PMATH 646: INTRODUCTION TO COMMUTATIVE ALGEBRA NOTES

HEESUNG YANG

1. January 06

Throughout this course, we will assume that R is a commutative ring with unity 1.

Proposition 1.1 (Zorn's lemma)**.** *$(\mathscr{S}, \leq)$ is a partially ordered set, and suppose that for $(s_\alpha)_{\alpha \in J}$, we have $\alpha <_J \beta \Rightarrow s_\alpha \leq_{\mathscr{S}} s_\beta$. If it exists $s \in S$ such that $s \geq s_\alpha$ for all $\alpha \in J$ then $\mathscr{S}$ has a maximal element.*

Remark 1.1. In this course, we will use Zorn's lemma mostly with $\mathscr{S}$ = collection of ideals in a ring R, with $\leq$ given by $\subseteq$. For instance, if R is a non-trivial ring (i.e., $0 \neq 1$, then R has a maximal ideal. In fact, if I is a proper ideal of R then there exists a maximal ideal M such that $I \subseteq M$.

Proof of the above remark. Let $\mathscr{S} = \{J \subseteq R : J \text{ ideal}, I \subseteq J \subsetneq R\}$. If I is a proper ideal of R, then $I \in \mathscr{S}$ so $\mathscr{S} \neq \emptyset$. Notice that if X is a totally ordered set and $\{I_\alpha\}_{\alpha \in X}$ isa chain in $\mathscr{S}$ (i.e., $\alpha <_X \beta \Rightarrow I_\alpha \subseteq I_\beta$), then $\bigcup_{\alpha \in X} I_\alpha =: J \supseteq I$. If $a, b \in J$, then there exists $\alpha, \beta \in X$ such that $a \in I_\alpha$ and $b \in I_\beta$ with either $I_\alpha \subseteq I_\beta \Rightarrow a, b \in I_\beta \Rightarrow a + b \in I_\beta \subseteq J$ or $\beta \leq_X \alpha \Rightarrow I_\beta \subseteq I_\alpha \Rightarrow b, a \in I_\alpha \Rightarrow b + a \in I_\alpha \subseteq J$.

If $\alpha \in J, r \in R$ then there exists $\alpha \in X$ such that $a \in I_\alpha \Rightarrow ra \in I_a \subseteq J$. So J is an ideal and $J \supseteq I$. To show that $J \in \mathscr{S}$ we must show that $J \subsetneq R$. But this follows from the fact that if $J = R$ then $1 \in J$ hence $1 \in I_\alpha$ for some α, which is a contradiction. Hence we can conclude that every chain in $\mathscr{S}$ has an upper bound, so by Zorn's lemma there exists a maximal ideal $M \in \mathscr{S}$. Thus $M \supseteq I$. If there is another maximal ideal M' such that $M \subsetneq M' \subsetneq R$ then $M \in \mathscr{S}$ and $M' \supsetneq M$, contradicting the maximality. Thus M must be the only maximal ideal, as required. □

Example 1.2. Take R to be an abelian group that does not have a maximal proper subgroup. For instance, let $R = \{\alpha \in \mathbb{C}^* : \text{ there exists } m \geq 1 \text{ such that } \alpha^{2^m} = 1\}$. Observe that any proper subgroup of R is finite, so we can always make any proper subgroup bigger. Thus R has no maximal proper subgroups. To make R into a ring without unity, we will define addition ($\oplus$) and multiplication ($\odot$) as $r \odot s = 1$ (here, 1 is actually the additive identity 0) and $r \oplus s = r \cdot s$. This R has no maximal ideals. Thus, for our above argument to work, we need R to have unity.

Theorem 1.3 (Chinese remainder theorem for rings)**.** *Let R be a commutative ring with* 1 *and $I_1, \ldots, I_k \subseteq R$ ideals satisfying*

$$\bigcap_{i=1}^{k} I_i = (0) \text{ and } I_i + I_j = R \text{ whenever } i \neq j$$

Date: 6 April 2015.

(in other words, the I_i are pairwise comaximal*). Then we have*

$$R \cong \prod_{i=1}^{k} R/I_i.$$

Definition 1.4. Let R be a ring. Then an *R-module* M is just an abelian group $(M, +)$ endowed with a map $R \times M \to M$ defined as $(r, m) \mapsto rm$ satisfying, for $r \in R$ and $m, n \in M$:

(1) $r \cdot (s \cdot m) = (rs) \cdot m$
(2) $r(m + n) = rm + rn$
(3) $(r + s)m = rm + sm$
(4) $1_R m = m$.

Example 1.5. If $R = \mathbb{F}$ a field and V is an $\mathbb{F}$-module, then V is an $\mathbb{F}$-vector space. If $R = \mathbb{Z}$, then M is an abelian group.

Example 1.6. If $R = \mathbb{R}[x]$ and a $M = \mathbb{C}$, define $p(x) \cdot \lambda = p(i) \cdot \lambda$.

Definition 1.7. Let R be a ring and M an R-module. Then the *annihilator of M* denoted by $\mathrm{Ann}_R(M)$ is defined to be

$$\mathrm{Ann}_R(M) = \{r \in R : rm = 0 \text{ for all } m \in M\}.$$

Remark 1.2. $\mathrm{Ann}_R(M)$ is an ideal of R. If $r, s \in \mathrm{Ann}_R(M)$ implies that $(r + s) \cdot m = r \cdot m + s \cdot m = 0_M + 0_M = 0_M$ for all $m \in M$. If $a \in \mathrm{Ann}_R(M)$ and $r \in R$, then $(ra)m = r(am) = r \cdot 0_M = 0_M$. It is trivially true that $0_R \in \mathrm{Ann}_R(M)$.

Remark 1.3. If $S = R/\mathrm{Ann}_R(M)$ then M has the structure of an S-module. Indeed, if $s \in S$ and $s = r + \mathrm{Ann}_R(M)$ and we define $s \cdot m := r \cdot m$ then the given multiplication is well-defined by the annihilator's property.

2. January 08

Recall that if $I = \mathrm{Ann}(M)$, then M inherits a structure as an R/I-module. If $r \equiv s \pmod{I}$, then $r - s \in I$, or $(r - s) \cdot m = 0$ for all $m \in M$. Therefore $r \cdot m = s \cdot m$. Therefore, M gets an R/I-module structure via the rule $(r + I) \cdot m := r \cdot m \in M$.

Definition 2.1. An R-module M is *faithful* if $\mathrm{Ann}_R(M) = (0)$.

Remark 2.1. If $I = \mathrm{Ann}_R(M)$, then M is a faithful R/I-module.

Definition 2.2. If $N \subseteq M$ and M is an R-module and N is an R-module, then we will call N an R-submodule of M if:

(1) $n_1, n_2 \in N$ implies $n_1 + n_2 \in N$;
(2) $r \in R, n \in N$ implies $r \cdot n \in N$; and
(3) $0_M \in N$.

Remark 2.2. Some remarks on modules and submodules:

(1) R is an R-module.
(2) If I is an ideal of R, then I is an R-submodule of R.

(3) If M is an R-module and I is an ideal of R, then we can construct an R-submodule IM of M, where

$$IM = \left\{ \sum_{i=1}^{n} x_i m_i : x_i \in I, m_i \in M \right\}.$$

(4) If $N \subseteq M$ is an R-submodule of M, we can form a quotient module $M/N = \{m+N : m \in M\}$, where

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N \text{ and } r(m + N) = rm + N.$$

Definition 2.3. If R is a ring and M, N are two R-modules, then we say that a map $f : M \to N$ is an *R-module homomorphism* if:

(1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ for all $m_1, m_2 \in M$
(2) $f(rm) = rf(m)$ for all $r \in R$ and $m \in M$.

Remark 2.3. More facts about modules:

(1) $\ker(f) = \{m \in M : f(m) = 0\} \subseteq M$ is a submodule.
(2) $\mathrm{im}(f) = \{f(m) : m \in M\} \subseteq N$ is a submodule.
(3) $\ker(f) = (0)$ iff f is injective
(4) $\mathrm{im}(f) = N$ iff f is surjective
(5) If $f : M \to M'$ is a surjective R-module homomorphism, then $M/\ker(f) \cong M'$ ("First isomorphism theorem").

Definition 2.4. For two R-modules M and N, define

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

If $f : M \to M$, then f is said to be an *endomorphism*, and we write

$$\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M, M).$$

Remark 2.4. Notice that $\mathrm{Hom}_R(M, N)$ is itself an R-module, where $(f + g)(m) := f(m) + g(m)$ and $(rf)(m) := rf(m) = f(rm)$. Then it is a straightforward verification. If $M = N$, then $\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M, M)$ is a ring. Define the composition map $\circ$ as multiplication.

Example 2.5. If $R = \mathbb{C}$ and $M = \mathbb{C}^{2\times 1}$ and $N = \mathbb{C}^{3\times 1}$, then $\mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^2, \mathbb{C}^3) = \mathrm{M}_{3\times 2}(\mathbb{C})$. Similarly, if $R = \mathbb{C}$ and $M = \mathbb{C}^2$, then $\mathrm{End}_{\mathbb{C}}(\mathbb{C}^2) \cong \mathrm{M}_2(\mathbb{C})$.

Definition 2.6. A module M is *simple* if (0) and M are its only R-submodules.

Definition 2.7. We call D a *division ring* if every non-zero element of D has a multiplicative inverse. Note that a division ring *need not be commutative*. Thus, a commutative division ring is a field.

Lemma 2.8 (Schur's lemma)**.** *If M is a simple R-module then $\mathrm{End}_R(M)$ is a division ring.*

2.1. **Direct sum and direct product.**

Definition 2.9. Let X be an index set and $\{M_\alpha\}_{\alpha\in X}$ is a collection of R-modules. Then *the direct sum of M_α* is defined as

$$\bigoplus_{\alpha\in X} M_\alpha = \{(m_\alpha)_{\alpha\in X} : m_\alpha \in M_\alpha \text{ and } \{\alpha \in X : m_\alpha \neq 0\} \text{ is finite}\}$$

The *direct product* of M_α is

$$\prod_{\alpha \in X} M_\alpha = \{(m_\alpha)_{\alpha \in X} : m_\alpha \in M_\alpha\}.$$

Clearly, we have $\bigoplus M_\alpha \subseteq \prod M_\alpha$.

Example 2.10. Suppose $R = \mathbb{Z}$. Then is $M_1 \cong M_2$ as modules, where

$$M_1 := \bigoplus_{i=1}^{\infty} \mathbb{Z}, M_2 := \prod_{i=1}^{\infty} \mathbb{Z}?$$

The answer is *no*, since M_1 is countable while M_2 is uncountable. Therefore M_1 and M_2 have different cardinality.

Definition 2.11. An R-module M is called *free* if there exists a set X such that

$$M \cong \bigoplus_{i \in X} R.$$

More intuitively, M is free if there exists a subset $\mathcal{B} = \{m_x : x \in X\} \subseteq M$ ("basis") such that every element of M has a unique expression

$$m = \sum_{x \in X} r_x m_x \text{ where } r_x = 0 \text{ for all but finitely many } x \in X.$$

Remark 2.5. To see the equivalence, let $e_y \in \bigoplus_{x \in X} R$ and $y \in X$ be the sequence with a 1 in the y-th coordinate and zeroes everywhere else. Then

$$f : \bigoplus_{x \in X} R \to M, f((r_x)_{x \in X}) = \sum_{x \in X} r_x m_x$$

is bijective.

Question (Hard question)**.** Is $\prod_{i=1}^{\infty} \mathbb{Z}$ a free $\mathbb{Z}$-module? (Answer: No. You will prove this in Assignment #1.)

Remark 2.6. If R is a field, then every R-module is free (Zorn's lemma exercise!). But if $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$, then M is *not* free. Note that, since $2 \cdot m = 0 \cdot m$ for all $m \in M$, there can be no *unique* representation of m. That is, we can get a (non-empty) spanning set, but it is not linearly independent.

Definition 2.12. We will write that $R^X := \bigoplus_{x \in X} R$ and if $|X| = n < \infty$, then we write $R^n := \bigoplus_{i=1}^{n} R$. If $R = R^X$, then we call $|X|$ the *rank* of the free module M.

Remark 2.7. We cannot answer this yet, but it is indeed true that the rank is well-defined, i.e., $R^n \cong R^m$ implies $n = m$. Note that the rank is well-defined only when R is commutative. If R is non-commutative, one can construct an example where $R \cong R^2$.

3. January 09

3.1. Exact sequences.

Definition 3.1. Suppose that M, M', M'' are R-modules, and let $f : M'' \to M$ and $g : M \to M'$. Then the sequence $M'' \xrightarrow{f} M \xrightarrow{g} M'$ is said to be *exact at* M if $\mathrm{im}(f) = \ker(g)$. More generally, if

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_n} M_{n+1},$$

then the sequence is exact if $\mathrm{im}(f_i) = \ker(f_{i+1})$ for all $i = 1, 2, \ldots, n-1$. More specifically, an exact sequence of the form

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

is called a *short exact sequence*.

Remark 3.1. If the sequence

$$0 \to M'' \xrightarrow{f} M \xrightarrow{g} M' \to 0 \tag{1}$$

is short exact, then:

(a) $0 \to M'' \xrightarrow{f} M$ is exact, so f is injective, and $\mathrm{im}(0 \to M'')$ is)). So we have $(0) = \ker(f)$, so f is indeed injective.
(b) $M'' \xrightarrow{f} M \xrightarrow{g} M'$ is exact, so $\mathrm{im}(f) = \ker(g)$.
(c) $M \xrightarrow{g} M' \to 0$ is exact, so $\mathrm{im}(g) = \ker(M' \to 0) = M'$. Thus g is surjective.

If (1) is short-exact, then $M/f(M'') \cong M'$ as R-modules, by the first isomorphism theorem. Indeed, note that $g : M \to M'$ is surjective, $M/\ker(g) \cong \mathrm{im}(g) = M'$. But $\ker(g) = \mathrm{im}(f) = f((M'')$ so $M/f(M'') \cong M'$.

Example 3.2. If M and N are R-modules, then the mappings

$$i : M \hookrightarrow M \oplus N, \pi_2 : M \oplus N \to N$$

defined as $i(m) = (m, 0)$ and $\pi_2(m, n) = n$ give a short exact sequence

$$0 \to M \xrightarrow{i} M \oplus N \xrightarrow{\pi_2} N \to 0.$$

Example 3.3. Consider the short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z} \xrightarrow{g} \mathbb{Z}/2\mathbb{Z} \to 0,$$

where $f(n) = 2n$ and $g(n) = n + 2\mathbb{Z}$. But note that we have $\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \ncong \mathbb{Z}$.

3.2. Splitting.

Definition 3.4. A short-exact sequence

$$0 \longrightarrow M'' \xrightarrow{f} M \underset{\tau}{\overset{g}{\rightleftarrows}} M' \longrightarrow 0$$

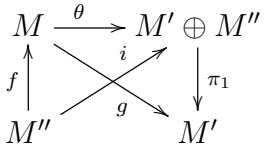
is said to *split* if there exists an R-module homomorphism $\tau : M \to M$ such that $g \circ \tau = \mathrm{id}_M$.

Lemma 3.5 (Splitting lemma)**.** *If*

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

is a short exact sequence, then the following are equivalent:

(1) there exists an R-module isomorphism $\theta : M \to M' \oplus M''$ such that
  (a) $\theta \circ f(m'') = (0, m'')$ for all $m'' \in M''$ and
  (b) $\pi_1 \circ \theta(m) = g(m)$ for all $m \in M$.
(2) there exists $\tau : M' \to M$ such that $g \circ \tau = \mathrm{id}_{M'}$.
(3) there exists $\sigma : M \to M''$ such that $\sigma \circ f = \mathrm{id}_{M''}$.



Proof. ((1) $\Rightarrow$ (2)) Suppose we have the map $\theta : M \to M' \oplus M''$. We want to construct a map $\tau : M' \to M$. Do this via $\tau(m') = \sigma^{-1}(m', 0)$. Then $g \circ \tau(m') = g(\theta^{-1}(m', 0)) \stackrel{?}{=} m'$. But then $\pi_1 \circ \theta(m) = g(m)$, so we can plug in $m = \theta^{-1}(m', 0)$. Thus $\pi_1(\theta(\theta^{-1}(m', 0)) = g(\theta^{-1}(m', 0)) = \pi_1(m', 0) = m'$.

((1) $\Rightarrow$ (3)) We have θ and want to construct $\sigma M \to M''$. Define $\sigma(m) := \pi_2(\theta(m))$. Now need to verify: $\sigma \circ f = \mathrm{id}''_M$, i.e., we must show that $\sigma(f(m'')) = m''$, and $\pi_2(\theta(f(m'))) = \pi_2 \circ i(m'') = \pi_2(0, m'') = m''$.

((3) $\Rightarrow$ (1)) We want to define $\theta : M \to M' \oplus M''$. Define $\theta(m) = (g(m), \sigma(m))$, where

$$0 \longrightarrow M'' \underset{\sigma}{\overset{f}{\rightleftarrows}} M \xrightarrow{g} M' \longrightarrow 0$$

We need $\pi_1(g(m), \sigma(m)) = \pi_1(\theta(m)) \stackrel{?}{=} g(m)$ and $\sigma \circ f(m'') = (0, m'')$. But then by exactness, $(g(f(m'')), \sigma \circ f(m'') = (0, m'')$.

((2) $\Rightarrow$ (1)) This time define instead $\psi : M' \oplus M'' \to M$ by $\psi(m', m'') = \tau(m') + f(m)$.

$$0 \longrightarrow M'' \xrightarrow{f} M \underset{\tau}{\overset{g}{\rightleftarrows}} M' \longrightarrow 0$$

We claim that ψ is an isomorphism. For injectivity, consider $\ker(\psi)$. Notice that if $\tau(m') + f(m) = 0$ and we apply g, then $g \circ \tau(m') + g \circ f(m'') = 0$. But by exactness, we have $g \circ f(m'') = 0$ and $g \circ \tau(m') = m'$. Hence $m' = 0$ (by injectivity of f), as required. Now we need to show surjectivity. Pick $m \in M$. We must show that there exists $m'' \in M''$ and $m' \in M'$ such that $m = \tau(m') + f(m'')$. Apply g to get $g(m) = m'$. Notice that $m - \tau(m') = m - \tau(g(m)) = f(m'')$ for some m, since $m - \tau(g(m)) \in \ker g = \mathrm{im}\, f$. So there exist m', m'' such that $\psi(m, m'') = m$.

Now define $\theta(m) = \psi^{-1}(m)$. Check if $\pi_1 \circ \psi^{-1}(m) = g(m)$ and $\psi^{-1} \circ f(m'') = (0, m'')$. This is a straightforward verification. □

4. January 13

Note that if $M \cong M'' \oplus M'$ and

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

is a short exact sequence, we *do not necessarily have* a section for g or f.

Example 4.1. If $R = \mathbb{Z}$ and $M' = (\mathbb{Z}/2\mathbb{Z})^\omega, M'' = \mathbb{Z}, M = \mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^\omega$, then clearly $M \cong \mathrm{M}'' \oplus M'$. Let $f : M'' \to M, g : M \to M'$ such that $f(n) = (2n, 0, 0, 0, 0, \dots)$ and $g(n, \varepsilon_1, \varepsilon_2, \varepsilon_3, \dots) = (n + 2\mathbb{Z}, \varepsilon_1, \varepsilon_2, \varepsilon_3, \dots)$. Then the given sequence is exact. But note that

g does not have a section, i.e., there cannot exist $\tau : M' \to M$ such that $g \circ \tau = \mathrm{id}_{M'}$, since every element in $(\mathbb{Z}/2\mathbb{Z})^\omega$ has order 2, but M is torsion-free ($\mathbb{Z}$ cannot have any torsion element). Notice that $g \circ \tau(1, 0, 0, \dots) = (0, *, *, *, \dots)$, so $g \circ \tau$ cannot possibly be $\mathrm{id}_{M'}$.

4.1. **Structure theorem for modules over a PID.**

Definition 4.2. An R-module M is called *cyclic* if there exists $m \in M$ such that $M = Rm$.

Example 4.3. If $R = \mathbb{Z}$, then $N = \mathbb{Z}/5\mathbb{Z} = \langle 1 + 5\mathbb{Z} \rangle$ is cyclic, but $M = \mathbb{Z} \oplus \mathbb{Z}$ is not.

Remark 4.1. If M is cyclic with $M = Rm$, we have an R-module homomorphism $\varphi : R \to M$ is surjective, and is given by $\varphi(r) = rm$. Then $I := \ker \varphi$ is an ideal of R, and by the fist isomorphism theorem, $R/I \cong M$ as *modules*. Note that $I = \mathrm{Ann}_R(M)$.

Definition 4.4. Let R be a ring and let M be an R-module. Recall that M is a *finitely-generated R-module* if there exist $d \geq 1$ and $m_1, \dots, m_d \in M$ such that $M = Rm_1 + Rm_2 + \cdots + Rm_d$.

Theorem 4.5 (Structure theorem for finitely-generated modules over a PID)**.** *Let R be a PID and let M be a f.g. R-module. Then there exists* unique *$d \geq 0$ and some prime elements $\pi_1, \pi_2, \dots, \pi_s \in R$ ($s \geq 0$ and not necessarily distinct but is unique up to ordering) such that $M \cong R^d \oplus R/(\pi_1^{i_1}) \oplus \cdots \oplus R/(\pi_s^{i_s})$.*

Proof. We prove it by induction on the number of generators d. Let $d = 1$ (base case). This case is immediate since this means M is cyclic. Thus $M \cong R/I$ for $I = \mathrm{Ann}_R(M)$. We have two cases. If $I = (0)$, then $M \cong R^1$, the free R-module of rank 1. If $I \neq (0)$, then $I = (a)$ for some non-zero $a \in R$. Since every PID is a UFD, a has a unique factorization $u\pi_1^{i_1} \cdots \pi_s^{i_s}$ where u is a unit and π_i's are distinct prime elements. So $I = (\pi_1^{i_1} \cdots \pi_s^{i_s})$. For $k = 1, \dots, s$, let $J_k = (\pi_k^{i_k})$. We claim that J_k's are comaximal (i.e., $k \neq l$ implies $J_k + J_l = R$) and $\bigcap_{k=1}^{s} J_k = I$. Indeed, if $k \neq l$ then $J_k + J_l = (\pi_k^{i_k}, \pi_l^{i_l}) = (b)$ since R is a PID. Therefore $(b) \supseteq (\pi_k^{i_k})$ and $(b) \supseteq (\pi_l^{i_l})$. Hence $b \mid \pi_k^{i_k}$ and $b \mid \pi_l^{i_l}$. Since π_k and π_l are distinct, it follows that $b = 1$, as required. For the second part of the claim, one direction is easy: note that since I is contained in J_k for all k we have $I \subseteq \bigcap_{k=1}^{s} J_k$. If $b \in \bigcap_{k=1}^{s} J_k$, then $b \in (\pi_k^{i_k})$ for all k. Hence $\pi_k^{i_k} \mid b$ for all k, hence $\pi_1^{i_1} \cdots \pi_s^{i_s} \mid b$. Hence $b \in (\pi_1^{i_1} \cdots \pi_s^{i_s}) = I$.

So by the Chinese remainder theorem,

$$R/I \cong \prod_{i=1}^{s} R/J_i = \prod_{k=1}^{s} R/(\pi_k^{i_k})$$

as rings. But this is a stronger condition that being isomorphic as modules. Thus we can make the analogous statement as modules. This completes the base case.

Now suppose the results holds whenever M is generated by fewer than d elements. Consider $M = \langle m_1, \dots, m_d \rangle = Rm_1 + Rm_2 + \cdots + Rm_d$.

Case 1. $r_1m_1 + \cdots + r_dm_d = 0$ implies $r_1 = r_2 = \cdots = r_d = 0$.

In this case, it is immediate that $M \cong R^d$.

Case 2. There exists non-zero $(r_1, r_2, \dots, r_d)$ such that $r_1m_1 + r_2m_2 + \cdots + r_dm_d = 0$.

Consider the set $\mathscr{S}$ consisting of all d-tuples $(n_1, \dots, n_d) \in M^d$ such that $M = Rn_1 + Rn_2 + \cdots + Rn_d$. Given $(n_1, \dots, n_d) \in \mathscr{S}$, let $J_{(n_1,\dots,n_d)} := \{r \in R : rn_1 \in Rn_2 + \cdots + Rn_d\} =$

$\mathrm{Ann}(M/(Rn_2 + \cdots + Rn_d))$. Notice that if $r_1n_1 + \cdots + r_dn_d = 0$ then $r_1n_1 = -(r_2n_2 + \cdots + r_dn_d) \in Rn_2 + \cdots + Rn_d$. It is not hard to see that $J_{(n_1,\ldots,n_d)}$ is an ideal. Here comes the key **trick**: pick $(n_1, n_2, \ldots, n_d) \in \mathscr{S}$ such that $J_{(n_1,\ldots,n_d)}$ is maximal in the collection of ideals $\{J_{(n_1,\ldots,n_d)} : (n_1, \ldots, n_d) \in M^d\}$. Here, the following fact comes in handy: if $\mathscr{T}$ is a non-empty collection of ideals in a PID then there exists $J \in \mathscr{T}$ that is maximal in $\mathscr{T}$ with respect to $\supseteq$. We will finish the proof in the next lecture. □

5. January 15

Lemma 5.1. *If $\mathscr{T}$ is a non-empty collection of ideals in a PID then there exists $J \in \mathscr{T}$ that is maximal in $\mathscr{T}$ with respect to $\supseteq$.*

Proof. Let $(a_i) \in \mathscr{T}$, and if (a_i) is maximal, we are done. If not, choose (a_2) so that $(a_2) \supsetneq (a_1)$ and if (a_2) maximal, stop. We see that either we will eventually produce a maximal element of $\mathscr{T}$ or we will produce an infinite ascending chain

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

of ideals in $\mathscr{T}$. Let

$$J := \bigcup_{i=1}^{\infty} (a_i) = (b)$$

(since R is a PID). Then $b \in J$, so there exists j such that $b \in (a_j)$, or $(b) = (a_j)$. This is a contradiction since this implies $(b) \supseteq (a_{j+1}) \supsetneq (a_j) \supseteq (b)$. □

Proof of Theorem 4.5 (continued). Now that we proved Lemma 5.1, we can finish off the proof. Pick $(n_1, n_2, \ldots, n_d) \in \mathscr{S}$ if $J_{(n_1,\ldots,n_d)}$ is maximal in the set $\{J_{(v_1,\ldots,v_d)} : (v_1, \ldots, v_d) \in \mathscr{S}\}$. Note that there exists $r \in R$ such that $J_{(n_1,\ldots,n_d)} = (r)$ since R is a PID. We claim (to be proved later) that if $rn_1 + \cdots + r_dn_d = 0$, then $r \mid r_2, \ldots, r \mid r_d$. So write $r_i = ra_i$ for all $2 \le i \le d$ and let $n_1' = n_1 + a_2n_2 + \cdots + a_dn_d$ and $n_i' = n_i$ for all $2 \le i \le d$. Now if we let $N_1 := Rn_1 \subseteq M$ and $N_2 := Rn_2 + Rn_d \subseteq M$, then by induction hypothesis, N_1 and N_2 both have a decomposition of the desired form; hence, so does $N_1 \oplus N_2$.

We clearly have $N_1 + N_2 = M$. Thus we only need to check that $N_1 \cap N_2 = (0)$ to ensure that $M \cong N_1 \oplus N_2$. So if $a \in N_1 \cap N_2$, then $a \in N_1$, i.e., $a = un_1'$, and since $a \in N_2$, a must be of the form $u_2n_2' + \cdots + u_dn_d'$. Notice that $rn_1' = r(n_1 + a_2n_2 + \cdots + a_dn_d) = rn_1 + ra_2n_2 + \cdots + ra_dn_d = rn_1 + r_2n_2 + \cdots + r_dn_d = 0$. Therefore, if $a \in N_1 \cap N_2$ and $a \neq 0$, then $r \nmid u$. Hence $(u, r) \supsetneq (r)$ if $a \neq 0$. But $un_1' = u_2n_2' + \cdots + u_dn_d' \in Rn_2' + Rn_3' + \cdots + Rn_d'$ and $rn_1' = 0 \in Rn_2' + \cdots + Rn_d'$, form which it follows that

$$J_{(n_1',\ldots,n_d')} \supseteq (u, r) \supsetneq (r) = J_{(n_1,\ldots,n_d)}.$$

But this contradicts the fact that our choice of $J_{(n_1,\ldots,n_d)}$ is maximal. Now it remains to prove the claim we initially assumed. □

Lemma 5.2. *If $rn_1 + \cdots + r_dn_d = 0$, then $r \mid r_2, \ldots, r \mid r_d$.*

Proof. Suppose that $rn_1 + r_2n_2 + \cdots + r_dn_d = 0$ and there exists $i > 1$ such that $r \nmid r_i$. Without loss of generality, let $i = 2$. Let $s = \gcd(r_1, r_2)$ and $(s) \supsetneq (r)$. Write $r = sa, r_2 = sb$ with $\gcd(a, b) = 1$. There fore there exist $c, d \in R$ such that $ca + db = 1$. Take the relation: $rn_1 + r_2n_2 + \cdots + r_dn_d = s(an_1 + bn_2) + r_3n_3 + \cdots + r_dn_d = 0$. Make a new spanning set for M: $n_1' = an_1 + bn_2, n_2' = -dn_1 + cn_2, n_3' = n_3', \ldots, n_d = n_d'$. From this we have $cn_1' - bn_2' = (ac + bd)n_1 + (bc - bc)n_2 = n_1$ while we have $dn_1' + an_2' = n_2$. Now,

note that $s(an_1 + bn_2) + r_3n_3 + \cdots + r_dn_d = 0$, hence $sn_1' + r_3n_3' + \cdots + r_dn_d' = 0$. Thus $J_{(n_1',n_2',\ldots,n_d')} \supseteq (s) \supsetneq (r)$, contradicting the maximality assumption. □

6. January 15: Introduction to tensor products

Definition 6.1. Let R be a ring and let M, N be two R-modules. A module $M \otimes_R N$ is called the *tensor product of M and N over R.*

So how do we build this tensor product?

(1) Start by building a free module F with a basis $\{e_{(m,n)} : (m,n) \in M \times N\}$. We will take a submodule $G \subseteq F$. G will be the R-submoudle of F spanned by all elements of the following forms: $e_{(m_1+m_2,n)} - e_{(m_1,n)} - e_{(m_2,n)}, e_{(m,n_1+n_2)} - e_{(m,n_1)} - e_{(m,n_2)}, e_{(rm,n)} - re_{(m,n)}, e_{(m,rn)} - re_{(m,n)}$.
(2) Define $M \otimes_R N := F/G$, and define $e_{(m,n)} + G =: m \otimes n$.

Remark 6.1. It is important to know that *not every element can be expressed as $m \otimes n$.*

Question. What is $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/3\mathbb{Z})$?

Solution: In this case, the free module we need is $F = \mathbb{Z}e_{(0,0)} \oplus \mathbb{Z}e_{(0,1)} \oplus \mathbb{Z}e_{(0,2)} \oplus \mathbb{Z}e_{(1,0)} \oplus \mathbb{Z}e_{(1,1)} \oplus \mathbb{Z}e_{(1,2)}$. We claim in fact that $F = G$. For any $i \in \mathbb{Z}/2\mathbb{Z}$ and $j \in \mathbb{Z}/3\mathbb{Z}$, we have

$$e_{(i,j)} = e_{(i\cdot 1, j\cdot 1)} = ie_{(1,j\cdot 1)} = ije_{(1,1)} \equiv 0 \pmod{G},$$

since $e_{(1,1)} = e_{(3,1)} = 3e_{(1,1)} = e_{(1,3)} = e_{(1,0)=0}$ by bilinearity. Thus $F/G = (0)$.

7. January 16

We defined tensor product last time. Now we talk about the most useful property of tensor products: *universal property*. Consider a bilinear map

$$\phi : M \times N \to M \otimes_R N$$

defined as $(m,n) \mapsto m \otimes n = e_{(m,n)} + G \in F/G$. Note, however, that ϕ is *generally not surjective.*

Proposition 7.1 (Universal property of tensor products)**.** *Let M, N, P be R-modules and suppose that $f : M \times N \to P$ is R-bilinear. Then*

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & P \\ \downarrow{\scriptstyle \phi} & \nearrow_{\exists! \tilde{f}} & \\ M \otimes_R N & & \end{array}$$

Then these exists a unique $\tilde{f} \in \mathrm{Hom}(M \otimes_R N, P)$ *such that $\tilde{f} \circ \phi = f$.*

Proof. Suppose F is a free R-module with basis $\{e_\alpha\}$ and if P is an R-module, then any map $\phi : \{e_\alpha\} \to P$ extends uniquely to an element $\widehat{\phi} \in \mathrm{Hom}(F, P)$. So what do we do? For any R-module homomorphism $f : M \times N \to P$, we have a *unique* homomorphism $\psi : F \to P$ such that $e_{(m,n)} \mapsto f(m,n)$. This implies that $\psi|_G = 0$ since

$$\psi(e_{(rm,n)} - re_{(m,n)}) = \psi(e_{(rm,n)}) - r\psi(e_{(m,n)}) = f(rm,n) - rf(m,n) = 0,$$

with the last equality following from the fact that f is bilinear. This means that we can define an R-module homomorphism $\tilde{f} : F/G \to P$ such that $\tilde{f}(x + G) = \psi(x)$. This is

well-defined since $x+G = y+G \Leftrightarrow x-y \in G \Leftrightarrow \psi(x) = \psi(y)$. So $\tilde{f} \circ \phi(m,n) = \tilde{f}(m \otimes n) = \tilde{f}(e_{(m,n)} + G) = \psi(e_{(m,n)}) = f(m,n)$. $\square$

Remark 7.1. Note that $M \otimes_R N$ is spanned as an R-module by $\{m \otimes n : m \in M, n \in N\}$. Write any $x + G \in F/G$ as follows:

$$x + G = \sum r_i e_{(m_i,n_i)} + G \to \sum r_i m_i \otimes n_i \in M \otimes_R N.$$

Example 7.2. Compute $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$. In this case $F = \mathbb{Z}e_{(0,0)} + \mathbb{Z}e_{(0,1)} + \mathbb{Z}e_{(1,0)} + \mathbb{Z}e_{(1,1)}$. As we did last time, $e_{(i,j)} \equiv ie_{(1,j)} \equiv ije_{(1,1)} \pmod{G}$. So $F/G = \mathbb{Z}(e_{(1,1)} + G) = \mathbb{Z}(1 \otimes 1)$. Since $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0(1 \otimes 1) = 0$, so F/G is either $\mathbb{Z}/2\mathbb{Z}$ or (0). We claim that $(\mathbb{Z}/2\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$. Let $P = \mathbb{Z}/2\mathbb{Z}$. We say that if the tensor product were zero, then $\tilde{f}$ will have to send everything to zero, but $f(1,1) = 1 \neq 0$. So the claim follows.

Theorem 7.3 (Uniqueness of tensor product)**.** *There exists a* unique *R-module $M \otimes_R N$ with bilinear $\phi : M \times N \to M \otimes_R N$ with respect to having the universal property for all R-module P and bilinear $f : M \times N \to P$.*

Proof. Suppose that we have R-modules A and B with bilinear map $\phi : M \times N \to A$ and $\psi : M \times N \to B$ with the universal property. So by the universal property, there exists a unique $\tilde{\psi}$ such that $\tilde{\psi} \circ \phi = \psi$.

$$\begin{array}{ccc} M \times N & \xrightarrow{\psi} & B \\ \downarrow{\scriptstyle \phi} & \nearrow_{\exists! \tilde{\psi}} & \\ A & & \end{array} \quad \text{and} \quad \begin{array}{ccc} M \times N & \xrightarrow{\phi} & A \\ \downarrow{\scriptstyle \psi} & \nearrow_{\exists! \tilde{\phi}} & \\ B & & \end{array}$$

Similarly, there exists a unique $\tilde{\phi}$ such that $\tilde{\phi} \circ \psi = \phi$.

We claim that $\tilde{\phi} \circ \tilde{\psi} = \mathrm{id}_A$ and $\tilde{\psi} \circ \tilde{\phi} = \mathrm{id}_B$. We just need to do one of them since we can apply the symmetric argument for the other one. We know that the image of ϕ must span A. So $\tilde{\phi} \circ \tilde{\psi}(\phi(m,n)) = \phi(m,n)$ for all m, n. Another possible method is to consider the fact that the following diagram must commute:

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi} & A \\ \downarrow{\scriptstyle \phi} & \nearrow_{\exists! \tilde{\phi} \circ \tilde{\psi}} & \\ A & & \end{array}$$

Since $\tilde{\phi} \circ \tilde{\psi} = \mathrm{id}_A$ works and that must be unique, the claim follows. $\square$

Example 7.4. If $m, n \geq 2$, what is $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z}$? We claim that $\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z}$ where $d = \gcd(m,n)$. Consider the commutative diagram

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\psi} & \mathbb{Z}/d\mathbb{Z} \\ \downarrow{\scriptstyle \phi} & \nearrow & \\ \mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} & & \end{array}$$

$\psi : (a,b) \mapsto (ab)$ is bilinear and onto. The tensor product is spanned by $i \otimes j = ij(1 \otimes 1)$. But then $d(1 \otimes 1) = (am + bn)(1 \otimes 1) = am \otimes 1 + bn \otimes 1 = 0$. Hence the claim follows.

Proposition 7.5 (Properties of tensor product)**.** *The following hold:*

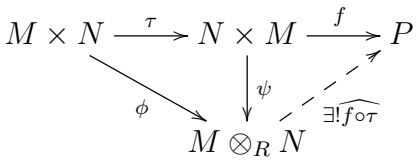
(1) (commutativity) $M \otimes_R N \cong N \otimes_R M$

(2) (associativity) $(M \otimes_R N) \otimes_R P \cong M \otimes_R (N \otimes_R P) \cong M \otimes_R N \otimes_R P$

8. January 20

Proposition 8.1. $M \otimes_R N \cong N \otimes_R M$.

Proof. Consider the following commutative diagram:



where $\tau : (m, n) \mapsto (n, m)$ and $\psi : (n, m) \mapsto m \otimes n$. Note $\widehat{f \circ \tau} \circ \psi = f$.

So $M \otimes_R N$ satisfies the universal property for $N \times M$ with $\psi : N \times M \to M \otimes_R N$ bilinear. Therefore $M \otimes_R N \cong N \otimes_R M$. □

8.1. Tensor product of maps.

Definition 8.2. If $f : M \to P$ and $g : N \to Q$ are homomorphisms, then we can make a bilinear map $\psi : M \times N \to P \otimes_R Q$ such that $(m, n) \mapsto f(m) \otimes g(n)$. This map $f \otimes g$ is said to be the *tensor product of f and g.*

This map is bilinear, since

$$\begin{aligned}(rm_1 + m_2, n) &\overset{\psi}{\mapsto} f(rm_1 + m_2) \otimes g(n) \\ &= (rf(m_1) + f(m_2)) \otimes g(n) \\ &= rf(m_1) \otimes g(n) + f(m_2) \otimes g(n) = r\psi(m_1, n) + \psi(m_2, n).\end{aligned}$$

So if $\widehat{\psi} : M \otimes_R N \to P \otimes_R Q$ is defined as $\psi(m \otimes n) = f(m) \otimes g(n)$, then $\widehat{\psi} \circ \phi = \psi$. In particular, $\psi(m, n) = \widehat{\psi}(m \otimes n) = f(m) \otimes g(n)$.

It is customary to let $f \otimes g$ denote $\widehat{\psi}$. So in summary, if $f \in \mathrm{Hom}(M, P)$ and $g \in \mathrm{Hom}(N, Q)$ then there exists a unique $f \otimes g \in \mathrm{Hom}(M \otimes N, P \otimes Q)$ such that $(f \otimes g)(m \otimes n) = f(m) \otimes g(n)$.

One important special case is the following: if $f : M \to N$, then $f \otimes \mathrm{id}_C : M \otimes C \to N \otimes C$ is $(f \otimes \mathrm{id}_C)(m \otimes c) = f(m) \otimes c$.

Theorem 8.3. *If $M \overset{f}{\to} N \overset{g}{\to} P \to 0$ is exact and C is an R-module, then the sequence*

$$M \otimes_R C \overset{f \otimes \mathrm{id}_C}{\to} N \otimes_R C \overset{g \otimes \mathrm{id}_C}{\to} P \otimes_R C \to 0$$

is exact also.

One can check that $g \otimes \mathrm{id}_C$ is onto. Note that $P \otimes_R C$ is generated by $p \otimes c \leftrightarrow g(n) \otimes c \leftrightarrow (g \otimes \mathrm{id}_C)(n \otimes c)$. In general, however $0 \to M \to N$ being exact *does not imply* that $0 \to M \otimes C \to N \otimes C$ is exact.

Example 8.4. Let $M = N = \mathbb{Z}$ and $C = \mathbb{Z}/2\mathbb{Z}$, and $R = \mathbb{Z}$. If $f : M \to N$ such that $f(m) = 2m$, then indeed f is injective. However,

$$0 \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z} \overset{f\otimes \mathrm{id}_C}{\to} \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$$

is not exact: $f \otimes \mathrm{id}_C$ is the zero map, since $(f \otimes \mathrm{id}_C)(n \otimes \varepsilon) = 2n \otimes \varepsilon = n \otimes 2\varepsilon = n \otimes 0 = 0$.

Definition 8.5. An R-module is *flat* if $0 \to A \otimes M \to B \otimes M$ is exact whenever $0 \to A \to B$ is exact. M is *faithfully flat* if M is flat, and $A \otimes_R M \neq (0)$ whenever $A \neq (0)$.

Example 8.6. $\mathbb{Q}$ is faithful and flat as a $\mathbb{Z}$-module but is not faithfully flat. Recall that $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}/2\mathbb{Z} = (0)$.

Proposition 8.7. *Let R be a ring and M an R-module. Then $R \otimes_R M \cong M$.*

Proof. Let $\phi : R \times M \to M$ given by $(r, m) \mapsto rm$. It is easy to verify that this is bilinear. Suppose that $R \times M \to P$ is bilinear.

$$\begin{array}{ccc} R \times M & \xrightarrow{\psi} & P \\ \downarrow{\scriptstyle \phi} & \nearrow_{\exists! \widetilde{\psi}} & \\ M & & \end{array}$$

Our goal is to find a unique homomorphism $\widetilde{\psi}$ such that $\widetilde{\psi} \circ \phi = \psi$. Since ψ is bilinear, we have $\psi(r, m) = \psi(r \cdot 1, m) = r\psi(1, m)$. We want $\widetilde{\psi}(m) = \widetilde{\psi} \circ \phi(1, m) \overset{?}{=} \psi(1, m)$. This (uniquely determined) $\widetilde{\psi}$ is a homomorphism, since ψ is bilinear: $\widetilde{\psi}(rm_1 + m_2) = \psi(1, rm_1 + m_2) = r\psi(1, m_1) + \psi(1, m_2) = r\widetilde{\psi}(m_1) + \widetilde{\psi}(m_2)$. □

8.2. **Direct sums.**

Theorem 8.8. *If $\{M_\alpha\}_{\alpha \in I}$ is a collection of R-modules and C is an R-module, then*

$$\left(\bigoplus_{\alpha \in I} M_\alpha \right) \otimes_R C \cong \bigoplus_{\alpha \in I} (M_\alpha \otimes_R C).$$

Proof. We will prove the two direct sum case $(M \oplus N) \otimes C \cong (M \otimes C) \oplus (N \otimes C)$, since the same argument can be extended for the general case. Let $\pi_1 : M \oplus N \to M$ and $\pi_2 : M \oplus N \to N$ be the projection maps. We will make linear maps $\pi_1 \otimes \mathrm{id} : (M \oplus N) \otimes C \to M \otimes C$ and $\pi_2 \otimes \mathrm{id} : (M \oplus N) \otimes C \to N \otimes C$ and construct $(\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id}) : (M \oplus N) \otimes C \to (M \otimes C) \oplus (N \otimes C)$. Let $i_1 : M \hookrightarrow M \oplus N$ and $i_2 : N \hookrightarrow M \oplus N$ be inclusion maps $i_1(m) = (m, 0)$ and $i_2(n) = (0, n)$. The inclusion maps give maps $i_1 \otimes \mathrm{id} : M \otimes C \to (M \oplus N) \otimes C$ and $i_2 \otimes \mathrm{id} : N \otimes C \to (M \oplus N) \otimes C$. The two maps extend to a map $(M \otimes C) \oplus (N \otimes C) \to (M \oplus N) \otimes C$ such that $(i_1 \otimes \mathrm{id})(m \otimes c, n \otimes c') = i_1(m) \otimes c$. So we get a map $h : (M \otimes C) \oplus (N \otimes C) \to (M \oplus N) \otimes C$ where $h = i_1 \otimes \mathrm{id} + i_2 \otimes \mathrm{id}$. Notice

$$\begin{aligned} (\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id}) \circ h(m \otimes c, n \otimes c') &= (\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id})[(m, 0) \otimes c + (0, n) \otimes c'] \\ &= (m \otimes c + 0 \otimes c', 0 \otimes c + n \otimes c') = (m \otimes c, n \otimes c'). \end{aligned}$$

Hence $(\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id}) \circ h = \mathrm{id}_{(M \otimes C) \oplus (N \otimes C)}$. For the other way,

$$\begin{aligned} h \circ (\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id})((m, n) \otimes c) &= h(m \otimes c, n \otimes c) \\ &= (m, 0) \otimes c + (0, n) \otimes c = (m, n) \otimes c. \end{aligned}$$

Therefore $h \circ (\pi_1 \otimes \mathrm{id}, \pi_2 \otimes \mathrm{id}) = \mathrm{id}_{(M\oplus N)\otimes C}$. Notice that this is enough to prove that it is identity since we proved the identity over all the generating elements, which implies that it is the identity over all elements. □

9. January 22

Corollary 9.1. *If $R^X \cong R^Y$ (X, Y index sets, R a* commutative *ring), then $|X| = |Y|$.*

Proof. Let P be a maximal ideal of R. Let $F = R/P$. Then $R^X \cong R^Y$ so $R^X \otimes_R F \cong (R/P)^X = F^X$. Therefore $R^X \cong R^Y \Rightarrow F^X \cong F^Y$ as R-modules. Recall the following fact:

Claim. If M and N are isomorphic R-modules then $\mathrm{Ann}(M) = \mathrm{Ann}(N) = I$ is an ideal of R. Then M and N are isomorphic as R/I-modules.

Proof of the claim. Let $\phi : M \to N$ be an R-module isomorphism, and let $\overline{r} = r + I \in R/I$. Create an R/I-module isomorphism $\overline{\phi}(m) = \phi(m)$ and $\overline{\phi}(\overline{r} \cdot m) = \phi(rm) = r\phi(m) = \overline{r}\phi(m)$. One can check that $\overline{\phi}$ is well-defined and bijective. □

Now we consider the annihilators of F^X. Note that $F^X \cong (R/P)^X$, Since $\mathrm{Ann}(F^X) = \mathrm{Ann}(F^Y) = P$ and since $F^X \cong F^Y$ as R-modules, ist follows that $F^X \cong F^Y$ as F-modules. Therefore $|X| = |Y|$. □

9.1. Algebras, base change, and extension of scalars.

Definition 9.2. Let R be a ring. Then an *R-algebra* S is just a ring equipped with a ring homomorphism $\alpha : R \to S$ satisfying $\alpha(1_R) = 1_S$.

Example 9.3. Every ring is a $\mathbb{Z}$-algebra, since $\alpha : \mathbb{Z} \to R$ given by $\alpha(n) = n \cdot 1_R$ is a ring homomorphism.

Example 9.4. $\mathbb{C}[x, y]$ is a $\mathbb{C}$-algebra, with $\alpha : \mathbb{C} \to \mathbb{C}[x, y]$ being defined to be $\alpha(c) = c$, where c is a constant polynomial.

Example 9.5. $\mathbb{C}$ is an $\mathbb{R}$-algebra, with $\alpha : \mathbb{R} \to \mathbb{C}$ given by $\alpha(c) = c$.

Notice that if S is an R-algebra then S inherits an R-module structure as well. Given $r \in R, s \in S$, define $r \cdot s := \alpha(r)s \in S$, where $\alpha : R \to S$ is a ring homomorphism such that $\alpha(1_R) = 1_S$. Notice also then that if S is an R-algebra and M is an R-module then we can form the tensor product $S \otimes_R M$ which is another R-module.

But note also that we can endow $S \otimes_R M$ with an S-module structure, via the rule

$$s_1 \cdot (s_2 \otimes m) := s_1 s_2 \otimes m,$$

and extend linearly, i.e., $(s_1 + s_2)(s' \otimes m) = s_1(s' \otimes m) + s_2(s' \otimes m)$.

So we started with an R-module M for some ring R; and then for some R-algebra S, we created an S-module $S \otimes_R M$, hence "extending" scalars. This process is therefore called either *base change* or *extension of scalars*. So why is this interesting?

Remark 9.1. As a motivating example, imagine that V is a $\mathbb{Q}$-vector space. And it is easy to see that $\mathbb{C}$ is a $\mathbb{Q}$-algebra. Let $V_{\mathbb{C}} := V \otimes_{\mathbb{Q}} \mathbb{C}$ is a $\mathbb{C}$-vector space. If $V \cong \mathbb{Q}^n$, then $V \otimes_{\mathbb{Q}} \mathbb{C} \cong (\underbrace{\mathbb{Q} \oplus \cdots \oplus \mathbb{Q}}_{n \text{ times}}) \otimes_{\mathbb{Q}} \mathbb{C} \cong \bigoplus_{i-1}^{n} (\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{C}) \cong \mathbb{C}^n$.

Remark 9.2 (A useful construction). If A and B are R-algebras then we can form $A \otimes_R B$, which is an R-module. But it actually has the structure of an R-algebra. For instance, if we let $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$, and α defined to be $\alpha(r) \otimes 1 = 1 \otimes \beta(r)$, define $\gamma : R \to A \otimes_R B$ to be $\gamma(r) = \alpha(r) \otimes 1 = 1 \otimes \beta(r)$. This gives us the R-algebra structure.

9.2. **Noetherian rings.**

Definition 9.6. Let R be a ring. We say R is *Noetherian* if every *ascending chain* of ideals of R terminates. That is, if $I_1 \subseteq I_2 \subseteq \cdots$ is an ascending chain, then there exists n such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

Example 9.7. Every PID is Noetherian. Also, a field is Noetherian, since it only has two ideals: itself and the zero ideal. Alternately, you can observe that a field is a PID, hence Noetherian.

Example 9.8. Let $R = \mathbb{C}[x_1, x_2, \dots]$. Then the following chain

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$$

is an ascending chain of infinite length. Hence R is not Noetherian.

Definition 9.9. Let R be a ring and let M be an R-module. THen M is *Noetherian* if every ascending chain of submodules of M terminates.

Remark 9.3. R is Noetherian as a ring if and only if R is Noetherian as an R-module.

Example 9.10. If $R = \mathbb{Z}$ and $M = \mathbb{Q}$, then $\mathbb{Q}$ is not Noetherian as a $\mathbb{Z}$-module, since the following ascending chain does not terminate: $\mathbb{Z} \cdot 1 \subsetneq \mathbb{Z} \cdot \frac{1}{2} \subsetneq \mathbb{Z} \cdot \frac{1}{4} \subsetneq \mathbb{Z} \cdot \frac{1}{8} \subsetneq \cdots$.

Proposition 9.11. *Let R be a ring. And the the following statements are equivalent:*

(1) R is Noetherian
(2) Every ideal I is finitely generated
(3) Every non-empty collection of $\mathscr{S}$ of ideals has a maximal element with respect to $\subseteq$.

Remark 9.4. One can prove analogous statements for modules in a similar manner.

Proof. ((2) $\Rightarrow$ (3)) Let $\mathscr{S}$ be a non-empty collection of ideals, and if $\mathscr{S}$ does not have a maximal element, then we can produce a chain $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. Now let $J = \bigcup I_i$. By (2), we have $J = (a_1, a_2, \dots, a_s)$. For all $i \in \{1, 2, \dots, s\}$, there exists ni such that $a_i \in I_{n_i}$. Let $N = \max(n_1, n_2, \dots, n_s)$, so $J = (a_1, \dots, a_s) \in I_n \subsetneq J$, or $I_n = J$. But this is a contradiction.

((2) $\Rightarrow$ (1)) Same idea: start with $I_1 \subsetneq I_2 \subsetneq \cdots$ then let $J = \bigcup I_i$ cannot be finitely-generated by the same reason.

($\neg$(2) $\Rightarrow$ $\neg$(3)) Let $J = (a_1, a_2, a_3, \dots)$ be an ideal that is not finitely generated and $a_{i+1} \in\not\in (a_1, \dots, a_i)$ for all i. Let $\mathscr{S} = \{(a_1, \dots, a_i) : i \geq 1\}$. Then $\mathscr{S}$ has no maximal element, since $(a_1, \dots, a_n) \subsetneq (a_1, \dots, a_{n+1})$. $\square$

10. January 23

Proposition 10.1. *Let R be a ring and let M be an R-module. Let N be a submodule of M. Then M is Noetherian if and only if N and M/N are Noetherian.*

Proof. Let $\pi : M \to M/N$ be the canonical surjection. Recall that by the correspondence theorem, the map $P \subset M \mapsto \pi(P) \subset M/N$ gives an inclusion-preserving bijection between submodules of M/N and submodules of M that contain N.

($\Rightarrow$) If $N_1 \subseteq N_2 \subseteq \cdots$ is a chain in N, then it is also a chain in M. Therefore it must terminate. Similarly, if $A_1 \subseteq A_2 \subseteq \cdots$ is a chain in M/N then $\pi^{-1}(A_1) \subseteq \pi^{-1}(A_2) \subseteq \pi^{-1}(A_3)\cdots$ is a chain in M. Therefore it must terminate also. The claim now follows.

($\Leftarrow$) Suppose that N and M/N are Noetherian, and let $M_1 \subseteq M_2 \subseteq \cdots$ are Noetherian. Then $M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$ is a chain in N. So there exists m such that $M_m \cap N = M_{m+1} \cap N = \cdots$. Also, $\pi(M_1) \subseteq \pi(M_2) \subseteq \cdots$ is a chain in M/N so there exists some p such that $\pi(M_p) = \pi(M_{p+1}) = \cdots$. Let $n = \max(m, p)$. We claim that this implies $M_n = M_{n+1} = M_{n+2} = \cdots$.

Let $x \in M_{n+i}$. We know that $M_{n+i} \supseteq M_n$. It is enough to show that $x \in M_n$. Since $\pi(M_{n+i}) = \pi(M_n)$, there exists $y \in M_n$ such that $\pi(x) = \pi(y)$. Then $\pi(x - y) \equiv 0$, so $x - y \in N \cap M_{n+i} = N \cap M_n$. So $x - y = z \in M_n$ so $x = y + x \in M_n$. □

Corollary 10.2. *If M and N are Noetherian, then $M \oplus N$ is Noetherian.*

Proof. Note that $(M \oplus N)/M \cong N$, since $M \cong M \oplus (0)$. □

Example 10.3. Note that the infinite direct sums of Noetherian modules *need not be Noetherian.* Let $R = \mathbb{Z}$ and $M = \bigoplus \mathbb{Z}$. Then M is not finitely generated as a $\mathbb{Z}$-module, so M cannot be Noetherian.

Corollary 10.4. *If R is Noetherian and M is a finitely-generated R-module, then M is Noetherian.*

Proof. Prove by induction in the number of generators d. If $d = 0$ then the claim is evident. Let $d = 1$. Then there exists $m \in M$ such that $M = Rm$. Then $r \mapsto rm$ is a surjective map, and by the first isomorphism theorem $M \cong R/I$. Then M is Noetherian since R is Noetherian as an R-module and R/I is a quotient.

So assume that this is true for all $d < n$. Let $M = \langle m_1, \ldots, m_n \rangle$. Then $N = \langle m_1, \ldots, m_{n-1} \rangle$. By the induction hypothesis, N is Noetherian and $M/N = R(m+N)$, so M/N is Noetherian. Therefore M is Noetherian as well. □

10.1. Maximality principle.

Meta-theorem. *If R is a Noetherian ring and one chooses an ideal I in R that is maximal with respect to some "nice" property, then I is a prime ideal.*

Definition 10.5. Recall that we define the *product of the two ideals I and J* to be

$$IJ := \left\{ \sum_{i=1}^{d} i_t j_t : d \geq, i_1, \ldots, i_k \in I, j_1, \ldots, j_k \in J \right\} \subseteq R.$$

Theorem 10.6 (Noether)**.** *Let R be a Noetherian ring and I be a proper ideal of R. Then there exist $m \geq 1$ and prime ideals $P_1, \ldots, P_m$ (not necessarily distinct) such that $P_1P_2P_3 \cdots P_m \subseteq I$.*

Proof. Suppose the statement is not true. Let $\mathscr{S}$ be the collection of proper ideals that do not contain a finite product of prime ideals. By assumption, $\mathscr{S} \neq \emptyset$. Pick $I \in \mathscr{S}$ maximal. We will show that I must be prime. And then we will let $m = 1$ and $P_1 = I$ hence $P_i \subseteq I$, which is a contradiction.

Suppose I is not prime. Then there must exist $a, b \in R \setminus I$ such that $ab \in I$. Now let $J_1 := I + Ra$ and $J_2 := I + Rb$. Notice that $I \subsetneq J_1$ and $I \subsetneq J_2$. Also note that $J_1J_2 = (I + Ra)(I + Rb) \subset I + Rab \subseteq I$. By maximality, $J_1, J_2 \notin \mathscr{S}$. So there exist $P_1, \ldots, P_m, Q_1, \ldots, Q_n$ prime ideals such that $P_1P_2 \cdots P_m \subseteq J_1$ and $Q_1Q_2 \cdots Q_n \subseteq J_2$. Therefore $P_1P_2 \ldots P_mQ_1 \ldots Q_n \subseteq J_1J_2 \subseteq I$. □

Remark 10.1. Without loss of generality, we may choose the P_i so that they contain I. If I is a proper ideal of R and R is Noetherian and $P_1P_2 \cdots P_m \subseteq I$ and $P_1, P_2, \ldots P_m \supseteq I$, then if Q is a prime ideal and $Q \supseteq I$ then $Q \supseteq P_i$.

Assume not. Then for $i = 1, 2, \ldots, m$,there exist $a_i \in P_i \setminus Q$ so $a_1a_2 \cdots a_m \in P_1 \cdots P_m \subseteq I \subseteq Q$. This is a contradiction: note that $\overline{a_1} \cdots \overline{a_n} = 0$ in R/Q so there exists j such that $\overline{a_j} = 0$ hence $a_j \in Q$.

So there are only finitely many primes in R that are minimal with respect to containing I.

Definition 10.7. Let R be a ring and I an ideal of R. Then *the radical of I* is

$$\sqrt{I} := \bigcap_{\substack{P \supseteq I \\ P \text{ prime}}} P.$$

Example 10.8. If $R = \mathbb{Z}/4\mathbb{Z}$, then what is $\sqrt{(0)}$? Note that out of three ideals $(0), 2(\mathbb{Z}/4\mathbb{Z})$, $4(\mathbb{Z}/4\mathbb{Z})$, we see that $2(\mathbb{Z}/4\mathbb{Z})$ is the only prime ideal. Therefore $\sqrt{(0)} = 2(\mathbb{Z}/4\mathbb{Z})$.

11. January 27

Note that if R is Notherian, then $\sqrt{I} = P_1 \cap \cdots \cap P_s$, i.e., there are only finitely many ideals containing I.

Theorem 11.1. *Let R be a ring. Then $\sqrt{(0)}$ is nil ideal, i.e., if $x \in \sqrt{(0)}$ then there exists $n = n(x) \geq 1$ such that $x^n = 0$.*

Proof. Suppose not. THen there exists $x \in I := \sqrt{(0)}$ such that x is not nilpotent. Let $T = \{1, x, x^2, x^3, \cdots\}$. Then $0 \notin T$. Let $\mathscr{S} = \{J : J \text{ ideal}, J \cap T = \emptyset\}$. Then $\mathscr{S} \neq \emptyset$ because $(0) \cap T = \emptyset$, meaning $(0) \in \mathscr{S}$.

If R is Noetherian, we just let J be a maximal element of $\mathscr{S}$. If not, then we use Zorn's lemma to produce a maximal element. Namely, let $\{J_\alpha\}$ be a chain of $\mathscr{S}$ and look at $\bigcap J_\alpha$. Think about why this is in $\mathscr{S}$. Therefore Zorn's lemma gives a maximal element of $\mathscr{S}$.

Let J be a maximal element of $\mathscr{S}$. We claim that J is prime. To see this, if we assume that J is not prime, then there must exist $a, b \in R \setminus J$ such that $ab \in J$. Write $J_1 := J + Ra$ and $J_2 := J + Rb$. Since J is maximal in $\mathscr{S}$, and $J \subsetneq J_1, J_2$, we see that $J_1, J_2 \notin \mathscr{S}$. Thus there

must exist $n_1, n_2 \geq 1$ such that $x^{n_1} \in J_1$ and $x^{n_2} \in J_2$. Then $x^{n_1+n_2} \in J_1 J_2 \subseteq J + Rab \subseteq J$, but this contradicts the fact that $J \cap T = \emptyset$.

Therefore $J \in \mathscr{S}$ is prime. But this is a contradiction! Recall that

$$J \supseteq \bigcap_{\substack{P \supseteq (0) \\ P \text{ prime}}} P = \sqrt{(0)},$$

since J is a prime; therefore $x \in J$. The claim follows. □

Corollary 11.2. *If I is an ideal of R and $x \in \sqrt{I}$, then there exists $n = n(x) \geq 1$ such that $x^n \in I$.*

Proof. Let $S := R/I$ and apply the correspondence theorem to see that $\sqrt{(0)} \in S$ is matched with $\sqrt{I}$ in R. If $x \in \sqrt{I}$ then $(x + I)^n = 0$ in S, so $x^n \in I$. □

Proposition 11.3. *If R is a ring, then $a_0 + a_1 x + \cdots + a_n x^n \in R[x]$ is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_n$ are nilpotent.*

Proposition 11.4. *Let R be a Noetherian ring and I a nil ideal of R. Then I is nilpotent, i.e., $I^n = (0)$ for some $n \geq 1$.*

Proof. Suppose otherwise. Let $\mathscr{S} = \{J : J \text{ ideal of } R, \pi(I) := (I + J)/J \text{ is not nilpotent in } R/J, \pi : R \to R/J \text{ canonical projection}\}$. Since $(0) \in \mathscr{S}$, then $\mathscr{S} \neq \emptyset$. Let $J \in \mathscr{S}$ be a maximal element. We claim that J is prime. Otherwise, then we can find $a, b \in R \setminus J$ such that $ab \in J$. Let $J_1 = J + Ra, J_2 = J + Rb$. By maximality of J, neither J_1 nor J_2 can be in $\mathscr{S}$. Hence $\pi(I)$ in R/J_i is nilpotent for $i = 1, 2$.

(Aside: What does it meant to say that $\pi(I)$ is in R/L, where $\pi : R \to R/L$? Note that $\pi(I)$ is nilpotent if and only if $\pi(I)^n = (0)$ if and only if $(I + L)^n/L = L/L$ if and only if $I^n \subseteq L$. Therefore there exist $n_1, n_2 \geq 1$ such that $I^{n_1} \subseteq J_1$ and $I^{n_2} \subseteq J_2$, from which $I^{n_1+n_2} \subseteq J_1 J_2 \subseteq J$ follows.)

Therefore we produced $J \in \mathscr{S}$ that is also a prime. But then we see that $\pi(I)$ is a nil ideal but not a nilpotent ideal in R/J (integral domain). But the only nilpotent element in R/J is 0, meaning $\pi(I) \subseteq (0)$ and this is a contradiction. The result follows. □

Theorem 11.5 (Hilbert's basis theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian also.*

Remark 11.1. Subring of a Noetherian ring need not be Noetherian! Note that $R = \mathbb{C}(x_1, x_2, \ldots)$ is Noetherian since R is a field, but within R lies a polynomial ring $\mathbb{C}[x_1, x_2, \ldots]$. The polynomial ring is not Noetherian.

Lemma 11.6. *If S is Noetherian, then so is S/I (correspondence).*

Corollary 11.7. *The converse of Hilbert's basis theorem holds also. Just let $S := R[x]$ and $I := (x)$.*

Corollary 11.8. *If R is a Noetherian, then $R[x_1, x_2, \ldots, x_s]$ is Noetherian also (by induction). Therefore $R[x_1, \ldots, x_s]/I$ is Noetherian.*

Definition 11.9. A ring of the form $R[x_1, \ldots, x_s]/I$ is called a *finitely generated R-algebra*. Particularly, if k is a field, then a finitely generated k-algebra is Noetherian.

Notation. Given $p(x) = p_0 + p_1 x + \cdots + p_n x^n \in R[x]$ with $p_n \neq 0$, define $\text{in}(p(x)) = p_n \in R$.

Proof. Let I be an ideal of $R[x]$. We will show that I is finitely generated as an ideal. Pick $f_1(x) \in I \setminus \{0\}$ of smallest degree. Then let $d_1 = \deg f_1(x); a_1 = \text{in}(f_1(x))$; and let $J_1 = a_1R$. Let $I_1 = f_1(x)R(x) \subseteq I$. If $I = I_1$, we are done. Otherwise, choose $f_2(x) \in I \setminus I_1$ with minimal degree. Let $d_2 = \deg f_2$, and let $a_2 = \text{in}(f_2)$. Let $J_1 \subseteq J_2 := a_1R + a_2R$ and $I_2 = f_1(x)R[x] + f_2(x)R[x] \subseteq I$. Note that $d_2 \geq d_1$ because we picked f_1 to be the polynomial of the *smallest degree*. The idea is that this process should stop at some point, and we will use that fact to show that J_i must terminate also. □

12. January 29

Theorem 12.1 (Hilbert basis theorem)**.** *If R is Noetherian, then $R[x]$ is Noetherian also.*

Proof. Let I be an ideal of $R[x]$. We will show that I is finitely generated as an ideal. Without loss of generality let I be a non-zero ideal.

Step 1. Pick $f_1(x) = a_1x^{d_1} + \text{lower degree terms} \in I \setminus \{0\}$ of minimal degree d_1. Note $a_1 = \text{in}(f_1) \in R$; then let $I_1 = f_1(x)R[x] \subseteq I$, and define $J_1 = a_1R$.

Step 2. If $I = I_1$, stop. We are done by letting $I = (f_1(x))$. Otherwise, pick $f_2(x) = a_2x^{d_2} + \text{lower degree terms} \in I \setminus I_1$ of minimal degree. Let $I_2 = f_1(x)R[x] + f_2(x)R[x]$, and let $J_2 = a_1R + a_2R$. Recall that $d_2 \geq d_1$. In general, we keep going in order to produce $f_1(x), \ldots, f_{n-1}(x) \in R[x], a_1, \ldots, a_{n-1} \in R, d_1, \ldots, d_{n-1} \in \mathbb{N}$; and let $I_{n-1} := f_1(x)R[x] + \cdots + f_{n-1}(x)R[x]$ and $J_{n-1} = a_1R + a_2R + \cdots + a_{n-1}R$, where $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_{n-1} \subseteq I$ and $J_1 \subseteq J_2 \subseteq \cdots \subseteq J_{n-1} \subseteq R$.

If $I = I_{n-1}$, we can stop: I is finitely generated. Otherwise, pick $f_n(x) = a_nx^{d_n} + \cdots + a_0 \in I \setminus I_{n-1}$ of minimal degree d_n. As before, we have $d_1 \leq d_2 \leq \cdots \leq d_{n-1} \leq d_n$, with $I_n = I_{n-1} + f_n(x)R[x]$ and $J_n := J_{n-1} + a_nR$. If there exists m such that $I = I_m$, then we have that I is generated by $(f_1(x), \ldots, f_n(x))$, and we are done. Thus we may assume that $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$. But since R is Noetherian, the chain $J_1 \subseteq J_2 \subseteq \cdots$ must terminate in R. Hence there must exist m such that $J_m = J_{m+1} = \cdots$. We claim that this implies $I_m = I_{m+1}$, thereby deriving a contradiction.

Recall that we picked $f_{m+1}(x) \in I \setminus I_m$ of minimal degree so that $\deg f_{m+1} \geq \deg f_m$. Now $a_{m+1} \in J_{m+1} = J_m = a_1R + \cdots + a_mR$. So there exists $r_1, \ldots, r_m \in R$ such that $a_{m+1} = r_1a_1 + \cdots + r_ma_m$. Since $r_1f_1(x), r_2f_2(x), \cdots r_mf_m(x) \in I_m$ Note that $d_{m+1} \geq d_1, \ldots, d_m$. So $f_{m+1}(x) - r_1x^{d_{m+1}-d_1}f_1(x) - r_2x^{d_{m+1}-d_2}f_2(x) - \cdots - r_mx^{d_{m+1}-d_m}f_m(x) =: g(x)$. Hence $g(x)$ has degree at most $d_{m+1} - 1$. Note that $g(x) \in I_m$. Since $f_{m+1}(x) \in I \setminus I_m$ was chosen as an element of smallest degree in $I \setminus I_m$ and $\deg(g(x)) < d_{m+1} = \deg(f_{m+1})$ we have $g(x) \in I_m$. But this implies that $f_{m+1}(x) = g(x) + r_1^{d_{m+1}-d_1}f_1(x) + \cdots + r_mf_m(x)x^{d_{m+1}-d_m} \in I_m$, a contradiction. Hence $I = I_m$. □

12.1. **Jacobson radicals.**

Definition 12.2. Let R be a ring. We define the *Jacobson radical* of R to be

$$J(R) := \bigcap_{M \text{ maximal ideal}} M \supseteq \bigcap_{P \text{ prime}} = \sqrt{(0)}.$$

Example 12.3. $J(\mathbb{Z}) = \bigcap_{p \text{ prime}} p\mathbb{Z} = (0)$. In this case, the nilradical and Jacobson radical are equal.

Example 12.4. Let $R = \{ab^{-1} : a \in \mathbb{Z}, b \in \mathbb{Z}, b \equiv 1 \pmod 2\}$. Then the maximal ideal of R is $P = \{ab^{-1} : a \equiv 0 \pmod 2, b \equiv 1 \pmod 2\}$. Then we have a homomorphism $\phi : R \to \mathbb{Z}/2\mathbb{Z}$ defined by $\phi(ab^{-1}) = a + 2\mathbb{Z} = ab^{-1} + 2\mathbb{Z}$, and $\ker \phi = P$. In fact, P is the *only* maximal ideal of R. If $Q \subsetneq R$ is a proper ideal, then $Q \subseteq P$. Suppose otherwise. Then there exists $ab^{-1} \in R \setminus P$. We know that a must be odd since $ab^{-1} \notin P$. But then $ba^{-1} \in R$ so ab^{-1} is a unit. Therefore $1 = (ab^{-1})(ba^{-1}) \in R(a/b) \subseteq Q$. So P is the maximal ideal So $J(R) = P = 2R$.

Now we prove some propositions that give alternate definitions of Jacobson radicals

Proposition 12.5. *$x \in J(R) \Leftrightarrow 1 + ax$ is a unit of R for all $a \in R$.*

Proof. ($\Rightarrow$) Suppose that $x \in J(R)$ and $a \in R$. Then $ax \in J(R)$. Suppose that $1 + ax$ is not a unit. Then $R(1 + ax) \subsetneq R$. So there must exist a maximal ideal M such that $1 + ax \in M$. But since $ax \in J(R)$, by definition $ax \in M$. Therefore $1 \in M$. Contradiction!

($\Leftarrow$) Suppose that $1 + ax$ is a unit for all $a \in R$ but $x \notin J(R)$. Then there must exist a maximal ideal M such that $x \notin M$. So $x + M \in R/M$, and $x + M \neq 0 + M$. Clearly R/M is a field. So there must exist $a + M \in R/M$ so that $(-a + M)(x + M) = 1 + M$. Therefore $(1 + ax) + M = 0 + M$, so $1 + ax \in M$. Contradiction! □

Definition 12.6. A ring R is called a *Jacobson ring* if for every prime ideal P of R we have $J(R/P) = (0)$.

Example 12.7. Any field is a Jacobson ring. $\mathbb{Z}$ is another example of a Jacobson ring.

13. January 30

Remark 13.1. If R is a Jacobson ring, then by the correspondence theorem

$$\bigcap_{\substack{M \supset P \\ M \text{ maximal}}} M = P,$$

so

$$\bigcap_{M \text{ maximal}} M = \bigcap_{P \text{ prime}} P.$$

Theorem 13.1 (Nakayama's lemma)**.** *Let R be a ring and M be a* finitely generated *R-module. If $J(R)M = M$, then $M = (0)$.*

Example 13.2. Let $R = \{f(x)/g(x), f(x), g(x) \in \mathbb{C}[x], g(0) \neq 0\}$ be a ring. Then $J(R) = xR$, and xR is a maximal ideal of R and xR is *the* maximal ideal. Since the map givens by $f(x)/g(x) \mapsto f(0)/g(0)$ is a surjective homomorphism with kernel xR, by the first isomorphism theorem we have $R/xR \cong \mathbb{C}$. $J(R) = xR$ since xR is the unique maximal ideal.

Now consider $M = \mathbb{C}(x)$, and $r \in R, f(0)/g(0) \in M$. We say that, if $rf(x)/g(x) \in M$ then $J(R)M = M$.

If $a(x)/b(x) \in M$ then $a(x)/b(x) = x[a(x)/(b(x)x)]$. Therefore $J(R)M = M$. So we really need M to be finitely generated.

Remark 13.2 (Usefulness of Nakayama's lemma). If R is a local ring with the unique maximal ideal P and if M is a finitely-generated R-module then M/PM is an R/P-module. Since R/P is a field, we can view M/PM as an $R/P(= F)$-vector space.

If $m_1, \dots, m_d \in M$ have the property that $\overline{m_1}, \dots, \overline{m_d} \in M/PM$ form a basis for M/PM as an F-vector space, then $M = Rm_1 + Rm_2 + \cdots + Rm_d$. We will try to prove this claim.

Let $N = Rm_1 + \cdots + Rm_d$, which is indeed a submodule of M. Define $A = M/N$. Then $J(R)A = PA = P(M/N) = (PM + N)/N$. But $PM + N = M$ because $M/PM = \langle m_1, \dots, m_d \rangle$ meaning that $M/PM = \overline{N}$, so equivalently $PM + N = M$. So by Nakayama's lemma, $A = 0$. Therefore $M = N$.

Proof of Theorem 13.1. Suppose that M is finitely generated and $J(R)M = M$ with $M \neq (0)$. Then because M is finitely generated and non-zero, there exists $d \geq 1$ and $m_1, \dots, m_d \in M$ such that $M = Rm_1 + \cdot + Rm_d$. Morevover, we may assume that d is minimal with respect to there being a generating set of size d.

$J(R)M = M$, so $M = \{j_1 m_1 + \cdots + j_d m_d : j_1, \dots, j_d \in J(R)\}$. We have $m_d = j_1 m_1 + \cdots + j_d m_d$ for some $j_1, \dots, j_d \in J(R)$. Write $(1 - j_d)m_d = j_1 m_1 + \cdots + j_{d-1} m_{d-1}$. But then $1 - j_d$ is a unit, so $m_d \in (1 - j_d)^{-1} j_1 m_1 + \cdots + (1 - j_d)^{-1} j_{d-1} m_{d-1} \in Rm_1 + \cdots + Rm_{d-1}$. Hence $M = Rm_1 + Rm_2 + \cdots + Rm_{d-1}$, but this contradicts the minimality of d. So $M = (0)$. $\square$

13.1. **Localization.**

Example 13.3. We start with a specific example, to give an idea on what localization is about. Think of $R = \mathbb{Z}$ and $S = \mathbb{Z} \setminus \{0\}$. Then $\mathbb{Q} = S^{-1}R = \{(a, b) : a \in R, b \in S\}/\sim$ where $(a, b) \sim (c, d)$ iff $a/b = c/d$. This is an example of localization.

Definition 13.4. Let R be a ring. A subset $S \subseteq R \setminus \{0\}$ is said to be *multiplicatively closed* if:

- $1 \in S$
- $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$

Given a ring R and a multiplicatively closed subset $S \subseteq R$, we can define the *localization of R with respect to S*, which we denote $S^{-1}R$.

As a set, $S^{-1}R = R \times S/\sim$ where $(r_1, s_1) \sim (r_2, s_2)$ iff there exists some $s' \in S$ such that $s'(s_1 r_2 - s_2 r_1) = 0$. We claim that $\sim$ is an equivalence class. We will only prove transitivity since the other two are evident. Suppose that $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. So there exist $s', s'' \in S$ such that

$$s'(s_2 r_1 - s_1 r_2) = 0 \tag{2}$$

$$s''(s_3 r_2 - s_2 r_3) = 0. \tag{3}$$

So we need to construct s''' so that $s'''(s_3 r_1 - s_1 r_3) = 0$:

$$\begin{aligned} s'' s_3 \times (2) - s_1 s' \times (3) &= s'' s_3 s_2 r_1 - s'' s_3 s' s_1 r_2 + s'' s_3 s' s_1 r_2 - s'' s_2 s_a s' r_3 \\ &= s' s_2 s''(r_1 s_3 - r_3 s_1) = 0. \end{aligned}$$

So letting $s''' = s' s_2 s''$ proves the claim.

We see that $R \times S/\sim$ is a ring, with addition and multiplication being

$$\begin{aligned} s_1^{-1} r_1 \cdot s_2^{-1} r_2 &= (s_1 s_2)^{-1}(r_1 r_2) \\ s_1^{-1} r_1 + s_2^{-1} r_2 &= (s_1 s_2)^{-1}(r_1 s_2 + r_2 s_1). \end{aligned}$$

You can check if it's well-defined and satisfies ring axioms.

14. February 3

We know that $\mathbb{Z} \subset \mathbb{Q}$,but it is not necessarily true in general that R embeds into $S^{-1}R$. Consider the following example:

Example 14.1. Let $R = \mathbb{Z} \times \mathbb{Z}$ and $S = ((\mathbb{Z} \setminus \{0\}) \times \{0\}) \cup \{(1,1)\}$. Then S is multiplicatively closed, and $0 \notin S$. Let $(a,b),(c,d) \in R$ and $(s,t),(s',t') \in S$. Then $((a,b),(s,t)) \sim ((c,d),(s',t')) \Leftrightarrow \exists (v,0) \in S$ such that $(v,0)\cdot(a,b)\cdot(s',t') = (v,0)\cdot(c,d)\cdot(s,t)$. This happens iff $as' = cs$. Thus, $S^{-1}R \to Q$, with embedding $[(a,b),(s,t)] \mapsto as^{-1}$.

In particular, $R \to S^{-1}R$ defined by $r \mapsto 1^{-1}r$ is *not* an embedding since the map is not injective. To see why, note that $(0,b)$ is in the kernel for any $b \in \mathbb{Z}$.

Definition 14.2. We say that S is *regular* if S does not contain zero divisors.

Proposition 14.3. *If S is regular, then $R \to S^{-1}R$ defined as $r \mapsto 1^{-1}r$ is an embedding.*

Proof. If $1^{-1}r = 1^{-1}r'$, then there must exist $s \in S$ such that $s(r - r') = 0$. But since S is regular, s cannot be a zero-divisor. Hence $r = r'$. □

Remark 14.1. If $I \subset R$ is an ideal and $S \subset R$ is multiplicatively closed, then $S^{-1}I = \{s^{-1}r : s \in S, r \in R\}$ is an ideal of $S^{-1}R$.

14.1. Universal property of localization.

Theorem 14.4 (Universal property of localization)**.** *Let R be a ring and S be a multiplicatively closed regular subset of R. Then if T is another ring, and $\phi : R \to T$ is a ring homomorphism such that $\phi(S) \subset T^\times$ (units of T), then ϕ extends to a homomorphism from $S^{-1}R$ into T, and this extension is unique: if ϕ is injective, then the extension is injective as well.*

Proof. We first prove the existence. We define $\psi : S^{-1}R \to T$ by $\psi(s^{-1}r) = \phi(s)^{-1}\phi(r)$. We will show that this extension works. Note that $\phi(s)^{-1}$ exists since $\phi(s) \in T^\times$. First, we need to show that ψ is well-defined. Let $s_1^{-1}r_1 = s_2^{-1}r_2$. Then there exists $s_3 \in S$ such that $s_3(s_1r_2 - s_2r_1) = 0$. Since s_3 is not a zero-divisor, $s_1r_2 = s_2r_1$. Hence $\phi(s_1)\phi(r_2) = \phi(s_2)\phi(r_1)$, from which $\phi(s_1)^{-1}\phi(r_1) = \phi(s_2)^{-1}\phi(r_2)$. Therefore, ψ is well-defined. If $r \in R$, then $\psi(1^{-1}r) = (\phi(1))^{-1}\phi(r) = \phi(r)$, so ψ indeed extends ϕ.

We need ψ to be a homomorphism:

$$\begin{aligned}\psi(s_1^{-1}r_1s_2^{-1}r_2) &= \psi((s_1s_2)^{-1}(r_1r_2)) = \phi(s_1s_2)^{-1}\phi(r_1r_2)\\ &= \phi(s_1)^{-1}\phi(r_1)\phi(s_2)^{-1}\phi(r_2) = \psi(s_1^{-1}r_1)\psi(s_2^{-1}r_2).\end{aligned}$$

Also,

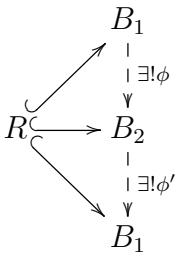
$$\begin{aligned}\psi(s_1^{-1}r_1 + s_2^{-1}r_2) &= \psi((s_1s_2)^{-1}(s_2r_1 + s_1r_2)) = \phi(s_1s_2)^{-1}\phi(s_2r_1 + s_1r_2)\\ &= \phi(s_1)^{-1}\phi(s_2)^{-1}(\phi(s_1)\phi(r_2) + \phi(s_2)\phi(r_1)) = \psi(s_1^{-1}r_1) + \psi(s_2^{-1}r_2).\end{aligned}$$

This proves existence.

Suppose that $f : S^{-1}R \to T$ is any extension of ϕ to a homomorphism. Then $1 = f(1) = f(s^{-1}s) = f(s^{-1})f(s) = f(s^{-1})\phi(s)$. Therefore $f(s^{-1}) = \phi(s)^{-1}$. So $f(s^{-1}r) = f(s^{-1})F(R) = \phi(s)^{-1}\phi(r) = \psi(s^{-1}r)$, proving uniqueness.

Finally, assume that ϕ is injective and let $s^{-1}r \in \ker\psi$. Then $\phi(s)^{-1}\phi(r) = 0$, so $r \in \ker\phi$. But since ϕ is injective, we have $r = 0$. Consequently, ψ is injective. □

Remark 14.2. Uniqueness gives that $S^{-1}R$ is a unique ring up to isomorphism with the universal property. Suppose B_1, B_2 both have this universal property. Then note that $\phi' \circ \phi = \mathrm{id}_{B_1}$. Reverse the role of B_1 and B_2 to get $\phi \circ \phi' = \mathrm{id}_{B_2}$. Hence $B_1 \cong B_2$ as desired.



Example 14.5. Suppose that $f \in R$ is not nilpotent, and let $S = \{1, f, f^2, \dots\}$. Let $R_f := S^{-1}R$.

If P is a prime ideal in R and $S = R \setminus P$, then S is multiplicatively closed. Write $R_P := S^{-1}R$. Note that R_P has an ideal $PR_p = \{s^{-1} : S \notin P, r \in P\}$. We shall show that PR_P is a prime ideal.

Let $T := \mathrm{Frac}(R/P)$. Define $\phi : R \to T$ by $r \mapsto (r + P)/1$. If $s \in S = R \setminus P$, then $\phi(s) \in T^\times$. Let $\psi : R_P \to T$ be the unique extension of ϕ (universal property).

Note that ψ is surjective. If $x = (a+P)/(b+P)$, where $b \notin P$, then $b \in S$ and $\psi(b^{-1}a) = x$. Hence $\ker(\psi)$ is a maximal ideal of R_P, since T is a field. But $\ker\psi = \{s^{-1}r, s \in S, r \in P\} = PR_P$. So PR_P is a maximal ideal of R_P *a fortiori*.

15. February 5

Definition 15.1. A ring R is a *local ring* if it has a unique maximal ideal.

Recall that if R_P is a local ring (R a ring and P a prime ideal) then PR_P is a (in fact *the*) maximal ideal.

Proposition 15.2. *If R is a ring and $\mathfrak{M}$ is a maximal ideal, then $\mathfrak{M}$ is the* unique *maximal ideal of R if and only if $1 + x$ is a unit for all $x \in \mathfrak{M}$.*

Proof. If $\mathfrak{M}$ is unique, then $J(R) = \bigcap_{P \text{ maximal}} P = \mathfrak{M}$, so $1+x$ is a unit for all $x \in J(R) = \mathfrak{M}$. If $\mathfrak{M}$ is not unique, then there exists a maximal ideal $\mathfrak{Q} \neq \mathfrak{M}$. Then $\mathfrak{Q} + \mathfrak{M} = R$. So there exists $q \in \mathfrak{Q}$ and $x \in \mathfrak{M}$ such that $q - x = q + (-x) = 1$. So $q = 1 + x$. But q is not a unit since $q \in \mathfrak{Q}$. But $x \in \mathfrak{M}$ so there exists $\mathfrak{M}$ such that $1 + x$ is not a unit. Contradiction! $\square$

So $\mathfrak{P}R_\mathfrak{P}$ is the unique maximal ideal of $R_\mathfrak{P}$. To see why, start with $x \in \mathfrak{P}R_\mathfrak{P}$. Then $x = s^{-1}a$ where $s \in S = R \setminus \mathfrak{P}$ and $a \in \mathfrak{P}$. So $1 + x = s^{-1}s + s^{-1}a = s^{-1}(s + a)$, so letting $s + a = t \in \mathfrak{P}$ we have $(s^{-1}t)^{-1} = t^{-1}s$ so $t \in S$.

Definition 15.3. Let R be a ring and $S \subseteq R$ be a multiplicatively closed subset that has no zero divisors (regular). Given an ideal J of R, we say that J is *S-saturated* if whenever $s \in S$ and $x \in R$ are such that $sx \in J$ we necessarily have $x \in J$.

Example 15.4. If $R = \mathbb{Z}$ and $S = \{1, 2, 2^2, 2^3, \cdots\}$ then $3\mathbb{Z}$ is S-saturated but $4\mathbb{Z}$ is not.

Proposition 15.5. *Let R be a ring and let S be a multiplicatively closed set of regular elements. Then there exists an inclusion-preserving bijection between the poset of proper ideals of $S^{-1}R$ and the poset of S-saturated ideals of R that intersects with S trivially.*

Example 15.6. Let $R = \mathbb{Z}$ and $S = \{1, 2, 2^2, 2^3, \dots\}$. Then $S^{-1}R$ has proper ideals. The proper ideals of $S^{-1}R$ are $S^{-1}(nR)$ where $n > 1$ and n odd.

Proof. Let I be an ideal of $S^{-1}R$ and J an ideal of R such that $J \cap S = \emptyset$. Consider the mappings $f : I \mapsto f(I) = I \cap R$ and $g : J \mapsto S^{-1}J$, and verify that they are bijections.

First, if I is a proper ideal of $S^{-1}R$, then what is $g \circ f(I)$? We claim that $g \circ f(I) = S^{-1}(I \cap R) \stackrel{?}{=} I$. Notice that $I \cap R \subseteq I$ and since I i an ideal, we have $S^{-1}(I \cap R) = S^{-1}I = I$, as desired. Conversely, to see that $I \subseteq S^{-1}(I \cap R)$, let $x \in I$. Then $x = s^{-1}a$ for some $s \in S$ and $a \in R$. Since I is an ideal of $S^{-1}R$, $sx = a \in I$ so $a \in I \cap R$. Thus $x = s^{-1}a \in S^{-1}(I \cap R)$. Thus $I \subseteq S^{-1}(I \cap R)$.

If J is an S-saturated ideal of R and $J \cap S = \emptyset$, then what is $f \cap g(J)$? We claim that $f \cap g(J) = S^{-1}J \cap R = J$. The inclusion $J = 1^{-1}J \cap R \subseteq S^{-1}J \cap R$ is clear. For the other way, start with $x \in S^{-1}J \cap R$. Then $x \in S{-}1J$, so there exist $s \in S$ and $j \in J$ such that $x = s^{-1}j$. So $sx = j \in J$. So $x \in J$ since J is S-saturated. Thus $x \in R$. So $S^{-1}J \cap R \subseteq J$.

Notice that if I is a proper ideal of $S^{-1}R$, then $f(I)$ is S-saturated. Notice that if I is a proper ideal of $S^{-1}R$, then $f(I)$ is S-saturated. Next, if J an S-saturated ideal of R and $J \cap S = \emptyset$ then $g(J) = S^{-1}J$ is a proper ideal. Otherwise, then $1 \in S^{-1}J$ so $s^{-1}j = 1$ for some $s \in S$ and $j \in J$, hence $j = s$, which is a contradiction. □

Corollary 15.7. *Let R be a ring and let $S \subseteq R$ be a multiplicative closed subset of regular elements. If R is Noetherian, then $S^{-1}R$ is Noetherian.*

Remark 15.1. Notice that the converse *does not hold*. Consider $R = \mathbb{C}[x_1, x_2, \dots]$ and $S = R \setminus \{0\}$. Then $S^{-1}R = \mathbb{C}(x_1, x_2, \dots)$. $S^{-1}R$ is a field of fraction of R, so $S^{-1}R$ is automatically Noetherian. But R is not Noetherian.

Proof. Let $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$ be a chain of ideals in $S^{-1}R$. If $J_n = S^{-1}R$ for some n, then $J_n = J_{n+1} = J_{n+2} = \cdots$. Otherwise, we can apply the map f to get a chain $f(J_1) \subseteq f(J_2) \subseteq f(J_3) \subseteq \cdots$ of ideals in R. Since R is Noetherian, there exists n such that $f(J_n) = f(J_{n+1}) = \cdots$. Hence $J_n = g(f(J_n)) = J_{n+1} = g(f(J_{n+1})) = \cdots$. So $S^{-1}R$ is Noetherian as well, as required. □

Theorem 15.8. *Suppose that F is a field and K/F is a* finitely generated *(not necessarily finite) field extension. If L is an intermediate field between F and K (i.e., $F \subseteq L \subseteq K$), then L/F is also a finitely-generated field extension.*

Remark 15.2. The above theorem need not hold when it comes to algebras. Note that $\mathbb{C}[x, y]$ is a finitely-generated $\mathbb{C}$-algebra, but $\mathbb{C}[x^i y^{i+1} : i \geq 1]$ is not a finitely generated subalgebra of $\mathbb{C}[x, y]$.

Remark 15.3. Let's come back to the correspondence mappings f and g we discussed in the proof of Proposition 15.5. These bijections restrict to bijections between prime ideals of $S^{-1}R$ and $\{\mathfrak{P} \subseteq R : \mathfrak{P} \text{ prime}, \mathfrak{P} \cap S = \emptyset\}$.

16. February 6

Definition 16.1. Given a ring R, we let $\mathrm{Spec}(R)$ denote the *set of prime ideals of R.*

Remark 16.1. $\mathrm{Spec}(R)$ is a poset with respect to $\subseteq$.

Example 16.2. $\mathrm{Spec}(\mathbb{Z}) = \{2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, 7\mathbb{Z}, \cdots\}$.

Let R be a ring, and $S \subseteq R$ a multiplicatively closed regular set. Last time, we gave an inclusion-preserving bijection between the set of proper ideals of $S^{-1}R$ and the set of S-saturated ideals of R that intersect with S trivially, with the map given by $I \overset{f}{\mapsto} I \cap R$ and $S^{-1}J \overset{g}{\hookleftarrow} J$.

These bijections send prime ideals to prime ideals. If P is prime in $S^{-1}R$, then $f(P \cap R) \subseteq R$ is prime in R. To see why, suppose that $ab \in f(P)$ with $a, b \in R$. Then $ab \in P \cap R \subseteq P$, so $a \in P$ or $b \in P$. Therefore $a \in P \cap R = f(P)$ or $b \in P \cap R = f(P)$.

Conversely, if $Q \leq R$ with Q prime, then $Q \cap S = \emptyset$: notice that this implies that Q is S-saturated. Suppose $s \in S, x \in R$ and $sx \in Q$. Thus $s \in Q$ or $x \in Q$, hence $x \in Q$. Then $g(Q)$ is prime in $S^{-1}R$. Suppose that $s_1^{-1}a, s_2^{-1}b \in S^{-1}R$ and $s_1^{-1}as_2^{-1}b \in g(Q)$. Thus $(s_1s_2)^{-1}(ab) \in g(Q)$, hence $ab \in g(Q) \cap R = Q$. Thus $a \in Q$ or $b \in Q$, which implies that $s_1^{-1}a \in g(Q)$ or $s_2^{-1}b \in g(Q)$. Hence the maps f and g restrict to:

$$\operatorname{Spec}(S^{-1}R) \longleftrightarrow \{Q \in \operatorname{Spec}(R) : Q \cap S = \emptyset\}.$$

Example 16.3 (One special case). Let R be a ring and x a non-zero divisor. Let $S = \{1, x, x^2, \cdots\}$. Then there is a correspondence between

$$\operatorname{Spec}(R_x) \longleftrightarrow \{Q \in \operatorname{Spec}(R) : Q \cap \{1, f, f^2, \cdots\} = \emptyset\} = \{Q \in \operatorname{Spec}(R) : f \notin Q\}.$$

Example 16.4. Let R be a integral domain, and let P be a prime ideal. Let $S = R \setminus P$. Then $S^{-1}R = R_P$. Then there is a correspondence

$$\operatorname{Spec}(R_P) \longleftrightarrow \{Q \in \operatorname{Spec}(R) : Q \cap S = \emptyset\} = \{Q \in \operatorname{Spec}(R) : Q \subset P\}.$$

This gives another proof that R_P is a local ring.

Example 16.5 ($\operatorname{Spec}(R)$ vs $\operatorname{Spec}(R_P)$ vs $\operatorname{Spec}(R/P)$). $\operatorname{Spec}(R)$ denotes the set of all prime ideals of R. Recall that $\operatorname{Spec}(R_P)$ and the set of prime ideals of R contained in P have one-to-one correspondence. On the other hand, by the correspondence theorem of ideals, we see that $\operatorname{Spec}(R/P)$ and the set of prime ideals of R containing P a prime ideal have one-to-one correspondence.

Remark 16.2. In Assignment #2, you will show that if K is a field extension of a field F then K is finitely generated as an extension of F. This can be deduced by showing that $K \otimes_F K$ is Noetherian. In fact, in the assignment you will show that if $K \otimes_F K$ is Noetherian, then any field L with $F \subseteq L \subseteq K$ is finitely generated over F.

Theorem 16.6. *Let $F \subseteq K$ be a finitely-generated field extension. If $F \subseteq L \subseteq K$ and L is a field, then L/F is finitely generated as well.*

Proof. By Assignment #2, it suffices to show that $K \otimes_F K$ is Noetherian.

Step 1. Since K/F is finitely generated, there exist $a_1, a_2, \ldots, a_d \in K$ such that $K = F(a_1, a_2, \ldots, a_d)$. Let $A = F[a_1, a_2, \ldots, a_d] = \{\sum \alpha_{i_1,\ldots,i_d} a_1^{i_1} \cdots a_d^{i_d} : \alpha_{i_1,\ldots,i_d} = 0 \text{ for all but finitely many } (i_1, \ldots, i_d)\}$. Then A is a finitely generated F-algebra. So by the Hilbert basis theorem, A is Noetherian.

Step 2. On Assignment #2, you will show that if A and B are finitely generated F-algebra, then $A \otimes_F B$ is ale finitely generated. So since $A = F[a_1, \ldots, a_d]$ is finitely generated as an F-algebra, so is $A \otimes_F A$. Again by the Hilbert basis theorem, $A \otimes_F A$ is Noetherian.

Step 3. Let $S = A \setminus \{0\}$, which is multiplicatively closed and regular. Let $T = \{s_1 \otimes s_2 : s_1, s_2 \in S\}$. We will show that $T^{-1}(A \otimes_F A) \cong S^{-1}A \otimes_F S^{-1}A = K \otimes_F K$ and that T is

regular. So, if $A \otimes_F A$ is Noetherian, then $T^{-1}(A \otimes_F A)$ is Noetherian, which shows that $K \otimes_F K$ is Noetherian (then we are home free). $\square$

Proposition 16.7. *Let A, B be F-algebras and let S, T be multiplicatively closed, regular subsets of A and B respectively. Then if $U = \{s \otimes t : s \in S, t \in T\}$, then $U^{-1}(A \otimes_F B) \cong S^{-1}A \otimes_F T^{-1}B$.*

Proof. Let $f : A \to S^{-1}A$ given by $a \mapsto 1^{-1}a$ and $g : B \to T^{-1}B$ given by $b \mapsto 1^{-1}b$. SO we have a homomorphism $f \otimes g : A \otimes_F B \to S^{-1}A \otimes_F T^{-1}B$. Notice that if $s \otimes t \in U \mapsto f(s) \otimes g(t) = s \otimes t$, then $s \otimes t$ is a unit in $S^{-1}A \otimes T^{-1}B$ with inverse $s^{-1} \otimes t^{-1}$. So $f \otimes g$ extends to a homomorphism. SInce $f \otimes g : U^{-1}(A \otimes_F B) \to S^{-1}A \otimes_F T^{-1}B$ by the universal property of localization, all that remains is to show $f \otimes g$ is an isomorphism:

(1) $f \otimes g$ is surjective
$S^{-1}A \otimes T^{-1}B$ is generated by things of the form $s^{-1}a \otimes t^{-1}b = f \otimes g((s \otimes t)^{-1}(a \otimes b))$.
(2) $f \otimes g$ is injective
One has to be careful here: even though $f : A \to C$ and $g : B \to D$ are injective, $f \otimes g : A \otimes_R B \to C \otimes_R D$ *need not* be injective. Consider $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ defined by $[a] \mapsto [2a]$. But $f \otimes f$ has the non-trivial kernel, since $(f \otimes f)(1 \otimes 1) = 2 \otimes 2 = 0$.

$\square$

Example 16.8. If $F = \mathbb{Q}$ and $K = \mathbb{Q}(\pi, \sqrt{2})$, then $A = \mathbb{Q}[\pi, \sqrt{2}]$ is finitely generated F-algebra. Note that

$$A = \left\{ \sum c_{ij} \pi^i \sqrt{2}^j : c_{ij} \in \mathbb{Q}, c_{ij} = 0 \text{ for all but finitely many } (i,j) \right\}.$$

17. February 10

Proposition 17.1. *If A, B, C, D are F-vector spaces and $f : A \to C$ and $g : B \to D$ are injective, then $f \otimes g : A \otimes_F B \to C \otimes_F D$ is also injective.*

Proof. Let $\{X_\alpha\}_{\alpha \in I}$ be a basis for A and $\{Y_\beta\}_{\beta \in J}$ a basis for B. Since f and g are injective, the subsets $\{f(X_\alpha)\}_{\alpha \in I} \subseteq C, \{g(y_\beta)\}_{\beta \in J} \subseteq D$ are both linearly independent. So we can extend $\{f(X_\alpha)\}_{\alpha \in I}$ to a basis $\{z_\gamma\}_{\gamma \in I'}$ for C and similarly extend $\{g(y_\beta)\}_{\beta \in J}$ to a basis $\{w_\delta\}_{\delta \in J'}$ for D. Recall that $\{x_\alpha \otimes y_\beta\}_{(\alpha,\beta) \in I \times J}$ form an F-basis for $A \otimes_F B$. So if $f \otimes g$ is not injective, then there exists $c_{\alpha,\beta} \in F$ not all zero such that $c_{\alpha,\beta} = 0$ for all but finitely many $(\alpha, \beta) \in I \times J$ and such that $(f \otimes g)(\sum c_{\alpha,\beta} x_\alpha \otimes y_\beta) = 0$, or $\sum c_{\alpha,\beta}(f(x_\alpha) \otimes g(y_\beta)) = 0$.

Notice that we may write this as $\sum_{(\gamma,\delta) \in I' \times J'} d_{\gamma,\delta} z_\gamma \otimes w_\delta = 0$, where $d_{\gamma,\delta} = 0$ for all but finitely many (γ, δ), and $d_{\gamma,\delta}$ are not all zero. But this is a contradiction, since $\{z_\gamma \otimes w_\delta\}_{(\gamma,\delta) \in I' \times J'}$ form a basis for $C \otimes_F D$. $\square$

Corollary 17.2. $S^{-1}A \otimes_F T^{-1}B \cong (S \otimes T)^{-1}(A \otimes_F B)$.

Remark 17.1. If S and T are regular in A and B respectively, then $S \otimes T = \{s \otimes t : s \in S, t \in T\} \subseteq A \otimes_F B$ is regular also. Since S and T have no zero divisors, it follows that $f : A \to A$ and $g : B \to B$ given by $f(a) = sa$ and $g(b) = tb$ are injective. Therefore $f \otimes g : A \otimes_F B \to A \otimes_F B$ is injective also, so $s \otimes t$ cannot be a zero divisor.

17.1. **Hilbert's Nullstellensatz ("zero-locus theorem" or "theorem of zeroes").**

Definition 17.3. Recall that R is a *Jacobson ring* if for any $P \in \operatorname{Spec}(R)$ we have $J(R/P) = (0)$.

Example 17.4. Any field F, the polynomial ring of a field $F[x]$, and the ring of (rational) integers $\mathbb{Z}$ are all Jacobson rings.

Definition 17.5. Recall that if R is a ring and S is a ring, then S is an *R-algebra* if there exists a (not necessarily injective) homomorphism from R to S such that $\alpha(1_R) = 1_S$. We say S is *finitely generated as an R-algebra* if there exists $n \geq 1$ and $s_1, \ldots, s_n \in S$ such that every $x \in S$ can be expressed as a polynomial $p(s_1, \ldots, s_n)$ with the coefficients of p in R.

Remark 17.2. Equivalently, if S is finitely generated by $s_1, \ldots, s_n$ as an R-algebra, then there exists a surjective homomorphism $\phi : R[x_1, \ldots, x_n] \to S$ given by $p(x_1, \ldots, x_n) \mapsto p(s_1, \ldots, s_n)$. Therefore if $I = \ker \phi$, then by the first isomorphism theorem we have $S \cong R[x_1, \ldots, x_n]/I$.

Theorem 17.6 (General Nullstellensatz)**.** *Let R be a Jacobson ring and let S be a finitely generated R-algebra. Then*

(1) S is also a Jacobson ring.
(2) if $\mathfrak{M} \subseteq S$ is a maximal ideal of S, then $\alpha(R) \cap \mathfrak{M} =: \mathfrak{N}$ is a maximal ideal of $\alpha(R)$ and $S/\mathfrak{M} =: F$ is a finite extension of $\alpha(R)/\mathfrak{N}$.

Let's first consider a special case: when $R = k = \overline{k}$, an algebraically closed field. Write $S = k[x_1, \ldots, x_n]/I$ where I is a proper ideal. Notice that there is a correspondence between the set of maximal ideals of S and ideals $\mathfrak{M}$ of $k[x_1, \ldots, x_n]$ containing I. So $S/(\text{maximal ideal}) \cong k[x_1, \ldots, x_n]/\mathfrak{M}$ of which the latter is a field and is a finite extension over k. Then $\mathfrak{N} := \mathfrak{M} \cap k$ is a maximal ideal of k, so $\mathfrak{N} = (0)$ and $k/\mathfrak{N} = k$.

If k is algebraically closed, then a finite extension of k must be k itself. Therefore $k[x_1, \ldots, x_n]/\mathfrak{M} \cong k$ so there exist $\lambda_1, \ldots, \lambda_n$ such that $\mathfrak{M} = (x_1 - \lambda_1, \ldots, x_n - \lambda_n)$, with the isomorphism ϕ given by $p(x_1, \ldots, x_n) \mapsto p(\lambda_1, \ldots, \lambda_n)$. Thus $\ker \phi = \mathfrak{M}$.

So far, we haven't seen any "zero locus". So how does this fit in? Start with $f_1(x_1, \ldots, x_n)$, $\ldots, f_d(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ and k algebraically closed (i.e., $k = \overline{k}$). If $I = (f_1, \ldots, f_d)$ is a proper ideal of $k[x_1, \ldots, x_n]$, then there exists $\mathfrak{M} = (x_1 - \lambda_1, \ldots, x_n - \lambda_n) \supseteq I$. This means that $f_1, \ldots, f_d$ are in the kernel of ϕ. Therefore $f_i(\lambda_1, \ldots, \lambda_d) = 0$ for all $1 \leq i \leq d$. Thus $(\lambda_1, \ldots, \lambda_d)$ is the so-called "zero locus".

18. February 12

To do the general Nullstellensatz, we will use the so-called "Rabinowitsch trick", which gives a useful characterization of Jacobson rings.

Theorem 18.1 (Rabinowitsch trick)**.** *Let R be a ring. Then the following are equivalent:*

(1) R is a Jacobson ring.
(2) $J(R/P) = (0)$ for all $P \in \operatorname{Spec}(R)$
(3) For all $P \in \operatorname{Spec}(R)$, P is the intersection of all the maximal ideals containing P.
(4) Whenever $P \in \operatorname{Spec}(R)$, and $T := R/P$ has the property that there exists a non-zero $b \in T$ such that $T_b := \{1, b, b^2, \ldots\}^{-1}T = T[b^{-1}]$ is a field, then T is already a field.

Proof. ((1) $\Rightarrow$ (4)) Suppose that R is Jacobson and let $P \in \mathrm{Spec}(R)$ and let $T := R/P$. Suppose that there exists $b \in T \setminus \{0\}$ such that T_b is a field. Our goal is to show that T is a field. Recall that there is a one to one correspondence between the prime ideals of T_b and the prime ideals of T that *do not* contain b. But since we assume that T_b is a field, it follows that $\mathrm{Spec}(T_b) = \{(0)\}$. Therefore by the correspondence every non-zero prime ideal of T contains b. Now if T is not afield, then every maximal iaedl of T contains b. Therefore, we have

$$J(T) = \bigcap_{\mathfrak{M} \text{ maximal}} \mathfrak{M} \ni b,$$

which implies $J(T) \neq (0)$. But this is a contradiction since R is Jacobson and $T = R/P$.

((4) $\Rightarrow$ (1)) Suppose that whenever $T = R/P$ has the property that there exists a non-zero $b \in T$ such that T_b is a field we must have T is a field. We must show that $J(R/Q) = (0)$ for all $Q \in \mathrm{Spec}(R)$. Towards a contradiction, suppose that $J(R/P) \neq 0$ for some prime ideal P. Let $S = R/P$. Pick $0 \neq b \in J(S)$. Then every maximal ideal of S contains b. Consider the ring $S_b := S[\frac{1}{b}]$. Then there exists a maximal ideal Q of S_b. Recall that there is a bijective correspondence between the two following sets:

$$\begin{aligned} \{\text{prime ideals of } S_b\} &\longleftrightarrow \{\text{prime ideals of } S \text{ that do not contain } b\} \\ Q &\longmapsto S \cap Q \\ S_b Q &\longmapsfrom Q' \end{aligned}$$

So then there exists $Q' \in \mathrm{Spec}(S)$ such that $S_b Q' = Q$ and $b \notin Q'$. Notice that Q' is *not* maximal since $b \notin Q'$. So S/Q' is not a field. Let $0 \neq \bar{b}$ be the image of b in S/Q'. Then $(S/Q')[\frac{1}{b}] \cong S[\frac{1}{b}]/S[\frac{1}{b}]Q' = S_b/Q$, but S/Q' is not a field. Since $R \twoheadrightarrow S \twoheadrightarrow S/Q$, we have $S/Q \cong R/I$ for some prime ideal I of R. This is a contradiction because $(R/I)[\frac{1}{b}]$ is a field but R/I is not.

((1) $\Leftrightarrow$ (2) $\Leftrightarrow$ (3)) These directions are immediate from the definition of the Jacobson ring. $\square$

Theorem 18.2 (Full Nullstellensatz)**.** *Suppose that R is a Jacobson ring, and S is a finitely-generated R algebra, i.e., $S \cong R[x_1, \ldots, x_d]/I$ for some ideal I. Suppose $\alpha(R) = R/(R \cap I)$. Then:*

(1) S is Jacobian.
(2) If $\mathfrak{M}$ is a maximal ideal of S, then $\mathfrak{N} := \mathfrak{M} \cap \alpha(R)$ is a maximal ideal of $\alpha(R)$ and $S/\mathfrak{M}$ is a finite field extension of $\alpha(R)/\mathfrak{N}$.

Proof. Suppose that R is Jacobson. Then R/J is also Jacobson for any proper ideal J. If Q is a prime ideal of R/J, then there exists $P \supset J$ in R such that $R/P = (R/J)/Q$ – since $J(R/P) = (0)$, then $J((R/J)/Q) = (0)$, implying that R/J is Jacobson also. Notice that S is a finitely generated $\alpha(R)$-algebra

$$S \cong (\alpha(R))[x_1, \ldots, x_d]/I, I \cap \alpha(R) = (0).$$

Therefore, without loss of generality we may assume that $\alpha(R) = R$.

The key steps of the proof are the following:

(i) Show that the theorem is true when $S = R[x]$. This is the hardest step.
(ii) Use induction to show that the theorem is true for $S = R[x_1, \ldots, x_d]$

(iii) Use correspondence to show that the theorem is true fro $S = R[x_1, \ldots, x_d]/I$ with $I \cap R = (0)$.

We will assume (i) for now and prove (ii) and (iii).

(ii) Assuming (i), we have that $R[x]$ is Jacobson where R is Jacobson. Therefore, by induction we have $R[x_1, \ldots, x_d]$ Jacobson for any d. Write $S := R[x_1, \ldots, x_d]$. Next, let $\mathfrak{M}$ be the maximal ideal of $S = R[x_1, \ldots, x_d]$. Write $S = T[x_d]$, where $T = R[x_1, \ldots, x_{d-1}]$. So $S/\mathfrak{M}$ is a finite extension of $T/\mathfrak{N}$ where $\mathfrak{N} := T \cap \mathfrak{M}$ by (i). Also note that $\mathfrak{N}$ is a maximal ideal of T.

Argue by induction on d, we then have $T/\mathfrak{N}$ is a finite extension of $R/(R \cap \mathfrak{N})$. Since $[S/\mathfrak{M} : T/\mathfrak{N}], [T/\mathfrak{N}, R/(R \cap \mathfrak{M})] < \infty$, the claim follows.

(iii) We have by (ii) that $R[x_1, \ldots, x_d]$ Jacobson $\Rightarrow S := R[x_1, \ldots, x_d]/I$ is Jacobson and $I \cap R = (0)$. Let $\mathfrak{M}$ be a maximal ideal of S. Note that there is a correspondence between

$$\{\text{maximal ideals of } S\} \longleftrightarrow \{\text{maximal ideals of } R[x_1, \ldots, x_d] \text{ containing } I\}$$
$$\mathfrak{M} \subseteq R[x_1, x_2, \ldots, x_d]/I \longmapsto \mathfrak{M}' \subseteq R[x_1, \ldots, x_d].$$

Then $\mathfrak{N} := \mathfrak{M}' \cap R$ is maximal by (ii), and $R[x_1, \ldots, x_d]/\mathfrak{M}' \cong S/\mathfrak{M}$, and $[R[x_1, \ldots, x_d]/\mathfrak{M}' : R/\mathfrak{N}], [S/\mathfrak{M}, R/\mathfrak{N}] < \infty$, and $\mathfrak{M} \cap R = \mathfrak{M}' \cap R = \mathfrak{N}$.

So it remains to prove the Nullstellensatz when $S = R[x]$. Let's look at special case $R = k, S = k[x]$. Consider the case when $|k| = \infty$. Why is S Jacobson? To answer this, we need to consider what $\operatorname{Spec}(S)$ looks like. If $P \neq (0)$, then $P = (f(x))$ where $f(x)$ is irreducible, making P maximal. So $J(k[x]/P) = (0)$ since $k[x]/P$ is a field. And so $k[x]/P \cong k[x]/(f(x))$, and $[k[x]/(f(x)) : k/(k \cap P)] < \infty$. Note that $k = k/(k \cap P)$ and $[k[x]/(f(x)) : k/(k \cap P)] = \deg f(x)$.

Why is $J(k[x]) = (0)$? Observe that

$$J(k[x]) = \bigcap_{f(x) \text{ irred.}} (f(x)) \subseteq \bigcap_{\lambda \in k} (x - \lambda) = (0),$$

if $|k| = \infty$. □

19. February 13

Proof of Theorem 18.2 cont'd. To show that $S = R[x]$ is Jacobson where R is Jacobson and P a prime ideal of R, let $T = S/P = R[x]/P$ and let $R' = R/(R \cap P)$. We must show that if T_b is a field and b is non-zero, then T is a field. Notice that $R[x]/P \cong R'[x]/Q$ for some prime ideal Q of $R'[x]$ and $Q \cap R' = (0)$. Assume that $T_b = \operatorname{Frac}(T)$. We claim that $Q \neq (0)$. Suppose otherwise. Then $T = R[x]/Q = R'[x]$. If $K = \operatorname{Frac}(R')$, then $T \subseteq K[x] \subseteq \operatorname{Frac}(T)$, hence $T_b = \operatorname{Frac}(T) \subseteq K[x]_b \subseteq \operatorname{Frac}(T)_b = \operatorname{Frac}(T)$. Therefore $K[x]_b = \operatorname{Frac}(T)$. We showed that $K[x]$ is Jacobson, so by the Rabinowitsch trick, $K[x]_b$ is a field, making $K[x]$ a field, which is a contradiction. If $T = R'[x]/Q$ and $Q \cap R' = (0)$ and $Q \neq (0)$ with $T_b = \operatorname{Frac}(T)$ a field, we need to show that T is in fact a field. Since $Q \cap R' = (0)$, we have an injection $T \mapsto K[x]/K[x]Q$. Note that $K[x]/K[x]Q = \mathscr{S}^{-1}R'[x]/\mathscr{S}^{-1}Q$, where $\mathscr{S} = R' \setminus \{0\}$, image in $R'[x]/Q$. Now T_b is a field, so $(K[x]/K[x]Q)_b$ i a field too. Therefore T_b is a localization of T_b. Thus $K[x]$ is Jacobson, so $Q_1 := K[x]Q$ has the property that $K[x]/Q_1$ is a field. Hence Q_1 is a maximal ideal in $K[x]$. Also, since $d = [k[x]/Q : k] < \infty$, we have $Q_1 = (x^d + b_{d-1}x^{d-1} + \cdots + b_0)$ with $b_i \in K = \operatorname{Frac}(R')$. So clearing the denominators,

we get $a_d x^d + \cdots + a_0 \in Q = k[x] \cap Q_1$ with $a_d \neq 0$. So just inverts a_d to form R'_{a_d}. Then $Q_0 := QR'_{a_d}[x] \ni (x^d + a_{d-1}a_d^{-1}x^{d-1} + \cdots + a_0 a_d^{-1})$.

Then the image $\overline{x}$ of $x \in R'_{a_d}[x]/Q_0$ satisfies a monic polynomial

$$x_d + a_{d-1}a_d^{-1}x^{d-1} + \cdots + a_0 a_d^{-1} = 0. \tag{\dagger}$$

Recall that $R'[x]/Q = T$ so $R'_{a_d}[x]/Q_0 = T_{a_d}$ and that $R'_{a_d} \subseteq T_{a_d}$. Since T_{a_d} is generated by $\overline{x}$ over R'_{a_d}, we have $T_{a_d} \subseteq R'_{a_d} + R'_{a_d}\overline{x} + \cdots + R'_{a_d}\overline{x}^{d-1}$ by (†). By assumption, T_b is a field, so $T_{a_d b} = (T_b)_{a_d}$ is a field. Therefore $(R'_{a_d}[x])_b$ is a field. So T_{a_d} is a finite module over R'_{a_d} spanned by $1, \overline{x}, \ldots, \overline{x}^{d-1}$. Now we claim that there exists $m \geq 1$ so that $c_0, c_1, \ldots, c_m \in R'_{a_d}$ not all zero satisfies $c_0 + c_1 b + \cdots + c_m b^m = 0$. To see why, write

$$\begin{aligned} 1 &= 1 \\ b &= \alpha_{1,0} + \alpha_{1,1}\overline{x} + \cdots + \alpha_{1,d-1}\overline{x}^{d-1} \quad (\alpha_{ij} \in R'_{a_d}) \\ b^2 &= \alpha_{2,0} + \cdots + \alpha_{2,d-1}\overline{x}^{d-1}. \end{aligned}$$

So think of $b^i \to (\alpha_{i,0}, \ldots, \alpha_{i,d-1}) \in (R'_{a_d})^{d-1} \subseteq K^{d-1}$.

If $m > d$, then $1, b, b^2, b^3, \cdots, b^m$ are linearly dependent over K. So there exist $\gamma_0, \ldots, \gamma_m \in K$ not all zero such that $\gamma_0 + \gamma_1 b + \gamma_2 b^2 + \cdots + \gamma_m b^m = 0$. Now clear the denominator to get $c_0 + c_1 + \cdots + c_m b^m = 0$.

Without loss of generality, let $c_0 \neq 0$ and $c_m \neq 0$. So $c_0 + c_1 b + \cdots + c_m b^m = 0$ Invert c_0 to get $1 = b(-c_1 c_0^{-1} - \cdots - c_m c_0^{-1} b^{m-1})$ in $(R'_{a_d})_{c_0}[x]/R'_{a_d,c_0}Q$. Write $\widetilde{Q} := R'_{a_d,c_0}Q$. This means that b is a unit in $R'_{a_d,c_0}[x]/\widetilde{Q} = T_{a_d,c_0}$.

Now T_b is a field, so $(T_{a_d,c_0})_b$ is a field. But b is a unit, so T_{a_d,c_0} os a field. So T_{a_d,c_0} is a finite module over R'_{a_d,c_0}. By "the black box" from the last lecture, T_{a_d,c_0} if a field then R_{a_d,c_0} is a field. And then by the Rabinowitsch trick, R' is a field, whence $R' = K$. So $S = R'[x]/Q = K[x]/Q$. $K[x]/Q$ is Jacobson already, so indeed $S = R[x]$ is Jacobson.

Now the last step is to show that $\mathfrak{M}$ is an ideal of S where $\mathfrak{M} \cap R =: \mathfrak{N}$ is maximal in R and $[S/\mathfrak{M} : R/fN] < \infty$. But we just showed that if $\mathfrak{M} \subseteq S$ is a maximal ideal, then $R' = R/R \cap \mathfrak{M}$ is a field. To see why, if $S/\mathfrak{M} = R'[x]/P$ and $P \cap R' = (0)$. Note $R'[x]/P$ is a field and $R' \cap P = (0)$. And everything in R' is a unit, so $R = K$. □

20. February 24: Integral extensions

Let $R \subseteq S$ be rings. Then $1_R = 1_S$. If $i : R \hookrightarrow S$ is an inclusion map, then i gives an R-algebra structure.

Definition 20.1. We say that S is an *integral extension* of R if every $s \in S$ satisfies a monic polynomial equation with coefficients in R, i.e., there exists $n \geq 1$ and $r_0, \ldots, r_{n-1} \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$.

Example 20.2. $\mathbb{Q}$ is not an integral extension of $\mathbb{Z}$. Take $s = \frac{1}{2} \in \mathbb{Q}$. If s were integral over $\mathbb{Z}$, then $s^n + r_{n-1}s^{n-1} + \cdots + r_0 = 0$ for some $r_i \in \mathbb{Z}$. Therefore $2^{-n} + r_{n-1}2^{-(n-1)} + \cdots + r_1 2^{-1} + r_0 = 0$. Thus we see that the sum of an integer and $\frac{1}{2}$ is 0, which is impossible.

Example 20.3. $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is integral over $\mathbb{Z}$, since every $s = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ satisfies $x^2 - 2ax + a^2 - 2b^2 = 0$.

Definition 20.4. An element $s \in S$ is called *integral over* R if it satisfies a monic polynomial equation with coefficients in R.

Proposition 20.5. *If $R \subseteq S$, and S is a finitely-generated R-module, then S is an integral extension of R.*

Proof. Write $S = Ra_1 + \cdots + Ra_d$, where $a_1, \ldots, a_d \in S$. Let $s \in S$. We need to find a monic polynomial. Notice that there exist $r_{ij} \in R$ with $1 \leq i, j \leq d$ such that

$$s \cdot a_i = \sum_{j=1}^{d} r_{ij} a_j.$$

Then

$$s \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1d} \\ r_{21} & \ddots & & r_{2d} \\ \vdots & & \ddots & \vdots \\ r_{d1} & r_{d2} & \cdots & r_{dd} \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix}.$$

Thus

$$(sI - A) \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

where $A = (r_{ij}) \in \mathrm{M}_d(\mathbb{R})$ and $I : S^d \to S^d$ the identity map. If we multiply by $(sI - A)^{\mathrm{adj}} := (-1)^{i+j} \det((sI - A)_{ji})$ (where $(sI - A)_{ij}$ denotes the $(d-1) \times (d-1)$ matrix with the j-th row and the i-th column of $sI - A$ removed), then indeed $\det(sI - A)a_i = 0$ for all i. Therefore $\det(sI - A)(Ra_1 + \cdots + Ra_d) = 0$, so $\det(sI - A) = 0$. Note that $\det(sI - A)$ is a polynomial; let $\det(sI - A) =: p_A(s)$. Note that $p_A(s)$ is a monic polynomial with coefficients in R. $\square$

We will now show that if $S \supseteq R$ then $T := \{s \in S : s \text{ integral over } R\}$ forms a ring with $R \subseteq T \subseteq S$.

Example 20.6. Let $R = \mathbb{Z}$ and $S = \overline{\mathbb{Q}}$. Then $T = A = \{s \in \overline{\mathbb{Q}} : s \text{ is a root of a monic integer polynomial}\}$ is a ring, and A is said to be the set of algebraic integers.

Proposition 20.7. *Let $R \subseteq S$ be rings and let $s \in S$. Then the following are equivalent:*

(1) s is integral over R;
(2) there exists a finitely-generated R-submodule M of S such that $sM \subseteq M$ and $sM \neq (0)$.

Proof. ((1) $\Rightarrow$ (2)) If s is integral over R, then there exists $n \geq 1$ and $r_i \in R$ such that $s^n + r_{n-1}s^{n-1} + \cdots + r_1 + r_0 = 0$. Let $M = R + Rs + Rs^2 + \cdots + Rs^{n-1}$. Then M is a finitely-generated R-module, with $1 \in M$ hence $sM \neq (0)$. Also, note that

$$\begin{aligned} sM &= s(R + Rs + \cdots + Rs^{n-1}) = Rs + Rs^2 + \cdots + Rs^n \\ &= Rs + Rs^2 + \cdots + R(-r_{n-1}s^{n-1} - \cdots - r_1 s - r_0) \\ &\subseteq R + Rs + \cdots + Rs^{n-1} = M. \end{aligned}$$

((2) $\Rightarrow$ (1)) Suppose that $1 \in M = Ra_1 + \cdots + R_{a_d}$ with $sM \neq (0)$ and $sM \subseteq M$. As before,

$$sa_i = \sum_{j=1}^{d} r_{ij} a_j, \quad r_{ij} \in R.$$

If $A = (r_{ij})$ such that

$$(sI - A) \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

then $\det(sI - A)a_i = 0$ for all i hence $\det(sI - A) = 0$, which is enough to show that s is integral over R (see the proof of Proposition 20.5). $\square$

Corollary 20.8. *If $T = \{s \in S : s$ integral over $R\}$, then T is a ring with $R \subseteq T \subseteq S$.*

Proof. Let $x, y \in T$. Then x and y are integral over R. So we have $x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0$ and $y^m + r'_{m-1}y^{m-1} + \cdots + r'_1 y + r'_0 = 0$. Now let

$$M = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} Rx^i y^j \subseteq S.$$

Then M is finitely generated and $1 \in M$. Notice that $xM \subseteq M$. To see why, note that

$$x(x^i y^j) = \begin{cases} x^{i+1} y^j & (\text{if } i < n-1) \\ (-(r_{n-1}x^{n-1} + r_{n-2}x^{n-2} + \cdots + r_1 x + r_0)y^j) & (\text{if } i = n-1). \end{cases}$$

So $xM \subseteq M$, and similarly $yM \subseteq M$. So $(x+y)M \subseteq xM + yM \subseteq M + M \subseteq M$, and similarly $xyM \subseteq x(yM) \subseteq xM \subseteq M$. THerefore $x+y$ and xy are integral over R and hence are in T. Also, $T \supseteq R$: if $r \in R$ then r satisfies $x - r = 0$. Hence T is a ring containing R. $\square$

Definition 20.9. Given $R \subseteq S$, the ring

$$T := \{s \in S : s \text{ is integral over } R\}$$

is called the *integral closure* of R in S. Specifically, if R is an integral domain, then the integral closure of R is the integral closure of R in $\mathrm{Frac}(R)$, the field of fractions of R.

Example 20.10. Let $R = \mathbb{C}[t^2, t^3] \subseteq \mathbb{C}[t]$. What is the integral closure of R? In fact it's $\mathbb{C}[t]$. First, notice that t is a root of $x^2 - t^2 \in R[x]$. So t is integral over R. Thus $\mathbb{C}[t]$ is contained in the integral closure of R.

If $s \in \mathbb{C}(t)$ is integral over R, then it is also integral over $\mathbb{C}[t]$. Thus $R \subseteq \mathbb{C}[t]$. So it suffices to show that $\mathbb{C}[t]$ is integrally closed. For this, it suffices to prove the following theorem, which we shall prove on Thursday.

21. February 26

Theorem 21.1. *Let R be a UFD. Then R is integrally closed.*

Proof. Let $ab^{-1} \in \mathrm{Frac}(R)$ with $\gcd(a,b) = 1$ with $b \neq 0$ and ab^{-1} integral over R. Then because ab^{-1} is integral over R, there exist $n \geq 1$ and $r_0, \ldots, r_{n-1} \in R$ such that

$$(ab^{-1})^n + r_{n-1}(ab^{-1})^{n-1} + \cdots + r_0 = 0.$$

Multiply both sides by b^n to get

$$a^n + \underbrace{r_{n-1}a^{n-1}b + \cdots + r_1 ab^{n-1} + r_0 b^n}_{\text{multiple of } b} = 0.$$

So $b \mid a^n$. But $\gcd(a,b) = 1$, hence $\gcd(a^n, b) = 1$. Therefore b is a unit, so $ab^{-1} \in R$. Thus the integral elements of $\mathrm{Frac}(R)$ over R are precisely the elements of R. □

21.1. **Lying over & going up.**

Remark 21.1. The theorems we shall cover in this section will tell us about prime ideals in S in terms of prime ideals in R when S is an integral extension over R.

Theorem 21.2. *Let $R \subseteq S$ with $1_R = 1_S$ be an integral extension. If $\mathfrak{p} \in \mathrm{Spec}(R)$, then there exists $\mathfrak{q} \in \mathrm{Spec}(S)$ ($\mathfrak{q}$ is in general* not unique*) such that $\mathfrak{q} \cap R = \mathfrak{p}$. Moreover, if $\mathfrak{q}_1 \in \mathrm{Spec}(S)$ is such that $\mathfrak{q}_1 \cap R \subsetneq \mathfrak{p}$, then there exists $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \supsetneq \mathfrak{q}_1$ and $\mathfrak{q} \cap R = \mathfrak{p}$.*

Example 21.3. If $S = \mathbb{Z}[\sqrt{2}]$ and $R = \mathbb{Z}$, and $\mathfrak{p} = (2)$, then $\mathfrak{q} = (\sqrt{2})$.

Example 21.4. If $R = \mathbb{Z}$ and $S = \mathbb{Z}[\sqrt{3}]$ and $\mathfrak{p} = (5)$, then $\mathfrak{q}$ can be $(1 + 2i)$ or $(1 - 2i)$.

Proof. Let $\mathfrak{p}_1 = \mathfrak{q}_1 \cap R$ be an ideal of R. We claim that $\mathfrak{p}_1$ is a prime ideal of R, since $\mathfrak{q}_1$ is prime.

First reduction: we may replace S by $S/\mathfrak{q}_1$ and R by $R/\mathfrak{p}_1 = R/(R \cap \mathfrak{q}_1)$. Then S is still integral over R, so we may assume that $\mathfrak{q}_1 = (0)$ – and it suffices to show that there must exist $\mathfrak{q}$ so that $\mathfrak{q} \cap R = \mathfrak{p}$. Now let $U := R \setminus \mathfrak{p} \subseteq S$. Recall that this set is multiplicatively closed. Time for the second reduction.

Second reduction: Replace S by $U^{-1}S$ and R by $U^{-1}R = R_{\mathfrak{p}}$. Then by a question in Assignment #3, $U^{-1}S$ is integral over $U^{-1}R$. We can reduce to this case by results on localization.

So now R is a local ring with the unique maximal ideal $\mathfrak{p}$ (which is $\mathfrak{p}R_{\mathfrak{p}}$ based on the notation used in the second reduction). And S is still integral over R. Consider the ideal $\mathfrak{p}S \subseteq S$. If $\mathfrak{p}S \subsetneq S$, then there must exist a maximal ideal $\mathfrak{k}$ such that $\mathfrak{k} \supseteq \mathfrak{p}S$ so that $\mathfrak{k}$ is prime. Note that $\mathfrak{k} \cap R \subsetneq R$ since $1 \in \mathfrak{k}$. So we see that $\mathfrak{k} \cap R \subseteq \mathfrak{p}$, since $\mathfrak{p}$ is a unique maximal ideal. But then $\mathfrak{k} \cap R \supseteq \mathfrak{p}S \cap R \supseteq \mathfrak{p}$, so $\mathfrak{k} \cap R = \mathfrak{p}$. So take $\mathfrak{q} = \mathfrak{k}$ and we are done.

So we may assume that $\mathfrak{p}S = S$. In particular, assume that $1 \in \mathfrak{p}S$. Thus there exist $p_1, p_2, \ldots, p_d \in \mathfrak{p}$ and $s_1, \ldots, s_d \in S$ such that $p_1 s_1 + \cdots + p_d s_d = 1$. Let S' be the R-algebra generated by $s_1, \ldots, s_d$.

Then $\mathfrak{p}S' = S'$. Note that $p_1 s_1 + \cdots + p_d s_d = 1 \in \mathfrak{p}S'$. So $S' \subseteq (p_1 s_1 + \cdots + p_d s_d S' \subseteq \mathfrak{p}S'S' \subseteq \mathfrak{p}S'$. Also, by the integrality of S' (over R), S' is also a finitely generated R-*module*,

which is stronger than being finitely generated as an R-algebra. Let's try to explore why. Note that

$$S' = \sum_{i_1,\dots,i_d} Rs_1^{i_1}s_2^{i_2}\cdots s_d^{i_d} \subseteq \sum_{\substack{0\le i_j\le n_j-1\\ 0\le j\le d}} Rs_1^{i_1}\cdots s_d^{i_d} =: M.$$

But then S is integral over R so there exist $n_i \ge 1$ such that $s_i^{n_i} \in Rs_i^{n_i-1} + \cdots + Rs_i + R$. Also, M is a finitely generated R-module. So we have $\mathfrak{p}M = M$ and $\mathfrak{p} = J(R)$. So by Nakayama's lemma it follows $M = (0)$. But this is a contradiction, since $1 \in S'$ means $S' \supseteq R$. □

One corollary to this theorem is incomparability:

Corollary 21.5. *Suppose $R \subseteq S$ is an integral extension with $1_R = 1_S$. If $\mathfrak{q} \neq \mathfrak{q}' \in \mathrm{Spec}(S)$ and $\mathfrak{q} \cap R = \mathfrak{q}' \cap R = \mathfrak{p}$, then $\mathfrak{q}$ and $\mathfrak{q}'$ are* incomparable*: that is, $\mathfrak{q} \not\subset \mathfrak{q}'$ and $\mathfrak{q}' \not\subset \mathfrak{q}$.*

Proof. Suppose that $\mathfrak{q}' \subsetneq \mathfrak{q}$. Then $\mathfrak{q}' \cap R = \mathfrak{p}$. So if we mod out by $\mathfrak{q}'$ then we can replace S by $S/\mathfrak{q}'$ and R by $R/(R \cap \mathfrak{q}') = R/\mathfrak{p}$. Notice that S is still integral over R. Now this reduces to the case when $\mathfrak{p} = (0), \mathfrak{q}' = (0), \mathfrak{q} \neq (0), \mathfrak{q} \cap R = (0)$. Now pick $x \in \mathfrak{q} \setminus \{0\}$. Then x is integral over R so there exists $n \ge 1$ and $r_{n-1}, \dots, r_0 \in R$ such that $x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0$. Without loss of generality, let $r_0 \neq 0$, which we can do since S is an integral domain and $x \neq 0$.

But now, note $r_0 = -x^n - r_{n-1}x^{n-1} - \cdots - r_1 x$, so $r_0 \in R \cap \mathfrak{q}$ since each monomial on the RHS is in $\mathfrak{q}$. That is, $r_0 \in R \cap \mathfrak{q} = \mathfrak{p} = (0)$, so $r_0 = 0$, hence a contradiction. Thus it is impossible to have $(0) \subsetneq \mathfrak{q} \subseteq S$ such that $\mathfrak{q} \cap R = (0)$ with R integral domain, as required. □

22. February 27

Definition 22.1. Given a ring R, we define the *Krull dimension of R* to be

$$\mathrm{Kdim}(R) := \sup\{n : \text{there exist a chain } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n \text{ of prime ideals in } R\}.$$

Example 22.2. Every field F has $\mathrm{Kdim}(F) = 0$. We have $\mathrm{Kdim}(\mathbb{Z}) = 1$, since $(0) \subsetneq (p)$ is the only chain available, where p is prime. $\mathrm{Kdim}(F[x]) = 1$, since the only prime ideal chains can be $(0) \subsetneq (p(x))$ where $p(x)$ is irreducible.

Theorem 22.3. *If $R \subseteq S$ and S an integral extension of R with $1_R = 1_S$, then* $\mathrm{Kdim}(R) = \mathrm{Kdim}(S)$.

Example 22.4. Let K be a finite field extension of $\mathbb{Q}$, i.e., $[K : \mathbb{Q}] < \infty$. Then if we take $R = \mathbb{Z}$ then $S = \{s \in K : s \text{ integral over } \mathbb{Z}\} = \mathbb{A} \cap K =: \mathcal{O}_K$ (where $\mathbb{A}$ is the set of algebraic numbers), and $\mathcal{O}_K$ is said to be *the ring of integers* or *a number ring*. Since $\mathrm{Kdim}(\mathbb{Z}) = 1$, it follows that $\mathrm{Kdim}(\mathcal{O}_K) = 1$.

Proof. First suppose that $\mathrm{Kdim}(R) \ge n$. So there exists a chain $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_n$ in $\mathrm{Spec}(R)$. Now we use lying over and going up, so that for any prime ideals $P_0 \subsetneq P_1 \subsetneq R$ and $Q_0 \cap R = P$ where Q_0 is a prime ideal in S, then there exists Q_1 an ideal of S such that $Q_1 \cap R = P_1$. Do this for any chain of ideals of R, there exists a chain $Q_0 \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_n$ in $\mathrm{Spec}(S)$ with $Q_i \cap R = P_i$. So $\mathrm{Kdim}(S) \ge n$.

If $\mathrm{Kdim}(S) \ge n$, then there exists a chain $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n$ in $\mathrm{Spec}(S)$. Take $P_i := Q_i \cap R$ prime ideals. Then we have $P_0 \subseteq P_1 \subseteq \cdots \subseteq P_n$. How do we know that the

containment is strict? Suppose otherwise. But this contradicts the fact that Q_0 and Q_1 must be incompatible, by Corollary 21.5. Thus the strict containment follows. $\square$

Proposition 22.5. *Suppose R is Noetherian. Then the following are equivalent:*

(1) R has Krull dimension 0
(2) All prime ideals of R are maximal.
(3) If N is the nilradical of R (i.e., $N = \sqrt{(0)} = \{x : x \text{ nilpotent}\}$), then $R/N \cong F_1 \times F_2 \times \cdots \times F_s$ for $s \geq 1$, where each F_i is a field.

Proof. ((1) $\Leftrightarrow$ (2)) Take $P \in \operatorname{Spec}(R)$. If P is not maximal then there must exist a maximal ideal $\mathfrak{M}$ such that $\mathfrak{M} \supsetneq P$, so $\operatorname{Kdim}(R) \geq 1$, which is a contradiction. The other direction is immediate.

((3) $\Rightarrow$ (1)) We claim that $F_1 \times \cdots \times F_s$ has Krull dimension 0. First, if P is a prime ideal, then we claim that there exists $j \in \{1, \ldots, s\}$ such that $P = F_1 \times \cdots \times F_{j-1} \times (0) \times F_{j+1} \times \cdots \times F_s$. If we let $e_1 = (1_{F_1}, \ldots, 0_{F_s}), e_2 = (0_{F_1}, 1_{F_2}, \cdots, 0_{F_s}), \cdots, e_s = (0, 0, \cdots, 1_{F_s})$, then we have $e_k \cdot e_l = 0$ whenever $k \neq l$. Thus $e_k e_l \in P$, so either e_k or e_l is in P. Therefore there must exist j such that $e_1, \ldots, e_{j-1}, e_{j+1}, \ldots, e_s \in P$. So there must exist P such that

$$P \supseteq F_1 \times \cdots \times F_{j-1} \times (0) \times F_{j+1} \times \cdots \times F_s =: I_j.$$

So if we let $F_1 \times F_2 \times \cdots \times F_s / I_j \to F_j$ such that $(a_1, a_2, \ldots, a_s) \mapsto a_j$, then the kernel of this map is I_j. Therefore I_j is maximal, so $P = I_j$. Therefore all the prime ideals of R are maximal, which implies that $\operatorname{Kdim}(R) = 0$.

((1) $\Rightarrow$ (3)) Suppose that R has $\operatorname{Kdim}(R) = 0$. Since R is Noetherian, there exist $P_1, P_2, \ldots, P_s \in \operatorname{Spec}(R)$ such that $(0) \subseteq P_i$ for all $1 \leq i \leq s$, and such that if Q is another prime in R containing (0) then $Q \supseteq P_i$ for some i. This implies that $\operatorname{Spec}(R) = \{P_1, \ldots, P_s\}$, and if $Q \notin \operatorname{Spec}(R)$ and $Q \supseteq P_i$ for some i, then $Q = P_i$, which is a contradiction. This proves that every P_i is maximal. Therefore $P_i + P_j = R$ whenever $i \neq j$. By the Chinese Remainder theorem, we have

$$R/N = R/\bigcap_{i=1}^{s} P_i \cong \prod_{i=1}^{s} R/P_i \cong \prod_{i=1}^{s} F_i,$$

proving the desired direction. $\square$

Lemma 22.6. *Let R be a ring with $\operatorname{Kdim}(R) = d$. Then $d + 1 \leq \operatorname{Kdim}(R[x]) \leq 2d + 1$.*

Proof. Let $P_0 \subsetneq P_1 \subsetneq P_2 \subsetneq \cdots \subsetneq P_d$ be a chain in $\operatorname{Spec}(R)$. Let $Q_i = P_i R[x] = \{a_0 + a_1 x + \cdots + a_m x^m : m \geq 0, a_0, \cdots, a_m \in P_i\}$. Then $R[x]/Q_i \cong (R/P)[x]$. Note that $(R/P_i)[x]$ is an integral domain. So $Q_0 \subsetneq Q_1 \subseteq \cdots \subsetneq Q_d$ is a chain in $\operatorname{Spec}(R[x])$. Then $R[x]/Q_d \cong (R/P_d)[x]$ and (x) is a prime ideal in this ring. So by the correspondence of chains, we have $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_d \subsetneq (Q_d, x)$ is a chain of length $d + 1$.

For the other bound, suppose that there is a chain

$$Q_0 \subsetneq Q_1 \subsetneq Q_2 \subsetneq \cdots \subsetneq Q_{2d+1} \subsetneq Q_{2d+2}$$

in $\operatorname{Spec}(R[x])$. Let $P_i = Q_i \cap R$. Then $P_0 \subseteq P_1 \subseteq \cdots P_{2d+2}$ is a chain in $\operatorname{Spec}(R)$. So we have a chain of length $2d+3$. But note that this is impossible unless some ideals are equal, since we cannot have more than $d + 1$ distinct ideals in this chain. By the pigeonhole principle, there exists some i so that $P_i = P_{i+1} = P_{i+2}$. Thus we have $Q_i \subsetneq Q_{i+1} \subsetneq Q_{i+2}$ in $\operatorname{Spec}(R[x])$ where all three of them contain P. So by correspondence there exists a chain $\widetilde{Q_i} \subsetneq \widetilde{Q_{i+1}} \subsetneq \widetilde{Q_{i+2}}$

in $\operatorname{Spec}((R/P)[x]) = \operatorname{Spec}(R[x]/PR[x])$. Let $S = R/P$ so we have $\widetilde{Q_i} \subsetneq \widetilde{Q_{i+1}} \subsetneq \widetilde{Q_{i+2}}$ in $\operatorname{Spec}(S[x])$. Moreover $\widetilde{Q_i} \cap S = \widetilde{Q_{i+1}} \cap S = \widetilde{Q_{i+2}} \cap S = (0)$.

Let $T = S \setminus \{0\}$, which is multiplicatively closed since S is an integral domain. Thus $T^{-1}S = \operatorname{Frac}(S) =: K$. Then $\widetilde{Q_j} \cap T = \emptyset$ for $j = i, i+1, i+2$. So by the results from localization, there exist prime ideals $\widehat{\widetilde{Q_i}} \subseteq \widehat{\widetilde{Q_{i+1}}} \subseteq \widehat{\widetilde{Q_{i+2}}}$ in $T^{-1}(S[x]) = (T^{-1}S)[x] = K[x]$. But then $\operatorname{Kdim}(K[x]) = 1$ since K is a field. This is a contradiction since we just constructed a chain of length 2. □

23. March 3: Noether normalization

Theorem 23.1 (Noether normalization theorem)**.** *Let R be a finitely generated k-algebra for some field k. Then there exists a k-subalgebra S of R such that*

(1) $S \cong k[x_1, x_2, \ldots, x_d]$, where $d = \operatorname{Kdim}(R)$;
*(2) R is a finitely-generated S-*module*.*

Remark 23.1. Hard part of the proof of the normalization theorem is proving that $d = \operatorname{Kdim}(R)$. This is the part we will get to later.

Proposition 23.2. *If R is a finitely generated k-algebra then $\operatorname{Kdim}(R) < \infty$.*

Proof. Recall that $R \cong k[x_1, \ldots, x_m]/I$. So $\operatorname{Kdim}(R) = \operatorname{Kdim}(k[x_1, \ldots, x_m]/I) \leq \operatorname{Kdim}(k[x_1, \ldots, x_m])$ by the correspondence. We showed that if $\operatorname{Kdim}(R) = s$ then $s+1 \leq \operatorname{Kdim}(R[x]) \leq 2s+1$. By induction we have $\operatorname{Kdim}(k[x_1]) = 1$, and $\operatorname{Kdim}(k[x_1, x_2]) \leq \operatorname{Kdim} k[x_1][x_2] \leq 3$, and so forth. So by induction we have $\operatorname{Kdim}(k[x_1, \ldots, x_m]) \leq 2^m - 1$. □

Proof of the normalization theorem. Let m be the number of generators for the k-algebra R. We will do this by induction on m. Let's say $R = k[a_1, \ldots, a_m]$ (not necessarily a polynomial ring). Then $\{a_1, \ldots, a_m\}$ is a set of generators.

Start with the base case $m = 1$. Then $R = k[a_1]$. So $R \cong k[x]/I$, where $I = (0)$ or $I = (p(x))$ where $p(x)$ is the minimal polynomial of a_1. If $I = (0)$ then $R \cong k[x]$. So $S = k[a_1] \cong k[x]$ and $R = S$ so R is a finitely generated S-module. If $I = (p(x))$ with $p(x) \neq 0$, then $R \cong k[x]/(p(x))$ is e-dimensional k-vector space where $e = \deg p(x)$. In this case, take $S = k$; and $\dim_k R < \infty$, so R is a finitely generated S-module.

Induction hypothesis: let's assume that the claim holds whenever R is generated by fewer than m elements. Consider the case when $R = k[a_1, \ldots, a_m]$, the k-algebra generated by $a_1, \ldots, a_m$. First, suppose that $a_1, \ldots, a_m$ are algebraically independent over k. In this case, we have $R \cong k[x_1, \ldots, x_d]$. To see why, consider the map $\phi : k[x_1, \ldots, x_m] \to R$ defined by $x_i \mapsto a_i$. Note that $\ker \phi = (0)$, so in this case $S = R \cong k[x_1, \ldots, x_m]$ and S is clearly a finitely generated R-module as $S = R$.

Now suppose that $a_1, \ldots, a_m$ are not algebraically independent over k. So there exists a non-trivial polynomial relation $q(a_1, \ldots, a_m) = 0$. Before proceeding, we turn to an exercise which will appear in Assignment #4: prove that there exist natural numbers $A_1, \ldots, A_{m-1} > 0$ such that $q(x_1 + x_m^{A_1}, \ldots, r_{m-1} + r_m^{A_{m-1}}, x_m) = Cx_m^D + p(x_1, \ldots, x_m)$ where $C \neq 0$ is a constant and $p(x_1, \ldots, x_m)$ is a polynomial such that the degree of x_m is less than D.

We can find $u_1, \ldots, u_m$ such that $a_i = u_i + u_m^{A_1}$ for all $i = 1, \ldots, m-1$ and $a_m = u_m$, as $u_i = a_i - u_m^{A_1} = a_i - a_m^{A_i} \in R$. Notice also that $k[u_1, \ldots, u_m] = k[a_1, \ldots, a_m] = R$. One

direction ($\supseteq$) follows since $a_i = u_i + u_m^{A_i}$ for all $i < m$ and the other one ($\subseteq$) follows since $u_i = a_i - a_m^{A_i}$.

Notice that (by the aforementioned exercise)

$$0 = q(a_1, \dots, a_m) = q(u_1 + u_m^{A_i}, \dots, u_{m-1} + u_m^{A_{m-1}}, u_m) = C \cdot u_m^D + \sum_{i=0}^{D-1} p_i(u_1, \dots, u_{m-1}) u_m^i \quad (*)$$

Now let $T = k[u_1, \dots, u_{m-1}]$. Then $R = T[u_m] = T + Tu_m + \cdots + Tu_m^{D-1}$ by $(*)$. So R is a finite T-module. But T is generated by fewer than m elements, so by the induction hypothesis there exists $S \cong k[x_1, \dots, x_d]$ such that T is a finite S-module. So since R is a finitely generated T-module and T a finitely generated S-module, then R is a finitely generated S module. Thus we are done. □

To show that $\operatorname{Kdim} k[x_1, \dots, x_d] = d$ and that R is a finitely generated $k[x_1, \dots, x_d]$-module implies that $\operatorname{Kdim}(R) = d$, we will need the *Gelfand-Kirillov dimension* and integrality.

Let k be a field, and let A be a finitely generated k-algebra. And let V be a finite-dimensional k-vector space with $V \subseteq A$ such that $1 \in V$ and V contains a set of generators of A. Define $V^2 := \operatorname{span}_k\{vw : v, w \in V\} \supset V$ since $1 \in V$. If $x_1, \dots, x_m$ is a basis for V then $\{x_i x_j : i, j \in \{1, \dots, m\}\}$ span V^2. Similarly, we get the chain $V \subseteq V_2 \subseteq V^3 \subseteq \cdots$ and $\dim_k V^n < \infty$ for all $n \geq 1$.

We now define the Gelfand-Kirillov dimension:

Definition 23.3. The *Gelfand-Kirillov dimension* of a finitely generated k-algebra $\operatorname{GKdim}(A)$ is defined to be

$$\operatorname{GKdim}(A) := \limsup_{n \to \infty} \frac{\log(\dim V^n)}{\log n}.$$

Remark 23.2. We will see that this does not depend on V. That is, we get the same result for any finite-dimensional k-subspace of A that contains 1 and a set of generators. Also, intuitively speaking one can think that if $\dim V^n \sim Cn^d$ for some $C > 0$ then $d = \operatorname{GKdim}(A)$.

Example 23.4. $\operatorname{GKdim}(k[x]) = 1$. Take $V = k + kx = \operatorname{span}\{1, x\}$, and $V^n = \operatorname{span}\{1, x, x^2, \dots, x^n\}$ with $\dim V^n = n + 1$. Then

$$\operatorname{GKdim}(k[x]) = \limsup_{n \to \infty} \frac{\log(n+1)}{\log n} = 1.$$

Example 23.5. What about $\operatorname{GKdim}(k[x, y])$? Let $V = k + kx + ky = \operatorname{span}\{1, x, y\}$. Then $V^n = \operatorname{span}\{x^i y^j : i + j \leq n\}$ so $\dim V^n = \binom{n+2}{2} \sim \frac{n^2}{2}$.

24. March 5

Suppose that k is a field, A a finitely generated k-algebra, and $V \subseteq A$ a finite-dimensional k-vector subspaces of A with $1 \in V$ and V contains a set of generators for A (such V is said to be a *generating subspace* for A). We defined the Gelfand-Kirillov dimension last time.

Proposition 24.1. *The definition of the Gelfand-Kirillov dimension is independent of choice of generating subspace.*

Proof. Suppose that V and W are two generating subspaces. Then $V \subseteq V^2 \subseteq V^3 \subseteq \cdots \subseteq \bigcup V^n = A$, and $W \subseteq W^2 \subseteq W^3 \subseteq \cdots \subseteq \bigcup W^n = A$. It follows that there exists $p, q \geq 1$ such that $V \subseteq W^p$ and $W \subseteq V^q$. Therefore it follows that $V^n \subseteq W^{pn}$ for all $n \geq 1$. Therefore

$$\begin{aligned}\limsup_{n\to\infty} \frac{\log(\dim V^n)}{\log n} &\leq \limsup_{n\to\infty} \frac{\log(\dim(W^{pn}))}{\log n} \\ &= \limsup_{n\to\infty} \frac{\log(\dim(W^{pn}))}{\log(pn)} \cdot \frac{\log(pn)}{\log n} \\ &\leq \limsup_{n\to\infty} \frac{\log(\dim W^n)}{\log n}.\end{aligned}$$

And similarly since $W \subseteq V^q$, we see that

$$\limsup_{n\to\infty} \frac{\log(\dim W^n)}{\log n} \leq \limsup_{n\to\infty} \frac{\log(\dim V^n)}{\log n}.$$

□

Proposition 24.2. *If A is a finitely generated k-algebra then* $\mathrm{GKdim}(A) = 0$ *if and only if* $\dim_k A < \infty$*; and if* $\dim_k A > 0$ *then* $\mathrm{GKdim}(A) \geq 1$.

Proof. If $\dim_k A < \infty$, then $V = A$ is a generating subspace. But now $V^2 = V^3 = \cdots = A$ for all $n \geq 1$, so

$$\mathrm{GKdim}(A) = \limsup_{n\to\infty} \frac{\log(\dim_k(A))}{\log n} = 0,$$

as $\log(\dim_k(A))$ is a finite quantity and $\log n \to \infty$. Conversely, suppose that $\dim_k(A) = \infty$, and let V be a generating subspace for A. Thus $V \subsetneq V^2 \subsetneq V^3 \subsetneq \cdots$. If $V^i = V^{i+1}$ for some i then $V^i \cdot V = V^{i+1} \cdot V = V^{i+2}$, so by induction we have $V^n = V^i$ for all $n \geq i$. This means $\dim_k A < \infty$, a contradiction. SInce $V \subsetneq V^2 \subsetneq V^3 \subsetneq \cdots$, we have $\dim V^n \geq n$, and so

$$\limsup_{n\to\infty} \frac{\log(\dim V^n)}{\log n} \geq \limsup_{n\to\infty} \frac{\log n}{\log n} = 1.$$

□

Theorem 24.3. *Let $d \geq 1$. Then* $\mathrm{GKdim}(k[x_1, \ldots, x_d]) = d$.

Proof. Let $V = k + kx_1 + kx_2 + \cdots + kx_d$. Then

$$V^n = \mathrm{span}\{x_1^{i_1} \cdots x_d^{i_d} : i_1 + \cdots + i_d \leq n\}.$$

So $\dim V^n = \binom{n+d}{d}$. To see why, note that we can create a bijection between $\{x_1^{i_1} \cdots x_d^{i_d} : i_1 + \cdots + i_d \leq n\}$ and the set of all ways of placing d X's into $n+d$ slots, and there are $\binom{n+d}{d}$ ways to do this. Since

$$\begin{aligned}\binom{n+d}{d} &= \frac{(n+d)\cdots(n+1)}{d!} = \frac{n^d}{d!}\left(1 + O\left(\frac{1}{n}\right)\right). \\ \frac{\log(\dim V^n)}{\log n} &= \frac{\log \frac{n^d}{d!}(1 + O(\frac{1}{n}))}{\log n} \\ &= \frac{d\log n - \log d! + \log(1 + O(n^{-1}))}{\log n} = \frac{d\log n}{\log n} - \frac{\log d!}{\log n} + \frac{O(n^{-1})}{\log n} \to d\end{aligned}$$

as $n \to \infty$. Thus $\mathrm{GKdim}(k[x_1, \ldots, x_d]) = d$. □

Our main theorem that we hope to prove is the following:

Theorem 24.4. *Let k be a field and let A be a finitely generated k-algebra. Then* $\mathrm{GKdim}(A) = \mathrm{Kdim}(A)$.

Corollary 24.5. $\mathrm{Kdim}(k[x_1, \ldots, x_d]) = d$.

The proof of the main theorem will use two facts, one from Assignment #3 and the other from Assignment #4:

(1) (from Assignment #3) If $R \subseteq S$ and S is a finitely generated R-module, then S is integral over R; hence $\mathrm{Kdim}(S) = \mathrm{Kdim}(R)$ if S is a finite R-module.
(2) (from Assignment #4) If $R \subseteq S$ and S is a finitely-generated R-module then $\mathrm{GKdim}(R) = \mathrm{GKdim}(S)$.

Proof of the main theorem. Notice that if A is a finitely generated k-algebra then by the Noether normalization theorem there exists $B \subseteq A$ such that $B \cong k[y_1, \ldots, y_d]$ such that A is a finite B-module. Since A is finite as a B-module, we see that A is integral over B hence $\mathrm{Kdim}(A) = \mathrm{Kdim}(B) \geq d$.

Also A is finitely generated as a B-module, so $\mathrm{GKdim}(A) = \mathrm{GKdim}(B) = d$. So we sat least know that $\mathrm{Kdim}(A) \geq \mathrm{GKdim}(A)$. Let

$$\alpha = \inf\{\mathrm{GKdim}(A) : A \text{ finitely generated such that } \mathrm{Kdim}(A) > \mathrm{GKdim}(A)\}.$$

So there exists A such that $\mathrm{Kdim}(A) > \mathrm{GKdim}(A)$ and $\mathrm{GKdim}(A) < \alpha + \frac{1}{2}$. So now by the Noether normalization theorem that there exists d and $B \cong k[y_1, \ldots, y_d]$ with $B \subseteq A$ such that $[A : B] < \infty$ so $\mathrm{Kdim}(A) = \mathrm{Kdim}(B)$ and $\mathrm{GKdim}(A) = \mathrm{GKdim}(B) = d$. Since $\mathrm{Kdim}(A) > \mathrm{GKdim}(A)$, we have $\mathrm{Kdim}(A) \geq d+1$. So we are in the situation where we may assume $\mathrm{Kdim}(k[x_1, \ldots, x_d]) \geq d+1$. That means that there exists a chain $(0) \subsetneq P_1 \subsetneq \cdots \subsetneq P_{d+1}$ in $\mathrm{Spec}(k[x_1, \ldots, x_d])$. Then we claim that $\mathrm{Kdim}(k[x_1, \ldots, x_d]/P_1) \geq d$, and that if B is a finitely generated k-algebra that is also an integral domain and $I \neq (0)$ is an ideal of B then $\mathrm{GKdim}(B/I) \leq \mathrm{GKdim}(B) - 1$.

Once we have the claim, we see that $\mathrm{Kdim}(k[x_1, \ldots, x_d]/P_1) \geq d$ and $\mathrm{GKdim}(k[x_1, \ldots, x_d]/P_1) \leq d - 1 < \alpha$. But by the definition of α, we see that $\mathrm{GKdim}(k[x_1, \ldots, x_d]/P_1) = \mathrm{Kdim}(k[x_1, \ldots, x_d]/P_1)$, which is a contradiction. We will prove the necessary claims tomorrow and move on to transcendence degree. □

25. March 6

We need the following claim to finish off the proof:

Claim. Let A be a finitely generated k-algebra that is an integral domain. If I is a non-zero ideal of A then $\mathrm{GKdim}(A/J) \leq \mathrm{GKdim}(A) - 1$.

Proof. Let $\pi : A \to A/I$ be the canonical surjection. Let V be a generating space for A. Then $\pi(V) =: \overline{V}$ is a generating space for A/J. For each $n \geq 1$, pick a subspace W_n of V^n such that $\pi(W_n) = \overline{V}^n$ and $\dim W_n = \dim(\overline{V}^n)$.

Pick $f \in V \backslash \{0\}$ such that $f \in I$. Then we claim that the sum $W_n + fW_{n-1} + \cdots + f^{n-1}W_1 \subseteq V^n$ is a direct sum. Suppose that is not the case. Then there exists $w_i \in W_i$, $i = 1, \ldots, n$ not all zero so that $w_n + fw_{n-1} + f^2w_{n-2} + \cdots + f^{n-1}w_1 = 0$. So there exists a largest $m \leq n$ such that $w_m \neq 0$. So $f^{n-m}w_m + \cdots + f^{n-1}w_1 = 0$ with $w_m \neq 0$. Since A is an integral domain, we see that $fw_{m-1} + \cdots + f^{m-1}w_1 \in I$. Now apply π to see that $\pi(w_m) = 0$ and

$\pi(I) = (0)$. But $\dim(W_m) = \dim(\overline{V}^m)$ and $\pi(W_m) = \overline{V}^m$. Hence π is injective meaning that $w_m = 0$, but this is a contradiction.

Now we want to show that $\mathrm{GKdim}(A/I) \leq d-1$, where $d = \mathrm{GKdim}(A)$. Suppose that $\mathrm{GKdim}(A/I) > d-1$. Then $\mathrm{GKdim}(A/I) \geq d$. Let $\varepsilon < 1$. This means that $\dim(\overline{V}^n) \geq n^{d-\varepsilon}$ for infinitely many n. To see why, assume that this is not true. Then $\dim(\overline{V}^n) < n^{d-\varepsilon}$, hence

$$\frac{\log \dim(\overline{V}^n)}{\log n} < \frac{(d-\varepsilon)\log n}{\log n} = d - \varepsilon$$

for all sufficiently large n. Hence

$$\mathrm{GKdim}(A/I) = \limsup_{n\to\infty} \frac{\log \dim \overline{V}^n}{\log n} \leq d - \varepsilon < d,$$

which is a contradiction. By assumption, $\dim W_n = \dim \overline{V}^n$. So $\dim W_n \geq n^{d-\varepsilon}$ for infinitely many n. Now $\overline{V}^n \subseteq \overline{V}^{n+1} \subseteq \cdots \subseteq \overline{V}^{2n}$, so $\dim W_n \leq \dim W_{n+1} \leq \cdots \leq \dim W_{2n}$. Thus there are infinitely many n such that $\dim W_{2n}, \cdots \dim W_n \geq n^{d-\varepsilon}$. Recall that $W_{2n} \oplus fW_{2n-1} \oplus f^2W_{2n-2} \oplus \cdots \oplus f^{2n-1}W_1 \subsetneq V^{2n}$. So

$$\begin{aligned}\dim V^{2n} &\geq \dim(W_{2n}) + \dim(fW_{2n-1}) + \cdots + \dim(f^nW_n) + \cdots + \dim(f^{2n-1}W_1)\\ &\geq \dim(W_{2n}) + \dim(W_{2n-1}) + \cdots + \dim(W_n) \geq n^{d-\varepsilon}\cdot n = n^{d+1-\varepsilon}.\end{aligned}$$

Therefore

$$\frac{\log \dim V^{2n}}{\log(2n)} \geq \frac{(d+1-\varepsilon)\log n}{\log 2n},$$

so

$$d = \mathrm{GKdim}(A) \approx \limsup_{n\to\infty} \frac{\log \dim V^n}{\log n} \geq d + 1 - \varepsilon > d,$$

which is a contradiction. □

Corollary 25.1. *Let A be a finitely generated k-algebra. Then* $\mathrm{Kdim}(A[x]) = \mathrm{Kdim}(A) + 1$.

Proof. We already showed that $\mathrm{Kdim}(A[x]) \geq \mathrm{Kdim}(A) + 1$. Now by Noether normalization there exists $B \subseteq A$ such that $B \cong k[x_1, \ldots, x_d]$, with $d = \mathrm{Kdim}(A)$ and A a finitely generated B-module.

Write $A = Ba_1 + \cdots + Ba_s$. Then $A[x] = B[x]a_1 + \cdots + B[x]a_s$. Thus $A[x]$ is a finitely generated $B[x]$-module. And we know by Assignment #3 that $\mathrm{Kdim}(A[x]) = \mathrm{Kdim}(B[x]) = \mathrm{Kdim}(k[x_1, \ldots, x_d][x]) = d + 1$ (note $B[x] \cong k[x_1, \ldots, x_d][x]$). □

25.1. **Transcendence degree.**

Definition 25.2. Suppose that K is a field extension of a field k. Then a set $\mathscr{S} \subseteq K$ is *algebraically independent* if every finite subset $\{x_1, \ldots, x_d\}$ of $\mathscr{S}$ has the property that if $p(x_1, \ldots, x_d) = 0$ and $p(t_1, \ldots, t_d) \in k[t_1, \ldots, t_d]$ then $p(t_1, \ldots, t_d) = 0$. We define the *transcendence degree of K/k* to be

$$\mathrm{trdeg}_k K = \sup\{\#\mathscr{S} : \mathscr{S} \text{ algebraically independent subset of } K\}.$$

We will only worry about finite transcendence degree.

Theorem 25.3. *Let k be a field and let A be a finitely generated k-algebra that is an integral domain and let $K = \mathrm{Frac}(A)$. Then $\mathrm{Kdim}(A) = \mathrm{trdeg}_k K$.*

Proof. Let $d = \mathrm{Kdim}(A)$. By Noether normalization, there exists $B \cong k[x_1, \ldots, x_d]$ with $B \subseteq A$ and A a finitely generated B-module. Let $b_1, \ldots, b_d$ be a set of generators for B. So $B = k[b_1, \ldots, b_d] \cong k[x_1, \ldots, x_d]$. Then the set $\{b_1, \ldots, b_d\} \subseteq K$ is algebraically independent over k. So $\mathrm{trdeg}_k K \geq d$.

Now suppose that $\mathrm{trdeg}_k K > d$. Then there exists $c_1, \ldots, c_{d+1} \in K$ algebraically independent over k. Since $K = \mathrm{Frac}(A)$, we can write each c_i in the fraction form. Take the least common multiple of the denominators. So there exist $b \in A \setminus \{0\}$ and $a_1, \ldots, a_{d+1} \in A$ such that $c_1 = a_1/b, \ldots, c_{d+1} = a_{d+1}/b$. Thus $k[y_1, \ldots, y_{d+1}] \cong k[c_1, \ldots, c_{d+1}] \subseteq A[b^{-1}]$. Now $\mathrm{Kdim}(A[b^{-1}]) \leq \mathrm{Kdim}(A) = d$. $A[b^{-1}]$ is finitely generated so $\mathrm{GKdim}(A[b^{-1}]) \leq d$ as well. Thus $k[c_1, \cdots, c_{d+1}]$ has G-K dimension $d+1$ but $A[b^{-1}]$, which contains $k[c_1, \ldots, c_{d+1}]$ has G-K dimension d. This is a contradiction, according to the claim below.

Claim. If $R \subseteq S$ and R, S finitely generated k-algebra, then $\mathrm{GKdim}(R) \leq \mathrm{GKdim}(S)$.

To see why the claim is true, start by picking V a generating space for R. Now add in a set of generators for S to obtain a generating space $W \supset V$ for S. Then $\dim(V^n) \leq \dim(W^n)$ for all n. Thus $\mathrm{GKdim}(R) \leq \mathrm{GKdim}(S)$. □

26. March 10

Definition 26.1. Given a ring R and $P \in \mathrm{Spec}(R)$, we define the *height of P* to be

$$\mathrm{ht}(P) := \mathrm{Kdim}(R_P) = \sup\{n : Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n, Q_n \subseteq P, Q_i \in \mathrm{Spec}(R)\}.$$

Definition 26.2. For any R, we define M-Spec(R) to be the set of maximal ideals of R, i.e.,

$$\text{M-Spec}(R) := \{M : M \text{ a maximal ideal of } R\}.$$

Now we shall put a topology on $\mathrm{Spec}(R)$. Then M-Spec(R) will inherit the subspace topology. Particularly, we will put the *Zariski topology*:

Definition 26.3. We define the closed sets of the *Zariski topology* as follows: if I is an ideal of R, then

$$C_I := \{P \in \mathrm{Spec}(R) : P \supseteq I\}.$$

Let's verify if this topology is indeed a topology. Clearly, $C_R = \emptyset$ and $\mathrm{Spec}(R) = C_{(0)}$. Let's check if $C_{I_1} \cup \cdots \cup C_{I_n} = C_{\bigcap I_j}$. This is clear since

$$\mathfrak{P} \in C_{I_1} \cup \cdots \cup C_{I_n} \Leftrightarrow \mathfrak{P} \supseteq I_1 \text{ or } \mathfrak{P} \supseteq I_2 \text{ or } \cdots \mathfrak{P} \supseteq I_n$$
$$\Leftrightarrow \mathfrak{P} \supseteq \bigcap_{j=1}^{n} I_j$$

For the last $\Leftrightarrow$, the $\Rightarrow$ is obvious, so let's just show the $\Leftarrow$ direction. Suppose that $\mathfrak{P} \supseteq \bigcap I_j$ but does not contain any I_j. Then there exists $a_j \in I_j \setminus \mathfrak{P}$ for $j = 1, 2, \ldots, n$. So $a_1 a_2 \cdots a_n \in \bigcap I_j \subseteq \mathfrak{P}$. But then $\mathfrak{P}$ is a prime ideal so $a_j \in \mathfrak{P}$ for some j. Contradiction, so we proved what we wanted to show.

Notice that an *arbitrary* union of C_{I_j}'s need not be closed.

Example 26.4. Let $R = \mathbb{C}[x]$, so $\mathrm{Kdim}(R) = 1$, since $(0) \subsetneq (x-\lambda)$ are the only available chains of prime ideals. Suppose $I = (p(x))$. Then

$$C_I = \{(x-\lambda) : (x-\lambda) \supseteq (p(x))\},$$

so there is a bijection between C_I and $\{\lambda \in \mathbb{C} : p(\lambda) = 0\}$, as $(x-\lambda) \supseteq (p(x)) \Leftrightarrow x - \lambda \,|\, p(x)$. Thus C_I is a finite set. So in this case,

$$C_I = \begin{cases} \mathrm{Spec}(R) & \text{if } I = (0) \\ \text{finite set} & \text{if } I \neq (0) \\ (0) & \text{if } I = R. \end{cases}$$

Then $Z := \bigcup_{n \in \mathbb{Z}} C_{(x-n)}$ is not closed, since Z is countably infinite while $\mathrm{Spec}(R)$ is uncountably infinite.

Finally, it remains to show that the arbitrary intersection of the C_I's is closed. Namely, we show

Proposition 26.5. $\bigcup_\alpha C_{I_\alpha} = C_{\sum I_\alpha}$.

Proof. $P \in \bigcup_\alpha C_{I_\alpha} \Leftrightarrow P \in C_{I_\alpha}$ for all $\alpha \Leftrightarrow P \supseteq I_\alpha$ for all $\alpha \Leftrightarrow P \supseteq \sum I_\alpha$. □

Remark 26.1. We actually only need to consider C_I when $I = \sqrt{I}$, since $C_I = C_{\sqrt{I}}$. Note that $I \subseteq \sqrt{I}$, so if $P \supseteq I$ then $P \supseteq I$. But if $P \supseteq I$, then

$$P \supseteq \bigcap_{\substack{Q \supseteq I \\ Q \text{ prime}}} Q = \sqrt{I},$$

so $P \supseteq I \Leftrightarrow P \supseteq \sqrt{I}$. Hence $C_I = C_{\sqrt{I}}$.

Remark 26.2. Clearly, if $I \supseteq J$, then $C_I \subseteq C_J$.

We consider some specific examples of $\mathrm{Spec}(R)$.

Example 26.6. $\mathrm{Spec}(\mathbb{Q}) = \{(0)\}$. $\mathrm{Spec}(\mathbb{Z}) = \{(p) : p \text{ prime number}\}$.

Let $P \in \mathrm{Spec}(R)$. Then what is the closure of P? Recall that the closure $\overline{P} = C_P = \{Q \in \mathrm{Spec}(R) : Q \supseteq P\}$. Then $\{\overline{P}\} = \{P\}$ if and only if P is maximal. Also, P is dense (i.e., $\overline{P} = \mathrm{Spec}(R)$) if and only if $P = \sqrt{(0)}$.

Example 26.7. In $\mathrm{Spec}(\mathbb{Z})$, every point is closed; the dense point is (0). If I is an ideal in $\mathbb{Z}$, then either $I = (0) \Rightarrow C_I = \mathrm{Spec}(\mathbb{Z})$, or for $n \geq 2$, $I = (n) \Rightarrow C_I = \{(p) : (p) \supseteq (n)\} = \{(p) : p \,|\, n\}$. Clearly, if $I = \mathbb{Z}$ then $C_I = \emptyset$. Thus this topology is a *cofinite* topology since the complement of an open set is finite.

Example 26.8. Let $R = \mathbb{Z}_{(2)}$. Then there is a correspondence between $\mathrm{Spec}(\mathbb{Z}_{(2)})$ and the set $\{P \in \mathrm{Spec}(Z) : P \subseteq (2)\}$. (2) is a closed point in $\mathbb{Z}$ and (0) is the dense point in $\mathbb{Z}$. Similarly, by this correspondence, $2\mathbb{Z}_{(2)}$ is a closed point and (0) is the dense point. We will elaborate on this point more in the following theorem:

Theorem 26.9. *Let R be an integral domain. Suppose also that $P \in \operatorname{Spec}(R)$, and that*

$$X = \{Q \in \operatorname{Spec}(R) : Q \subseteq P\}$$

with the subspace topology. We showed that there is a correspondence:

$$X \overset{bij'n}{\longleftrightarrow} \operatorname{Spec}(R_P)$$
$$Q \overset{f}{\longmapsto} QR_P$$
$$J \cap R \overset{g}{\longmapsto} J.$$

Then f and g are continuous bijections and so X is homeomorphic to $\operatorname{Spec}(R_P)$. If C is a closed subset of $\operatorname{Spec}(R_P)$, then $C = C_I$ where I is an ideal of R_P. That is, $C = \{Q \in \operatorname{Spec}(R_P) : Q \supseteq I\}$.

Proof. Note that

$$f^{-1}(C) = \{L \in \operatorname{Spec}(R) : L \subseteq P, f(L) = LR_P \supseteq I\} = \{L \in \operatorname{Spec}(R) : L \supseteq I \cap R\} \cap X,$$

which is closed in X. Also, note that $LR_P \supseteq I \Leftrightarrow L = LR_P \cap R \supseteq I \cap R$, as required.

Conversely, if $C \subseteq X$ is closed, then

$$C = X \cap \{L \in \operatorname{Spec}(R) : L \supseteq I\}$$

for some radical ideal I. So

$$\begin{aligned} g^{-1}(C) &= \{LR_P : L \supseteq I; L \subseteq P\} = \{LR_P : L \supseteq I\} \\ &= \{LR_P : LR_P \supseteq IR_P\} = \{Q \in \operatorname{Spec}(R_P) : Q \supseteq IR_P\} = C_{IR_P} \subseteq \operatorname{Spec}(R_P). \quad \square \end{aligned}$$

27. March 12

Let R be a ring and $X = \operatorname{Spec}(R)$, where the closed sets are of the form $C_I = \{P \in \operatorname{Spec}(R) : P \supseteq I\}$. Recall that we can only consider the cases when $I = \sqrt{I}$ and $J = \sqrt{J}$ hence $C_I = C_{\sqrt{I}}$ and $C_J = C_{\sqrt{J}}$. If $C_I \supseteq C_J$, then $\{P : P \supseteq I\} \supseteq \{P : P \supseteq J\}$, hence $I \subseteq J$. Conversely, if $C_I \supseteq C_J$ then whenever $P \supseteq J$ then $P \supseteq I$. Hence

$$\bigcap_{\substack{P \text{ prime} \\ P \supseteq J}} P \supseteq \bigcap_{\substack{P \text{ prime} \\ P \supseteq I}} P.$$

So $\sqrt{J} \supseteq \sqrt{I}$ so $J \supseteq I$ as required.

Remark 27.1. C_I with the subspace topology on $\operatorname{Spec}(R)$ is homeomorphic to $\operatorname{Spec}(R/I)$. This claim follows from correspondence. Let $f : C_I \to \operatorname{Spec}(R/I)$ such that $f(P) = \overline{P}$ where $\overline{J}$ is the image of J under the natural map $J \mapsto J/I$. Then f is a bijection, since by the correspondence theorem we have

$$C_I = \{P : P \supseteq I\} \longleftrightarrow \operatorname{Spec}(R/I)$$
$$P \overset{1-1}{\longleftrightarrow} \overline{P}$$

To see that f isa homeomorphism, note that if J is an ideal of R/J then there exists an ideal $L \supseteq I$ of R such that $\overline{L} = J$, by correspondence. So we have

$$f^{-1}(C_J) = f^{-1}(\{Q \in \operatorname{Spec}(R/I) : Q \supseteq J\}) = \{P \in \operatorname{Spec}(R) : P \supseteq I\} = C_L \subseteq C_I,$$

so f is indeed continuous. Conversely, if C is a closed subset of C_I, then $C = C_L$ for some $L \supseteq I$. Then note that $f(C_L) = \{Q \in \mathrm{Spec}(R/I) : Q \supseteq I\} = C_{\overline{L}}$. Therefore f^{-1} is continuous so f is a homeomorphism.

This example fits more generally into the following framework. Consider the following problem from Assignment #4. In Assignment #4, you will show that if $\phi^* : R \to S$ is a ring homomorphism, then an induced map $\phi : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ defined as $\phi(P) \mapsto (\phi^*)^{-1}(P) =: Q$ is a continuous map. In this setting, if $\phi^* : R \to R/I$ given by $r \mapsto r + I$ gives a continuous map, then the image of $\phi : \mathrm{Spec}(R/I) \to \mathrm{Spec}(R)$ is C_I, and this $\phi = f^{-1}$.

So far, we have been talking about closed sets. What about open sets then? Start with $f \in R$. Let's define $U(f) := \mathrm{Spec}(R) \setminus C_{(f)} = \{P \in \mathrm{Spec}(R)\} \setminus \{P : P \supseteq (f) \Leftrightarrow f \in P\} = \{P \in \mathrm{Spec}(R) : f \in P\}$. Note that $\{P \in \mathrm{Spec}(R) : f \in P\} \cong \mathrm{Spec}(R_f)$. Then $U(f)$ is indeed open.

Definition 27.1. Such $U(f)$ is said to be a *principal open set.*

Remark 27.2. The sets $U(f)$ form a basis for the Zariski topology. Notice also that if U is an open set with $U = \mathrm{Spec}(R) \setminus C_I$ and if $f \in I$ then $U(f) \subseteq U$. Note that if $f \in I$ then $\sqrt{(f)} \subseteq \sqrt{I}$, so $C_I \subseteq C_{(f)}$. Therefore $\mathrm{Spec}(R) \setminus C_{(f)} \subseteq \mathrm{Spec}(R) \setminus C_I$, or $U(f) \subseteq U$ as desired.

Theorem 27.2. *Let R be a ring. Then the following are equivalent:*

(1) $\mathrm{Spec}(R)$ *is disconnected*
(2) R has an idempotent $e \neq 0, 1$
(3) $R \cong R_1 \times R_2$ where both R_1 and R_2 are non-trivial.

Proof. ((1) $\Rightarrow$ (2)) Suppose that $\mathrm{Spec}(R)$ is disconnected. Then there exist I, J ideals of R such that $\mathrm{Spec}(R) = C_I \sqcup C_J$, where $\sqcup$ denotes the disjoint union. So if $C_I \cap C_J = \emptyset$, then $C_{I+J} = \emptyset$. On the other hand, if $C_I \cup C_J = \mathrm{Spec}(R)$ then $C_{I \cap J} = C_{IJ} = \mathrm{Spec}(R)$. Note that $C_{I+J} = \emptyset \Leftrightarrow I + J = R$, and that $C_{IJ} = \mathrm{Spec}(R) \Leftrightarrow \bigcap_{P \text{ prime}} P = \sqrt{(0)} \supseteq IJ$. Since $I + J = R$, there exist $x \in I$ and $y \in J$ such that $x + y = 1$ and $xy \in IJ \subseteq \sqrt{(0)}$, i.e., $(xy)^n = 0$ for some $n \geq 1$. Now

$$1 = (x+y)^{2n} = \underbrace{x^{2n} + \binom{2n}{1} x^{2n-1}y + \cdots + \binom{2n}{n} x^n y^n}_{=:e} + \underbrace{\binom{2n}{n+1} x^{n-1}y^{n+1} \cdots + \binom{2n}{2n-1} xy^{2n-1} + y^{2n}}_{=1-e}.$$

It is easy to see that $e(1-e) = 0$. Why? note that $e \in x^n R$ and $1 - e \in y^n R$ so $e(1-e) \in (xy)^n R = (0)$. So $e^2 = e$. So we are done once we show that $e \neq 0, 1$. But this is easy: since $e \in x^n R \subseteq I \subsetneq R$ and $1 - e \in J \subsetneq R$, we see that $e \neq 1$ and $1 - e \neq 1$. Therefore $e \neq 0, 1$ as required.

((2) $\Rightarrow$ (3)) Suppose that there exists $e \in R, e \neq 0, 1$ such that $e^2 = e$. Let $R_1 = Re$ and $R_2 = R(1-e)$. Since $e \neq 0, 1$ neither R_1 nor R_2 is the zero ring. So R_1 anD R_2 are rings with identities as e and $1 - e$ respectively. Now the following claim comes in handy:

Claim. If f is an idempotent in R then Rf is a ring with unit f.

If $r \in R$ then $rf \in Rf$. Thus $(rf)f = rf^2 = rf$, and $f(rf) = rf^2 = rf$. Also, $(rf) \cdot (sf) = rsf$ and $rf + sf = (r+s)f$ as desired.

Define $\phi : R \to R_1 \times R_2$ by $\phi(r) = (re, r(1-e))$. We claim that ϕ is an isomorphism. ϕ is a homomorphism since

$$\begin{aligned}
\phi(r_1 + r_2) &= ((r_1 + r_2)e, (r_1 + r_2)(1-e)) \\
&= (r_1 e, r_1(1-e)) + (r_2 e, r_2(1-e)) = \phi(r_1) + \phi(r_2) \\
\phi(r_1 r_2) &= (r_1 r_2 e, r_1 r_2 (1-e)) \\
&= (r_1 r_2 e^2, r_1 r_2 (1-e)^2) = (r_1 e r_2 e, r_1(1-e) r_2 (1-e)) \\
&= \phi(r_1)\phi(r_2).
\end{aligned}$$

For injectivity, suppose $\phi(r) = (0,0)$. That is, $re = 0$ and $r(1-e) = 0$. therefore $re + r(1-e) = r = 0$. As for surjectivity, given any $ae \in Re$ and $b(1-e) \in R(1-e)$, we have $\phi(ae + b(1-e)) = (ae, b(1-e))$. So $R \cong R_1 \times R_2$ as claimed.

$((3) \Rightarrow (1))$ This one is quite immediate. If $R = R_1 \times R_2$ then $I = R_1 \times \{0\}$ is an ideal, and similarly $J = \{0\} \times R_2$ is an ideal. Clearly $IJ = (0,0)$ and $I + J = R$ so $C_I \sqcup C_J = \operatorname{Spec}(R)$ as required. □

Definition 27.3. A topological space X is *reducible* if there exist proper closed subsets C_1 and C_2 (not necessarily disjoint) such that $X = C_1 \cup C_2$. Otherwise, X is said to be *irreducible*.

Remark 27.3. Evidently, if X is disconnected, then X is automatically reducible. However, the converse is *false*.

28. March 13

Can we find a ring R such that $\operatorname{Spec}(R)$ is connected but reducible?

Example 28.1. Let $R = \mathbb{C}[x,y]/(x,y)$. Let $\overline{x}, \overline{y}$ denote the images of x and y in R. Then $\operatorname{Spec}(R)$ is reducible since $C_{(\overline{x})} \cup C_{(\overline{y})} = \operatorname{Spec}(R)$: $\bar{x}\bar{y} = 0$ so if $P \in \operatorname{Spec}(R)$ then $\bar{x}\bar{y} \in P$. So $\bar{x} \in P$ or $\bar{y} \in P$ so $P \in C_{(\bar{x})}$ or $P \in C_{(\bar{y})}$. Now we need to show that $\operatorname{Spec}(R)$ is connected. Notice

$$R = \{c + \bar{x}p(\bar{x}) + \bar{y}q(\bar{y}) : c \in C, p(t), q(t) \in \mathbb{C}[t]\}.$$

We showed that $\operatorname{Spec}(R)$ is disconnected if and only if there is an idempotent $e \neq 0, 1$. If $e = c + \bar{x}p(\bar{x}) + \bar{y}q(\bar{y})$ is an idempotent, so $(c + \bar{x}p(\bar{x}) + \bar{y}q(\bar{y}))^2 = c^2 + 2c\bar{x}p(\bar{x}) + 2c\bar{y}q(\bar{y}) + \bar{x}^2 p(\bar{x})^2 + \bar{y}^2 q(\bar{y})^2$. Hence $\deg(\bar{x}p(\bar{x})) = \deg(\bar{y}q(\bar{y})) = 0$. Thus $e = c \in \mathbb{C}$ so $e = 0, 1$. So $\operatorname{Spec}(R)$ is connected.

Theorem 28.2. $\operatorname{Spec}(R)$ *is irreducible if and only if* $N := \sqrt{(0)}$ *is a prime ideal. Therefore,* $\operatorname{Spec}(R)$ *is irreducible if and only if* R/N *is an integral domain.*

Proof. $\operatorname{Spec}(R) \cong \operatorname{Spec}(R/N)$, so we may assume without loss of generality that R is reduced (i.e., $(0) = \sqrt{(0)}$). Now if R is not an integral domain, then there exist $a, b \in R \setminus \{0\}$ such that $ab = 0$. Then $\operatorname{Spec}(R) = C_{(a)} \cup C_{(b)} = C_{(a)\cap(b)} = C_{(ab)} = C_{(0)} = \operatorname{Spec}(R)$. So if R is not an integral domain, then $\operatorname{Spec}(R)$ is reducible.

If $\operatorname{Spec}(R)$ is reducible, then $\operatorname{Spec}(R) = C_I \cup C_J = C_{IJ}$. So $IJ = (0)$ and $I, J \neq (0)$. Pick $a \in I \setminus \{0\}$ and $b \in J \setminus \{0\}$ such that $ab = 0$. Thus R is not an integral domain, as desired. □

Corollary 28.3. *$C_I \subseteq \operatorname{Spec}(R)$ is irreducible if and only if $\sqrt{I}$ is a prime ideal.*

Proof. $\operatorname{Spec}(R/I) \cong C_I = C_{\sqrt{I}} \cong \operatorname{Spec}(R/\sqrt{I})$, and $S = R/\sqrt{I}$ is reduced. Thus C_I is irreducible if and only if S is an integral domain. This is equivalent to saying that $\sqrt{I}$ is a prime ideal. □

Theorem 28.4. *Let R be a ring. Then $\operatorname{Spec}(R)$ is quasi-compact. That is, if $\operatorname{Spec}(R) = \bigcup U_\alpha$ where U_α open sets, then there exists a finite collection of open sets $\{U_{\alpha_1}, \dots, U_{\alpha_s}\}$ such that $\operatorname{Spec}(R) = \bigcup_{i=1}^{s} U_{\alpha_i}$.*

Proof. Suppose that $\operatorname{Spec}(R) = \bigcup_\alpha U_\alpha$, where $U_\alpha = \operatorname{Spec}(R) \setminus C_{I_\alpha}$ for some ideal I_α of R. Then $\bigcup U_\alpha = \operatorname{Spec}(R)$ if and only if $\bigcap C_{I_\alpha} = \emptyset$ if and only if $C_{\sum I_\alpha} = \emptyset$; and this is equivalent to saying that $\sum I_\alpha = R$. So there exist $i_{\alpha_k} \in I_{\alpha_k}$ such that $i_{\alpha_1} + \cdots + i_{\alpha_s} = 1$. This would mean that $I_{\alpha_1} + \cdots + I_{\alpha_s} = R$. Thus $C_{\sum I_{\alpha_i}} = \emptyset$, so $\bigcap_{i=1}^{s} C_{I_{\alpha_i}} = \emptyset$. So $\bigcap_{i=1}^{s} U_{\alpha_i} = \operatorname{Spec}(R)$. □

Let R be Noetherian. When is $\operatorname{Spec}(R)$ Hausdorff?

Theorem 28.5. *Suppose that R is a Noetherian ring. Then the following are equivalent:*

(1) $\operatorname{Kdim}(R) = 0$
(2) $\operatorname{Spec}(R)$ *is compact and Hausdorff*
(3) $\operatorname{Spec}(R)$ *is finite and discrete*
(4) $R/N \cong F_1 \times \cdots F_s$ *where* $N = \sqrt{(0)}, s \geq 1$ *and* F_i *fields.*

Proof. Earlier we showed (1) ⇔ (4), and we just showed (3) ⇒ (2) ⇒ (1). Thus we only need to show (4) ⇒ (3). If $R/N \cong F_1 \times F_s$ then $\operatorname{Spec}(R) \cong \operatorname{Spec}(R/N) \cong \operatorname{Spec}(F_1 \times F_s)$. But since $F_1 \times F_s$ is Noetherian and has Krull dimension 0, it has only finitely many prime ideals, all of which are maximal. So $|\operatorname{Spec}(R)| < \infty$ and each point is closed. Therefore the topology is discrete. □

28.1. **Noetherian topological spaces.**

Definition 28.6. Let X be a topological space. We say that X is a *Noetherian topological space* if whenever $C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$ is a descending chain of closed subsets of X then there exists n such that $C_n = C_{n+1} = C_{n+2} = \cdots$.

Definition 28.7. If X is a topological space, then we can define the Krull dimension of X to be

$$\operatorname{Kdim}(X) := \sup_n \{\text{there exists a chain } C_0 \supsetneq C_1 \supsetneq \cdots \supsetneq C_n, C_i \text{ irreducible subsets}\}.$$

Example 28.8. If R is a ring then $\operatorname{Kdim}(R) = \operatorname{Kdim}(\operatorname{Spec}(R))$.

28.2. **Artinian rings.**

Definition 28.9. A ring R is *Artinian* if every *descending* chain of ideals terminates, i.e., if $I_1 \supseteq I_2 \supseteq \cdots$ then there exists n such that $I_n = I_{n+1} = I_{n+2} = \cdots$. An R-module M is *Artinian* if it satisfied the descending chain condition on submodules.

Proposition 28.10. *R is Artinian if and only if R is Artinian as an R-module.*

Proof. Just as with the Noetherian case, the same proof shows that R is Artinian iff every non-empty subset of ideals has a minimal element with respect to inclusion. □

29. March 17

Lemma 29.1. *If R is a ring and*

$$0 \to M_1 \to M \xrightarrow{\pi} M_2 \to 0$$

is a short exact sequence of R-modules, then M is Artinian if and only if M_1 and M_2 are Artinian.

Proof. ($\Rightarrow$) This is clear, since $M_2 \cong M/M_1$ and $M_1 \subseteq M$.

($\Leftarrow$) Suppose that M_1 and M_2 are Artinian, and let $N_1 \supseteq N_2 \supseteq \cdots$ be a descending chain of submodules in M. Without loss of generality, let $M_1 \subseteq M$. Then $N_1 \cap M_1 \supseteq N_2 \cap M_1 \supseteq \cdots$ is a descending chain in M, and since M_1 is Artinian there exists i such that $N_i \cap M_1 = N_{i+1} \cap M_1 = \cdots$. Similarly, we have that $\pi(N_1) \supseteq \pi(N_2) \supseteq \cdots$, which must stabilize as M_2 is Artinian (i.e., exists j such that $\pi(N_j) = \pi(N_{j+1}) = \cdots$.

Let $n \geq \max(i, j)$. Then we claim that $N_n = N_{n+1}$ implies $N_{\max(i,j)} = N_{\max(i,j)+1} = \cdots$. Thus the chain terminates so M is Artinian. Since $n \geq j$ we have $\pi(N_n) = \pi(N_{n+1})$. We also know that $N_{n+1} \subseteq N_n$, so we need to show that $N_{n+1} \supseteq N_n$. Suppose $x \in N_n$. Then $\pi(x) \in \pi(N_n) = \pi(N_{n+1})$, so there exists $y \in N_{n+1}$ such that $\pi(x) = \pi(y)$. Hence $\pi(x-y) = 0$ so $x, y \in M_1$. But then $x - y \in N_n$, so $x - y \in N_n \cap M_1 = N_{n+1} \cap M_1$ since $n \geq i$. Hence $x - y \in N_{n+1}$ so $x \in y + N_{n+1} \subseteq N_{n+1}$. □

Proposition 29.2. *If R is a ring in which $(0) = M_1 M_2 \cdots M_s$, where M_i's are maximal ideals in R, then R is Artinian if and only if R is Noetherian.*

Proof. ($\Leftarrow$) Let $A_1 = M_1, A_2 = M_1 M_2, A_3 = M_1 M_2 M_3, \ldots, A_s = M_1 M_2 M_3 \cdots M_s = (0)$ and $A_0 = R$. Suppose that R is Noetherian but not Artinian. Then $A_0 \cong R$ is not Artinian as an R-module. However, $A_s = (0)$ is Artinian as an R-module. Therefore, there must exist some largest i such that $A_i = M_1 M_2 \cdots M_i$ is not Artinian but $A_{i+1} = M_1 M_2 \cdots M_{i+1}$ is. Note that

$$0 \to A_{i+1} \to A_i \to A_i/A_{i+1} \to 0$$

is a short exact sequence. Our goal is to show that A_i/A_{i+1} is Artinian, since that would imply that A_i is Artinian, when R is Artinian (hence a contradiction). So it suffices to show that $A_i/A_{i+1} = M_1 M_2 \cdots M_i / M_1 M_2 \cdots M_{i+1}$ is Artinian. Notice that M_{i+1} annihilates A_i/A_{i+1} so A_i/A_{i+1} inherits the structure of an F-module, where $F := R/M_{i+1}$. Since R is Noetherian, A_i is Noetherian also. Therefore A_i/A_{i+1} is Noetherian as an R-module. Therefore A_i/A_{i+1} is Noetherian as an F-module or equivalently as an F-vector space. Recall that an F-vector space is Noetherian as an F-module if and only if the vector space is finite-dimensional. Therefore $\dim_F A_i/A_{i+1} < \infty$. Another fact: suppose that F is a field and V is an F-vector space. Then V is Artinian as an F-module if and only if V is finite-dimensional. Hence A_i/A_{i+1} is an Artinian F-module, so A_i/A_{i+1} is Artinian as an R-module, as M_{i+1} annihilates A_i/A_{i+1}. Contradiction!

($\Rightarrow$) Let $A_1 = M_1, A_2 = M_1 M_2, A_3 = M_1 M_2 M_3, \ldots, A_s = M_1 M_2 M_3 \cdots M_s = (0)$ and $A_0 = R$. Suppose that R is Artinian but not Noetherian. Then $A_0 \cong R$ is not Noetherian as an R-module. However, $A_s = (0)$ is Noetherian as an R-module. Therefore, there must exist some largest i such that $A_i = M_1 M_2 \cdots M_i$ is not Noetherian but $A_{i+1} = M_1 M_2 \cdots M_{i+1}$ is. Note that

$$0 \to A_{i+1} \to A_i \to A_i/A_{i+1} \to 0$$

is a short exact sequence. Our goal is to show that A_i/A_{i+1} is Noetherian, since that would imply that A_i is Noetherian, whence R is Noetherian (hence a contradiction). So it suffices to show that $A_i/A_{i+1} = M_1M_2\cdots M_i/M_1M_2\cdots M_{i+1}$ is Noetherian. Notice that M_{i+1} annihilates A_i/A_{i+1} so A_i/A_{i+1} inherits the structure of an F-module, where $F := R/M_{i+1}$. Since R is Artinian, A_i is Artinian also. Therefore A_i/A_{i+1} is Artinian as an R-module. Therefore A_i/A_{i+1} is Artinian as an F-module or equivalently as an F-vector space. Recall that an F-vector space is Artinian as an F-module if and only if the vector space is finite-dimensional. Therefore $\dim_F A_i/A_{i+1} < \infty$. Another fact: suppose that F is a field and V is an F-vector space. Then V is Noetherian as an F-module if and only if V is finite-dimensional. Hence A_i/A_{i+1} is an Noetherian F-module, so A_i/A_{i+1} is Noetherian as an R-module, as M_{i+1} annihilates A_i/A_{i+1}. Contradiction! □

30. March 19

Theorem 30.1. *R is Artinian if and only if R is Noetherian and has* $\mathrm{Kdim}(R) = 0$.

Proof. ($\Leftarrow$) If R is Noetherian and has Krull dimension 0, then by Noether's result, there exist prime ideals $P_1, \ldots, P_s$ such that $P_1P_2\cdots P_s = (0)$. Since $\mathrm{Kdim}(R) = 0$, each P_i is maximal so (0) is a product of maximal ideals and R is Noetherian. Thus by Proposition 29.2, R is Artinian.

($\Rightarrow$) For this direction, we need to prove a few claims first.

Claim (Claim 1). Let R be Artinian and let $P \in \mathrm{Spec}(R)$. Then P is maximal. In particular, $\mathrm{Kdim}(R) = 0$.

Proof of Claim 1. Let $S = R/P$. By correspondence, S is Artinian and S is an integral domain. We will then show that S is a field. Let $x \in S \setminus \{0\}$. Consider the chain $xS \supseteq x^2S \supseteq x^3S \supseteq \cdots$. Since S is Artinian, there exists n such that $x^nS = x^{n+1}S$. So if $x^n \in x^{n+1}S$, then there exists $y \in S$ such that $x^n = x^{n+1}y$. Divide both sides by x^n to get $xy = 1$. Therefore x has an inverse meaning that S is a field. □

Claim (Claim 2). Let R be Artinian. Then $\mathrm{Spec}(R)$ is finite.

Proof of Claim 2. Suppose that we have distinct prime ideals $P_1, P_2, \ldots$. Note that by Claim 1, we know all of them are maximal. Consider the chain

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \cdots.$$

This chain terminates, so there exists n such that

$$\bigcap_{i=1}^{n} P_i = \bigcap_{i=1}^{n+1} P_i.$$

Therefore $P_1\cdots P_n \subseteq P_{n+1}$. Recall that the P_i"s are all distinct and all maximal by Claim 1. Therefore there exists $a_i \in P_i \setminus P_{n+1}$ for all $i = 1, \ldots n$. So $a_1\cdots a_n \subseteq P_1\cdots P_n \subseteq P_{n+1}$. But this contradicts the fact that P_{n+1} is prime and none of a_i's are in P_{n+1}. The claim follows. □

Claim (Claim 3). If R is Artinian then $J(R)$ is nilpotent.

Proof. Let $J = J(R)$. Consider the chain $J \supseteq J^2 \supseteq J^3 \supseteq \cdots$. Since R is Artinian, there exists n such that $J^n = J^{n+1} = \cdots$. So $J^n = J^{2n}$. Trick: Let $\mathscr{S} := \{I \subseteq R : I \text{ ideal of } R, I \subseteq J^n, IJ^n \neq (0)\}$. Note that $\mathscr{S} \neq \emptyset$, since $J^n \in \mathscr{S}$: notes that $J^n J^n = J^{2n} = J^n = (0)$. Since R is Artinian, there exists a minimal elements $L \in \mathscr{S}$. So $LJ^n \neq (0)$ but if $L' \subsetneq L$ then $L'J^n = (0)$. Since $LJ^n \neq (0)$, there exists $x \in L$ such that $xJ^n \neq (0)$.

We claim that $L = Rx$. Since $x \in L$, clearly $Rx \subseteq L$. Since $xJ^n \neq (0)$, we have $J^n Rx \neq (0)$. Thus by minimality $L = Rx$. Now by assumption we have $J^n L \neq (0)$., and $J^n J^n L = J^n L \neq (0)$. Thus $J^n L = L$ by minimality. But then since $J^n L \subseteq JL = L$, by Nakayama's lemma $L = (0)$ (recall that $L = Rx$ is finitely generated). Contradiction! □

Claim 1 gives us $\operatorname{Kdim}(R) = 0$. Claim 2 says that $\operatorname{Spec}(R) = \{P_1, \ldots, P_k\}, k \geq 1$. Moreover, by Claim 1, $P_1, \ldots, P_k$ are maximal so

$$J(R) = \bigcap_{i=1}^{k} P_i \supseteq P_1 \cdots P_k.$$

So by Claim 3, we know there exists $m \geq 1$ such that $J(R)^m = (0)$. Therefore $J(R)^m = (0) \supseteq (P_1 P_2 \cdots P_k)^m$, which is a finite product of maximal ideals. So (0) is the finite project of maximal ideals, and since R is Artinian, Lemma 29.2 give us that R is Noetherian. □

Corollary 30.2. *If R is Artinian and $J(R) = (0)$, then $R \cong F_1 \times \cdots \times F_s$ with $s \geq 1$ and F_i fields.*

Proof. $(0) = J(R) = P_1 \cap P_2 \cap \cdots \cap P_k$ where each P_i is maximal. Therefore P_i's are pairwise co-maximal. So by the Chinese remainder theorem we have

$$R = R/\bigcap_{i=1}^{s} P_i \cong \prod_{i=1}^{s} R/P_i.$$

Letting $F_i := R/P_i$ yields the result. □

Definition 30.3. Let R be a *noncommutative* ring. Then we say that R is *(left-)Artinian* if ever descending chain of *left ideals* $L_1 \supseteq L_2 \supseteq \cdots$ terminates. The *Jacobson radical of R* $J(R)$ is defined to be

$$J(R) = \bigcap_{M \text{ max. left ideals}} M.$$

Theorem 30.4 (Artin-Wedderburn theorem)**.** *Let R be a ring (not necessarily commutative). If R is left-Artinian with $J(R) = (0)$, then*

$$R = \prod_{i=1}^{s} \mathrm{M}_{n_i}(D_i),$$

where $\mathrm{M}_{n_i}(D_i)$ is the matrix ring over the division ring D_i.

30.1. **Primary decomposition.**

Remark 30.1 (Motivation). If I is an ideal of R and $I \subseteq P_i$ for $i = 1, \ldots, s$ are the maximal ideals so that $\sqrt{I} = P_1 \cap \cdots \cap P_s$. In particular, if $I = \sqrt{I}$ then I is a finite intersection of prime ideals.

Definition 30.5. Let I a proper ideal of R. We say that I is *primary* if whenever $xy \in I$ we have either $x \in I$ or there exists n such that $y^n \in I$. Equivalently, I is primary if whenever $xy \in I$ at least one of the following holds:

- $x \in I$
- $y \in I$
- there exists n such that $x^n, y^n \in I$.

Example 30.6. Let $R = \mathbb{Z}$. Then $6\mathbb{Z}$ is not primary since if $x = 3, y = 2$ then $xy \in 6\mathbb{Z}$ but $x \notin 6\mathbb{Z}$ and $y^n \notin 6\mathbb{Z}$ for all $n \geq 1$. $8\mathbb{Z}$ is primary: if $xy \in 8\mathbb{Z}$ then $8 \,|\, xy$. Therefore either $8 \,|\, x$ or $2 \,|\, y$ so $8 \,|\, y^3$. Thus either $x \in 8\mathbb{Z}$ or $y^3 \in 8\mathbb{Z}$. $3\mathbb{Z}$ is primary, since if $xy \in 3\mathbb{Z}$ (i.e., $3 \,|\, xy$) then either $x \in 3\mathbb{Z}$ or $y^1 \in 3\mathbb{Z}$.

Lemma 30.7. *Let $n > 1$. Then $n\mathbb{Z}$ is primary if and only if $n = p^k$ for some p prime and and $k \geq 1$.*

Proof. If $n \neq p^k$ then $n = ab$ with $a, b > 1$ and $\gcd(a, b) = 1$. So $n \nmid a, n \nmid b$ hence $n \nmid a^k, n \nmid b^k$. Conversely, if $n = p^k\mathbb{Z}$ and $xy \in p^k\mathbb{Z}$ then either $p^k \,|\, x, p^k \,|\, y$ or ($p \,|\, x$ and $p \,|\, y$). Therefore $p^k \,|\, x^k$ and $p^k \,|\, y^k$. Thus either $x \in p^k\mathbb{Z}, y \in p^k\mathbb{Z}$ or $x^k, y^k \in p^k\mathbb{Z}$. □

Proposition 30.8. *Let Q be primary. Then $\sqrt{Q}$ is a prime ideal.*

Proof. Suppose that $\sqrt{Q}$ is not prime. THen there exist x, y such that $xy \in \sqrt{Q}$ but $x, y \notin \sqrt{Q}$. Because $xy \in \sqrt{Q}$ we have $x^n y^n \in Q$ for some $n \geq 1$. Now no power of x can be in Q, and the same holds for y. This means that Q is not primary, which is a contradiction. □

31. March 20

Recall that last time we proved that

(1) If P is prime then P is primary.
(2) If P is primary then $\sqrt{P}$ is prime.

In general, the converse of (2) does *not* hold.

Example 31.1. Let $R := \mathbb{C}[x, y, z]/(xy - z^2) = \mathbb{C}[\bar{x}, \bar{y}, \bar{z}]$ where $\bar{x}\bar{y} = \bar{z}^2$. Let $P = (\bar{x}, \bar{z}) \subseteq R$. Notice that $R/P = \mathbb{C}[\bar{x}, \bar{y}, \bar{z}/(\bar{x}, \bar{z}) \cong \mathbb{C}[x, y, z]/(xy - z^2, x, z) = \mathbb{C}[x, y, z]/(x, z) \cong \mathbb{C}[y]$ which is an integral domain. Since R/P is an integral domain, P is prime. Let $Q = P^2$. Then $\sqrt{Q} = P$ prime but we claim that Q is not primary. Clearly $\bar{x} \cdot \bar{y} \in Q$, since $\bar{x} \cdot \bar{y} = \bar{z} \cdot \bar{z} \in P^2 = Q$. If Q is primary, either $\bar{x} \in Q$ or $\bar{y} \in Q$ for some $n \geq 1$.

Notice that if $\bar{y}^n \in Q = P^2$ then $\bar{y}^n \in P$. But $R/P \cong \mathbb{C}[t]$ (let $\bar{x}, \bar{z} \mapsto 0$ and $\bar{y} \mapsto t$) so $\bar{y}^n \notin P$ because $t^n \neq 0$. Also, $\bar{x} \notin Q$. Why? Note that $P^2 = (\bar{x}, \bar{x}\bar{z}, \bar{z}^2)$. This means that $\bar{x} \in P^2$ if and only if $x \in (x^2, xz, z^2, xy - z^2)$, but this cannot happen. Hence $\bar{y}^n \notin Q$ for all $n \geq 1$ and $\bar{x} \in Q$ so Q is not primary.

There is a partial converse, however.

Proposition 31.2. *Let Q be an ideal of R and suppose that $P := \sqrt{Q}$ is a maximal ideal. Then Q is primary.*

Proof. Let $S = R/Q$. Then S is a local ring with the unique maximal ideal $P/Q =: M$. Since S is local, if $x \in S \setminus M$ is a unit in S. Suppose that $xy \in Q$. This means $\bar{x} \cdot \bar{y} = 0 \in S$. If $\bar{x} \notin M$, then $\bar{x}$ is a unit. So $\bar{y} = 0$ in S so $y \notin Q$. If $\bar{y} \notin M$, then $\bar{y}$ is a unit. Therefore $\bar{x} = 0 \in S$ so $x \in Q$. If $\bar{x}, \bar{y} \in M$ then there exists n such that $\bar{x}^n = \bar{y}^n = 0$ so x^n and y^n are in Q. □

Definition 31.3. Let I be a proper ideal of R. We say that I is *reducible* if $I = J \cap K$ for some ideals J, K where $J \supsetneq I$ and $K \supsetneq I$. I is irreducible if whenever $I = J \cap K$ and $J, K \supseteq I$ ideals, we have $J = I$ or $K = I$.

Proposition 31.4. *Let R be a Noetherian ring. Then every proper ideal is a finite intersection of irreducible ideals.*

Proof. Suppose otherwise. Then $\mathscr{S} := \{I : I$ ideal; not a finite intersection of irreducible ideals$\}$ is non-empty. Since R is Noetherian, there exists a maximal element J of $\mathscr{S}$. J is not irreducible, so there exists $I.K \supsetneq J$ such that $J = I \cap K$. Now $I, K \notin \mathscr{S}$ by maximality of J, so $I = L_1 \cap L_2 \cap \cdots \cap L_s$, and $K = N_1 \cap \cdots \cap K_t$ where each of the L_i's and N_j's is irreducible. So $J = I \cap K = L_1 \cap \cdots \cap L_s \cap N_1 \cap \cdots \cap N_t$, so J is a finite intersection of irreducible ideals. So $\mathscr{S} = \emptyset$, as desired. □

Theorem 31.5. *Let R be a Noetherian ring. Then every ideal I of R has a decomposition $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$ where each Q_i is primary.*

This theorem follows immediately from the following lemma:

Lemma 31.6. *Let R be a Noetherian ring. Then every irreducible ideal is primary.*

Proof. Let I be an irreducible ideal, and let $S := R/I$, and suppose that $x, y \in R$ and $xy \in I$. We need to show that either $x \in I$ or $y^n \in I$ for some $n \geq 1$. In S, we have $\bar{x} \cdot \bar{y} = 0$ and we must show that either $\bar{x} = 0$ or $\bar{y}^n = 0$ for some $n \geq 1$. We also know that (0) is an irreducible ideal in S. We know this because of correspondence. Suppose that $\bar{x} \neq 0$. We will show that $\bar{y}^n - 0$ for some $n \geq 1$ and we are done. For $m \geq 1$, let

$$J_m = \{a \in S : a\bar{y}^m = 0\},$$

which is an ideal of S; and we also hate $J_1 \subseteq J_2 \subseteq J_3 \subseteq \cdots$. Therefore, since R is Noetherian, there exists n such that $J_n = J_{n+1}$. In other words, if $a\bar{y}^{n+1} = 0$, then $a\bar{y}^n = 0$. From this we claim that

Claim. $(0) = (\bar{x}) \cap (\bar{y}^n)$.

Suppose that $a \in (x) \cap (\bar{y}^n)$. Then $a = b\bar{x}$ and $a = c\bar{y}^n$. So $a\bar{y} = b\bar{x}\bar{y} = 0$. Hence $a\bar{y} = c\bar{y}^n \cdot \bar{y} = c\bar{y}^{n+1} = 0$. So $c \in J_{m+1} = J_m$. Thus $c\bar{y}^n = a = 0$. So $(0) = (\bar{x}) \cap (\bar{y}^n)$. But (0) is irreducible, so $\bar{y}^n = 0$ since we assumed that $\bar{x} \neq 0$. So (0) is primary, which implies that I is primary also. □

Remark 31.1. This is quite nice for R Noetherian integral domain of Krull dimension 1. Here Q is primary if and only if $Q = (0)$ or $\sqrt{Q}$ is maximal. Then every non-zero $I = Q_1 \cap \cdots \cap Q_s$ where each $\sqrt{Q_i}$ is maximal.

32. March 24: Valuation rings

Definition 32.1. Let K be a field. A *valuation* ν on K is a map $\nu : K \to \mathbb{Z} \cup \{\infty\}$ such that:

(1) $\nu(a) = \infty \Leftrightarrow a = 0$,
(2) $\nu(ab) = \nu(a) + \nu(b)$ where $\infty + n = n + \infty = \infty + \infty = \infty$,
(3) $\nu(a + b) \geq \min(\nu(a), \nu(b))$.

Example 32.2 (p-adic valuation). Let $K = \mathbb{Q}$ and p a prime number. For $n \in \mathbb{Z}$ non-zero, write $n = p^k n'$ with $p \nmid n'$. Define $\nu_p(n) = k$; and if $m/n \in \mathbb{Q}$ with $m \in \mathbb{Z}$ and n non-zero integer, define $\nu(m/n) := \nu(m) - \nu(n)$. One can check easily that this is well-defined and is a valuation.

Example 32.3. Let K be the field of rational functions on $\mathbb{C}$, $\mathbb{C}(x)$. Given $f(x) \in K \setminus \{0\}$, we shall define

$$\nu(f(x)) = \begin{cases} n & \text{if } f(x) \text{ has a zero at } x = 0 \text{ of order } n \geq 0 \\ -n & \text{if } f(x) \text{ has a pole at } x = 0 \text{ of order } n \geq 0 \\ 0 & \text{if } f(x) \text{ is analytic at } x = 0 \text{ and } f(0) = 0 \end{cases}$$

Time for some comparison between the two:

	$K = \mathbb{C}(x)$	$K = \mathbb{Q}$
Starting ring	$\mathbb{C}[x]$	$\mathbb{Z}$
Valuation	$\nu(p(x)) =$ order of zero at $x = 0$	$\nu(n) = k$ where $p^k \parallel n$
Associated ideal	(x)	$p\mathbb{Z}$
	$\nu(p(x)) = k \Leftrightarrow p(x) \in (x)^k \setminus (x)^{k+1}$	$\nu(n) = k \Leftrightarrow n \in (p\mathbb{Z})^k \setminus (p\mathbb{Z})^{k+1}$

Definition 32.4. Let K be a field and let $\nu : K \to \mathbb{Z} \cup \{\infty\}$ be a valuation. We define the *valuation ring of* ν:

$$\mathcal{O}_\nu = \{a \in K : \nu(a) \geq 0\}.$$

As it turns out, $\mathcal{O}_\nu$ is a ring. If $a, b \in \mathcal{O}_\nu$ then $\nu(ab) = \nu(a) + \nu(b) \geq 0$ so $ab \in \mathcal{O}_\nu$; similarly, $\nu(a + b) \geq \min(\nu(a), \nu(b)) \geq 0$ so $a + b \in \mathcal{O}_\nu$. Finally, since $\nu(0) = \infty$ and $\nu(1) = 0$, it follows that $0, 1 \in \mathcal{O}_\nu$. But there is more.

Remark 32.1. $\mathcal{O}_\nu$ is a *local ring* with the maximal ideal $\mathfrak{M}_\nu := \{a \in \mathcal{O}_\nu : \nu(a) > 0\}$. It is straightforward to see that $\mathfrak{M}_\nu$ is an ideal. If $x \in \mathcal{O}_\nu \setminus \mathfrak{M}_\nu$ then $\nu(x) = 0$ (and x is a unit). Therefore, $\nu(x^{-1} \cdot x) = \nu(1) = 0$. Therefore, $0 = \nu(x) + \nu(x^{-1})$, so $\nu(x^{-1}) = 0$. Hence $x^{-1} \in \mathcal{O}_\nu$ so $x \in \mathcal{O}_\nu^*$. Hence $\mathfrak{M}_\nu$ is the unique maximal ideal of $\mathcal{O}_\nu$.

Example 32.5. Let $K = \mathbb{Q}, p = 2$, and ν be the 2-adic valuation. What is $\mathcal{O}_\nu$? Let

$$\mathcal{O}_\nu = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \equiv 1 \pmod 2 \right\}, \mathfrak{M} = 2\mathcal{O}_\nu.$$

Example 32.6. $K = \mathbb{C}(x)$, and ν be the valuation as defined before.Then

$$\mathcal{O}_\nu = \left\{ \frac{p(x)}{q(x)} : q(0) \neq 0 \right\}.$$

Then $\mathfrak{M}_\nu = x\mathcal{O}_\nu$.

33. March 26

Definition 33.1. A ring of the form $\mathcal{O}_\nu$ is called a *discrete valuation ring (DVR).*

Remark 33.1. Recall that $\mathcal{O}_\nu$ is a local ring with the unique maximal ideal $\mathfrak{M}_\nu := \{a : \nu(a) > 0\} \subseteq \mathcal{O}_\nu$.

Proposition 33.2. *Let R be a DVR. Then R is a PID.*

Proof. Let I be an ideal of R. If $I = (0)$ or $I = R$, then I is evidently principal. So without loss of generality assume that $(0) \neq I \subseteq \mathfrak{M}_\nu$. Pick $a \in I$ with $\nu(a)$ minimal. We say that $I = (a)$. To see this, suppose that $\nu(y) \in I \setminus \{0\}$ where $\nu(y) \geq \nu(a)$. Let $K = \mathrm{Frac}(R)$. Then $ya^{-1} \in K$ and $\nu(ya^{-1}) = \nu(y) - \nu(a) \geq 0$. Therefore $ya^{-1} \in R$. So $y = (ya^{-1})a \in R$, so $Ra \subseteq I \subseteq Ra$. Thus $I = (a)$. □

Question. What are the possible Krull dimensions of a PID?

Solution: 0 and 1, and that's it. Let's see why. Suppose that R is a PID. Consider the chain $(0) \subsetneq P \subsetneq Q$ with P, Q prime ideals. Since R is a PID, there exist $x, y \in R$ such that $P = (x)$ and $Q = (y)$. $x \in (y)$ so $x = ay$ for some $a \in R$. So $ay \in (x)$ so $a \in (x)$. Thus $a = xb$ for some b, so $x = ay = xby$. Hence $1 = by$ so $1 \in (y)$. But this is a contradiction since (y) is proper. Therefore $\mathrm{Kdim}(R) \leq 1$.

Corollary 33.3. *If R is a DVR with a non-trivial valuation, then R is a PID, so R is Noetherian with Krull dimension* 1.

Proof. We saw that R is a PID, so it is Noetherian and is finitely generated. We know that R has the (non-zero) unique maximal ideal $\mathfrak{M}_\nu$ which is clearly a prime ideal. Therefore $\mathrm{Kdim}(R) \geq 1$. Hence $\mathrm{Kdim}(R) = 1$. □

Theorem 33.4. *Let R be a DVR. Then R is integrally closed (that is, if $x \in K$ be integral over R (that is, if $K = \mathrm{Frac}(R)$ and $x \in K$ and x is a solution to some monic polynomial over R, then $x \in R$).*

Proof. Let $K = \mathrm{Frac}(R)$ and let $x \in K$ be integral over R. Then there exists $n \geq 1, r_0, r_1, \ldots, r_{n-1} \in R$ such that

$$x^n + r_{n-1}x^{n-1} + \cdots + r_1 x + r_0 = 0.$$

To show that $x \in R$, we need to show that $\nu(x) \geq 0$. Suppose toward a contradiction that $\nu(x) = c < 0$. Then $\nu(x^n) = nc$ and $\nu(r_i x^i) = \nu(r_i) + \nu(x^i) = \nu(r_i) + ic \geq ic$ for all $i < n$. Now $x^n = -r_{n-1}x^{n-1} - r_{n-2}x^{n-2} - \cdots - r_1 x - r_0$. Note that $\nu(a_1 + a_2 + \cdots + a_n) \geq \min(\nu(a_1), \ldots, \nu(a_n))$, since ν is a valuation. So we have

$$\begin{aligned} nc = \nu(x^n) = \nu(-r_{n-1}x^{n-1} - \cdots - r_1 x - r_0) &\geq \min(\nu(r_{n-1}x^{n-1}), \ldots, \nu(r_0)) \\ &\geq \min((n-1)c, (n-2)c, \ldots, 0) = (n-1)c. \end{aligned}$$

So $nc \geq (n-1)c$, hence $c \geq 0$ as required. □

34. March 27

Theorem 34.1. *Let A be a Noetherian local domain of* $\mathrm{Kdim}(A) = 1$*. Let P be its maximal ideal of A. Then the following are equivalent:*

(1) A is a DVR
(2) A is integrally closed
(3) P is principal
(4) $\dim_k P/P^2 = 1$, where $k := A/P$, also called a residue field
(5) every non-zero ideal of A is of the form P^n for some $n \geq 0$
(6) there exists a non-zero x in A such that every non-zero ideal of A is of the form (x^m) for some $m \geq 0$.

Remark 34.1 (Why DVRs are useful). To see why DVRs are useful, we need to consider the general strategy in commutative algebra.

(1) Input: Some Noetherian integral domain R and some problem
(2) Step 1: Show that you can reduce to the case where R is integrally closed by considering its integral closure.
(3) Step 2: For each prime P of height 1 in R, we have $R \hookrightarrow R_P$, which is a DVR (Noetherian and has Krull dimension 1).

Example 34.2. Let p be a prime. Then consider $X = \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \cdots$. Note that $\mathbb{Z}_p \subseteq X$, and that $\mathbb{Z}/p^i\mathbb{Z}$ can be given the discrete, compact topology. So X is a compact topological space and one can show that $\mathbb{Z}_p \subseteq X$ is a closed subset of X. Thus $\mathbb{Z}_p$ is a compact topological space under the subspace topology – and it is also a ring., with the usual multiplication and addition. Clearly $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ with injection given by $n \mapsto ([n]_p, [n]_p^2, \dots)$. Also the image of this injection is dense. Thus $\mathbb{Z}_p$ is a DVR with the maximal ideal $p\mathbb{Z}_p$.

Now let's move to the proof of Theorem 34.1.

Proof. ((1) $\Rightarrow$ (2)) We just did it today.

((2) $\Rightarrow$ (3)) Pick $x \in P \setminus P^2$. Why can we do this? By Nakayama's lemma if $P = P^2$ then $P = J(A)P = P^2$, so $P = (0)$ since P is finitely-generated. Now $\sqrt{(x)} = P$, so there exists $m \geq 1$ such that $P^m \subseteq (x)$. Pick the smallest n so that $P^n \subseteq (x)$. If $n = 1$ then we are done, since $P = (x)$. So let $n > 1$, without loss of generality so that $P^{n-1} \subsetneq (x)$. Pick $b \in P^{n-1} \setminus (x)$. Let $y = b/x$. Then $y \notin A$. Otherwise, we would have $b = yx \in (x)$, a contradiction. On the other hand, $Py = (Pb)/x$ because since $b \in P^{n-1}$, we have $Pb/x \subseteq P^n x^{-1} \subseteq A$ recall that $P^n \subseteq (x)$. Thus $Py \subseteq A$ so Py is an ideal of A. Thus, either $Py \subseteq P$ or $Py = A$. If $Py = A$, then $Pb/x = A$ so $Pb = Ax$. But since $n > 1$, $b \in P^{n-1} \subseteq P$. Thus $Ax \subseteq P \cdot P = P^2$. But this contradicts the fact that $a \in P \setminus P^2$. If $Py = P$, then $P \subseteq A$ is a finitely-generated A-module with A an integral and $Py \subseteq P$. So y is integral over A. But since A is integrally closed, $y \in A$. This is a contradiction! Therefore $n = 1$ and $P = (x)$.

((3) $\Rightarrow$ (4)) Suppose that $P = (x), x \neq 0$. We need to show that $\dim_k P/P^2 = 1$. Write $P = Ax$. So $P/P^2 = Ax/P^2$. Now if $a \in A$ then $ax + P^2 = \bar{a}(x + P^2)$, with $\bar{a} \in k = A/P$. So $P/P^2 = k(x + P^2)$. The claim follows.

((4) $\Rightarrow$ (5)) We observe that we can get ((4) $\Rightarrow$ (3)) by applying Nakayama's lemma. Notice that P/P^2 is one-dimensional over k, so there exists $x \in P \setminus P^2$ such that $x + P^2$ generates P/P^2 as an A/P-module. Therefore P/P^2 is a finitely-generated A/P-module. We claim

that $P = (x)$. Why? Suppose $M = P/(x)$. Then $PM = (P^2 + (x))/(x) = P/(x) = M$. Recall that $P = J(A)$, so by Nakayama's lemma we have $P/(x) = M = (0)$. Therefore $P = (x)$. Now let $I \neq (0)$ be an ideal of A. Again, let $\sqrt{I} = P$ so that there exists n such that $P^n \subseteq I$. In particular, there exists some largest natural number m such that $I \subseteq P^m$. Otherwise, we would have $I \subseteq P^n$ and $P^n \subseteq I$, meaning $I = P^n$ and we will be done.

So we have $I \not\subseteq P^{m+1} = (x^{m+1})$. Pick $y \in I \setminus (x^{m+1})$. But then $y \in (x^m)$ so $y = ax^m$, where $a \notin (x) = P$. So $a \in A \setminus P$. Therefore a is a unit so $(y) = (x^m) \subseteq I \subseteq P^m = (x^m)$ so in fact $P^m = I$.

((5) $\Rightarrow$ (6)) Pick $x \in P \setminus P^2$. Now $(x) = P^m$ for some $m \geq 0$. Notice that $1 \leq m < 2$, since $x \in P \setminus P^2$. Hence $m = 1$ so $P = (x)$. Thus $P^n = (x^n)$ for all $n \geq 0$, as required.

((6) $\Rightarrow$ (1)) Define a map $\nu : A \setminus \{0\} \to \mathbb{N}_{\geq 0}$ by $\nu(a) = m$, where $m \geq 0$ is the unique non-negative integer such that $a \in P^m \setminus P^{m+1}$. But here is one question we need to address before proceeding: why can't $0 \neq a$ be in (x^m) for all $m \geq 0$? You will see why in Assignment #4. For this reason, ν is well-defined.

We extend $\nu : K \to \mathbb{Z} \cup \{\infty\}$ by $\nu(a/b) = \nu(a) - \nu(b)$ for $a, b \in A$ with $b \neq 0$ (as in the example with $\mathbb{Q}_p$) and $\nu(0) = \infty$. Then we claim that ν is a valuation and that A is the valuation ring of ν.

Since A is local, we have $P = (x)$. If $a \in A \setminus \{0\}$, then $(a) = (x^m)$ so $a = ux^m$ for some unit u (i.e., $\nu(u) = 0$). Similarly, if $a, b \in A \setminus \{0\}$ then $a = ux^m$ and $b = u'x^n$ where u, u' units. Thus $a/b = u(u')^{-1}x^{m-n}$, so $\nu(a/b) = m - n$.

Notice that $\nu(a/b) \geq 0 \Leftrightarrow m - n \geq 0 \Leftrightarrow a/b = u(u')^{-1}x^d$ with $d = m - n \geq 0$. Hence $a/b \in A$. So $A = \{a/b \in K^* : \nu(a/b) \geq 0\} \cup \{0\}$. Now we should check that ν is a valuation. Indeed, if $\alpha = u_1x^{d_1}, \beta = u_2x^{d_2}$ with $u_1, u_2 \in A^*$ and $d_1, d_2 \in \mathbb{Z}$, then $\nu(\alpha\beta) = d_1+d_2 = \nu(\alpha)+\nu(\beta)$. Also, note that $\alpha+\beta = u_1x^{d_1}+u_2x^{d_2} = x^{d_1}(u_1+u_2x^{d_2-d_1}) \in A$. If $d_1 \leq d_2$, then $\nu(\alpha + \beta) = d_1 + \nu(u_1 + u_2x^{d_2-d_1}) \geq d_1$. Similarly, $\nu(\alpha + \beta) \geq d_2$ if $d_2 \leq d_1$. So ν is indeed a valuation, as desired. $\square$

35. March 31: Dedekind domains

Definition 35.1. A *Dedekind domain* is a Noetherian integral domain A that is integrally closed (in $\mathrm{Frac}(A)$) and has $\mathrm{Kdim}(A) = 1$.

Remark 35.1. If P is a maximal ideal of A, then A_P is a DVR.

Example 35.2. $\mathbb{Z}, k[t]$ (k field) are Dedekind domains. If $[K : \mathbb{Q}] < \infty$ then $\mathcal{O}_K$, the integral closure of $\mathbb{Z}$ in K, is a Dedekind domain.

Theorem 35.3. *In a Dedekind domain R, every non-zero ideal I has a factorization into prime ideals*

$$I = P_1^{m_1} \cdots P_r^{m_r}.$$

Moreover, this factorization is unique up to permutation of factors.

Historically speaking, Dedekind domains arose in number theory with FLT. It used to be thought that by some that $\mathbb{Z}[e^{2\pi i/n}]$ is a UFD – until Kummer pointed out that this is wrong.

Remark 35.2 (Strategy for proving Theorem 35.3). Our strategy is as follows:

(1) Use primary decomposition: $I = Q_1 \cap \cdot \cap Q_s$, with Q_i primary
(2) Show that in a Dedekind domain, $(0) \neq Q$ primary implies that $Q = P^m$ where P is maximal and $m \geq 1$.

(3) Use (1) and (2) to show that $I = P_1^{m_1} \cap \cdots \cap P_s^{m_s}$ with each P_i distinct
(4) Show that $P_1^{m_1} \cap \cdots \cap P_s^{m_s} = P_1^{m_1} \cdots P_s^{m_s} = I$.
(5) Use local rings to prove uniqueness.

Note that Step 4 follows from the following fact: if $I_1, \ldots, I_s$ are pairwise comaximal ideals of R, then $I_1 \cap I_2 \cap \cdots \cap I_s = I_1 I_2 \cdots I_s$. The inclusion $I_1 I_2 \cdots I_s \subseteq I_1 \cap \cdots \cap I_s$ is immediate. Fro the reverse inclusion, let's consider the $s = 2$ case for insight. If $I_1 + I_2 = R$, then there exist $a \in I_1, b \in I_2$ such that $a + b = 1$. If $x \in I_1 \cap I_2$, then $x = x \cdot 1 = x \cdot a + x \cdot b \in I_1 I_2$. In general, if $I_1, \ldots, I_s$ are pairwise comaximal, then I_i and $\bigcap_{j \neq i} I_j$ are comaximal.

Without loss of generality, consider I_1 and $I_2 \cap I_3 \cap \cdots \cap I_s$. We know for each j, there exist $a_j \in I_1$ and $b_j \in I_j$ such that $a_j + b_j = 1$. Thus I_1 and $I_2 \cdots I_s$ are comaximal. So $1 = (a_2 + b_2)(a_3 + b_3) \cdots (a_s + b_s) = x + b_2 b_3 \cdots b_s \in I_2 \cap \cdots I_s$. For each j there exist $c_j \in I_j$ and $d \in \prod_{k \neq j} I_k$ such that $c_j + d_j = 1$. Therefore if $x \in I_1 \cap \cdots \cap I_s$ then $x = x \cdot 1 = x(c_1 + d_1) \cdots (c_s + d_s) \in I_1 I_2 \cdots I_s$, so $I_1 \cap \cdots \cap I_s = I_1 I_2 \cdots I_s$, as required.

Proposition 35.4. *Let A be a Noetherian integral domain of Krull dimension 1. Then the following are equivalent:*

(1) A is integrally closed (equivalently, A is a Dedekind domain)
(2) Every primary ideal in A is of the form P^m where $m \geq 1$ and P is prime
(3) If P is a prime ideal of A, then A_P is a DVR.

Proof. ((1) $\Rightarrow$ (3)) Suppose A is integrally closed. If P is a prime ideal of A then A_P is also integrally closed. Let's see why this must be the case. In fact, a more general fact holds: if R is integrally closed in $K = \mathrm{Frac}(R)$ and is S is multiplicatively closed, then $S^{-1}R$ is integrally closed in K. We will prove this more general fact instead. Suppose that $x \in K$ is integral over $S^{-1}R$. So there exists a monic polynomial $x^n + (r_{n-1}s_{n-1}^{-1})x^{n-1} + \cdots + r_0 s_0^{-1} = 0$. Write $s = s_{n-1}s_{n-2} \cdots s_1 s_0$. Then there exist $r_0', \cdots, r_{n-1}' \in R$ so that $x^n + (r_{n-1}' s^{-1})x^{n-1} + \cdots + (r_1' s^{-1})x + r_0' s^{-1} = 0$. Multiply by s^n to get

$$(sx)^n + r_{n-1}'(sx)^{n-1} + (r_{n-2}' s)(sx)^{n-2} + \cdots + (r_1' s^{n-2})(sx) + r_0' s^{n-1} = 0.$$

Therefore, sx is integral over R. Since R is integrally closed, $sx \in R$. Therefore $x \in S^{-1}R$, so $S^{-1}R$ is indeed integrally closed.

From this we see that A_P is also integrally closed. So A_P is a local Noetherian ring with Krull dimension one, so A_P is a DVR.

((3) $\Rightarrow$ (1)) Suppose that $P \in \mathrm{Spec}(A)$ and A_P is a DVR. Assume that $C \subseteq K = \mathrm{Frac}(A)$ is the integral closure of A. So $A \subseteq C \subseteq K$. Our goal is to show that $A = C$. Let $f : A \to C$ be the inclusion map. We will show that f is surjective. Suppose that there exists $c \in C \setminus A$, and let P be the maximal ideal of A. Then $A_P \subseteq S^{-1}C$ where $S = A \setminus P \subseteq C$. Now A_P is integrally closed and observe that $S^{-1}C$ is integral over A_P.

Suppose $s^{-1}c \in S^{-1}C$. If $c^n + a_{n-1}c^{n-1} + \cdots + a_0 = 0$, then multiplying by s^{-n} we see that $s^{-n}c^n + a_{n-1}s^{-n}c^{n-1} + \cdots + a_0 s^{-n} = 0$. So we have $(s^{-1}c)^n + a_{n-1}s^{-1}(s^{-1}c)^{n-1} + \cdots + a_0 s^{-n} = 0$, so $s^{-1}c$ is indeed integral over A_P.

Since A_P is integrally closed and $S^{-1}C$ is integral over A_P, we see that $A_P = S^{-1}C \ni c$ for all P. So if $c \in C \setminus A$ then $c \in S^{-1}C$ so $c = ax^{-1}$where $x \in A \setminus P$. So for each maximal ideal P, there is $a_p \in A$ and $x_p \in A \setminus P$ such that $c = a_p x_p^{-1}$, i.e., $x_p c = a_p \in A$. Let $J = \{r \in A : rc \in A\}$. Then J is an ideal of A. Notice that if $J \neq A$ then $J \subseteq P$ for some

maximal ideal P. But then $x_p \in J$ and $x_p \notin P$ so $J = A$. Hence $1 \in J$ so $c \in A$. This is a contradiction! $\square$

36. April 2

Theorem 36.1. *Let A be a Noetherian integral domain with Krull dimension 1. Then the following are equivalent:*

(1) A is integrally closed
(2) Every primary ideal is a prime power.
(3) Every local ring A_P with $P \neq (0)$ prime ideal, is a DVR.

Proof. We showed (1) $\Leftrightarrow$ (3) last class. Let's show (2) $\Leftrightarrow$ (1,3).

Suppose that (2) holds. Let P be a non-zero prime ideal (so P is maximal). Consider the local ring A_P. We will show that A_P is a DVR. Let J be a non-zero ideal of A_P. Then there is a correspondence (by the correspondence theorem) $J \leftrightarrow (J \cap A)A_P$. What is the radical of J an ideal of A_P? Note that we can let $\sqrt{J} = PA_P$. Since A_P is Noetherian there exists n such that $(PA_P)^n \subseteq J$. Letting $I = J \cap A$, we see that $P^n \subseteq I$. Then $\sqrt{I} = P$ since P is maximal. Recall that if $\sqrt{I}$ is maximal then I is primary. Therefore there is m such that $P^m = I$. But then $J = IA_P = P^m A_P = (PA_P)^m$, so A_P is a DVR (by Theorem 34.1(6)).

Conversely, suppose that (1) holds. Let I be a primary ideal and $P = \sqrt{I}$ (P maximal). Since A_P is a DVR, $IA_P = (PA_P)^m = P_m A_P$ for some $m \geq 1$. We are done once we show that $P^m = I$. We know that we have a bijection between the proper ideals of A_P and S-saturated (i.e., if J is an ideal and $xs \in S$ with $s \in S$ then $x \in J$) ideals of A contained in P, where $S = A \setminus P$. The bijection is $J \leftrightarrow J \cap A$ (where J is an ideal of A_P and $J \cap A$ an ideal of A).

Since $IA_P = P^m A_P$, we have $IA_P \cap A = P^m A_P \cap A$. We claim that $IA_P \cap A = I$ and $P^m A_P \cap A = P^m$, hence $P^m = I$. We will show that I and P^m are S-saturated. Suppose that $rs \in I$. Since I is primary, either $x \in I$ or $s^n \in I$, but we know that $s^n \notin I$ since $s^n \notin P$ to begin with (thus $s \notin P$ since P is a prime ideal). So I is S-saturated. Similarly, P^m is also S-saturated. Thus by the bijection we see that $IA_P = P^m A_P \Rightarrow I = P^m$, as required. $\square$

Now we are ready to prove Theorem 35.3.

Proof of Theorem 35.3. Let I be a proper non-zero ideal of A. Then I has a primary decomposition $I = Q_1 \cap \cdots \cap Q_s$. By our last theorem, A is a Dedekind domain, so Theorem 36.1(1), we have that every primary ideal is a prime power. It implies that there exist $P_1, \ldots, P_s$ prime (maximal) ideals such that $Q_i = P_i^{m_i}$. Now write $I = P_1^{m_1} \cap \cdots \cap P_s^{m_s}$. Without loss of generality, we can let $P_1, \ldots, P_s$ be pairwise distinct, with s taken to be minimal with respect to this property. Then $P_1^{m_1}, \cdots P_s^{m_s}$ are pairwise comaximal (as to why we can do this, see Remark 36.1). Then we have $P_1^{m_1} \cap P_2^{m_2} \cap \cdots \cap P_s^{m_s} = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s} = I$. So we have at least one factorization into prime ideals. To see uniqueness, suppose that $I = P_1^{m_1} \cdots P_s^{m_s} = Q_1^{n_1} \cdots Q_t^{n_t}$, where $P_1, \ldots, P_s$ are pairwise distinct and $Q_1, \ldots, Q_t$ are pairwise distinct (and $m_i, n_i \geq 1$).

Claim. $\{P_1, \ldots, P_s\} = \{Q_1, \ldots, Q_t\}$.

To see why, if $Q_j \notin \{P_1, \ldots, P_s\}$ then $P_1^{m_1} \cdots P_s^{m_s} = Q_1^{n_1} \cdots Q_t^{n_t} \subseteq Q_j$. So $P_1^{m_1} \cdots P_s^{m_s} \in Q_j$. If no $P_i \subseteq A_j$, then for each i there exists $a_i \in P_i \setminus Q_j$ such that $a_1^{m_1} a_2^{m_2} \cdots a_s^{m_s} \in$

$P_1^{m_1} \cdots P_s^{m_s} \subseteq Q_j$. But this is a contradiction so there exists i such that $P_i \subseteq Q_j$. But since P_i is maximal, indeed $P_i = Q_j$. This proves $\{Q_1, \ldots, Q_t\} \subseteq \{P_1, \ldots, P_s\}$ and by symmetry the reverse inclusion follows.

So now we can consider $I = P_1^{m_1} \cdots P_s^{m_s} = P_1^{n_1} \cdots P_s^{n_s}$ with $m_i, n_j \geq 1$. Now it suffices to who what $m_i = n_i$ for all i. Let's look at this in the local ring A_{P_i}:

$$IA_{P_i} = (P_1^{m_1} \cdots P_s^{m_s})A_{P_i} = (P_1^{n_1} \cdots P_s^{n_s})A_{P_i}$$
$$(P_1^{m_1} \cdots P_s^{m_s})A_P = \prod_{i=1}^{s} (P_i A_{P_i})^{m_i} = (P_i A_{P_i})^{m_i}$$
$$(P_1^{n_1} \cdots P_s^{n_s})A_{P_i} = (P_1 A_{P_1})^{n_1} \cdots (P_i A_{P_i})^{n_i} \cdots (P_s A_{P_s})^{n_s} = (P_i A_{P_i})^{n_i}.$$

Note that, if J an ideal of A and $\emptyset \neq J \cap S \ni s$ then $S^{-1}J$ is an ideal of $S^{-1}A$. Then $s \in A$ so $1 = ss^{-1} \in S^{-1}A$. Thus if P and Q are distinct maximal ideals then $PA_Q = A_Q$. Therefore we have $(P_i A_{P_i})^{m_i} = (P_i A_{P_i})^{n_i}$. We just need to show that $m_i = n_i$. If not, assume $m_i < n_i$ without loss of generality. Then we would have that $(P_i A_{P_i})^{m_i} = (P_i A_{P_i})^{m_i+1} = \cdots = (P_i A_{P_i})^{n_i}$. But by Nakayama's lemma, $(P_i A_{P_i})^{n_i} = (0)$, which is a contradiction since $P_i \neq (0)$ and A an integral domain. So $m_i \geq n_i$; similarly, by symmetry we can show that $m_i \leq n_i$. Therefore $m_i = n_i$ as desired. □

Remark 36.1. Take s to be minimal. If some $P_i = P_j$ then take $P_i^{m_i} \cap P_j^{m_j} = P_i^{\max(m_i, m_j)}$. So we would get a shorter expression. Now $P_1^{m_1}, \ldots, P_s^{m_s}$ are pairwise comaximal. To show this, we will prove the following general claim: if P and Q are comaximal then P^n and Q^m are comaximal. If P and Q are comaximal, then there exist $x \in P, y \in Q$ such that $x + y = 1$ hence $P + Q = A$. Now $(x+y)^{m+n} = 1$, and

$$(x+y)^{m+n} = \underbrace{x^{m+n} + \binom{m+n}{1} x^{m+n-1}y + \cdots + \binom{m+n}{m} x^n y^m}_{\in P^n}$$
$$+ \underbrace{\binom{m+n}{m+1} x^{n-1}y^{m+1} + \cdots + \binom{m+n}{m+n} y^{m+n}}_{\in Q^m} = 1,$$

so $P^n + Q^m = A$.

This is the official end of the course materials for commutative algebra!

37. April 6

Theorem 37.1. *Let A be an integral domain and suppose that every non-zero ideal factors into prime ideals. Then A is a Dedekind domain.*

Proof. We will prove a special case of this theorem, namely when A is Noetherian.

Suppose that $(0) \subsetneq Q \subsetneq P$, where $Q, P \in \operatorname{Spec}(A)$. Then notice that A_P has the same factorization property as A. So in particular, the ideal $QA_P + (PA_P)^2$ must factor into prime ideals, say $QA_P + (PA_P)^2 = L_1 \cdots L_s$ where $s \geq 1$ and $L_i \in \operatorname{Spec}(A_P)$. Notice that $s \leq 1$ also, since otherwise each $L_i \in PA_P$, which would mean that $L_1 \cdots L_s \subseteq (PA_P)^s \subseteq (PA_P)^2$. One can show that $Q \not\subseteq P^2$ (exercise!). So this gives us a contradiction, because $QA_P + (PA_P)^2 \supsetneq (PA_P)^2$. Therefore $s = 1$, so $QA_P + (PA_P)^2 = L$, where L is prime.

Also, if $x \in PA_P$ then $x^2 \in (PA_P)^2 \subseteq L$. Because L is prime, it follows that $x \in L$. So $L \supseteq PA_P$ so $L = PA_P$ since PA_P is the maximal ideal of A_P. Now $QA_P + (PA_P)^2 = PA_P$, so if $M = PA_P/QA_P$, then $(PA_P)M = ((PA_P)^2 + QA_P)/QA_P = PA_P/QA_P = M$. Therefore, by Nakayama's lemma, $M = (0)$. Thus $PA_P = QA_P$, hence $P = Q$, a contradiction. Therefore A has $\operatorname{Kdim}(A) = 1$.

To see that A is integrally closed, let $x \in P \setminus P^2$ with $P \in \operatorname{Spec}(A)$ and $P \neq (0)$. Let $J = Ax + P^2$. Then arguing as before, we see $J = P$. So $Ax + P^2$, hence $M = P/Ax$ and $PM = M$. So by Nakayama, $M = (0)$. Hence $P = Ax$, so A is integrally closed by Theorem 34.1. □

One important skills to have as a mathematician is knowing lots of examples. Also, it is important to think of analogies to get an insight on an unknown but seemingly similar setting. What is equally important is to ask questions about weakening hypotheses, generalizing, and study converses.

Question. Give an example of examples of integral domain(s) such that:

(1) is Noetherian and integrally closed but does not have Krull dimension 1.
(2) is Noetherian and has Krull dimension 1 but not integrally closed.
(3) has Krull dimension 1 and is integrally closed but is not Noetherian.

Solution: For the first part, note that $\mathbb{C}$ and $\mathbb{C}[x, y]$ are the examples. For the second part, note that the integral closure of $\mathbb{C}[t]$ is the integral closure of $\mathbb{C}[t^2, t^3]$. The third part is slightly harder, but here is an example: $R := \mathbb{C}[x, \sqrt{x}, \sqrt[4]{x}, \dots]$. This is not Noetherian since $(x) \subsetneq (\sqrt{x}) \subsetneq \cdots$ is an strictly increasing chain of ideals. Note that R has Krull dimension 1 since R is integral over $\mathbb{C}[x]$ and $\mathbb{C}[x]$ has Krull dimension 1. Finally, to see that R is integrally closed, write $K := \operatorname{Frac}(R)$. If $\theta \in K$, then $\theta = p\sqrt[2^m]{x}/q\sqrt[2^n]{x}$ for some $n \geq 1$ with $p, q \in \mathbb{C}[t]$. If θ is integral over S, then there exists a monic polynomial such that

$$\theta^m + c_{m-1}(\sqrt[2^L]{x})\theta^{m-1} + \cdots + c_0(\sqrt[2^L]{x}) = 0$$

for some $L \geq 1$. Let $N = \max(L, n)$. Then $\theta \in \mathbb{C}(\sqrt[2^N]{x})$ and is integral over $\mathbb{C}[\sqrt[2^N]{x}] \cong \mathbb{C}[t]$, and $\mathbb{C}[t]$ is an UFD hence integrally closed. So $\theta \in \mathbb{C}[\sqrt[2^N]{x}] \subseteq S$.

Theorem 37.2 ("Fermat's last theorem")**.** *Let $a(t), b(t), c(t) \in \mathbb{C}[t]$, relatively prime and non-constant. Let $n > 2$. Then $a(x)^n + b(x)^n \neq c(x)^n$.*

Proof. First, we can assume that $\deg(a(x)) \geq \max(\deg b(x), \deg c(x))$. Also, we can assume that $\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1$. Suppose that

$$a(x)^n + b(x)^n = c(x)^n. \tag{$*$}$$

Differentiate both sides to get

$$na(x)^{n-1}a'(x) + nb(x)^{n-1}b'(x) = nc(x)^{n-1}c'(x). \tag{$\dagger$}$$

Then $nc'(x) \times (*) - c(x) \times (\dagger)$ gives us $a(x)^{n-1}[nc'(x)a(x) - na'(x)c(x)] + b(x)^{n-1}[nb(x)c'(x) - nb'(x)c(x)] = 0$.

Divide both sides by n to get

$$a(x)^{n-1}[c'(x)a(x) - a'(x)c(x)] = -b(x)^{n-1}[b(x)c'(x) - b'(x)c(x)].$$

But since $\gcd(a,b)=1$, indeed $a(x)^{n-1} \mid b(x)c'(x)-c(x)b'(x)$. Now $\deg(b(x)c'(x)-c(x)b'(x)) \leq \deg b(x)+\deg c(x)-1 \leq 2\deg a(x) \leq (n-1)\deg a(x)$ since $n \geq 3$. So $bc'-cb'=0$ hence

$$\frac{d}{dx}\left(\frac{b}{c}\right)=0.$$

So $b(x)=\lambda c(x)$ for some $\lambda \in \mathbb{C}$. But this means $b(x), c(x) \in \mathbb{C}$ but this is a contradiction as $\gcd(b,c)=1$. □

Department of Pure Mathematics, University of Waterloo, 200 University Avenue West, Waterloo, ON, Canada N2L 3G1

E-mail address: hsyang@uwaterloo.ca