I RINGS AND MODULES

- A ring, $I \subset A$ **ideal** when $A \cdot I \subset I$; $\mathrm{Ker}(f : A \to B)$ is an ideal.

- For $f : A \to B$ ring hom, $I \subset \mathrm{Ker}\, f \iff f$ factorizes through A/I, ie, $\exists\, \bar{f} : A/I \to B : f = \bar{f} \circ \pi$.

Proposition: Let A be a ring and $I \subset A$ ideal. There's a 1-1 correspondence

$$\left\{ \begin{array}{c} \text{ideals of} \\ A/I \end{array} \right\} \;=\; \left\{ \begin{array}{c} \text{ideals } J : \\ I \subset J \subset A \end{array} \right\} \qquad \begin{array}{c} \bar{J} \longmapsto \pi^{-1}(\bar{J}) \\ \pi(J) \longleftarrow J \end{array}$$

- $x \in A$ **proper** if x is neither 0 nor invertible
- $x \in A$ **irreducible** if it is not the product of two proper elements.
- $x \in A$ **zero divisor** if $\exists\, 0 \neq y \in A : xy = 0$.
- $x \in A$ **nilpotent** if $\exists\, n > 0 : x^n = 0$
- $x \in A$ **unit** or **invertible** if $\exists\, y \in A : xy = 1$. A^* is the set of units.

A **integral domain** if there's no non-trivial zero divisors. Ie, $xy = 0 \Rightarrow x = 0$ or $y = 0$.

An ideal $\mathfrak{p}$ is **prime** if $\mathfrak{p} \neq A$ and it holds that $xy \in \mathfrak{p} \iff x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ ($\Leftarrow$) always)

An ideal $\mathfrak{m}$ is **maximal** if $\mathfrak{m} \neq A$ and the only ideal which strictly contains to $\mathfrak{m}$ is A.

$\mathfrak{p}$ prime $\iff A/\mathfrak{p}$ domain ; $\mathfrak{m}$ maximal $\iff A/\mathfrak{m}$ field.

A **principal ideal domain** (PID) if it is a domain and every ideal is principal, $\mathfrak{a} = (a)$ for some $a \in A$.

A **unique factorization domain** (UFD) if it is a domain and every element is a product of irreducible elements in a unique way up to order and units.

PID $\Rightarrow$ UFD, but $\not\Leftarrow$ (eg. $(2, x)$ in $\mathbb{Z}[x]$)

Proposition: Let A be a domain.

1) $(a) = (b) \iff \exists\, u \in A^* : b = a \cdot u$

2) $A[x]$ domain

3) $(A[x])^* = A^* = A - 0$

- $(0) \in \operatorname{Spec} A \iff A$ domain.
- If A is PID, then the Bezout identity holds: if $d = \gcd(a,b)$, $\exists r, s \in A : d = r \cdot a + s \cdot b$.

Lemma (Euclides): Let A be PID and $0 \neq a \in A$. Then the following are equivalent:

1) a irreducible
2) (a) maximal ideal
3) (a) prime ideal.

Ie, if A is a PID, $\operatorname{Spec} A = \{0, (a)\}_{a \text{ irred}}$; $\operatorname{Max}(A) = \{(a)\}_{a \text{ irred}}$.

Lemma: Let A be a UFD and $0 \neq a \in A$. Then

$$a \text{ irreducible} \iff (a) \text{ prime}$$

Ie, $$(\operatorname{Spec} A)|_{\text{principal}} = \{0, (a)\}_{a \text{ irred}}.$$

Theorem: Every non-zero ring has maximal ideals

Corollary: Every ideal $\neq A$ is contained in a maximal ideal

Corollary: $a \notin A^* \iff a$ is contained in some maximal ideal, ie,

$$\boxed{A = A^* \amalg \bigcup_{\mathfrak{m} \in \operatorname{Max}(A)} \mathfrak{m}}$$

Definition: Let A be a ring. The nilradical of A is the set of nilpotent elements

$$\operatorname{Nil}(A) := \{a \in A : \exists n > 0 : x^n = 0\}$$

and we say that A is reduced when $\operatorname{Nil}(A) = 0$.

Proposition*: $\operatorname{Nil}(A) = \bigcap_{\substack{\mathfrak{p} \subset A \\ \text{prime}}} \mathfrak{p}$, thus in particular it is an ideal.

Definition: Let A be a ring. The Jacobson radical is

$$\mathrm{Jac}(A) := \{ x \in A : \forall y \in A ,\ 1 - xy \in A^* \}$$

Proposition: $\mathrm{Jac}(A) = \bigcap_{\substack{\mathfrak{m} \subset A \\ \text{maximal}}} \mathfrak{m}$, thus an ideal in particular.

OPERATIONS WITH IDEALS

Definition: Let A be a ring and I, J ideals.

a) Given a subset $S \subset A$, the ideal generated by S is the smallest ideal which contains S. Explicitly,

$\langle S \rangle = \{ \text{finite sums } a_1 s_1 + \dots + a_r s_r \}$.

b) The sum $I + J$ is the smallest ideal which contains I and J. Ie, $I + J = \langle I \cup J \rangle = \{ a + b : a \in I, b \in J \}$

c) The product IJ is the ideal generated by the products ab, $a \in I$, $b \in J$, $IJ = \{ a_1 b_1 + \dots + a_r b_r \}$.

d) The intersection $I \cap J$ is the set-theoretic intersection.

Definition: Two ideals I, J are coprimes if $I + J = A$.

- The following properties generalize the properties of gcd and lcm for integers:

Proposition:

1) $IJ \subset I + J$
2) $I(J+K) = IJ + IK$
3) $I \cap (J+K) \supseteq I \cap J + I \cap K$, and $=$ holds if either $J \subset I$ or $K \subset I$
4) $I + (J \cap K) \subseteq I + J \cap I \cap K$
5) $(I+J)(I \cap J) \subset IJ$
6) if I, J coprimes, then $IJ = I \cap J$.

Proposition: Let $I_1, \dots, I_r \subset A$ be ideals, and let $\pi : A \to A/I_1 \times \dots \times A/I_r$.

1) if all ideals are coprime two by two, then $I_1 \cdots I_r = I_1 \cap \dots \cap I_r$.

2) π surjective $\Leftrightarrow$ I_i's are coprimes two by two

3) π injective $\Leftrightarrow$ $I_1 \cap \dots \cap I_r = 0$.

Proposition*: Let $\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_m$ primes, and $\mathfrak{a}, \mathfrak{a}_1, \dots, \mathfrak{a}_n$ ideals

1) $\mathfrak{a} \subset \bigcup_i \mathfrak{p}_i \Rightarrow \mathfrak{a} \subset \mathfrak{p}_k$ for some k

2) $\bigcap \mathfrak{a}_i \subseteq \mathfrak{p} \Rightarrow \mathfrak{a}_k \subseteq \mathfrak{p}$ for some k, and if $=$, then $=$ as well.

Definition. Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Their <u>ideal quotient</u> is

$$(\mathfrak{a} : \mathfrak{b}) = \{ x \in A : x\mathfrak{b} \subset \mathfrak{a} \}.$$

Definition. Let $\mathfrak{a}$ be an ideal. The <u>radical</u> of $\mathfrak{a}$ is

$$\operatorname{rad} \mathfrak{a} = \sqrt{\mathfrak{a}} := \{ x \in A : x^n \in \mathfrak{a} \text{ for some } n > 0 \}.$$

- $\operatorname{Nil}(A) = \sqrt{0}$.

Proposition. $\operatorname{rad} \mathfrak{a} = \bigcap_{\substack{\mathfrak{a} \subset \mathfrak{p} \\ \mathfrak{p} \text{ prime}}} \mathfrak{p}$

MODULES

Definition: Let A be a ring. An <u>A-module</u> is an abelian group M together with a ring hom. $A \longrightarrow \mathrm{End}(M)$

- K-mod $= K$-vs, $\mathbb{Z}$-mod $=$ ab gp, $K[x]$-mod $= E$ vs $+$ $T: E \to E$,
- G finite gp, $K[G]$ the group algebra of G over K. Then $K[G]$-mod $= K$-representation of G.

Definition: $S \subset M$ subset, $\langle S \rangle$ is the smallest submodule containing M, and we say that S <u>generates</u> or <u>spans</u> M if $\langle S \rangle = M$.

Definition: The <u>annihilator ideal</u> of M is

$$\mathrm{Ann}(M) := \mathrm{Ker}\,(A \longrightarrow \mathrm{End}(M)) = \{ a \in A \ : \ aM = 0 \}.$$

and M is <u>faithful</u> if $\mathrm{Ann}(M) = 0$.

- If $\mathfrak{a} \subset \mathrm{Ann}(M)$, then every A-module is also a $A/\mathfrak{a}$-module.

Lemma: 1) If $M'' \subseteq M' \subseteq M$, then $\dfrac{M/M''}{M'/M''} \simeq M/M'$.

2) $N_1, N_2 \subseteq M$, then $\dfrac{N_1 + N_2}{N_1} \simeq \dfrac{N_2}{N_1 \cap N_2}$

3) $N_1 \subset M_1$, $N_2 \subset M_2$, then $\dfrac{M_1 \oplus M_2}{N_1 \oplus N_2} \simeq M_1/N_1 \oplus M_2/N_2$.

Definition: Let $\{m_i\}_{i \in I} \subset M$. We say that the family <u>generates</u> M if $\langle m_i \rangle = M$, ie, when the morphism $\phi: A^{(I)} \to M$ is surjective $\left(A^{(I)} := \bigoplus_I A \right)$, and we say that it is a <u>basis</u> when it is <u>isomorphism</u>, and in this case we say that M is <u>free</u>. When I is finite, and $\{m_i\}$ generates, we say that M is <u>finitely generated</u>.

NAKAYAMA LEMMA

Definition: An ring $\mathcal{O}$ is <u>local</u> if it only has one maximal ideal.

- Eg: $\mathbb{Z}/n\mathbb{Z}$ local $\Leftrightarrow n = p^k$; $K[x]/(p(x))$ local $\Leftrightarrow p(x) = r(x)^k$, $r(x)$ irreducible.

• A local with maximal $\mathfrak{m}$ $\iff$ $A^* = A - \mathfrak{m}$.

<u>Lemma</u> (Nakayama, local): Let $\mathcal{O}$ be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finite-generated $\mathcal{O}$-module.

$$M = 0 \iff \underbrace{M \otimes_{\mathcal{O}} \mathcal{O}/\mathfrak{m} = M/\mathfrak{m}M}_{\text{this is a } \mathcal{O}/\mathfrak{m}\text{-vs}} = 0 \iff \mathfrak{m}M = M$$

Ie, a module is 0 $\iff$ it is 0 as vs $\Rightarrow$ a quotient is 0.

<u>Corollary</u>: Let $N \subset M$ $\mathcal{O}$-modules with M finitely-generated, and $\mathfrak{m}$ the max id of $\mathcal{O}$.

1) $N + \mathfrak{m}M = M \Rightarrow N = M$

2) $M = \langle m_1, \dots m_r \rangle \Rightarrow M/\mathfrak{m}M = \langle \overline{m_1}, \dots, \overline{m_r} \rangle$. this is a $\mathcal{O}/\mathfrak{m}$-vs

* <u>Sneak peak</u>: We'll see that both the lemma & cor. are true in a ring A changing $\mathfrak{m}$ by an ideal $\mathfrak{a} \subset$ Jac(A).

<u>SPECTRUM OF A RING</u>

<u>Definition</u>: Let A be a ring. The <u>spectrum</u> of A is $\mathrm{Spec}(A) := \{\text{primes ideals of } A\}$.

<u>Proposition</u>: Denote, for an ideal $I \subset A$, $(I)_0 = V(I) := \{x \in \mathrm{Spec}\, A : I \subset \mathfrak{p}_x\}$. Then

1) $\mathrm{Spec}\, A = (0)_0$, and $\emptyset = (A)_0$.

2) $\bigcap_{i \in I} (\mathfrak{a}_i)_0 = (\sum \mathfrak{a}_i)_0$

3) $\bigcup_{i=1}^{n} (\mathfrak{a}_i)_0 = (\bigcap \mathfrak{a}_i)_0$

• These 3 properties says that the $(\ )_0$ is closed under arbitrary intersections and finite unions; ie, it defines a topology:

Definition: We call Zariski topology over Spec A to the one that has as closed subsets

$\{ (I)_0 : I \text{ ideal} \}$.

Proposition: $\overline{\{x\}} = (\mathfrak{p}_x)_0$, $x \in \text{Spec } A$.

Corollary: $\{x\}$ is closed $\Leftrightarrow$ x is maximal

Corollary: Spec A is T_1 (ie, every singleton is closed) $\Leftrightarrow$ Max A = Spec A − (0). (ie, dim $A = 1$)

Examples: 1) Spec $\mathbb{Z} = \{(0), (2), (3), (5), \dots\}$, endowed with the cofinite topology

2) Spec $k = \{(0)\}$, discrete topology

3) Spec $\mathbb{C}[x] = \{(x-\lambda) : \lambda \in \mathbb{C}\} \cup \{0\}$, cofinite topology.

Given a ring hom $\phi: A \to B$, it induces a map in Spec, $\phi^*: \text{Spec } B \to \text{Spec } A$.

Lemma: ϕ^* is continuous: $(\phi^*)^{-1}(\mathfrak{a})_0 = (\mathfrak{a}B)_0$

That is, Spec defines a functor

$$\text{Spec}: \text{Rng}^{op} \to \text{Top}.$$

Notation: For a ring hom $\phi: A \to B$, if $\mathfrak{b} \subset B$ is a (prime) ideal, $\phi^{-1}(\mathfrak{b})$ is a (prime) ideal too, that we will denote as $\mathfrak{b} \cap A$. Conversely, if $\mathfrak{a} \subset A$ is an ideal, then $\phi(\mathfrak{a})$ is not in general an ideal (unless ϕ is surjective), but it generates an ideal $\langle \phi(\mathfrak{a}) \rangle$ that we'll denote as $\mathfrak{a}B$.

Theorem: $\pi: A \to A/\mathfrak{a}$ induces a homeom in Spec restricting to the image,

$$\text{Spec}(A/\mathfrak{a}) \overset{\pi^*}{=\!=} (\mathfrak{a})_0.$$

FLATNESS

- Let $\varphi : M_1 \to M_2$ be a module hom. If N is another module, then it induces a map $\varphi \otimes Id : M_1 \otimes N \to M_2 \otimes N$ ($=$ unique map st $m_1 \otimes n \mapsto \varphi(m_1) \otimes n$). It defines a functor $- \otimes_A N$

<u>Proposition</u>: $- \otimes_A N$ is <u>right-exact</u>, but not left-exact in general. ($\&$ Hom $(M,-)$ / $(-,M)$ is left-exact)

- <u>Eg</u>: If $0 \neq a \in A$ is a non-zero divisor, then $- \otimes_A A/(a)$ is not left exact.

<u>Definition</u>. We say that an A-module N is <u>flat</u> when the functor $- \otimes_A N$ is exact.

<u>Proposition</u>: Let N be an A-module. The following are equivalent:

1) N is flat (ie, it takes ses into ses)
2) $- \otimes_A N$ takes exact sequences into exact sequences.
3) $- \otimes_A N$ preserves injective maps: $M' \to M$ inj $\Rightarrow$ $M' \otimes N \to M \otimes N$ inj
4) ____________________ between finitely generated modules.

<u>Theorem</u>*: Let A be a ring and M fg, $\mathfrak{a} \subset A$ and $\phi : M \to M$ st $\phi(M) \subseteq \mathfrak{a} M$. Then ϕ satisfies an equation of the form $\phi^n + a_{n-1}\phi^{n-1} + \dots + a_1 \phi + a_0 = 0$, $a_i \in \mathfrak{a}$.

II : LOCALIZATION

Definition: Let A be a ring. A *multiplicative set* is a subset $S \subset A$ st

1) $1 \in S$
2) $s, s' \in S \Rightarrow ss' \in S$.

- Eg: $S = A - 0$ if A domain, $S = A - \mathfrak{p}$, $S = \{a^n : n \geq 0\}$.
- A domain $\Leftrightarrow$ $A - 0$ is a multiplicative system
- $\mathfrak{p}$ prime $\Leftrightarrow$ $A - \mathfrak{p}$ ——————.

Definition: Let A be a ring and $S \subset A$ a multiplicative set. Consider the following eq. relation on $A \times S$:

$$(a, s) \equiv (a', s') \Leftrightarrow \exists u \in S : (as' - a's)u = 0.$$

We call the *localization of A wrt S* to the quotient $A_S = S^{-1}A := A \times S / \equiv$, and denote every eq. class $\overline{(a,s)}$ as $\frac{a}{s}$.

- A_S is a ring defining $\frac{a}{s} + \frac{a'}{s'} := \frac{as' + a's}{ss'}$, $\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$, with zero $\frac{0}{1}$ and unit $\frac{1}{1}$.

Definition: The canonical morphism $j : A \longrightarrow A_S$, $a \longmapsto \frac{a}{1}$ is called *localization morphism*.

Lemma: 1) $\frac{a}{1} = 0 \Leftrightarrow \exists s \in S : as = 0$. Thus if A domain & $0 \notin S \Rightarrow j$ injective, ie, $\frac{a}{1} = 0 \Leftrightarrow a = 0$

2) $A_S = 0 \Leftrightarrow 0 \in S$.

3) If A domain and $0 \notin S$, then $\frac{a}{s} = \frac{a'}{s'} \Leftrightarrow as' = a's$.

Theorem (Universal Property of localization): The localization of a ring A is "another" ring A_S together with a morphism $j : A \to A_S$ st $j(A) \subset A_S^*$ and it is universal wrt this property. Ie, if $\varphi : A \to B$ is a ring hom st $\varphi(A) \subset B^*$, then $\exists! \, \overline{\varphi} : A_S \to B$: $\varphi = \overline{\varphi} \circ j$.

$$\begin{tikzcd}
A \arrow[r, "\varphi"] \arrow[d, "j"'] & B \\
A_S \arrow[ur, dashed, "\overline{\varphi}"'] &
\end{tikzcd}$$

~~**Lemma** $A_{\mathfrak{p}} := A_{A-\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.~~

- $\mathfrak{a}A_S = A_S \iff S \cap \mathfrak{a} \neq \emptyset$ $\quad \left(\mathfrak{a}A_S \overset{not}{=} \mathfrak{a}_S = \{ \frac{a}{s} : a \in \mathfrak{a} \} \right)$

- $\mathfrak{b} \neq A_S \Rightarrow S \cap (\mathfrak{b} \cap A) = \emptyset$.

Lemma 1) If $\mathfrak{b} \subset A_S$, $\exists\ \mathfrak{a}\ (:= \mathfrak{b} \cap A) \subset A$ st $\mathfrak{b} = \mathfrak{a}A_S$.

2) If $\mathfrak{p} \subset A$, $\mathfrak{p} \cap S = \emptyset$, $\exists\ \mathfrak{p}_S\ (:= \mathfrak{p}A_S) \subset A_S$ st $\mathfrak{p} = \mathfrak{p}_S \cap A$.

Theorem: There is a 1-1 correspondence

$$\operatorname{Spec} A_S \;=\; \{ x \in \operatorname{Spec} A : \mathfrak{p}_x \cap S = \emptyset \}$$

$$\mathfrak{p}_S = \mathfrak{p}A_S \longleftarrow\!\!\!\mapsto \mathfrak{p}$$

Corollary: $\operatorname{Spec} A_{\mathfrak{p}_x} = \{ y \in \operatorname{Spec} A : \mathfrak{p}_y \subset \mathfrak{p}_x \}$, and it is a local ring with maximal ideal $\mathfrak{p}_x A_{\mathfrak{p}_x}$

$$\begin{array}{ccc} \mathfrak{p}_y A_{\mathfrak{p}_x} & \longleftarrow\!\!\!\mapsto & \mathfrak{p}_y \\ \cap & & \cap \\ \mathfrak{p}_x A_{\mathfrak{p}_x} & \longleftarrow\!\!\!\mapsto & \mathfrak{p}_x \end{array}$$

CHANGE OF BASIS AND RESTRICTION OF SCALARS

- Let us fix a ring hom $\varphi : A \to B$.

- <u>Restriction of scalars</u>: Let M be a B-module. We can endow it with an A-module structure by setting $a \cdot m := \varphi(a) \cdot m$, and it's denoted as M_A when it is thought as A-mod.

- <u>Change of basis</u>: Let M be a A-mod. Note that B has a nat. structure of A-mod setting $a \cdot b := \varphi(a)\, b$, so we can perform $M \otimes_A B$ as A-modules. But this is also a B-module with multiplication $b \cdot (m \otimes b') := m \otimes bb'$.

These constructions define functors $\quad \begin{array}{c} \mathrm{Mod}_B \to \mathrm{Mod}_A \\ M \longmapsto M_A \end{array} \quad \& \quad \begin{array}{c} \mathrm{Mod}_A \to \mathrm{Mod}_B \\ M \longmapsto M \otimes_A B \end{array}$

Proposition: The previous functors define an adjunction

$$\mathrm{Mod}_A \underset{RS}{\overset{CB}{\rightleftarrows}} \mathrm{Mod}_B \quad , \qquad CB = - \otimes_A B \qquad RS = -_A$$

ie,

$$\mathrm{Hom}_B(B \otimes_A M, N) = \mathrm{Hom}_A(M, N_A)$$

$$f \longmapsto (m \mapsto f(1 \otimes m))$$

$$(b \otimes m \mapsto b \cdot g(m)) \longleftarrow g$$

, We have another functor (viewing B as A-mod via φ) $\mathrm{Hom}_A(B, -) : \mathrm{Mod}_A \to \mathrm{Mod}_B$, where for M A-mod, $f \in \mathrm{Hom}_A(B, M)$, $(b \cdot f)(b') := f(bb')$.

Proposition: There is an adjunction

$$\mathrm{Hom}_A(B, -) : \mathrm{Mod}_A \rightleftarrows \mathrm{Mod}_B : RS$$

i.e.,

$$\mathrm{Hom}(N_A, M) = \mathrm{Hom}(N, \mathrm{Hom}(B, M))$$

$$f \longmapsto (n \mapsto (b \mapsto f(bn)))$$

$$(n \mapsto g(n)(1)) \longleftarrow g$$

LOCALIZATION OF MODULES

Definition: Let M be a A-module and let $S \subset A$ be a multiplicative system. The <u>localization</u> of M by S is

$$M_S := M \times S / \equiv$$

where $(m, s) \equiv (m', s') \Leftrightarrow \exists u \in S : (ms' - m's)u = 0$, and $\overline{(m,s)} = \frac{m}{s}$.

• Setting $\frac{m}{s} + \frac{m'}{s'} := \frac{ms' + m's}{ss'}$, $\frac{a}{s} \cdot \frac{m}{s'} := \frac{am}{ss'}$ endow M_S with a structure of A_S-module, thus also with structure of A-module, $a \cdot \frac{m}{s} := \frac{a}{1}\frac{m}{s} = \frac{am}{s}$.

Theorem (Universal Property of the localization of Modules): Let A be a A-mod and N a A_S-mod. If $\varphi : M \to N$ is a A-mod homomorphism, and $S \subset A$ is a multiplicative system, there exists a unique A_S-mod hom $\bar{\varphi} : M_S \to N$ st $\bar{\varphi} \circ j = \varphi$

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "j"'] & N \\ M_S \arrow[ur, dashed, "\bar{\varphi}"'] & \end{tikzcd} \quad , \text{ ie, } \quad \mathrm{Hom}_{A_S}(M_S, N) = \mathrm{Hom}_A(M, N).$$

Corollary: $M_S \simeq M \otimes_A A_S$, the change of basis, thus $M_S \otimes_{A_S} N_S \simeq (M \otimes_A N)_S$.

Corollary: Let M, N A-mod, $S \subset A$ mult. sys. If $\varphi : M \to N$ is an A-module homomorphism, then exists a unique A_S-mod homomorphism $\varphi_S : M_S \to N_S$ st $\varphi_S \circ j^M = j^N \circ \varphi$

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "j^M"'] & N \arrow[d, "j^N"] \\ M_S \arrow[r, dashed, "\exists \varphi_S"] & N_S \end{tikzcd} \quad , \quad \boxed{\varphi_S\left(\frac{m}{s}\right) = \frac{\varphi(m)}{s}}$$

In particular, the localization of modules defines a functor $\mathrm{Mod}_A \to \mathrm{Mod}_{A_S}$.

Proposition (Properties):

1) $0_S = 0$
2) $(\mathrm{Id}_M)_S = \mathrm{Id}_{M_S}$
3) $(f \circ g)_S = f_S \circ g_S$
4) $(f + g)_S = f_S + g_S$

Theorem: The localization is an exact functor, ie, if $M' \xrightarrow{f} M \xrightarrow{g} M''$ is exact, so is $M'_S \xrightarrow{f_S} M_S \xrightarrow{g_S} M''_S$.

Corollary: 1) $N \subseteq M$ A-submodule $\Rightarrow$ $N_S \subseteq M_S$ A_S-submodule

2) $N \subseteq M \Rightarrow (M/N)_S \simeq M_S/N_S$

3) $(N+N')_S \simeq N_S + N'_S$

4) $(N \cap N')_S \simeq N_S \cap N'_S$

5) $(\bigoplus M_i)_S \simeq \bigoplus (M_i)_S$

6) $(\mathfrak{a}M)_S = \mathfrak{a}_S M_S$

7) $(A/\mathfrak{a})_S = A_S/\mathfrak{a}_S$

8) $(M/\mathfrak{a}M)_S = M_S/\mathfrak{a}_S M_S$.

And for a module homomorphism $\varphi: M \to N$,

9) $(\operatorname{Ker} \varphi)_S \simeq \operatorname{Ker} \varphi_S$

10) $(\operatorname{Im} \varphi)_S \simeq \operatorname{Im} \varphi_S$

11) $(\operatorname{Coker} \varphi)_S \simeq \operatorname{Coker} \varphi_S$.

Definition: We say that a property for rings (or modules) is local when for any ring A (or A-mod. M), it verifies the property $\Leftrightarrow$ $A_\mathfrak{p}$ (or $M_\mathfrak{p}$) verifies it $\forall \mathfrak{p} \in \operatorname{Spec} A$.

Proposition: A module being 0 is a local property, i.e., tfae:

1) $M = 0$

2) $M_\mathfrak{p} = 0 \quad \forall \mathfrak{p} \in \operatorname{Spec} A$

3) $M_\mathfrak{m} = 0 \quad \forall \mathfrak{m} \in \operatorname{Max} A$.

Corollary: Let $\varphi: M \to N$ be a module homomorphism.

1) Being injective is a local property.

2) —— surjective ——————.

3) —— isomorphism ——————.

Corollary: Being flat is a local property, i.e., tfae:

1) M is a flat A-module
2) $M_{\mathfrak{p}}$ is a flat $A_{\mathfrak{p}}$-module $\forall \mathfrak{p} \in \operatorname{Spec} A$
3) $M_{\mathfrak{m}}$ is a flat $A_{\mathfrak{m}}$-module $\forall \mathfrak{m} \in \operatorname{Max} A$.

- We can now easily prove the general version of Nakayama:

Lemma (Nakayama): Let A be a ring, M a finitely generated module and $\mathfrak{a} \subset \operatorname{Jac} A$ an ideal. Then

$$M = 0 \iff \mathfrak{a} M = M.$$

Corollary: Let $N \subset M$ be a submodule, M finitely-generated, and $\mathfrak{a} \subset \operatorname{Jac} A$. Then

$$N + \mathfrak{a} M = M \Rightarrow N = M$$

- A_S is a flat A-mod
- $\operatorname{nil} A_S = (\operatorname{nil} A)_S$
- $\operatorname{ann}(M_S) = (\operatorname{ann} M)_S$, when M f.g.

III : PRIMARY DECOMPOSITION

<u>Definition</u> : Let A be a ring. An ideal $\mathfrak{a} \neq A$ is <u>primary</u> when

$$ab \in \mathfrak{a} \Rightarrow a \in \mathfrak{a} \text{ or } b^n \in \mathfrak{a} \text{ for some } n \geq 1.$$

<u>Proposition</u> : $\mathfrak{a}$ primary $\Leftrightarrow$ $A/\mathfrak{a} \neq 0$ and every zero divisor of $A/\mathfrak{a}$ is nilpotent.

<u>Examples</u> : 1) In $\mathbb{Z}$, primary ideals are 0 & (p^n), p prime

2) In $K[x]$, $(p(x)^m)$, $p(x)$ irreducible (in general in A PID, (a^m) with a irreducible).

- $\mathfrak{p}$ prime $\Rightarrow$ $\mathfrak{p}$ primary

<u>Lemma</u> : $\mathfrak{a}$ primary $\Rightarrow$ $\sqrt{\mathfrak{a}}$ prime.

<u>Definition</u> : Let $\mathfrak{a}$ be a primary ideal, so that $\mathfrak{p} := \sqrt{\mathfrak{a}}$ is prime. Then $\mathfrak{a}$ is called <u>$\mathfrak{p}$-primary</u>, or that $\mathfrak{p}$ is the <u>associated</u> prime of $\mathfrak{a}$.

<u>Warning</u> : primary ideals $\neq$ powers of primes, ie, $\mathfrak{p}$ prime $\not\Rightarrow$ $\mathfrak{p}^n$ primary ; and $\sqrt{\mathfrak{a}}$ prime $\not\Rightarrow$ $\mathfrak{a}$ primary, but

<u>Lemma</u> : $\sqrt{\mathfrak{a}}$ maximal $\Rightarrow$ $\mathfrak{a}$ primary

<u>Lemma</u> : If $B \to A$ ring hom and $\mathfrak{a}$ is $\mathfrak{p}$-primary, then $\mathfrak{a} \cap B$ is $(\mathfrak{p} \cap B)$-primary.

<u>Proposition</u> : Let S be a multiplicative set of A and let $\mathfrak{a}$ be a $\mathfrak{p}$-primary ideal.

1) If $\mathfrak{p} \cap S \neq \emptyset$, then $\overset{\mathfrak{a}_S}{\mathfrak{a}A_S} = A_S$

2) If $\mathfrak{p} \cap S = \emptyset$, then $\overset{\mathfrak{a}_S}{\mathfrak{a}A_S}$ is $\mathfrak{p}A_S$-primary and $\mathfrak{a} = A \cap (\mathfrak{a}A_S)$. In particular

$$\boxed{\mathfrak{a} = A \cap (\mathfrak{a}A_{\mathfrak{p}})}$$

That is, two $\mathfrak{p}$-primary ideals are the same if they are the same locally at $\mathfrak{p}$.

Lemma: The intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

Definition: Let $\mathfrak{a} \subset A$ be an ideal. A minimal primary decomposition of $\mathfrak{a}$ is a decomposition

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

as intersection of primary ideals such that

i) All $\sqrt{\mathfrak{q}_i}$ are different

ii) $\mathfrak{a} \neq \mathfrak{q}_1 \cap \cdots \cap \hat{\mathfrak{q}}_i \cap \cdots \mathfrak{q}_n \quad \forall i.$

We say that $\mathfrak{a}$ is a decomposable ideal.

- By the lemma, if an ideal admits a primary decomposition, it admits a minimal one (deleting redundant terms if necessary).

Theorem: Let $0 = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a minimal primary decomposition of the 0 ideal. Then if $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$,

$$\{\text{Zero divisors of } A\} = \bigcup_{i=1}^{n} \mathfrak{p}_i$$

Theorem (Uniqueness of the associated prime ideals): The collection of associated prime ideals to a minimal primary decomposition of a decomposable ideal does not depend on the decomposition.

Definition: Let $\mathfrak{a}$ be a decomposable ideal. The collection of associated ideals to any primary decompositions is called the prime ideals associated to $\mathfrak{a}$

Definition: Let $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ a minimal primary decomposition. Since $(\mathfrak{a})_0 = \bigcup_i (\mathfrak{q}_i)_0$, if a prime ideal $\mathfrak{p}$ is minimal among prime ideals containing $\mathfrak{a}$, then $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ for some i, and we say that $\mathfrak{q}_i$ is a non-embedded component and $\mathfrak{p}$ is a minimal or isolated prime. The others are called embedded components and their radicals are embedded prime ideals

<u>Theorem</u> (Uniqueness of nonembedded components): Let $\mathfrak{a} = \bigcap_i \mathfrak{q}_i$ m.p.d. If $\mathfrak{p}$ is a minimal prime ideal corresponding to a irreducible component of $(\mathfrak{a})$, then $\mathfrak{p} = \sqrt{\mathfrak{q}_i}$ for some $\mathfrak{q}_i$, and

$$\mathfrak{q}_i = A \cap (\mathfrak{a} A_{\mathfrak{p}}),$$

ie, such a component $\mathfrak{q}_i$ does not depend on the decomposition.

In other words, the terms $\mathfrak{q}_i$ with $\sqrt{\mathfrak{q}_i}$ minimal are unique.

IV : INTEGRAL DEPENDENCE

Definition : Let $A \to B$ be a ring hom. We say that an element $b \in B$ is integral over A if it satisfies some relation $b^n + a_{n-1} b^{n-1} + \dots + a_1 b + a_0 = 0$, $a_i \in A$, and B is endowed with the A-algebra structure given by the morphism.

We say that $A \to B$ is a integral morphism or B is integral over A when every element of B is integral over A.

Definition : A ring hom $A \to B$ is finite if B is finitely gen. as A-module : $B = Ab_1 + \dots + Ab_n$; as A-module. In such a case, any f.g. B-mod M is f.g as A-mod too.

Definition : An A-module M is faithful if $\operatorname{Ann} M = 0$.

Theorem (Characterization of integral element) : Let $A \to B$ be a ring hom and $b \in B$. The following are eq :

1) b is integral over A
2) $A[b]$ is a f.g. A-module (ie, $A \to A[b]$ is finite)
3) b belongs to a subalgebra C of B which is fg as A-module
4) There is a faithful $A[b]$-module B which is fg as A-module

Corollary : If $b_1 \dots b_n$ are integral over A, then $A[b_1 \dots b_n]$ is a finitely generated A-module.

Corollary : The set C of integral elements of B over A is a subring, called the integral closure of A in B.

Corollary . The integral dependence is stable under change of basis. If B is integral over A, then $B \otimes_A D$ is integral over D for all A-algebra D.

Corollary . The composite of integral morphisms is integral.

Proposition: Let $f: A \to B$ be integral, $\mathfrak{b} \subset B$ ideal and $S \subset A$ multipl. system.

1) $\bar{f}: A/A\cap\mathfrak{b} \longrightarrow B/\mathfrak{b}$ is integral

2) $f_S: A_S \to B_S$ integral.

Definition: Let $A \to B$ be a ring hom. We say that A is <u>integrally closed</u> in B if the integral closure $C = A$, ie, if there is no more integral elements apart the ones of A. If A is a domain, then A is integrally closed when it is in $\operatorname{Frac} A = A_{A-0}$.

Lemma. Let $A \to B$ ring hom and let C be the integral closure of A in B. If S is a multiplicative system, then C_S is the integral closure of A_S in B_S.

Proposition: Let A be a domain. Tfae:

1) A integrally closed.

2) A_x ———— $\forall x \in \operatorname{Spec} A$

3) A_x ———— $\forall x \in \operatorname{Max} A$.

GOING UP & DOWN

Definition: Let $f: A \to B$ be a ring hom. We say that f satisfies the <u>going-up condition</u> if $\forall \mathfrak{p} \subset \mathfrak{p}'$ prime ideals in A and $\mathfrak{q}$ in B above $\mathfrak{p}$ (ie, in the fiber of $\mathfrak{p}$ by f^*), there exists $\mathfrak{q}'$ above $\mathfrak{p}'$ st $\mathfrak{q} \subset \mathfrak{q}'$.

$$\begin{array}{ccccc} \operatorname{Spec} B & & \mathfrak{q} & \subset & \exists\, \mathfrak{q}' \\ \downarrow f^* & & \downarrow & & \downarrow \\ \operatorname{Spec} A & & \mathfrak{p} & \subset & \mathfrak{p}' \end{array}$$

Analogously, we say that f satisfies the <u>going-down</u> condition if $\forall \mathfrak{p} \subset \mathfrak{p}'$ in A and $\mathfrak{q}'$ in B above $\mathfrak{p}'$, there exists $\mathfrak{q}$ above $\mathfrak{p}$ st $\mathfrak{q} \subset \mathfrak{q}'$.

$$\begin{array}{ccccc} \operatorname{Spec} B & & \exists\, \mathfrak{q} & \subset & \mathfrak{q}' \\ \downarrow f^* & & \downarrow & & \downarrow \\ \operatorname{Spec} A & & \mathfrak{p} & \subset & \mathfrak{p}' \end{array}$$

Lemma: Let $A \to B$ be an integral, injective morphism between integral domains. Then

$$A \text{ field} \iff B \text{ field}.$$

Corollary: Let $A \to B$ integral, $\mathfrak{q} \subset B$ prime. Then

$$\mathfrak{q} \text{ maximal} \iff A \cap \mathfrak{q} \text{ maximal}$$

Theorem (Going-up): Any integral morphism $A \to B$ satisfies the going-up.

Theorem (Going-down): Any integral morphism, with A, B domains and A integrally closed, satisfies the going down.

VALUATION RINGS

Definition Let K be a field and $\mathcal{O}, \mathcal{O}' \subset K$ local subrings with maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$ resp. We say that $\mathcal{O}'$ dominates $\mathcal{O}$ if $\mathcal{O} \cap \mathfrak{m}' = \mathfrak{m}$.

Consider Σ the set of all local subrings of K ordered by the dominance relation.

Theorem Let K be a field, and let $\mathcal{O} \subset K$ be a subring. The following conditions are equivalent:

1) $\mathcal{O}$ is a local subring which is a maximal element in Σ, and $\operatorname{Frac} \mathcal{O} = K$

2) If $x \in K^* \Rightarrow x \in \mathcal{O}$ or $x^{-1} \in \mathcal{O}$

3) There is a totally ordered abelian group Γ together with a map

$$v : K \longrightarrow \Gamma \cup \{\infty\}$$

satisfying

i) $v(xy) = v(x) + v(y)$

ii) $v(x+y) \geq \min(v(x), v(y))$

iii) $v(x) \geq 0 \iff x \in \mathcal{O}$

In such a case $\mathcal{O} = \{x \in K : v(x) \geq 0\}$ and $\operatorname{Frac} \mathcal{O} = K$

Definition: A ring $\mathcal{O}$ satisfying any of the previous conditions is called a valuation ring.

Examples: 1) $v_p : \mathbb{Q} \longrightarrow \mathbb{Z}$, $v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$, $a, b \in \mathbb{Z}$, with $v_p(a = p^n a') := n$ with a' not multiple of p. This is called the p-adic valuation.

2) More generally, if $\mathcal{O}$ is a local ring of maximal $\mathfrak{m}$ and $\operatorname{Frac} \mathcal{O} = K$, with the extra property that $a \in \mathfrak{m}^r - \mathfrak{m}^{r+1}$, $b \in \mathfrak{m}^s - \mathfrak{m}^{s+1} \Rightarrow ab \in \mathfrak{m}^{r+s} - \mathfrak{m}^{r+s+1}$, then

$v_{\mathfrak{m}}(a) :=$ maximum integer r s.t. $a \in \mathfrak{m}^r$ induces a valuation $v_{\mathfrak{m}}\left(\frac{a}{b}\right) := v_{\mathfrak{m}}(a) - v_{\mathfrak{m}}(b)$.

This is called the $\mathfrak{m}$-adic valuation.

1) is a particular case of 2) by setting $\mathcal{O} = \mathbb{Z}_{(p)}$ and $K = (\mathbb{Z}_{(p)})_{\mathbb{Z}_{(p)} - 0} \cong \mathbb{Z}_{\mathbb{Z} - 0} = \mathbb{Q}$.

V : NOETHERIAN AND ARTINIAN MODULES

Lemma: Let $(X, \leq)$ be a poset. Then these following are equivalent:

1) Ascending Chain Condition (acc): Every increasing chain (= sequence), of elements stabilizes: $\forall\ x_1 \leq x_2 \leq \dots\ \exists\, n \in \mathbb{N} : x_n = x_{n+1} = x_{n+2} = \dots$

2) Maximality Condition: Every non-empty subset of X has a maximal element.

Definition: Let M be an A-module, and let Σ be the set of submodules ordered by $\subseteq$.

a) M is Noetherian if every increasing chain in Σ stabilizes (ie, acc $\Leftrightarrow$ max. cond)

b) M is Artinian ——— decreasing ——————— (dcc)

Proposition: M Noeth $\Longleftrightarrow$ every submodule is finite generated.

Corollary: M Noeth $\Rightarrow$ M f.g.

Lemma: Let $0 \to M' \to M \to \overline{M} \to 0$ be a ses of A-mod.

$$\begin{matrix} M \text{ Noeth} & \Longleftrightarrow & M', \overline{M} \text{ Noeth} \\ \text{Art} & & \text{Art} \end{matrix}$$

Corollary:

1) Submodules of Noeth (Art) is Noeth (Art)
2) Quotients of Noeth (Art) is Noeth (Art)
3) Direct sum of Noeth (Art) is Noeth (Art)

- Recall that any ring A has a canonical str. of A-mod, and submodules $=$ ideals.

Definition: A ring A is called Noetherian (Artin) when it is Noeth (Art) as A-module, ie, when the set of ideals satisfies the acc (dcc).

Proposition: If A is Noeth (Artin), and M is a A-mod, then M Noeth (Art) $\iff$ M is finite generated

Examples 1) K field is Noeth & Art.

2) PID are Noeth, ie, $\mathbb{Z}$, $K[x]$, ...

3) Finite ab gps (as $\mathbb{Z}$-mod)

4) $K[x_1, x_2, \ldots]$ is not Noeth; neither is $\mathcal{C}(\mathbb{R})$.

Definition: A chain of submodules of M is a sequence

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq \cdots \subsetneq M_n = M$$

and its length is n. A composition series (cs) is a maximal chain, ie, st all M_i / M_{i-1} are simple: they are modules with no proper submodules.

Definition: The length of M is the smallest of the lengths of composition series on M.

In general $\mathbb{Z}/p\mathbb{Z}$ is simple (as they are fields).

Proposition: If M has a cs of length n $\Rightarrow$ all cs have length n and $\ell(M) = n$, and every chain can be extended to a composition series.

Proposition. M has a cs $\iff$ M is Noeth and Artin.

Theorem (Jordan-Holder): Any two cs of M have the same quotients M_i/M_{i-1} up to order.

Proposition Let E be a K-vs. Tfae:

1) E is finite dimensional

2) E has finite length

3) E is Noeth

4) E is Artin

and in such a case, dim = length.

Proposition. Let B be an A-algebra which is fg as A-mod. If A is Noeth $\Rightarrow$ B is Noeth.

Example. $\mathbb{Z}[i]$ is a fg $\mathbb{Z}$-alg, and $\mathbb{Z}$ Noeth $\Rightarrow$ $\mathbb{Z}[i]$ Noeth.

Proposition: A Noeth $\Rightarrow$ A_S Noeth, S multipl. system.

Theorem (Hilbert basis): A Noetherian $\Rightarrow$ $A[x]$ and $A[[x]]$ are Noetherians

Corollary: 1) A Noeth $\Rightarrow$ $A[x_1 \dots x_n]$ Noetherian

2) A Noeth $\Rightarrow$ any finite generated A-algebra B is Noeth

3) Every f.g ring is Noeth

4) Every f.g k-algebra is Noeth

Theorem (Weak Nullstellensatz): Let A be a f.g. k-algebra and let $\mathfrak{m}$ be a maximal ideal of A. Then $A/\mathfrak{m}$ is a finite field extension of k. In particular, if k is alg closed, $A/\mathfrak{m} \simeq k$.

PRIMARY DECOMPOSITION IN NOETHERIAN RINGS

Definition: An ideal $\mathfrak{a} \subset A$ is *irreducible* if $\mathfrak{a} = \mathfrak{b} \cap \mathfrak{c} \Rightarrow \mathfrak{a} = \mathfrak{b}$ or $\mathfrak{a} = \mathfrak{c}$.

Lemma: A Noeth $\Rightarrow$ every ideal is intersection of irreducible ideals.

Lemma: If A Noeth, then irreducible $\Rightarrow$ primary.

Theorem: In a Noetherian ring, every ideal has a primary decomposition.

Proposition: A Noeth $\Rightarrow$ $(\sqrt{\mathfrak{a}})^n \subset \mathfrak{a}$ for any ideal $\mathfrak{a} \subset A$, for some $n \geq 1$.

- For arbitrary rings, we saw that if $\sqrt{\mathfrak{a}}$ maximal $\Rightarrow$ $\mathfrak{a}$ primary.

Proposition: Let A be Noeth. TFAE:

1) $\mathfrak{a}$ is $\mathfrak{m}$-primary

2) $\sqrt{\mathfrak{a}} = \mathfrak{m}$

3) $\exists\, n > 0$: $\mathfrak{m}^n \subseteq \mathfrak{a} \subseteq \mathfrak{m}$.

Theorem (Uniqueness of prime ideals): Let A be Noeth. The prime ideals appearing in a primary decomposition do not depend on the decomposition.

ARTINIAN RINGS

Proposition: Let A be Artin. Then $\operatorname{Spec} A = \operatorname{Max} A$, and its cardinality is finite.

Definition. A *chain* of prime ideals is a sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n .$$

and we say that its length is n. The (Krull) dimension of A is the supremum of the lengths of chains of prime ideals.

Examples: 1) $\dim k = 0$, 2) $\dim \mathbb{Z} = 1$, 3) $\dim k[x] = 1$

4) $\dim \mathbb{Z}[x] = 2$, 5) $\dim k[x_1, x_2, \ldots] = \infty$ 6) $\dim \mathbb{Z}/n\mathbb{Z} = 0$ $(n \neq 0, \pm 1)$

Lemma: Let A be a ring such that the zero ideal is product of maximal ideals, $0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Then

$$A \text{ Noeth} \iff A \text{ Artinian}$$

Theorem: $\boxed{A \text{ Artin} \iff A \text{ Noeth} + \dim A = 0}$

Theorem (Classification of Artinian rings). Every Artinian ring decomposes, in a unique way up to order, as a finite direct product of local Artinian rings,

$$A \simeq \mathcal{O}_1 \times \cdots \times \mathcal{O}_m$$

Ex: $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{k_r}\mathbb{Z}$, $n = p_1^{k_1} \cdots p_r^{k_r}$.

VI : DEDEKIND DOMAINS AND DISC. VALUA. RINGS

• We'll focus on Noeth of dim 1 :

Proposition: Let A be a Noeth ring of dim 1. Every non-zero ideal decomposes, in a unique way up to order, as a product of primary ideals with different radicals.

Lemma: Let A be a domain of dim 1. Then

$$\operatorname{Spec} A = \operatorname{Max} A \amalg \{0\}.$$

• Recall that we said that even though in $\mathbb{Z}$ primary ideals are (p^n), $(p)^n$, primary ideals are not powers of primes. But when this is the case...

Definition: A Dedekind domain is a Noetherian domain of dim 1 st every primary ideal is a power of a prime ideal.

Examples: $\mathbb{Z}$, $k[x]$, DIP's in general.

Theorem: If A is Dedekind, every non-zero ideal factorizes uniquely (up to order) as product of prime ideals,

$$\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_r^{k_r}$$

Theorem: Let A be Noeth of dim 1. Tfae:

1) A Dedekind

2) A integrally closed

3) A_x is a discrete valuation ring $\forall x \in \operatorname{Spec} A$.

Proposition. Let $\mathcal{O}$ be a Noetherian, local ring of dim 1, and let $\mathfrak{m}$ be its max ideal. TFAE:

1) $\mathcal{O}$ discrete valuation ring

2) $\mathcal{O}$ int. closed

3) $\mathfrak{m}$ principal

4) $\dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$

Corollary: Every PID is Dedekind.

FRACTIONAL IDEALS

Definition: Let A be a domain and let $K = \operatorname{Frac} A$. A fractional ideal of A is a A-submodule $M \subseteq K$ such $\exists\ x \in A - 0 : xM \subseteq A$.

Examples: 1) $\mathfrak{a} \subset A$ ideal; 2) $u \in K$, then Au; 3) any finite gen. A-submodule of K.

Lemma. If A Noeth, every fractional ideal is a f.g. A-submodule.

Definition: A A-submodule $M \subset K$ is invertible if $\exists\ N \subset K : MN = A$.

Lemma: M invertible $\Rightarrow$ M finite-generated, and therefore fractional ideal.

Proposition: Let $M \subseteq K$ be a finite gen. A-submodule. Being invertible is a local property; i.e., TFAE

1) M invertible

2) M_x —— $\forall\ x \in \operatorname{Spec} A$

3) —— $\forall\ x \in \operatorname{Max} A$.

Proposition: Let $\mathcal{O}$ be a local integral domain.

$\mathcal{O}$ DVR $\Leftrightarrow$ every non-zero fractional ideal is invertible

Theorem: Let A be a domain

A Dedekind $\Leftrightarrow$ every non-zero fractional ideal is invertible

Lemma: M, N invertible $\Rightarrow MN$ invertible.

- That is, the set of invertible ideals forms an abelian gp. Moreover, every non-zero principal fractional ideal (u) is invertible (take (u^{-1})); and product is closed under multiplication: $(u)(u') = (uu')$.

Definition: The class group of A is the quotient

$$Cl(A) := \frac{\text{invertible ideals}}{\text{principal fractional ideals}}$$

VII : COMPLETIONS

Definition: A *top group* is a topological space G together with a gp structure s.t. $(x,y) \mapsto xy$, $x \mapsto x^{-1}$ are continuous.

Proposition: Let G be a top space. Tfae:

1) G is a top gp
2) G is a group object in Top
3) $\mathrm{Hom}(-,G) : \mathrm{Top}^{op} \to \mathrm{Set}$ factorizes by Gp.
$$\begin{tikzcd} \mathrm{Top}^{op} \arrow[r, dashed] \arrow[rr, bend left, "\mathrm{Hom}(-,G)"] & \mathrm{Gp} \arrow[r, "\text{forget}"] & \mathrm{Set} \end{tikzcd}$$

Lemma: If G is a top group, then $T_2 \Leftrightarrow T_1$.

- For a top space X, and $x \in X$, I will denote $\mathcal{U}(x) := \{\text{open nbhds of } x\} \subset \mathcal{V}(x)$.

Lemma Let G be a top gp and $H := \bigcap_{U \in \mathcal{U}(e)} U$. Tfae:

1) H is a subgroup
2) $H = \overline{\{e\}}$
3) G/H is Hausdorff
4) G Hausdorff $\Leftrightarrow H = \{e\}$

Warning: In what follows, we let G be an ab gp and 1st countable, and we let (G_n) be a *fundamental system* of e, ie, a base of nbhds of e st $G_n \subseteq G_{n-1}$, with the extra property that G_n are subgroups.

Lemma: The collection of nbhds of points $\{\mathcal{V}(x) : x \in X\}$ determine the topology on X.

Example: 1) $p^n\mathbb{Z} \subset \mathbb{Z}$, 2) $(x^n) \subset k[x]$, 3) $\mathfrak{a}^n \subset A$ ($\mathfrak{a}$ ideal)

4) $\mathfrak{a}^n M \subset M$ (M A-mod)

Definition: Let $\dots \xrightarrow{f_3} A_3 \xrightarrow{f_3} A_2 \xrightarrow{f_2} A_1$ be a sequence of ab groups (inverse system). The inverse limit or limit is the set of all coherent sequences,

$$\varprojlim A_n := \{ (a_i) \in \prod A_i \ : \ f_i(a_i) = a_{i-1} \}.$$

- We see $\varprojlim A_n$ as top space by endowing A_i with the discrete top and $\varprojlim A_i$ with the initial topology given by the projections $\pi_i : \varprojlim A_n \to A_i$.

Lemma: Let G be a top gp with fundamental system (G_n). The inclusions $G_n \hookrightarrow G_{n-1}$ induce maps $G/G_n \to G/G_{n-1}$; and each of $A_n := G/G_n$ has the discrete topology.

Definition. The completion of G is $\hat{G} := \varprojlim G/G_n$.

Example. $\widehat{K[x]} = K[[x]]$, namely $K[[x]] \longrightarrow \varprojlim_n K[x]/(x^n)$, $\sum_{i=0}^{\infty} a_i x^i \mapsto \left(\left[\sum_{i=0}^{n} a_i x^i \right] \right)$,

Lemma: the natural map

$$\begin{aligned} \varphi : G &\longrightarrow \hat{G} \\ g &\longmapsto (\bar{g})_n \end{aligned}$$

is continuous

Definition. G is complete when φ is an isomorphism of top gps.

- If $f : G \to H$ is a morphism of top gps, given $i \in \mathbb{N}$ by cont $\exists\, n_i \in \mathbb{N} : f(G_{n_i}) \subset H_i$ thus there is a cont map $\bar{f} : G/G_{n_i} \to H/H_i$. Then f induces a morphism between the completions,

$$\begin{aligned} \hat{f} : \hat{G} &\longrightarrow \hat{H} \\ (g_n) &\longmapsto \hat{f}(g_n)|_i := \bar{f}(g_{n_i}) \end{aligned}$$

and it does not depend on the choice of n_i, and it is well-def and cont.

Definition: A morphism of inverse systems $\varphi : (A_n, f_n) \to (B_n, g_n)$ is a sequence of maps $\varphi_n : A_n \to B_n$ s.t.

$$\begin{tikzcd} A_n \arrow[r, "\varphi_n"] \arrow[d, "f_n"'] & B_n \arrow[d, "g_n"] \\ A_{n-1} \arrow[r, "\varphi_{n-1}"] & B_{n-1} \end{tikzcd}$$

A sequence $A \to B \to C$ of inverse systems is exact when it is exact levelwise.

- If $A \xrightarrow{\varphi} B$ is a morphism of inverse systems, there is an induced maps $\varprojlim A_n \xrightarrow{\hat{\varphi}} \varprojlim B_n$,
  $\hat{\varphi}((a_n)) := (\varphi_n(a_n))_n$

Proposition: Taking inverse limit is a left-exact functor, i.e., if $0 \to A \to B \to C \to 0$ is exact, so then $0 \to \varprojlim A_n \to \varprojlim B_n \to \varprojlim C_n \to 0$ is ~~exact~~, left-exact

Moreover, if (A, f_n) is a surjective inverse limit (i.e., f_n is surj $\forall n$), then the previous seq is exact.

- If A is a ring and $\mathfrak{a}$ is an ideal, $(\mathfrak{a}^n)$ is a fund. system and $\hat{A} = \varprojlim A/\mathfrak{a}^n$ has a natural structure of ring with multiplication levelwise. If $\mathcal{O}$ is local, the "completion of $\mathcal{O}$" will mean of course completion at $\mathfrak{m}$.

Theorem (Cohen structure): Let $\mathcal{O}$ be a local, complete, Noeth ring containing a field as subring, and set $k = \mathcal{O}/\mathfrak{m}$. Then $\mathcal{O}$ is a quotient of $k[[x_1, \dots x_n]]$,

$$\mathcal{O} \simeq \frac{k[[x_1, \dots, x_n]]}{I}.$$

Example. If $\mathfrak{a} = (x_1, \dots, x_n)$, then $\widehat{k[x_1, \dots x_n]} = k[[x_1, \dots x_n]]$.

Lemma: Let A be a ring and $I, \mathfrak{a} \subset A$ ideals, ~~and~~ $\mathfrak{a}$ defining a fund. system. Then $\bar{\mathfrak{a}} = \mathfrak{a} A/I$ defines a fu. system and

$$\widehat{(A/I)} = \hat{A}/I$$

Corollary: let $0 \to G' \xrightarrow{i} G \xrightarrow{\pi} \bar{G} \to 0$ be a ses of gps, and let G_n be a fund system of G.
Then $(i^{-1}(G_n))$ and $\pi(G_n)$ are fund. syst of G' and $\bar{G}$, and the sequence of top gps

$$0 \to \hat{G'} \to \hat{G} \to \hat{\bar{G}} \to 0$$

is exact.

Corollary: $\hat{G}_n$ is a subgp of $\hat{G}$, and $\hat{G}/\hat{G}_n \simeq G/G_n$

Corollary: $\hat{G}$ is complete, ie, $\varphi: \hat{G} \to \hat{\hat{G}}$ is an isomph of top gp.

FILTRATIONS

Definition: A filtration on an A-mod M is a ~~seq~~ chain

$$\cdots \subseteq M_2 \subseteq M_1 \subseteq M_0 = M,$$

and if $\mathfrak{a} \subset A$ is an ideal, we say that it is an $\mathfrak{a}$-filtration if $\mathfrak{a} M_i \subseteq M_{i+1}$ $\forall i$ (when $\mathfrak{a} M_i = M_{i+1}$ for i large we say $\mathfrak{a}$-stable filtration)

Lemma: Stable $\mathfrak{a}$-filtrations have "bounded difference", ie, if $(M_n)(M_n')$ are M then

$$M_{k+i} \subseteq M_i', \quad M_{k+i}' \subseteq M_i, \quad \text{for some } k \in \mathbb{N}.$$

In particular, all stable $\mathfrak{a}$-filt. on M determines the same topology.

GRADED RINGS AND MOD

Definition: A graded ring is a ring A together with a collection (A_i) of ~~subrings~~ subgps st $A_i A_j \subset A_{i+j}$ and $\bigoplus A_i \to A$ is an isomphm.

If A is graded, an A-mod M is graded if $M = \bigoplus M_i$ and $A_i M_j \subset M_{i+j}$.

Proposition: let A be a graded ring.

$$A \text{ Noeth} \iff A_0 \text{ Noeth and } A \text{ is a finite-gen } A_0\text{-algebra}.$$

Definition: let A be a ring and $\mathfrak{a} \subset A$. The blow-up algebra is $A^* := \bigoplus_{n\geq 0} \mathfrak{a}^n$. $(\mathfrak{a}^0 = A)$
For an A-mod M and a $\mathfrak{a}$-filtration M_n, $M^* := \bigoplus M_n$ is A^*-module.

Theorem (Artin-Rees): let A be Noeth, $\mathfrak{a} \subset A$ and M A-mod, $M' \subset M$ submod.

Then the filtrations $(\mathfrak{a}^n M')$ and $((\mathfrak{a}^n M) \cap M')$ have bounded difference, thus induce the same top on M.

Corollary (Exactness of completions): If $0 \to M' \to M \to \overline{M} \to 0$ is exact, so is the sequence of $\mathfrak{a}$-adic completions

$$0 \to \hat{M}' \to \hat{M} \to \hat{\overline{M}} \to 0.$$

Theorem: If A is Noeth and M is f.g., then $\hat{A} \otimes_A M \simeq \hat{M}$

Corollary: $\hat{A}$ is flat as A-mod, i.e., $\hat{A} \otimes - : \mathrm{Mod}_A \to \mathrm{Mod}_A$ is exact.

COMPLETIONS OF LOCAL RINGS

Proposition: $\mathcal{O}$ local with maximal $\mathfrak{m}$ $\Rightarrow$ $\hat{\mathcal{O}}$ local with maximal $\hat{\mathfrak{m}}$

Theorem (Krull): let A be Noeth, $\mathfrak{a} \subset A$, and let M be an A-mod. Then

$$\mathrm{Ker}\,(M \xrightarrow{\varphi} \hat{M}) = \bigcap_{n\geq 0} \mathfrak{a}^n M = \{x \in M : (1+a)x = 0 \text{ for some } a \in \mathfrak{a}\}$$

Corollary: If $\mathcal{O}$ is local Noetherian, then

$$\mathrm{Ker}\,(\mathcal{O} \to \hat{\mathcal{O}}) = \bigcap_{i\geq 0} \mathfrak{m}^i = 0.$$

Eg: $\mathcal{O}_x$ ring of germs is not Noeth

Theorem: A Noeth $\Rightarrow$ $\hat{A}$ Noeth

VIII DIMENSION THEORY

• Let A be a graded Noeth ring, ie, A_0 Noeth and A fg A_0-alg, say generated by $x_1, \dots, x_s$ elements of degree $k_i = \deg x_i$. Let M be a fg A-mod, and graded, so M_n is a fg A_0-mod.

<u>Definition</u>: Let λ be an additive function on fg modules with values in $\mathbb{Z}$. The <u>Poincaré series</u> of M wrt λ is

$$P(M,t) := \sum_{n=0}^{\infty} \lambda(M_n)\, t^n \in \mathbb{Z}[[t]].$$

<u>Theorem</u> (Hilbert-Serre): The Poincaré series is a rational function of the form

$$P(M,t) = \frac{p(t)}{\prod_{i=1}^{s} (1-t^{k_i})}, \qquad p(t) \in \mathbb{Z}[t]$$

<u>Corollary</u>: If $k_i = 1\ \forall i$, then for $n \gg 0$, $\lambda(M_n)$ is a polynomial in n with coeff. in $\mathbb{Q}$ of degree $d-1$, called <u>Hilbert polynomial</u>.

<u>DIMENSION THEORY FOR NOETH LOCAL RINGS</u>

• Let $\mathcal{O}$ be Noeth local and $\mathfrak{q}$ a $\mathfrak{m}$-primary ideal.

<u>Proposition</u>: Let M be a fg $\mathcal{O}$-mod and let (M_n) be a stable $\mathfrak{q}$-filtration.

1) M/M_n has finite length $\forall n$
2) For $n \gg 0$, $\ell(M/M_n)$ is a polynomial in n, of degree $\min(\#\text{gen of } \mathfrak{q})$
3) The degree of the leading coefficient does not depend on the choice of the filtration.

<u>Definition</u>: The <u>characteristic polynomial</u> is the polynomial $\chi(n) = \ell(M/\mathfrak{q}^n M)$, $n \gg 0$, coming from the filtration $M_n = \mathfrak{q}^n M$.

Corollary: $\ell(\mathcal{O}/q^n)$, $n>>0$, is a polynomial in n of degree $\leq \min(\#\text{gen of } q)$.

Proposition: $\deg \chi_q(n) = \deg \chi_m(n)$, where q is m-primary.

- Set $d(\mathcal{O})$ for the common degree of $\chi_m(n)$, $n>>0$.

- For $(\mathcal{O}, m)$ Noeth local, we have 3 invariants:

  (a) $\dim \mathcal{O}$

  (b) $d(\mathcal{O})$

  (c) $\delta(\mathcal{O}) :=$ least number of generators of an m-primary ideal.

Theorem: $\dim \mathcal{O} = d(\mathcal{O}) = \delta(\mathcal{O})$.

Corollary: Let $\mathcal{O}$ be a Noeth local ring with max. m.

1) $\dim \mathcal{O} = \dim \hat{\mathcal{O}} < \infty$

2) If $x \in \mathcal{O}$ is neither invertible nor zero-divisor, then

$$\boxed{\dim \mathcal{O}/(x) = \dim \mathcal{O} - 1}$$

3) $\dim \mathcal{O} \leq \dim_{\mathcal{O}/m} m/m^2$.

theorem (Krull's principal ideal): Let A be Noeth and let $x \in A$ be neither invertible nor zero divisor. Then every minimal prime of (x) has height 1, ie, for every p minimal in $(x)_0$,

$$\dim A_p = 1.$$

example: $\dim \dfrac{k[x_1 \cdots x_n]}{(f)} = n-1$, f neither zero nor invertible

Proposition: If A Noeth, then $\boxed{\dim A[x_1 \cdots x_n] = \dim A + n}$

REGULAR LOCAL RINGS

Definition. Let $\mathcal{O}$ be Noeth local of dim. $\mathcal{O} = d$. We say that $\mathcal{O}$ is regular if $\dim_{\mathcal{O}/m} m/m^2 = d$

- Set $G(\mathcal{O}) := \bigoplus_{k=0}^{\infty} m^k/m^{k+1}$

Theorem: Let $\mathcal{O}$ be Noeth local. TFAE:

1) $\mathcal{O}$ regular
2) $G(\mathcal{O}) \simeq k[x_1, \dots, x_d]$
3) m is generated by d elements

Proposition: A Noeth $\Rightarrow A[[x_1, \dots, x_n]]$ Noeth (in particular $k[[x_1 - x_n]]$)

Proposition: $\mathcal{O}$ Regular $\Rightarrow \mathcal{O}$ domain

Proposition: Let $\mathcal{O}$ be Noeth local of dim 1

$$\mathcal{O} \text{ regular} \Leftrightarrow \mathcal{O} \text{ DVR}$$

Proposition: $\mathcal{O}$ Noeth local, then $\mathcal{O}$ regular $\Leftrightarrow \hat{\mathcal{O}}$ regular.

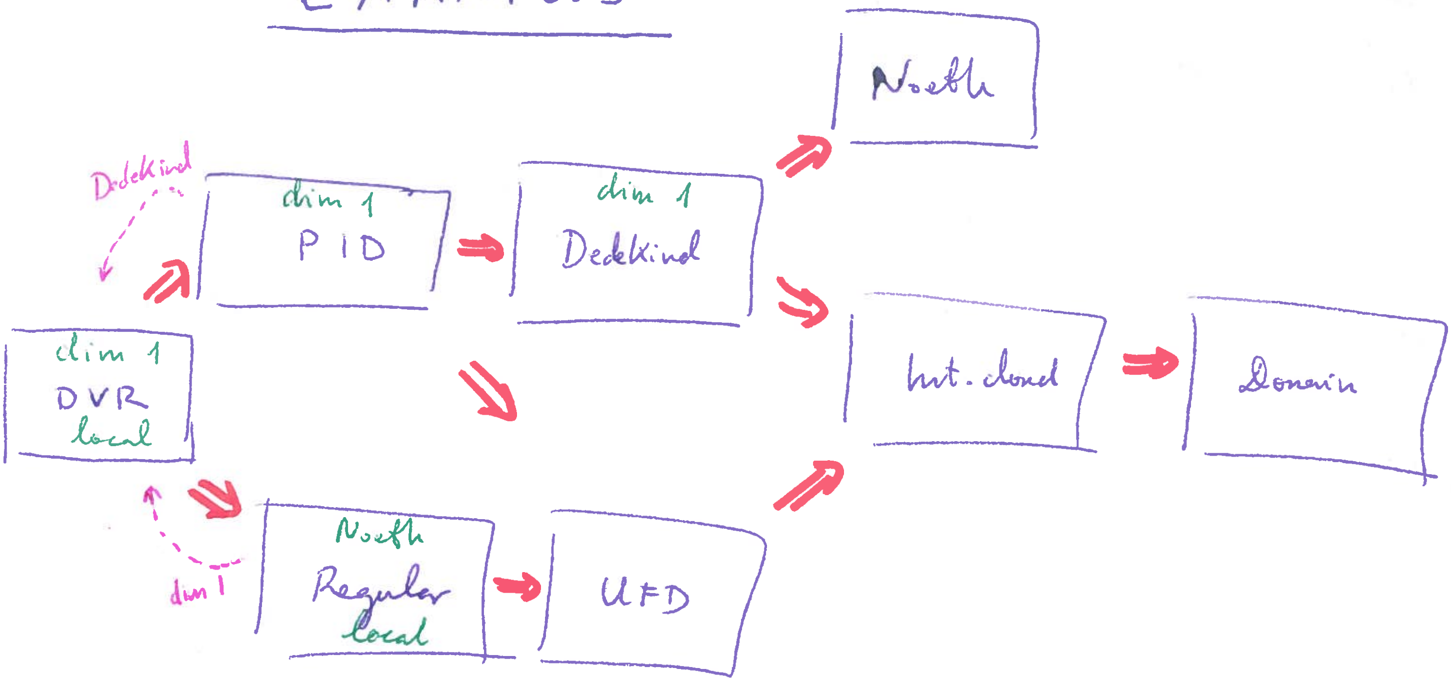
Lemma: A ring, m maximal, then $\hat{A} \simeq \hat{A}_m$ are regular (with the m-adic completion)

- $\dfrac{1}{(1-t)^s} = \sum_{n=0}^{\infty} \dfrac{(s+n-1)!}{(s-1)!\,n!} t^n$

- For the m-adic completion, $\chi_m(n) \underset{n \gg 0}{=} \ell(A/m^n) = \sum_{i=0}^{n-1} \dim(m^i/m^{i+1})$

- For an arithmetic series $a_n = a_1 + (n-1)K$, then $\sum_{i=1}^{n} a_i = \dfrac{n(a_1 + a_n)}{2}$.

EXAMPLES



- Lemme Gauss : A UFD $\Rightarrow$ $A[x]$ UFD & A_S UFD
- $\mathfrak{m} \subset A$ max, then $A/\mathfrak{m}^k$ local.
- $\mathcal{O}$ Noeth local domain dim 1, then

  int closed $\Leftrightarrow$ Dedekind $\Leftrightarrow$ DVR $\Leftrightarrow$ $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$.
- Hilbert Basis : A Noeth $\Rightarrow$ $A[x_1 .. x_n]$, $A[[x_1 .. x_n]]$ Noeth
- $\boxed{\text{Artin}}$ = Noeth of dim 0.
- $\mathcal{O}$ Noeth local dim 1, then

  DVR $\Leftrightarrow$ regular.
- A Noeth, $\dim A[x_1 \ldots x_n] = \dim A + n$

  $\dim \dfrac{k[x_1 .. x_n]}{(f)} = n-1$, f neither 0 nor invertible

- $\mathfrak{m} \subset A$, $\hat{A}$ the $\mathfrak{m}$-adic compl is <u>local</u>, as $\hat{A} \simeq \hat{A}_{\mathfrak{m}}$
- $(\widehat{A/I}) = \hat{A}/I$
- $\dim \mathcal{O} \le \dim_{\mathcal{O}/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$, and $\boxed{\text{Regular}}$ means that it is $=$.
- $\boxed{\text{Dedekind}}$ $=$ Noeth, dom, dim 1 $+$ <u>A int. closed</u> (can be checked!)
- $\boxed{\text{DVR}}$ $=$ Dedekind $+$ PID

- <u>PID</u> : k, $\mathbb{Z}$, $k[x]$, $\mathbb{Z}[i]$
- <u>Local</u> : $A_{\mathfrak{p}}$, $A/\mathfrak{m}^k$, k, $k[x_1, x_2, \dots]$, $\mathcal{O}/I$, $\mathcal{O}_x$, $k[\![x_1 \dots x_n]\!]$, $\hat{A}$ $\mathfrak{m}$-adic compl
- <u>Noeth</u> : $\mathbb{Z}$, $k[x]$, k-EV, direct sums, localiz, quotient, subrings, poly. ring
- <u>Artin</u> : $\mathbb{Z}/n\mathbb{Z}$, $k[x]/(x^n)$, k
- <u>Dim</u> :
  - 0 : k, $\mathbb{Z}/n\mathbb{Z}$, $\dfrac{k[x_1, x_2, \dots]}{(x_1, x_2, \dots)}$
  - 1 : $\mathbb{Z}$, $k[x]$, $k[\![x]\!]$
  - 2 : $\mathbb{Z}[x]$, $k[x,y]$, $k[\![x,y]\!]$
  - $\vdots$
  - n : $k[x_1 \dots x_n]$
- <u>Dedekind</u> : $\mathbb{Z}$, $k[x]$, $k[\![x]\!]$,
- <u>Regular</u> : $\left(\dfrac{\mathbb{Z}[x,y]}{(xy - p)}\right)_{(x,y,p)}$
- <u>Complete</u> : $k[\![x]\!]$, quotients of $k[\![x_1 \dots x_n]\!]$, Artin local

  $\wedge$ preserves quotients, local, noeth, exactness
- DVR : $\mathbb{Z}_p$, $k[\![x]\!]$