Lecture 1

§1 Three theorems of McCoy

R is always a commutative ring with unity 1_R. $U(R)$ is the group of units of R. $\mathcal{C}(R)$ is the set of *regular* elements of R, i.e. the set of non-zero-divisors. $\mathcal{Z}(R)$ is the set of zero-divisors, the complement of $\mathcal{C}(R)$. $(\{a_i\}) = (a_1, a_1, \dots)$ is the ideal generated by the set $\{a_i\}$; this is also written $\sum a_i R$. The principle ideal (a) is $aR = Ra$. The notation $I \triangleleft R$ means that I is an ideal in R.

Theorem 1.1. *Let $A = R[x]$. Let $f = a_n x^n + \cdots + a_0 \in A$. If there is a non-zero polynomial $g \in A$ such that $fg = 0$, then there exists $r \in R \setminus \{0\}$ such that $f \cdot r = 0$.*

Proof. Choose g to be of minimal degree, with leading coefficient bx^d. We may assume that $d > 0$. Then $f \cdot b \neq 0$, lest we contradict minimality of g. We must have $a_i g \neq 0$ for some i. To see this, assume that $a_i \cdot g = 0$, then $a_i b = 0$ for all i and then $fb = 0$. Now pick j to be the largest integer such that $a_j g \neq 0$. Then $0 = fg = (a_0 + a_1 x + \cdots a_j x^j)g$, and looking at the leading coefficient, we get $a_j b = 0$. So $\deg(a_j g) < d$. But then $f \cdot (a_j g) = 0$, contradicting minimality of g. □

Theorem 1.2 (Prime Avoidance)**.** *Let $I_1, \dots, I_n \triangleleft R$. Let $A \subset R$ be a subset which is closed under addition and multiplication. Assume that at least $n-2$ of the ideals are prime. If $A \subseteq I_1 \cup \cdots \cup I_n$, then $A \subseteq I_j$ for some j.*

Proof. Induct on n. If $n = 1$, the result is trivial. The case $n = 2$ is an easy argument: if $a_1 \in A \setminus I_1$ and $a_2 \in A \setminus I_2$, then $a_1 + a_2 \in A \setminus (I_1 \cup I_2)$.

Now assume $n \geq 3$. We may assume that for each j, $A \not\subseteq I_1 \cup \cdots \cup \hat{I}_j \cup \cdots I_n$.[1] Fix an element $a_j \in A \setminus (I_1 \cup \cdots \cup \hat{I}_j \cup \cdots I_n)$. Then this a_j must be contained in I_j since $A \subseteq \bigcup I_j$. Since $n \geq 3$, one of the I_j must be prime. We may assume that I_1 is prime. Define $x = a_1 + a_2 a_3 \cdots a_n$, which is an element of A. Let's show that x avoids *all* of the I_j. If $x \in I_1$, then $a_2 a_3 \cdots a_n \in I_1$, which contradicts the fact that $a_i \notin I_j$ for $i \neq j$ and that I_1 is prime. If $x \in I_j$ for $j \geq 2$. Then $a_1 \in I_j$, which contradicts $a_i \notin I_j$ for $i \neq j$. □

Definition 1.3. An ideal $I \triangleleft R$ is called *dense* if $rI = 0$ implies $r = 0$. This is denoted $I \subseteq_d R$. This is the same as saying that ${}_R I$ is a faithful module over R.

If I is a principal ideal, say Rb, then I is dense exactly when $b \in \mathcal{C}(R)$. The easiest case is when R is a domain, in which case an ideal is dense exactly when it is non-zero.

If R is an integral domain, then by working over the quotient field, one can define the rank of a matrix with entries in R. But if R is not a domain, rank becomes tricky. Let $\mathcal{D}_i(A)$ be the i-th *determinantal ideal* in R, generated by all the determinants of $i \times i$ minors of A. We define $\mathcal{D}_0(A) = R$. If $i \geq \min\{n, m\}$, define $\mathcal{D}_i(A) = (0)$.

[1] The hat means omit I_j.

Note that $\mathcal{D}_{i+1}(A) \supseteq \mathcal{D}_i(A)$ because you can expand by minors, so we have a chain

$$R = \mathcal{D}_0(A) \supseteq \mathcal{D}_1(A) \supseteq \cdots \supseteq (0).$$

Definition 1.4. Over a non-zero ring R, the *McCoy rank* (or just *rank*) of A to be the maximum i such that $\mathcal{D}_i(A)$ is dense in R. The rank of A is denoted $rk(A)$.

If R is an integral domain, then $rk(A)$ is just the usual rank. Note that over any ring, $rk(A) \leq \min\{n, m\}$.

If $rk(A) = 0$, then $\mathcal{D}_1(A)$ fails to be dense, so there is some non-zero element r such that $rA = 0$. That is, r zero-divides all of the entries of A.

If $A \in \mathbb{M}_{n,n}(R)$, then A has rank n (full rank) if and only if $\det A$ is a regular element.

► **Exercise 1.1.** Let $R = \mathbb{Z}/6\mathbb{Z}$, and let $A = diag(0,2,4)$, $diag(1,2,4)$, $diag(1,2,3)$, $diag(1,5,5)$ (3×3 matrices). Compute the rank of A in each case.

Solution .

A	$\mathcal{D}_1(A)$	$\mathcal{D}_2(A)$	$\mathcal{D}_3(A)$	
$diag(0,2,4)$	(2)	(2)	(0)	$3 \cdot (2) = 0$, so $rk = 0$
$diag(1,2,4)$	R	(2)	(2)	$3 \cdot (2) = 0$, so $rk = 1$
$diag(1,2,3)$	R	R	(2)	$3 \cdot (2) = 0$, so $rk = 2$
$diag(1,5,5)$	R	R	R	so $rk = 3$

■

Lecture 2

Let $A \in \mathbb{M}_{n,m}(R)$. If R is a field, the rank of A is the dimension of the image of $A : R^m \to R^n$, and $m - rk(A)$ is the dimension of the null space. That is, whenever $rk(A) < m$, there is a solution to the system of linear equations

$$0 = A \cdot x \tag{2.1}$$

which says that the columns $\alpha_i \in R^n$ of A satisfy the dependence $\sum x_i \alpha_i = 0$. The following theorem of McCoy generalizes this so that R can be any non-zero commutative ring.

Theorem 2.2 (McCoy)**.** *If R is not the zero ring, the following are equivalent:*

1. *The columns $\alpha_1, \ldots, \alpha_m$ are linearly dependent.*
2. *Equation 2.1 has a nontrivial solution.*
3. *$rk(A) < m$.*

Corollary 2.3. *If $R \neq 0$, the following hold*

(a) If $n < m$ (i.e. if there are "more variables than equations"), then Equation 2.1 has a nontrivial solution.

(b) R has the "strong rank property": $R^m \hookrightarrow R^n \implies m \leq n$.

(c) R has the "rank property": $R^n \twoheadrightarrow R^m \implies m \leq n$.

(d) R has the "invariant basis property": $R^m \cong R^n \implies m = n$.

Proof of Corollary. (a) If $n < m$, then $rk(A) \leq \min\{n, m\} = n < m$, so by Theorem 2.2, Equation 2.1 has a non-trivial solution.

$(a \Rightarrow b)$ If $m > n$, then by (a), any R-linear map $R^m \to R^n$ has a kernel. Thus, $R^m \hookrightarrow R^n$ implies $m \leq n$.

$(b \Rightarrow c)$ If $R^n \twoheadrightarrow R^m$, then since R^m is free, there is a section $R^m \hookrightarrow R^n$ (which must be injective), so $m \leq n$.

$(c \Rightarrow d)$ If $R^m \cong R^n$, then we have surjections both ways, so $m \leq n \leq m$, so $m = n$. □

Corollary 2.4. *Let $R \neq 0$, and A some $n \times n$ matrix. Then the following are equivalent (1) $\det A \in \mathcal{C}(R)$; (2) the columns of A are linearly independent; (3) the rows of A are linearly independent.*

Proof. The columns are linearly independent if and only if Equation 2.1 has no non-trivial solutions, which occurs if and only if the rank of A is equal to n, which occurs if and only if $\det A$ is a non-zero-divisor.

The transpose argument shows that $\det A \in \mathcal{C}(R)$ if and only if the rows are independent. □

Proof of the Theorem. $0 = Ax = \sum \alpha_i x_i$ if and only if the α_i are dependent, so (1) and (2) are equivalent.

(2 $\Rightarrow$ 3) Let $x \in R^m$ be a non-zero solution to $A \cdot x = 0$. If $n < m$, then $rk(A) \leq n < m$ and we're done. Otherwise, let B be any $m \times m$ minor of A (so B has as many columns as A, but perhaps is missing some rows). Then $Bx = 0$; multiplying by the adjoint of B, we get $(\det B)x = 0$, so each x_i annihilates $\det B$. Since $x \neq 0$, some x_i is non-zero, and we have shown that $x_i \cdot \mathcal{D}_m(A) = 0$, so $rk(A) < m$.

(3 $\Rightarrow$ 2) Assume $r = rk(A) < m$. We may assume $r < n$ (adding a row of zeros to A if needed). Fix a nonzero element a such that $a \cdot \mathcal{D}_{r+1}(A) = 0$. If $r = 0$, then take x to be the vector with an a in each place. Otherwise, there is some $r \times r$ minor not annihilated by a. We may assume it is the upper left $r \times r$ minor. Let B be the upper left $(r+1) \times (r+1)$ minor, and let $d_1, \ldots, d_{r+1}$ be the cofactors along the $(r+1)$-th row. We claim that the column vector $x = (ad_1, \ldots, ad_{r+1}, 0, \ldots, 0)$ is a solution to Equation 2.1 (note that it is non-zero because $ad_{r+1} \neq 0$ by assumption). To check this, consider the product of x with the i-th row, $(a_{i1}, \ldots, a_{im})$. This will be equal to a times the determinant of B', the matrix B with the $(r+1)$-th row replaced by the i-th row of A. If $i \leq r$, the determinant of B' is zero because it has two repeated rows. If $i > r$, then B' is an $(r+1) \times (r+1)$ minor of A, so its determinant is annihilated by a. □

Corollary 2.5. *Suppose a module ${}_RM$ over a non-zero ring R is generated by $\beta_1, \ldots, \beta_n \in M$. If M contains n linearly independent vectors, $\gamma_1, \ldots, \gamma_n$, then the β_i form a free basis.*

Proof. Since the β_i generate, we have $\gamma = \beta \cdot A$ for some $n \times n$ matrix A. If $Ax = 0$ for some non-zero x, then $\gamma \cdot x = \beta Ax = 0$, contradicting independence of the γ_i. By Theorem 2.2, $rk(A) = n$, so $d = \det(A)$ is a regular element.

Over $R[d^{-1}]$, there is an inverse B to A. If $\beta \cdot y = 0$ for some $y \in R^n$, then $\gamma By = \beta y = 0$. But the γ_i remain independent over $R[d^{-1}]$ since we can clear the denominators of any linear dependence to get a dependence over R (this is where we use that $d \in \mathcal{C}(R)$), so $By = 0$. But then $y = A \cdot 0 = 0$. Therefore, the β_i are linearly independent, so they are a free basis for M. □

Lecture 3

§2. The Nilradical and Jacobson radical

The three spectra of a commutative ring R are denoted $\operatorname{Spec}(R) = \{\mathfrak{p} \lhd R \text{ prime}\}$, $\operatorname{Max}(R) = \{\mathfrak{m} \lhd R \text{ maximal}\}$, and $\operatorname{Min}(R) = \{\mathfrak{p} \lhd R \text{ minimal prime}\}$. $\mathfrak{p}$ will always be a prime ideal.

The *nilradical* of R is $\operatorname{Nil} R = \{r \in R | r^n = 0 \text{ for some } n \gg 0\}$. This is an ideal in R (since R is commutative). This is a special case of the "radical formation". If $I \lhd R$, then define $\sqrt{I}$ (sometimes denoted $\operatorname{rad} I$) to be the elements $r \in R$ so that $r^n \in I$ for some $n > 0$. In particular, $\operatorname{Nil} R = \sqrt{0}$.

Lemma 3.1. $\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$

Proof. The inclusion $\sqrt{I} \subseteq \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p}$ is clear. If $r \notin \sqrt{I}$, then $\{1, r, r^2, \dots\}$ is disjoint from $\sqrt{I}$. Take an ideal J containing I which is maximal with respect to not intersecting $\{1, r, r^2, \dots\}$. We wish to show that J is prime, so assume $a, b \notin J$ and $ab \in J$. Then there is some $r^n = j_1 + xa \in J + (a)$ and $r^m = j_2 + yb \in J + (b)$ by maximality of J. But then

$$r^{n+m} = j_1 j_2 + x a j_2 + j_1 y b + x y a b \in J.$$

Contradicting the construction of J. □

Definition 3.2. R is called *reduced* if $\operatorname{Nil} R = 0$. An ideal I is called *reduced* (or *radical*) if $I = \sqrt{I}$.

Definition 3.3. A prime $\mathfrak{p} \supseteq I \lhd R$ is a *minimal prime over* I if there there is no prime $\mathfrak{p}'$ such that $I \subseteq \mathfrak{p}' \subset \mathfrak{p}$.

Every $\mathfrak{p} \supseteq I$ contains a minimal prime over I (by Zorn's Lemma). In particular, $\sqrt{I} = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \bigcap_{\mathfrak{p}' \text{ min'l over } I} \mathfrak{p}'$.

Definition 3.4. The *Jacobson radical* $\operatorname{rad} R$ is the intersection of all maximal ideals.

Note that the maximal ideals of R are in bijection with isomorphism classes of simple R-modules.[1] How does the correspondence work? $\mathfrak{m} \mapsto R/\mathfrak{m}$, which is a simple module. On the other hand, given a simple module S, the annihilator of S is a maximal ideal.[2]

Given this correspondence, one can conclude that $\operatorname{rad} R = \{r \in R | rS = 0 \text{ for all simple modules } S\}$ In noncommutative theory, this is one definition of the Jacobson radical.

Lemma 3.5 (Key Property of $\operatorname{rad}(R)$)**.** *An ideal $I \lhd R$ is contained in* $\operatorname{rad}(R)$ *if and only if* $1 + I \subseteq U(R)$.

[1] A *simple* module is a non-zero module with no proper submodules.

[2] For noncommutative rings, many maximal ideals can correspond to the same isomorphism class of simple module.

That is, $\operatorname{rad} R$ is the largest ideal I such that $1 + I \subseteq U(R)$.

Proof. Say $I \subseteq \operatorname{rad} R$, and $i \in I$. Then if $1 + i$ is not a unit, it is in some maximal ideal $\mathfrak{m}$. But $i \in \mathfrak{m}$, so $1 \in \mathfrak{m}$. Contradiction.

Conversely, assume $1 + I \subseteq U(R)$ and that there is an $i \in I \smallsetminus \operatorname{rad} R$. Then there is some maximal ideal $\mathfrak{m}$ that doesn't contain i. The ideal generated by i and $\mathfrak{m}$ is all of R, so we have $1 = ri + m$ for $r \in R$ and $m \in \mathfrak{m}$. Then $m = 1 - ri \in 1 + I \subseteq U(R)$. Contradiction. □

Lemma 3.6. $\operatorname{Nil} R \subseteq \operatorname{rad} R$.

Proof #1. Maximal ideals are prime, so $\bigcap \mathfrak{p} \subseteq \bigcap \mathfrak{m}$. □

Proof #2. $1 + \operatorname{Nil} R \subseteq U(R)$ because $(1 + r)^{-1} = 1 - r + r^2 - \cdots \in R$ whenever r is nilpotent. The result follows from Lemma 3.5. □

Proof #3. Any nilpotent element is in every maximal ideal. □

Next we discuss two important classes of rings.

Definition 3.7. R is called *Jacobson semisimple* if $\operatorname{rad} R = 0$.

Definition 3.8. R is called *rad-nil* if $\operatorname{rad} R = \operatorname{Nil} R$.

Clearly J-semisimple implies rad-nil.

Example 3.9. Some J-semisimple rings: $\mathbb{Z}$, $k[x]$ when k is a field, $\mathbb{Q}[x, y]/(xy)$. •

Lemma 3.10 (Nakayama's Lemma 2.9)**.** *For $J \lhd R$, the following are equivalent:*

1. $J \subseteq \operatorname{rad}(R)$
2. *Any finitely generated R-module M satisfying $M = JM$ is zero.*
3. *For any R-modules $N \subseteq M$ with M/N finitely generated, $M = N + JM$ implies $M = N$.*

Proof. $(1 \Rightarrow 2)$ If $M \neq 0$, let $x_1, \ldots, x_n$ is a minimal generating set for M (with $n > 0$). Since $JM = M$, we have $x_n = j_1 x_1 + \cdots + j_n x_n$ for $j_i \in J \subseteq \operatorname{rad}(R)$. But then $(1 - j)x_n = j_1 x_1 + \cdots j_{n-1} x_{n-1}$, and $1 - j \in U(R)$, so x_n may be removed from the generating set, contradicting minimality.

$(2 \Rightarrow 3)$ Apply (2) to M/N.

$(3 \Rightarrow 1)$ If $y \in J \smallsetminus \operatorname{rad}(R)$, then there is a maximal ideal $\mathfrak{m}$ not containing y. But then $R = \mathfrak{m} + JR$, so (3) implies $\mathfrak{m} = R$. □

Corollary 3.11 (2.10)**.** *Let J and M be as above. Elements $x_1, \ldots, x_n \in M$ generate M if and only if their images $\bar{x}_1, \ldots, \bar{x}_n$ generate M/JM.*

Proof. Take $N = Rx_1 + \cdots + Rx_n$. □

Definition 3.12. R is *local* if $|\operatorname{Max} R| = 1$.

We write "$(R, \mathfrak{m})$ is local", where $\mathfrak{m}$ is the unique maximal ideal. Note that if R is local then $R \neq 0$. Also note that we do not require R to be Noetherian. Two major sources of local rings:

1. Take any maximal ideal $\mathfrak{m} \lhd R$, and consider $R/\mathfrak{m}^t$, where t is a positive integer. The unique maximal ideal is $\mathfrak{m}/\mathfrak{m}^t$.

2. If $\mathfrak{p} \lhd R$ is a prime, then you can form the localization $R_{\mathfrak{p}}$, whose unique maximal ideal is $\mathfrak{p}R_{\mathfrak{p}}$.

Note that in a local ring $(R, \mathfrak{m})$, $U(R) = R \smallsetminus \mathfrak{m}$. Also note that $R/\mathfrak{m}$ is a field, called the *residue field* of R.

Definition 3.13. R is *semi-local* if $|\operatorname{Max} R| < \infty$.

Semi-localization: Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \lhd R$ be primes. The complement of the union, $S = R \smallsetminus \bigcup \mathfrak{p}_i$, is closed under multiplication, so we can localize. $R[S^{-1}] = R_S$ is called the *semi-localization* of R at the $\mathfrak{p}_i$.

The result of semi-localization is always semi-local. To see this, recall that the ideals in R_S are in bijection with ideals in R contained in $\bigcup \mathfrak{p}_i$. Assume $\mathfrak{p}R_S$ is maximal in R_S, then $\mathfrak{p} \subseteq \bigcup \mathfrak{p}_i$. By prime avoidance (Theorem 1.2), $\mathfrak{p}$ must be in one of the $\mathfrak{p}_i$, so the only maximal ideals are $\mathfrak{p}_i R_S$.

Definition 3.14. For a finitely generated R-module M, define $\mu_R(M)$ to be the smallest number of elements that can generate M.

This is not the same as the cardinality of a minimal set of generators. For example, 2 and 3 are a minimal set of generators for $\mathbb{Z}$ over itself, but $\mu_{\mathbb{Z}}(\mathbb{Z}) = 1$.

Theorem 3.15. *Let R be semi-local with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Let $k_i = R/\mathfrak{m}_i$. Then*

$$\mu_R(M) = \max\{\dim_{k_i} M/\mathfrak{m}_i M\}$$

The proof is in the notes. [[★★★ find a short proof]]

Lecture 4

§3 Associated Primes of Modules

For any module ${}_RM$, you can consider

1. $\operatorname{ann} M \lhd R$, the annihilator of M.
2. $\mathcal{Z}(M) = \{r \in R | rm = 0 \text{ for some nonzero } m \in M\}$ (defined for $M \neq 0$). This is no longer an ideal of R, buy it contains $\operatorname{ann} M$.
3. $\operatorname{Ass} M = \{\mathfrak{p} \in \operatorname{Spec} R | \mathfrak{p} = \operatorname{ann}(m) \text{ for some non-zero } m \in M\}$. We call $\operatorname{ann}(m)$ a *point annihilator*. Clearly any such $\mathfrak{p}$ contains $\operatorname{ann} M$.
4. $\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R | M_{\mathfrak{p}} \neq 0\}$.

A very important case is when $M = R/I$ is cyclic (where $I \lhd R$). In this case, $\operatorname{ann} R/I = I$, $\mathcal{Z}(R/I) = \{r \in R | rm \in I \text{ for some } m \in R \smallsetminus I\}$.

How to deal with $\operatorname{Ass} M$

Lemma 4.1. *For $\mathfrak{p} \in \operatorname{Spec} R$, and suppose you are given ${}_RM$, then $\mathfrak{p} \in \operatorname{Ass} M$ if and only if $R/\mathfrak{p} \hookrightarrow M$.*

Proof. If $f : R/\mathfrak{p} \hookrightarrow M$ then $\mathfrak{p} = \operatorname{ann}(f(1))$. If $\mathfrak{p} = \operatorname{ann}(x)$, then $f : R \to M$ defined by $f(1) = x$ has kernel $\mathfrak{p}$. □

Lemma 4.2. *If $N \subseteq M$, then $\operatorname{Ass} N \subseteq \operatorname{Ass} M$.*

Proof. $\mathfrak{p} \in \operatorname{Ass} N \Rightarrow \mathfrak{p} = \operatorname{ann}(x) \Rightarrow \mathfrak{p} \in \operatorname{Ass} M$. □

Lemma 4.3 (Herstein)**.** *Any maximal point annihilator of M is an associated prime.*

Proof. Let $\operatorname{ann}(x)$ be a maximal point annihilator. To check that $\operatorname{ann}(x)$ is prime, assume $ab \in \operatorname{ann}(x)$ and $b \notin \operatorname{ann}(x)$. Then $bx \neq 0$, so $\operatorname{ann}(x) = \operatorname{ann}(bx)$ by maximality. But $abx = 0$, so $a \in \operatorname{ann}(bx) = \operatorname{ann}(x)$. □

Note that if M is not noetherian, there may not be any maximal point annihilators, so this does not prove existence of an associated prime.

Example 4.4. Here an a non-zero module M with $\operatorname{Ass} M = \varnothing$. Take suitable R, and let $M = {}_RR$. Take $R = \mathbb{Q}[x_1, x_2, \dots]/(x_i^2)_{i=1,2,\dots}$. In this ring, there is a unique prime $\mathfrak{p} = (x_1, x_2, \dots)$. In particular, R is a local ring. If $\operatorname{Ass} R \neq \varnothing$, then $\mathfrak{p} = \operatorname{ann}(m)$ for some nonzero m. But then m kills every x_i. However, if any polynomial annihilates $\mathfrak{p}$, write it so that all terms are square-free, but then take x_N with N larger than any indices appearing in m, and $mx_N \neq 0$. •

Example 4.5. Let $R = \mathbb{Z}$. Then $\operatorname{Ass}(\mathbb{Z}) = \{(0)\}$, $\operatorname{Ass}(\mathbb{Q}) = \{(0)\}$, $\operatorname{Ass}(\mathbb{Z} \oplus \mathbb{Z}/60) = \{(0), (2), (3), (5)\}$, and $\operatorname{Ass}(\mathbb{Q}/\mathbb{Z}) = \operatorname{Max} \mathbb{Z} = \operatorname{Spec} \mathbb{Z} \smallsetminus \{(0)\}$. •

For every M, $\mathcal{Z}(M)$ is a union of prime ideals. In general, there is an easy characterization of sets Z which are a union of primes: it is exactly when $R \setminus Z$ is a *saturated multiplicative set*. This is Kaplansky's Theorem 2.

Definition 4.6. A multiplicative set $S \neq \varnothing$ is a *saturated multiplicative set* if for all $a, b \in R$, $a, b \in S$ if and only if $ab \in S$. ("multiplicative set" just means the "if" part)

To see that $\mathcal{Z}(M)$ is a union of primes, just verify that its complement is a saturated multiplicative set.

Let $M = R/I$. Then $\operatorname{Ass}(R/I)$ is often called "the set of primes associated to I". For any set S and ideal $I \lhd R$, we define $I : S = \{r \in R | r \cdot S \subseteq I\}$. Of course, you can replace S by the ideal generated by S. Then $\operatorname{Ass} R/I$ consists of prime ideals of the form $I : x$.

Example 4.7. Take $R = k[x, y, z]$, where k is an integral domain, and let $I = (x^2 - yz, x(z-1))$. Any prime associated to I must contain I, so let's consider $\mathfrak{p} = (x^2 - yz, z - 1) = (x^2 - y, z - 1)$, which is $I : x$. It is prime because $R/\mathfrak{p} = k[x]$, which is a domain. To see that $I : x \subseteq \mathfrak{p}$, assume $tx \in I \subseteq \mathfrak{p}$; since $x \notin \mathfrak{p}$, $t \in p$, as desired.

There are two more associated primes, but we will not find them here. •

Proposition 4.8.

1. *If $N \subseteq M$, then* $\operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass} M/N$
2. *If $M = \bigoplus_{i=1}^n M_i$, then* $\operatorname{Ass} M = \bigcup_{i=1}^n \operatorname{Ass} M_i$.

Proof. (1) Observation: If $N \subseteq R/\mathfrak{p}$ is a nonzero submodule, then $\operatorname{Ass} N = \{\mathfrak{p}\}$. To see this, take $x \in R \setminus \mathfrak{p}$; then $\mathfrak{p} : x = \mathfrak{p}$ by primeness of $\mathfrak{p}$.

Now if $\mathfrak{p} \in \operatorname{Ass} M$, we have $R/\mathfrak{p} \hookrightarrow M$; call the image Y. If $N \cap Y = 0$, then $Y \cong R/\mathfrak{p} \hookrightarrow M/N$, so $\mathfrak{p} \in \operatorname{Ass}(M/N)$. Otherwise, $N \cap Y \subseteq Y$ is a nonzero submodule, so $\{\mathfrak{p}\} \in \operatorname{Ass}(N \cap Y) \subseteq \operatorname{Ass} N$.

(2) The containment $\subseteq$ follows from (1), and the containment $\supseteq$ follows from Lemma 4.2. □

Lecture 5

Example 5.1. Let's compute the primes associated to $I = \mathfrak{p}_1\mathfrak{p}_2$ under the assumptions that (1) $\mathfrak{p}_1 = (x)$, where x is regular; (2) There is some $y \in \mathfrak{p}_2 \smallsetminus \mathfrak{p}_1$.

We claim that $I : y = \mathfrak{p}_1$ and $I : x = \mathfrak{p}_2$, which would show that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are associated prime. The inclusions $\supseteq$ are clear. For the other inclusion, assume $ty \in I = \mathfrak{p}_1\mathfrak{p}_2 \subseteq \mathfrak{p}_1$. Since $y \notin \mathfrak{p}_1$, we get $t \in \mathfrak{p}_1$, as desired. If $tx \in I = \mathfrak{p}_1\mathfrak{p}_2 = x\mathfrak{p}_2$. Since x is regular, we can cancel it, so $t \in \mathfrak{p}_2$.

Now we'd like to show that there are no other associated primes. We have $I = \mathfrak{p}_1\mathfrak{p}_2 \subseteq \mathfrak{p}_1 = (x) \subseteq R$, so any associated prime is an associated prime of $R/\mathfrak{p}_1$ or of $\mathfrak{p}_1/\mathfrak{p}_1\mathfrak{p}_2 \cong R/\mathfrak{p}_2$ (via multiplication by x). But we showed that the only associated prime of $R/\mathfrak{p}$ is $\mathfrak{p}$. •

Example 5.2. Now let's specialize the previous example to $R = k[x, y]$ where k is a field, and x and y as in the previous example: $\mathfrak{p}_1 = (x)$ and $\mathfrak{p}_2$ is one of the following:

- $\mathfrak{p}_2 = (y)$, $I = (xy)$. In this case, we see that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are the minimal primes over I; if $\mathfrak{p} \supseteq I = \mathfrak{p}_1\mathfrak{p}_2$, then $\mathfrak{p}$ must be one or the other since it is minimal (it must contain one since $\mathfrak{p}$ is prime).
- $\mathfrak{p}_2 = (x, y)$, $I = (x^2, xy)$. Here it is clear that $\sqrt{I} = (x)$. The remarkable thing is that (x, y) is an "embedded associated prime" to I. We call an associated prime if it contains another embedded prime; if it doesn't contain an associated prime, it is called an "isolated prime" of I. •

Recall that $\operatorname{Supp} M = \{\mathfrak{p} \in \operatorname{Spec} R | M_\mathfrak{p} \neq 0\}$. If $I \subseteq R$ is a subset, then we define $\mathcal{V}(I) = \{\mathfrak{p} \in \operatorname{Spec} R | I \subseteq \mathfrak{p}\}$.

Proposition 5.3. *For any module M over R, let $I = \operatorname{ann} M$.*

1. *"Specialization": If $\mathfrak{p}' \subseteq \mathfrak{p}$ and $\mathfrak{p}' \in \operatorname{Supp} M$, then $\mathfrak{p} \in \operatorname{Supp} M$.*
2. $\operatorname{Ass} M \subseteq \operatorname{Supp} M$.
3. $\operatorname{Supp} M \subseteq \mathcal{V}(I)$.
4. *If M is finitely generated, then* $\operatorname{Supp} M = \mathcal{V}(I)$.

Proof. (1) Let $\mathfrak{p}' \subseteq \mathfrak{p}$ and assume $\mathfrak{p} \notin \operatorname{Supp} M$, so $M_\mathfrak{p} = 0$. Then $M_{\mathfrak{p}'} = (M_\mathfrak{p})_{\mathfrak{p}'} = 0$.

(2) If $\mathfrak{p} \in \operatorname{Ass} M$, then $R/\mathfrak{p} \hookrightarrow M$. Localizing, we get $R_\mathfrak{p}/\mathfrak{p}_\mathfrak{p} = (R/\mathfrak{p})_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$, so $M_\mathfrak{p}$ contains a field, so it is non-zero.

(3) Take $\mathfrak{p} \notin \mathcal{V}(I)$, so there is some $i \in I \smallsetminus \mathfrak{p}$ so that $iM = 0$. This implies that $M_\mathfrak{p} = 0$.

(4) Say $M = \sum_{i=1}^n Rm_i$. Take $\mathfrak{p} \in \mathcal{V}(I)$ and assume it is not a supporting prime, so $M_\mathfrak{p} = 0$. Then for each i, there is some $r_i \notin \mathfrak{p}$ so that $r_i m_i = 0$. Then $r = r_1 \cdots r_n$ kills all of M, so it is in I, but not in $\mathfrak{p}$ (since $\mathfrak{p}$ is prime). Contradiction. □

"Minimal primes consist of zero divisors"

Proposition 5.4 (Theorem 84 in Kaplansky)**.** *For any module M, any minimal prime $\mathfrak{p}$ over $I = \operatorname{ann} M$ must lie in $\mathcal{Z}(M)$.*

In particular, taking $M = R$, we get that minimal primes in R lie in $\mathcal{Z}(R)$. Note that there are *no chain conditions* on M in this proposition.

Proof. Let $I \subseteq \mathfrak{p}$ and we know $I \subseteq \mathcal{Z}(M)$. Then $R/\mathfrak{p}$ and $R \smallsetminus \mathcal{Z}(M)$ are multiplicative sets away from I. Let S be the multiplicative set generated by these two. We claim that S is disjoint from I. To see this, assume $a \notin \mathfrak{p}$ and $b \notin \mathcal{Z}(M)$ such that $ab \in I$, so $abM = 0$. But $bM = M$ by assumption, so $aM = 0$, so $a \in I \subseteq \mathfrak{p}$, which is a contradiction.

Thus, there is some prime $\mathfrak{p}' \supseteq I$ which is disjoint from S. It follows that $\mathfrak{p}' \subseteq \mathfrak{p}$, and $\mathfrak{p}$ is minimal over I, so $\mathfrak{p}' = \mathfrak{p}$. Similarly, $\mathfrak{p}' \subseteq \mathcal{Z}(M)$. That is, $\mathfrak{p} \subseteq \mathcal{Z}(M)$, as desired. □

Theorem 5.5. *Let $I \lhd R$ be a radical ideal, and consider the cyclic module R/I.*

1. *$\mathcal{Z}(R/I) = \bigcup_{\mathfrak{p} \text{ min'l over } I} \mathfrak{p}$.*

"A radical ideal has no embedded points"

2. *Every $\mathfrak{p} \in \operatorname{Ass}(R/I)$ is a minimal prime over I.*

Proof. (1) The inclusion $\supseteq$ is clear from the previous proposition. Given $x \in \mathcal{Z}(R/I)$, fix $y \notin I$ such that $xy \in I$. Then $I \subsetneq I : x$ (since $y \notin I$). So there is a minimal prime $\mathfrak{p}$ over I such that $I : x \not\subseteq \mathfrak{p}$ (since I is the intersection of minimal primes over it). But $x \cdot (I : x) \subseteq \mathfrak{p}$, which implies that $x \in \mathfrak{p}$.

(2) Let $\mathfrak{p} = I : m$ be an associated prime, where $m \notin I$. Then $m \notin \mathfrak{p}$, lest $m \cdot m = 0 \in I$, which would imply $m \in I$ since I is radical. Now assume that there is some $\mathfrak{p}'$ so that $\mathfrak{p} \supsetneq \mathfrak{p}' \supseteq I$. Fix $x \in \mathfrak{p} \smallsetminus \mathfrak{p}'$. Then $xm \in I \subseteq \mathfrak{p}'$, which implies $m \in \mathfrak{p}$. Contradiction. □

"Ass M behaves well under localization"

Proposition 5.6. *Let $S \subseteq R$ be a multiplicative set disjoint from some prime $\mathfrak{p}$. For any module M, if $\mathfrak{p} \in \operatorname{Ass} M$, then $\mathfrak{p}_S \in \operatorname{Ass}(M_S)$. If $\mathfrak{p}$ is finitely generated, then the converse holds.*

Assuming all primes in $\operatorname{Ass} M$ are finitely generated, this can be rewritten as the equality

$$\operatorname{Ass}(M_S) = \operatorname{Ass}(M) \cap \operatorname{Spec}(R_S).$$

This is proven in the notes. [[★★★]]

Lecture 6

§4 Noetherian Rings and Noetherian Induction

Recall the following facts about rings and modules with chain conditions.

1. A module is noetherian if and only if every submodule is finitely generated.
2. A module is noetherian and artinian if and only if it has a (finite) composition series (quotients are simple). The Jordan-Hölder theorem tells us that the quotients are unique up to permutation.
3. If $N \subseteq M$, M is noetherian (resp. artinian) if and only if both N and M/N are.
4. If R is noetherian, then M is noetherian if and only if it is finitely generated.

Theorem 6.1 (I. S. Cohen)**.** *A ring R is noetherian if and only if all prime ideals are finitely generated.*

For the proof, we need the following lemma and proposition.

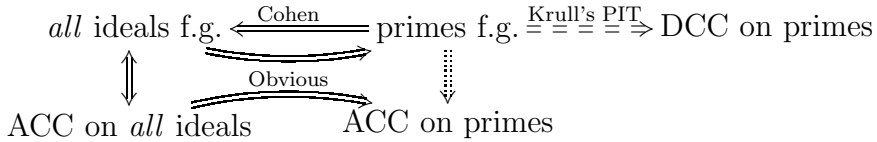
Lemma 6.2 (Oka's Lemma)**.** *Let $I \lhd R$ and $b \in R$. If $I + (b)$ and $I : b$ are finitely generated, then so is I.*

Proof. Since $I+(b)$ is finitely generated, it can be written as $I_0+(b)$ for some finitely generated ideal $I_0 \subseteq I$. Then $I = I_0 + b(I : b)$ is finitely generated. □

Proposition 6.3. *If $I \lhd R$ is maximal with respect to* not *being finitely generated (i.e. every $J \supsetneq I$ is f.g.), then I is prime.*

Proof. Clearly $I \neq R$. Suppose I is not prime, so there are $a, b \notin I$, with $ab \in I$. Then $I + (b)$ and $I : b$ ($\ni a$) are finitely generated. By Oka's Lemma, I is finitely generated, which is a contradiction. □

Proof of Theorem 6.1. Assume all primes in R are finitely generated, and that $\mathcal{F} = \{\text{non-f.g. ideals}\} \neq \varnothing$. Since the union of non-finitely-generated ideals is not finitely generated, Zorn's Lemma gives us a maximal element, which is prime by Proposition 6.3, so it is finitely generated by assumption. Contradiction. □



Theorem 6.4 (Noetherian Induction Principle)**.** *Let R be a noetherian ring, let $\mathcal{P}$ be a property, and let $\mathcal{F}$ be a family of ideals R. Suppose the inductive step: if all ideals in $\mathcal{F}$ strictly larger than $I \in \mathcal{F}$ satisfy $\mathcal{P}$, then I satisfies $\mathcal{P}$. Then all ideals in $\mathcal{F}$ satisfy $\mathcal{P}$.*

Proof. Assume $\mathcal{F}_{\text{crim}} = \{J \in \mathcal{F} | J \text{ does not satisfy } \mathcal{P}\} \neq \varnothing$. Since R is noetherian, $\mathcal{F}_{\text{crim}}$ has a maximal member I. By maximality, all ideals in $\mathcal{F}$ strictly containing I satisfy $\mathcal{P}$, so I also does by the inductive step. □

Definition 6.5. An element r is *irreducible* if it cannot be written as a product of two non-units. A (proper) ideal I is *irreducible* if it cannot be written as the intersection of two strictly larger ideals. (irreducible ideals are primary! [[★★★ ref this result]])

Example 6.6. For a noetherian ring R, we can prove the following results by checking the inductive step in each case. For the first two, take $\mathcal{F}$ to be the set of all ideals.

1. Every ideal is a finite intersection of irreducible ideals.

   Assume every ideal strictly containing I is a finite intersection of irreducible ideals. If $I = R$, it is the empty intersection. If I is irreducible, then we're done. Otherwise, $I = J_1 \cap J_2$ for strictly larger ideals J_1 and J_2. By assumption, J_i is a finite intersection of irreducible ideals, so I is also.

2. ($R \neq 0$) Every ideal in R contains a finite product of primes.

   Assume any ideal larger than I contains a finite product of primes. If I is prime or R, we're done. Otherwise, there are ideals J_1 and J_2 which contain I such that $J_1 J_2 \subseteq I$. Since each J_i contains a finite product of primes, so does I.

3. (R a domain) Every $r \notin (0) \cup U(R)$ is a finite product of irreducible elements.

   Here we let $\mathcal{F}$ be non-zero, non-R, principal ideals, and let $\mathcal{P}$ be the statement that the generator is a finite product of irreducible elements (note that this is independent of the choice of generator since R is a domain). [[★★★ finish ... easy]]

4. If $J = \sqrt{J}$, then J is a *finite* intersection of primes. (Kaplansky's Theorems 87 and 88)

   Take $\mathcal{F}$ to be the set of radical ideals.[[★★★ finish]]

   As a corollary, for any $I \lhd R$ in a noetherian ring, there are finitely many minimal primes over I. •

Note that the examples where $\mathcal{F}$ is not the set of all ideals illustrate that to apply noetherian induction, you only need the ideals *in* $\mathcal{F}$ to satisfy the ascending chain condition.

Lecture 7

Noetherian Descent

Certain theorems about commutative rings can be proven by a reduction to the noetherian case (the Hilbert basis theorem is secretly being used). If the statement $\mathcal{F}$ you want to prove only involves a finite number of elements of R, say $a_1, \ldots, a_n$. Then look at the ring R_0 generated by $1, a_1, \ldots, a_n$. It is the homomorphic image of the ring $\mathbb{Z}[x_1, \ldots, x_n]$. By the Hilbert basis theorem, this ring is noetherian, so homomorphic images are also noetherian.

Here is a typical application. A non-zero commutative ring satisfies the strong rank property ($R^m \hookrightarrow R^n$ implies $m \leq n$). The strong rank property can be rephrased as $R^{n+1} \not\hookrightarrow R^n$ (module theoretically). This can be formulated as, "a homogeneous system of n equations and $n+1$ unknowns has a a nontrivial solution". It suffices to solve this system in R_0, so apply descent. Now we just have to prove it in a noetherian ring. $R^{n+1} \hookrightarrow R^n$ can be easily contradicted in the noetherian case. Think of R^{n+1} as $X_1 = R^n \oplus R$; think of this R as generated by x, so the image of R^{n+1} is an image of R^n direct sum with another module. Now repeat by embedding R^{n+1} into the copy of R^n. Then the module generated by $x, x_1, \ldots, x_n$ gives an infinite ascending chain.

§5 Artinian Rings

Definition 7.1. The *(Krull) dimension* of a commutative ring R is defined as $\dim R = \sup\{\text{lengths of chains of primes}\}$.

In particular, a zero dimensional ring is one in which every prime ideal is maximal: $\operatorname{Spec} R = \operatorname{Max} R$.

Definition 7.2 (von Neumann)**.** An element $a \in R$ is called *von Neumann regular* if there is some $x \in R$ such that $a = axa$.

Definition 7.3 (McCoy)**.** A element $a \in R$ is *π-regular* if some power of a is von Neumann regular.

Definition 7.4. A element $a \in R$ is *strongly π-regular* (in the commutative case) if the chain $aR \supseteq a^2R \supseteq a^3R \supseteq \cdots$ stabilizes.

A ring R is von Neumann regular (resp. (strongly) π-regular) if every element of R is.

Theorem 7.5 (5.2)**.** *For a commutative ring R, the following are equivalent.*

1. $\dim R = 0$.
2. *R is rad-nil (i.e.* $\operatorname{rad} R = \operatorname{Nil} R$*) and* $R/\operatorname{rad} R$ *is von Neumann regular.*

3. R is strongly π-regular.

4. R is π-regular.

And any one of these implies

5. $\mathcal{C}(R) = U(R)$; any non-zero-divisor is a unit.

Proof. $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4 \Rightarrow 1$ and $4 \Rightarrow 5$. We will not do $1 \Rightarrow 2 \Rightarrow 3$ here.

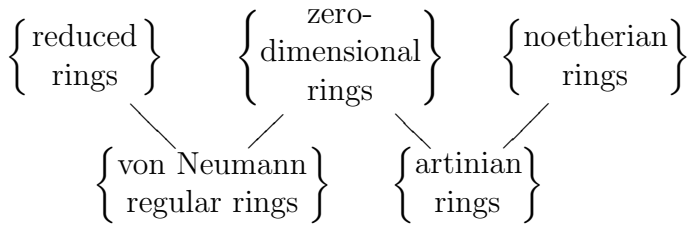
$(3 \Rightarrow 4)$ Given $a \in R$, there is some n such that $a^n R = a^{n+1} R = a^{2n} R$, which implies that $a^n = a^n x a^n$ for some x.

$(4 \Rightarrow 1)$ Is $\mathfrak{p}$ maximal? Let $a \notin \mathfrak{p}$. Since a is π-regular, we have $a^n = a^{2n}x$, so $a^n(1 - a^n x) = 0$, so $1 - a^n x \in \mathfrak{p}$. It follows that a has an inverse mod $\mathfrak{p}$.

$(4 \Rightarrow 5)$ Using $1 - a^n x = 0$, we get an inverse for a. □

Example 7.6. Any local rad-nil ring is zero dimensional, since 2 holds. In particular, for a ring S and $\mathfrak{m} \in \operatorname{Max} S$, $R = S/\mathfrak{m}^n$ is zero dimensional because it is a rad-nil local ring. •

Example 7.7 (Split-Null Extension)**.** For a ring A and A-module M, let $R = A \oplus M$ with the multiplication $(a, m)(a', m') = (aa', am' + a'm)$ (i.e. take the multiplication on M to be zero). In R, M is an ideal of square zero. (A is called a *retract* of R because it sits in R and can be recovered by quotienting by some complement.) If A is a field, then R is a rad-nil local ring, with maximal ideal M. •



Lecture 8

A topological point: Spec R is always T_0 (each point has a neighborhood that misses *some* other point). Spec R is T_1 (points are closed) if and only if it is T_2 (Hausdorff) if and only if $\dim R = 0$.[[★★★ check this]]

Remark 8.1. The separation axioms are called T_i because they are "Trennung's" axioms.

Corollary 8.2 (to the last theorem)**.** *The following are equivalent.*

- *R is von Neumann regular*
- *R is reduced and* $\dim R = 0$
- *$R_{\mathfrak{m}}$ is a field for all $\mathfrak{m} \in \operatorname{Max}(R)$ (In particular, R is "locally noetherian").*

Proposition 8.3. *If R is artinian, then*

1. $\dim R = 0$,
2. *$J := \operatorname{rad} R$ is nilpotent, and*
3. *R is semi-local.*

Proof. (2) see notes

(1) For each $a \in R$, $aR \supseteq a^2R \supseteq \cdots$ stabilizes (i.e. R is strongly π-regular), so $\dim R = 0$ by Theorem from last time.

(3) Among all finite products of maximal ideals, choose one that is minimal, say $I = \mathfrak{m}_1 \cdots \mathfrak{m}_n$. Then for any maximal ideal $\mathfrak{m}$, $\mathfrak{m}I = I$ by minimality, so $I \subseteq \mathfrak{m}$, so some $\mathfrak{m}_i \subseteq \mathfrak{m}$ for some i since $\mathfrak{m}$ is prime. Then $\mathfrak{m} = \mathfrak{m}_i$ by maximality. □

This gives a characterization of semi-local rings R via chain conditions.

Corollary 8.4. *A ring R is semi-local if and only if $R/\operatorname{rad} R$ is artinian.*

Proof. ($\Leftarrow$) Assume R/J is artinian ($J := \operatorname{rad} R$), so R/J is semi-local. By any maximal ideal in R contains J, so they are in bijection with maximal ideals of R/J. So R is semi-local.

($\Rightarrow$) If R is semi-local, with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. In §2, we showed that since $J = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, $R/J \cong \prod_{i=1}^n R/\mathfrak{m}_i$. So R/J is a finite product of fields, so it is artinian. □

Lemma 8.5 (Key Lemma for Akizuki)**.** *Let R be a ring with (not necessarily distinct) maximal ideals $\mathfrak{m}_1, \ldots \mathfrak{m}_n$ such that $\mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Then R is noetherian if and only if R is artinian.*

Proof. Look at the filtration

$$R \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0.$$

The filtration factor $\mathfrak{m}_1 \cdots \mathfrak{m}_i / \mathfrak{m}_1 \cdots \mathfrak{m}_{i+1}$ is a $R/\mathfrak{m}_{i+1}$ vector space. In a vector space, noetherian and artinian are both equivalent to finite dimensional. R is noetherian if and only if each filtration factor is noetherian, which occurs if and only if each factor is artinian, which occurs if and only if R is artinian! □

Theorem 8.6 (Akizuki)**.** *For any ring R, the following are equivalent.*

1. *R is artinian.*
2. *R is noetherian and* $\dim R = 0$.
3. *${}_RR$ has finite length.*
4. All *finitely generated modules ${}_RM$ have finite length.*
5. *There is a faithful module ${}_RM$ of finite length.*
6. *There is a faithful finitely generated artinian module ${}_RM$.*

Proof. $3 \Rightarrow 4 \Rightarrow 1 \Rightarrow 2 \Rightarrow 5 \Rightarrow 3$ and $5 \Rightarrow 6 \Rightarrow 1$

($3 \Rightarrow 4$) We have ${}_RR^n \twoheadrightarrow M$, and $lg(R^n) = n \cdot lg(R) \geq lg(M)$.

($4 \Rightarrow 1$) Apply (4) to ${}_RR$.

($1 \Rightarrow 2$) We already have $\dim R = 0$ from the Proposition. We also know that R is semi-local, with maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Then $\operatorname{rad} R = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n$ is nilpotent. So $(\mathfrak{m}_1 \cdots \mathfrak{m}_n)^t = 0$ for some big t. Then by the Key lemma, R is noetherian.

($2 \Rightarrow 5$) From the second example of noetherian induction, $(0) = \mathfrak{p}_1 \cdots \mathfrak{p}_n$ (every ideal contains a finite product of primes). Since $\dim R = 0$, these $\mathfrak{p}_i$ are maximal. By the Key lemma, R is artinian, so ${}_RR$ is a faithful module of finite length.

($5 \Rightarrow 3$) If ${}_RM$ is finite length, it is finitely generated, say $M = Rm_1 + \cdots Rm_k$. We have a map $R \to M^k = M \oplus \cdots \oplus M$ given by $r \mapsto (rm_1, \cdots, rm_k)$. This is an R-module homomorphism, and it is injective because M is faithful (no r can kill all the generators). Now $lg(R) \leq k \cdot lg(M) < \infty$.

($5 \Rightarrow 6$) ${}_RR$ is already a faithful module of finite length.

($6 \Rightarrow 1$) Same argument as $5 \Rightarrow 3$, but with "finite length" replaced by "artinian". □

Remark 8.7. (6) is not equivalent to (6′) There is a faithful artinian module ${}_RM$. For example, take $R = \mathbb{Z}$ and $M = \varinjlim \mathbb{Z}/p^n\mathbb{Z}$, the Prüfer p-group. Then M is artinian (all the submodules are $\mathbb{Z}/p^k\mathbb{Z}$), and faithful, but not finitely generated.

Remark 8.8. Note that artinian implies noetherian! This statement is true for rings (even non-commutative rings), but not for modules. Take the same example $M = \varinjlim \mathbb{Z}/p^n\mathbb{Z}$ over $\mathbb{Z}$. However, there is a module-theoretic statement which is related.

Corollary 8.9. *For a finitely generated module M over any commutative ring R, the following are equivalent.*

1. *M is an artinian module.*
2. *M has finite length (i.e. is noetherian and artinian).*
3. *$R/\operatorname{ann} M$ is an artinian ring.*

Note that we don't assume that R is noetherian (as in Eisenbud).

Lecture 9

- Every finitely generated module M over an artinian ring R has finite length.
- Every finite length module M over any (commutative) ring R "arises in this way"

Proof of Corollary 8.9 (5.11). $(3 \Rightarrow 2)$

$$lg_R(M) = lg_{R/\operatorname{ann} M}(M) < \infty$$

by Akizuki.

$(2 \Rightarrow 1)$ clear

$(1 \Rightarrow 3)$ $R/\operatorname{ann} M$ has a finitely generated faithful artinian module, namely M. Now use Akizuki. □

Theorem 9.1 (Akizuki-Cohen)**.** *Any artinian ring R is a* finite *direct product of local artinian rings $R_1, \ldots, R_n$, whose isomorphism types (as rings) are uniquely determined.*

Proof. Let $J = \operatorname{rad} R = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ (R is semi-local by [[★★★]]). We also know that J is nilpotent, so $(\mathfrak{m}_1 \cdots \mathfrak{m}_n)^t = 0$ for large enough t. By the Chinese Remainder Theorem,

$$R = \frac{R}{\mathfrak{m}_1^t \cdots \mathfrak{m}_n^t} \cong \prod R/\mathfrak{m}_i^t.$$

But $R/\mathfrak{m}_i^t$ is a local ring (with maximal ideal $\mathfrak{m}_i/\mathfrak{m}_i^t$) and artinian (being a quotient of an artinian ring). Uniqueness follows from Exercise 9. □

Definition 9.2. R is a *principal ideal ring* (or *PIR*) if every ideal of R is principal.

Theorem 9.3 (5.13)**.** *Let $(R, \mathfrak{m})$ be a local artinian ring. Then the following are equivalent.*

1. *R is a PIR.*
2. *$\mathfrak{m}$ is principal.*
3. $\dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.
4. *R is a "chain ring" (for any ideals I and J, either $I \subseteq J$ or $J \subseteq I$).*

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

$(4 \Rightarrow 2)$ Let $\mathfrak{m} = Ra_1 + \cdots + Ra_n$. Since R is a chain ring, we may assume $Ra_1 \supseteq Ra_i$. Then $\mathfrak{m} = Ra_1$.

$(3 \Rightarrow 1, 4)$ Find $a \in \mathfrak{m}$ such that $\bar{a}$ generates $\mathfrak{m}/\mathfrak{m}^2$ over $R/\mathfrak{m}$. By Nakayama's lemma, $\mathfrak{m} = Ra$. Let's show that any non-zero $I \lhd R$ is principal. We know that $\mathfrak{m}$ is nilpotent, so there is a largest integer r such that $I \subseteq \mathfrak{m}^r$ (so $I \not\subseteq \mathfrak{m}^{r+1}$. Let $y \in I \smallsetminus \mathfrak{m}^{r+1}$. We can write $y = ta^r$ because $y \in \mathfrak{m}^r$. Then t must be a unit, lest $y \in \mathfrak{m}^{r+1}$. So $Ra^r = Ry \subseteq I \subseteq Ra^r$. If follows that I is principal, and that all the ideals are of the form $\mathfrak{m}^r$, proving (4). □

Definition 9.4. A 0-dimensional Gorenstein ring is a local artinian ring in which the zero ideal is irreducible.

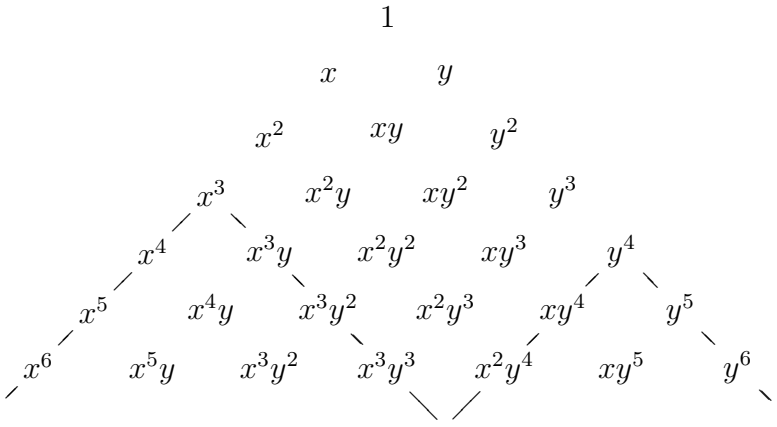
Example 9.5. Finite rings are artinian. For example $\mathbb{Z}/60$. We have $\mathbb{Z}/60 \cong \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/5$ illustrating Akizuki-Cohen. •

Example 9.6. Let A is any ring, and let $\mathfrak{m}$ be a finitely generated maximal ideal in A. Let I be any ideal containing some $\mathfrak{m}^k$. Then $R = A/I$ is artinian. The only prime ideal is $\mathfrak{m}/I$, so this is a local zero-dimensional ring ... it is noetherian because all primes are finitely generated, so it is artinian. •

Example 9.7. In a local artinian ring $(R, \mathfrak{m})$, we have the filtration

$$R \supseteq \mathfrak{m} \supseteq \cdots \supseteq \mathfrak{m}^n = 0$$

where consecutive quotients are vector spaces over $k = R/\mathfrak{m}$. You may form a generating function $f(t)$ out of these dimensions, which will be a polynomial. For example, use the construction from the previous example, with $A = k[x, y]$, $\mathfrak{m} = (x, y)$ and $I = (x^3, y^4)$, so $R = A/I$. Then we get that $\mathfrak{m}^6 = 0$, and $f(t) = 1 + 2t + 3t^2 + 3t^3 + 2t^4 + 1t^5$ by inspection (just look at the number of (surviving) generators in each line).



Note that in the case of a PIR, $f(t) = 1 + t + t^2 + \cdots + t^{n-1}$ (the coefficient of t is 1 if and only if you are in a PIR). •

Example 9.8. "a ring where $x^5 = 0$ but $x^6 \neq 0$" Let $A = k[x^2, x^3] \subseteq k[x]$; note that $x \notin A$. Take $I = x^5 A$ and let $R = A/I$, and find $f(t)$. Write a k-basis for everything: A has basis $\{1, x^2, x^3, x^4, \dots\}$; I has basis $\{x^5, x^7, x^8, x^9, \dots\}$. Then $f(t) = 1 + 2t + t^2 + t^3$.

Note that A is the coordinate ring of the cuspidal cubic. •

Lecture 10

§6 Associated Primes over Noetherian Rings

Proposition 10.1.

1. *If R is noetherian and ${}_RM \neq 0$, then* $\operatorname{Ass} M \neq \varnothing$.
2. *If ${}_RM$ is noetherian, then* $|\operatorname{Ass} M| < \infty$.

Example 10.2. The following usually give good counter-examples. Look at $M = \mathbb{Q}/\mathbb{Z}$ or look at $R = k \times k \times \cdots$, where k is a field. Notice that M is faithful over $\mathbb{Z}$. •

Proof. (1) If $M \neq 0$, then the set of point annihilators is non-empty, so there is a maximal element by the noetherian hypothesis. By Herstein's lemma, we've found an associated prime.

(2) Let $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \in \operatorname{Ass} M$ be an infinite number of distinct associated primes of M. Then you can find some $R/\mathfrak{p}_1 \hookrightarrow M$. Since $\operatorname{Ass}(R/\mathfrak{p}_1) = \{\mathfrak{p}_1\}$, the other primes must be associated primes of $M/(R/\mathfrak{p}_1)$. This gives you an ascending chain of submodules of M, contradicting the noetherian hypothesis. □

Theorem 10.3 (6.2)**.** *Let $M \neq 0$ be a module over a noetherian ring R. Then $\mathcal{Z}(M) = \bigcup \mathfrak{p}_i$, where the $\mathfrak{p}_i$ are maximal point annihilators. If M is finitely generated, then this is a* finite *union, and any ideal $A \subseteq \mathcal{Z}(M)$ lies in some $\mathfrak{p}_i$. In particular, $Am = 0$ for some non-zero element $m \in M$. (This last part is Theorem 82 of Kaplansky[1])*

Proof. It is enough to show $\mathcal{Z}(M) \subseteq \bigcup \mathfrak{p}_i$. Note that $\mathcal{Z}(M)$ is the union of all point annihilators. Since R is noetherian, every point annihilator is in some maximal point annihilator.

If M is finitely generated, then $\operatorname{Ass} M$ is finite by the proposition, so the union is finite. If $A \subseteq \mathcal{Z}(M)$ is closed under addition and multiplication, then by prime avoidance, A is in some $\mathfrak{p}_i = \operatorname{ann} m_i$. □

In general, for a given M, the set $\operatorname{Ass} M$ is the important set of primes, as far as the behavior of M is concerned.

Proposition 10.4. *Let R be a noetherian ring.*

1. *Let $M' \subseteq M$ over R, and let $m \in M$. Then $m \in M'$ if and only if $m/1 \in M'_{\mathfrak{p}}$ for every $\mathfrak{p} \in \operatorname{Ass}(M/M')$.*
2. *$f : M \to Q$ is injective if and only if $f : M_{\mathfrak{p}} \to Q_{\mathfrak{p}}$ is injective for every $\mathfrak{p} \in \operatorname{Ass} M$.*

[1] Kaplansky says it is one of the most useful facts about commutative rings.

3. *$g : N \to M$ is surjective if and only if $g_{\mathfrak{p}} : N_{\mathfrak{p}} \to M_{\mathfrak{p}}$ is surjective for every $\mathfrak{p} \in \operatorname{Ass}(M/g(N)) = \operatorname{Ass}(\operatorname{coker} g)$.*

Proof. First we do the "if" parts:

1. We may replace M by M/M' and assume $M' = 0$. Suppose $m \neq 0$, then $\operatorname{ann} m \subseteq \mathfrak{p} \in \operatorname{Ass} M$ (some maximal annihilator) by the noetherian hypothesis on R. Then if $m/1 = 0$ in $M_{\mathfrak{p}}$, there is some $x \in R \smallsetminus \mathfrak{p}$ so that $xm = 0$, contradicting $\operatorname{ann} m \subseteq \mathfrak{p}$.

2,3. If $f(m) = 0$, then $m/1 \in M_{\mathfrak{p}}$ must be zero because $f_{\mathfrak{p}}(m/1) = 0$ and $f_{\mathfrak{p}}$ are all injective. By part (1), $m = 0$. For (3), use part (1), with $M' = g(N)$.

$$\begin{array}{ccc} M_{\mathfrak{p}} & \xrightarrow{f_{\mathfrak{p}}} & Q_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ M & \xrightarrow{f} & Q \end{array} \qquad \begin{array}{ccc} N_{\mathfrak{p}} & \xrightarrow{g_{\mathfrak{p}}} & M_{\mathfrak{p}} \\ \uparrow & & \uparrow \\ N & \xrightarrow{g} & M \end{array}$$

the "only if" parts are elsewhere □

From now on, assume R is noetherian and M is finitely generated. We will write $I = \operatorname{ann} M$. Let $(B, \leq)$ be a poset. The set of maximal elements of B is denoted B^*. Similarly, B_* is the set of minimal elements.

Example 10.5. $\operatorname{Spec}(R)^* = \operatorname{Max}(R)$ and $\operatorname{Spec}(R)_* = \operatorname{Min}(R)$. Finally, $\mathcal{V}(I)_*$ is the set of minimal primes over R. •

Given R and M as above, we want to study $\operatorname{Ass}(M)^*$ and $\operatorname{Ass}(M)_*$.

Lemma 10.6 (Star Principle)**.** *Let $A \subseteq (B, \leq)$.*

1. *If for every $b \in B$, there is an $a \in A$ so that $b \leq a$, then $A^* = B^*$.*

2. *If for every $b \in B$, there is an $a \in A$ so that $a \leq b$, then $A_* = B_*$.*

Proof. Totally obvious. □

Theorem 10.7. *For the given M, $\operatorname{Ass}(M)^* = \{$point annihilators$\}^* = \{$ideals $\subseteq \mathcal{Z}(M)\}^*$.*

Proof. Clearly $\operatorname{Ass}(M) \subseteq \{\text{point annihilators}\} \subseteq \{\text{ideals} \subseteq \mathcal{Z}(M)\}$. To get the desired conclusion, it suffices to check that every ideal $A \subseteq \mathcal{Z}(M)$ is contained in some associated prime. This is Theorem 10.3. □

How about $\operatorname{Ass}(M)_*$? The following proposition is key.

Proposition 10.8.

1. *Any minimal prime* $\mathfrak{p}$ *over* $I = \operatorname{ann}(M)$ *is in* $\operatorname{Ass} M$.

2. $\operatorname{Ass}(R/I) \subseteq \operatorname{Ass}(M)$.

Proof. (1) By an earlier result, $\mathfrak{p}_\mathfrak{p}$ is a minimal prime over $\operatorname{ann}(M_\mathfrak{p}) \supseteq I_\mathfrak{p}$. Thus, $\mathfrak{p}_\mathfrak{p} \subseteq \mathcal{Z}(M_\mathfrak{p})$ because minimal primes always consist of zero-divisors. Since $M_\mathfrak{p}$ is finitely generated over the noetherian ring $R_\mathfrak{p}$, $\mathfrak{p}_\mathfrak{p}$ must annihilate some nonzero $m/1$. But $\mathfrak{p}_\mathfrak{p}$ is maximal in $R_\mathfrak{p}$, so $\mathfrak{p}_\mathfrak{p} = \operatorname{ann}(m/1)$, so $\mathfrak{p}_\mathfrak{p} \in \operatorname{Ass}(M_\mathfrak{p})$. By 5.5 (3.16), $\mathfrak{p} \in \operatorname{Ass} M$.

(2) Let $\mathfrak{p}_0 \in \operatorname{Ass}(R/I)$. Write $\mathfrak{p}_0 = I : b$ for some $b \notin I$. Look at $N = bM \neq 0$. Then $\operatorname{ann}(N) = \{r \in R | rbM = 0\} = \{r \in R | rb \in I\} = I : b = \mathfrak{p}_0$. Thus, $\mathfrak{p}_0$ is a minimal prime over $\operatorname{ann}(N) = \mathfrak{p}_0$, so it is an associated prime of N. It follows that $\mathfrak{p}_0 \in \operatorname{Ass} M$. □

Theorem 10.9. $\operatorname{Ass}(M)_* = \operatorname{Supp}(M)_* = \mathcal{V}(I)_* = \operatorname{Ass}(R/I)_*$.

Proof. Let $\mathcal{V}(I)_* = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. $\mathcal{V}(I) = \operatorname{Ass}(R/I)_*$ by applying the first equality to $M = R/I$. $\operatorname{Supp} M = \mathcal{V}(I)$, so applying $-_*$ we get the second equality.

It happens that $\operatorname{Ass}(M)_* = \operatorname{Supp}(M)_*$ even if M is not finitely generated. First note that $\operatorname{Ass} M \subseteq \operatorname{Supp} M$. Now we need to show that any supporting prime $\mathfrak{p}$ contains an associated prime. We have that $M_\mathfrak{p} \neq 0$, so $M_\mathfrak{p}$ has an associated prime $(\mathfrak{p}_0)_\mathfrak{p}$ with $\mathfrak{p}_0 \subseteq \mathfrak{p}$ (since $R_\mathfrak{p}$ is noetherian). Since R is noetherian, $\mathfrak{p}_0$ is finitely generated, so $\mathfrak{p}_0 \in \operatorname{Ass} M$. □

Lecture 11

Definition 11.1. $\mathfrak{p} \in \left\{ \begin{array}{c} \operatorname{Ass}(M)_* \\ \operatorname{Ass}(M)^* \\ \operatorname{Ass}(M) \smallsetminus \operatorname{Ass}(M)_* \end{array} \right\}$ is called $\left\{ \begin{array}{c} \textit{isolated} \\ \textit{maximal} \\ \textit{embedded} \end{array} \right\}$.

Example 11.2. Let $R = \mathbb{Z}$ and $M = \mathbb{Z} \oplus \mathbb{Z}/60$. Then $\operatorname{Ass} M = \{(0), (2), (3), (5)\}$, so (0) is an isolated prime, and (2), (3), and (5) are embedded maximal primes. •

Example 11.3. k a field, $R = k[x, y]$, $M = R/I$ for $I = x \cdot (x, y)$. Then $\operatorname{Ass}(R/I) = \{(x), (x, y)\}$, so (x) is an isolated prime and (x, y) is a maximal embedded prime. •

Example 11.4. $R = k[x, y]$, $M = R/I$ with $I = (xy)$. Then $\operatorname{Ass}(R/I) = \{(x), (y)\}$, so both primes are isolated and maximal, and there are no embedded prime. •

If we look at $\operatorname{Ass}(R/I)$, then things are much simpler when I is a radical ideal. By the stuff in lecture 5, all $\mathfrak{p} \in \operatorname{Ass}(R/I)$ are minimal primes over I. Then there cannot be any containments, so $\operatorname{Ass}(R/I)$ has no comparisons as a poset. Therefore, all primes "associated to I" are isolated (there are no embedded primes).

Definition 11.5. The *total ring of quotients* of a commutative ring R, denoted $Q(R)$, is the localization of R at $\mathcal{C}(R)$.

Note that $R \hookrightarrow Q(R)$, and if you invert anything else, you kill stuff.

Theorem 11.6. *A noetherian ring R is reduced if and only if $Q(R)$ is a finite direct product of fields.*

Proof. ($\Leftarrow$) is clear because $R \subseteq Q(R)$, and $Q(R)$ is reduced.

($\Rightarrow$) $\mathcal{Z}(R) = \mathfrak{p}_1 \cup \cdots \mathfrak{p}_n$ where $\mathfrak{p}_i$ are the minimal primes, so $Q(R)$ is the semi-localization of R at these primes. Since R is reduced, $\bigcap \mathfrak{p}_i = \sqrt{(0)} = (0)$. So $Q(R)$ is semi-local, with maximal ideals $\mathfrak{P}_1$, $\ldots$, $\mathfrak{P}_n$. Since $\bigcap \mathfrak{p}_i = (0)$, we also get $\bigcap \mathfrak{P}_i = (0)$. To see this, assume $x \in \bigcap \mathfrak{P}_i$, then $x = \frac{p_i}{s_i}$ for each i. Then $s_1 \cdots s_n x \in \mathfrak{p}_i$ for each i, so it is zero. Since each s_i is regular, we get $x = 0$. Then we get

$$Q(R)/(0) \cong \prod Q(R)/\mathfrak{P}_i$$

so $Q(R)$ is a finite direct product of fields. □

Example 11.7. If R is not noetherian, the result fails. Let $R = k \times k \times \cdots$. Then R is reduced and von Neumann regular, so it is zero-dimensional, so $C(R) = U(R)$. In particular $Q(R) = R$, which is not a finite product of fields. •

Definition 11.8. A prime filtration of a module M is a finite filtration where each consecutive quotient is $R/\mathfrak{p}$.

Theorem 11.9. *A finitely generated module M over a noetherian ring R has a prime filtration. Furthermore,* $\mathrm{Ass}(M)_* = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}_*$*, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ are the primes occurring in the filtration.*

Proof. Go from the bottom and use the fact that (over a noetherian ring) every non-zero module has an associated prime. $R/\mathfrak{p}_1 \hookrightarrow M$, then $R/\mathfrak{p}_2 \hookrightarrow M/(R/\mathfrak{p}_1)$, etc.

Finally, apply the Star principle to the containment $\mathrm{Ass}(M) \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\} \subseteq \mathrm{Supp}(M)$. We already saw that any supporting prime contains an associated prime. □

Lecture 12

picture of history

Useful mnemonics (6.9):

$$\bigcap\{\mathfrak{p} \in \operatorname{Ass}(M)_*\} = \sqrt{\operatorname{ann}(M)} \subseteq \mathcal{Z}(M) = \bigcup\{\mathfrak{p} \in \operatorname{Ass}(M)^*\}$$

where the equalities require all noetherian hypotheses (though the containment is true in general).

Definition 12.1 (Lasker, 1905)**.** An ideal $\mathfrak{q} \subsetneq R$ is *primary* if $ab \in \mathfrak{q}$ and $b \notin \mathfrak{q}$ implies that $a^n \in \mathfrak{q}$ for some n.

We'd like to do primary decomposition for modules because it doesn't cost any more work, so we need to generalize this definition.

Definition 12.2. If M is an R-module. We call a submodule $Q \subsetneq M$ *primary* (in M) if $\sqrt{\operatorname{ann}(M/Q)} = \mathcal{Z}(M/Q)$ (you get "$\subseteq$" for free). i.e. for every $a \in R$ and $x \in M \smallsetminus Q$ with $ax \in Q$, we have $a^n M \subseteq Q$ for some n.

Warning 12.3. This definition is not completely standard in the literature, and the fact that M/Q may not be finitely generated often mucks things up.

Proposition 12.4. *Suppose $Q \subsetneq M$ is primary. Then $\mathfrak{q} := \operatorname{ann}(M/Q)$ is a primary ideal, and $\mathfrak{p} := \sqrt{\mathfrak{q}}$ is prime.*

Proof. Clearly $\mathfrak{q} \subsetneq R$ since $1 \in R \smallsetminus \mathfrak{q}$. Let $a, b \in R$, with $ab \in \mathfrak{q}$ and $b \notin \mathfrak{q}$. Then $abM \subseteq Q$ but $bM \not\subseteq Q$. So $a \in \mathcal{Z}(M/Q) = \sqrt{\operatorname{ann}(M/Q)}$ (since $Q \subsetneq M$ is primary), so $a^n \in \mathfrak{q}$ for some n.

Finally, we check that $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is prime. Let $ab \in \mathfrak{p}$ with $b \notin \mathfrak{p}$. Then we have $a^n b^n \in \mathfrak{q}$ and $b^n \notin \mathfrak{q}$. Since $\mathfrak{q}$ is primary, $(a^n)^N \in \mathfrak{q}$ for some N, so $a \in \mathfrak{p}$, as desired. □

Definition 12.5. Henceforth we will say that Q is $\mathfrak{p}$*-primary.*

Proposition 12.6. *If $Q, Q' \subsetneq M$ are both $\mathfrak{p}$-primary, then $Q \cap Q'$ is $\mathfrak{p}$-primary.*

Proof. Let $\mathfrak{q} = \operatorname{ann}(M/Q)$, $\mathfrak{q}' = \operatorname{ann}(M/Q')$, and assume $a \in \mathcal{Z}\big(M/(Q \cap Q')\big)$, with $ax \in Q \cap Q'$, where $x \notin Q \cap Q'$. We may assume $x \notin Q$. Then $a \in \mathcal{Z}(M/Q)$, so $a \in \sqrt{\mathfrak{q}} = \mathfrak{p} = \sqrt{\mathfrak{q}'}$ since Q is primary. Then $a^n M \subseteq Q \cap Q'$ for some n, as desired. □

Proposition 12.7. *Let R be a noetherian ring, and let $Q \subsetneq M$ with M/Q finitely generated. Then $Q \subsetneq M$ is primary if and only if $|\operatorname{Ass}(M/Q)| = 1$. In fact, if Q is $\mathfrak{p}$-primary, then $\operatorname{Ass}(M/Q) = \{\mathfrak{p}\}$.*

Proof. ($\Rightarrow$) For this direction, we don't use that M/Q is finitely generated. We know that $\mathrm{Ass}(M/Q) \neq \varnothing$ since R is noetherian. Let $P \in \mathrm{Ass}(M/Q)$, then $P \supseteq \mathrm{ann}(M/Q) =: \mathfrak{q}$, so $P \supseteq \sqrt{\mathfrak{q}} =: \mathfrak{p}$. On the other hand, if $a \in P$, then $a = \mathrm{ann}(m)$, so $a \in \mathcal{Z}(M/Q) = \sqrt{\mathfrak{q}} = \mathfrak{p}$. So $P = \mathfrak{p}$.

($\Leftarrow$) Say $\mathrm{Ass}(M/Q) = \{\mathfrak{P}\}$. Then we get

$$\begin{aligned}\mathcal{Z}(M/Q) &= \bigcup\{P \in \mathrm{Ass}(M/Q)^*\} \\ &= \mathfrak{P} \\ &= \bigcap\{P \in \mathrm{Ass}(M/Q)_*\} \\ &= \sqrt{\mathrm{ann}(M/Q)}.\end{aligned}$$

□

Definition 12.8. A module $Q \subsetneq M$ is called *irreducible* if it cannot be written as the intersection of two strictly larger submodules.

Lemma 12.9 (Noether's Lemma)**.** *Suppose M is a noetherian module over a ring R. Then any $Q \subseteq M$ is a finite intersection of irreducible submodules.*

Proof. Noetherian induction. If all submodules containing Q are finite intersections of irreducibles, then so is Q. □

Theorem 12.10 (Noether's Theorem)**.** *Say R is noetherian and M/Q is finitely generated. If Q is irreducible, then Q is primary.*

Proof. Assume $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Ass}(M/Q)$. Say $R/\mathfrak{p}_i \cong K_i/Q \subseteq M/Q$ for $i = 1, 2$. If $Q \subsetneq K_1 \cap K_2$, then there is some $x \in K_1 \cap K_2 \smallsetminus Q$, which gives a non-zero element of $K_i/Q \subseteq M/Q$. But then the annihilator of x in M/Q must be $\mathfrak{p}_i$ (since $K_i/Q \cong R/\mathfrak{p}_i$), so $\mathfrak{p}_1 = \mathfrak{p}_2$, which would imply that Q is primary.

Thus, we may assume $Q = K_1 \cap K_2$. [[★★★ finish]] □

Definition 12.11. Suppose $N \subsetneq M$. Then an equality of the form $N = Q_1 \cap \cdots \cap Q_n$ is called a *primary decomposition of N* if Q_i is $\mathfrak{p}_i$-primary, with all of the $\mathfrak{p}_i$ distinct. This decomposition is called *minimal* (or *irreducible*) if no Q_i can be omitted.

Note that the decomposition if minimal exactly when $\bigcap_{i \neq j} Q_j \not\subseteq Q_i$ for each i.

Lecture 13

Example 13.1.

1. Prime ideals are primary.
2. In a rad-nil local ring (0-dimensional local ring), any proper ideal is primary. As a consequence, if $\mathfrak{m} \in \operatorname{Max} R$ for any ring R, and $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$, then $\mathfrak{q}$ is $\mathfrak{m}$-primary.
3. In a UFD, a principal ideal (a) is primary if and only if a is 0 or a power of an irreducible element; see Ex. 52.
4. In $R = k[x, y]$, where k is a field. Then $I = (x^2, xy)$ is *not* primary. In the factor ring, y is a zero-divisor because $xy \in I$, but y is not nilpotent modulo I.
5. Let $\mathfrak{q} = (y^2, x + yz) \lhd k[x, y, z]$. We claim that $\mathfrak{q}$ is $\mathfrak{p}$-primary for $\mathfrak{p} = (x, y)$. First check that $\mathfrak{p} = \sqrt{\mathfrak{q}}$. $R/\mathfrak{q} = k[x, y, z]/(y^2, x + yz) \cong k[y, z]/(y^2)$, in which every zero-divisor is nilpotent because (y^2) is primary in $k[y, z]$. •

Theorem 13.2 (Lasker-Noether Primary Decomposition)**.** *Let R be noetherian and $N \subsetneq M$, with M/N finitely generated. Then N has a minimal primary decomposition in M.*

Proof. First write $N = Q_1 \cap \cdots \cap Q_n$, where the Q_i are irreducible. By Noether's theorem, each Q_i is $\mathfrak{p}_i$-primary for some prime $\mathfrak{p}_i$.

If $\mathfrak{p}_i = \mathfrak{p}_j$, we may replace Q_i and Q_j by $Q_i \cap Q_j$, which is also $\mathfrak{p}_i$-primary. Now we may assume the $\mathfrak{p}_i$ are distinct.

Now remove unneeded Q_i until we have a minimal decomposition. □

What can we say about uniqueness? Recall some facts about localization of modules at a multiplicative set $S \subseteq R$.

Definition 13.3. The *S-saturation of Q* is $\{m \in M | sm \in Q \text{ for some } s \in S\}$.

▶ **Exercise 13.1.** The saturation of Q is Q^{ec}, the contraction of the extension of Q, i.e. "$Q_S \cap M$"$= i^{-1}(Q_S)$, where $i : M \to M_S$.

Lemma 13.4. *$Q \subsetneq M$. Suppose $S \cap \mathcal{Z}(M/Q) = \varnothing$, then $Q^{ec} = Q$.*

Proof. if $m \in Q^{ec}$, then $sm \in Q$ for some $s \in S$, which implies $m \in Q$ since $s \notin \mathcal{Z}(M/Q)$. The reverse inclusion is clear. □

We will apply this to the situation where Q is a $\mathfrak{p}$-primary submodule of M and $S = R \setminus \mathfrak{p}$.

Theorem 13.5 (Main Uniqueness Theorem)**.** *Same hypotheses as in the Lasker-Noether Theorem. Let $N = Q_1 \cap \cdots \cap Q_n$ be* any *minimal primary decomposition, where Q_i is $\mathfrak{p}_i$-primary. Then*

1. $\mathrm{Ass}(M/N) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. *In particular, all the $\mathfrak{p}_i$ are uniquely determined (up to permutation).*
2. *If $\mathfrak{p} \in \mathrm{Ass}(M/N)_*$ is an isolated prime, then $Q_i = N^{ec}$ (with respect to localization at $\mathfrak{p}_i$). In particular, Q_i is uniquely determined.*

Proof.

1. $M/N \hookrightarrow \bigoplus M/Q_i$, so $\mathrm{Ass}(M/N) \subseteq \bigcup \mathrm{Ass}(M/Q_i) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Now let's show that $\mathfrak{p}_1 \in \mathrm{Ass}(M/N)$. Fix $x \in (Q_2 \cap \cdots \cap Q_n) \smallsetminus Q_1$ (such an x exists by minimality of the decomposition). Since $\mathfrak{p}_1$ is finitely generated (R noetherian), $\mathfrak{p}_1^{k+1} x \subseteq Q_1$ for some $k \gg 1$; choose the minimal such k. Then there is some $y \in \mathfrak{p}_1^k x \smallsetminus Q_1$. Then we have $\bar{y} \in M/N$ is non-zero, and that $\mathfrak{p}_1 y = 0 \in M/N$, so $\mathfrak{p}_1 \subseteq \mathrm{ann}(\bar{y})$. For the reverse inclusion, suppose $r\bar{y} = 0$, so $ry \in N \subseteq Q_1$. Thus, $r \in \mathcal{Z}(M/Q_1) = \mathfrak{p}_1$.
2. Let $\mathfrak{p} = \mathfrak{p}_i$ be an isolated prime. By assumption, $\mathfrak{p}_j \not\subseteq \mathfrak{p}$ for $j \neq i$. Choose k large enough so that $\mathfrak{p}_j^k M \subseteq Q_j$ (for $j \neq i$) (M/N finitely generated). But $\mathfrak{p}_j^k \not\subseteq \mathfrak{p}$. Now consider localization at $\mathfrak{p}$; we get $(\mathfrak{p}_j)_{\mathfrak{p}}^k M_{\mathfrak{p}} = M_{\mathfrak{p}} = (Q_j)_{\mathfrak{p}}$ for each $j \neq i$. Localizing the equation $N = Q_1 \cap \cdots \cap Q_n$, we get

$$N_{\mathfrak{p}} = (Q_1 \cap \cdots \cap Q_n)_{\mathfrak{p}} = \bigcap_j (Q_j)_{\mathfrak{p}} = (Q_i)_{\mathfrak{p}}.$$

   So we get $N^{ec} = Q_i^{ec} = Q_i$. □

Example 13.6 (A point from last time)**.** The $\mathfrak{p}_i$ being distinct doesn't guarantee minimality of the decomposition. If $N = Q_1 \cap Q_2 \cap Q_3$. Choose some $\mathfrak{p}$ containing $\bullet$

Lecture 14

Combining Theorem 5.5 and Proposition 10.8, we have that $\operatorname{Ass}(R/I) = \operatorname{Spec}(R/I)_*$, i.e. R/I has no embedded primes.

Example 14.1 (Nonuniqueness of minimal primary decomposition (Noether))**.** We saw last time that primary components at isolated primes are unique, but at embedded primes, we don't have uniqueness. Take $R = k[x, y]$ where k is a field. Let $I = x \cdot (x, y)$, then $\operatorname{Ass}(R/I) = \{\mathfrak{p}_1 = (x), \mathfrak{p}_2 = (x, y)\}$. $\mathfrak{p}_1$ is isolated and $\mathfrak{p}_2$ is embedded.

Let's find some primary decompositions $I = \mathfrak{q}_1 \cap \mathfrak{q}_2$. The $\mathfrak{q}_1$ should be unique since $\mathfrak{p}_1$ is isolated: $\mathfrak{q}_1$ is the saturation of I with respect to localization at $\mathfrak{p}_1$. Since $xy \in I$, but $y \notin \mathfrak{p}_1$, so $x \in I^{ec}$, so $I^{ec} = (x) = \mathfrak{q}_1$.

Take $\mathfrak{q}_{2,a} := (x^2, y + ax) \supseteq (x, y)^2 = \mathfrak{p}_2^2$, so it is $\mathfrak{p}_2$-primary. Clearly $I \subseteq \mathfrak{q}_1 \cap \mathfrak{q}_{2,a}$. To see that this is an equality, assume $g_0 x = g_1 x^2 + g_2(y + ax)$, then $x | g_2$ since we are in a UFD; but then $f \in I$, a contradiction.

Finally, to contradict uniqueness, we must show that $\mathfrak{q}_{2,a} \neq \mathfrak{q}_{2,b}$ for $a \neq b$. If $\mathfrak{q}_{2,a} = \mathfrak{q}_{2,b}$, then $\mathfrak{q}_{2,a}$ contains $(b - a)x$, so it contains x. But $R/\mathfrak{q}_{2,a} \cong k[x]/(x^2)$, so $x \notin \mathfrak{q}_{2,a}$.

We could have also chosen $\mathfrak{q}_2 = (x^2, xy, y^\mu)$ for $\mu \geq 2$. This way, we get infinite non-uniqueness even if the ground field is not infinite. •

Example 14.2. Here are some example types:

1. I is primary, so $I = I$ is a MPD.
2. R a UFD, and $(a) \neq (0)$. Then factor a into irreducibles $u\pi_1^{r_1} \cdots \pi_n^{r_n}$, then $(a) = \bigcap(\pi_i^{r_i})$ by CRT. Each $(\pi_i^{r_i})$ is (π_i)-primary, and (π_i) is an isolated prime.
3. If R is a Dedekind domain and $\mathfrak{a} \subseteq R$ is an ideal. Then we get $\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n} = \bigcap \mathfrak{p}_i^{r_i}$ by CRT.

•

Example 14.3. To appreciate machine computation, try doing the following by hand: $R = \mathbb{Q}[x, y]$ and $I = \left(x^2 - (y + 1)^3, (y^2 - 1)^2\right)$. Then $\mathfrak{p}_1 = (x^2 - 8, y - 1)$ and $\mathfrak{p}_2(x, y + 1)$, which are maximal (so they are both isolated since they are not comparable). The primary components are $\mathfrak{q}_1 = \left(x^2 - 12y + 4, (y - 1)^2\right)$ and $\mathfrak{q}_2 = \left(x^2, (y + 1)^2\right)$. •

Theorem 14.4. *If R is noetherian, and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is any MPD. Then $I = \sqrt{I}$ if and only if $\mathfrak{q}_1 = \mathfrak{p}_i$ for all i. In this case, $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are exactly the minimal primes over I; in particular, the MPD is unique (up to permutation).*

Proof. ($\Leftarrow$) Clear.

($\Rightarrow$) Assume $I = \sqrt{I}$. By (6.12 Lam), MPD is unique (there are no embedded primes). But we know that $\operatorname{Ass}(R/I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, the set of minimal primes over I. However, $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_n$ since I is radical. By uniqueness of the decomposition, $\mathfrak{q}_i = \mathfrak{p}_i$ □

Remark 14.5 (Non-existence of MPD). Let R be von Neumann regular. Observe that every ideal is radical since $a^2 \in I \Rightarrow a = a^2 x \in I$. It follows that every primary ideal is prime. Take, for example, $R = k \times k \times \cdots$. Then the zero ideal has no primary decomposition: otherwise we would have $(0) = \mathfrak{p}_1 \cap \cdots \mathfrak{p}_n$, which would imply that $\operatorname{Ass} R \subseteq \{\mathfrak{p}_1, \cdots, \mathfrak{p}_n\}$, which is false because $\operatorname{Ass} R$ is infinite.

§8 More Theorems on Noetherian Rings

Theorem 14.6 (Krull's Intersection Theorem, preliminary version)**.** *Let I is an ideal in a noetherian ring R, and M is a finitely generated module. Define $N := \bigcap_{n=0}^{\infty} I^n M$. Then $I \cdot N = N$.*

There will be a very slick proof in the notes. Here is another one.

Proof. Assume $IN \subsetneq N$. Take a MPD for IN as a submodule of M, say $IN = Q_1 \cap \cdots \cap Q_n$, where Q_i is $\mathfrak{p}_i$-primary. Then $N \not\subseteq Q_i$ for some i. Then $\operatorname{Ass}\big((N + Q_i)/Q_i\big) \subseteq \operatorname{Ass}(M/Q_i) = \{\mathfrak{p}_i\}$, so we must have equality because over a noetherian ring, associated primes exist. Choose k such that $\mathfrak{p}_i^k M \subseteq Q_i$ (since $\mathfrak{p}_i$ is finitely generated). Then $I \cdot \left(\frac{N+Q_i}{Q_i}\right) = 0$, so $I \subseteq \operatorname{ann}\left(\frac{N+Q_i}{Q_i}\right) \subseteq \mathfrak{p}_i$. But $N \subseteq I^k M$ by definition of N, and $I^k M \subseteq \mathfrak{p}_i^k M \subseteq Q_i$. Contradiction. □

Lecture 15

In exercise I.67, "$(x,y)^2$" should be "$(x_1,x_2)^2$".

Example 15.1. Let $I = (x^2-yz, x(z-1)) \triangleleft k[x,y,z]$. Then $\mathfrak{p}_1 = (x,z) = I : y(z-1)$, $\mathfrak{p}_2 = (x,y) = I : z(z-1)$, $\mathfrak{p}_3 = (x^2-y, z-1) = I : x$, and $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3$. In particular, I is radical. •

We want to understand what $IN = N$ means.

Let $I \triangleleft R$ and ${}_RM$ finitely generated. Let $E = \mathrm{End}_R(M)$, which is not commutative in general. We may view M as an E-module ${}_EM$. Since every element in R commutes with all of E, E is an R-algebra (i.e. There is a homomorphism $R \to E$ sending R into the center of E).

Lemma 15.2 (Determinant Trick)**.**

1. *Every $\phi \in E$ such that $\phi(M) \subseteq IM$ satisfies a monic equation of the form $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$, where each $a_i \in I$, i.e. ϕ is "integral over I".*
2. *$IM = M$ if and only if $(1-a)M = 0$ for some $a \in I$.*

Proof. (1) Fix a finite set of generators, $M = Rm_1 + \cdots + Rm_n$. Then we have $\phi(m_i) = \sum_j a_{ij}m_j$, with $a_{ij} \in I$ by assumption. Let $A = (a_{ij})$. Then these equations tell us that $(I\phi - A)\vec{m} = 0$. Multiplying by the adjoint of the matrix $I\phi - A$, we get that $\det(I\phi - A)m_i = 0$ for each i. It follows that $\det(I\phi - A) = 0 \in E$. But $\det(I\phi - A) = \phi^n + a_1\phi^{n-1} + \cdots + a_n$ for some $a_i \in I$.

(2) The "if" part is clear. The "only if" part follows from (1), applied to $\phi = \mathrm{Id}_M$. □

Remark 15.3. Determinant trick (part 2) actually includes Nakayama's Lemma, because if I is in $\operatorname{rad} R$, $(1-a)$ is a unit, so $M = (1-a)M = 0$.

Corollary 15.4. *For a finitely generated ideal $I \triangleleft R$, $I = I^2$ if and only if $I = eR$ for some $e = e^2$.*

Proof. ($\Leftarrow$) clear.

($\Rightarrow$) Apply determinant trick (part 2) to the case $M = {}_RI$. We get $(1-e)I = 0$ for some $e \in I$, so $(1-e)a = 0$ for each $a \in I$, so $a = ea$, so I is generated by e. Letting $a = e$, we see that e is idempotent. □

Corollary 15.5 (Vasconcelos-Strooker Theorem)**.** *For any finitely generated module M over* any *commutative R. If $\phi \in \mathrm{End}_R(M)$ is onto, then it is injective.*

Proof. We can view M as a module over $R[t]$, where t acts by ϕ. Apply the determinant trick (part 2) to $I = t \cdot R[t] \subseteq R[t]$. We have that $IM = M$ because ϕ is surjective, so $m = \phi(m_0) = t \cdot m_0 \in IM$. It follows that there is some $th(t)$ such that $(1 - th(t))M = 0$. In particular, if $m \in \ker\phi$, we have that $0 = (1-h(t)t)m = 1 \cdot m = m$, so ϕ is injective. □

Now we can make Krull's intersection theorem more impressive:

Theorem 15.6 (Krull's Intersection Theorem)**.** *Let M be finitely generated over a noetherian ring R, and let $I \lhd R$ be an ideal. Define $N = \bigcap_{n\geq 0} I^n M$. Then $N = \{m \in M | (1-a)m = 0$ for some $a \in I\}$.*

Proof. The inclusion $\supseteq$ is trivial since $m = am = a^2m = \cdots \in I^n M$ for each n. The other inclusion follows from the preliminary version and the determinant trick (part 2), noting that N remains finitely generated. □

Here are some special cases of the Krull intersection theorem.

Corollary 15.7. *If $I \lhd R$ is a proper ideal in a noetherian domain, then $\bigcap_{n\geq 0} I^n = 0$.*

Proof. The set $1 - I$ consists of non-zero elements, and hence non-zero-divisors. Apply Krull to $M = R$. □

Corollary 15.8. *Let M be finitely generated over a noetherian ring R. Let $J \subseteq \operatorname{rad} R$. Then $\bigcap_{n\geq 0} J^n M = 0$.*

Proof. Again, $1 - J$ consists of units. □

Lecture 16

Exercise 68: You should assume that the characteristic of k is not 2.
Exercise 71: A non-Marot ring example.

The easy form of Krull's intersection theorem is: If $(R, \mathfrak{m})$ is local noetherian and M is finitely generated, then $\bigcap_{n\geq 0} \mathfrak{m}^n M = 0$.

Example 16.1. Counterexample if R is not noetherian. Let $R = \mathbb{Q}[x_1, x_2, \dots]/(x_{i+1}^2 = x_i, x_1 = 0)$, with $\mathfrak{m} = (x_1, x_2, x_3, \dots)$. Then $\mathfrak{m} = \mathfrak{m}^2 = \mathfrak{m}^3 = \cdots$, so $\bigcap \mathfrak{m}^n = \mathfrak{m} \neq 0$. •

Example 16.2. Counterexample if M is not finitely generated. Let $R = \mathbb{Z}_{(p)}$, which is local with maximal ideal $p\mathbb{Z}_{(p)}$. Take $M = {}_R\mathbb{Q}$, which is not finitely generated. Then we get that $\mathfrak{m}M = pR \cdot M = p\mathbb{Q} = \mathbb{Q} = M$, so $\bigcap \mathfrak{m}^n M = M \neq 0$. •

Next we study a class of rings studied by Jean Marot (french guy). Recall that $\mathcal{C}(R)$ is the set of non-zero-divisors. These elements are called regular.

Definition 16.3. An ideal I is *regular* if I contains a regular element.

Definition 16.4. A ring R is *Marot* if every regular ideal can be generated by regular elements. (i.e. a regular ideal I is generated by $I \cap \mathcal{C}(R)$.)

Note that this class of rings includes integral domains (regular is the same as non-zero). Also, rings R such that $\mathcal{C}(R) = U(R)$ are Marot (the only regular ideal is all of R). For example, zero-dimensional rings have this property. In particular, artinian rings are zero-dimensional.

Definition 16.5. R has *few zero divisors* if $\mathcal{Z}(R)$ is a finite union of primes.

Lemma 16.6. *Let R be a ring with few zero divisors. Then for any $a \in R$ and any $b \in \mathcal{C}(R)$, there is some $r \in R$ such that $a + br \in \mathcal{C}(R)$. (i.e. every coset of bR intersects $\mathcal{C}(R)$, provided b is regular.)*

Proof. Write $\mathcal{Z}(R) = \bigcup_{i=1}^n \mathfrak{p}_i$. We may assume there are no inclusions among the $\mathfrak{p}_i$. After relabelling, we may assume that $a \in \mathfrak{p}_i$ for $i \leq k$ and $a \notin \mathfrak{p}_i$ for $i > k$. We may assume $k \neq 0$, lest a be regular, in which case $r = 0$ works.

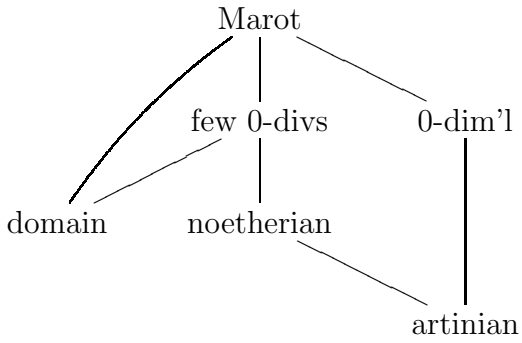
If $\bigcap_{i=1}^k \mathfrak{p}_i \smallsetminus \bigcup_{j=k+1}^n \mathfrak{p}_j = \varnothing$, then by prime avoidance, there is some j such that $\bigcap_i \mathfrak{p}_i \subseteq \mathfrak{p}_j$. Then since $\mathfrak{p}_j$ is prime, we get $\mathfrak{p}_i \subseteq \mathfrak{p}_j$ for some i, contradicting the fact that there are no inclusions among the $\mathfrak{p}$'s.

Thus, we may choose $r \in \bigcap_{i=1}^k \mathfrak{p}_i \smallsetminus \bigcup_{j=k+1}^n \mathfrak{p}_j$, so $r \in \mathfrak{p}_i$ exactly when $a \notin \mathfrak{p}_i$. Then we get $a + rb \in \mathcal{C}(R)$. □

Theorem 16.7. *Noetherian ⇒ few zero divisors ⇒ Marot.*

Proof. If R is noetherian, then $\mathcal{Z}(R)$ is the union of the finitely many "maximal primes", $\bigcup_{\mathfrak{p}\in \mathrm{Ass}(R)^*} \mathfrak{p}$.

If $b \in I \cap \mathcal{C}(R)$, and $a \in I$, then by the Lemma, we get some r_a so that $c_a = a + r_a b \in \mathcal{C}(R) \cap I$. Then I is clearly generated by b, together with all the c_a. □



None of these implications is reversible. It doesn't take much thought to produce examples to demonstrate this.

Proposition 16.8. *Suppose R is Marot, and $I \triangleleft R$ is a proper regular ideal. Assume*

$$\text{for every } a, b \in \mathcal{C}(R), \qquad ab \in I \Rightarrow a \in I \text{ or } b \in I \tag{$*$}$$

Then I is prime.

Proof. Assume I is not prime, with $x, y \notin I$, but $xy \in I$. Then $I + (x) \supsetneq I$ is regular as well, so it is generated by regular elements. Those generators cannot all lie in I, so there is some generator $a \notin I$. Similarly, there is some regular generator $b \in (I + (y)) \smallsetminus I$. Then $ab \in (I + (x))(I + (y)) \subseteq I$, contradicting $(*)$. □

Theorem 16.9 (E. D. Davis)**.** *A commutative ring R has few zero divisors if and only if the total ring of quotients $Q(R)$ is a semi-local ring. In particular, if R is noetherian, $Q(R)$ is semi-local.*

Proof. ($\Rightarrow$) Write $\mathcal{Z}(R) = \bigcup_{i=1}^{n} \mathfrak{p}_i$, with no inclusions among the $\mathfrak{p}_i$. Then $Q(R)$ is the localization at the complement of this set, which is the semi-localization of R at this finite set of primes, so $Q(R)$ is semi-local.

($\Leftarrow$) Assume $Q(R)$ is semi-local, with $\mathrm{Max}(Q(R)) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$. Form the contractions $\mathfrak{p}_i = \mathfrak{m}_i \cap R$ (recall that $R \hookrightarrow Q(R)$). We claim that each $\mathfrak{p}_i$ consists of zero-divisors; otherwise, $\mathfrak{p}_i$ would contain a regular element, which would become a unit upon localization. Now we will show that $\mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_n \subseteq \mathcal{Z}(R)$ is an equality. If $r \in \mathcal{Z}(R)$, then $r \cdot a = 0$ for some $a \neq 0$, so $rQ(R) \neq Q(R)$, so $r \in \mathfrak{m}_i$ for some i. Then $r \in \mathfrak{p}_i$, as desired. □

Lecture 17

Chapter II. Affine Varieties and the Nullstellensatz ("NSS")

§1. Affine algebraic sets
§2. General Topology
§3. Zariski Prime Spectrum
§4. Hilbert's Nullstellensatz

Proposition 17.1 ("Going Up"). *Let $R \subseteq S$ be commutative rings with unit, and let S be finitely generated as an R-module. Then if R is noetherian, so is S.*

Proof. ${}_RS$ is a noetherian, so ${}_SS$ is noetherian, i.e. S is noetherian as a ring. □

Theorem 17.2 (Eakin-Nagata-(Formanek)[1], "Going Down"). *The converse of the above proposition is true.*

§1. Affine algebraic sets

We fix some fields $k \subseteq K$, fix $A = k[x_1, \ldots, x_n]$, and let K^n be n-space over K.

Let $S \subseteq A$ be a subset. Define $V_K(S) = \{a \in K^n | f(a) = 0 \text{ for all } f \in S\}$; we call this an algebraic k-set. Clearly, we may replace S by the ideal it generates, so we will always take S to be an ideal. Since A is noetherian, S is always finitely generated.

On the other hand, if $Y \subseteq K^n$ is a subset, then we can define $I(Y)$, the ideal in A of functions vanishing on Y. Note that $I(Y)$ is always a radical ideal.

Both directions are inclusion-reversing. We always have $Y \subseteq V_K\big(I(Y)\big)$, trivially. Equality holds if and only if $Y = V_k(\text{something})$. It is also clear that $J \subseteq I\big(V_K(J)\big)$. Equality holds if and only if $J = I(\text{something})$.

Definition 17.3. The *Zariski k-topology* on K^n has closed sets of the form $V_K(J)$.

In this topology, the k-points are closed because $(a_1, \ldots, a_n)$ is the vanishing set of $(x_1 - a_1, \ldots, x_n - a_n) \lhd A$. You get a topology because $\bigcap_i V_K(J_i) = V_K\big(\sum_i J_i\big)$ (this is an arbitrary intersection!) and $V_K(J_1) \cup V_K(J_2) = V(J_1 \cap J_2)$.

1. If $Y \subseteq K^n$ is a subset, then the closure of Y is $V_K\big(I(Y)\big)$.
2. If $J \lhd A$, then $\sqrt{J} \subseteq I\big(V_K(J)\big)$. In general, this is not an equality.

Theorem 17.4 (Hilbert's Nullstellensatz). *If $\bar{k} \subseteq K$, then $\sqrt{J} = I\big(V_K(J)\big)$.*

We will prove this theorem in §4.

The problem with general $k \subseteq K$ is as follows.

[1] Formanek did something that works for non-commutative rings.

Example 17.5. Let $k = K = \mathbb{R}$ and $J = (x^2 + y^2)$. Then J is a prime ideal, so $J = \sqrt{J}$. However, $V_K(J) = \{(0,0)\}$, so $I\big(V_K(J)\big) = (x, y)$, which is strictly larger than $\sqrt{J}$.

Even worse, if $J = (x^2 + y^2 + 1)$, then J is still radical, but $V_K(J) = \varnothing$, so $I\big(V_K(J)\big) = A$. •

Definition 17.6. An *affine k-algebra* is a finitely generated (as an algebra) commutative k-algebra. (i.e. these are homomorphic images of $k[x_1, \ldots, x_n]$)

By the Hilbert basis theorem, affine k-algebras are always noetherian.

Definition 17.7. If Y is a k-algebraic set in K^n, then the *k-coordinate ring $k[Y]$ of Y* is $A/I(Y)$.

Since $I(Y)$ is always radical, $k[Y]$ is always reduced.

Definition 17.8. An algebraic k-set Y is *k-irreducible* if it is non-empty and cannot be written as the union of two proper closed subsets. We also call Y a *variety*.

Proposition 17.9. *A k-algebraic set $Y \subseteq K^n$ is irreducible if and only if $I(Y)$ is prime if and only if $k[Y]$ is a domain.*

In this case, we define $k(Y) = Q(k[Y])$ to be the function field of Y.

Warning 17.10. If you start with $J \in \operatorname{Spec} A$, $V_K(J)$ need not be a variety!

Example 17.11. Let $k = K = \mathbb{F}_2$ and let $J = (x + y)$, which is prime.

Then $V_K(J) = \{(0,0), (1,1)\}$, which is not irreducible since K^2 is discrete! In particular, $I\big(V_K(J)\big) = (x, y) \cap (x + 1, y + 1) \supsetneq J$. •

§2. General Topology

Proposition 17.12. *For a topological space X, the following are equivalent.*

1. *Open sets in X satisfy ACC.*
2. *Every non-empty family of open sets has a maximal member.*
3. *Every non-empty family of closed sets has a minimal member.*
4. *Closed sets in X satisfy DCC.*

Proof. Easy. □

Definition 17.13. If any of the above hold, we call X *noetherian*.

Proposition 17.14. *Noetherian spaces are compact.*

Proof. Given a cover of a noetherian space X, consider the family of finite unions. There is a maximal member, which must cover all of X by maximality. □

Corollary 17.15. *For $k \subseteq K$, every k-algebraic set, with the Zariski topology, is noetherian and hence compact.*

Proof. Since A is noetherian, K^n is noetherian as a topological space. Finally, closed subsets of noetherian spaces are noetherian. □

Lecture 18

noetherian $\Rightarrow$ subspaces are noetherian $\Rightarrow$ subspaces are compact. If $K \supseteq k$, then the k-topology on K^n is noetherian (hence compact).

Proposition 18.1. *If X is a non-empty topological space, then the following are equivalent.*

1. *X is not the union of two proper closed subsets.*
2. *Any two non-empty open sets intersect.*
3. *Any non-empty open set is dense in X.*

Proof. easy exercise. □

In this case, we call X *irreducible*. In particular, "irreducible subspace" is meaningful (a subspace which is irreducible in the subspace topology).

Corollary 18.2. *$Y \subseteq X$ is an irreducible subspace if and only if $\overline{Y}$ is irreducible.*

Proof. Follows from the fact that an open set intersects Y is and only if it intersects $\overline{Y}$. □

Example 18.3. Singleton subspaces (and therefore their closures) are irreducible. •

Definition 18.4. A maximal irreducible subset Y of X is called an *irreducible component* of X.

Such a Y is always closed because $Y \subseteq \overline{Y}$, which is irreducible, so by maximality, $Y = \overline{Y}$.

Proposition 18.5.
1. *Any irreducible set in X is contained in some irreducible component.*
2. *X is the union of its irreducible components.*

Proof. (1) Zorn's Lemma. (2) Every point is in some irreducible component by (1). □

Note that in a Hausdorff space, any two points are separated by open sets, so they cannot be in an irreducible component together, i.e. only irreducible sets are points.

Theorem 18.6. *If X is noetherian, then the number of irreducible components is finite. If $\{X_i\}$ are the irreducible components, all of them are needed to cover X.*

Proof. If X_i can be omitted, it is contained in the remaining union, so it must be contained in one of the other components (since it is irreducible), contradicting the fact that it is a maximal irreducible set.

[[★★★]] □

Theorem 18.7. *Given $k \subseteq K$, let $X \subseteq K^n$ be a k-algebraic set. The irreducible components of X (in the k-topology) are given by $V_K(\mathfrak{p}_i)$, where the $\mathfrak{p}_i$ are the minimal primes over the ideal $I(X)$. Moreover, $\mathfrak{p}_i = I\big(V(\mathfrak{p}_i)\big)$.*

Note that it would be wrong to say that $I\big(V(\mathfrak{p})\big) = \mathfrak{p}$ for all primes because $V(\mathfrak{p})$ may be empty. Note that we don't use the Nullstellensatz.

Proof. check the proof in the notes [[★★★]]. □

Generic Points: For a subset $Y \subseteq X$, a point $y \in Y$ is called a generic point of Y if $\overline{\{y\}} = Y$. Note that to have a generic point, Y must be closed and irreducible. In general, these conditions are not sufficient! In classical algebraic geometry, even k-varieties need not have generic points!

Example 18.8. Let $k = \bar{k}$, and $Y = V(y - x^2)$, the parabola. Y is irreducible, but it has no generic point in the k-topology because points are closed (since $k = \bar{k}$). •

Classically, we take $k \subseteq K$ to have infinite transcendence degree (e.g. $\mathbb{Q} \subseteq \mathbb{C}$). In this case, k-varieties in K^n will have generic points. In the example above, take $K = \operatorname{Frac}\left(\frac{k[s,t]}{(t^2-s)}\right)$. Then $(\bar{s}, \bar{t})$ is a generic point for the parabola.

§3. Zariski Prime Spectrum

	algebraic	geometric
Classical	$k[x_1, \ldots, x_n]$	K^n, k-algebraic sets, etc.
Grothendieck	any (commutative) R	$\operatorname{Spec} R$

Define $\mathcal{V}(J) = \{\mathfrak{p} \in \operatorname{Spec} R | J \subseteq \mathfrak{p}\}$.

Theorem 18.9.

1. *Taking $\mathcal{V}(J)$ to be closed sets gives a topology on* $\operatorname{Spec} R$.
2. *The sets $\mathcal{D}(f) = \operatorname{Spec} R \smallsetminus \mathcal{V}(f)$, $f \in R$, are a basis for the topology.*
3. $\operatorname{Spec} R$ *is a compact T_0 space.*[1]

Proof. (1) This follows from $\bigcap \mathcal{V}(J_\alpha) = \mathcal{V}\big(\sum J_\alpha\big)$ and $\mathcal{V}(J_1) \cup \mathcal{V}(J_2) = \mathcal{V}(J_1 \cap J_2)$.

(2) An open set is of the form $\operatorname{Spec} R \smallsetminus \mathcal{V}(J) = \bigcup_{f \in J} \mathcal{D}(f)$.

(3) If $\mathfrak{p}, \mathfrak{p}' \in \operatorname{Spec} R$ are distinct, then there is some $f \in \mathfrak{p} \smallsetminus \mathfrak{p}'$ or $f \in \mathfrak{p}' \smallsetminus \mathfrak{p}$, say the former. Then $\mathcal{D}(f)$ contains $\mathfrak{p}'$ but note $\mathfrak{p}$. This proves T_0. If you have a cover, then refine it to a cover by open sets of the form $\mathcal{D}(f_\alpha)$. Then the f_α generate the unit ideal [[★★★]], so a finite number of them give 1, so those $\mathcal{D}(f_\alpha)$ cover. □

[1] Given two points, one of them (you don't know which) has an open neighborhood avoiding the other.

Lecture 19

Spec R is connected if and only if R has only trivial idempotents. All of the closed and open (*clopen*) sets of Spec R are $\mathcal{V}(e)$, where e is an idempotent.

Proposition 19.1. *For any ring R, the following are equivalent.*

1. $\dim R = 0$.
2. Spec R *is* T_1 *(points are closed).*
3. Spec R *is* T_2 *(hausdorff).*
4. Spec R *is a Boolean space (compact, hausdorff, and totally disconnected).*
5. Spec R *is* T_4 *(normal).*

Example 19.2. Spec $\mathbb{Z} = \{(0), (2), (3), (5), (7), \dots\}$. For $n \neq 0$, $\mathcal{V}\big((n)\big) = \{p | p$ divides $n\}$, which is finite; it is clear that any finite set (not containing (0)) can be realized this way. So the non-empty open sets are the cofinite sets contining (0). •

Example 19.3. Let R be the semi-localization of $\mathbb{Z}$ at $\{p_1, \dots, p_r\}$. Now the non-empty open sets are all the subsets containing (0). •

Example 19.4. If R is a PID, then prime ideals are generated by irreducible elements. The non-empty open sets are still the cofinite sets containing (0). •

Definition 19.5. For a subset $Y \subseteq$ Spec R, we define $\mathcal{I}(Y) := \bigcap_{\mathfrak{p} \in Y} \mathfrak{p}$, which is a radical ideal in R.

Proposition 19.6. *Here are some fairly easy results.*

1. *If $J \lhd R$, $\mathcal{I}\big(\mathcal{V}(J)\big) = \sqrt{J}$.*
2. *For $Y \subseteq$ Spec R, $\mathcal{V}\big(\mathcal{I}(Y)\big) = \overline{Y}$. In particular, $\overline{\{\mathfrak{p}\}} = \mathcal{V}(\mathfrak{p})$.*
3. *$\mathfrak{p}$ is a closed point if and only if it is a maximal ideal.*

That is, we have an inclusion-reversing bijection between radical ideals and closed sets. Note that Spec R is noetherian if and only if radical ideals satisfy ACC. In this case, the set of minimal primes is finite. Observe that if R is noetherian, then so is Spec R, but the converse is false.

$$\begin{array}{ccc}
\left\{\begin{array}{c}\text{radical}\\ \text{ideals}\end{array}\right\} & \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} & \left\{\begin{array}{c}\text{closed}\\ \text{sets}\end{array}\right\} \\
\cup\text{I} & & \cup\text{I} \\
\left\{\begin{array}{c}\text{prime}\\ \text{ideals}\end{array}\right\} & \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} & \left\{\begin{array}{c}\text{irreducible}\\ \text{closed sets}\end{array}\right\} \\
\cup\text{I} & & \cup\text{I} \\
\left\{\begin{array}{c}\text{minimal}\\ \text{primes}\end{array}\right\} & \underset{\mathcal{I}}{\overset{\mathcal{V}}{\rightleftarrows}} & \left\{\begin{array}{c}\text{irreducible}\\ \text{components}\end{array}\right\}
\end{array}$$

§4 Hilbert's Nullstellensatz

Fix a field k.

Definition 19.7. If M is an R-module, we say that M is *module-finite* if M is finitely generated as a module. If S is an R-algebra, we say it is *ring-finite* if it is finitely generated as an R-algebra.

Lemma 19.8. *Let $S = k(x_1, \dots, x_r)$, with $r \geq 1$. Then S is not ring-finite over k.*

Sketch of Proof. Assume not. Then $S = k[f_1/g, \dots, f_\ell/g]$ (we can choose a common denominator). But then every rational function can be written with denominator a power of g, which is clearly false. □

Theorem 19.9 (Artin-Tate Theorem)**.** *Let $R \subseteq S \subseteq T$ be rings, with R noetherian, T ring-finite over R and module-finite over S. Then S is ring-finite over R.*

Sketch of Proof. We have $T = R[t_1, \dots, t_n] = \sum_{j=1}^{m} Sy_j$ (choose one of the y_j to be 1), so we get $t_i = \sum s_{ij} y_j$ and $y_i y_j = \sum s_{ij\ell} y_\ell$. Consider $S_0 := R[s_{ij}, s_{ij\ell}] \subseteq S$, which is noetherian by Hilbert's basis theorem, and it is ring-finite over R. Note that $T = \sum S_0 y_j$ by construction, so T is module-finite over S_0. So T is a noetherian module over S_0, so S is module finite over S_0 (as a submodule of a noetherian module-finite module). So S is module-finite over a ring-finite guy over R, so it is ring-finite. □

Lecture 20

Correction to cross-reference: p. 61, line −12, the reference is to exercise I.70, not to I.55.

We forgot to say that if $f : R \to S$ is a ring homomorphism, then $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is defined as $f^*(\mathfrak{p}) = \mathfrak{p}^c = f^{-1}(\mathfrak{p})$. Then we have $(f^*)^{-1}\big(\mathcal{V}(J)\big) = \mathcal{V}\big(f(J)\big)$, so f^* is continuous. We also get $(f \circ g)^* = f^* \circ g^*$, so $R \rightsquigarrow \operatorname{Spec} R$ is a contravariant functor from the category of commutative unital rings to the category of compact T_0 spaces.

Remark 20.1. If R and S are not commutative, $f^{-1}(\mathfrak{p})$ is not prime in general!

Lemma 20.2 (Zariski)**.** *If T is a ring-finite field extension of k, then T is a module-finite extension of k.*

Proof. We have $T = k[t_1, \dots, t_n]$, and we need to prove that each t_i is algebraic over k. Assume not. Then after relabeling, we may assume $t_1, \dots, t_r$ (with $r \geq 1$) is a transcendence base for T over k. Then T is module-finite over $k(x_1, \dots, x_r)$ (by definition of transcendence base). By the Artin-Tate theorem, we get that $k(x_1, \dots, x_r)$ is ring-finite over k, contradicting Lemma 19.8. □

We can restate Zariski's lemma in the following way.

Theorem 20.3. *Let A be an affine k-algebra, and let $\mathfrak{m} \in \operatorname{Max}(A)$, then $T = A/\mathfrak{m}$ is a finite field extension of k.*

Proof. We have that T is an affine k-algebra (i.e. it is ring-finite over k), and it is a field, so Zariski's lemma applies to give the desired result. □

Corollary 20.4. *If $f : B \to A$ is a k-algebra homomorphism of affine k-algebras. Then $f^* : \operatorname{Spec} A \to \operatorname{Spec} B$ takes closed points to closed points (i.e. takes $\operatorname{Max} A$ to $\operatorname{Max} B$).*

Proof. We need to prove that if $\mathfrak{m} \in \operatorname{Max} A$, then $f^{-1}(\mathfrak{m})$ is maximal. We have injections $k \hookrightarrow B/f^{-1}(\mathfrak{m}) \hookrightarrow A/\mathfrak{m}$, and by the theorem, $A/\mathfrak{m}$ is a finite extension of k. But we know that a ring inside an algebraic extension is a field (because the inverse of an element is a polynomial in that element by algebraicity). □

Corollary 20.5. *Let $\mathfrak{m} \lhd A = k[x_1, \dots, x_n]$, then $\mathfrak{m}$ is maximal if and only if there is an* algebraic point *$(a_1, \dots, a_n) \in \bar{k}^n$ such that $\mathfrak{m} = \mathcal{I}\big((a_1, \dots, a_n)\big)$. In particular, if $k = \bar{k}$, $\mathfrak{m}$ is maximal if and only if it is of the form $(x - a_1, \dots, x - a_n)$.*

Proof. If $\mathfrak{m}$ is maximal, then we have an algebraic extension $k \hookrightarrow A/\mathfrak{m} \overset{\varphi}{\hookrightarrow} \bar{k}$, and we have $\varphi(x_i) = a_i$ for some a_i. For all $f \in A$, we have $\phi(f) = f(a_1, \dots, a_n)$. If $f \in \mathfrak{m}$, then clearly $\phi(f) = 0$, so $f(a_1, \dots, a_n) = 0$.

Conversely, if $\mathfrak{m} = \mathcal{I}\big((a_1, \dots, a_n)\big)$, then we have the evaluation map at $(a_1, \dots, a_n)$ inducing $A/\mathfrak{m} \hookrightarrow \bar{k}$. Then $A/\mathfrak{m}$ is a ring in an algebraic extension of k, so it is a field, proving that $\mathfrak{m}$ is maximal. □

Corollary 20.6 (Weak NSS)**.** *If $J \triangleleft A = k[x_1, \dots, x_n]$ is proper, $V_{\bar{k}}(J) \neq \varnothing$.*

Proof. Enlarging J, we may reduce to the case $J = \mathfrak{m} \in \operatorname{Max} A$, noting that $V_{\bar{k}}(\mathfrak{m}) \subseteq V_{\bar{k}}(J)$. By the previous corollary, $(a_1, \dots, a_n)$ is an algebraic point on which all of $\mathfrak{m}$ vanishes, as desired. □

Corollary 20.7. *Every maximal ideal $\mathfrak{m} \subseteq A = k[x_1, \dots, x_n]$ can be generated by n irreducible polynomials of the form $f_1(x_1)$, $f_2(x_1, x_2)$, …, $f_n(x_1, \dots, x_n)$ (f_i only uses the first i variables).*

Proof. In the notes. [[★★★]] □

Theorem 20.8. *Every affine k-algebra A is a* Hilbert ring*, i.e. every prime ideal is an intersection (possibly infinite) of maximal ideals.*

Proof. Let $\mathfrak{p} \in \operatorname{Spec} A$, and let $s \notin \mathfrak{p}$; we wish to find a maximal ideal $\mathfrak{m} \supseteq \mathfrak{p}$ such that $s \notin \mathfrak{m}$. Consider the localization $A_s = A[s^{-1}]$, in which the extension $\mathfrak{p}A_s$ of $\mathfrak{p}$ is some proper ideal, so there is some maximal ideal $M \in \operatorname{Max} A_s$ such that $\mathfrak{p}A_s \subseteq M$. Since A and A_s are both affine, $M^c \in \operatorname{Max} A$ by Corollary 20.4, and $\mathfrak{p} \subseteq M^c$, with $s \notin M^c$, as desired. □

More generally, if R is Hilbert, then any ring-finite extension S of R is Hilbert. The above theorem is the case where R is a field.

Lecture 21

Theorem 21.1 (Strong NSS)**.** *For any field k, let $J \lhd A = k[x_1, \dots, x_n]$. Then $g \in A$ vanishes on $V_{\bar{k}}(J)$ if and only if $g \in \sqrt{J}$. That is, $I\big(V_{\bar{k}}(J)\big) = \sqrt{J}$.*

Proof. We need only to prove $\Rightarrow$, as the other direction is trivial. This is often done with the Rabinowich trick, but we will take a ring-theoretic approach. First note that $\sqrt{J} = \bigcap_{J \subseteq \mathfrak{p}} \mathfrak{p} = \bigcap_{J \subseteq \mathfrak{m}} \mathfrak{m}$ since A is a Hilbert ring. So it suffices to check that $g \in \mathfrak{m}$ for each $\mathfrak{m} \supseteq J$. We saw last time that a maximal ideal is exactly the vanishing ideal of an algebraic point $a = (\alpha_1, \dots, \alpha_n) \in \bar{k}^n$, $\mathfrak{m} = \mathcal{I}(\{a\})$. Since J vanishes on $\{a\}$, $a \in V_{\bar{k}}(J)$. By assumption, $g(a) = 0$, so $g \in \mathfrak{m}$, as desired. □

Remark 21.2. We used the Weak NSS in the proof that maximal ideals are vanishing ideals of algebraic points.

Corollary 21.3. *Let $f, g \in A[x_1, \dots, x_n]$, and assume f is square-free and non-zero. Then $f|g$ if and only if $V_{\bar{k}}(f) \subseteq V_{\bar{k}}(g)$.*

Proof. $\Rightarrow$ is trivial. By the strong NSS applied to $J = (f)$. Since g vanishes on $V_{\bar{k}}(J)$, $g^r = f \cdot h$ for some h. Each prime dividing f must then divide g. Since f is square-free, $f|g$. □

Theorem 21.4. *Let $J \lhd A$, where A is an affine k-algebra. Then A/J is artinian if and only if $\dim_k A/J < \infty$. If A is a polynomial ring, then this occurs if and only if $|V_{\bar{k}}(J)|$ is finite. Furthermore, $|V_{\bar{k}}(J)| \leq \dim_k A/J$.*

Warning 21.5. In the literature, such a J is called a "zero-dimensional" ideal. This is confusing because A/J is artinian if it is zero-dimensional *as a ring*, not as a k-vector space.

Proof. If A/J is finite-dimensional over k, then it is clearly artinian. For the other direction, apply Akizuki-Cohen [[★★★]] to reduce to: An affine *local* artinian k-algebra $(R, \mathfrak{m})$ is finite dimensional over k. If R is a field, then we are done by Zariski's lemma. In particular, $\dim_k R/\mathfrak{m} < \infty$. We also know that $\mathfrak{m}$ is nilpotent (the jacobson radical in an artinian ring is always nilpotent) and that $\dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1} < \infty$ because $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ is finitely generated over $R/\mathfrak{m}$. It follows that $\dim_k R < \infty$.

Now let's consider the case where $A = k[x_1, \dots, x_n]$. We want to show that $\dim A/J < \infty$ (i.e. A/J is artinian) if and only if $V_{\bar{k}}(J)$ is finite and that $|V_{\bar{k}}(J)| \leq \dim_k A/J$. First reduce to the case $k = \bar{k}$; the conditions do not change when you tensor up to $\bar{k}$. We may also assume that J is radical; again, the conditions don't change when we replace J by $\sqrt{J}$ (uses exercise I.47), noting that $|V_{\bar{k}}(J)|$ stays the same, and $\dim_k A/J$ gets smaller.

Recall that $J = \sqrt{J} = \bigcap_{\mathfrak{m} \supseteq J} \mathfrak{m}$, and each $\mathfrak{m}$ is of the form $(x_1 - a_1, \dots, x_n - a_n)$, where $(a_1, \dots, a_n) \in V_k(J)$. For the implication $\Rightarrow$, we note that if A/J is artinian,

then it is semi-local, so there are only finitely many $\mathfrak{m}$ containing J, so $V_k(J)$ is finite. For the implication $\Leftarrow$, we note that $|V_k(J)| < \infty$ is the number of maximal ideals containing J, so A/J is semi-local with Jacobson radical equal to zero (since J is radical). By an earlier fact [[★★★]] $A/J = \frac{A/J}{\mathrm{rad}(A/J)}$ is the product of all its residue fields (all of which are k), so $\dim_k A/J = |V_k(J)|$. □

Connection between k-algebraic sets $Y \subseteq K^n$ and $\mathrm{Spec}\, k[Y]$. There is a canonical map $\varphi : Y \mapsto \mathrm{Spec}\, k[Y]$, but it is neither one-to-one nor onto in general.

Lecture 22

Recall that a typical maximal ideal in $k[x_1, \dots, x_n]$ is of the form $I(y)$, where $y \in \bar{k}^n$ is an algebraic point.

Let K/k be a fixed extension. As usual, we have the ideal $I(\{y\})$ for every $y \in K^n$, and we have $k[y]$, the coordinate ring $k[x_1, \dots, x_n]/I(\{y\}) = k[y_1, \dots, y_n]$, which is an affine k-algebra.

Definition 22.1. If $y, z \in K^n$, then we say that y *specializes to* z (written $y \rightsquigarrow z$) if there is a k-algebra homomorphism $k[y] \to k[z]$ taking y_i to z_i (in particular, it is surjective).

Clearly $y \rightsquigarrow z$ if and only if $I(y) \subseteq I(z)$. Furthermore, this occurs if and only if $z \in \overline{\{y\}} = V_K\big(I(y)\big)$. Therefore, we can thing of $\overline{\{y\}}$ as $\{z | y \rightsquigarrow z\}$.

Definition 22.2. If $y, z \in K^n$, $y \rightsquigarrow z$, and $z \rightsquigarrow y$, then we say that y and z are *k-conjugate* (written $y \leftrightsquigarrow z$).

It follows immediately that $y \leftrightsquigarrow z$ if and only if $\overline{\{z\}} = \overline{\{y\}}$. In particular, k-conjugacy is an equivalence relation; we write $[y]$ for the equivalence class of y. Note that $[y] \subseteq \overline{\{y\}}$.

Definition 22.3. We say that $y = (y_1, \dots, y_n) \in K^n$ is *k-algebraic* if each y_i is algebraic over k.

Note y is algebraic if and only if $k[y]$ is a field ($\Leftarrow$ follows from Zariski's Lemma), which occurs if and only if $I(y)$ is maximal. Moreover, if y is algebraic, then $y \rightsquigarrow z$ implies that $y \leftrightsquigarrow z$. i.e. "algebraic points cannot be further specialized".[1] So in the case when y is algebraic, $[y] = \overline{\{y\}}$.

Remark 22.4. Any k-point (*k-rational point*) is always algebraic.

Example 22.5. $k = \mathbb{Q}$ and $K = \mathbb{Q}[\sqrt[3]{2}]$, with $y = \sqrt[3]{2}$. Then $[y] = \overline{\{y\}} = V_K(x^3 - 2) = \{y\}$. So y is a closed point, but not a k-rational point.

If we take K to be the normal hull (Galois hull) of $k(y)$, then $[y] = V_K(x^3 - 2) = \{y, \omega y, \omega^2 y\}$, where $\omega^3 = 1$. •

Example 22.6. Choose k a field which is not perfect, with characteristic $p > 0$. Then there is some $a \in k \smallsetminus k^p$. Take $y \in \bar{k}$ such that $y^p = a$. Then consider any K which contains y. Then $[y] = V_K(x^p - a) = \{y\}$, so y is closed! •

Given a k-algebraic set $Y \subseteq K^n$, we can construct a map $\varphi : Y \to \operatorname{Spec} k[Y]$, given by $y \mapsto I(y)$ (which is always prime). Since $I(Y) \subseteq I(y)$, we get that $I(y) \in \operatorname{Spec} k[Y]$. Let $\varphi(y) = \mathfrak{p}_y = I(y)/I(Y)$. The map φ is always continuous. To see this, consider a closed set $\mathcal{V}(\bar{J}) \subseteq \operatorname{Spec} k[Y]$, where $J \supseteq I(Y)$. Then $\varphi^{-1}\big(\mathcal{V}(\bar{J})\big) = Y \cap V(J)$, which is closed.

In general, φ is neither 1-to-1 nor onto. Let's describe the image and fibers of φ.

[1] "Being algebraic is very special, and you cannot make it more special."

Theorem 22.7. *Let $y, z \in Y$. Then*

1. *$\varphi(y) = \varphi(z)$ if and only if $y \leftrightsquigarrow z$. In particular, the fibers of φ are the k-conjugacy classes in Y.*[2]
2. *$y \in Y_{alg}$ (i.e. y is algebraic) if and only if $\varphi(y) \in \operatorname{Max} k[Y]$. In particular, $\varphi(Y_{alg}) = \operatorname{Max} k[Y]$ and the fiber containing y is $\overline{\{y\}}$.*
3. *A prime $\mathfrak{p}/I(Y) \in \operatorname{Spec} k[Y]$ is in the image of φ if and only if $\mathfrak{p} = I\big(V_K(\mathfrak{p})\big)$ and $V_K(\mathfrak{p})$ has a generic point.*

Proof. Items 1 and 2 are clear. Let's do $\Rightarrow$ for 3. Suppose $\mathfrak{p}/I(Y)$ is in the image of φ, so $\mathfrak{p} = I(y)$, then $\mathfrak{p} = I\big(V_K(\mathfrak{p})\big)$ by [[★★★]]. Since $V_K(\mathfrak{p}) = V_K\big(I(y)\big)$, y is a generic point for $V_K(\mathfrak{p})$. The converse is dry formal work [[★★★]]. □

Special cases of 3 above:

1. if $\bar{k} \subseteq K$, then we can delete the hypothesis $\mathfrak{p} = I\big(V_K(\mathfrak{p})\big)$ because of the NSS.
2. If K is a "universal domain" ($K = \bar{K}$, and K/k has infinite transcendence degree), then φ is onto because we can remove the condition that $V_K(\mathfrak{p})$ has a generic point.
3. If $K = \bar{k}$, $\operatorname{im}\varphi = \operatorname{Max}(k[Y])$. Moreover, there is a 1-to-1 correspondence $\{k\text{-subvarieties of } Y\} \leftrightarrow \operatorname{Spec} k[Y]$, with $V \leftrightarrow I(V)/I(Y)$.
4. If $K = \bar{k} = k$, then $\varphi(a_1, \ldots, a_n) = (x_1 - a_1, \ldots, x_n - a_n)/I(Y)$.

[2] Since Y is closed, a conjugacy class that intersects Y must be contained in Y.

Lecture 23

Chapter III. Integral Extensions and Normal Domains.

§1. Going up Theorem. (Cohen-Siedenberg theorems)

§1. Going Up Theorem

Let $R \subseteq S$ be a ring extension, and let $I \lhd R$.

Definition 23.1. We say $s \in S$ is *integral over* I if there is a monic $p \in I[x] \subseteq R[x]$ so that $p(s) = 0$. If every $s \in S$ is integral over R, then we say that S/R is an *integral extension.*

Example 23.2. If S and R are fields, then S/R integral is the same as S/R being algebraic. •

Example 23.3. If every $s \in S$ satisfies $s^{n(s)} = s$ (with each $n(s) \geq 2$), then S is integral over any sub-ring. The same is true if S is any ring of algebraic integers (as soon as all the coefficients are integers, we're on the gravy train). •

Example 23.4. If $d \in \mathbb{Z}$, then $\sqrt{d}$ is always integral over $\mathbb{Z}$. More interestingly, if $d = 1 + 4b$, then $\alpha = \frac{1+\sqrt{d}}{2}$ is integral over $\mathbb{Z}$ because $\alpha^2 - \alpha - b = 0$. •

Example 23.5. Let $M \subseteq R$ be a multiplicatively closed set, and let S/R be an integral extension, then $M^{-1}S/M^{-1}R$ is integral. •

Proposition 23.6. *If S/R is a ring extension, and $s \in S$, then the following are equivalent.*

1. *s is integral over R.*
2. *$R[s]$ is module-finite over R.*
3. *$s \in T$ for some ring T between R and S that is module-finite over R.*
4. *There is a faithful $R[s]$-module M that is module-finite over R.*

In particular, if S/R is module-finite, then it is integral.

Proof. $1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 4$ are clear. $4 \Rightarrow 1$ follows from the determinant trick: we get $R[s] \hookrightarrow \mathrm{End}_R(M)$ [[★★★ finish]]. □

Corollary 23.7. *If $s_1, \ldots, s_n$ are integral over R, then $R[s_1, \ldots, s_n]$ is module-finite over R. In particular, the elements of S that are integral over R form a sub-ring of S, called the* integral closure *of R inside S.*

Corollary 23.8 (Transitivity of integrality)**.** *If T/S and S/R are integral, then T/R is integral.*

Proposition 23.9. *Let $I \triangleleft R \subseteq S$, and let C be the integral closure of R in S. Then the elements of S that are integral over I are exactly $\sqrt{I \cdot C}$ (the radical in C, though it doesn't matter). In particular, it is an ideal in C.*

Remark 23.10. Note that the elements integral over I are the same as the elements integral over $\sqrt{I}$. If $S = R$, then the result says that elements of R integral over I are exactly $\sqrt{I}$.

Proof. Let $c \in C$ be integral over R, so $c^n + a_1 c^{n-1} + \cdots + a_n = 0$ with $a_j \in I$. It follows immediately that $c \in \sqrt{I \cdot C}$. For the other containment, let $c \in \sqrt{I \cdot C}$. Let $c^n = b_1 c_1 + \cdots + b_m c_m$, where $b_j \in I$ and $c_j \in C$. Then $M = R[c, c_1, \ldots, c_m]$ is module-finite over R. Now $c^n M \subseteq \sum b_i M \subseteq I \cdot M$. By the determinant trick, c^n is integral over I. Hence c is integral over I.[[★★★ why not just use the proposition above]] □

Lemma 23.11. *If $I \triangleleft R$ is a proper ideal and S/R is integral, then $I \cdot S \neq S$.*

Proof. Assume not, so $1 = a_1 s_1 + \cdots + a_n s_n$, with $a_j \in I$ and $s_j \in S$. Then $M = R[s_1, \ldots, s_n]$ is module-finite over R. Now we have $I \cdot M = M$. By the determinant trick, there is some $a \in I$ so that $(1 - a)M = 0$, so $1 = a \in I$, contradicting that I is proper. □

Lecture 24

Typos: p 73 (proof 4.1) "g^m prime to g" should be "g^m prime to $1+g$"
p 76, ref to $*$ in rmk 4.15 should ref to 4.16.

Example 24.1. $k \subsetneq R \subseteq S = k[x]$, then S/R is integral because x is integral over R, since R must contain some monic polynomial in x. •

Theorem 24.2 (Going Up)**.** *Let S/R be integral.*

1. *(Lying over) For every $\mathfrak{p} \in \operatorname{Spec} R$, there is some $\mathfrak{P} \in \operatorname{Spec} S$ so that $\mathfrak{P} \cap R = \mathfrak{p}$. This means that $\operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.*
2. *(Going up) If $I \subseteq \mathfrak{p} \subseteq R$ and $J \subseteq S$ lying over I, then there is some prime $\mathfrak{P} \supseteq J$ lying over $\mathfrak{p}$.*
3. *(Incomparability) If $\mathfrak{P} \subsetneqq \mathfrak{P}'$, then $\mathfrak{P} \cap R \subsetneqq \mathfrak{P}' \cap R$.*

Proof. (1) First assume $(R, \mathfrak{p})$ is local, then $\mathfrak{p}S \neq S$, so $\mathfrak{p}S$ is in some maximal ideal $\mathfrak{m} \subseteq S$, then $\mathfrak{m} \cap R$ contains $\mathfrak{p}$ and is prime (in particular, not all of R), so it is equal to $\mathfrak{p}$. In the general case, just localize at $\mathfrak{p}$ first.

(2) Pass to the integral extension $R/I \hookrightarrow S/J$ and apply Lying over.

(3) Pass to $R/\mathfrak{p} \hookrightarrow S/\mathfrak{P}$ to assume $\mathfrak{p} = 0$ and $\mathfrak{P} = 0$. Then we need to prove that if $\mathfrak{P}' \neq 0$, then $\mathfrak{p} := R \cap \mathfrak{P}' \neq 0$. Choose $x \in \mathfrak{P}' \smallsetminus \{0\}$; then we have $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, with n minimal. Then $a_n = -x(x^{n-1} + a_1 x^{n-2} + \cdots) \in \mathfrak{P}' \cap R$. Finally, since n is minimal and S ($S/\mathfrak{P}$) is a domain, $a_n \neq 0$. □

Corollary 24.3. *Let S/R be integral.*

1. *If $\mathfrak{P} \in \operatorname{Spec} S$, then $\mathfrak{P}$ is maximal if and only if $\mathfrak{P} \cap R \in \operatorname{Max} R$.*
2. $\operatorname{rad} R = R \cap \operatorname{rad} S$.
3. *If S is a domain, then R is a field if and only if S is a field.*
4. *If S is (semi-)local, then so is R.*

We also get the following analog of the Eakin-Nagata Theorem

Corollary 24.4. *Let $R \subseteq S$ be rings, such that S is module-finite (in particular integral) over R. Then R is artinian if and only if S is artinian.*

Proof. $\Rightarrow$ A finitely generated module over an artinian ring is artinian, so ${}_RS$ is artinian, so ${}_SS$ is artinian.

$\Leftarrow$ If S is artinian, then it is noetherian, then by Eakin-Nagata, R is also noetherian. Since S is artinian, every prime is maximal, so R is also 0-dimensional. By Akizuki, R is artinian. □

§2. Going Down Theorem and Krull Dimension

Definition 24.5. Let $Q(R) = \big(\mathcal{C}(R)\big)^{-1}R$ be the total ring of fractions of R. We say that R is *integrally closed* if it is equal to its integral closure in $Q(R)$. If R is an integrally closed domain, then we say it is a *normal domain*.

Remark 24.6. Any localization of a normal domain is again a normal domain.

Proposition 24.7. *Any UFD is a normal domain.*

Proof. Let a/b be integral over R. We may assume a/b is in lowest terms (a and b have no common prime divisors), with b not a unit. Then we have $(a/b)^n + c_1(a/b)^{n-1} + \cdots + c_n = 0$, so $a^n + c_1a^{n-1}b + \cdots + c_nb^n = 0$. It follows that $b|a^n$, so some prime dividing b divides a, a contradiction. □

Lemma 24.8. *Let R be a normal domain with $Q(R) = K$, let L be a field extension of K, and let $s \in L$ be algebraic over K with minimal polynomial $f(x) = x^n + c_1x^{n-1} + \cdots + c_n \in K[x]$. Given $I \triangleleft R$, s is integral over I if and only if $c_i \in \sqrt{I}$ for all i. In particular, s is integral over R if and only if $f(x) \in R[x]$.*

Proof. ($\Leftarrow$) Suppose $c_i\sqrt{I}$ for all i. Then s is integral over $\sqrt{I}$, and so integral over I.

($\Rightarrow$) Assume s is integral over I. Let $(x - s_1)\cdots(x - s_n)$ be a complete factorization of f is $\overline{K}[x]$, say with $s_1 = s$. Then $K(s_j) \cong K(s)$ for each j, so each s_j is integral over I [[★★★ you can see this easier because the minimal poly must divide the monic]]. Each c_j is an elementary symmetric function in the s_i, so c_j is integral over I. Since R is integrally closed, $c_j \in R$. Finally, the only elements of R that are integral over I are in $\sqrt{I}$. □

Lecture 25

Lemma 25.1 (Contracted prime criterion, II.3.15)**.** *If $f : R \to C$, then $\mathfrak{p} \in \operatorname{Spec} R$ is a contracted prime (is f^{-1} of a prime) if and only if $\mathfrak{p} = \mathfrak{p}^{ec}$.*

Lemma 25.2. *If S/R is integral, $I \lhd R$, and $s \in S$. Then s is integral over I if and only if $s \in \sqrt{I \cdot S}$ if and only if the non-leading coefficients of the irreducible polynomial of s are in $\sqrt{I}$ (this last part assumes that R is normal and S is a domain).*

Theorem 25.3 (Going Down)**.** *If S/R is integral, with S a domain and R a normal domain, then for every pair of primes $\mathfrak{p} \subseteq \mathfrak{p}' \subseteq R$ and prime $\mathfrak{P}'$ lying over $\mathfrak{p}'$, there is a prime $\mathfrak{P} \in \operatorname{Spec} S$ contained in $\mathfrak{P}'$ which lies over $\mathfrak{p}$.*

Proof. It suffices to show that $\mathfrak{p}$ is a contracted prime under $f : R \to C = S_{\mathfrak{P}'}$; that is, to show that $\mathfrak{p} = \mathfrak{p}^{ec} = R \cap \mathfrak{p}C$. If not, there is an element $r \in R \cap \mathfrak{p}C$ but $r \notin \mathfrak{p}$. We can write $r = s/t$ where $s \in \mathfrak{p}S$ and $t \in S \smallsetminus \mathfrak{P}'$.

picture

Let the minimal polynomial of s over $K = Q(R)$ be $s^n + c_1 s^{n-1} + \cdots + c_n = 0$. Then a minimal equation for t over K is obtained by dividing by r^n, so $t^n + \frac{c_1}{r} t^{n-1} + \cdots + \frac{c_n}{r^n} = 0$; let $c_i/r^i = d_i$. Since t is integral over R, the d_i are in R. We have that $s \in \mathfrak{p}S$, so s is integral over $\mathfrak{p}$, so $c_i \in \sqrt{\mathfrak{p}} = \mathfrak{p}$. Then $c_i = d_i r^i$, and $r \notin \mathfrak{p}$, so $d_i \in \mathfrak{p}$, so t is integral over $\mathfrak{p}$. Thus, $t \in \sqrt{\mathfrak{p}S} \subseteq \mathfrak{P}'$, contradicting that $t \notin \mathfrak{P}'$. □

Krull dimension and height.

Definition 25.4. If $\mathfrak{p} \in \operatorname{Spec} R$, then the *height* of $\mathfrak{p}$ is the supremum of lengths of chains of primes contained in $\mathfrak{p}$; $\mathfrak{p} \supsetneq \mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ has length n. Some people use the words *rank* or *altitude* instead of height.

In particular, $ht(\mathfrak{p}) = 0$ means that $\mathfrak{p}$ is a minimal prime. If R is a domain, then note that (0) is a prime, so the primes that you want to call "minimal" are actually height 1.

Definition 25.5. The *(Krull) dimension* of a ring R is the supremum of heights of primes in R.

Theorem 25.6. *Let S/R be integral, then*

1. *$\dim R = \dim S$, and*
2. *for $\mathfrak{P} \in \operatorname{Spec} S$, $\mathfrak{p} = \mathfrak{P} \cap R$, then $ht(\mathfrak{P}) \leq ht(\mathfrak{p})$, with equality if S is a domain and R is normal.*

Proof. (1) By incomparability, prime chains in S contract to prime chains in R, so $\dim R \geq \dim S$. By going up, prime chains in R lift to prime chains in S, so $\dim R \leq \dim S$.

(2) Incomparability also shows that $ht(\mathfrak{P}) \leq ht(\mathfrak{p})$. If S is a domain and R is normal, then going down applies, so a prime chain from $\mathfrak{p}$ lifts to a prime chain from $\mathfrak{P}$ (without going down, you wouldn't get a chain with upper bound $\mathfrak{P}$). □

In particular, if $\mathfrak{P}$ contracts to a minimal prime, then it is minimal. The converse is not true in general.

§3. Normal and Completely Normal Domains

Lemma 25.7. *Let $f \in S[x]$ be monic, then $f = \prod(x - a_i) \in S'[x]$ for a suitable ring extension S'/S.*

Proof. Induct on $\deg f = n$, simultaneously over all rings. If $n = 1$, we're done. If $n > 1$, then consider the embedding $S \hookrightarrow S[t]/\big(f(t)\big)$. Then we use the division algorithm for monic polynomials, we get $f(x) = (x - t)g(x)$, and $g(x)$ has smaller degree, so we can split it in some extension. □

Lemma 25.8 (Monicity lemma)**.** *Let R be integrally closed in S, and let $f \in S[x]$ and $h \in R[x]$ be monic. Then if $f|h$ in $S[x]$, then $f \in R[x]$.*

Proof. By the previous lemma, we have $f = \prod(x - a_i)$ in some S'. Then each a_i satisfies the monic h, so a_i are integral over R. Let b_i be the coefficients of f, then the b_i are symmetric functions in the a_j, so the b_i are integral over R. Since R is integrally closed, $f \in R[x]$ □

Lecture 26

Example 26.1. Counterexample for Going down when R is normal, but S is not a domain. Take $S = \mathbb{Z} \times \mathbb{Z}_2$ and let $R = \mathbb{Z} \cdot 1_S$. The minimal primes in S are $\mathfrak{P}'' = (0) \times \mathbb{Z}_2$ and $\mathfrak{P}' = \mathbb{Z} \times (0)$. $\mathfrak{P}''$ contracts to the minimal prime (0), but $\mathfrak{P}'$ contracts to $\mathfrak{p}' = 2R$, which is not minimal; that is, we have $ht(\mathfrak{P}') \lneq ht(\mathfrak{p}')$. •

Proposition 26.2. *If S/R is a ring extension, and $C \subseteq S$ is the integral closure of R, then $C[x]$ is the integral closure of $R[x]$ in $S[x]$.*

Proof. Clearly $C[x]$ is integral over $R[x]$ because C and x are integral over $R[x]$. Now it suffices to show that $C[x]$ is integrally closed; i.e. we've reduced to the case where R is integrally closed in S, and we'd like to show that $R[x]$ is integrally closed in $S[x]$. Let $f \in S[x]$ be integral over $R[x]$, with $G(t) = t^n + g_{n-1}(x)t^{n-1} + \cdots + g_0(x) \in R[x][t]$ monic so that $G(f) = 0$. Choose $r > \max\{\deg f, \deg g_i\}$, then $G(x^r) \in R[x]$ is monic! Now we adjust f in the following way: define $f_0 = x^r - f \in S[x]$, which is monic. Define $H(t) := G(x^r - t) \in R[x][t]$, so $H(f_0) = G(f) = 0$. Say $H(t) = (-1)^n t^n + h_{n-1}(x)t^{n-1} + \cdots + h_0(x)$, with $h_i \in R[x]$. We have $H(0) = h_0(x) = G(x^r)$ is monic in $R[x]$, and since $H(f_0) = 0$, we get that $f_0 | h_0$. By the Monicity lemma from last time, $f_0 \in R[x]$. Then $f = x^r - f_0 \in R[x]$. □

Theorem 26.3. *A domain R is normal if and only if $R[x]$ is normal.*

Proof. ($\Leftarrow$) If $\alpha \in K := Q(R)$ is integral over R and $R[x]$ is integrally closed in $K(x) = Q(R[x])$, then $\alpha \in R[x]$ and $\alpha \in K$. But $R[x] \cap K = R$, so R is normal.

($\Rightarrow$) If R is integrally closed in K, then by the proposition, $R[x]$ is integrally closed in $K[x]$. Since $K[x]$ is a UFD, it is integrally closed in $Q(K[x]) = K(x)$. It follows that $R[x]$ is integrally closed in $K(x) = Q(R[x])$. □

Definition 26.4. If S/R is a ring extension. An element $s \in S$ is *almost integral* over R if $R[s] \subseteq T \subseteq S$, where T is some module-finite module over R.[1]

Remark 26.5. The definition depends on S (not just on s), because R is to be found in S. Note that the definition is the same as $\{s^i | i \geq 0\} \subseteq T$. Integral implies almost integral (we can take $T = R[s]$). If R is noetherian, then if s is almost integral over R, it is integral over R (since T is module-finite, so is $R[s]$). If s is almost integral over R, then it is also almost integral over any $R' \supseteq R$.

Example 26.6 ($D + (x)$ construction)**.** Almost integral is strictly weaker than integral. Let D be a normal domain with $K = Q(D)$, and let $R = \{f(x) \in K[x] | f(0) \in D\} = D + x \cdot K[x]$. Let $S = K(x)$. Any element of $s \in K \subseteq K(x)$ is almost integral over R because $s^i x \in R$, so $s^i \in \frac{1}{x}R = T \subseteq S$. But if $s \in K \setminus D$, then s is not integral over R; otherwise there would be some monic $s^n + f_1(x)s^{n-1} + \cdots f_n(x) = 0$. Taking $x = 0$, we get that s is integral over D, so it is in D, a contradiction. Note that this implies that R is not noetherian. •

[1] Krull made this definition in 1928. I didn't make it up last night.

Lecture 27

Do some (two) exercises (from chapter II)!

Then we can form the "complete integral closure of R in S".

Proposition 27.1. *If $s_1, \dots, s_n \in S$ are almost integral over R, then $R[s_1, \dots, s_n]$ lies in some finitely generated R-module in S. In particular, the complete integral closure of R in S, $C := \{s \in S | s \text{ almost integral over } R\}$, is a subring of S. If $C = R$, we say R is completely integrally closed in S.*

Definition 27.2. If $S = Q(R)$, then we denote the integral closure of R in S by R^* and the complete integral closure of R in S by $R^\dagger$. We call $R^\dagger$ the *complete integral closure* of R. If $R = R^\dagger$, we say that R is *completely integrally closed*.

Remark 27.3. Note that if R is completely integrally closed, then it is integrally closed since $R \subseteq R^* \subseteq R^\dagger$. If R is noetherian, $R^\dagger = R^*$. Note that $R^\dagger = \{s \in Q(R) | \text{there is some } d \in \mathcal{C}(R) \text{ such that } ds^i \in R \text{ for all } i\}$.

If R is a completely integrally closed domain, it is called a *completely normal domain*.

Proposition 27.4. *If R is a UFD, then it is a completely normal domain.*

Proof. Let $K = Q(R)$, and assume $a/b \in K \setminus R$ is almost integral over R. We may assume that a and b have no common prime factors, and that there is some prime π dividing b (lest $a/b \in R$). Choose a non-zero $d \in R$ so that $da^i/b^i \in R$ for all $i \geq 0$, so $da^i = b^i$. It follows that $\pi^i | d$ for all i, contradicting unique (finite) factorization of d. □

Now let's pursue the completely normal analogues of the results on $R[x]$ when R is normal.

Proposition 27.5. *Let C be the complete integral closure of R in S, then $C[x]$ is the complete integral closure of $R[x]$ in $S[x]$.*

S $S[x]$

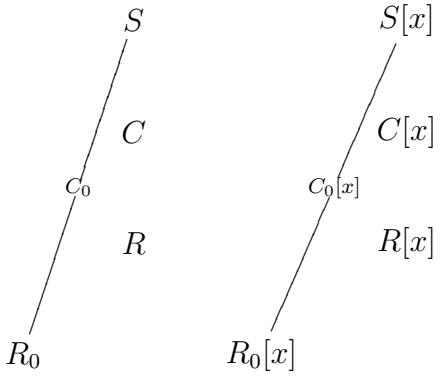
C $C[x]$

R $R[x]$

Proof. Elements of $C[x]$ are clearly almost integral over $R[x]$ since C and x are almost integral over $R[x]$ (and almost integral elements form a ring). If $f(x) = \sum s_j x^j \in S[x]$ is almost integral over $R[x]$, then we'd like to show that each s_j is almost integral over R. Fix $g_1, \dots, g_m \in S[x]$ such that $f(x)^i \in \sum_{k=1}^m R[x] \cdot g_k$ for all i. The leading term of $f(x)^i$ is $s_n^i x^{n \cdot i}$. It follows that all powers of s_n lie in the R-module generated by all the coefficients of the g_k, so it is almost integral over R, so they are in C. Then $f - s_n x^n$ is still almost integral over $R[x]$. Inducting on degree, we get that $f \in C[x]$ □

Corollary 27.6. *A domain R is completely normal if and only if $R[x]$ is.*

The proof is the same as before. In fact, we get a second (less tricky) proof of this result with the word "completely" removed using noetherian descent.



Take $f \in S[x]$ integral over $R[x]$, then it satisfies some monic polynomial. Let R_0 be the ring generated over $\mathbb{Z} \cdot 1$ by all the coefficients involved everywhere ... this ring is noetherian, so the word "completely" can be removed. We get that $f \in C_0[x] \subseteq C[x]$.

Power series case: $R[x] \rightsquigarrow R[[x]]$. If R is completely normal, then so is $R[[x]]$ (this fails for normality!).

Theorem 27.7 (Hilbert basis theorem for power series)**.** *If R is noetherian, then so is $A := R[[x]]$.*

Proof. By Cohen's theorem, it suffices to prove that any $\mathfrak{p} \in \operatorname{Spec} A$ is finitely generated. Let $I \lhd R$ be the ideal of all constant terms of elements in $\mathfrak{p}$. Since R is noetherian, I is finitely generated, say $I = \sum_{i=1}^{n} a_i R$.

Case 1: If $x \in \mathfrak{p}$, then $\mathfrak{p} = I \cdot A + x \cdot A$, so $\mathfrak{p}$ is generated by $n+1$ elements.

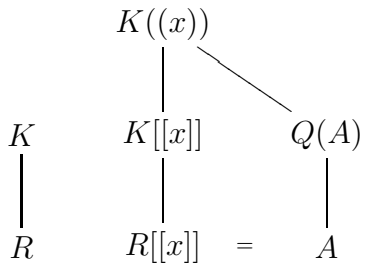
Case 2: If $x \notin \mathfrak{p}$, choose $f_i \in \mathfrak{p}$ so that $f_1(0) = a_i$. We claim that $\mathfrak{p}$ is generated by the f_i. Let $f \in \mathfrak{p}$, then we can choose b_i so that $f - \sum b_i f_i = x \cdot g$ for some $g \in A$. Since $x \notin \mathfrak{p}$, $g \in \mathfrak{p}$. Repeating the argument for g and inducting, we get $f = \sum (b_i + x c_i + x^2 d_i + \cdots) f_i$. □

Theorem 27.8. *Let R be a domain, with quotient field K and $A = R[[x]]$. Then*

1. *If A is normal, then R is normal.*
2. *A is completely normal if and only if R is completely normal*
3. *A is noetherian and normal if and only if R is noetherian and normal.*

Proof. (3) follows from (2) and the Hilbert basis theorem for power series. The direction $\Leftarrow$ in (1) and (2) are done as before (in the case $A = R[x]$). It remains to

prove that if R is completely normal, then so is A.



Assume $f \in Q(A)$ is almost integral over A. Then as an element of $K((x))$, f is almost integral over $K[[x]]$, which is a PID (so a UFD), so it is completely normal. It follows that $f \in K[[x]]$. Say $f = a_0 + a_1 x + \cdots$. We want to show that each a_i is in R. By almost integrality, there is some $h \in A \setminus \{0\}$ so that $h \cdot f^i \in A$ for all $i \geq 0$. We will show by induction that $a_j \in R$. Suppose $a_0, \ldots, a_j \in R$. Then $f' = a_0 + \cdots a_{j-1}x^{j-1} \in A$, and $h \cdot (f - f')^i \in A$ for all $i \geq i$. Suppose $h = dx^m + \cdots$, with $d \in R$ non-zero. Now we have

$$h(f - f')^i = da_j^i x^{m+ij} + \cdots \in A$$

so $da_j^i \in R$ for all i. It follows that a_j is almost integral over R. □

Corollary 27.9. *If k is a field, then $A_n = k[[x_1, \ldots, x_n]]$ is noetherian and normal.*

In fact, Weierstraß showed that A_n is even a UFD.

Lecture 28

Definition 28.1. A ring R is called *good* (called *property* $*$ in the notes) if for every non-unit $a \in R$, $\bigcap(a^i) = 0$.

"good" is a necessary condition for certain normality properties.

Proposition 28.2. *R is good if any of the following hold.*

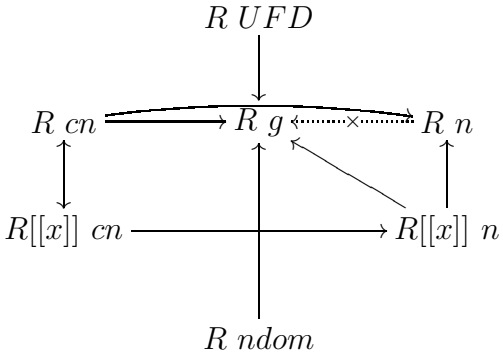
1. *R is a UFD.*
2. *R is a noetherian domain.*
3. *R is completely normal.*
4. *$R[[x]]$ is completely normal.*

Proof. 1 and 2 we've done already [[★★★]]. Assume R is a bad domain, so $0 \neq d = \bigcap(a^i)$ for some $a \in R$. Then $d(a^{-1})^i \in R$ for all i. Then $a^{-1} \notin R$ is almost integral over R, contradicting complete normality.

Believe for the moment that there is an $f = x + b_2x^2 + \cdots \in \mathbb{Z}[[x]]$ such that $f^2 - f + x = 0$. Now replace x by $\frac{x}{a^2}$. Then we have $f(x/a^2)^2 - f(x/a) + x/a^2 = 0$, so if we define $g := a \cdot f(x/a^2)$, we have $g^2 - ag + x = 0$, so g is integral over $A = R[[x]]$ (even over $R[x]$). Note that $dg \in A$ since d "clears" the denominators, so $g \in QA$. But $g \notin A$, which we can see by expanding it (we get a $1/a$ coefficient).

Finally, the f above can be constructed by looking at the constraints on the b_i, or solve with the quadratic equation ... you get catalan numbers as coefficients. □

picture



Example 28.3 (a normal R with $A = R[[x)$**.**] not normal] Take $R_0 = \mathbb{Q}[x, y] \subseteq \mathbb{Q}[x, y/x] \subseteq \mathbb{Q}[x, y/x^2] \subseteq \cdots$, so $R_i = \mathbb{Q}[x, y/x^i]$. Consider $R = \bigcup R_i$. Each $R_i \cong \mathbb{Q}[x, t]$ is normal, from which it is easy to prove that R is normal, but $x^i | y$ for all i, and x is not a unit. So R is bad. •

For another example, refine the $D + (x)$ idea. Take D a normal domain, with $D \subsetneq K = Q(D)$. Define $R = D + (x) \subseteq K[x]$.

Proposition 28.4. *R is normal and has complete integral closure $R^\dagger = K[x]$ and is bad.*

Proof. Suppose $g \in K(x) = Q(R)$ is integral over R, so $g^n + f_1 g^{n-1} + \cdots + f_n = 0$, with $f_i \in R$. Evaluating at 0, we see that $g(0)$ is integral over D, so $g(0) \in D$, so $g \in R$. Thus, R is normal.

Take a non-unit $a \in D$, then $x/a^i \in R$ for all i, so $x \in \bigcap(a^i)$, so R is bad. $\square$

Lecture 29

If L/K is a finite field extension, then there is a trace function $T_{L/K} : L \to K$. Any $\ell \in L$ is a K-linear operator $L \to L$, so it has a trace valued in K. Note that if L'/L is another finite extension, $T_{L'/K} = T_{L/K} \circ T_{L'/L}$.

Theorem 29.1. *Let R be a normal domain, with $K = Q(R)$, L/K be a finite separable field extension, and let S be the integral closure of R in L. Then $L = Q(S)$ and there is a K-basis $\{u_i\}$ of L so that $S \subseteq \bigoplus Ru_i$.*

Proof. We need two facts:

1. $T(S) \subseteq R$. To see this, let $s \in S$, then we have $T(s) = T_{K(s)/K}\big(T_{L/K(s)}(s)\big) = [L : K(s)] \cdot T_{K(s)/K}(s)$, which is in R because the minimal polynomial of s has coefficients in R (since s is integral over R).

2. The K-bilinear pairing $(x, y) = T(xy)$ is non-degenerate. This follows from the separability of L over K.

Let $\alpha \in L$. Then there is some nonzero $r \in R$ so that $r\alpha$ is integral over R. To see this, clear denominators in the minimal polynomial of α to get $r\alpha^n + \cdots = 0$; then multiply by r^{n-1} to get $(r\alpha)^n + \cdots = 0$. Therefore, there is a K-basis $\{v_i\}$ of L so that $\{v_i\} \subseteq S$. It follows that $Q(S) = L$. Let $\{u_i\}$ be the "dual K-basis" of $\{v_i\}$ with respect to the pairing above. For any $s \in S$, we have $s = \sum a_i u_i$ with $a_i \in K$. Then $(s, v_j) = a_j = T(s \cdot v_j)$ is in the image of S under T, which is in R. □

Corollary 29.2. *Assume in the situation above that R is noetherian. Then S is module-finite over R and is therefore a noetherian normal domain. If R is a PID, then S is free over R of rank $[L : K]$.*

In the classical case, $R = \mathbb{Z}$ and $K = \mathbb{Q}$. Then L is a number field, and S is the ring of algebraic integers in L. The corollary above says that S is a noetherian normal domain of dimension 1 (a.k.a. a *Dedekind domain*), and is free over $\mathbb{Z}$. In fact, if R is Dedekind, then we can show that S is Dedekind without the separability assumption.

§4. Valuation Domains

1932: Krull wrote a paper, Allgemeine Bewerungstheorie.
1935: Krull wrote a book, Idealtheorie.

Valuation rings (or *valuation domains*) are

- local
- always normal
- noetherian if and only if they are DVRs (or fields)

– possibly infinite dimensional

Proposition 29.3. *For any domain R with quotient field K, the following are equivalent.*

1. *For every non-zero $x \in K$, either $x \in R$ or $x^{-1} \in R$.*
2. *For $a, b \in R$, either $a|b$ or $b|a$ in R.*
3. *The ideals in R form a chain under inclusion. In particular, R is local.*

Such an R is called a valuation ring of K.

Proof. $3 \Rightarrow 2 \Rightarrow 1$ are immediate. Let's do $1 \Rightarrow 3$. Assume 3 does not hold, so there are ideals $I, J \triangleleft R$ with no inclusion relation. Let $a \in I \smallsetminus J$ and $b \in J \smallsetminus I$. Then consider $x = a/b \in K$; $x \notin R$ and $x^{-1} \notin R$, lest $a \in J$ or $b \in I$. □

Definition 29.4. $Val(K)$ is the set of valuation rings of K (including K in particular).

Let $\mathfrak{m} \in \operatorname{Max} R$, with R a valuation ring. Then $K^\times = U(R) \sqcup \mathfrak{m} \smallsetminus \{0\} \sqcup \left\{x^{-1} | x \in (\mathfrak{m} \smallsetminus \{0\}) \smallsetminus \{0\}\right\}$.

Proposition 29.5. *Let L/K be a field extension, $(V, \mathfrak{p}) \in Val(L)$, and let $R = V \cap K$ and $\mathfrak{m} = \mathfrak{p} \cap K$. Then $(R, \mathfrak{m}) \in Val(K)$. That is, $Val(\text{-})$ is a contravariant functor.*

Proof. For $x \in K \smallsetminus R$, $x^{-1} \in V \cap K = R$, so R is a valuation ring of K. Now we will show that $R \smallsetminus \mathfrak{m} = U(R)$ to prove that $\mathfrak{m}$ is the unique maximal ideal of R. Take $x \in R \smallsetminus \mathfrak{m}$, then $x^{-1} \in V \cap K = R$. □

Example 29.6. Let K be an algebraic extension of $\mathbb{F}_p$. What is $Val(K)$? Take any $R \in Val(K)$. Then $\mathbb{F}_p \subseteq R \subseteq K$, so R is a field. Since $Q(R) = K$, we have $R = K$ •

Example 29.7. Let $R = \mathbb{Z}$ and $K = \mathbb{Q}$. Then $Val(K) = \{\mathbb{Q}, \mathbb{Z}_{(p)}\}$. To see this, let $(R, \mathfrak{m}) \in Val(K)$, with $R \neq K$. Then $\mathfrak{m} \neq 0$, so $\mathbb{Z} \cap \mathfrak{m} = (p)$ for some prime p. It follows that $\mathbb{Z} \smallsetminus (p) \subseteq U(R)$, so $\mathbb{Z}_{(p)} \subseteq R$. But $\mathbb{Z}_{(p)}$ is a maximal subring of $\mathbb{Q}$. •

Lecture 30

Exercise III.3: (reciprocal polynomial trick) Show that a unit $u \in S$ is integral over a subring R if and only if $u \in R[u^{-1}]$.

Theorem 30.1. *For a local ring $(R, \mathfrak{m})$, the following are equivalent.*

1. *R is a PID but not a field.*
2. *R is a noetherian normal domain of dimension 1.*
3. *R is noetherian and $\mathfrak{m} = (\pi)$ is principal, with $\pi \notin \operatorname{Nil} R$.*
4. *R is noetherian, $\mathfrak{m} \notin \operatorname{Nil} R$, and $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.*

If these hold, R is called a discrete valuation ring (DVR).

Proof. omitted, but not trivial! [[★★★]] □

Remark 30.2. In a DVR, the ideals are all of the form $\mathfrak{m}^i$ (with $i \geq 0$), and $\dim_{R/\mathfrak{m}} \mathfrak{m}^i/\mathfrak{m}^{i+1} = 1$. $K^\times = U(R) \times \langle \pi \rangle$ (as a group).

Definition 30.3. The element π is called a *uniformizer* of R.

Example 30.4.

DVR	π	$Q(R)$	$U(R)$
$\mathbb{Z}_{(p)}$	p	$\mathbb{Q}$	$\{a/b \mid a, b \text{ prime to } p\}$
$k[[x]]$	x	$k((x))$	$\{a_0 + a_1 x + \cdots \mid a_0 \neq 0\}$
$R = \{f/g \mid f, g \in k[x], \deg f \leq \deg g\}$	$1/x$	$k(x)$	$\{f/g \mid \deg f = \deg g\}$

•

General properties of valuation rings

Theorem 30.5. *Let $R \in Val(K)$, then*

1. *R is normal.*
2. *R is a Bézout ring (every finitely generated ideal is principal).*
3. *Every ring between R and K is also a valuation ring.*
4. *For every $\mathfrak{p} \in \operatorname{Spec} R$, $R/\mathfrak{p}$ is a valuation ring.*
5. *Every proper radical ideal is prime.*
6. *For any proper ideal $I \lhd R$, $I_\infty = \bigcap I^n$ is prime. Moreover, every prime $\mathfrak{p} \not\supseteq I$ is contained in I_∞.*

Proof. (1) Take $u \in K \smallsetminus R$. Then $u^{-1} \in R$, so $R = R[u^{-1}]$, so u is not integral over R by exercise III.3. (2) If I is generated by $a_1, a_2, \ldots, a_n$, then the ideals generated by the a_i form a chain, so I is principal. (3) follows from the first point in the definition of a valuation ring. (4) immediate as for (3). (5) Take $ab \in I$, and assume $a = rb$ for some $r \in R$. Then $(rb)^2 = r \cdot ab \in I$, so $rb = a \in I$. (6) Let $a, b \notin I_\infty$, so $a \notin I^m$ and $b \notin I^n$. Then we have $I^m \subseteq aR$ and $I^n \subseteq bR$. Suppose $ab \in I^{n+m}$, then $ab \in I^m I^n \subseteq aI^n$, so $b \in I^n$. Contradiction. Thus, $ab \notin I^{n+m}$, so $ab \notin I_\infty$. Finally, assume $\mathfrak{p} \not\supseteq I$, then $\mathfrak{p} \not\supseteq I^n$ for each n. Thus, $\mathfrak{p} \subseteq I^n$ for each n, so $\mathfrak{p} \subseteq I_\infty$. □

Question 1: What are the noetherian valuation rings?
Question 2: What are the completely normal valuation rings?

Corollary 30.6. *Let $(R, \mathfrak{m})$ be a valuation ring of K.*

1. *R is noetherian if and only if R is a DVR or a field.*
2. *The following are equivalent.*
   - *(a) R is completely normal.*
   - *(b) R is good (nothing is infinitely divisible by a non-unit).*
   - *(c) $\dim R \leq 1$.*

Proof. (1) $\Leftarrow$ is obvious. Assume R is noetherian, then by the Bézout property, R is a PID. Hence, R is a DVR or a field.

(2) $(a) \Rightarrow (b)$ was done in the last section. $(b) \Rightarrow (c)$ We must show that there is no prime between (0) and $\mathfrak{m}$. Assume there is such a $\mathfrak{p}$, then choose $x \in \mathfrak{m} \smallsetminus \mathfrak{p}$, so $(x) \not\subseteq \mathfrak{p}$. Then $0 = (x)_\infty \supseteq \mathfrak{p}$. $(c) \Rightarrow (a)$ Assume R is not completely normal, so there is some $x \in Q(R) \smallsetminus R$ and $d \in R$ nonzero so that $dx^{-i} \in R$ for all $i \geq 0$. Let $y = x^{-1}$, so $d \in y^i R$ for every $i \geq 0$, so $d \in (y)_\infty$. Thus, $(y)_\infty$ is a non-zero prime ideal. Moreover, if $y = ry^2$, then y would be a unit (since we are in a domain), so $y \notin (y)^2$, so $y \notin (y)_\infty$, so $(y)_\infty$ is not equal to $\mathfrak{m}$. □

Next time: if $R \subseteq K$ is a subring, then $Val_R(K)$ is the set of *relative valuation rings* R' of K which contain R. If $R \in Val(K)$, we'll describe this family.

Welcome to the Krull world

Corollary 30.7. *If $(R, \mathfrak{m})$ is a valuation ring with $\dim R \geq 2$, then $\mathfrak{m}_\infty = \bigcap \mathfrak{m}^n \neq 0$.*

Exercise III.6: replace "$S_{\mathfrak{P}}/R_{\mathfrak{p}}$ with $S_{\mathfrak{P}}/\operatorname{im}(R_{\mathfrak{p}})$.
III.21: $f(x) = \sum_{n=0}^{\infty} \frac{x^n}{2^{n^2}} \in \mathbb{Q}((x))$. This exercise is a little "provisional".

Notation: $D\text{-}Val(K)$ is the set of *discrete* valuation rings of K (this set may be empty).

Example 30.8. If K is an algebraic extension of $\mathbb{F}_p$, then $Val(K) = \{K\}$, $D\text{-}Val(K) = \varnothing$. •

Example 30.9. Take K so that $K^\times = (K^\times)^n$ for some fixed $n \geq 2$. Then $D\text{-}Val(K) = \varnothing$. If $(R, (\pi))$ is a DVR of K, then $\pi = a^n$ for some n, so a is integral over R, so it is in R (because R is normal). But then $(a) = (\pi)^m = (a)^{n+m}$. contradiction. •

For any subring $R \subseteq K$, we defined $Val_R(K)$ to be the elements of $Val(K)$ which contain R. If $R \in Val(K)$, then $Val_R(K)$ is just the set of rings between R and K.

Theorem 30.10 (4.12)**.** *Describing all R' so that $R \subseteq R' \subseteq K$, where $(R, \mathfrak{m}) \in Val(K)$. A typical R' is of the form $R_\mathfrak{p}$, where $\mathfrak{p} \subseteq \mathfrak{m}$ is a prime in R. Furthermore, $\mathfrak{p}R_\mathfrak{p} \overset{!}{=} \mathfrak{p}$ is the maximal ideal.*

Proof. omitted.[[★★★]] □

Consequently, the map $\mathfrak{p} \mapsto R_\mathfrak{p}$ defines an inclusion reversing bijection $\operatorname{Spec} R \leftrightarrow Val_R(K)$. In particular, $Val_R(K)$ is a chain because $\operatorname{Spec} R$ is a chain. The longest chain is the Krull dimension of R. In particular, $\dim R = 1$ if and only if R is a maximal subring of K. DVRs are 1-dimensional, but not all 1-dimensional valuation rings are DVRs.

Definition 30.11. $Val^R(K) = \{R' \in Val(K) | R' \subseteq R \subseteq K\}$. This is only meaningful if $R \in Val(K)$ since any ring containing a valuation ring is a valuation ring (so we would have $Val^R(K) = \varnothing$ if $R \notin Val(K)$).

How do you tell the difference between $Val_R(K)$ and $Val^R(K)$? Well, $Val_R(K)$ has the R below, and $Val^R(K)$ has the R above.

Theorem 30.12 (4.13)**.** *For $(R, \mathfrak{m}) \in Val(K)$, there is an inclusion preserving bijection $Val^R(K) \leftrightarrow Val(R/\mathfrak{m})$, with $R' \mapsto R'/\mathfrak{m} =: \overline{R'}$. Note that $\mathfrak{m} \subseteq \mathfrak{m}' \subseteq R' \subseteq R$, so this makes sense.*

Corollary 30.13 (4.14, Dimension-Summation formula)**.** *In the setting above,* $\dim R' = \dim \overline{R'} + \dim R$.

Proof. easy chain composition argument. □

This allows us to come up with examples of valuation rings with dimension bigger than 1.

Places: intuitively, a place is a "generalized field homomorphism" that may send may elements to "∞".

Definition 30.14. Let K and Ω be fields. Then a *place* is a map $\phi : K \to \Omega \sqcup \{\infty\} =: \Omega_\infty$ so that ϕ is a "field homomorphism " with the usual rules of addition and multiplication for ∞ ($\infty \pm \infty$, $0/0$, ∞/∞, and $\infty \cdot 0$ are undefined).

There is a triumvirate of ideas which are basically the same: valuation rings, places, and Krull valuations.

Working with a place is equivalent to working with a valuation in the following way. Suppose ϕ is a place, then define $R = \phi^{-1}(\Omega)$. R is a valuation ring of K [[★★★]]. Conversely, given a valuation ring $(R, \mathfrak{m})$ of K, there is a place $K \to R/\mathfrak{m} \sqcup \{\infty\}$, sending R to $R/\mathfrak{m}$ in the usual way, and $K \smallsetminus R$ to ∞.

We say $K \to \Omega_\infty$ is the *trivial place* if $\phi(K) \subseteq \Omega$ (i.e. a good old field homomorphism)

Lecture 32

Supplemental points:

- A valuation ring is the same thing as a local Bézout domain.
- A 1-dimensional valuation ring $(R, \mathfrak{m})$ with $\mathfrak{m}$ principal is the same thing as a DVR.
- If R is a valuation ring and $n \leq \infty$, then $\dim R = n$ if and only if $|\operatorname{Spec} R| = n + 1$.
- If $k \subseteq K$ is a subfield, then $Val_k(K)$ is the *Zariski space* (or *Zariski Riemann Surface*) for K/k.

Composition of places: Let $(R, \mathfrak{m}), (R', \mathfrak{m}') \in Val(K)$, with $R' \subseteq R$ (so that $\mathfrak{m} \subseteq \mathfrak{m}' \subseteq R' \subseteq R$). Then we showed that $R'\mathfrak{m} \in Val(R/\mathfrak{m})$, so it comes with a place σ [[★★★]], and we get a commutative diagram of places.

$$\begin{array}{ccc} K & \xrightarrow{\phi} & (R, \mathfrak{m})_\infty \\ & \searrow^{\phi'} & \uparrow_{\sigma} \\ & & (R', \mathfrak{m}')_\infty \end{array} \qquad R' \xrightarrow{\frac{R'}{\mathfrak{m}}} R'/\mathfrak{m}$$

That is, $\phi' = \sigma \circ \phi$. We shoed earlier that $\dim R' = \dim(R'/\mathfrak{m}) + \dim R$. We can phrase this as $\dim(\sigma \circ \phi) = \dim \sigma + \dim \phi$.

Valuation rings on $K = k(x)$. Let's construct examples of $R \in Val_k(K)$ (points in the Zariski Riemann surface).

Example 32.1. Fix a monic irreducible $\pi(x) \in k[x]$, then define $R = k[x]_{(\pi)}$. R is a DVR; it is called the "π-adic valuation ring". $\Omega = k[x]/(\pi) = k[\theta]$ (note that this is already a field), where $\theta = \bar{x}$. The π-adic place is $\phi : K \to \Omega_\infty$, with $\phi(f/g) = f(\theta)/g(\theta)$. Since f/g can be assumed to be in lowest terms, we know when to send f/g to infinity.

In the special case where $\pi = x - a$, then $\theta = \bar{x} = a$, so the place is $f/g \mapsto f(a)/g(a)$. •

Example 32.2. Set $y = 1/x$, then $K = k(x) = k(y)$. Consider the (y)-adic place (or $1/x$ place) is the one with valuation ring $k[y]_{(y)}$. Let's figure out what this ring is in terms of x. If $r(x)$ is a non-zero rational function $\frac{a_0x^n+\cdots+a_n}{b_0x^m+\cdots+b_m} = \frac{x^n(\cdots)}{x^m(\cdots)} = y^{m-n}\frac{a_0+\cdots+a_ny^n}{b_0+\cdots+b_my^m}$. Thus, $\phi(r(x)) = \begin{cases} 0 & m > n \\ \infty & m < n \\ a_0/b_0 & m = n \end{cases}$. So the valuation ring is $S = \{f/g | f, g \in k[x], g \neq 0, \deg f \leq \deg g\}$, with uniformizer $y = 1/x$. •

Theorem 32.3. *$Val_k(K)$ is the exactly the set of rings described in the two examples above.*

Proof. Same as in the computation of all valuation rings of $\mathbb{Q}$. □

If $k = \bar{k}$, then there are only linear irreducibles, so we get a valuation ring in $Val_k(K)$ for every point in $\mathbb{P}^1_k$. Thus the terminology "Zariski Riemann surface".

Definition 32.4. A valuation ring $(R, \mathfrak{m})$ has *principal type* if $\mathfrak{m} = (\pi) \neq 0$. We still call π a uniformizer, but there is no noetherian hypothesis. Equivalently, we can say that $\mathfrak{m}$ is non-zero and finitely generated (because R is Bézout).

These rings emulate DVRs. In dimension 1, these are exactly DVRs. Note that if R is noetherian, Krull's principal ideal theorem doesn't apply, so $\mathfrak{m}$ can have large height even through it is principal. We say that a place has principal type if the corresponding valuation ring does.

Claim. *In the composition of places picture, if σ (i.e. $R'/\mathfrak{m}$) has principal type, then so does ϕ' (i.e. R' has principal type).*

Proof. Write $\mathfrak{m}' = \pi R' + \mathfrak{m}$, with $\pi \notin \mathfrak{m}$. Since $(\pi) \not\subseteq \mathfrak{m}$, we must have $\mathfrak{m} \subseteq (\pi)$. This implies that $\mathfrak{m}' = (\pi)$, so R' has principal type. □

Example 32.5.

$$\begin{array}{ccc} K = \mathbb{Q}(x) & \xrightarrow[\mathbb{Q}[x]_{(x)}]{\phi} & \mathbb{Q}_\infty \\ & \searrow^{\phi'} & \downarrow{\scriptstyle \mathbb{Z}_{(p)}}\ \sigma_p \\ & & (\mathbb{F}_p)_\infty \end{array}$$

We get that ϕ' has principal type because the maximal ideal of $\mathbb{Z}_{(p)}$ is principal. Let R' be the valuation ring associated to ϕ'. Then $\dim R' = 2$ and R' has principal type. $R' = \{f(x)/g(x) \big| x \nmid g(x), f(0)/g(0) \in \mathbb{Z}_{(p)}\}$. The uniformizer is p. •

Lecture 33

If k is a field, and $F = k(x_1, \ldots, x_{n-1})$, $K = k(x_1, \ldots, x_n) = F(x_n)$. Then there is an $R \in Val_k(K)$ of principal type with residue field k and $\dim R = \ell$ for any $0 \leq \ell \leq n$.

"Compose and induct": $K = F(x_n) \xrightarrow{(x_n)\text{-adic}} F_\infty \searrow k_\infty$

§5 Krull Valuations

In this section KV means "Krull valuation" and OAG means "ordered abelian group".

Definition 33.1. An *OAG* is an (additive) abelian group $(\Gamma, \leq)$, where $\leq$ is a total ordering of Γ that respects the addition (i.e. $a \leq b \Rightarrow a + c \leq b + c$).

Given such a Γ, we define the *positive cone* of Γ by $\Gamma^+ := \{a \in \Gamma | a \geq 0\}$. Γ^+ is a sub-monoid of Γ that satisfies the properties $\Gamma^+ \cap -\Gamma^+ = \{0\}$ and $\Gamma^+ \cup -\Gamma^+ = \Gamma$. Conversely, if $P \subseteq \Gamma$ is a sub-monoid satisfying these properties, and Γ does not have an order, then we may define an order by $a \leq b \Leftrightarrow b - a \in P$.

Remark 33.2.

– An OAG is always torsion-free.

– Any subgroup of an OAG is also an OAG.

– We may reverse the order and get another OAG. Note that this is not true for ordered fields ($1 = 1 \cdot 1$ implies that 1 is in the positive cone).

– Morphisms of OAGs are order-preserving.

– Given OAGs $(\Gamma_i, \leq)$, we may define an order on $\Gamma = \Gamma_1 \times \cdots \Gamma_n$ lexicographically. In the case $n = 2$, the positive cone looks like $(\Gamma_1^+ \smallsetminus 0) \times \Gamma_2 \cup 0 \times \Gamma_2^+$.

Example 33.3. The zero group, $\mathbb{Z}$, $\mathbb{Q}$, ... (irrational stuff), $\mathbb{R}$ are OAGs with their usual orderings. For instance, if $\alpha_1, \ldots, \alpha_n \in \mathbb{R}$ are $\mathbb{Q}$-linearly independent, then we may take Γ to be $\sum \alpha_i \mathbb{Z}$ or $\sum \alpha_i \mathbb{Q}$. For example, $\mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}[\sqrt[3]{2}]$. These are isomorphic to $\mathbb{Z}^2$ and $\mathbb{Z}^3$. Note that you can also put lexicographic orderings on these groups. •

Definition 33.4. Given a domain A, a *KV* is a map to an OAG $v : A \smallsetminus \{0\} \to \Gamma$ such that

1. $v(ab) = v(a) + v(b)$ for a, b non-zero.
2. $v(a + b) \geq \min\{v(a), v(b)\}$ if a, b, and $a + b$ are non-zero.

It is useful to introduce $\Gamma_\infty := \Gamma \sqcup \{\infty\}$, and define $v(0) = \infty$ and $\Gamma < \infty$. We also define $a + \infty = \infty$ for all $a \in A$, $\infty + \infty = \infty$ (this is different from what we did with places)

Proposition 33.5. *1.* $v(\pm 1) = 0$.

2. $v(-a) = v(a)$ *for all* $a \in A$.

3. (Predictable value property) If $v(a_1), \ldots, v(a_n)$ *are all distinct, then* $v(a_1 + \cdots + a_n) = \min\{v(a_i)\}$.

Proposition 33.6. $v : A \smallsetminus \{0\} \to \Gamma$ *as above can be uniquely extended to a KV* $v : Q(A) \smallsetminus \{0\} \to \Gamma$.

Proof. Uniqueness is easy because we must have $v(a/b) = v(a) - v(b)$ for a, b non-zero. For existence, use this formula as a definition and verify the conditions in the definition.[1] □

Definition 33.7. If $v : K^\times \to \Gamma$ is a KV on a field K, then the image $v(K^\times)$ is called the *value group* of v. It is an OAG (unlike in the case of a domain, where you only get a monoid).

Definition 33.8. $|\cdot| : A \smallsetminus \{0\} \to \Gamma$, where Γ is a (multiplicative) OAG, is called a *KV* if $|ab| = |a| \cdot |b|$ and $|a + b| \geq \max\{|a|, |b|\}$ for a, b, and $a + b$ non-zero.

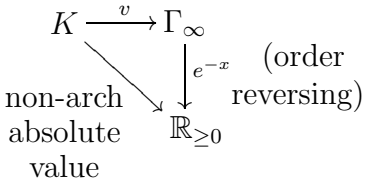
This is the same definition, but with Γ written multiplicatively and the order reversed. These are also called *non-archimedean absolute values* when $\Gamma = \mathbb{R}_{>0}$ and A is a field. Instead of introducing "∞", we introduce "0".

Theorem 33.9. *A valuation on a field* $v : K \to \Gamma_\infty$ *determines a valuation ring* $R_v := \{a \in K | v(a) \geq 0\} \in Val(K)$. *Conversely, a valuation ring* $R \in Val(K)$ *determines a KV* $v_R : K^\times \to \Gamma_R := K^\times / U(R)$, *suitably ordered.*

[1] "I don't think I've ever checked this."

Lecture 34

There are non-archimedean absolute values ($|a+b| \leq \max\{|a|,|b|\}$) and Krull valuations. The archimedean absolute values are exactly the real Krull valuations.



An OAG $(\Gamma, \leq)$ is called *archimedean* if for all $x, y > 0$ in Γ if there is some $n \in \mathbb{N}$ such that $nx > y$.

Theorem 34.1 (Hölder, 1901)**.** *$(\Gamma, \leq)$ is archimedean if and only if it can be order embedded into $(\mathbb{R}, \leq)$.*

Thus, non-archimedean absolute values are the Krull valuations with archimedean ordered group. How confusing!

Relating KVs to valuation rings. Suppose $v : K \to \Gamma_\infty$ is a KV, then we may define $R_v := \{a \in K | v(a) \geq 0\}$. This is a valuation ring with $\mathfrak{m}_v = \{a \in K | v(a) > 0\}$. Conversely, if $R \in Val(K)$, define a KV $v : K^\times \to \mathrm{Prin}(R)$, where $\mathrm{Prin}(R)$ is the group of principal fractional ideals $aR \subseteq {}_RK$, where $a \in K^\times$. When R is a valuation ring, $\mathrm{Prin}(R)$ is an OAG, ordered by REVERSE inclusion. Then define $v(a) = aR$ and check that $v(ab) = abR = aR \cdot bR = v(a) + v(b)$ and that $v(a+b) = (a+b)R \supseteq v(a), v(b)$.

There is another useful view of the value group. Look at $K^\times / U(R)$, ordered by $aU(R) \leq bU(R)$ when $b/a \in R$. Then we have an order isomorphism $K^\times/U(R) \to \mathrm{Prin}(R)$, given by $aU(R) \mapsto aR$.

Corollary 34.2. *There is a one to one correspondence between $Val(K)$ and equivalence classes of KVs on K, where $v : K^\times \twoheadrightarrow \Gamma$ and $v' : K^\times \twoheadrightarrow \Gamma'$ are equivalent if there is an order isomorphism between Γ and Γ'.*

Definition 34.3. A KV $K \twoheadrightarrow \Gamma \cong \mathbb{Z}$ is called a *discrete valuation*. Rings corresponding to discrete valuations are DVRs.

Example 34.4. If A is a UFD, with quotient field K and some irreducible element π (so π generates a prime ideal). Define $v = v_\pi : A \setminus \{0\} \to \mathbb{Z}$ by $v(a) = \max\{n | \pi^n \text{ divides } a \text{ in } A\}$; this is called the π-adic KV. It is easy to check that this is a KV. This valuation corresponds to the DVR $A_{(\pi)}$. Here are some examples of such things.

- $A = \mathbb{Z}$ and $\pi = p$, then you get the usual p-adic valuation on $\mathbb{Q}$.
- $A = k[[x]]$ and $\pi = x$, then $v(f)$ is the order of vanishing (or of a pole) at 0.

- $A = k[x]$, and π a monic irreducible, then you get the $\pi(x)$-adic valuation.
- $A = k[x]$, and $v : k[x] \smallsetminus \{0\} \to \mathbb{Z}$ given by $f \mapsto -\deg(f)$. This gives a discrete valuation on $k(x)$. This is the $1/x$-adic valuation!

•

Example 34.5. What is the transcendence degree of $k(\!(t)\!)$ over k? It must be ∞, because it cannot be any integer like 17.

Then we can embed $K = k(x_1, \ldots, x_n) \hookrightarrow k(\!(t)\!)$ and use the t-adic valuation, giving a discrete valuation on K! We need to check that this valuation is non-trivial.

$$K \qquad k(\!(t)\!)$$

$$R \qquad k[[t]] = V$$

$$\mathfrak{m} \qquad tV$$

We have $k \subseteq R/\mathfrak{m} \hookrightarrow V/tV = k$, so $R/\mathfrak{m} = k$. Thus, the valuation ring R is non-trivial (it is not all of K). •

We haven't proven that $tr.d._k k(\!(t)\!) = \infty$, and I [Lam] think it is hard. Let's show that $tr.d._{\mathbb{Q}} \mathbb{Q}(\!(t)\!) \geq 2$. We claim that t and $e^t = \sum t^n/n!$ are algebraically independent. Assume that $f_0(t)(e^t)^n + f_1(t)(e^t)^{n-1} + \cdots = 0$. We may assume that not all of the $f_i(t)$ are divisible by $t - 1$. Then substitute $t = 1$ to get that e is algebraic over $\mathbb{Q}$, a contradiction!

For general k, we can also show that t and $1 + t^{1!} + t^{2!} + t^{3!} + \cdots$ are algebraically independent.

Lecture 35

The notes have been revised to contain some more stuff. When is $(R, \mathfrak{m})$ or principal type? Here are some necessary and sufficient conditions (individually ... any of them is enough)

- $\mathfrak{m} \neq \mathfrak{m}^2$
- R surjects onto a DVR.
- $\Gamma^+ \setminus \{0\}$ has a least element.

Any OAG Γ is a valuation group. That is, there is a surjective valuation $v : K \twoheadrightarrow \Gamma_\infty$. For example, let $\Gamma = \mathbb{Q}$ with the usual ordering. This produces a valuation ring $(R, \mathfrak{m})$ which is not of principal type ($\mathfrak{m} = \mathfrak{m}^2$).

To prove the result, form the group algebra $A = k\Gamma$ over a fixed field k, with formal basis $\{t_\alpha | \alpha \in \Gamma\}$, with $t_\alpha t_\beta = t_{\alpha+\beta}$. Given $f \in A$, we have $f = \sum a_\alpha t_\alpha = a_{\alpha_0} t_{\alpha_0} +$"higher terms" with $a_{\alpha_0} \neq 0$ ... we're taking α_0 to be the least element that appears. Define $v(f) = \alpha_0$. It is immediate that this v is a valuation, and that it surjects onto Γ. In particular, A is a domain. Note that the residue field is k.

Convex subgroups of an OAG: A subgroup $G \subseteq \Gamma$ is called *convex* (or *isolated*) if whenever $0 \leq a \leq b$ and $b \in G$, we also have $a \in G$.

Theorem 35.1. *Convex subgroups are exactly the kernels of OAG morphisms.*

Proof. If $G = \ker(\phi : \Gamma \to \Gamma')$ and $0 \leq a \leq b$ with $\phi(b) = 0$, then we get $0 \leq \phi(a) \leq 0$, so $\phi(a) = 0$.

Conversely, if G is a convex subgroup of Γ, then we declare a non-identity coset positive if all elements are positive. After some checking, this makes Γ/G into an OAG, and the natural map $\Gamma \to \Gamma/G$ is an OAG morphism. [[★★★]] □

Lemma 35.2. *Convex subgroups of* Γ *form a chain (under inclusion).*

Proof. easy to check [[★★★]] □

Definition 35.3. The *order-rank* of an OAG is the order type of the chain of convex subgroups. If you're a baby, you can define o-rk$(\Gamma) = n \in \mathbb{Z}$ if Γ has exactly $n + 1$ convex subgroups, and ∞ otherwise.

There is an order reversing bijection between convex subgroups of Γ and prime ideals in R (any valuation ring with valuation group Γ), given by $G \mapsto \{a \in R | v(a) > G\}$.

$$0 \qquad \mathfrak{m}$$

$$\Gamma \qquad (0)$$

– As a corollary, o-rk$(\Gamma) = \dim R$.

– o-rk$(\Gamma) \leq 1$ corresponds to Γ being archimedean.

– o-rk$(\Gamma) \leq rk(\Gamma) := \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma)$.

§6. Characterizations of Normal Domains

Lemma 35.4 (Chevalley)**.** *Let $K \supseteq V$ be rings, and let $u \in U(K)$. If $I \lhd V$ is a proper ideal, then either $I \cdot V[u] \neq V[u]$ or $I \cdot V[u^{-1}] \neq V[u^{-1}]$.*

Proof. Tricky calculation. [[★★★]] □

Theorem 35.5 (Existence theorem for valuation rings)**.** *Let S be a sub-ring of a field K, and let $\mathfrak{p} \in \operatorname{Spec} S$. Then there exists a valuation ring $(V, \mathfrak{m}) \in Val(K)$ containing S such that $\mathfrak{m} \cap S = \mathfrak{p}$.*

Proof. Localize at $\mathfrak{p}$ first, so we may assume S is local and $\mathfrak{p}$ is the maximal ideal.

Consider the family $\mathcal{F} = \{T | S \subseteq T \subseteq K, \mathfrak{p}T \neq T\}$, ordered by inclusion. It is easy to see that Zorn's lemma applies to give a maximal member V. Then check that V is a valuation ring of K: if $u, u^{-1} \in K \smallsetminus V$, then you could extend V by Chevalley's lemma, contradicting maximality, so either $u \in V$ or $u^{-1} \in V$. □

Definition 35.6. Let $(S, \mathfrak{p})$ and $(V, \mathfrak{m})$ be local rings, with $S \subseteq V$. We say that V *deominates* S (written $V \geq S$ or $S \leq V$) if $\mathfrak{m} \cap S = \mathfrak{p}$.

This can be understood in two alternative ways. It is sufficient for $\mathfrak{p} \subseteq \mathfrak{m}$, or to say that $\mathfrak{p}V \subsetneq V$.

In general, if K/F is a field extension and $(V, \mathfrak{m})$ is a local ring in K, then $(S, \mathfrak{p}) = (F \cap V, F \cap \mathfrak{m})$ a local ring dominated by $(V, \mathfrak{m})$. To see that S is local, let $a \in S \smallsetminus \mathfrak{p} \subseteq V \smallsetminus \mathfrak{m}$, then a is invertible in V and the inverse must lie in F, so a is invertible in S.

Given a field K, define $Loc(K)$ to be the set of local rings in K.

Theorem 35.7. *For every field K, $Loc(K)^* = Val(K)$, where $loc(K)$ is ordered by dominance.*

Proof. If $S \in Loc(K)^*$, then there is a $V \in Val(K)$ so that $V \geq S$ [[★★★]]. This implies $V = S$. Conversely, if $(V, \mathfrak{m}) \in Val(K)$, then if $V' \geq V$ in $Loc(K)$, $\mathfrak{m}' \subseteq \mathfrak{m}$, so V' cannot dominate V, so V is maximal in $Loc(K)$. □

Lecture 36

Results presented in the notes:

1. K/k field extension, with $v : K^\times \twoheadrightarrow \Gamma$ trivial on k, then o-rk$\Gamma \leq rk(\Gamma) \leq tr.d._k K$.

2. $tr.d._k K = 1$, $R \in Val_k(K)$, then R is a DVR. See Hartshorne §I.6.

Theorem 36.1. *Let $R \subseteq K$ is a sub-ring of a field, with integral closure C. Define $T = \bigcap\{V \in Val_R(K)\}$. Then $C = T$. We could also define the intersection T by restricting to those V whose maximal ideals contract to a maximal ideal in R. In particular, if R is local, then we only intersect those V which dominate R.*

Corollary 36.2. *A domain is normal if and only if it is an intersection of some family of valuation rings of its quotient field.*

Proof of Theorem. $C \subseteq T$: each V is normal and contains R, so integral elements over R are contained in each V.

Conversely, assume $x \notin C$. By the reciprocal polynomial trick (Ex. III.3) $x \notin R[x^{-1}] = S$. Then $x^{-1} \notin U(S)$ (let $x \in S$). Choose some $\mathfrak{p} \in \text{Max}(S)$ containing x^{-1}. By the existence theorem, there is some $(V, \mathfrak{m}) \in Val(K)$ so that $S \subseteq V$ and $\mathfrak{m} \cap S = \mathfrak{p}$. We have that $x^{-1} \in \mathfrak{p} \subseteq \mathfrak{m}$, so $x \notin V$.

Claim: $\mathfrak{m} \cap R$ is a maximal ideal in R.
$\mathfrak{m} \cap R = \mathfrak{m} \cap S \cap R = \mathfrak{p} \cap R$. Consider the map $R \to S \to S/\mathfrak{p}$; since x^{-1} is killed by the second map, the composition is onto, with kernel $\mathfrak{p} \cap R$. Since we chose $\mathfrak{p} \in \text{Max}(S)$, $S/\mathfrak{p}$ is a field, so $\mathfrak{p} \cap R$ is maximal. □

Theorem 36.3. *Let R be a noetherian domain with quotient field K. Then R is normal if and only if*

(Nor1) *for any height 1 prime $\mathfrak{p} \in R$, $R_\mathfrak{p}$ is a DVR, and*

(Nor2) *for any $0 \neq a \in R$, all primes in the set $\text{Ass}\big(R/(a)\big)$ have height 1.*

In this case, $R = \bigcap_{ht(\mathfrak{p})=1} R_\mathfrak{p}$.

Proof. Suppose Nor1 and Nor2. First we check $R = \bigcap_{ht(\mathfrak{p})=1} R_\mathfrak{p}$. If this holds, then since each $R_\mathfrak{p}$ is normal, R is normal. Let $a, b \in R$ with $a \neq 0$, an assume $b/a \in R_\mathfrak{p}$ for each $\mathfrak{p}$ of height 1. Consider a minimal primary decomposition $aR = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, with $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Each $\mathfrak{p}_i$ has height 1 [[★★★]], so they are all isolated primes, so each $\mathfrak{q}_i$ is determined: $\mathfrak{q}_i = aR_{\mathfrak{p}_i} \cap R$. By assumption, $b \in aR_{\mathfrak{p}_i} \cap R = \mathfrak{q}_i$, so $b \in aR$, so $b/a \in R$.

Now suppose R is normal. To verify Nor1, take $\mathfrak{p}$ of height 1. Then $R_\mathfrak{p}$ is clearly normal, local, noetherian, and dimension 1, so by an earlier characterization, $R_\mathfrak{p}$ is a DVR. To verify Nor2, consider $\mathfrak{p} \in \text{Ass}(R/aR)$. Localize at $\mathfrak{p}$, so we may assume

$(R, \mathfrak{p})$ is local. We want to show that $ht(\mathfrak{p}) = 1$. We can write $\mathfrak{p} = aR : b$, with $b \neq 0$ in aR, so $a^{-1}b\mathfrak{p} \subseteq R$.

Case 1: If $a^{-1}b\mathfrak{p} = R$, $\mathfrak{p} = ab^{-1}R$, so $\mathfrak{p}$ is principal with generator a/b. This implies $R_{\mathfrak{p}}$ is a DVR (being a noetherian local domain with principal maximal ideal), so it is dimension 1, so $ht(\mathfrak{p}) = 1$.

Case 2: If $a^{-1}b\mathfrak{p} \subsetneq R$, then $a^{-1}b\mathfrak{p} \subseteq \mathfrak{p}$, so by the determinant trick, $a^{-1}b$ is integral over R. Since R is normal, $a^{-1}b \in R$, so $b \in aR$, a contradiction. □

Some other results follow.

Theorem 36.4. *A noetherian domain R is a UFD if and only if every height 1 prime is principal.*

The proof depends on the following result.

Theorem 36.5. *A domain R is a UFD if and only if*

1. *every non-zero non-unit is a finite product of irreducible elements, and*
2. *every irreducible element generates a prime ideal.*

Lecture 37

Easy applications of the Existence theorem:

1. K/F any field extension, then $Val(K) \twoheadrightarrow Val(F)$
2. K/k algebraic if and only if $Val_k(K) = \{K\}$.
3. $Val(K) = \{K\}$ if and only if K is algebraic over some $\mathbb{F}_p$.
4. charaterization of noetherian normal domains via height 1 primes. (Later, we'll do some Krull ring stuff, maybe)

We'd like to characterize UFDs.

Theorem 37.1 (Characterization of UFDs)**.** *For a domain R, the following are equivalent.*

1. *R is a UFD.*
2. *Every non-zero prime ideal contains a prime element.*
3. *Principal ideal satisfy ACC, and every irreducible element is prime.*

Proof. $3 \Rightarrow 2$. Let $\mathfrak{p} \in \operatorname{Spec} R$ be non-zero. Fix a non-zero $a \in \mathfrak{p}$, and write $a = p_1 \cdots p_n$ with the p_i irreducible (we can do this because we have ACC on principal ideals). Then some p_i is in $\mathfrak{p}$, and p_i is prime by assumption.

$2 \Rightarrow 1$. Form the multiplicative set $S = \{up_1 \cdots p_n | u \in U(R), n \geq 0, p_i \text{ prime}\}$. We claim that this multiplicative set is saturated, i.e. whenever $ab \in S$, a and b are in S. This is because any factor of $up_1 \cdots p_n$ is of the same form; suppose $xy = up_1 \cdots p_n$, then p_1 divides either x or y, so we cancel it and induct. Thus, $R \smallsetminus S = \cup \mathfrak{p}_i$ is a union of primes (by earlier stuff). If some $\mathfrak{p}_i$ is non-zero, then it contains a prime element p, which would be in S. Thus, each $\mathfrak{p}_i$ is zero, so $S \cup \{0\} = R$. So every non-zero element has a prime factorization, from which uniqueness follows in the usual way (note that we needed a prime factorization, not just an irreducible factorization).

$1 \Rightarrow 3$. In a UFD, it is clear that irreducible elements are prime. If ACC fails for principal ideals, we have $a_1 R \subsetneq a_2 R \subsetneq \cdots$. Then we have $a_n = r_{n+1} a_{n+1}$, where r_{n+1} is not a unit. Then $a_1 = r_2 a_2 = r_2 r_3 \cdots r_{n+1} a_{n+1}$ for any n. Thus, a_1 is divisible by n primes (counting multiplicity) for any n, a contradiction. □

Let's assume the following theorem for the moment.

Theorem 37.2 (Krull's Principal Ideal Theorem)**.** *Let R be noetherian. If $\mathfrak{p}$ is a minimal prime over some principal ideal aR, then $ht(\mathfrak{p}) \leq 1$.*

Theorem 37.3. *Let R be a domain. If R is a UFD, then every height 1 prime is principal. If R is noetherian, then the converse is true.*

Proof. ($\Rightarrow$) Consider $\mathfrak{p} \in \operatorname{Spec}_1(R)$.[1] Consider a non-zero $a \in \mathfrak{p}$, so $a = p_1 \cdots p_n$, for some primes p_i. Then some $p_i \in \mathfrak{p}$, so $0 \subsetneq (p_i) \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is height 1, we get $\mathfrak{p} = (p_i)$.

($\Leftarrow$) Now we assume R is noetherian and every height 1 prime is principal. We will verify property 2 in the characterization of UFDs. If $\mathfrak{p}$ is a non-zero prime, it contains some non-zero principal ideal aR. By Zorn's Lemma, there is a minimal prime $\mathfrak{p}'$ over aR contained in $\mathfrak{p}$. By the PIT, $\mathfrak{p}'$ has height 1 (it cannot be zero because we are in a domain). By assumption, $\mathfrak{p}'$ is principal, generated by some prime element (which is in $\mathfrak{p}$). □

Easy fact: If R is a UFD and S is a multiplicative set, then $R_S = S^{-1}R$ is a UFD.

Theorem 37.4 (Nagata)**.** *Assume R is a domain, and S is a multiplicative set generated by some family $\{p_i\}$ of prime elements. Then R is a UFD if and only if R has ACC_{prin} and R_S is UFD.*

Proof. ($\Rightarrow$) Follows from the easy fact and the characterization of UFDs.

($\Leftarrow$) Assuming the given conditions, we will check condition 2 of the characterization of UFDs. Fix a non-zero $\mathfrak{p} \in \operatorname{Spec} R$. If $\mathfrak{p} \cap S \neq \varnothing$, then $\mathfrak{p}$ contains a prime element because S is generated by prime elements and $\mathfrak{p}$ is prime. So assume $\mathfrak{p} \cap S = \varnothing$. Upon localizing at S, we know that $\mathfrak{p}_S$ contains some prime element because R_S is a UFD. Take $\pi \in \mathfrak{p}$ which maps to a prime element $\pi \in \mathfrak{p}_S$ (we can scale by "units" from S if needed). If π is divisible by some p_i, say $\pi = \pi_1 p_i$, then $\pi_1 \in \mathfrak{p}$ and π_1 maps to the same prime element (well, an associate) in $\mathfrak{p}_S$. Repeating, we may assume π has no factor p_i (because we have ACC on principal ideals in R). Now we claim that π is a prime in $\mathfrak{p}$. To check this, assume $\pi | ab$. Locally, we have $\pi | a$ (or b), so $p_{i_1} \cdots p_{i_k} a = \pi r$ for some $r \in R$ and some p_{i_j}. Since no p_i divides π, they must all divide r. So $a = \pi r'$ for some $r' \in R$, so $\pi | a$. Thus, π is prime, as desired. □

We all know the following theorem.

Theorem 37.5 (Gauss)**.** *If R is a UFD, then $R[x]$ is a UFD.*

However, $R[[x]]$ may fail to be a UFD, even if R is noetherian.

Example 37.6. Let $R = \mathbb{F}_2[x, y, z]/(x^2 + y^3 + z^7)$. This is a noetherian UFD, but $R[[t]]$ is not a UFD. •

Theorem 37.7. *If R is a PID, then $A = R[[x]]$ is a UFD.*

Proof. Again, we'll check that second condition for A. Let $\mathfrak{P} \in \operatorname{Spec} A$ be non-zero. If $\mathfrak{P} \cap R$ is generated by n elements, then $\mathfrak{P}$ is generated by at most $n+1$ elements (we only need the extra generator if $x \in \mathfrak{P}$) as in the proof of the Hilbert basis theorem. If $x \in \mathfrak{P}$, we are done because x is a prime element. If $x \notin \mathfrak{P}$, $\mathfrak{P}$ is generated by n elements. Since R is a PID, $n = 1$, so $\mathfrak{P}$ is principal, generated by some prime element. □

[1] $\operatorname{Spec}_n R$ denotes the set of height n primes of R.

Lecture 38

Normality is a local property. If you localize a UFD, it is still a UFD, but if all the localizations at maximal ideals are UFDs, the ring need not be a UFD, so being a UFD is not a local property. For example, $R = \mathbb{Z}[\sqrt{-5}]$, then $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ are two essensially different factorizations (you can check that all the everything is irreducible using the norm). Since R is the full ring of algebraic integers of $\mathbb{Q}[\sqrt{-5}]$, it is a Dedekind domain, so all its localizations are DVRs, so they are UFDs.

How do you use the Nagata theorem to check if a domain R is a UFD? Find a prime element $p \in R$, and look at $R[1/p]$. We know by the theorem that if the later is a UFD, then so is R. Perhaps we can find some UFD which localizes to $R[1/p]$.

For example, consider $R_n = \mathbb{R}[x_0, \cdots, x_n]/(x_0^2 + \cdots + x_n^2 - 1)$, the coordinate ring of the n-sphere, and let $A_n = R_n \otimes_{\mathbb{R}} \mathbb{C}$.

Theorem 38.1. *(1) R_n is a UFD if $n \geq 2$. (2) A_n is a UFD if $n \geq 3$ (or if $n = 1$).*

Proof. (1) First we show that $1-x_0 \in R$ is prime. To see this, note that $R/(1-x_0) = \mathbb{R}[x_1, \ldots, x_n]/(x_1^2 + \cdots + x_n^2 = 0)$. Since $n \geq 2$, the sum of squares is irreducible, so it is prime. Thus, $R/(1-x_0)$ is a domain.

Let $t := (1-x_0)^{-1}$. The localization is $\mathbb{R}[x_0, \cdots, x_n, t] = \mathbb{R}[tx_1, \ldots, tx_n, t^{-1}]$ (all these adjunctions are done in the quotient ring of R). To see this, note that tx_i is in the left hand side, and $t^{-1} = 1 - x_0$ is also in the left hand side. To see the reverse inclusion, note that $x_0 = 1 - t^{-1}$ and $x_i = t^{-1} \cdot tx_i$ for $i \geq 1$. Finally, $(tx_1)^2 + \cdots (tx_n)^2 = t^2 - t^2x_0^2 = t^2 - (t-1)^2 = 2t - 1$, so t is in the right hand side. But $\mathbb{R}[tx_1, \cdots, tx_n]$ is a polynomial ring (which contains t by the computation above), and the right hand side is the localization at t.

(2) For $n = 1$, we have $\mathbb{C}[x_0, x_1]/(x_0^2 + x_1^2)$. We change variables to $z = x_0 + ix_1$ and $\bar{z} = x_0 - ix_1$. Then the relation is $z\bar{z} = 1$, so $\bar{z} = z^{-1}$. Thus, we have the ring $\mathbb{C}[z, z^{-1}]$, the Laurent polynomial ring, which is a UFD.

Now we do $n \geq 3$.

Case 1: $n = 2k$ with $k \geq 2$. Do a change of variables to get $A_n = \mathbb{C}[z_0, \cdots, z_{2k}]/(z_0^2 + z_1z_2 + \cdots + z_{2k-1}z_{2k} = 1)$. Now we check that z_1 is a prime: $A/(z_1) = \mathbb{C}[z_0, z_2, \cdots, z_{2k}]/(z_0^2 + z_3z_4 + \cdots + z_{2k-1}z_{2k} = 1) = A_{n-2}[z_2]$ which is a domain. Is $A[z_1^{-1}]$ a domain? Well, $A[z_1^{-1}] = \mathbb{C}[z_0, z_1, \cancel{z_2}, z_3 \cdots, z_{2k}, z_1^{-1}]/(z_0^2 + z_1z_2 + \cdots + z_{2k-1}z_{2k} = 1) = \mathbb{C}[z_0, z_1, z_3 \cdots, z_{2k}][z_1^{-1}]$ is a localization of a UFD, so it is a UFD.

Case 2: $n = 2k + 1$ with $k \geq 1$. As in case 1, we change variables to get $A_n = \mathbb{C}[z_0, \cdots, z_{2k+1}]/(z_0z_1 + \cdots + z_{2k-1}z_{2k} = 1)$. Then z_0 is a prime: $A_n/(z_0) \cong A_{n-2}[z]$ is a domain (this is why $n = 2$ doesn't work, because $A_{n-2} = A_0$ is not a domain). Now check that $A[z_0^{-1}] = \mathbb{C}[z_0, \cdots, z_{2k+1}, z_0^{-1}]/(z_0z_1 + \cdots + z_{2k-1}z_{2k} = 1) = \mathbb{C}[z_0, z_2, \cdots, z_{2k+1}][z_0^{-1}]$ is a localization of a UFD. □

Theorem 38.2. *R_1 and A_2 are not UFDs.*

Intuitively, $R_1 = \mathbb{R}[x,y]/(x^2+y^2=1)$, so we get $x^2 = (1+y)(1-y)$, and we can believe that these are two different factorizations. $A_1 = \mathbb{C}[x,y,z]/(x_2+y^2+z^2=1)$, so we get $(x+iy)(x-iy) = (1-z)(1+z)$.

Chapter IV. Dedekind domains and Krull domains

We will only give an overview.

Let R be a domain, with $K = Q(R)$. A *fractional ideal* is an R-submodule $A \subseteq {}_RK$ so that there exists a non-zero $r \in R$ so that $rA \subseteq R$.

Example 38.3.

- Any ideal $I \lhd R \subseteq K$ is a fractional ideal; actual ideals are sometimes called *integral* ideals.
- If $A \subseteq {}_RK$ is finitely generated, then it is a fractional ideal.
- $s \in K$ is almost integral (all powers have a common denominator) if and only if $R[s]$ is a fractional ideal. •

Given fractional ideals A and B, $A \cdot B = \{\sum a_i b_i\}$ is a fractional ideal. Thus, the set of fractional ideals $Id(R)$ forms a monoid (with identity R).

Definition 38.4. An R-submodule $A \subseteq {}_RK$ is called *invertible* if there is some R-submodule $B \subseteq {}_RK$ so that $A \cdot B = R$.

Such an A is always finitely generated as an R-module (express 1 as $\sum a_i b_i$ and show that the a_i generate), so all invertible ideals are fractional ideals. The invertible fractional ideals are exactly the invertible elements of the monoid $Id(R)$. Let $Inv(R)$ be the group of invertible fractional ideals. We have that $Prin(R)$, the set of principal fractional ideals, forms a subgroup. The factor group $C(R) = Inv(R)/Prin(R)$ is called the *ideal class group* of R.

Definition 38.5. A domain R is *Dedekind* if (1) R is noetherian, (2) R is normal, and (3) $\dim R \leq 1$.[1]

The following hold for Dedekind domains.

1. R is a field or R is noetherian with $R_{\mathfrak{m}}$ a DVR for all $\mathfrak{m} \in \operatorname{Max} R$.
2. All non-zero fractional ideals are invertible ($Id(R) = Inv(R)$).
3. Every ideal is a finite product of primes (note that we do not assume noetherian)

[1]Some people like to say $\dim R = 1$ to exclude fields from being Dedekind. We allow fields to be Dedekind so that PIDs $\Rightarrow$ Dedekind. However, we like to think of Dedekind domains as locally DVRs, which fails for fields. Whatever, you can never make everybody happy.

Lecture 39

Final Exam: Do three exercises.
R is a domain throughout. $C(R) = Inv(R)/Prin(R)$ is the ideal class group. The following are equivalent.

- R is a Dedekind domain
- R is noetherian, normal, and of dimension ≤ 1 (this is the definition)
- non-zero ideals are invertible
- for all $I \triangleleft R$, $I = \mathfrak{p}_1^{r_1} \cdots \mathfrak{p}_n^{r_n}$ uniquely (except for $I = 0$), with $n \geq 0$ and $r_i \geq 1$.

This last condition is a very important one.

Robert Lee Moore's method: he would write all the theorems and definitions in a subject and have his students figure out the proofs.

A dozen things every Good Algebraist should know about Dedekind domains. R is a Dedekind domain.

1. R is local $\iff$ R is a field or a DVR.
2. R semi-local $\implies$ it is a PID.
3. R is a PID $\iff$ it is a UFD $\iff$ $C(R) = \{1\}$
4. R is the full ring of integers of a number field $K \implies |C(R)| < \infty$, and this number is the *class number* of K.
5. $C(R)$ can be any abelian group. This is Clayborn's Theorem.
6. For any non-zero prime $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong R/\mathfrak{p}$ as an R-module.
7. "To contain is to divide", i.e. if $A, B \triangleleft R$, then $A \subseteq B \iff A = BC$ for some $C \triangleleft R$.
8. (Generation of ideals) Every non-zero ideal $B \triangleleft R$ is generated by two elements. Moreover, one of the generators can be taken to be any non-zero element of B.
9. (Factor rings) If $A \triangleleft R$ is non-zero, then R/A is a PIR.
10. (Steinitz Isomorphisms Theorem) If $A, B \triangleleft R$ are non-zero ideals, then $A \oplus B \cong {}_R R \oplus AB$ as R-modules.
11. If ${}_R M$ is a finitely generated torsion-free R-module of rank n,[1] then it is of the form $M \cong R^{n-1} \oplus A$, where A is a non-zero ideal, determined up to isomorphism.

[1] The rank is defined as $rk(M) = \dim_{Q(R)} M \otimes_R Q(R)$.

12. If ${}_RM$ is a finitely generated torsion R-module, then M is uniquely of the form $M \cong R/A_1 \oplus \cdots \oplus R/A_n$ with $A_1 \subsetneq A_2 \subsetneq \cdots \subsetneq A_n \subsetneq R$.

Bonus. Any finitely generated ${}_RM$ can be written as $M \cong M_t \oplus M/M_t$, where M_t is the torsion submodule.

Theorem 39.1 (Very Strong Krull-Akizuki Theorem)**.** *Let R be a noetherian domain of Krull dimension 1, with $K = Q(R)$. Let L/K be a finite field extension, and let S be a ring $R \subseteq S \subseteq L$. Then S is noetherian of dimension ≤ 1.*

Corollary 39.2. *If the R is also normal (so it is Dedekind), then the integral closure of R in L is a Dedekind domain.*

We knew this result in the special case when L/K is a finite separable extension.

Prüfer Domains in some sense generalize Dedekind to non-noetherian and higher-dimensional cases.

Definition 39.3. A domain R is *Prüfer* if every non-zero finitely generated ideal is invertible.

Clearly Prüfer and noetherian is Dedekind.

Example 39.4. {Valuation rings} $\subseteq$ {Bézout domains} $\subseteq$ {Prüfer}. •

There are about 20 different characterization of Prüfer domains. Here are a few.

Theorem 39.5. *Let R be a domain. The following are equivalent.*

1. *R is Prüfer.*
2. *For any $\mathfrak{m} \in \operatorname{Max} R$, $R_{\mathfrak{m}}$ is a valuation ring.*
3. *$A \cap (B + C) = (A \cap B) + (A \cap C)$ for all ideals $A, B, C \lhd R$.*
4. *All ideals in R are flat modules.*

Krull domains & Divisors.

Mori's heartbreak story. Let R be a ring with quotient field K. We'd like to form R^*, the integral closure of R. Mori discovered that if R is noetherian, R^* need not be noetherian.

But the implication R noetherian implies R^* noetherian holds in the following cases:

1. $\dim R = 1$, by the Very Strong Krull-Akizuki Theorem, with $L = K$.
2. (Mori, Nagata) $\dim R = 2$.
3. R is an affine algebra.

Grothendieck defined *Japanese rings*, which have to do with this stuff.

Definition 39.6. $R \subseteq K$ as usual is a *Krull domain* if there exists a family $\{R_i\}_{i \in I} \subseteq DVal(K)$ (DVRs of K) such that

1. $R = \bigcap R_i$
2. for all non-zero $a \in R$, $a \in U(R_i)$ for almost all i.

From the viewpoint of valuation theory, let $v_i : R_i \twoheadrightarrow \mathbb{Z} \cup \infty$, then $R = \{x \in K | v_i(x) \geq 0 \text{ for all } i\}$ and for all non-zero $x \in R$, $v_i(x) = 0$ for almost all i.

The set $\{R_i\}$ is called the *defining family* of R.

Lecture 40

Two corrections to the notes:
p. 129, line 8: change "Every" to "Up to associates, every"
p. 131, line 20: Change "the polynomial ring" to "a polynomial ring".

Note that a Krull domain is always completely normal (because DVRs are always completely normal).

Example 40.1.

1. Take R a finite intersection of DVRs of K (then the second condition is automatically satisfied.
2. Noetherian normal domains are Krull. We can take $\{R_i\} = \{R_{\mathfrak{p}} | \mathfrak{p} \in \operatorname{Spec}_1 R\}$. Recall that an element is in a finite number of height 1 primes.
3. UFDs are Krull. The defining family is the set of $R_{(\pi)}$, where π is a prime element. •

Theorem 40.2. $\{$*Krull domains of dimension* $\leq 1\} = \{$*Dedekind domains*$\}$.

$\supseteq$ is clear. For the other direction, the only hard part is to show that R is noetherian. We won't do it here.

Krull domains behave very well with respect to "closure properties":

1. R Krull $\implies$ any localization of R is Krull.
2. R Krull $\implies R[\{x_i\}_{i \in I}]$ is Krull.
3. R Krull $\implies R[[x]]$ is Krull.
4. Let R be Krull with $Q(R) = K$, and let L be a finite extension of K, with S the integral closure of R in L. If R is Krull, then so is S.
5. (Mori-Nagata Theorem) If R is a noetherian domain then the integral closure R^* is Krull.

Theorem 40.3. *If R is Krull, then for every $\mathfrak{p} \in \operatorname{Spec}_1 R$, $R_{\mathfrak{p}}$ is a DVR. Moreover, $\{R_{\mathfrak{p}} | \mathfrak{p} \in \operatorname{Spec}_1 R\}$ is a defining family for R.*

Definition 40.4. If R is a Krull domain, the *divisor class group* is $Cl(R) = \frac{D(R)}{div(K^\times)}$. $D(R)$ is the group of *divisors*, the free abelian group on the set of height 1 primes. For each height 1 prime $\mathfrak{p}$, we have a valuation $v_{\mathfrak{p}}$. We define the set of *principal divisors* to be $div(K^\times) = \{div(f) = \sum v_{\mathfrak{p}}(f)\mathfrak{p} | f \in K^\times\}$.

Theorem 40.5. *If R is a Krull domain, then $Cl(R)$ is trivial if and only if R is a UFD.*

$\Leftarrow$ is clear because each height 1 prime is principal. The other way is not hard either.

Finally, the ideal class group $C(R)$ injects into $Cl(R)$ (with equality if R is regular, whatever that means).

Chapter IV: Dimension Theory

Definition 40.6. Let k be a field, and let B be a k-algebra. We define $tr.d._k B = \sup\{tr.d._k(B/\mathfrak{p}) | \mathfrak{p} \in \mathrm{Min}(B)\}$.

Theorem 40.7 (Noether normalization)**.** *Let k be a field, and B an affine k-algebra. Then there exist algebraically independent (over k) $x_1, \ldots, x_n \in B$ such that B is integral over $A = k[x_1, \ldots, x_n]$. In particular, since B is finitely generated over k, it is module-finite over A.*

Example 40.8. Let $B = k[t^2, t^3] \subseteq k[t]$. Here $A = k[t^2]$, and it is clear that t^3 is integral over A. •

Example 40.9. Let $B = k[t, t^{-1}]$. Take $A = k[t + t^{-1}]$. Then note that t and t^{-1} satisfy $(x - t)(x - t^{-1}) = x^2 - (t + t^{-1})x + 1 \in A[x]$. •

Proof. Write $B = k[y_1, \ldots, y_m]$ and induct on m. The case $m = 0$ is trivial. If $y_1, \ldots, y_m$ are algebraically independent, we take $A = B$ and we're done. Thus, we may assume there is some dependence $f(y_1, \ldots, y_m) = 0$. Take r larger than any exponent in f. Define $z_i := y_i - y_1^{r^{i-1}}$ for $i \geq 2$. Then we get that $0 = f(y_1, z_2 + y_1^r, z_3 + y_1^{r^2}, \ldots, z_m + y_1^{r^m})$ has leading term by_1^N for some huge N and $b \neq 0$. This equation tells us that y_1 is integral over $B' := k[z_2, \ldots, z_m]$. It is clear that all the other y_i are also integral over B', so B is integral over B'. By induction, we can find a polynomial ring A so that B' is integral over A. □

It is clear that $tr.d._k B \leq m$.

Lecture 41

In the notes, p. 129, line 7 (statement of (6.19)), the "if" part needs a correction.

We replace B by S and A by R.

Basic trick:

$(*)$ If B/A is an integral extension of k-domains, then $tr.d._k B = tr.d._k A$. This is because the field extension $Q(A) \subseteq Q(B)$ is algebraic.

Theorem 41.1. *Keep all notation from before.*

1. $n = tr.d._k S$
2. *for* $I \lhd S$, $tr.d._k S/I \leq tr.d._k S$
3. n *is the largest integer* d *such that* S *has* d *algebraically independent elements*
4. *for all* k*-subalgebras* $T \subseteq S$, $tr.d._k T \leq tr.d._k S$.

Proof. (1) Let $\mathfrak{P} \in \operatorname{Spec} S$, $\mathfrak{p} = \mathfrak{P} \cap R$. Then $R/\mathfrak{p} \subseteq S\mathfrak{P}$ is integral. By $(*)$, $tr.d._k S/\mathfrak{P} = tr.d._k R/\mathfrak{p} \leq n$. By Going Up, there is a $\mathfrak{P}_0 \in \operatorname{Spec} S$ (which we may assume is minimal) so that $\mathfrak{P}_0 \cap R = (0)$. Now we have $R \subseteq S/\mathfrak{P}_0$. By $(*)$, $n = tr.d._k R = tr.d._k S/\mathfrak{P}_0 \leq tr.d._k S$.

(2) Consider $I \lhd S$. We may assume $I \in \operatorname{Spec} S$. By what we did in part (1), we get $tr.d._k(S/I) \leq n = tr.d._k S$.

(3) Let d be as defined. We already know $n \leq d$. Say that $R_0 = k[t_1, \ldots, t_d]$ is a polynomial algebra in S. Say $\operatorname{Min} S = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_r\}$, and let $\mathfrak{p}_i = \mathfrak{P}_i \cap R_0$. We have that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq \mathfrak{P}_1 \cdots \mathfrak{P}_r \cap R_0 \subseteq \operatorname{Nil}(S) \cap R_0 = \operatorname{Nil} R_0 = 0.$$

It follows that some $\mathfrak{p}_i$ is zero, say $\mathfrak{p}_1 = 0$. By $(*)$ applied to $R_0 = R_0/\mathfrak{p}_1 \subseteq S/\mathfrak{P}_1$ to get $d = tr.d._k R_0 = tr.d._k S/\mathfrak{P}_1 \leq tr.d._k S = n$.

(4) follows from (3) immediately. □

In $k[x_1, \ldots, x_n]$, there is an obvious chain of primes

$$(0) \subsetneq (x_1) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n)$$

which implies that $\dim k[x_1, \ldots, x_n] \geq n$.

Theorem 41.2. *For every affine* k*-algebra* S, $\dim S = tr.d._k S$.

Remark 41.3. This theorem includes Zariski's Lemma, which says that an affine algebra over k which is a field must be a finite algebraic extension. To see this from the theorem, let S be a field, then $\dim S = 0$. It follows that $tr.d._k S = 0$, so S is algebraic over k. It is finite because S is finitely generated.

This provides an alternative approach to Hilbert's Nullstellensatz.

Before we prove the theorem, we need a lemma.

Lemma 41.4. *Let S be a k-affine domain with $tr.d._k S = n$, and let $\mathfrak{p} \in \operatorname{Spec}_1 S$. Then $tr.d._k(S/\mathfrak{p}) = n - 1$.*

Proof. Case 1: assume $S = k[x_1, \ldots, x_n]$ is a polynomial algebra. In this case, height 1 primes are principal, so $\mathfrak{p} = (f)$ for some f. Say f has positive degree with respect to x_1, so $f = g_r(x_2, \ldots, x_n)x_1^r + \cdots$. We have that $k[x_2, \ldots, x_n] \cap (f) = (0)$ (just look at degree with respect to x_1). It follows that $k[x_2, \ldots, x_n] \hookrightarrow S/(f)$, so $\bar{x}_2, \ldots, \bar{x}_n$ are algebraically independent in $S/\mathfrak{p}$. By $\bar{x}_1$ is algebraic over $Q(k[\bar{x}_2, \ldots, \bar{x}_n])$ as witnessed by f. This, $tr.d._k S/\mathfrak{p} = n - 1$.

Case 2: reduction to case 1. Let $R = k[x_1, \ldots, x_n]$ be a Noether normalization for S, and let $\mathfrak{p}_0 = \mathfrak{p} \cap R$. Observe that Going Down applies (because S is a domain and R is normal). It follows that $ht_R(\mathfrak{p}_0) = ht_S(\mathfrak{p}) = 1$. By case 1, we get that $tr.d.(R/\mathfrak{p}_0) = n - 1$. By $(*)$, we get that $tr.d.R/\mathfrak{p}_0 = tr.d.(S/\mathfrak{p})$. □

Proof of Theorem 41.2. Let $n = tr.d._k S$. We induct on n. If $n = 0$, then S is algebraic over k. Then for any minimal prime $\mathfrak{P} \subseteq S$, $S/\mathfrak{P}$ is a field. Thus, minimal primes are maximal, so S has dimension 0.

Now assume the equation is true up to $n - 1$. After replacing S by a Noether normalization (without affecting $\dim S$ or $tr.d._k S$), we may assume $S = k[x_1, \ldots, x_n]$ is a polynomial algebra. Consider any prime chain of length r in this polynomial algebra. Let $\mathfrak{p}$ be the smallest non-zero prime in the chain, and let $f \in \mathfrak{p}$ be a non-zero irreducible, then (f) is prime and contained in $\mathfrak{p}$. By case 1 of the Lemma, $tr.d._k S/(f) = n - 1$. By the inductive hypothesis, $\dim S/(f) = n - 1$. But $S/(f)$ has a prime chain of length $r - 1$. Thus, $r - 1 \leq n - 1$, so $r \leq n$. □

Lecture 42

What we would've done next:

1. Generalized princepal ideal theorem: R noetherian, $\mathfrak{p}$ minimal prime over $(a_1, \ldots, a_n$, then $ht(\mathfrak{p}) \leq n$.
   Corollary 1: Spec R satisfies DCC (the length of a chain from $\mathfrak{p}$ is bounded by $ht(\mathfrak{p}) < \infty$ (R noetherian, so $\mathfrak{p}$ is finitely generated)).
   Corollary 2: R local $\Rightarrow \dim R < \infty$
   (Nagata): There exist "bad noetherian rings" which are infinite dimensional noetherian domains.

2. R noetherian of dimension $n \Longrightarrow \dim R[x] = n + 1$.
   In general, $n + 1 \leq \dim R[x] \leq 2n + 1$ ("Seidenberg bounds"), and these bounds are tight.

Definition 42.1. A ring R is *catenary* if given any two primes $\mathfrak{p} \subsetneq \mathfrak{p}'$, any two maximal prime chains from $\mathfrak{p}$ to $\mathfrak{p}'$ have the same length.

Nagata showed that there are noetherian domains which are not catenary.

Definition 42.2. If $\mathfrak{p} \in \operatorname{Spec} R$, then $\dim \mathfrak{p} := \dim R/\mathfrak{p}$.

Theorem 42.3. *Any k-affine algebra S is catenary (even if S is not a domain). In fact, any saturated prime chain from $\mathfrak{p}$ to $\mathfrak{p}'$ has length $\dim \mathfrak{p} - \dim \mathfrak{p}'$. If S is a domain, then all maximal ideals have the same height.*

Proof. Consider any chain $\mathfrak{p} \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}'$. Then we get the chain

$$S/\mathfrak{p} \twoheadrightarrow S/\mathfrak{p}_1 \twoheadrightarrow \cdots \twoheadrightarrow S/\mathfrak{p}_r = S/\mathfrak{p}'$$

Here $\mathfrak{p}_i/\mathfrak{p}_{i-1}$ is height 1 in $S/\mathfrak{p}_{i-1}$, so each arrow decreases the transcendence degree by exactly 1. Therefore, $tr.d._k S/\mathfrak{p}' = tr.d._k S/\mathfrak{p} - r$.

$$r = tr.d._k S/\mathfrak{p} - tr.d._k S/\mathfrak{p}' = \dim S/\mathfrak{p} - \dim S/\mathfrak{p}' = \dim \mathfrak{p} - \dim \mathfrak{p}'.$$

To get the last statement, take $\mathfrak{p} = 0$ and $\mathfrak{p}' = \mathfrak{m}$. Then we get that $ht(\mathfrak{m}) = \dim S$. □

Note that the last statement fails in general.

Example 42.4. Take $S = k \times k[x_1, \ldots, x_n]$. Then $ht(0 \times k[x_1, \ldots, x_n]) = 0$, but $ht\big(k \times (x_1, \ldots, x_n)\big) = n$. •

But that example is not connected.

Example 42.5. $S = k[x, y, z]/(xy, xz)$. •

But this example is not a domain. In general, for any prime $\mathfrak{p}$ in any ring S, we have

$$ht(\mathfrak{p}) + \dim \mathfrak{p} \leq \dim S.$$

Theorem 42.6. *Let S be an affine algebra, with $\operatorname{Min} S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Then the following are equivalent.*

1. *$\dim \mathfrak{p}_i$ are all equal.*
2. *$ht(\mathfrak{p}) + \dim \mathfrak{p} = \dim S$ for all primes $\mathfrak{p} \in \operatorname{Spec} S$. In particular, if S is a domain, we get this condition.*

Proof. $(1 \Rightarrow 2)$ $ht(\mathfrak{p})$ is the length of some saturated prime chain from $\mathfrak{p}$ to some minimal prime $\mathfrak{p}_i$. This length is $\dim \mathfrak{p}_i - \dim \mathfrak{p} = \dim S - \dim \mathfrak{p}$ (by condition 1). Thus, we get (2).

$(2 \Rightarrow 1)$ Apply (2) to the minimal prime $\mathfrak{p}_i$ to get $\dim \mathfrak{p}_i = \dim S$ for all i. □

We finish with a (non-affine) noetherian domain S with maximal ideals of different heights. We need the following fact.

Fact: If R is a ring with $a \in R$, then there is a canonical R-algebra isomorphism $R[x]/(ax-1) \cong R[a^{-1}]$, $x \leftrightarrow a^{-1}$.

Example 42.7. Let $\big(R, (\pi)\big)$ be a DVR with quotient field K. Let $S = R[x]$, and assume for now that we know that $\dim S = 2$. Look at $\mathfrak{m}_2 = (\pi, x)$ and $\mathfrak{m}_1 = (\pi x - 1)$. Note that $\mathfrak{m}_1$ is maximal because $S/\mathfrak{m}_1 = K$. It is easy to show that $ht(\mathfrak{m}_1) = 1$. However, $\mathfrak{m}_2 \supsetneq (x) \supsetneq (0)$, so $ht(\mathfrak{m}_2) = 2$. •

Now let's come back to result I.1.1. The result we've just proven says that $ax - 1 \in U(R[x])$ if and only if $a \in \operatorname{Nil} R$.