, Elementray Divisor form, we get

$$V \cong F[x]^r \oplus F[x]/\langle p_1(x)^{n_1}\rangle \oplus ... \oplus F[x]/\langle p_m(x)^{n_m}\rangle$$

We must have $r = 0$ as V is finite dimensional. Then, if we assume F is algebraically closed, we must have $p_i(x) = x - \lambda_i$ for some $\lambda_i \in F$ are the only irreducible polynomials.

Hence, we get $p_i(x)^{n_i} = (x - \lambda_i)^{n_i}$. Hence, for each i, let E_i be the basis of $F[x]/\langle p_i(x)^{n_i}\rangle$ given by method two. Let $E = (E_1, ..., E_m)$, we get

$$[T]_E = diag(J_{\lambda_1}^{n_1}, ..., J_{\lambda_m}^{n_m})$$

1.6 Algebra

Definition 1.6.1. An A-***algebra*** is a ring B with a ring homomorphism $f : A \to B$.

Remark 1.6.2. Let (B, f) be an A-algebra. Note f makes B into an A-module by letting $ab := f(a)b$, where $a \in A, b \in B$. Since f is a homomorphism, this indeed satisfies module axioms.

This A-module structure on B is compatible with the ring structure on B in the sense that $a(b_1b_2) = (ab_1)b_2$ for $a \in A, b_1, b_2 \in B$.

Remark 1.6.3. Suppose $(M, +)$ is an A-module that also has a multiplication such that $(M, +, \times)$ is a ring satisfying $a(m_1m_2) = (am_1)m_2$ for $a \in A, m_1, m_2 \in M$, then there exists a ring homomorphism $f : A \to M$ that makes M an A-algebra.

Indeed, consider $f(a) = a \cdot 1_M$, this should give us the desired homomorphism.

This remark and the above remark imply A-algebras are A-modules with compatible ring structure.

Example 1.6.4.

1. Let $A = \mathbb{Z}$, then $\mathbb{Z}$-algebras are just rings. Indeed, every $\mathbb{Z}$-algebra is a ring, and via $1_{\mathbb{Z}} \mapsto 1_R$ we get every ring is a $\mathbb{Z}$ algebra.

2. Let $A = k$ be a field, k-algebras are rings containing k as a subring: for any k-algebra (B, f), we have $f : k \to B$ is injective.
3. Let A be any ring, then $A[x_1, ..., x_n]$ is an A-algebra, with inclusion map $\subseteq$. Also, we have $A[x_1, ..., x_n]/I$ is A-algebra where $I \leq A[x_1, ..., x_n]$ with

$$A \xrightarrow{\subseteq} A[x_1, ..., x_n] \xrightarrow{\pi} A[x_1, ..., x_n]/I$$

where π is the quotient map.

Definition 1.6.5. Given A-algebra $f_1 : A \to B$ and $f_2 : A \to C$, an ***A-algebra homomorphism*** is an A-linear ring homomorphism $g : B_1 \to B_2$.

Remark 1.6.6. Equivalently, g is a ring homomorphism such that

$$\begin{tikzcd} A \arrow[r, "f_1"] \arrow[dr, "f_2"'] & B \arrow[d, "g"] \\ & C \end{tikzcd}$$

commutes.

Definition 1.6.7. An ***A-subalgebra*** of an A-algebra $f : A \to B$ is a subring $B_0 \subseteq B$ such that is an A-submodule. Equivalently, we may say B_0 is a subalgebra if $f(A) \subseteq B_0$. In that case, note

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "f"'] & B_0 \arrow[d, "\subseteq"] \\ & B \end{tikzcd}$$

commutes.

Remark 1.6.8. So, the inclusion map $\subseteq: B_0 \to B$ is an A-algebra homomorphism. We often say A-linear homomorphism instead of A-algebra homomorphism.

Definition 1.6.9. Suppose B is an A-algebra let $\Lambda \subseteq B$. Then the ***A-subalgebra generated by*** Λ is the smallest A-subalgebra of B that containing Λ. Note this is the same as intersection of all subalgebra of B containing Λ. This is denoted by $A[\Lambda]$.

Example 1.6.10. Show that

$$A[\Lambda] = \{p^f(a_1, ..., a_n) : n \geq 1, p \in A[x_1, ..., x_n], a_1, ..., a_n \in \Lambda\}$$

where $f : A \to B$ is the A-algebra and $p^f \in B[x_1, ..., x_n]$ is obtained from p by applying f to the coefficients.

Do this example!

Definition 1.6.11. B is ***finitely generated*** if $B = A[\Lambda]$ for some finite Λ.

Lemma 1.6.12. *Let B be A-algebra. B is finitely generated if and only if $B \cong A[x_1, ..., x_n]/I$ for some ideal $I \leq A[x_1, ..., x_n]$ and some polynomial ring $A[x_1, ..., x_n]$.*

Proof. (⇐): We have $A[x_1, ..., x_n]/I$ is generated by $\Lambda = \{x_1 + I, ..., x_n + I\}$. Any A-algebra isomorphism preserves finitely-generatedness.

(⇒): Suppose B is finitely generated by $\Lambda = \{b_1, ..., b_n\} \subseteq B$. Consider the ring homomorphism $\phi : A[x_1, ..., x_n] \to B$ given by $\phi(p(x_1, ..., x_n)) = p^f(b_1, ..., b_n)$ where $f : A \to B$ is the A-algebra structure on B. One should check this is an A-linear homomorphism.

ϕ is surjective since $B = A[\Lambda]$ and by an above exercise. Now, let $I = Ker(\phi)$, then $A[x_1, ..., x_n]/I \cong B$ as rings. This isomorphism is A-linear because ϕ is. ♡

Example 1.6.13. Note not every f.g. A-algebra is f.g. as an A-module. Indeed, we have $A[x]$ is f.g. A-algebra but $\{1, t, t^2, t_3, ...\}$ are A-linearly independent so $A[t]$ is not even of finite rank.

Definition 1.6.14. An A-algebra B is said to be ***finite*** if it is finitely generated as an A-module.

Remark 1.6.15. Note finite algebras are ***not necessarily*** finite.

Also, finite A-algebra are f.g. as A-algebra. Indeed, suppose B is an A-algebra, $x_1, ..., x_n \in B$ generates B as A-module. Then $B = \langle x_1, ..., x_n \rangle$.

Consider $A[x_1, ..., x_n] \subseteq B$, where $A[x_1, ..., x_n]$ is the A-subalgebra generated by $x_1, ..., x_n$. Hence $A[x_1, ..., x_n]$ is an A-submodule and so $A[x_1, ..., x_n] = B$.

Example 1.6.16. Let k be a field, then $B = k[x]/\langle x^2 \rangle$ is a f.g. k-algebra. This is a finite algebra. Let $\bar{t}$ be the coset $t + \langle t^2 \rangle$, then every element of B is of the form $a + b\bar{t}$ for some $a, b \in k$. Hence $\{1, \bar{t}\}$ generates B as a k-module, i.e. B is a finite k-algebra.

Definition 1.6.17. Fix an A-algebra $f : A \to B$. If M is a B-module then it has a natural A-module structure given by $a \in A, x \in M$ then $ax := f(a)x$. This is called ***restriction of scalars***.

Definition 1.6.18. Let M be an A-module, let $f : A \to B$ be an A-algebra. Consider the A-module $M \otimes_A B$. We have $M \otimes_A B$ is a B-module by setting, for $b \in B$, $\sum_i x_i \otimes b_i \in M \otimes_A B$, to be that $b(\sum_i x_i \otimes b_i) = \sum_i x_i \otimes bb_i$.

This is called ***extension of scalars***.

Proposition 1.6.19 (Prop 2.16)**.** *Let B be finite A-algebra, M be f.g. B-module. Then the restriction of scalars makes M a f.g. A-module.*

Proof. Indeed, if $b_1, ..., b_n$ generates B as A-module and $x_1, ..., x_m$ generates M as A-module. Then $\{b_i x_j : 1 \le i \le n, 1 \le j \le m\}$ generates M as an A-module. ♡

Proposition 1.6.20 (Prop 2.17)**.** *Suppose M is f.g. A-module, then $M \otimes_A B$ is a f.g. B-module.*

Proof. Consider $x_1, ..., x_m$ be generators of M, then $\{x_i \otimes 1 : 1 \le i \le m\}$ is a set of generators of $M \otimes_A B$.

Let $\alpha = \sum_i m_i \otimes b_i$, where each $m_i = \sum_{j=1}^m a_{ij}x_j$ for $a_{ij} \in A$. Then, we have

$$\begin{aligned}\alpha &= \sum_i(\sum_j a_{ij}x_j) \otimes b_i = \sum_{i,j} a_{ij}x_j \otimes b_i \\ &= \sum_{i,j} x_j \otimes a_{ij}b_j = \sum_j(\sum_i x_j \otimes a_{ij}b_i) \\ &= \sum_j(x_j \otimes \sum_i a_{ij}b_i) = \sum_j c_j(x_j \otimes 1), \quad c_j = \sum_i a_{ij}b_j \in B\end{aligned}$$

♡

Theorem 1.6.21 (Universal Proeprty of Tensor of Modules)**.** *Let M, N be two A-modules. Given any A-bilinear function $f : M \times N \to E$ where P is A-module, then the following commutes*

$$\begin{tikzcd} M \times N \arrow[r, "i"] \arrow[dr, "f"'] & M \otimes N \arrow[d, "\exists! \phi"] \\ & E \end{tikzcd}$$

where $\phi : M \otimes_A N \to E$ is a unique A-linear map.

Corollary 1.6.21.1. *We have a multi-linear universal proeprty, i.e. n-linear maps from $\prod_{i=1}^n N_i$ to P correspond to A-linear map between $\otimes_{i=1}^n N_i$ to P.*

Proof. Say $M \otimes_A N = C/D$ where $C = A^{M \times N}$ is the free A-module and D is the A-submodule generated by bilinearty relations.

Extend f to an A-linear map $f' : C \to E$ by $(a_{(x,y)} : x \in M, y \in N) \mapsto \sum_{x,y} a_{(x,y)} f(x, y)$. We have f' is A-lienar. Since f' is A-bilinear, we get $Ker(f') \supseteq D$. By universal property of quotient, we get unique $\overline{f} : C/D \to E$ such that

$$\overline{f}(x \otimes y) = \overline{f}((0, ..., 1, ...) + D) = f'(0, ..., 1, ...) = f(x, y)$$

♡

Remark 1.6.22. The point of this is that this is the defining property of tensor product, i.e. every A-linear map from $M \otimes N$ is obtained from consider A-bilinear maps from $M \times N$.

Remark 1.6.23. Now, let $f : A \to B$ and $g : A \to C$ be two A-algebra. We want to define an A-algebra structure on $B \otimes_A C$. We need a ring multiplication and the right one is $(b \otimes c)(b' \otimes c') = (bb') \otimes (cc')$.

Consider the map $B \times B \times C \times C \to B \otimes C$ given by $(b, b', c, c') \mapsto bb' \otimes cc'$. This is A-linear in each component, i.e. it is multi-linear. Hence, by universal proeprty we get an A-linear map from $B \otimes B \otimes C \otimes C$ to $B \otimes C$ and in particular note $B \otimes B \otimes C \otimes C \cong (B \otimes C) \otimes (B \otimes C)$.

Hence, we get an A-linear map from $(B \otimes C) \otimes (B \otimes C)$ to $B \otimes C$. Hence, we get a bilinear map from $(B \otimes C) \times (B \otimes C)$ to $B \otimes C$, i.e. we get our ring multiplication well-defined on $B \otimes_A C$. Viz, $B \otimes C$ is an A-algebra under the ring homomorphism $a \mapsto f(a) \otimes g(a)$.

Remark 1.6.24. Note $B \otimes_A C$ also has natural B and C algebra structure. Indeed, consider the map $b \mapsto b \otimes 1$ gives an B-algebra and $c \mapsto 1 \otimes c$ gives an C-algebra. Viz, we have the following diagram commutes where $D = B \otimes_A C$:

$$\begin{tikzcd} & B \arrow[dr, "id_B \otimes 1"] & \\ A \arrow[ur, "f"] \arrow[dr, "g"'] & & D \\ & C \arrow[ur, "1 \otimes id_C"'] & \end{tikzcd}$$

Example 1.6.25.

1. We have $\mathbb{Q}[x] \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}[x]$ as $\mathbb{R}$-algebras induced by $p(x) \otimes r \mapsto rp(t)$. We first show this is an isomorphism of $\mathbb{Q}$-module, then check it is an $\mathbb{R}$-algebra isomorphism.
2. We have $\mathbb{Q}[x] \otimes_{\mathbb{Q}} \mathbb{Q}[x] \cong \mathbb{Q}[x, y]$ as $\mathbb{Q}$-algebra via $p(x) \otimes q(x) \mapsto p(x)q(y)$. Note $x \otimes 1 \neq 1 \otimes x$ in $\mathbb{Q}[x] \otimes \mathbb{Q}[x]$.

Chapter 2

Ring

"Should you just be an algebraist or a geometer?" is like saying "Would you rather be deaf or blind?"

Michael Atiyah

2.1 Ring Of Fraction

Definition 2.1.1. Let A be a ring, let S be a subset of A. S is said to be ***multiplicatively closed*** if $1 \in S$ and $a, b \in S$ imply $ab \in S$.

Definition 2.1.2. Now, define an equivalence relation $\sim$ on $A \times S$ by $(a, s) \sim (b, t)$ if $(at - bs)v = 0$ for some $v \in S$.

Remark 2.1.3. Note in the above equivalence relation, syymmetry and flexivity are clear. Now, say $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$. Then, we have $(at - bs)v = 0$ and $(bu - ct)w = 0$. Hence, we get

$$atvuw - bsvuw = 0$$

and

$$buwvu - ctwvu = 0$$

Hence we have

$$(av - cs)twv = 0$$

Definition 2.1.4. Now, we define $S^{-1}A := A \times S/\sim$ where $\sim$ is the equivalence relation we defined above. This is called the ***ring of fractions with denominators from*** S (or the ***localization of*** A ***at*** S).

Remark 2.1.5. We view elements of $S^{-1}A$ as fractions with numerator in A and denominator in S and we also write $\frac{a}{s}$ to be the equivalence class at (a,s) as representative.

Remark 2.1.6. Note if $0 \in S$ if and only if $S^{-1}A = \langle 0 \rangle$. Hence we usually assume $0 \notin S$. We also remark $\frac{a}{s} = \frac{b}{t}$ if and only $(at - bs)v = 0$ for some $v \in S$. If A is an integral domain and $0 \notin S$, then $\frac{a}{s} = \frac{b}{t}$ iff $at = bs$.

Remark 2.1.7. In general, we make $S^{-1}A$ a ring by $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$ and $\frac{a}{s}\frac{b}{t} = \frac{ab}{st}$. One should check this is well-defined on $S^{-1}A$ and we have $A \to S^{-1}A$ given by $a \mapsto \frac{a}{1}$ is a ring homomorphism. Hence $S^{-1}A$ is an A-algebra.

Note the point of ring of fraction is that elements of S becomes units.

Example 2.1.8. When A is an integral domain and $S = A \backslash \{0\}$, then $S^{-1}A = Frac(A)$ is the field of fraction.

Theorem 2.1.9 (Universal Property Of Ring of Fraction)**.** *Let $g : A \to B$ be an A-algebra such that $g(s) \in B^{\times}$ for all $s \in S$. Then there exists unique A-lienar h such that $g = h \circ c$ where $c : A \to S^{-1}A$ maps a to $\frac{a}{1}$. Viz, the following commutes:*

$$\begin{tikzcd}
A \arrow[r, "g"] \arrow[d, "c"] & B \\
S^{-1}A \arrow[ur, "h"] &
\end{tikzcd}$$

Proof. Define $h(\frac{a}{s}) = g(a)g(s)^{-1}$. We first show it is well-defined, suppose $\frac{a}{s} = \frac{a'}{s'}$, then $(as' - a's)v = 0$ for some $v \in S$.

Then, apply g, we get $(g(a)g(s') - g(a')g(s))g(v) = 0$. Since $v \in S$, we have $g(v) \in B^{\times}$. Multiply both side by $g(v)^{-1}$, we get $g(a)g(s') - g(a')g(s) = 0$ and so $g(a)g(s') = (g(a')g(s'))^{-1}$.

We should check h is a ring homomorphism and note $h(\frac{a}{1}) = g(a)g(1)^{-1} = g(a)$.

If $h(x) = h'(x)$ and x is a unit, then $h(x^{-1}) = h'$ ♡

Definition 2.1.10. A ***local ring*** is a ring with only one maximal ideal.

Example 2.1.11.

1. Let $P \subsetneq A$ be a prime ideal, then $S := A \backslash P$ is multiplicatively closed as $1 \in S$ and $a, b \notin P$ then $ab \notin P$ as P is prime. Then we denote $S^{-1}A$ to be A_P and it called ***localization of*** A ***at*** P
   Note every proper ideal of A_P is contained in PA_P. Viz, consider A as embedded into A_P, then P is embedded in A_P, hence the extension ideal PA_P is generated by $\{\frac{a}{1} : a \in P\}$.
   Why? Because everything in $A_P \backslash PA_P$ is a unit in A_P. So A_P is a local ring with maximal ideal PA_P.
2. Let $f \in A$, let $S := \{1, f, f^2, f^3, ...\}$, this is multiplicatively closed. We denote $S^{-1}A = A_f$ and are called the localization of f.

2.2 Localization of Modules

Definition 2.2.1. Let M be an A-module, $S \subseteq A$ be multiplicatively closed. Then $S^{-1}M = M \times S/\sim$ where $\sim$ is the equivalence relation given by $(x, s) \sim (y, t)$ iff $\exists u \in S$ such that $u(sy - tx) = 0$ where $x, y \in M$ and $s, t, u \in S$.

We denote elements in $S^{-1}M$ by $\frac{x}{s}$ where $s \in M, s \in S$.

Remark 2.2.2. Note $S^{-1}M$ is an $S^{-1}A$-module by $\frac{x}{s} + \frac{y}{t} = \frac{tx+sy}{st}$ and $\frac{a}{t} \cdot \frac{x}{s} = \frac{ax}{ts}$ where $a \in A, s, t \in S$ and $x \in M$.

Note if $S = A \backslash P$, then we write M_P for $S^{-1}M$. Also, if $S = \{1, t, t^2, t^3, ...\}$, we write M_f for $S^{-1}M$.

Remark 2.2.3. Let S be multiplicatively closed. Note S^{-1} is a functor from A-modules to $S^{-1}A$-modules. M is an A-module then we define a natural $S^{-1}A$-module $S^{-1}M := \{\frac{m}{s} : m \in M, s \in S\}$. Also, if $f : M \to N$ is A-linear, then $S^{-1}f : S^{-1}M \to S^{-1}N$ is $S^{-1}A$-linear, where $S^{-1}f(\frac{m}{s}) = \frac{f(m)}{s}$.

Observe $S^{-1}(f \circ g) = S^{-1}f \circ S^{-1}g$, i.e. it is covariant.

Proposition 2.2.4 (Prop 3.3)**.** *S^{-1} is an **exact** functor, i.e.*

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

is exact then

$$S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$$

is exact.

Proof. Suppose $g \circ f = 0$, then $S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f = 0$, i.e. $Im(S^{-1}f) \subseteq Ker(S^{-1}g)$. Conversely, say $\frac{m}{s} \in Ker(S^{-1}g)$, then $S^{-1}g(\frac{m}{s}) = \frac{g(m)}{s} = 0$. Hence $tg(m) = 0$ for some $t \in S$ in M''. Observe $tg(m) = g(tm)$ and so $tm \in Ker(g) \subseteq Im(f)$. Hence $tm = f(m')$ for some $m' \in M'$ and so $\frac{tm}{s} = \frac{f(m')}{s}$ in $S^{-1}M$. Scalar multiply both side by $\frac{1}{t} \in S^{-1}A$, we get

$$\frac{m}{s} = \frac{f(m')}{ts} = S^{-1}f(\frac{m'}{ts}) \Rightarrow \frac{m}{s} \in Im(S^{-1}f)$$

♡

Corollary 2.2.4.1 (Cor 3.4)**.** *Let N, P be A-submodule of M.*

1. *Let $\iota : N \to M$ be the containment map, then $S^{-1}\iota : S^{-1}N \to S^{-1}M$ is injective.*
2. *There is a natural $S^{-1}A$ isomorphism*

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

3. *$S^{-1}(N + P) = S^{-1}N + S^{-1}P$ in $S^{-1}M$.*
4. *$S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$*

Proof. (1): Apply Proposition 2.2.4 to

$$0 \longrightarrow N \xrightarrow{\iota} M$$

Thus, we can and do view $S^{-1}N$ as an $S^{-1}A$-submodule of $S^{-1}M$.

(2): Apply Proposition 2.2.4 to

$$0 \longrightarrow N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \longrightarrow 0$$

and hence after S^{-1} it is still exact, i.e.

$$0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}\iota} S^{-1}M \xrightarrow{S^{-1}\pi} S^{-1}(M/N) \longrightarrow 0$$

and we get our isomorphism.

(3): Clear.

(4): Note $S^{-1}(N \cap P) \subseteq S^{-1}N \cap S^{-1}P$ is trivial. Now, suppose $\alpha \in S^{-1}M$ such that $\alpha = \frac{n}{s} = \frac{p}{t}$ where $n \in N, p \in P, s, t \in S$. Then, note there exists $u \in S$ so $u(tn - sp) = 0$ in M. Thus $(ut)n = (us)p =: x \in N \cap P$. Thus we observe

$$\frac{x}{uts} = \frac{(ut)n}{uts} = \frac{n}{s} = \alpha \Rightarrow \alpha \in S^{-1}(N \cap P)$$

♡

Definition 2.2.5. An A-module M is ***flat*** if for any exact sequence E, we have $E \otimes M$ (tensor M to each term) is flat.

Proposition 2.2.6 (Prop 3.5)**.** *We have*

$$S^{-1}M \cong M \otimes S^{-1}A$$

as $S^{-1}A$-module. Viz, $S^{-1}M$ is the extension of scalar of M from A to $S^{-1}A$.

Proof. We will first show those two are isomorphic as A-modules. Consider the map $h : M \times S^{-1}A \to S^{-1}M$ given by $h(m, a/s) = am/s$, this h is bilinear.

Hence, we get $f : M \otimes_A S^{-1}A \to S^{-1}M$ given by $f(m \otimes \frac{a}{s}) = \frac{am}{s}$. This map is surjective, i.e. $\frac{m}{s} = f(m \otimes \frac{1}{s})$ for arbitrary $\frac{m}{s} \in S^{-1}M$.

Let $g : S^{-1}M \to M \otimes_A S^{-1}A$ be the map $g(\frac{m}{s}) = m \otimes \frac{1}{s}$. We first show it is well-defined. Say $\frac{m}{s} = \frac{m'}{s'}$, i.e. $t(s'm - sm') = 0$ for some $t \in S$. Then, observe

$$\begin{aligned} m \otimes \frac{1}{s} - m' \otimes \frac{1}{s'} &= m \otimes \frac{ts'}{tss'} - m \otimes \frac{ts}{tss'} \\ &= ts'm \otimes \frac{1}{tss'} - tsm' \otimes \frac{1}{tss'} \\ &= (ts'm - tsm') \otimes \frac{1}{tss'} \\ &= 0 \otimes \frac{1}{tss'} = 0 \end{aligned}$$

Then, we should check g is A-linear and both $g \circ f$ and $f \circ g$ are both identity. Hence, we have $S^{-1}M \cong M \otimes_A S^{-1}A$ as A-module.

Finally, check f is $S^{-1}A$-linear and g is well-defined as $S^{-1}A$ map. However, we do not need to check linearity for g to conclude f is an isomorphism. ♡

Corollary 2.2.6.1 (Cor 3.6)**.** *$S^{-1}A$ is a flat A-module.*

Proof. Take arbitrary exact sequence

$$M' \otimes S^{-1}A \to M \otimes S^{-1}A \to M'' \otimes S^{-1}A$$

then we have the following diagram commutes

$$\begin{tikzcd} M' \otimes S^{-1}A \arrow[r, "f\otimes 1"] \arrow[d, "\cong"] & M \otimes S^{-1}A \arrow[r, "g\otimes 1"] \arrow[d, "\cong"] & M'' \otimes S^{-1}A \arrow[d, "\cong"] \\ S^{-1}M' \arrow[r, "S^{-1}f"] & S^{-1}M \arrow[r, "S^{-1}g"] & S^{-1}M'' \end{tikzcd}$$

Then apply Proposition 2.2.4 on the lower sequence. ♡

2.3 Contraction & Extension

Definition 2.3.1. Let $f : A \to B$ be an A-algebra,

1. Let $I \leq A$, the ideal $IB := \langle \{f(a) : a \in I\} \rangle$ is called the ***extension*** of I.
2. Let $J \leq B$, the ideal $J \cap A := f^{-1}(J)$ is called the ***contraction*** of J

Remark 2.3.2. If $Q \leq B$ is a prime ideal then $Q \cap A$ is prime. However, $Q \leq A$ is prime does not imply QB is prime.

Lemma 2.3.3. *Let $f : A \to S^{-1}A$ be an A-algebra where $f(a) = \frac{a}{1}$ and S be multiplicatively closed. Let $I \leq A$, then*

$$IS^{-1}A = \langle f(I) \rangle = S^{-1}I := \{\frac{a}{s} : a \in I, s \in S\}$$

Proof. Say $a \in I, s \in S$, then $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in I(S^{-1}A)$ as $\frac{1}{s} \in S^{-1}A$ and $\frac{a}{1}$ in $f(I)$. Thus $IS^{-1}A \supseteq S^{-1}I$.

Say $\sum_{i=1}^{n} \frac{b_i}{s_i}\frac{a_i}{1} \in IS^{-1}A = \langle f(I) \rangle$ where $b_i \in A, s_i \in S$ and $s_i \in I$. Then we have

$$\sum_{i=1}^{n} \frac{b_i}{s_i}\frac{a_i}{1} = \frac{\sum_{i=1}^{n} \left(\prod_{[n]-i} s_i\right) b_i a_i}{\prod_{i=1}^{n} s_i} \in S^{-1}I$$

where $\prod_{[n]-i} s_i$ means product from 1 to n taking out i. ♡

Proposition 2.3.4.

1. *If $J \leq S^{-1}A$ then $J = (J \cap A)S^{-1}A$. In particular, every ideal in $S^{-1}A$ is an extension ideal.*
2. *If $I \leq A$ is a contraction then $I = (IS^{-1}A) \cap A$*
3. *Let $I \leq A$, then $(IS^{-1}A) \cap A = (I : S)$ where $(I : S) := \{x \in A : \exists s \in S, sx \in I\}$ is called the* ***saturation****.*
4. *Let $I \leq A$, then I is contraction if and only if in A/I, no element of S/I is a zero divisor.*
5. *We have a bijective correspondence between the set of prime ideals in A that does not intersect S, denoted by[1] $Spec(A - S)$ and the set of prime ideals in $S^{-1}A$, denoted by $Spec(S^{-1}A)$ via*

$$\begin{aligned} F : Spec(A - S) &\to Spec(S^{-1}A) \\ P &\mapsto PS^{-1}A \end{aligned}$$

and

$$\begin{aligned} G : Spec(S^{-1}A) &\to Spec(A - S) \\ Q &\mapsto Q \cap A \end{aligned}$$

Proof. (1):

Note $(J \cap A)S^{-1}A = S^{-1}(J \cap A)$, i.e. $\frac{a}{s} \in (J \cap A)S^{-1}A$ if we have $a \in J \cap A$ and $s \in S$. Thus take $\frac{a}{s} \in (J \cap A)S^{-1}A$ be arbitrary. Since $a \in J \cap A$, this imply $f(a) \in J$, i.e. $\frac{a}{1} \in J$. Hence $\frac{a}{s} = \frac{1}{s}\frac{a}{1} \in J$ and so $J \supseteq (J \cap A)S^{-1}A$.

Say $\frac{x}{s} \in J$, then we have $\frac{x}{1} = s \cdot \frac{x}{s} \in J$. Thus $x \in J \cap A$ as we have $f(x) \in J \Rightarrow x \in f^{-1}(J)$. Hence we have $\frac{x}{s} \in S^{-1}(J \cap A) = (J \cap A)S^{-1}A$ as desired. The double inclusion means $J = (J \cap A)S^{-1}A$.

(2): Suppose $I = J \cap A$ for some $J \leq S^{-1}A$. Then $IS^{-1}A = (J \cap A)S^{-1}A = J$ and so $(IS^{-1}A) \cap A = J \cap A = I$. We remark this imply I is contraction iff $I = (IS^{-1}A) \cap A$.

(3):

$\supseteq$: Take $x \in (I : S)$ with $sx \in I$ where $s \in S$. Then $f(x) = \frac{x}{1} = \frac{sx}{s} \in S^{-1}I = IS^{-1}A$, i.e. $x \in f^{-1}(IS^{-1}A) = (IS^{-1}A) \cap A$. Hence $(I : S) \subseteq IS^{-1}A \cap A$.

$\subseteq$: Say $x \in (IS^{-1}A) \cap A$, then $\frac{x}{1} \in IS^{-1}A = S^{-1}I$. Hence $\frac{x}{1} = \frac{a}{s}$ for some $a \in I, s \in S$. Thus $tsx = ta$ for some $t \in S$ and so $tsx \in I$, i.e. $x \in (I : S)$.

(4):

$$\begin{aligned} I \text{ is contraction} &\Leftrightarrow I = (IS^{-1}A) \cap A \quad \text{by (2)} \\ &\Leftrightarrow I = (I : S) \quad \text{by (3)} \\ &\Leftrightarrow \forall x \in A, \forall s \in S(sx \in I \Rightarrow x \in I) \\ &\Leftrightarrow \forall \overline{x} \in A/I, \forall \overline{s} \in S/I(\overline{sx} = 0 \Rightarrow \overline{x} = 0) \end{aligned}$$

(5): Let $Q \in Spec(S^{-1}A)$, i.e. $Q \leq S^{-1}A$ is prime. Then we claim the following

[1] we remark that this is actually not a spectrum of any rings, but just a conveniences of notations

- $Q \cap A$ is prime in A,
- $Q \subsetneq S^{-1}A$ imply $Q \cap S = \emptyset$.

To see the first point, say $ab \in Q \cap A$, then $f(ab) \in Q \Rightarrow f(a) \in Q$ or $f(b) \in Q$ as Q is prime. Hence $a \in Q \cap A$ or $b \in Q \cap A$. To see the second point, we show for any ideals Q we have $Q \cap S \neq \emptyset$ imply $Q = S^{-1}A$. Indeed, since $0 \neq s \in Q \cap S$, we have $\frac{1}{s} \cdot s \in Q \Rightarrow 1 \in Q \Rightarrow Q = S^{-1}A$.

Therefore, we have $Q \cap A$ is prime in A and as $Q \subsetneq S^{-1}A$ we have $Q \cap S = \emptyset$. Viz, $G(Q) \in Spec(A - S)$ as claimed.

Conversely, let $P \leq A$ be so $P \cap S = \emptyset$. We show $S^{-1}A/S^{-1}P$ is integral domain and this would imply $F(P) = S^{-1}P$ is prime.

Note $S^{-1}A/S^{-1}P \cong S^{-1}(A/P)$ as A-module by Cor 3.4. In fact the A-module isomorphism is a ring homomorphism, hence they are isomorphic as rings(need to check).

Note
$$S^{-1}(A/P) \subseteq Frac(A/P)$$
where A/P is an integral domain, we have $S^{-1}(A/P)$ is a subring of a field. We claim $S^{-1}(A/P)$ is not a trivial ideal. Indeed, for the sake of contradiction say $P \cap S = \emptyset$ and $S^{-1}(A/P) = 0$. Note $S^{-1}(A/P) = 0$ imply $\forall a \in A$, $\frac{a+P}{s} = \frac{0+P}{1}$, i.e. $\exists t_a \in S, t_a(1 \cdot (a+P) - s(0+P)) = 0 + P$. This imply $t_a a + P = 0 + P$, i.e. $t_a a \in P$. Hence we have $(S^{-1}P) \cap A = (P : S) = A$ as our a was arbitrary. This imply $P = A$ as we take $a \in A$ to be arbitrary, then $a \in (S^{-1}P) \cap A$, i.e. $f(a) = \frac{a}{1} \in S^{-1}P$ and so $\frac{a}{1} = \frac{p}{s}$ where $p \in P, s \in S$. Thus $t(sa - p) = 0 \Rightarrow tp = tsa \Rightarrow tsa \in P$. However, $ts \in S$ so we must have $a \in P$ as P is prime and $P \cap S = \emptyset$. Thus $A \subseteq P \Rightarrow A = P$. Therefore $S \cap P = S \cap A = S$, a contradiction.

Hence we have $S^{-1}A/S^{-1}P$ is an integral domain and so $S^{-1}P$ is prime as desired.

Now we need to show the two maps are inverse of each other. Say we have $Q \leq S{-}1A$ be prime, then $Q = (Q \cap A)S^{-1}A$ so $F \circ G = Id$.

Conversely, let $P \leq A$ be prime and $P \cap S = \emptyset$, then A/P has only 0 as a zero divisor but $0 \notin \overline{S}$ since $S \cap P = \emptyset$. Hence $\overline{S}$ has no zero divisors in A/P. Thus by part (4) we have P is a contraction ideal and by part (2) we have $P = S^{-1}P \cap A$. Thus $G \circ F(P) = P$. ♡

2.4 Spectrum

Definition 2.4.1. We define the ***spectrum of*** A, $Spec(A)$, to be the set of all prime ideals in A equipped with the ***Zariski topology***: the closed sets are of the form $V(E) := \{P \in Spec(A) : P \supseteq E\}$ for $E \subseteq A$.

Proposition 2.4.2. *The topology above is indeed a topology.*

Proof. We have $Spec(A) = V(\emptyset) = V(0)$. We have $\emptyset = V(1) = V(A)$.

Next, note $\bigcap_{i\in I} V(E_i) = V(\bigcup_{i\in I} E_i)$. Indeed, take $P \in \bigcap_{i\in I} V(E_i)$, then $P \in V(E_i) \Rightarrow P \supseteq E_i$ for all $i \in I$, hence $P \supseteq \bigcup_{i\in I} E_i$ and so $P \in V(\bigcup_{i\in I} E_i)$. On the other hand, since P contains all of E_i, we have P contains each E_i and so indeed $\bigcap_{i\in I} V(E_i) = V(\bigcup_{i\in I} E_i)$ as claimed.

Before we show finite union is closed, we remark that $V(E) = V(\langle E\rangle)$ for all $E \subseteq A$. Take $P \in V(E)$, then $P \supseteq E$ and hence $P \supseteq \langle E\rangle$ trivially as P is an ideal. Conversely, we note $P \supseteq \langle E\rangle \supseteq E$.

Next, we claim $V(E) \cup V(F) = V(\langle E\rangle) \cup V(\langle F\rangle) = V(\langle E\rangle \cap \langle F\rangle)$. Indeed, say $P \supseteq \langle E\rangle\langle F\rangle$ and $P \not\supseteq \langle E\rangle$. Then $\langle F\rangle \subseteq P$ immediately as this is another characterisation of prime ideals. Therefore, we have $V(E) \cup V(F) \supseteq V(\langle E\rangle\langle F\rangle)$ and in particular we get $V(E)\cup V(F) \supseteq V(\langle E\rangle \cap \langle F\rangle)$ as $\langle E\rangle\langle F\rangle \subseteq \langle E\rangle \cap \langle F\rangle$ and $E \subseteq F \Rightarrow V(F) \subseteq V(E)$.

However, note $V(\langle E\rangle \cap \langle F\rangle) \supseteq V(\langle E\rangle) \cup V(\langle F\rangle) = V(E) \cup V(F)$ trivially, thus we have $V(E) \cup V(F)$ is closed as

$$V(E) \cup V(F) = V(\langle E\rangle \cap \langle F\rangle)$$

♡

Remark 2.4.3. Note basic Zariski open sets in $Spec(A)$ are of the form $D_f = \{P \in Spec(A) : f \notin P\}$ for all $f \in A$. We have $Spec(A)\backslash V(E) = \bigcup_{f\in E} D_f$ for arbitrary $E \subseteq A$ and so they are called basic Zariski open sets.

Now fix $f \in A$, consider $A_f = S^{-1}\langle 1, f, f^2, ...\rangle$. Note for $P \in Spec(A)$, we have $f \notin P$ if and only if $P \cap \langle 1, f, f^2, ...\rangle = \emptyset$. So, there exists a bijective Correspondence between D_f and $Spec(A_f)$ via extension and contraction. Viz, $P \mapsto PA_f$ and $Q \mapsto Q \cap A$.

Example 2.4.4. The map $P \mapsto PA_f$ and $Q \mapsto Q \cap A$ is a homeomorphism where D_f has the topology induced from $Spec(A)$ and $Spec(A_f)$ has Zariski topology.

Definition 2.4.5. Let $I \leq A$ be an ideal, we define the ***nil*-radical** $\sqrt{I}$ to be

$$\sqrt{I} = \{f \in A : \exists n \in \mathbb{N}, f^n \in I\}$$

Proposition 2.4.6 (Prop 1.8). *Given ideal $I \leq A$, we have*

$$\sqrt{I} = \bigcap\{P \in Spec(A) : P \supseteq I\}$$

Proof. It suffice to prove this statement in in A/I where $I = \langle 0\rangle$. We will show $\sqrt{0} = \bigcap_{P\in Spec(A)} P$.

Note $\subseteq$ is trivial.

Now, say $f \notin \sqrt{0}$. We will find a prime that does not contain f. Consider the localization A_f. Recall $S^{-1}A$ is trivial if and only if $0 \in S$. However, $0 \notin \langle 1, f, f^1, f^2, ...\rangle$ since $f \notin \sqrt{0}$.

Thus $A_f \neq \langle 0 \rangle$ and hence there exists $Q \in Spec(A_f)$. So $Q \cap A \in Spec(A)$ that does not contain f. ♡

Proposition 2.4.7 (Prop 3.16). *Suppose $f : A \to B$ an A-algebra. Let $P \in Spec(A)$, the following are equivalent:*

1. *P is the contraction ideal of a prime ideal.*
2. *P is a contraction of an ideal.*
3. *$P = PB \cap A$.*

Proof. (1) $\Rightarrow$ (2): Trivial.

(2) $\Rightarrow$ (3): Suppose $P = J \cap A$ for some $J \leq B$. Then $PB \cap A = [(J \cap A)B] \cap A \subseteq J \cap A = P$. However, the converse is clear. Hence we are done.

(3) $\Rightarrow$ (1): We want to find $Q \in Spec(B)$ such that $Q \cap A = PB \cap A$, i.e. $Q \supseteq PB$ such that $(Q \cap A) \cap (A \backslash P) = \emptyset$.

Let $S := f(A \backslash P) \subseteq B$. This is multiplicatively closed.

We claim $PB \cap S = \emptyset$. Say $x \in A \backslash P$ and $f(x) \in PB$, then $x \in f^{-1}(PB) = PB \cap A = P$ as we are assuming (3). This is a contradiction and so they indeed intersect trivially.

Now, consider $A \xrightarrow{f} B \longrightarrow S^{-1}B$. Since $PB \cap S = \emptyset$, we have $(PB)S^{-1}B$ is a proper ideal. Let M be a maximal ideal in $S^{-1}B$ that contains $(PB)S^{-1}B = PS^{-1}B$.

Let $Q = M \cap B \in Spec(B)$, we claim $Q \cap A = P$. Indeed, $\supseteq$ is trivial. Next, we note $Q \cap S = \emptyset$ since $Q = M \cap B$ and $M \in Spec(S^{-1}B)$. Hence $Q \subseteq B \backslash S = B \backslash f(A \backslash P)$ ♡

2.5 Primary Decomposition

Definition 2.5.1. For $Q \leq A$, Q is ***primary ideal*** if $Q \neq A$ and whenever $xy \in Q$ we have $x \in Q$ or $y^n \in Q$ for some n.

Remark 2.5.2. We have Q is primary if and only if in A/Q, every zero divisor is nilpotent.

Lemma 2.5.3. *Contraction of primary ideals are primary.*

Proof. Let $f : A \to B$ be an algebra. This induces an embedding from $A/Q \cap A$ to B/Q for any $Q \leq B$. Note in B/Q every zero divisor is nilpotent, so the subring of B/Q also has this property. Viz $Q \cap A$ is primary. ♡

Proposition 2.5.4 (Prop 4.1). *Let Q be primary ideal in A, then $\sqrt{Q}$ is the smallest prime ideal containing Q.*

Proof. Recall $\sqrt{Q} = \bigcap_{P \in Spec(A), Q \subseteq P} P$, i.e. if it is prime, it is the smallest prime that contains Q. Hence we only need to show it is prime.

Let $xy \in \sqrt{Q}$, then $x^m y^m \in Q$ for some $m > 0$. Thus $x^m \in Q$ or $y^{nm} \in Q$ for some $n > 0$. In either case we have $x \in \sqrt{Q}$ or $y \in \sqrt{Q}$. ♡

Lemma 2.5.5. *If A is a UFD and $p \in A$ is prime, then $\langle p^n \rangle$ is primary for any $n > 0$.*

Proof. Suppose $xy \in \langle p^n \rangle$. Consider the prime factorization $xy = p^m \prod_{i=1}^n q_i$ where $m \geq n$ and q_i are primes distinct from p. If $p^n \nmid x$, i.e. $x \notin \langle p^n \rangle$, then $p \mid y$. Indeed, if p^n does not divide x, this means x has at most $n-1$ copies of p in it's factorization and so we have at least one copy of p that is contributed from y. Thus $y \in \langle p \rangle$ and so $y^n \in \langle p^n \rangle$, i.e. $\langle p^n \rangle$ is primary. ♡

Example 2.5.6. Try to show, if A is a PID, then the converse of the above lemma is true: every primary ideal is of the form $\langle p^n \rangle$ for some prime $p \in A$ and $n > 0$.

Solution. Suppose A is a PID. Let Q be a primary ideal. Then we have $Q = \langle x \rangle$ as A is PID. Let $x = \prod_{i=1}^n p_i^{k_i}$ be the factorization of x where p_i's are all distinct primes as A is PID imply A is UFD.

Observe that since $p_1^{k_1} \prod_{i=1}^n p_i^{k_i} \in Q$ we have either $p_1^{k_1} \in Q$ or $(\prod_{i=1}^n p_i^{k_i})^{z_1} \in Q$. However, observe $p_1^{k_1} \in Q$ imply $x \mid p_1^{k_1}$ where we see clearly $p_1^{k_1} \mid x$. Hence, we have $p_1^{k_1}$ and x generates the same ideal (take elements in $\langle p_1^{k_1} \rangle$ then it can be written as elements in $\langle x \rangle$ and vice versa.), i.e. $Q = \langle p_1^{k_1} \rangle$ as desired.

If $(\prod_{i=1}^n p_i^{k_i})^{z_1} \in Q$, then that is preposterous! Indeed, $(\prod_{i=1}^n p_i^{k_i})^{z_1} \in Q$ imply x divides $(\prod_{i=1}^n p_i^{k_i})^{z_1}$. However, $(\prod_{i=1}^n p_i^{k_i})^{z_1}$ is missing the term $p_1^{k_1}$ which is in the unique factorization of x. A contradiction as x divides something imply that something contains $p_1^{k_1}$.

♠

Example 2.5.7. Note the converse of above lemma is not true for UFD in general.

Let $A = k[x, y]$ where k is a field. Consider $Q = \langle x, y^2 \rangle$.

We first claim Q is primary. Note $A/Q = k[x, y]/\langle x, y^2 \rangle \cong k[y]/\langle y^2 \rangle =: R$. Let $a + by \in R$ be a zero divisor, thus there exists $0 \neq a' + b'y \in R$ such that $0 = (a + by)(a' + b'y) = aa' + (ab' + a'b)y$. Thus we have $aa' = 0 \in k$ and $ab' + a'b = 0 \in k$. Hence we have $a = 0$ or $a' = 0$. Proof by cases shows that $a = 0$ in any cases and so every zero divisors of the form by. However, $(by)^2 = b^2 y^2 = 0 \in R$, i.e. all zero-divisor in R are nilpotent and so Q is primary.

We then claim $Q \neq P^n$ where P is prime ideal of A. Suppose $Q = P^n$ for some prime ideal P, then we observe (as an exercise) $\sqrt{Q} = \sqrt{\langle x, y^2 \rangle} = \langle x, y \rangle$. Also, we note (as an exercise) $\sqrt{P^n} = P$. Hence we have $P = \langle x, y \rangle$, i.e. we have

$\langle x, y^2\rangle = \langle x, y\rangle^n$. This is a contradiction as if $n > 1$ then $x \notin \langle x, y^2\rangle \backslash \langle x, y\rangle^n$. If $n = 1$ then $y \in \langle x, y\rangle \backslash \langle x, y^2\rangle$.

Example 2.5.8. Note ourside of UFD, it is not true that power of primes are primary.

Consider the example $A = k[x, y, z]/\langle xy - z^2\rangle$. Let $\overline{x}, \overline{y}, \overline{z}$ be the image of x, y, z in A. Let $P = \langle \overline{x}, \overline{z}\rangle = \langle x, z\rangle/\langle xy - z^2\rangle$. Thus we have

$$A/P = \frac{(k[x, y, z]/\langle xy - z^2\rangle)}{(\langle x, z\rangle/\langle xy - z^2\rangle)} \cong k[x, y, z]/\langle x, z\rangle \cong k[y]$$

Viz, P is prime as $k[y]$ is an integral domain.

We claim P^2 is not primary. Note $\sqrt{P^2} = P$. Next, $-\overline{y} \notin P = \sqrt{P^2}$. Also, $-\overline{x} \not P^2$ as else we have $x \in \langle x, z\rangle^2 + \langle xy - z^2\rangle \subseteq \langle x, y, z\rangle^2$, which is a contradiction. However, we note $(-\overline{y})(-\overline{x}) = \overline{xy} = \overline{z}^2 \in P^2$, this contradicts the definition of primary ideals.

Proposition 2.5.9. *Power of maximal ideals are primary.*

Proof. Let $M \leq A$ be maximal and $n > 0$. We have $\sqrt{M^n} = M$ and we note the nil-radical of A/M^n is M/M^n, which is maximal in A/M^n. This means M/M^n is the only prime ideal in $A/M^n =: R$.

Thus, for $\alpha \in R$, we have $\alpha \in M/M^n$ or α is a unit. If $\alpha \in M/M^n$ then $\alpha^n = 0$ and so α is nilpotent. Hence we have every element in R is either unit or nilpotent. In particular, every zero-divisors are nilpotent and so M^n is primary as desired. ♡

Remark 2.5.10. The proof of above proposition only used that $\sqrt{M^n} = M$ is maximal, i.e. if for $I \leq A$ such that $\sqrt{I}$ is maximal then I is primary.

Definition 2.5.11. Let $P \leq A$ be a prime ideal, $Q \leq A$ is an ideal. We say that Q is ***P-primary*** if it is primary and $\sqrt{Q} = P$.

Lemma 2.5.12 (Lemma 4.3)**.** *If $P \subseteq A$ is prime ideal, $Q_1, ..., Q_n$ are P-primary ideals, then $Q_1 \cap ... \cap Q_n$ is P-primary.*

Proof. Observe $\sqrt{Q_1 \cap ... \cap Q_n} = \bigcap_{i=1}^n \sqrt{Q_i} = \bigcap_{i=1}^n P = P$.

Thus, it suffice to show $Q_1 \cap ... \cap Q_n$ is primary. Suppose $xy \in Q_1 \cap ... \cap Q_n$ and $x \notin Q_1 \cap ... \cap Q_n$. Thus, for some i, we have $xy \in Q_i$ and $x \notin Q_i$. Thus $y \in \sqrt{Q_i} = P = \sqrt{Q_1 \cap ... \cap Q_n}$. The proof follows. ♡

Definition 2.5.13. A ***primary decomposition*** of an ideal $I \leq A$ is an expression of the form $I = Q_1 \cap ... \cap Q_n$ where each Q_i is primary.

We say I is ***decomposable*** if it has a primary decomposition.

Remark 2.5.14. In Noetherian ring, all proper ideals are decomposable.

Also, by Lemma 2.5.12, if $I = Q_1 \cap ... \cap Q_n$ is a primary decomposition and $\sqrt{Q_1} = \sqrt{Q_2}$, then $I = Q_1' \cap Q_3 \cap ... \cap Q_n$ is also a primary decomposition of I where

$Q_1' = Q_1 \cap Q_2$. So, if I is decomposable then it has a primary decomposition where the radicals are distinct.

Also, if $I = Q_1 \cap ... \cap Q_n$ and $Q_1 \supseteq \bigcap_{i=1}^{n} Q_i$ then $I = Q_2 \cap ... \cap Q_n$. Thus, we can find a primary decomposition where no $Q_i \supseteq \bigcap_{j \neq i} Q_j$.

Definition 2.5.15. A primary decomposition $I = Q_1 \cap ... \cap Q_n$ is called ***irredundant primary decomposition(IPD)*** if

1. $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$,
2. $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ for all i.

Remark 2.5.16. Every decomposable ideal has an irredundant primary decomposition.

Lemma 2.5.17 (Lemma 4.4)**.** *Suppose $P \leq A$ is prime, Q is P-primary. Then*

1. *If $x \in A \backslash Q$ then $(Q : x)$ is P-primary.*
2. *If $x \in A \backslash P$ then $(Q : x) = Q$.*

Proof. (1): Note $(Q : x) \subseteq P$ as if $xy \in Q$, since $x \notin Q$, we have $y \in \sqrt{Q} = P$. Also, note $Q \subseteq (Q : x)$. Hence, we get $P = \sqrt{Q} \subseteq \sqrt{(Q : x)} \subseteq \sqrt{P} = P$ and so $\sqrt{(Q : x)} = P$. Hence, it suffice to show $(Q : x)$ is primary now.

Let $yz \in (Q : x)$ with $y \notin (Q : x)$. Then $xyz \in Q$ but $xy \notin Q$. Since Q is primary, we have $z \in \sqrt{Q} = P = \sqrt{(Q : x)}$ and hence $(Q : x)$ is P-primary as desired.

(2): Take arbitrary element $y \in (Q : x)$, this means $xy \in Q$. If $xy \in Q$ and suppose $y \notin Q$ then $x \in \sqrt{Q} = P$, which is a contraction as $x \in A \backslash P$. Thus we must have $y \in (Q : x)$ imply $y \in Q$. Hence $(Q : x) \subseteq Q$ and we note $Q \subseteq (Q : x)$ holds trivially. This establishes the equality. ♡

Theorem 2.5.18 (1st Uniqueness Theorem For Primary Decomposition, Theorem 4.5)**.** *Suppose $I = Q_1 \cap ... \cap Q_n$ is an irredundant primary decomposition (IPD), then n and $\{\sqrt{Q_i} : 1 \leq i \leq n\}$ are independent of the particular irredundant decomposition, i.e. if $I = P_1 \cap ... \cap P_m$ is another IPD, then $m = n$ and $\{\sqrt{Q_i} : 1 \leq i \leq n\} = \{\sqrt{P_i} : 1 \leq i \leq m\}$.*

Proof. Strategy: To prove this, we will show that $\{\sqrt{Q_1}, ..., \sqrt{Q_n}\}$ is exactly the set of ideals in $\{\sqrt{(I : x)} : x \in A, \sqrt{(I : x)} \in Spec(A)\}$ where we recall $(I : x) := \{a \in A : xa \in I\}$ is the saturation.

Suppose $I = Q_1 \cap ... \cap Q_n$ is an IPD. Fix $x \in A$, then

$$\begin{aligned}(I : x) &= (Q_1 \cap ... \cap Q_n : x)\\ &= \bigcap_{i=1}^{n} (Q_i : x)\\ &= \left(\bigcap_{x \in Q_i} (Q_i : x)\right) \cap \left(\bigcap_{x \notin Q_i} (Q_i : x)\right)\\ &= \left(\bigcap_{x \in Q_i} A\right) \cap \left(\bigcap_{x \notin Q_i} (Q_i : x)\right)\\ &= \bigcap_{x \notin Q_i} (Q_i : x)\end{aligned}$$

Hence, let $P_i = \sqrt{Q_i}$ for $1 \leq i \leq n$, observe by Lemma 2.5.17 we have $\sqrt{(Q_i : x)} = P_i$ if $x \notin Q_i$ and so we get

$$\begin{aligned}\sqrt{(I : x)} &= \bigcap_{x \notin Q_i} \sqrt{(Q_i : x)}\\ &= \bigcap_{x \notin Q_i} P_i\end{aligned}$$

Exercise: If a prime ideal P contains a finite intersection of prime ideals $\bigcap_j P_j$ then $P = P_j$ for some j. Thus, if $x \in A$ is such that $\sqrt{(I : x)}$ is prime, then $\sqrt{(I : x)} = P_i$ for some i such that $x \notin Q_i$.

Conversely, fix $j = 1, ..., n$. Since $Q_j \not\supseteq \bigcap_{i \neq j} Q_i$, there is an $x \in \bigcap_{i \neq j} Q_j \backslash Q_j$. So $\sqrt{(I : x)} = \bigcap_{x \notin Q_i} P_i = P_j$.

Therefore, $\{P_1, ..., P_n\} = \{\sqrt{(I : x)} : x \in A, \sqrt{(I : x)} \in Spec(A)\}$ and this proves the uniqueness theorem. ♡

Definition 2.5.19. If I is decomposable and $I = Q_1 \cap ... \cap Q_n$ is an IPD Then the prime ideals $\sqrt{Q_1}, ..., \sqrt{Q_n}$ are called the ***prime ideals associated to*** I. This is denoted by $Assoc(I) = \{P_1, ..., P_n\}$.

Example 2.5.20. Consider $A = k[x, y]$ and $I = \langle x^2, xy \rangle$.

Then, we claim $I = \langle x \rangle \cap \langle x^2, y \rangle$. Indeed, $I \subseteq \langle x \rangle \cap \langle x^2, y \rangle$ should be clear. On the other hand, let $f \in \langle x \rangle \cap \langle x^2, y \rangle$ then $f = gx = h_1 x^2 + h_2 y$. Hence $x \mid h_2 y$ and since x, y are coprime, we have $x \mid h_2$. Thus $f = h_1 x^2 + h_3 xy$ for some h_3 with $h_2 = xh_3$. Thus $f \in I$ as desired.

Next, observe $\langle x \rangle$ is prime, hence primary. We have already seen that $\langle x^2, y \rangle$ is primary by Example 2.5.7(we see this is isomorphic to $\langle x, y^2 \rangle$).

Hence, $Q = \langle x \rangle \cap \langle x^2, y \rangle$ is an IPD of I.

Claim: $I = \langle x \rangle \cap \langle x, y \rangle^2$. Indeed, $I \subseteq \langle x \rangle \cap \langle x, y \rangle^2$ is clear. Conversely, take $f \in \langle x \rangle \cap \langle x, y \rangle^2$, then $f \in \langle x, y \rangle^2$ means every monomial of f is divisible by x^2, y^2 or xy. Since $f \in \langle x \rangle$, we have every monomial is divisible by x. Suppose a monomial m of f is divisible by y^2, then as it is divisible by x, we have $x \mid m$ and so $xy^2 \mid m \Rightarrow xy \mid m$. Thus, we have every monomial is divisible by x^2 or xy. Thus $f \in I$.

Since $\langle x, y \rangle$ is a maximal ideal, we have $\langle x, y \rangle^2$ is primary by Proposition 2.5.9. Thus, $P = \langle x \rangle \cap \langle x, y \rangle^2$ is another IPD.

The associated primes, using Q or P are $\langle x \rangle$ and $\langle x, y \rangle$. Hence, we can have containment within associated primes.

Definition 2.5.21. Let I be decomposable with associated prime ideals $P_1, ..., P_n$. The minimal elements of $\{P_1, ..., P_n\}$ are called the ***minimal associated primes*** of I.

Example 2.5.22. In example 2.5.20, we only have one minimal associated prime for $I = \langle x^2, xy \rangle$, namely $\langle x \rangle$.

Proposition 2.5.23 (Prop 4.6)**.** *Let I be decomposable. Then the minimal associated primes of I are precisely the minimal elements of the set $V(I) = \{P \in Spec(A) : P \supseteq I\}$.*

Proof. Let $Assoc(I) = \{P_1, ..., P_n\}$.

Claim: $P \in V(I)$ then $P \supseteq P_i$ for some $1 \leq i \leq n$. Indeed, we have $I = Q_1 \cap ... \cap Q_n$ with $\sqrt{Q_i} = P_i$. So $P \supseteq I = Q_1 \cap ... \cap Q_n$. So, we have $P = \sqrt{P} \supseteq \sqrt{I} = P_1 \cap ... \cap P_n$ and hence $P \supseteq P_i$ for some i.

Thus, suppose P_j is minimal in the list $Assoc(I)$. If there is a prime $I \subseteq P \subseteq P_j$. Then, by the claim, there exists $P_i \subseteq P$, i.e. $P_i \subseteq P \subseteq P_j$. By minimality, we have $P_i = P_j = P$ and so P_j is minimal in $V(I)$ as desired.

Conversely, suppose P is minimal in $V(I)$. By the claim, $P \supseteq P_i$ for some i. Minimality of P forces $P = P_i$, hence $P \in Assoc(I)$ and hence P is minimal in $Assoc(I)$. ♡

Corollary 2.5.23.1. *If I is decomposable then $V(I)$ has only finitely many minimal elements.*

Proof. Immediately. ♡

Corollary 2.5.23.2. *If I is decomposable then $\sqrt{I}$ is the intersection of the minimal associated primes of I.*

Proof. We know that $\sqrt{I} = \bigcap_{P \in V(I)} P$, which by Proposition 2.5.23 we have this intersection is the same as intersection of minimal elements of $V(I)$. ♡

Corollary 2.5.23.3. *If I is decomposable, then $\sqrt{I}$ has unique independent **prime** decomposition, i.e. $\sqrt{I} = P_1 \cap ... \cap P_n$ where $P_1, ..., P_n$ are prime ideals with $P_i \not\supseteq \bigcap_{j \neq i} P_j$ and this is unique upto ordering of $P_1, ..., P_n$.*

Proof. Say $I = Q_1 \cap ... \cap Q_n$ be IPD, let $P_i = \sqrt{Q_i}$. Order them so that $P_1, ..., P_l$ are the minimal for $l \leq n$.

Then $\sqrt{I} = P_1 \cap ... \cap P_n = P_1 \cap ... \cap P_l$. If $P_i \supseteq \bigcap_{j \neq i} P_j$ then $P_i \supseteq P_j$ for some $j \neq i$. This is a contradiction to the minimality of P_i in $\{P_1, ..., P_n\}$.

Uniqueness: Suppose $\sqrt{I} = P'_1 \cap ... \cap P'_{l'}$ be another irredundant prime decomposition of $\sqrt{I}$. Note that $P'_1 \cap ... \cap P'_{l'}$ and $P_1 \cap ... \cap P_l$ are also irreducible primary decomposition of $\sqrt{I}$. Thus, by Proposition 2.5.18 we have $l = l'$ and those set agrees. Hence we indeed have uniqueness as desired. ♡

Remark 2.5.24 (Geometric Interpretation)**.** A closed set is ***irreducible*** if it cannot be written as a union of two proper closed subsets. Let I be decomposable ideal in A with $\sqrt{I} = P_1 \cap ... \cap P_l$ be irredundant prime decomposition. Then, we observe $V(I) = V(\sqrt{I})$ trivially, then we have $V(\sqrt{I}) = V(P_1 \cap ... \cap P_l) = V(P_1) \cup ... \cup V(P_l)$. Hence, irredundant means $V(P_i) \not\subseteq \bigcup_{j=i} V(P_j)$. The fact that P_i are primes, we have $V(P_i)$ is irreducible.

Thus, we have shown $V(I)$ can be written uniquely as an irredundant finite union of irreducible closed sets. Those are called ***irreducible components of*** $V(I)$.

Proposition 2.5.25. *[Prop 4.7] If $\langle 0 \rangle$ is decomposable then the set of zero divisors D of A is the union of associated prime ideals of $\langle 0 \rangle$.*

Proof. Suppose $\langle 0 \rangle = Q_1 \cap ... \cap Q_n$ is an IPD with each Q_i is P_i-primary. Fix $x \neq 0$ in A, then

$$Ann(x) = (0 : x) \subseteq \sqrt{(0 : x)} = \bigcap_{i=1}^{n} \sqrt{(Q_i : x)}$$

If $x \notin Q_i$, then $(Q_i : x)$ is P_i-primary. If $x \in Q_i$ then $(Q_i : x) = A$. Hence

$$\bigcap_{i=1}^{n} \sqrt{(Q_i : x)} = \bigcap_{1 \leq i \leq n, x \notin Q_i} P_i$$

and as $x \notin \langle 0 \rangle = Q_1 \cap ... \cap Q_n$. Thus, there is $1 \leq i \leq n$ such that $x \notin Q_i$. Hence, for some i, we have $Ann(x) \subseteq P_i$ and so $D = \bigcup_{x \neq 0} Ann(x) \subseteq P_1 \cup ... \cup P_n$.

Conversely, fix D_i. Then by the proof of Theorem 2.5.18, we have $D_i = \sqrt{(0 : x)}$ for some $x \in A$. Since $P_i \neq A$ and so $x \neq 0$. Note $\sqrt{(0 : x)} \subseteq D$. ♡

2.6 Noetherian

Definition 2.6.1. A ***Noetherian ring*** is a ring where every ascending chain of ideals $I_1 \subseteq I_2 \subseteq \ldots$ is ***stationary***, i.e. there exists $n > 0$ so that $I_n = I_{n+1} = I_{n+2} = \ldots$.

Remark 2.6.2. Hence, any non-empty set of ideals of a Noetherian ring has a maximal element (by Zorn's lemma).

Definition 2.6.3. An ideal I is ***irreducible*** whenever $I = J_1 \cap J_2$ then $I = J_1$ or $I = J_2$.

Lemma 2.6.4 (Lemma 7.11)**.** *In a Noetherian ring, every ideal is an intersection of finitely many irreducible ideals.*

Proof. Suppose A is Noetherian. Let $\mathscr{S}$ be the set of ideals such that they are not finite intersection of irreducible ideals.

Assume $\mathscr{S}$ is not empty and seek a contradiction. By Noetherianity, let $I \in \mathscr{S}$ be maximal, we have I itself is not irreducible. Thus $I = J_1 \cap J_2$ for some ideals such that $J_1 \supsetneq I$ and $J_2 \supsetneq I$. Thus J_1, J_2 are not in $\mathscr{S}$ by maximality of I. Therefore, $J_1 = I_1 \cap \ldots \cap I_l$ and $J_2 = I_1' \cap \ldots \cap I_{l'}'$ where I_j and I_k' are irreducible ideals.

Hence $I = I_1 \cap \ldots \cap I_l \cap I_1' \ldots \cap I_{l'}'$ and so $I \notin \mathscr{S}$. This is a contradiction and proof follows. ♡

Lemma 2.6.5 (Lemma 7.12)**.** *In a Noetherian ring, irreducible ideals are primary.*

Proof. Suppose $I \subseteq A$ is an ideal. Note (by definition and correspondence theorem)

1. A/I is Noetherian.
2. I is primary if and only if $\langle 0 \rangle$ s primary in A/I.
3. I is irreducible if and only if $\langle 0 \rangle$ is irreducible in A/I.

Therefore, it suffice to prove that if A is Noetherian and $\langle 0 \rangle$ is irreducible then $\langle 0 \rangle$ is primary.

Suppose $xy = 0$ and $y \neq 0$. We want $x^n = 0$ for some n.

COnsider $Ann(x) \subseteq Ann(x^2) \subseteq Ann(x^3) \subseteq \ldots$. Hence, by Noetherianity there is $n > 0$ such that $Ann(x^n) = Ann(x^{n+1}) = \ldots$. We will show $x^n = 0$.

CLaim: $\langle x^n \rangle \cap \langle y \rangle = \langle 0 \rangle$. Indeed, take $a \in \langle x^n \rangle \cap \langle y \rangle$ imply $a = cy$ for some $c \in A$ and so $ax = cyx = 0$. Also, $a = bx^n$ for some $b \in A$ and so $0 = ax = bx^{n+1}$. Thus $b \in Ann(x^{n+1}) = Ann(x^n)$. Thus $a = 0$.

Since $\langle 0 \rangle$ is irreducible and $\langle 0 \rangle \neq \langle y \rangle$ and $\langle 0 \rangle = \langle y \rangle \cap \langle x^n \rangle$ we must have $\langle 0 \rangle = \langle x^n \rangle$. Hence $x^n = 0$. ♡

Corollary 2.6.5.1. *If A is Noetherian, every ideal is decomposable. Hence,*

1. *Every radical ideal has a unique irredundant prime decomposition.*
2. *Every Zariski closed set in $Spec(A)$ can be written uniquely as an irredundant union of finitely many irreducible closed subsets, called irreducible components.*
3. *Zero divisors of A is the union of the prime ideals associated to $\langle 0 \rangle$.*

Proposition 2.6.6. *A is Noetherian if and only if every ideal is finitely generated.*

Proof. ($\Leftarrow$): Given $I_1 \subseteq I_2 \subseteq \ldots$, let $I = \bigcup_{i>0} I_i$, this is an ideal of A because we have a chain of containment. By assumption $I = \langle a_1, \ldots, a_l \rangle$ for $a_1, \ldots, a_l \in A$. Thus, $a_1, \ldots, a_l \in A_n$ for some $n > 0$. Hence $I = \langle a_1, \ldots, a_l \rangle \subseteq I_n$ and $I_n \subseteq I$. This imply $I_n = I_{n+1} = I_{n+2} = \ldots$.

($\Rightarrow$): Suppose I is an ideal that is not finitely generated. Choose $a_0 \in I, a_1 \in I \backslash \langle a_0 \rangle$ and inductively $I_n = I \backslash \langle a_0, \ldots, a_{n-1} \rangle$. Then we get an ascending chain of proper containment, which imply A is not Noetherian. ♡

Definition 2.6.7. An A-module M is ***Noetherian*** if there is no strictly increasing chain of A-submodules in M.

Remark 2.6.8. M is Noetherian module if and only if every submodule is finitely generated. Also, we note A is a Noetherian ring if and only if A is a Noetherian A-module.

Remark 2.6.9. It is not true that for every A-algebra B, B is a Noetherian ring if and only if B is a Noetherian A-module.

Example 2.6.10.

1. All PID's are Noetherian.
2. Noetherianity is closed under localization. Say A is Noetherian, $S \subseteq A$ is multiplicatively closed, then $S^{-1}A$ is Noetherian. Indeed, let $J \in S^{-1}A$ be an ideal, then $J = IS^{-1}A$ for some ideal $I \leq A$. Thus if $I = \langle f_1, \ldots, f_r \rangle$ then $J = \langle \frac{f_1}{1}, \ldots, \frac{f_r}{1} \rangle$.
3. Noetherianity is closed under taking quotient. This is by Correspondence theorem.

Example 2.6.11. Subring of Noetherian rings need **not** to be Noetherian. Consider A be an integral domain, then $A \subseteq F := Frac(A)$. However, not all integral domains are Noetherian, e.g. $\mathbb{Q}[x_1, x_2, x_3, \ldots]$ is not Noetherian.

Lemma 2.6.12. *Consider*

$$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

be an short exact sequence of A-modules, then M is Noetherian if and only if M' and M'' are Noetherian.

Proof. ($\Rightarrow$): Easy.

($\Leftarrow$): Suppose M' and M'' are Noetherian. Consider $L_1 \subseteq L_2 \subseteq \ldots \subseteq M$ be an ascending sequence of submodules. Let n be large enough so that $f^{-1}(L_n) =$

$f^{-1}(L_{n+1}) = ...$ and $g(L_n) = g(L_{n+1}) = ...$ Thus, let $a \in L_{n+1}$, then

$$\begin{aligned} & g(a) \in g(L_{n+1}) = g(L_n) \\ \Rightarrow\ & g(a) = g(b), b \in L_n \\ \Rightarrow\ & a - b \in Ker(g) = Im(f) \\ \Rightarrow\ & a - b = f(c), c \in M' \\ \Rightarrow\ & c \in f^{-1}(L_{n+1}) = f^{-1}(L_n) \\ \Rightarrow\ & a - b = f(c) \in L_n \\ \Rightarrow\ & a \in L_n \end{aligned}$$

Thus $L_{n+1} \subseteq L_n$ and so $L_{n+1} = L_n$ as desired. ♡

Corollary 2.6.12.1. *A is Noetherian then A^n is Noetherian as A-modules.*

Proof. We use induction on n. If $n = 1$ then we are done. Suppose it holds for $n-1$.

Then, observe

$$0 \longrightarrow A^{n-1} \xrightarrow{\iota} A^n \xrightarrow{\pi} A^{n-1} \longrightarrow 0$$

where $\iota(a_1, ..., a_{n-1}) = (a_1, ..., a_{n-1}, 0)$ and $\pi(a_1, ..., a_n) = (a_1, ..., a_{n-1})$. This sequence is exact and we are done. ♡

Corollary 2.6.12.2. *A is Noetherian ring imply every finitely generated A-module is Noetherian.*

Proof. Since M is f.g. A-module, we have $M \cong A^n/N$ for $N \leq A^n$ a submodule. Thus

$$0 \longrightarrow N \longrightarrow A^n \longrightarrow A^n/M \longrightarrow 0$$

is exact by inclusion and quotient projection. ♡

Corollary 2.6.12.3. *A is Noetherian ring, fix $r \geq 0$. Let $M_r := \{f \in A[x] : deg(f) \leq r \text{ or } f = 0\}$. Then M_r is a Noetherian A-module.*

Proof. Note M_r is an A-submodule generated by $\{1, x, x^2, ..., x^r\}$. ♡

Remark 2.6.13. Note $M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3....$ Thus $A[x]$ is **not** Noetherian as A-module.

Theorem 2.6.14 (Hilbert's Basis Theorem)**.** *If A is a Noetherian, then $A[x]$ is Noetherian.*

Proof. Let $I \leq A[x]$, let $J = \{l.c.(f) : f \in I\} \cup \{0\} \subseteq A$ where $l.c.(f)$ means the leading coefficient of f.

Claim: J is an ideal. Take $a \in J$ with $l.c.(f) = a$ and $c \in A$ be arbitrary. Then $ca = c(l.c.(f)) = l.c.(ca)$ and so $ca \in J$. Next, take $a, b \in J$ with $a = l.c.(f)$ and $b =$

$l.c.(g)$ where $f, g \in I$. If $a = 0$ or $b = 0$ then it is closed under addition. Thus assume both a, b are non-zero. Thus, let $m = deg(f)$ and $n = deg(g)$ with $m \leq n$. Then, we have $deg(x^{n-m}f) = n = deg(g)$. Hence $l.c.(x^{n-m}f + g) = l.c.(x^{n-m}f) + l.c.(g) = a + b$ and so it is closed under addition. Hence J is an ideal as desired.

Thus, since A is Noetherian, we have $J = \langle a_1, ..., a_l \rangle$. For each $i = 1, ..., l$, let $f_i \in I$ be such that $l.c.(f_i) = a_i$. We may assume $a_i \neq 0$ and $f_i \neq 0$.

Let $I_i' = \langle f_1, ..., f_l \rangle \subseteq I$. Let $r_i = deg(f_i)$ for $1 \leq i \leq l$ and let $r = \max\{r_1, ..., r_l\}$.

Claim: If $f \in I$ then there are $g, h \in A[x]$ such that $f = g + h$, $deg(g) < r$ or $g = 0$ and $h \in I'$.

We will use induction on the degree of f. We may assume f is not 0. If $deg(f) < r$, then set $g = f$ and $h = 0$ and we are done the base case. Thus, we may assume $deg(f) := m \geq r$ and assume it holds for degree less than or equal to $m - 1$.

Let $a = l.c.(f) \in J$, then $a = \sum_{i=1}^{l} u_i a_i$ where $u_i \in A$. Then, consider

$$h := \sum_{i=1}^{l} u_i x^{m-r_i} f_i$$

and we will have $h \in I'$ and $deg(h) = m = deg(f)$ with $l.c.(h) = l.c.(f)$ as we observe $l.c.(u_i x^{m-r_i} f_i) = u_i a_i$ so $l.c.(h) = \sum_{i=1}^{l} u_i a_i = a$. Thus $f - h$ has degree at most $m - 1$. Hence, we can keep doing this until the term x^{m-r_i} does not make sense, i.e. by induction hypothesis we would have $f - h = g + h'$ where $h' \in I'$ and $g = 0$ or $deg(g) < r$. Thus we have $f = g + (h + h')$ where $h + h' \in I'$ and $deg(g) < r$ or 0. This proves the claim.

Hence we have I is finitely generated because we observe every elements of I can be written as $g + h$ where $g \in M_{r-1}$ and $g \in I$, which is finitely generated because M_{r-1} is finitely generated as A-modules. On the other hand, I' is finitely generated as ring by $f_1, ..., f_l$ and so I is finitely generated. ♡

Corollary 2.6.14.1. *Let A be Noetherian, every f.g. A-algebra is Noetherian.*

Proof. Let $b_1, ..., b_l \in B$ generate B as an A-algebra. Consider the A-linear homomorphism $\phi : A[x_1, ..., x_n] \to B$ given by $x_i \mapsto b_i$. This is surjective and we have $A[x_1, ..., x_n]/Ker(\phi) \cong B$ as A-algebra. Observe $A[x_1, ..., x_n]$ is Noetherian by apply Hilbert's basis theorem n times and hence B is Noetherian. ♡

Example 2.6.15. By above theorems,

1. Every f.g. ring is Noetherian. E.g. every PID is Noetherian.
2. Every f.g. k-algebra where k is a field is Noetherian.

Proposition 2.6.16 (Prop 7.14)**.** *Let A be Noetherian, $I \leq A$ be an ideal. Then $(\sqrt{I})^n \subseteq I$ for some $n > 0$.*

Proof. By Noetherianity, I is finitely generated, say $\sqrt{I} = \langle a_1, ..., a_r \rangle$. For each i, let $n_i > 0$ be such that $a_i^{n_i} \in I$.

Then observe $(\sqrt{I})^m = \langle \{\prod_{i=1}^r a_i^{p_i} : p_1 + ... + p_r = m\} \rangle$. Choose m large enough so that $p_1 + ... + p_r = m$ imply there exists some i so $p_i \geq n_i$, e.g. $m = r \cdot \max\{n_1, ..., n_r\}$.

For such m, if $p_1 + ... + p_r = m$, then $\prod_{i=1}^r a_i^{p_i} \in I$ and so $(\sqrt{I})^m \subseteq I$. ♡

Corollary 2.6.16.1. *Let A be Noetherian, then its nilradical is nilpotent.*

Proof. Apply 7.14 with $I = \langle 0 \rangle$. Recall an ideal is nilpotent means $I^m = \langle 0 \rangle$ for some $m > 0$. ♡

Corollary 2.6.16.2. *Let A be Noetherian. Let $\mathfrak{m} \leq A$ be a maximal ideal and $Q \leq A$ is an ideal. Then the following are equivalent:*

1. $\sqrt{Q} = \mathfrak{m}$.
2. Q *is* $\mathfrak{m}$*-primary.*
3. $\mathfrak{m}^n \subseteq Q \subseteq \mathfrak{m}$ *for some* n.

Proof. (1) $\Rightarrow$ (2) is immediate by the proof of Proposition 2.5.9 (check the remark after that proposition).

(2) $\Rightarrow$ (3): We know $\mathfrak{m} = \sqrt{Q}$ then apply Proposition 2.6.16.

(3) $\Rightarrow$ (1): Note since $\mathfrak{m}^n \subseteq \mathbb{Q} \subseteq \mathfrak{m}$ then we have $\sqrt{\mathfrak{m}^n} \subseteq \sqrt{Q} \subseteq \sqrt{\mathfrak{m}}$. However, $\sqrt{\mathfrak{m}^n} = \mathfrak{m} = \sqrt{\mathfrak{m}}$ and hence $\sqrt{Q} = \mathfrak{m}$ as desired. ♡

Proposition 2.6.17. *Let A be Noetherian. Let $P \in Spec(A)$, then P is an associated prime ideals of $\langle 0 \rangle$ if and only if $P = Ann(x)$ for some $x \in A$.*

Proof. Consider $\langle 0 \rangle = Q_1 \cap ... \cap Q_l$ to be an IPD. Let $P_i = \sqrt{Q_i}$, so that Q_i is P_i-primary. So $P_1, ..., P_l$ are the associated prime ideals of $\langle 0 \rangle$.

Fix i, by Proposition 2.6.16, we have $P_i^m \subseteq Q_i$. Then, we have

$$(\bigcap_{j \neq i} Q_j) P_i^m \subseteq \bigcap_j Q_j = \langle 0 \rangle$$

Let $m > 0$ be minimal such that $(\bigcap_{j \neq i} Q_j) P_i^m = \langle 0 \rangle$. Let $x \neq 0$ be so that $x \in (\bigcap_{j \neq i} Q_j) P_i^{m-1} \neq \langle 0 \rangle$, we will show $P_i = Ann(x)$.

Let $a \in P_i$, then

$$ax \in a \left((\bigcap_{j \neq i} Q_j) P_i^m \right) \subseteq (\bigcap_{j \neq i} Q_j) P_i^m = \langle 0 \rangle$$

Hence $a \in Ann(x)$ and so $P_i \subseteq Ann(x)$.

On the other hand, $\langle 0\rangle = \bigcap_j Q_j$. Observe

$$Ann(x) = (0 : x) = \bigcap (Q_j : x) = (Q_i : x)$$

where the last step is because for $i \neq j$, we have $x \in Q_j$ and so $(Q_j : x) = A$, i.e. it contributes nothing to the intersection if $i \neq j$.

However, $x \notin Q_i$, else $x \in \bigcap_j Q_j = \langle 0\rangle$, which contradicts $x \neq 0$. So, by Proposition 2.5.17, we have $(Q_i : x)$ is P_i-primary and hence $\sqrt{(Q_i : x)} = P_i$ and hence $(Q_i : x) \subseteq P_i$. Hence $Ann(x) \subseteq P_i$ and this gives us $P_i = Ann(x)$.

Conversely, suppose $x \in A$ such that $Ann(x) = P$ is prime. Then $P = \sqrt{P} = \sqrt{ann(x)} = \sqrt{(0 : x)}$. By Theorem 2.5.18, $P = P_i$ for some i as desired. ♡

Corollary 2.6.17.1 (Cor 7.17)**.** *Let A be Noetherian. Let I be proper ideal. The associated prime ideals of I are precisely the prime ideals of the form $(I : x)$ for some $x \in A$.*

Proof. Consider $\pi : A \to A/I$, note A/I is Noetherian. For $a \in A$, then one can check that $\pi^{-1}(Ann(\pi(x))) = (I : x)$ and so by Correspondence theorem we have $(I : x)$ is prime if and only if $ann(\pi(x))$ is prime. Therefore, P is associated prime to I if and only if $\pi(P)$ is associated prime to $\langle 0\rangle$. Now apply Proposition 2.6.17. ♡

Example 2.6.18. Show[2] that if R is Noetherian, then it is impossible for R to have only three prime ideals such that $P \subsetneq Q \subsetneq T$, i.e. we cannot have $Spec(R)$ have only three elements and they are in proper containment relation.

Solution. We claim the following:

Let R be Noetherian and $P \subsetneq Q \subsetneq T$ is a chain of distinct prime ideals in R. Then there are infinitely many primes I such that $P \subsetneq I \subsetneq T$.

Indeed, consider the quotient ring R/P and then localize R/P at T/P, which is a prime ideal in R/P, denote this by $\overline{R}_T$. We let $S = R/P - T/P$, then $\overline{R}_T = S^{-1}(R/P)$. This is a Noetherian local ring and integral domain and in particular, it has dimension 2 (a maximal chain will be $0 \subsetneq S^{-1}(Q/P) \subsetneq S^{-1}(T/P)$). We remark that any primes between P and T would have height 1 in $\overline{R}_T$ and if it is a prime with height 1 in $\overline{R}_T$ then we can recover a prime between P and T.

Suppose we only have finitely many height 1 primes in $\overline{R}_T$, then note $S^{-1}(T/P)$ is not contained in any one of those primes. Hence $S^{-1}(T/P)$ is not contained in their unions and so there exists $x \in T$ such that is not in any of the height 1 primes. Thus take the image of x in $\overline{R}_T$, say $\overline{x}$, we have a principal ideal $\langle \overline{x}\rangle$ with height not equal 1, a contradiction.

This finishes the proof of claim and we note this immediately imply if we have $P \subsetneq Q \subsetneq T$ then we have infinitely many primes, i.e. contradicts the condition we only have three primes. ♠

[2] Look up definition of dimension, height and Krull's principal ideal theorem

2.7 Integral Dependence and Valuation

Remark 2.7.1. Just recall that say $\phi : A \to B$ is an A-algebra and let $f \in A[x]$, we define $f^{\phi}(x)$ to be the polynomial in B such that we just apply ϕ to each coefficient of $f(x)$. From time to time, for $b \in B$ and $f \in A[x]$, we may just write $f(b)$ to mean $f^{\phi}(b)$.

Definition 2.7.2. Let $\phi : A \to B$ be an A-algebra and $b \in B$. We say b is ***integral*** over A if there is a monic polynomial $f \in A[x]$ such that $f^{\phi}(b) = 0$.

Remark 2.7.3. If A is a field, then b is integral over A if and only if b is algebric over a.

Example 2.7.4. Let $\frac{1}{2} \in \mathbb{Q}$ be an $\mathbb{Z}$-algebra. Then it is easy to see the smallest polynomial vanishes $\frac{1}{2}$ is $f(x) = 2x - 1$. Thus, $\frac{1}{2}$ is not integral over $\mathbb{Z}$ because we cannot find monic polynomial that vanishes $\frac{1}{2}$.

Proposition 2.7.5. *Let $q \in \mathbb{Q}$ be integral over $\mathbb{Z}$ if and only if $q \in \mathbb{Z}$.*

Proof. Say $q = \frac{r}{s}$ where $r, s \in \mathbb{Z}$, $s \neq 0$ and $gcd(r, s) = 1$. If q were integral over $\mathbb{Z}$ then

$$(\frac{r}{s})^2 + a_{n-1}(\frac{r}{s})^{n-1} + ... + a_0 = 0$$

where $a_{n-1}, ..., a_0$ are all in $\mathbb{Z}$. clearly the denominator, i.e. multiply by s^n, we get

$$r^n + \underbrace{a_{n-1}sr^{n-1} + ... + a_1 s^{n-1} r + a_0 s^n}_{\text{dividible by } s} = 0$$

Thus, we have s must divide r^n, i.e. $s = 1$ as r and s are coprime. Hence $q \in \mathbb{Z}$.

Conversely, if $q \in \mathbb{Z}$ then $x - q$ would vanish q, i.e. q is integral over $\mathbb{Z}$. ♡

Remark 2.7.6. In the textbook, we define integral with the assumption A is a subring of B. However, we defined integral for general A-algebras. In our definition, it can be shown that $b \in B$ is integral over A if and only if b is integral over $f(A) \subseteq B$, which is a subring of B.

This justify why textbook assumes A is subring of B.

Proposition 2.7.7 (Prop 5.1)**.** *Let $\phi : A \to B$ be an A-algebra and $b \in B$, then the following are equivalent:*

1. *b is integral over A.*
2. *$A[b] := \{f^{\phi}(b) : f(x) \in A[x]\}$, which is the A-subalgebra of B generated by b, is a finite A-algebra.*
3. *There is a fintie A-subalgebra $C \subseteq B$ such that $b \in C$.*

Proof. (1) $\Rightarrow$ (2): Suppose b is integral over A, which means $b^n + ... + a_1 b + a_0 = 0$ for some $n > 0$ and $a_0, ..., a_{n-1} \in A$. Let M be the A-submodule of B generated by $1, b, ..., b^{n-1}$. We show $M = A[b]$. Observe $M \subseteq A[b]$ trivially.

Conversely, note $A[b]$ is generated as A-submodule by $1, b, b^2, ...$, thus it suffice to show that $b^m \in M$ for all $m \geq 0$. If $m < n$ then we are done. Suppose it holds for $m \geq n$ and $b^k \in M$ for all $k < m$, we will show $b^m \in M$.

Note

$$\begin{aligned} b^m &= b^{m-n}b^n = b^{m-n}(-a_{n-1}b^{n-1} - ... - a_1 b - a_0) \\ &= -a_{n-1}b^{m-1} - a_{n-2}b^{m-2} - ... - a_0 b^{m-n} \end{aligned}$$

where each of $b^{m-1}, ..., b^{m-n}$ are in M by induction hypothesis and so $b^m \in M$ as desired.

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

(3) $\Rightarrow$ (1): We use Cayley-Hamilton for Modules, i.e. Proposition 1.2.5, let C be as in (3), let $\phi : C \to C$ given by $x \mapsto bx$. This is A-linear endomorphism on a finitely generated A-module. Hence, by Proposition 1.2.5, there is $n > 0$ and $a_0, ..., a_{n-1} \in A$ such that in the ring $End_A(C)$ we have

$$\phi^n + a_{n-1}\phi^{n-1} + ... + a_1\phi + a_0 = 0$$

Evaluate both side at $1 \in C$, we get

$$b^n + a_{n-1}b^{n-1} + ... + a_1 b + a_0 = 0$$

This establishes (1). ♡

Corollary 2.7.7.1 (Corollary 5.2). *Let $\phi : A \to B$ be an A-algebra. Let $b_1, ..., b_l \in B$ be integral over A. Then $A[b_1, ..., b_l]$ is a fintie A-subalgebra.*

Proof. We use induction on l. If $l = 1$, then Proposition 2.7.7's (1) $\Rightarrow$ (2) establishes the base case.

Suppose $l > 1$ and suppose it holds for all value less than l. Then, observe

$$A \xrightarrow{\subseteq} A[b_1, ..., b_{l-1}] \xrightarrow{\subseteq} B$$

is a chain of ring homomorphisms. Then, since b_l is integral over A, we have b_l is integral over $A[b_1, ..., b_{l-1}]$. Now apply (1) $\Rightarrow$ (2) of Proposition 2.7.7 to the algebra $A[b_1, ..., b_{l-1}] \to B$, we get $A[b_1, ..., b_{l-1}][b_l]$ is finitely generated as an $A[b_1, ..., b_{l-1}]$ modules. However, observe $A[b_1, ..., b_{l-1}]$ is finitely generated as A modules, hence we get $A[b_1, ..., b_l]$ is finitely generated as A-module as well. The proof follows. ♡

Definition 2.7.8. Let $\phi : A \to B$ be an A-algebra, then B is ***integral over*** A if every element of B is integral over A.

Remark 2.7.9. Integrality explains the gap between f.g. algebra and fintie algebra. Viz, B is an A-algebra, then B is finite A algebra if and only if B is a finitely generated A-algebra that is integral over A.

Proposition 2.7.10. *Let B be an A-algebra, then B is finite A-algebra if and only if B is finitely generated A-algebra that is integral over A.*

Proof. ($\Rightarrow$): By Proposition 2.7.7's (3) $\Rightarrow$ (1), we see that every b is integral over A.

($\Leftarrow$): Assume B is finitely generated and integral over A. Let $b_1, ..., b_l$ generates B as A-algebra. Then $B = A[b_1, ..., b_l]$ and since $b_1, ..., b_l$ are integral over A, by Proposition 2.7.7.1 we have $A[b_1, ..., b_l]$ is a finite A-algebra. ♡

Definition 2.7.11. An A-algebra $f : A \to B$ is ***integral*** if every element of B is integral over A.

Proposition 2.7.12. *B is an integral A-algebra and C is an integral B-algebra, then C is an integral A-algebra via* $A \xrightarrow{f} B \xrightarrow{g} C$.

Proof. Let $c \in C$, let $q(x) \in B[x]$ monic such that $q(c) = 0$. This exists as C is integral over B. Therefore, $q(x) = x^n + b_{n_1}x^{n-1} + ... + b_1x + b_0$. Hence c is integral over $A[b_0, ..., b_{n-1}] \subseteq B$. Hence $A[b_0, ..., b_{n-1}][c]$ is a finite $A[b_0, ..., b_{n-1}]$-algebra. By Corollary 2.7.7.1, we have $A[b_0, ..., b_{n-1}]$ is a finite A-algebra and thus $A[b_0, ..., b_{n-1}]$ is a finite A-subalgebra of C, i.e. c is integral over A by Proposition 2.7.7. ♡

Corollary 2.7.12.1. *Let $f : A \to B$ be an A-algebra, define $C = \{b \in B : b \text{ is integral over } A\}$. Then C is an A-subalgebra of B.*

Proof. Suppose $b_1, b_2 \in B$ are integral over A and $a \in A$. We have $b_1b_2, b_1 + b_2, ab_1 \in A[b_1, b_2]$ but $A[b_1, b_2]$ is a finite A-algebra. Hence, all those elements are integral over A. ♡

Definition 2.7.13. Let B be A-algebra, then $C = \{b \in B : b \text{ is integral over } A\}$ is called the ***integral closure*** of A in B.

Definition 2.7.14. Let $A \subseteq B$ a ring extension, we say A is ***integrally closed*** in B if A is equal the integral closure of A in B.

Lemma 2.7.15. *Let B be an A-algebra, C be the integral closure of A in B. Then C is integrally closed in B.*

Proof. Let $b \in B$, b is integral over $C \subseteq B$. We want to show $b \in C$.

Since b is integral, $C[b] \subseteq B$ is a finite C-algebra. Thus $C[b]$ is integral over C but C is integral over A. Therefore, $C[b]$ is integral over A and hence b is integral over A, i.e. $b \in C$ by definition. ♡

Example 2.7.16. $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. Note $\mathbb{Z}$ is an example of an ***integrally closed domain*** which is defined as an integral domain A which is integrally closed in $Frac(A)$.

Proposition 2.7.17. *Let B be an integral A-algebra,*

1. *Preservation by quotients: Let $J \subseteq B$ be an ideal then B/J is an integral $A/(J \cap A)$-algebra (recall $f : A \to B$ is the A-algebra then $J \cap A = f^{-1}(A)$)*
2. *Preservation by localization: Let $S \subseteq A$ be multiplicatively closed set, then $S^{-1}B$ is integral $S^{-1}A$-algebra.*

Proof.

(1): For $a \in A$ let $\overline{a}$ denote its image in $A/J \cap A$. Let $b \in B$, let $\bar{b}$ denote the image in B/J. Since b is integral over A we have $b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$ for some $n > 0$, $a_0, ..., a_{n-1} \in A$. Take the image of both sides in B/J to get

$$\overline{b}^n + \overline{a_{n-1}}\overline{b}^{n-1} + ... + \overline{a_0} = 0$$

Hence, we have $\bar{b}$ is integral over $A/J \cap A$. Note in particular, B/J is integral A-algebra since for any ideal $I \leq A$ we have $A \mapsto A/I$ is an integral A-algebra since A/I is finite A-algebra.

(2): Let $\frac{b}{s} \in S^{-1}B$, since b is integral ove A we have $b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$ for some $a_i \in A$. Multiply both sides by $\frac{1}{s^n} \in S^{-1}B$, we have

$$(\frac{b}{s})^n + \frac{a_{n-1}}{s}(\frac{b}{s})^{n-1} + \frac{a_{n-2}}{s^2}(\frac{b}{s})^{n-2} + ... + \frac{a_0}{s^n} = 0$$

This shows b/s is integral over $S^{-1}A$. ♡

Proposition 2.7.18. *Let $A \subseteq B$ be an extension of rings, with B integral over A. Then B is a field if and only if A is a field.*

Proof.

($\Rightarrow$): Let $0 \neq a \in A$. Since $A \subseteq B$ and B is a field, consider $b := \frac{1}{a} \in B$. Since B is integral over A we have $b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$ for some $n > 0$, $a_0, ..., a_{n-1} \in A$.

Since $b \neq 0$ we can divide both side by b^{n-1} in the field B and get

$$b + a_{n-1} + \frac{a_{n-2}}{b} + ... + \frac{a_0}{b^{n-1}} = 0$$

Thus

$$b = -a_{n-1} - \frac{a_{n-2}}{b} - ... - \frac{a_0}{b^{n-1}}$$

However, $b = \frac{1}{a}$ and so we have

$$b = -a_{n-1} - aa_{n-2} - a^2a_{n-3} - ... - a^{n-1}a_0 \in A$$

This imply A is a subfield of B.

($\Leftarrow$): Let A be a field and $A \subseteq B$ is an integral domain. Suppose B is integral over A. We want to show B is a field.

Let $0 \neq b \in B$ with
$$b^n + a_{n-1}b^{n-1} + ... + a_0 = 0$$
If $a_0 = 0$ then we may factor out a copy of b and get $b(b^{n-1} + a_{n-1}b^{n-2} + ... + a_1) = 0$ and since B is integral domain we have $b^{n-1} + a_{n-1}b^{n-2} + ... + a_1 = 0$. Thus we may assume $a_0 \neq 0$. ♡

Example 2.7.19 (Exercise)**.** Note this does not work when B is just an A-algebra in the direction $(\Rightarrow)$ in the above proof, i.e. assume B is a field and A-algebra. Indeed, consider A and $\mathfrak{m}$ a maximal ideal of A, then we have $A \to A/\mathfrak{m}$ is an integral A-algebra and it is clearly not true that $A/\mathfrak{m}$ is field if and only if A is a field.

Proposition 2.7.20. *Let B be an integral A-algebra and $P \in Spec(A)$, $Q \in Spec(B)$ with $Q \cap A = P$. Then we have Q is maximal if and only if P is maximal.*

Proof. Consider the following commutative diagram

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d] & B \arrow[d] \\
A/P \arrow[r, "integral"] & B/Q
\end{tikzcd}$$

We have B/Q is integral A/P-algebra by 2.7.17.1 and hence we have B/Q is a field if and only if A/P is a field, i.e. Q is maximal iff P is maximal. ♡

Chapter 3

Topics

3.1 Going Up Theorem

Definition 3.1.1. Let B be an A-algebra and $P \in Spec(A)$, $Q \in Spec(B)$. Then we say Q ***lies above*** P if $Q \cap A = P$.

Remark 3.1.2 (Geometric Meaning of "lies above")**.** Consider $f : A \to B$ an A-algebra. We get $f^* : Spec(A) \to Spec(A)$ via $Q \mapsto Q \cap A$. Then, we have $Q \in Spec(B)$ lies above P if and only if $f^*(Q) = P$. We also remark that f^* is actually continuous in the Zariski topology.

Theorem 3.1.3. *Let $A \subseteq B$ be an integral extension and $P \in Spec(A)$. There exists a prime ideal I in B lying above P. Viz, the map from $Spec(B)$ to $Spec(A)$ is surjective.*

Proof. Consider

$$\begin{tikzcd} A \arrow[r, "\subseteq"] \arrow[d] & B \arrow[d] \\ A_P \arrow[r] & B_P \end{tikzcd}$$

where we note $P \subseteq B$ so the localization $B_P = (A \backslash P)^{-1}(B)$ makes sense. We note B_P is not trivial and hence B_P contains a maximal ideal $N \subsetneq N_P$.

Let $Q = N \cap B$. Then, we have $Q \cap A = (N \cap B) \cap A = (N \cap A_P) \cap A$ as the above square commutes (so we can take contraction from $B_P \to B \to A$ or $B_P \to A_P \to A$).

However, A_P is a local ring, i.e. PA_P is the unique maximal ideal in A_P. Hence, we have $N \cap A_P = PA_P$ and so we have $Q \cap A = PA_P \cap A = P$ by the bijective correspondence.

This finishes the proof as we find Q lying above P. ♡

Proposition 3.1.4. *Let $A \subseteq B$ be an integral extension, $P \in Spec(A)$ and $Q, Q' \in Spec(B)$, both lying above P. If $Q \subseteq Q'$ then $Q = Q'$. Viz, $Spec(B) \to Spec(A)$ has separated fibers.*

Proof. Consider $S = A \backslash P$ and

$$\begin{array}{ccccc} A & \xrightarrow{\subseteq} & B & \xrightarrow{\pi} & B/Q \\ \downarrow & & \downarrow & & \downarrow \\ A_P & \xrightarrow{\subseteq_P} & B_P & \xrightarrow{\pi_P} & S^{-1}(B/Q) \end{array}$$

where we remark $\subseteq : A \to B$ is the inclusion map and π is the projection.

Now, observe $S^{-1}(B/Q) = S^{-1}B/S^{-1}Q = B_P/QB_P$. Since $Q \cap A = P$ and $Q \cap S = \emptyset$, we have by the correspondence theorem for prime ideals of localization that QB_P is prime in B_P.

Now we claim QB_P lies above PA_P. Consider the short exact sequence

$$0 \longrightarrow P \longrightarrow A \xrightarrow{\pi \circ \subseteq} B/Q$$

However, localization is an exact functor and hence we have

$$0 \longrightarrow S^{-1}P = PA_P \longrightarrow S^{-1}A = A_P \xrightarrow{\pi \circ \subseteq} S^{-1}B/Q = B_P/QB_P$$

is exact. Hence, we have $PA_P = Ker(S^{-1}(\pi \circ \subseteq)) = Ker(S^{-1}(\pi) \circ S^{-1}(\subseteq)) = Ker(\pi_P \circ \subseteq_P) = QB_P \cap A_P$. This proves the claim.

Since $\subseteq_P : A_P \to B_P$ is an integral extension, PA_P is maximal in A_P. Hence, we must have QB_P is maximal ideal in B_P by Proposition 2.7.20. We can do the same thing with $Q'B_P$ and hence we have $Q'B_P$ is maximal. However, $Q \subseteq Q'$ and so $QB_P \subseteq Q'B_P$ and so $QB_P = Q'B_P$. Now, by the correspondence theorem for localizations, we must have $Q = Q'$. ♡

Corollary 3.1.4.1. *Let B be Noetherian integral extension of A. Let $P \in Spec(A)$ then there is only finitely many prime ideal in B lying above P. Viz, $Spec(B) \to Spec(A)$ has finite fibers.*

Proof. Let $Q \in Spec(B)$ with $Q \cap A = P$. Then $Q \supseteq PB$. Now we show Q contains PB with minimality. Suppose $Q \supseteq Q' \supseteq PB$ with $Q' \in Spec(B)$. Then $P = Q \cap A \supseteq Q' \cap A \supseteq PB \cap A \supseteq P$. Hence we get $Q' \cap A = P$ and by Proposition 3.1.4, we have $Q' \subseteq Q$ and they both lying above P so $Q = Q'$. This establishes the minimality of Q, i.e. if Q lies above P then Q is a minimal prime containing PB.

However, B is Noetherian and so PB is decomposable. Hence, PB has finitely many minimal primes containing it as they must come from the minimal associated primes. So we only have finitely many prime lies above P. ♡

Proposition 3.1.5. *Let $P \subseteq P'$ be two prime ideals in A. Then there exists two prime ideals Q, Q' in B such that $Q \subseteq Q'$ and $Q \cap A = P$ and $Q' \cap A = P'$.*

Proof. First let $Q \in Spec(B)$ lying above P. Consider

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ A/P & \longrightarrow & B/Q \end{array}$$

Note B/Q is integral over A/P, hence by previous results we can find a prime in B/Q that lies above P'/P. It will be of the form $Q'/Q \subseteq B/Q$ with $Q' \supseteq Q$ a prime ideal. As we remark $Q' \cap A = P'$, we are done. ♡

Theorem 3.1.6 (Going Up Theorem)**.** *Let $A \subseteq B$ be integral extension. Let $P_1 \subseteq ... \subseteq P_r$ be a chain of prime ideals in A. Then there exists $Q_1 \subseteq Q_2 \subseteq ... \subseteq Q_r$ of prime ideals in B such that $Q_i \cap A = P_i$.*

Proof. By apply Proposition 3.1.5 we are done. ♡

3.2 Noether's Normalization Lemma

Definition 3.2.1. Let $v_1, ..., v_n \in k$ where k is a field, then we say $k_1, ..., k_n$ are ***algebraically independent*** if for all $0 \neq f \in k[x_1, ..., x_n]$ we have $f(k_1, ..., k_n) \neq 0$.

Lemma 3.2.2. *Let $f : A \to A$ be an surjective ring homomorphism and A is Noetherian. Then we have f is injective.*

Proof. Let $I_i = Ker(f^i) \leq A$ for $i = 1, 2, 3, ...$ and we see that $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ is an increasing chain. Since A is Noetherian we have the chain stabilizes at one point, say $I_n = I_{n+1} = ... = I_{2n} = I_{2n+1}...$.

Then we claim $Im(f^n) \cap Ker(f^n) = \{0\}$. Note $\{0\} \subseteq Im(f^n) \cap Ker(f^n)$ trivially. Now suppose $x \in Im(f^n) \cap Ker(f^n)$ and this means $x = f^n(y)$ for some $y \in A$ and $f^n(x) = 0$. Then we have $f^n(x) = f^{2n}(y) = 0$ and so $y \in Ker(f^{2n}) = Ker(f^n)$. Therefore, we have $x = f^n(y) = 0$ as desired.

Now, observe f is surjective so we have f^n is surjective and so $Im(f^n) = A$. Therefore, we have $Im(f^n) \cap Ker(f^n) = A \cap Ker(f^n) = 0$ and so $Ker(f^n) = 0$. Since $Ker(f) \subseteq Ker(f^n)$ we have f is injective and so it is isomorphism as desired. ♡

Lemma 3.2.3. *If A is Noetherian and $I \leq A$ an ideal. Then we have $A/I \cong A$ via $f : A/I \to A$ imply I is the trivial ideal.*

Proof. Let $\pi : A \to A/I$ be the projection map $x \mapsto x + I$. Then we have π is surjective. Thus we have $f \circ \pi : A \to A$ is a surjective ring homomorphism. Since A is Noetherian, by Lemma 3.2.2 we have $f \circ \pi$ is injective as well. However, observe $Ker(\pi) \subseteq Ker(f \circ \pi) = \langle 0 \rangle$ we have $Ker(\pi)$ is trivial and so I is the trivial ideal as $I = Ker(\pi)$. ♡

Proposition 3.2.4. *Let A be a k-algebra where k is a field. Then $\{a_1, ..., a_n\} \subseteq A$ is algebraically independent over k if and only if $k[a_1, ..., a_n]$ is isomorphic, as a k-algebra, to a polynomial ring over k in n variables.*

Proof. Let $a_1, ..., a_n$ be algebraically independent.

Consider the map
$$\phi : k[x_1, ..., x_n] \mapsto k[a_1, ..., a_n]$$
given by $f(x_1, ..., x_n) \mapsto f(a_1, ..., a_n)$. This map is clearly well-defined as it is the evaluation map. It is a ring homomorphism trivially as it is the evaluation map. It has trivial kernel because $a_1, ..., a_n$ are algebraically independent. It is surjective because, for any $a \in A$, we have $f = a \in k[x_1, ..., x_n]$ and so $f(a_1, ..., a_n) = a$. Thus ϕ is an isomorphism as desired.

Now, let $\phi : k[a_1, ..., a_n] \to k[x_1, ..., x_n]$ be the isomorphism. Now consider
$$\psi : k[x_1, ..., x_n] \to k[a_1, ..., a_n]$$
given by $f \mapsto f(a_1, ..., a_n)$.

We have ψ is surjective as $k[a_1, ..., a_n] = \{f(a_1, ..., a_n) : f \in k[x_1, ..., x_n]\}$. Thus, we have
$$k[x_1, ..., x_n]/Ker(\psi) \cong k[a_1, ..., a_n]$$
Thus, we have
$$k[x_1, ..., x_n]/Ker(\psi) \cong k[a_1, ..., a_n] \cong k[x_1, ..., x_n]$$
by composition of isomorphisms. Hence, we have an isomorphism
$$\tau : k[x_1, ..., x_n]/Ker(\psi) \to k[x_1, ..., x_n]$$

Now by Lemma 3.2.3 we have $k[x_1, ..., x_n]/Ker(\psi)$ and $k[x_1, ..., x_n]$ are Noetherian and τ is an isomorphism. Hence $Ker(\psi)$ is trivial and so $a_1, ..., a_n$ is algebraically independent as the only polynomial $f \in k[x_1, ..., x_n]$ that vanishes $(a_1, ..., a_n)$ is the zero polynomial. ♡

Theorem 3.2.5. *Let A be a finitely generated k-algebra where k is an infinite field. Then there exists $u_1, ..., u_l \in A$ that are algebraically independent over k such that A is integral over $k[u_1, ..., u_l]$.*

Proof. Since A is finitely generated, $A = k[a_1, ..., a_n]$ for some $a_1, ..., a_n \in A$. We will proceed by induction on n. If $n = 0$ then the claim is vacuously true.

Now assume $n > 0$ and the claim holds for value less than n. If $a_1, ..., a_n$ are algebraically independent over k, then let $l = n$ and $u_i = a_i$ and we are done.

Hence, we may assume that there is $0 \neq f \in k[x_1, ..., x_n]$ such that $f(a_1, ..., a_n) = 0$. Write $f = f_d + f_{d-1} + ... + f_1 + f_0$ where f_i is the ith homogeneous part of f and d is the total degree of f, i.e. add all degree of all variables (e.g. $x^2y^4z^1$ has total degree $2 + 4 + 1 = 7$).

Exercise: let $0 \neq g \in k[x_1, ..., x_n]$ where k is infinite. Then there are infinitely many $(a_1, ..., a_n) \in k^n$ such that $g(a_1, ..., a_n) \neq 0$. (We can do this by induction as it is clear for $n = 1$).

By apply the Exercise result, there exists $\lambda_1, ..., \lambda_n \in k$, not all zero, such that $f_d(\lambda_1, ..., \lambda_n) \neq 0$. WLOG we may assume $\lambda_n \neq 0$. Then we have

$$\begin{aligned}
0 &\neq f_d(\lambda_1, ..., \lambda_n) \\
&= f_d(\frac{\lambda_1}{\lambda_n}\lambda_n, \frac{\lambda_2}{\lambda_n}\lambda_n ..., \frac{\lambda_{n-1}}{\lambda_n}\lambda_n, \lambda_n) \\
&= \lambda_n^d f_d(\frac{\lambda_1}{\lambda_n}, ..., \frac{\lambda_{n-1}}{\lambda_n}, 1)
\end{aligned}$$

THe last line is obtained because f_d is homogeneous of degree d. Therefore, we may assume there exists $(\lambda_1, ..., \lambda_{n-1}, 1)$ so that $f_d(\lambda_1, ..., \lambda_{n-1}, 1) \neq 0$.

Now, since $A = k[a_1, ..., a_n]$, for each $j = 1, ..., n-1$, let $b_j := a_j - \lambda_j a_n$. Then we have

$$\begin{aligned}
0 &= f(a_1, ..., a_n) \\
&= f(b_1 + \lambda_1 a_n, ..., b_{n-1} + \lambda_{n-1} a_n, a_n) \\
&= \sum_{i=0}^{d} f_i(b_1 + \lambda_1 a_n, ..., b_{n-1} + \lambda_{n-1} a_n, a_n) \\
&= a_n^d f_d(\lambda_1, ..., \lambda_{n-1}, 1) \\
&\quad + \text{ terms of lower degree in } a_n \text{ with coefficients in } k[b_1, ..., b_{n-1}]
\end{aligned}$$

Since $f_d(\lambda_1, ..., \lambda_{n-1}, 1) \in k$ is not zero, we can divide through and get a monic polynomial with coefficients in $k[b_1, ..., b_{n-1}]$. Therefore, we have a_n is integral over $k[b_1, ..., b_{n-1}]$.

Hence we have $A = k[a_1, ..., a_n] = k[b_1, ..., b_{n-1}, a_n]$ and is integral over $k[b_1, ..., b_{n-1}]$. Therefore, by induction hypothesis, we can find $v_1, ..., v_l \in k[b_1, ..., b_{n-1}]$, algebraically independent over k, such that $k[b_1, ..., b_{n-1}]$ is integral over $k[u_1, ..., u_l]$. Hence we have A is integral over $k[u_1, ..., u_l]$ and the proof follows. ♡

Remark 3.2.6 (Geometric Meaning of Noether's Normalization)**.** Let k be an infinite field, A a finitely generated k-algebra. There is a polynomial ring $k[x_1, ..., x_l] \subseteq A$ such that A is integral over $k[x_1, ..., x_l]$.

So, there is an induced surjective and finite-to-one map

$$Spec(A) \to Spec(k[x_1, ..., x_n]) =: \mathbb{A}^l_k$$

Therefore, if A is f.g. k-algebra, then the spectrum is really close to the affine l-space over k, i.e. $\mathbb{A}^l_k$.

3.3 Hilbert's Nullstellensatz

Proposition 3.3.1. *Let k be an infinite field and A a finitely generated k-algebra. Let $\mathfrak{m} \subseteq A$ be a maximal ideal. Then $A/\mathfrak{m}$ is a finite algebric field extension of k.*

Proof. Note we have a sequence $k \xrightarrow{i} A \xrightarrow{\pi} A/\mathfrak{m}$ where i is embedding and π is surjective. Now, consider $\tau := \pi \circ i$, we have $\tau(1) = 1$ and so the kernel of τ is not k, i.e. it must be zero as k is a field. Hence we can embed k into $A/\mathfrak{m}$ and so $A/\mathfrak{m}$ is a field extension of k.

Now, since A is finitely generated k-algebra, so is $A/\mathfrak{m}$. Apply Noether's normalization lemma to $A/\mathfrak{m}$, we have $u_1, ..., u_l \in A/\mathfrak{m}$, which are algebraically independent over k such that

$$k \subseteq k[u_1, ..., u_l] \subseteq A/\mathfrak{m}$$

Since $A/\mathfrak{m}$ is a field, we must have $k[u_1, ..., u_l]$ is a field. Hence, we have $l = 0$ as this is the only case where $k[u_1, ..., u_l] \cong k[x_1, ..., x_n]$ is a field. Hence $k \subseteq A/\mathfrak{m}$ where $A/\mathfrak{m}$ is integral over k, i.e. $A/\mathfrak{m}$ is algebric over k as k is a field.

Now, integrality plus finitely generated k-algebra imply $A/\mathfrak{m}$ is a finite k-algebra and so the extension is finite. ♡

Theorem 3.3.2 (Weak Hilbert's Nullstellensatz)**.** *Let k be algebraically closed field. Let $I \subseteq k[x_1, ..., x_l]$ be an ideal. Then I is maximal if and only if I is of the form*

$$\langle x_1 - a_1, x_2 - a_2, ..., x_l - a_l \rangle$$

for some fixed $a_1, ..., a_l \in k$.

Proof. Suppose $I = \langle x_1 - a_1, ..., x_l - a_l \rangle$, we will show I is maximal. Consider $R := k[x_1, ..., x_l]/I$. Let $\overline{f}$ denote the image of f in $k[x_1, ..., x_l]/I$.

Note $k \subseteq k[x_1, ..., x_l]/I$ and so R is finitely generated k-algebra by $\overline{x_1}, ..., \overline{x_l}$. However, $\overline{x_i} = \overline{a_i}$ for $1 \leq i \leq l$ and so we must have $R = k$ as the generators are in k. Hence R is a field and so I is maximal.

Conversely, suppose $\mathfrak{m} \subseteq k[x_1, ..., x_l]$ is maximal. Then we have $R := k[x_1, ..., x_l]/\mathfrak{m}$ is a finite algebric extension by Proposition 3.3.1. However, k is algebraically closed, we have $R = k$. However, now we consider the projection map π from $k[x_1, ..., x_l]$

to R, we have $x_i \mapsto \overline{x_i}$ where $R = k$. Thus $\overline{x_i} = a_i$ for some $a_i \in k$. Hence we must have $\pi(x_i - a_i) = \pi(x_i) - \pi(a_i) = 0$ and so $\langle x_1 - a_1, ..., x_l - a_l \rangle \subseteq Ker(\pi) = \mathfrak{m}$. However, from the last direction, we see $\langle x_1 - a_1, ..., x_l - a_l \rangle$ is maximal and so we must have $\mathfrak{m} = \langle x_1 - a_1, ..., x_l - a_l \rangle$. ♡

Remark 3.3.3. Note the Nullstellensatz imply that there is a bijection between closed points of $\mathbb{A}^l_k = Spec(k[x_1, ..., x_l])$ and k^l.

Remark 3.3.4. Given an ideal I of $k[x_1, ..., x_n]$, then define

$$Z(I) := \{(a_1, ..., a_n) \in k^n : \forall f \in I, f(a_1, ..., a_n) = 0\}$$

By Weak Nullstellensatz, if k is algebraically closed and $I \leq k[x_1, ..., x_n]$ is proper ideal, then we must have $Z(I)$ is not empty. Indeed, we see this by noting since I is proper, $I \subseteq \mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal. Therefore, $\mathfrak{m} = \langle x_1 - a_1, ..., x_n - a_n \rangle$ and so $(a_1, ..., a_n) \in Z(\mathfrak{m}) \subseteq Z(I)$.

Remark 3.3.5. Now, instead of looking at the points vanishing all elements of an ideal, we also have the inverse operation. Namely, let Z be a subset of k^n, we define $I(Z) := \{f \in k[x_1, ..., x_n] : \forall z \in Z, f(z) = 0\}$. This is clearly an ideal.

However, what is $I(Z(J))$ for some ideal $J \leq k[x_1, ..., x_n]$?

Theorem 3.3.6 (Strong Hilbert's Nullstellensatz)**.** *Let $\mathcal{J}$ be an ideal of $k[x_1, ..., x_n]$ where k is algebraically closed, then we have*

$$I(Z(\mathcal{J})) = \sqrt{\mathcal{J}}$$

Proof. Note $I(Z(\mathcal{J})) \supseteq \sqrt{\mathcal{J}}$ is trivial.

Now let $f \notin \sqrt{\mathcal{J}}$, we will show $f \notin I(Z(\mathcal{J}))$. We will look for a tuple in $Z(\mathcal{J})$ on which f does not vanish. Note $f \notin \sqrt{\mathcal{J}}$, there exists a prime ideal $P \supseteq \mathcal{J}$ with $f \notin P$ as we recall the radical is the intersection of all primes containing $\mathcal{J}$.

Let $\overline{f}$ be the image of f in $A := k[x_1, ..., x_n]/P$. Then we have

$$k[x_1, ..., x_n] \xrightarrow{\pi} A \xrightarrow{\text{localize}} A_{\overline{f}}$$

Then note $A_{\overline{f}} = k[\overline{x_1}, ..., x_n, 1/\overline{f}]$ is a finitely generated k-algebra. Since $\overline{f}^m \neq 0$ for every $m \geq 0$, we have $A_{\overline{f}}$ is not trivial. Hence there exists a maximal ideal $\mathfrak{m} \subseteq A_{\overline{f}}$. Hence we have $A_{\overline{f}}/\mathfrak{m}$ is a finite algebraic extension of k by Proposition 3.3.1. However, note k is algebraically closed, we must have $A_{\overline{f}}/\mathfrak{m} = k$.

Therefore, we get a chain

$$k[x_1, ..., x_n] \longrightarrow A \longrightarrow A_{\overline{f}} \longrightarrow A_{\overline{f}}/\mathfrak{m} \longrightarrow k$$

and hence obtain, by composition of arrows, a k-algebra homomorphism

$$\tau : k[x_1, ..., x_n] \to k$$

Let $a_i := \tau(x_i) \in k$ for $1 \leq i \leq n$.

We claim $(a_1, ..., a_n) \in Z(\mathcal{J})$. Indeed, let $g \in \mathcal{J}$, we have

$$\begin{aligned} g(a_1, ..., a_n) &= g(\pi(x_1), ..., \pi(x_n)) \\ &= \pi(g(x_1, ..., x_n)) = \pi(g) \\ &= 0 \end{aligned}$$

as we note $g \in P$ and in the first stage, we have g got killed. This finishes our claim.

We claim $f(a_1, ...a_n) \neq 0$. Indeed, note $f(a_1, ..., a_n) = f(\pi(x_1), ..., \pi(x_n)) = \pi(f) = \pi(\overline{f} + \mathfrak{m})$. However, note $\overline{f} \notin \mathfrak{m}$ as $\overline{f}$ is a unit in $A_{\overline{f}}$ and hence π cannot map f to 0 as $\overline{f} + \mathfrak{m}$ is not zero in $A_{\overline{f}}/\mathfrak{m}$. This finishes our claim.

Hence we have $f \notin I(Z(\mathcal{J}))$ and the proof follows. Thus $I(Z(\mathcal{J})) = \sqrt{\mathcal{J}}$ as desired. ♡

3.4 Algebro-Geometric Correspondence

Remark 3.4.1 (Classical Correspondence)**.** Let k be algebraically closed field and $A := k[x_1, ..., x_n]$. Then there is a correspondence between radical ideals of A and algebraic subsets of k^n, i.e. sets of the form $Z(I)$ for some $I \leq A$. In particular, the map is $I \mapsto Z(I)$ and $S \mapsto I(S)$ with $I \leq A$ and $S \subseteq k^n$. For full detail, go check my PMATH 464 note.

Remark 3.4.2 (Modern Correspondence)**.** Let A be any ring, then there is an inclusion reversing bijective correspondence between the set of radical ideals of A and set of Zariski closed subsets in $Spec(A)$. In particular, the maps are $I \mapsto V(I)$ and $S \mapsto I(S) := \bigcap_{P \in S} P$ where $I \leq A$ and S is closed set in $Spec(A)$.

Indeed, observe if $S \subseteq Spec(A)$ then $I(V)$ is indeed a radical ideal as the intersection of prime ideals is radical.

On the other hand, let $I \leq A$ be radical ideal, then we need to show $I(V(I)) = I$. However, note $I(V(I)) = \bigcap_{P \in V(I)} P = \bigcap\{P \supseteq I, P \in Spec(A)\} = \sqrt{I} = I$.

Finally, we need to show if $S \subseteq Spec(A)$ is closed, we have $V(I(S)) = S$. Indeed, $S = V(J)$ for some ideal J. Then $V(I(S)) = V(I(V(J))) = V(\sqrt{J}) \subseteq V(J) = S$. Thus $V(I(S)) \subseteq S$. The other inclusion is trivial and so $V(I(S)) = S$ as desired.

Remark 3.4.3 (Functional Interpretation)**.** We want to view elements of A as functions on $Spec(A)$. To do this, consider $f \in A$ be arbitrary elements and let $P \in Spec(A)$. Then we have

$$\begin{tikzcd} A \arrow[r] & A_P \arrow[r] & A_P/PA_P := \kappa(P) \\ f \arrow[u, "\text{elements of}"] \arrow[rr, mapsto] & & f(P) \arrow[u, "\text{elements of}"'] \end{tikzcd}$$

Therefore, we consider $f(P)$ to be the image of f in A_P/PA_P.

Note this is a strange function because $\kappa(P)$ depends on the input P.

Now, note $f(P) = 0 \Leftrightarrow f \in P$ since $PA_P \cap A = P$. Hence, we have $I \subseteq A$, then

$$V(I) = \{P \in Spec(A) : \forall f \in I, f(P) = 0\}$$

This is just like $Z(I)$, if we accept the strange notion of functions.

In particular, if we apply this point of view to $A = k[x_1, ..., x_n]$, then we see $\kappa(P) = A_P/PA_P$ and by Noether normalization lemma we get $\kappa(P) = k$ for all P as k is algebraically closed.