## LECTURE 1

First, we assume that everyone knows what a ring is. If you don't, you should review the definition, but roughly speaking it is something like the integers–it has two binary operations (addition and multiplication) and there are various axioms you can look up. We will mostly be looking at rings that are commutative; that is, rings in which $xy = yx$ for all $x, y \in R$. **IMPORTANT: We always assume that our rings have a multiplicative identity $1 = 1_R$ and $1x = x1 = x$.** Other things you should already know:

(i) What an ideal is. contains zero, closed under + and under multiplication by $R$
(ii) what the quotient ring $R/I$ is.
(iii) What a unit, zero divisor, idempotent, nilpotent element, integral domain, field, PID, UFD are.
(iv) What a prime ideal is. For commutative rings $ab \in P$ if and only if $a \in P$ or $b \in P$. $R/P$ is an integral domain.
(v) What a maximal ideal is. $M$ maximal if and only if $R/M$ is a field. So $M$ maximal is also prime.
(vi) Zorn's lemma (and it's basic corollaries: maximal ideals exist; if $I$ is a proper ideal, there is a maximal ideal above it; every v.s. has a basis)
(vii) Chinese remainder theorem for rings.

That's probably it. One important thing I won't assume you know, but you might already know anyway, is what a module is.

Modules If $R$ is a ring, an *$R$-module* is an abelian group $M$ (with operation + and identity $0 = 0_M$) endowed with an action of $R$. What does this mean? We have a map $R \times M \to M$ written $(r, m) \mapsto r \cdot m$ satisfying the following relations for $r, s \in R$ and $m, n \in M$:

(i) $r(sm) = (rs)m$ (associativity)
(ii) $r(m + n) = rm + rn$ (bilinearity 1)
(iii) $(r + s)m = rm + sm$ (bilinearity 2)
(iv) $1_R m = m$.

Notice that $r0_M = 0_M$. Why? $r0_M = r(0_M + 0_M) = r0_M + r0_M$. Also $0_R \cdot m = 0_M$. Why? same reason. If $M$ is an $R$-module, we call the *annihilator* of $M$, $\mathrm{Ann}(M)$, the set of $r \in R$ such that $rm = 0$ for every $m \in M$. Notice that $\mathrm{Ann}(M)$ is an ideal. Why? 0 is in there. If $r, s$ in there so is $r + s$ and $ar$ is in there too. A module $M$ is *faithful* if $\mathrm{Ann}(M) = (0)$. What does this mean? Well, if $I = \mathrm{Ann}(M)$ then, morally, $M$ is an $R/I$ module. So this is saying that $M$ is really an $R$-module and not just a module that comes from lifting the structure of a module for $R/I$.

Examples.

(i) Let $F$ be a field and let $V$ be an $F$-module. Then $V$ is a vector space and any v.s. is an $F$-module. Annihilator of $V$ is (0) unless $V = (0)$.
(ii) Let $R = Z$ and let $M$ be an abelian group. Then $M$ is an $R$-module. $n \in Z$ and $x \in M$ then $nx = x + x + \cdots + x$ if $n > 0$ and $-x + \cdots - x$ $|n|$ times if $n < 0$. If $M = Z_3 \oplus Z_{10}$ what is the annihilator of $M$?
(iii) $R = \mathbb{R}[x]$ and $M = \mathbb{C}$. Well, we define $p(x) \cdot \lambda = p(i) \cdot \lambda$. What is the annihilator? We say that the module $M$ is finitely generated if there exist $m_1, \ldots, m_n$ in $M$ such that $M = Rm_1 + \cdots + Rm_m$. This is a bit like being finite-dimensional for a v.s. E.g. $R = Z$, $M = Q$ is not f.g. Proof. If $Q = Z\alpha_1 + \cdots + Z\alpha_d$ then pick a common denominator. $R = Z$, $M = Z_2 x Z_3$ is f.g. As before if $N \subseteq M$ and $N$ is a subgroup of $M$ and $rN \subseteq N$ then $N$ is called a submodule of $M$. One example is if $I$ is an ideal of $R$ Then $IM = \{\sum xm \colon x \in I, m \in M\}$ is a submodule of $M$. If $N \subseteq M$ is a submodule, we can form a quotient module: $M/N$. As a group this is just the quotient group $M/N$ (note that $N$ is normal since $M$ is abelian) and $r \cdot ([m]) = rm$ is well-defined. $[m] = m + N$. Show that the annihilator of $M/IM$ contains $I$ and hence we can regard if as an $R/I$-module.

If $R$ is a ring and $M$ and $N$ are two $R$-modules, we say that a map $f : M \to N$ is an $R$-module homomorphism if $f$ is a homomorphism of abelian groups $f(m_1 + m_2) = f(m_1) + f(m_2)$ and $f(rm) = rf(m)$. So it is like being an $R$-linear map. Example: if $f : V \to W$ is a linear transformation of $F$-v.s. then $f$ is an $F$-module homomorphism. Any homomorphism of abelian groups is a $Z$-module homomorphism. We can talk about homomorphisms being injective, onto, etc. And when it is bijective it is an isomorphism of $R$-modules and the inverse is again an $R$-module homomorphism (**Exercise**!) Notice that image and kernel are submodules and one to one if and only if kernel is trivial. Notice that we have a surjective homomorphism $f : M \to M/N$ given by $f(m) = m + N$. In general, if $f : M \to M'$ is onto then $M' \cong M/ker(f)$.

If $M$ and $N$ are two $R$-modules, we let $Hom_R(M, N)$ denote the set of $R$-module homomorphisms from $M$ to $N$. Notice that $Hom(M, N)$ is itself an $R$-module: if $f, g \in Hom_R(M, N)$ then so are $f + g$ and $-f$ and the zero map is the identity. Finally, if $r \in R$ then $r \cdot f(m) = f(rm)$ is a homomorphism. If $\{M_\alpha\}$, $\alpha \in X$ is a collection of $R$-modules, we can form the *direct sum*

$$M_1 = \bigoplus_\alpha M_\alpha.$$

This is all sequences $(m_\alpha)_\alpha$ with $m_\alpha = 0$ for all but finitely many $\alpha$. The sum is coordinate-wise and multiplication by $R$ is coordinate-wise. The *direct product* is just

$$M_2 = \prod_\alpha M_\alpha.$$

This is all sequences $(m_\alpha)_\alpha$. The sum is coordinate-wise and multiplication by $R$ is coordinate-wise. Notice that $M_1$ and $M_2$ are isomorphic if $|X| < \infty$. (**Exercise**. $R = Z$ show that $Z \oplus Z \cdots$ is not isomorphic to $Z \times Z \times \cdots$.) An $R$-module $M$ is *free* if there is a set $X$ such that $M \cong R^X$. If $X$ has size $n < \infty$, we'll write $R^n$ for $R^X$ and $R^\omega$ if $|X|$ is countably infinite. This says that $M$ has a basis.

E.g. if $R = F$ a field all $R$-modules are free. Proof an $F$-module is a v.s. Since every v.s. has a basis (**Exercise. Zorn!**) we see that $V = F^X$. E.g. if $R = Z$ and $M = Z/2Z$ then $M$ is not free. Let $R = Z$ and let $M = \prod_{i=1}^\infty Z$. Show that $M$ is not free **Tricky exercise!** If $M$ is a f.g. free module, then we call the *rank* of $R$ the cardinality of $|X|$, where $M \cong R^X$. Since $X$ is finite, this Question: is the rank well-defined? That is: why can't we have, say, $R^2 \cong R^3$. We know this is the case for fields. Every v.s. has a basis and all bases have the same cardinality **Exercise.**. In general, not well-defined if $R$ is not commutative. E.g., $x, y, x^*, y^*$ relations $x^*x = y^*y = 1$, $xx^* + yy^* = 1$. Then $R \cong R \oplus R$. For now we will just assume this, but we'll see how to derive this from the v.s. case after we do tensor products.

## Lecture 2

Exactness. Let $M, M', M''$ be $R$-modules and let $f : M" \to M$ and $g : M \to M'$ be homomorphisms. We say that

$$M'' \to M \to M'$$

is exact if the image of $f$ is equal to the kernel of $g$. In general, a sequence

$$M_1 \to M_2 \to \cdots \to M_n$$

is exact if each pair of consecutive maps is exact. A sequence of the form

$$0 \to M" \to M \to M' \to 0$$

is called a short exact sequence (s.e.s.) if it is exact. That means $f$ is injective; $im(f) = ker(g)$ and $g$ is onto. Notice that we have $M/M'' \cong M'$ as $R$-modules by the isomorphism theorem. We say that a s.e.s.

$$0 \to M" \to M \to M' \to 0$$

is *split* if there is a homomorphism $\tau : M' \to M$ (sometimes called a section) such that $g \circ \tau = \mathrm{id}_{M'}$.

Prop: the following are equivalent:

(i) $M \cong M' \oplus M''$.
(ii) there are maps $f, g$ such that $0 \to M'' \to M \to M' \to 0$ is a s.e.s. that splits.
(iii) there is a map $\sigma : M \to M''$ such that $\sigma \circ f = \mathrm{id}_{M"}$.

*Proof.* (2) => (1). Suppose we have (2). Let $h : M'' \oplus M' \to M$ be given by $h(m'', m') = f(m'') + \tau(m')$. Then $h$ is a homomorphism. $h$ is one to one. why? If $h(m'', m') = 0$ then $x = f(m'') = \tau(m')$. This means that $x$ is in image of $f$ which is kernel of $g$. So $g(x) = 0$. Thus $m' = g \circ \tau(m') = 0$. But now $f(m'') = 0$ so $m'' = 0$ since $f$ is one-to-one. Onto. Why? Given $m \in M$, we have $m - \tau(g(m))$ is in the kernel of $g$. So it is in image of $f$. Thus $m = f(m'') + \tau(g(m))$ So $m = h(m'', g(m))$. (1) $\implies$ (2) let $f(m'') = (m'', 0)$ and $g(m'', m') = m'$. Then (3) $\iff$ (1) is similar. Now define $k : M \to M' \oplus M''$ by $k(m) = (\sigma(m), g(m))$. □

## Lecture 3

If $R$ is a PID and $M$ is a f.g. $R$-module then we have a nice structure theorem for f.g. modules. Thm: Structure theorem for f.g. modules over a PID.

*Proof.* We prove this by induction on the number of generators of $M$. If $M = Rm$ (i.e., $M$ is a cyclic $R$-module. Then $M \cong R/\mathrm{Ann}(M)$. We take a homomorphism from $R \to M$ by $r \mapsto rm$. the kernel is $I = \mathrm{Ann}(M)$. So $M = R/I$. If $I = (0)$, $M$ Is free. Since a PID is a UFD, we have $I = (a) = (p_1^{j_1} \cdots p_m^{j_m})$. CRT. Assume true if we have $< d$ generators. Now consider $M$ that is $d$-generated. If $M = R^d$ great. Otherwise we get relations. Let $S$ be the set of all sets of $d$-generators for $M$. For $(m_1, \ldots, m_d) \in S$. Pick $r_1 m_1 + \cdots + r_d m_d = 0$, not all zero. Pick a set such that $(r_1)$ is maximal. (Let's talk about this step). Claim: $M \cong R/(r_1) \oplus N$ with $N$ generated by $d - 1$ elements. Claim: $r_1$ divides all the $r_i$. If not, $(r_1, r_i) = (s)$ strictly contains $(r_1)$ for some $i$. So $r_1 = as$ and $r_i = bs$. Notice that $gcd(a, b) = 1$. So $ca + db = 1$. Notice that the generating set $asm_1 + ... + bsm_i + \cdots = 0$. Now let $m'_j = m_j$ for $j \neq 1, i$ and $m'_1 = am_1 + bm_i$ and $m'_i = dm_1 - cm_i$. Then $m_1 = cm'_1 + bm'_i$ and $m_i = dm'_1 - am'_i$ so they generate and $asm_1 + r_2 m_2 + \cdots + bsm_i + \cdots$ can be written as $as(cm'_1 + bm'_i) + bs(dm'_1 - am'_i) + ... = sm'_1 + ...+$ so this contradicts minimality. So if we let $m''_1 = m'_1 + ...$ then we have $r_1 m''_1 = 0$ and this must be a direct summand. Why? If $um''_1 = c_2 m'_2 + \cdots + c_d m'_d$ then $(u, r_1)$ contains $r_1$ contradicting minimality. So $M =< m_1 > \oplus N$, $N$ is $d - 1$ generated and $< m_1 >$ is cyclic. □

Tensor products.

Let $R$ be a ring and let $M$ and $N$ be $R$-modules. The *tensor product* of $M$ and $N$ over $R$, $(M \otimes_R N)$, is an $R$-module. Defined as follows. For each $m \in M, n \in N$ we make a symbol $(m, n)$. We let $F$ denote the free $R$-module on all symbols of the form $(m, n)$. That is $F = \bigoplus_{(m,n)\in M\times N} R(m, n)$. This is an enormous module. We let $G$ denote the submodule of $F$ generated by all relations of the form

$$r(m, n) = (rm, n) = (m, rn)$$

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

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

In other words, we are adding all bilinear relations. We define $M \otimes_R N = F/G$ and we let $m \otimes n$ denote the image of $(m, n)$ in $F/G$. WARNING: Not everything in $M \otimes_R N$ is of the form $m \otimes n$. Generally, we need to take sums of tensors (this is the whole idea of entanglement in physics). Notice that the above relations say that the map $\phi : M \times N \to M \otimes N$ given by $(m, n) \mapsto m \otimes n$ is bilinear. In fact, the tensor product is defined by the following UNIVERSAL PROPERTY. The following is very helpful in proving facts about tensor products. If $P$ is an $R$-module and $h : M \times N \to P$ is a bilinear map. Then there is a unique $R$-module homomorphism $\tilde{h} : M \otimes N \to P$ such that $\tilde{h} \circ \phi = h$. Notice that the tensor product satisfies this property. Universal property says that tensor product is the unique up to isom module with this universal property.
**Exercise**

Probably a good idea to compute a few, to see what is going on. Let's first do a few without using universal property.

$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$. Proof. $F$ is $Z^6$. $(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)$. Notice that $(0, i) = 0(1, i) = 0 \bmod G$. Similarly, $(i, 0) = 0$. Now $(1, 1) = (1, 4) = 4(1, 1) = (4, 1) = (0, 1) = 0$. $(1, 2) = 2(1, 1) = (2, 1) = (0, 1) = 0$. So we see that the tensor product is zero.

$\mathbb{Z}_2 \otimes \mathbb{Z}_2 =$??. Let's see $(0, 0), (0, 1), (1, 0), (1, 1)$. and $2(1, 1) = 0$. So the tensor product has size at most 2. So it is either (0) of $Z_2$. Well, it is $Z_2$. Let $f : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to Z_2$ be given by $f(a \otimes b) = ab$. Notice that we can define it on $F$ and that everything in $G$ is sent to zero so it works.

$\mathbb{Z}_2 \otimes \mathbb{Z}_4 =$???. Let's see $(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3)$. Which go away. all with 0. $(1, 2)$ so we are left with 0, $(1, 1)$, $(1, 3) = 3(1, 1) = (1, 1)$ and $2(1, 1) = 0$. So it has size 0 or 2. Well, it is again $Z_2$. Define $m \otimes n = mf(n)$, where $f : Z_4 \to Z_2$ is the natural map. In general, $Z_n \otimes Z_m = Z_d$, $d = gcd(m, n)$. Proof. Well, let's see that it has size at most $d$. We have a map $f : Z_n \otimes Z_m \to Z_d$ by $f(m \otimes n) = g(m)h(n)$. Notice that $d(a \otimes b) = (xm + yn)(a \otimes b) = 0$. So every element of my group has order dividing $d$. Claim every tensor $a \otimes b = ab(1 \otimes 1)$. So it is generated by $1 \otimes 1$. The order is at most $d$ and at least $d$. Notice $a \otimes b$.

Let's redo this with the last one with the universal property. We have a map $Z_m \times Z_n \to Z_d$ by $(m, n) \to g(m)h(n)$. If we have a bilinear map $h : Z_m \times Z_n \to P$ then $h(a, b) = ah(1, b) = abh(1, 1)$. And $dh(1, 1) = (xm + yn)h(1, 1) = xmh(1, 1) + ynh(1, 1) = h(0, 1) + h(1, 0) = 0$. So there is a map $Z_d \to P$ given by $i \to i(1, 1)$. Then this works.

## Lecture 4

Prop. The following hold. $M \otimes N \cong N \otimes M$ (commutativity). $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$ (associativity).

*Proof.* **Exercise.** Commutativity is the universal property since $M \times N \cong N \times M$. For associativity, notice that a bilinear map on $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$ is a trilinear map on $M \times N \times P$. □

If $f : M \to N$ then we have $f : M \otimes C \to N \otimes C$ by $f(m \otimes c) = n \otimes c$. Check the relations in $G$.

Right exactness

Prop: If $M \to N \to P \to 0$ is exact then so is $M \otimes C \to N \otimes C \to P \otimes C \to 0$ (right exactness).

*Proof.* **Exercise** Notice that if $f : M \to N$ and $g : N \to P$ then the map $M \otimes C \to N \otimes C$ given by $f(m \otimes c) = f(m) \otimes c$ is well-defined. Add this. □

What's an example where $0 \to M \to N$ is exact but $0 \to M \otimes C \to N \otimes C$ is not? How about $M = N = Z$, $f$ is multi by 2. And $C = Z_2$.

Easy Prop: $R \otimes_R M = M$.

Proof. Let $\phi : R \times M \to M$ be given by $(r, m) \to rm$. This is bilinear. Notice that if $h : (R, M) \to P$ is bilinear then $h(r, m) = rh(1, m)$. Now define $\tilde{h} : M \to P$ by $\tilde{h}(m) = h(1, m)$. This is an $R$-module homomorphism since $rm \mapsto h(1, rm) = rh(1, m)$. Unique.

## Lecture 5

Prop: (direct sums) $(M \oplus N) \otimes C \cong M \otimes C \oplus N \otimes C$. Same for general direct sums.

*Proof.* Just use the natural maps $i : M \to M \oplus N$ and $\pi : M \oplus N \to M$, and the proof will write itself. □

Prop: Let $R$ be a ring and let $M$ be a free module—then rank is well-defined. Then $M \cong R^X \cong R^Y$ if and only if $|X| = |Y|$.

*Proof.* Let $P$ be a maximal ideal of $R$. Let $F = R/P$. Let $V = F \otimes_R M$. Then $V$ is an $F$-module. Why? $PV = 0$. Notice that $V = F \otimes_R M \cong F \otimes_R^X \cong (F \otimes_R R)^X \cong F^X$ and $V = F^Y$. So $F^X \cong F^Y$, which means that $|X| = |Y|$. □

An $R$-module $C$ is called *flat* if whenever $M \to N$ is 1-to-1, we have $M \otimes C \to N \otimes C$ is 1 to 1. Example. A free module is flat. We just saw $Z_2$ is not flat as a $Z$-module.

Algebras.

If $R$ is a commutative ring then a commutative $R$-algebra $S$ is just a commutative ring $S$ equipped with a ring homomorphism $\alpha : R \to S$. Notice every ring is a $Z$-algebra, $\alpha(n) = n \cdot 1_R$. We usually suppress $\alpha$ and just think of $r$ as being identified with $\alpha(r)$ in $S$ (even if it is not 1-to-1). Examples: $k[x_1, \ldots, x_n]$ is a $k$-algebra. $R[x]$ is an $R$-algebra. Ex. $C$ is a $Q$-algebra. Notice if $S$ is an $R$-algebra then $S$ is also an $R$-module.

Base change/extension of scalars for tensor products. If $S$ is an $R$-algebra and $M$ is an $R$-module, sometimes we'd rather work with an $S$-module. (Think of v.s. over $Q$ v.s. v.s. over $C$.) We can use tensor products to do this. If $S \otimes_R M$ is an $R$-module, but it gets a structure as an $S$-module too. $s(s' \otimes m) := (ss' \otimes m)$. Notice that $(s_1 + s_2)(s' \otimes m) = ...$

In fact, if $A$ and $B$ are two $R$-algebras, we can endow $A \otimes_R B$ with an $R$-algebra structure as follows. We define multiplication on $A \otimes_R B$ via $(a_1 \otimes b_1) \cdots (a_2 \otimes b_2) = (a_1 a_2 \otimes b_1 b_2)$ and extend via linearity. This is well-defined: **exercise!**

Noetherian rings.

Let $R$ be a ring. We say that $R$ is *noetherian* if every ascending chain of ideals $I_1 \subseteq I_2 \cdots$ terminates.

## Lecture 6

Prop: This is equivalent to every non-empty set of ideals having a maximal element and to every ideal being finitely generated as an ideal.

E.g. $R = PID$ is noetherian; $R = C[x_1, x_2, ...]$ is not noetherian. Let $R$ be a ring and let $M$ be an $R$-module. We say that $M$ is noetherian if every ascending chain of submodules terminates. Equivalently all submodules are f.g. and equivalent to every non-empty set of submodules having a maximal element.

E.g. $R = Z$, $M = Q$ is not noetherian. $R$ noetherian then $R$ is noetherian as an $R$-module.

Prop: Let $M$ be an $R$-module and $N$ be a submodule. Then $M$ is noetherian if and only if $M/N$ and $N$ are noetherian.

*Proof.* Any chain in $M/N$ lifts to a chain in $M$ containing $N$ so $M$ noetherian ==> $M/N$ noetherian. Any chain in $N$ is also a chain in $M$ so $M$ noetherian implies $N$ noetherian. Converse. If $M/N$ and $N$ are noetherian, let $J_1 < J_2 < \cdots$ be a chain. Then the chain $J_i \cap N$ terminates so there is some $m$ such that $J_m \cap N = J_{m+1} \cap N \cdots$. Now we have a map $\phi : M \to M/N$. Then $\phi(J_i) = (J_i + N)/N$. The chain $\phi(J_i)$ terminates so there is some $m'$ at which it stabilizes. Now let $n \geq \max(m, m')$. Claim $J_n = J_{n+1} = \cdots$. Let $x \in J_i$ for $i > n$. We have $J_n + N = J_i + N$ so $x = y + n$ for some $y \in J_n$ and some $n \in N$. Thus $y - x = n \in J_i \cap N$ and so $y - x \in J_n \cap N$, which means $y - x = u$ for some $u \in J_n \cap N$ so $y = x + u \in J_n$. Thus $J_i = J_n$ for all $i > n$. □

Exercise: (corollary) if $M$ and $N$ are noetherian modules then $M \oplus N$ is noetherian. Does this hold for infinite direct sums? Prop: Let $R$ be a noetherian ring and let $M$ be a f.g. $R$-module. Then $M$ is noetherian.

*Proof.* . $M$ is f.g. so there is some $F \cong R^d$ such that $F \to M$ is surjective. $F$ is noetherian by direct sum result. The kernel, $K$, is noetherian by submodule result. So $M \cong F/K$ is noetherian. □

Maximality principle: If one takes an ideal in a noetherian ring that is maximal with respect to having a "nice" property, one can often show it is a prime ideal. This is a nice trick, that we will use a lot in this course.

Let's give our first example of this principle in action—probably the first application of this idea, from E. Noether.

Prop: Let $R$ be a ring and let $I$ be a proper ideal of $R$. Then there exist prime ideals $P_1, \ldots, P_d \supseteq I$ such that $P_1 \cdot P_2 \cdots P_d \subseteq I$.

*Proof.* Suppose this is not the case. Let $\mathcal{S}$ be the set of all ideals $I$ for which this does not hold. Then $\mathcal{S}$ is non-empty, so we pick an ideal that is maximal in $\mathcal{S}$. Claim: $I$ is prime. Suppose not. Then there exist $a, b \notin I$ such that $ab \in I$. Let $J_1 = Ra + I$ and $J_2 = Rb + I$. Then $J_1$ and $J_2$ are bigger than $I$ so they are not in $\mathcal{S}$ by maximality. Thus there exist $P_1, \ldots, P_d \supseteq J_1$ such that

$P_1 \cdot P_2 \cdots P_d \subseteq J_1$ and $Q_1, \ldots, Q_e \supseteq J_2$ such that $Q_1 \cdots Q_e \subseteq J_2$. But now $P_1 \cdots P_d Q_1 \cdots Q_e \subseteq J_1 J_2 = (Ra+P)(Rb+P) \subseteq P$. Thus $I$ is prime. Now just take $P_1 = I$. Done! □

Let $R$ be a ring and let $I$ be an ideal in $R$. We call the *radical* of $I$, $\sqrt{I}$, the intersection of the prime ideals above $I$. If $R$ is noetherian, this intersection can be taken to be finite by Noether's theorem. Why? Exercise!

Let's see another application.

Prop: Let $R$ be a noetherian ring and let $I$ be the intersection of all prime ideals in $R$ (the radical ideal of (0). Then $I$ is a nil ideal.

*Proof.* Suppose that $I$ is not nil. Then pick $x$ in $I$ that is not nilpotent. Let $X = \{1, x, x^2, \ldots\}$. Let $\mathcal{S}$ be the set of ideals $I$ such that $I \cap X = \emptyset$. Since $(0) \in \mathcal{S}$, $\mathcal{S}$ is non-empty. Pick $J$ in $\mathcal{S}$ maximal. Claim: $J$ is prime. Proof. Suppose not. Then there are $a, b \in R \setminus J$ such that $ab \in J$. Let $J_1 = Ra + J$, $J_2 = Rb + J$. Then by maximality $x^m \in J_1$ and $x^n \in J_2$ for some $m, n$. Then $x^{m+n} \in J_1 J_2 \subseteq J$, contradiction. Thus $J$ is prime. But $I \subseteq J$ and $x \in I$ so $x \in J$, contradiction. □

REMARK: We can get this proof to work for general commutative rings using Zorn's lemma to produce a maximal element of $\mathcal{S}$.

Cor: If $x \in \sqrt{I}$ then there is some $n$ such that $x^n \in I$. Hence the name radical. Let's do one more application.

## Lecture 7

Prop: Let $R$ be a noetherian ring and let $I$ be a nil ideal. Then $I$ is nilpotent. (i.e., $I^m = (0)$ for some $m \geq 1$.)

*Proof.* Suppose not. Let $\mathcal{S}$ be the set of ideals $J$ such that $\phi(I)$ is nil but not nilpotent in $R/J$ where $\phi : R \to R/J$ is the canonical map. By assumption $(0) \in \mathcal{S}$. Pick $J$ maximal in $\mathcal{S}$. Claim: $J$ is prime. If not ... you get the idea. But now $\phi(I)$ is zero since $R/J$ is a domain, contradiction. □

Hilbert basis theorem

The Hilbert basis theorem says that if $R$ is noetherian then $R[x]$ is noetherian too. We note that if $R[x]$ is noetherian then $R$ is noetherian. (why? homomorphic image.)

Cor 1: If $R$ is noetherian then so is $R[x_1, \ldots, x_d]$ for $d < \infty$.

Cor 2: If $R$ is noetherian and $S$ is a fg $R$ algebra then $S$ is noetherian.

*Proof.* Given $p(x) \in R[x]$ let $in(p(x)) \in R$ be the leading coefficient of $R$. Let $I$ be an ideal in $R[x]$. If $I$ is zero, done. Pick $f_1(x)$ of smallest possible degree. Let $J_1 = (in(f_1)R)$. Pick $f_2$ of next degree. Then there is some $n$ such that $J_n = J_{n+1} = ....$ Claim $I = (f_1, ..., f_n)$. Why? If not, then $f_{n+1} \in I \setminus (f_1, \ldots, f_n)$. Then $m = deg(f_{n+1}) \geq d_i := deg(f_i)$ why? definition. So $in(f_{n+1}) = in(f_1)r_1 + ... + in(f_n)r_n$. Now look at $g := f_{n+1} - r_1 x^{m-d_1} f_1 - ....$ Then $g$ is not in $(f_1, ...., f_n)$ and it has smaller degree. Contradiciton! □

## Lecture 8

Remind that assignment is up. Tensor product ... multiplication?

Jacobson radical. The intersection of all maximal ideals is the Jacobson radical. Note that the Jacobson radical need not be nil. E.g. $a/b : bodd$ what is $J(R)$. A ring is a Jacobson ring if $R/P$ has Jacobson radical zero for every prime $P$. Example. $Z$, a field $F$, $F[x]$. Notice that the following holds:

Prop: $x \in J(R)$ off $1 + ax$ is a unit for every $a \in R$. Proof. Suppose $x \in J(R)$. If $1 + ax$ is not a unit then $R(1 + ax)$ is in a maximal ideal and so is $x$. If $1 - ax$ is a unit for every $a$ then for $P$ maximal, $R/P$ is a field. Now if $x$ is not in $P$ then there is some $a$ such that $ax = 1 \bmod P$. So $1 - ax$ is not a unit.

A ring $R$ is local if it has a unique maximal ideal $M$. A ring is semilocal if it has only finitely many maximal ideals. (Note that a field is local.) When we get to localization, we'll see the importance of local rings. This and Nakayama's lemma become very important.

Thm: Nakayama's lemma. Let $R$ be a ring and let $M$ be a f.g. $R$-module. Suppose that $JM = M$. Then $M = (0)$.

What if $R = a/b : bodd$. $J(R) = 2R$. $M = Q$. Then $J(R)M = M$. $M$ not f.g. Why is this useful? Well, often one has a f.g. module $M$ and one wants to say it is generated by $m_1, ...m_d$. Let $N =< m_1, ..., m_d >$. Then if $J(R)L = L$ where $L = M/N$, we are done. So this means $J(R)M + N = M$. If $J(R)$ is big. Like in a local ring, we are good. So for a local ring we can say that if images of $m_1, ..., m_d$ span $M/JM$ as an $R/J$-v.s. we are done.

*Proof.* Suppose $M$ is nonzero. Then it needs $\geq 1$ gen. Let $m_1, ..., m_d$ be a minimal set of gens. $m_1 = j_1 m_1 + ... + j_d m_d$. now what? □

# Lecture 9

Localization

Let $R$ be a ring and let $S$ be a multiplicatively closed subset of $R$ that does not contain zero (empty product is one). We make a ring $S^{-1}R = \{(r,s)\}/\sim$. Where $(r_1,s_1) \sim (r_2,s_2)$ iff $(r_1s_2 - r_2s_1)s_3 = 0$ for some $s_3 \in S$. check equiv relation. Addition and multiplication. Note that $R$ need not embed in $S^{-1}R$. E.g. $R = ZxZ$, $S = (Z - (0)x0)$. Then $((a,b),s) \sim (c,d,s')$ if and only if $(a,b)s't = (c,d)st$. Take $t = (1,0)$. Then $as' = cs$. So $S^{-1}R = Q$. If $S$ consists of regular elements (non-zero divisors) it is an embedding. (We'll focus on this case and we'll write $s^{-1}r$ for $[(r,s)]$. Universal property of localization. Let $S$ be a multi. closed set of regular elements. If $\phi : R \to T$ and $\phi(S) \subseteq T^*$ then $\phi$ extends to $S^{-1}R$ uniquely. Proof $s^{-1}r$ has to map to $\phi(s)^{-1}\phi(r)$ since $\phi(s)\phi(s)^{-1} = 1$. As before, uniqueness gives that localization is the unique—up to isom—ring with this property. If $B_1$ and $B_2$ both have this property (for a fixed set $S$) then we get a unique homomorphism from $B_1$ to $B_2$ and vice versa. These maps composition must be the identity by uniqueness.

Examples. $f$ non-nilpotent $S = 1, f, f^2, ...$ $S^{-1}R = R_f$. $P$ prime, complement is $S$. $S^{-1}R = R_P$.

$R_P$ is a local ring. Proof. Enough to show that if $x \in PR_P$ then $1 + ax$ is a unit.

## Lecture 10

Example. Let $R$ be a ring and let $S$ be a multiplicatively closed set of regular elements. We say that an ideal $J$ of $R$ is *$S$-saturated* if $sx \in J$ for some $s \in S$ then $x \in J$. Then we have a bijection of posets from the of proper ideals of $S^{-1}R$ to saturated ideals of $R$ that intersect $S$ trivially via $I$ in $S^{-1}R$ maps to $I \cap R$ (this is saturated). one way and $J$ in $R$ maps to $S^{-1}J$ the other way. Proof. $S^{-1}(I \cap R) = I$ for ideals in $S^{-1}R$. Why? containment and contains ... check. If $J$ is a saturated ideal of $R$ then $S^{-1}J \cap R = J$. Why? If $x = s^{-1}j \in S^{-1}J \cap R$ then $sx \in J$ so $x \in J$. Done.

Cor. Let $R$ be a ring and let $S$ be a multiplicatively closed set of regular elements. Then $S^{-1}R$ is noetherian. Proof. Use bijection to show ascending chain in $S^{-1}R$ lifts to an ascending chain in $R$. Must terminate upstairs, so it terminates downstairs.

Notice that every prime ideal is saturated and this bijection takes prime ideals to prime ideals. Why? Thus we have a bijection between primes ideals of $S^{-1}R$ and prime ideals of $R$ that miss $S$. Special case 1: $S = 1, f, f^2, ...$ Then the prime ideals in $S^{-1}R$ correspond to prime ideals of $R$ that do not contain $f$. Prime ideals in $R_P$ correspond to primes that are contained in $P$—this again shows why it is local. Compare with correspondence.

REMARK: If $A$ and $B$ are $F$-algebras ($F$ a field) and $S$ and $T$ are multiplicatively closed sets of regular elements then $S \otimes T$ is multiplicatively closed and $(S \otimes T)^{-1}(A \otimes_R B) \cong S^{-1}A \otimes S^{-1}B$. Why? Use U.P. We have an injective map $A \otimes_R B \to S^{-1}A \otimes T^{-1}B$. Why is it injective? Notice that a tensor product of injective maps need not be injective. (It is a common misperception that this should hold.) As an example, look at $Z_2 \otimes Z_2 \mapsto Z_4 \otimes Z_4$ with the map being $a \otimes b \mapsto 2a \otimes 2b$. Then $1 \otimes 1 \mapsto 2 \otimes 2 = 4 \otimes 1 = 0$. Over a field it is OK, because $A$ and $B$ are $F$-v.s. Pick a basis and use the assignment!)

Moreover $S \otimes T$ gets sent to units so it extends to an injective map $(S \otimes T)^{-1}(A \otimes_R B) \to S^{-1}A \otimes S^{-1}B$. The map is easily seen to be onto since $s^{-1}a \otimes t^{-1}b$ generate.

Corollary. Let $F$ be a field and let $K$ be a f.g. extension of $F$. Then $K \otimes_F K$ is noetherian. In particular, every subfield of $K$ is f.g. by the assignment.

Proof. $K = Frac(A)$, $A$ f.g. $F$-algebra. By the assignment $A \otimes_F A$ is f.g. so it is noetherian by HBT. Then $S = A \setminus \{0\}$ is multiplicatively closed and we have $K \otimes_F K \cong (S \otimes S)^{-1}(A \otimes_F A)$. Since $A \otimes_K A$ is noetherian we have $K \otimes_F K$ is too since it is a localization.

## Lectures 11–12

The Nullstellensatz

Recall that a ring $R$ is a Jacobson ring if the Jacobson radical of every prime homomorphic image is trivial. Equivalently, every prime ideal is the intersection of the maximal ideals above it. We will prove the following general Nullstellensatz.

Nullstelensatz: Let $R$ be a Jacobson ring and let $S$ be a f.g. $R$-algebra. Then $S$ is a Jacobson ring. If $M$ is a maximal ideal of $S$ then $M \cap R$ (remember that $\alpha : R \to S$ and so we will write $R$ for $\alpha(R)$ in $S$—in general $\alpha$ need not be injective, but this doesn't matter—we ll talk about this in class a bit) is a maximal ideal of $R$ and $S/M$ is a finite $R/M \cap R$ extension.

Corollary: If $S = \mathbb{C}[t_1, ..., t_m]$ then $S/M$ is $\mathbb{C}$ so every max ideal is $t_1 - \alpha_1, \ldots, t_m - \alpha_m$.

Proof. $R = \mathbb{C}$. Then $S/M$ is a finite extension of $\mathbb{C}$ and so it is $\mathbb{C}$. Spec and $M$-Spec.

## Lecture 13

Integral extensions

Let $R \subseteq S$ be rings. Then $S$ is an $R$-module. We say that $S$ is an integral extension of $R$ if every $s \in S$ satisfies a monic polynomial equation with coefficients in $R$. E.g., $Q$ is not an integral extension of $R$. $Z[\sqrt{2}]$ is an integral extension of $Z$.

Remark: If $R \subseteq S$ are rings and $S$ is a finite $R$-module then $S$ is integral. Why? Write $S = Ra_1 + \cdots + Ra_k$. Notice that if $s \in S$, we can associate an element of $M_k(R)$ via the rule $s\vec{a} = T(s)\vec{a}$, where $T$ is as defined in class. If $sa_i = 0$ for all $i$ then $sS = 0$ so $s = 0$. Now by Cayley hamilton theorem $s$ is integral.

Given $R \subseteq S$ we say that $s \in S$ is integral if it satisfies a monic polynomial equation with coefficients in $R$.

Theorem: The set of integral elements form a subring of $S$. This is called the integral closure of $R$ relative to $S$.

To prove this, we'll prove the following result:

TFAE: $x \in S$ is integral over $R$
there is a f.g. $R$-submodule $M$ of $S$ such that $Mx \subseteq M$.

*Proof.* If $x$ is integral then there is some $n$ such that $R[x] = M = R + Rx + \cdots + Rx^{n-1}$. Done. Conversely, if we have $M$ then $M = Ra_1 + \cdots + Ra_k$. We have a map given by $x \mapsto T(x)$ as before. Then $x$ satisfies its char poly by CH so we are done. □

*Proof.* Proof of theorem: If $a, b$ are integral of degrees $m$ and $n$, let $M = \sum Ra^i b^j$ with $i < m$ and $j < n$. This is a f.g. $R$-module that works. □

The integral closure of an integral domain $R$ is the integral closure relative to f.o.f. e.g. $C[t^2, t^3]$. If $R$ is equal to its integral closure we say it is integrally closed or we say it is a normal domain.

Theorem: If $R$ is a UFD then $R$ is integrally closed.

*Proof.* Let $a/b \in Frac(R)$ be integral. Then we may assume that $gcd(a, b) = 1$. Finish the proof. □

Important for exercise 3 in assignment 3.

## Lecture 14

Lying over and going up. Theorem: If $R \subseteq S$ is an integral extension, if $P \in Spec(R)$ then there is $Q \in Spec(S)$ with $Q \cap R = P$ (notice this is prime, why?). And we may find $Q \supseteq Q_1$ whenever $Q_1 \in Spec(S)$ with $Q_1 \cap R \subsetneq P$.

*Proof.* First, we may factor out $Q_1$ so we let $P_1 = Q \cap R$. Then replacing $R$ with $R/P_1$ and $S$ with $S/Q_1$ we still have integral extensions. Why? Then correspondence reduces it to lying over. Let $U = R - P$, which is multiplicatively closed. Then $U^{-1}S$ is integral over $U^{-1}R$. Why? So now replace $S$ with $U^{-1}S$ and $R$ with $U^{-1}R$. Then we have $R$ is local with maximal ideal $P$. If $PS \neq S$ then if $L$ is maximal above $PS$ then we have $L \cap R = P$. Why? Well, it contains $P$ and is proper and $P$ is maximal! Now if $PS = S$ then we have $p_1 s_1 + \cdots + p_m s_m = 1$. Let $S'$ be the $R$ algebra generated by $s_1, \ldots, s_m$. Then $S'$ is a finite $R$-module. Why? Integrality! Also $PS' = S'$. Why? $1 \in PS'$ so $S' = (PS')S' = PS'$. So Nakayama's lemma says that $S' = (0)$, contradiction. □

We also have incomparability for integral extensions. If $Q, Q'$ are distinct primes in $S$ with $Q \cap R = Q' \cap R$ then $Q, Q'$ are incomparable. (one cannot contain the other). Why? Suppose that $P = Q \cap R = Q' \cap R$ with $Q \subsetneq Q'$. Then replacing $R$ by $R/P$ and $S$ by $S/Q$ we may assume that $Q' \cap R = (0)$ with $Q'$ not zero. Now pick $x \in Q'$ not zero. Then $x$ is integral over $R$, which is a domain. Then $x^n + \cdots + r_0 = 0$ so $r_0 \in Q' \cap R$, contradiction, since we can make $r_0 \neq 0$.

## Lecture 15

Krull dimension

Given a ring $R$, we let $Kdim(R)$ denote the sup over lengths of ascending chains of prime ideals of $R$ (starting the count from 0). E.g. $Kdim(F) = 0$, $Kdim(F[x]) = 1$, $C[x, y] - - > 2$.

Theorem: If $R \subseteq S$ is an integral extension then $Kdim(S) = Kdim(R)$.

For now we will restrict to noetherian rings.

Noetherian of $dim = 0$ if and only if $R/N$ is a finite product of fields; $N$ is nil radial. $R$ has dimension 1 if every non minimal prime is maximal. A dedekind domain is a normal noetherian domain of Kdim 1.

Krull dimension of polynomial rings.
Lemma: the Krull dimension of $R[x]$ is between $dim(R)$ and $2dim(R) + 1$.

Proof. Suppose that $Q_0 \subseteq \cdots Q_m$ is a chain in $R[x]$. We claim that $Q_i \cap R \neq Q_{i+2} \cap R$. Why? If $P := Q_i \cap R = Q_{i+2} \cap R$. Replace $R = R/P$. Then we have primes $Q_i < Q_{i+1} < Q_{i+2}$ with $Q_j \cap R = (0)$ for $j = i, i+1, i+2$. Let $S = R - 0$. Then the $Q_j$ survive in $F[x] = S^{-1}R[x]$. But $F[x]$ has Kdim 1. So we get the upper bound. Lower bound is easy.

Noether normalization. Let $R$ be a f.g. $k$-algebra and then there is a polynomial subalgebra $S$ in $d = Kdim(R)$ variables with $R$ a finite $S$-module.

Proof. Induction on number of generators. If $R$ is generated by one elt. $R = K[a]$. If $a$ is algebraic over $K$ then $S = K$ otherwise $S = R$.

Assume true for $< m$ generators. Suppose $R = k[a_1, ..., a_m]$. If $a_1, \ldots, a_m$ are algebraically independent; done. If not. there is some nonzero $P(a_1, ..., a_m) = 0$. Exercise: There is a substitution $a_i = u_i + u_m^{A_i}$ for $i < m$ and $a_m = u_m$. Such that $P(u_1 + u_m^{A_1}, ..., u_m) = u_m^D + stuff$, where stuff is of lower degree in $u_m$. Then $R = k[u_1, ..., u_m]$. Then $R$ is a finite $T$ module $T = k[u_1, \ldots, u_{m-1}]$. By inductive hypothesis $T$ is integral over $S$ a polynomial ring in $d$ variables. Since $R$ is finite over $T$ and $T$ is finite over $S$, $R$ is finite over $S$. The result follows.

## Lecture 16

We've just shown that if $A$ is a f.g. $k$-algebra then $A$ is a finite free module over a polynomial ring $B = k[y_1, \dots, y_d]$. Moreover, $A$ is integral over $B$ so $Kdim(A) = Kdim(B)$. We'll show that $Kdim(B) = d$—we'll use an indirect proof, but a direct proof will be done (by you) on the assignment. This gives a strengthened version of NNT: $A$ is a f.g. module over a polynomial ring in $d = Kdim(A)$ variables. Right now all we know, however, is that $Kdim(K[x_1, \dots, x_d[) \geq d$ by using the polynomial extension estimates for Kdim.

Combinatorial Krull dimension. Let $A$ be a f.g. $k$-algebra. Given a $k$-subspace $V$ of $A$, we say $V$ is a frame for $A$ if $V$ is f.dim, $V$ generates $A$ as a $k$-algebra and $1 \in V$. Then $V < V^2 < \cdots$ and the union is all of $A$. We define the dimension function $d_V(n) = \dim(V^n)$. We define the combinatorial Krull dimension (Gelfand-Kirillov dimension) to be

$$GKdim(A) := \limsup_n \log(\dim(V^n))/log\, n.$$

Notice that $GKdim(A)$ is independent of choice of generating space $V$.

Remark: $GKdim(k[x_1, ..., x_d]) = d$.

Lemma: If $A$ is a finite $B$ module then $GKdim(A) = GKdim(B)$.

Cor. If $A$ is a f.g. $k$-algebra then the $GKdim(A) = Kdim(A)$.

Proof. We'll prove this by induction on $Kdim(A)$. We first remark that we have $Kdim(A) \geq GKdim(A)$. Why? NNT. Suppose that there is a ring $A$ with $Kdim(A) > GKdim(A)$. We'll pick such an example with $GKdim(A)$ minimal.
Reduction 1: WLOG $A$ is a polynomial ring. NNT.
So $A = k[x_1, ..., x_d]$. Then $Kdim(A) > d$ and $GKdim(A) = d$.

Let $P_0 < P_1 < \cdots < P_{d+1}$ be a chain of prime ideals of $A$. Then $Kdim(A/P_1) \geq d$. Why?

## Lecture 17

Claim: If $A$ is an integral domain and $I$ is nonzero then $GKdim(A/I) \leq GKdim(A) - 1$.
Let's see how this claim finishes this for us. $GKdim(A/P_1) \leq GKdim(A) - 1 = d - 1$. By minimality of GKdim of our counter-example, $GKdim(A/P_1) = Kdim(A/P_1) \geq d$, a contradiction.

Proof of claim: Pick $f$ nonzero in $I$. Let $V$ be a frame for $A$ that contains $f$. Let $W = \bar{V}$ be the image of $V$ in $A/I$. Then let $W_n \subseteq V^n$ be a subset with $dim(W_n) = dim(W^n)$ and $\bar{W}_n = W^n$. Then $W_n + W_{n-1}f + \cdots + W_0 f^n \in V^n$. This is direct. Why? Finally, if $GKdim(A/I) > GKdim(A) - 1$. Then let $d = GKdim(A)$. Then $dim(W^n) > n^{d-1+\epsilon}$ for infinitely many $n$. This means $dim(V^{2n}) \geq ndim(W^n) > n^{d+\epsilon}$ for infinitely many $n$. So GKdim$(A) > d$. Contradiction.

Cor. Let $A$ be a f.g. $k$-algebra. Then $Kdim(A[x]) = Kdim(A) + 1$.
Proof 1. By NNT $A$ is a finite $k[x_1, \dots, x_d]$-module. So $A[x]$ is a finite $k[x_1, \dots, x_d, x]$-module.

Proof 2. $A[x]$, $V$ a frame for $A$ then $V + kx$ is a frame for $A[x]$. Then $W^n = V^n \oplus V^{n-1}x + \cdots + kx^n$. So $dim(W^n) \leq \dim(V^n)(n+1)$. So GKdim$(A[x]) \leq GKdim(A) + 1$. So $Kdim(A[x]) \leq Kdim(A) + 1$. But we saw the other inequality already.

Transcendence degree

Let $F$ be an extension of a field $K$. We define $trdeg_K(F)$ to be the sup over the cardinality of sets of algebraically independent elements of $F$ over $K$ (possibly can be infinite).
We can define $GKdim(A)$ when $A$ is a not nec. f.g. $k$-algebra to be the sup of all GKdims of f.g. subalgebras of $A$. Notice $GKdim(A)$ is still either infinity or a nonnegative integer. GK dim gives us a nice connection between trdeg and Kdim.
Prop. Let $K$ be an extension of a field $F$. Then $GKdim_F(K) = trdeg_F(K)$. That is GKdim of $K$ as an $F$-algebra is the same as its transcendence degree.

Proof. If $x_1, \dots, x_d$ are algebraically independent then $K$ contains $F[x_1, \dots, x_d]$ so $GKdim(K) \geq d$. Thus $GK \geq trdeg$. Next suppose that $K$ has GKdim $m$. Then if $m < \infty$, $m$ is an integer and $K$ has a f.g. subalgebra $B$ of GKdimension $m$. It follows that $B$ contains a polynomial subalgebra on $m$ generators and so $K$ has trdeg $\geq m$. Thus trdeg is $\geq GKdim$. If $m$ is infinite then we get infinite trdeg too.

Lemma. If $A$ is a f.g. $k$-algebra that is an integral domain and $K$ is its field of fractions then $GKdim_k(K) = GKdim(A)$.
Proof. Let $B$ be a f.g. subalgebra of $K$. Then $B$ is generated by $s^{-1}a_1, \dots, s^{-1}a_m$. So $B$ is contained in the subalgebra $A_s$. So $GKdim(B) \leq GKdim(A_s)$. Next notice that $A_s \cong A[x]/(xs - 1)$. So $GKdim(A_s) \leq GKdim(A[x]) - 1$. Finally, $GKdim(A[x]) = Kdim(A[x]) = Kdim(A) + 1$. So $GKdim(A_s) \leq GKdim(A)$. So $Gkdim(K) \leq GKdim(A)$. On the other hand, $A$ is a f.g. subalgebra of $K$ so ...
One last thing. For a ring $R$, we can define the *height* of a prime ideal $P$. To be the Krull dimension of $R_P$. This is the same

as the length of the longest chain of prime ideals contained in $P$ (and including $P$). So we can define the Krull dimension to be the sup over all heights of primes. Height one primes are especially important—these come up in the study of divisors in algebraic geometry and discrete valuation rings.

Given a ring $R$, we let $X = \mathrm{Spec}(R)$ denote the collection of prime ideals of $R$. (Why is Spec non-empty?). We let $M\text{-}Spec(R)$ denote the set of maximal ideals of $R$. We can actually turn $Spec(R)$ into a topological space. (And $M$-spec too via subspace topology!) We define the closed sets as follows. Given $I$ an ideal in $R$ we let $C_I = \{P : P \supseteq I\}$. Then $C_I$ is the collection of closed sets. Let's see that it is a topology. $\emptyset = C_R$. $X = C_{(0)}$. Closed sets should be closed under finite unions. Enough to do 2. $C_I \cup C_J = \{P : P \supseteq I\} \cup \{P : P \supseteq J\} = \{P : P \supseteq IJ\}$. Why? If $P$ contains $IJ$ then if $P$ doesn't contain $I$ or $J$ there is $a \in I$ and $b \in J$. ... Arbitrary intersections. $\cap C_{I_\alpha} = C_{\sum I_\alpha}$. Why? If $P \supseteq I_\alpha$ for all $\alpha$ then it contains $I_\alpha$. Conversely, if $P \supseteq \sum I_\alpha$ then $P \supseteq I_\alpha$ for all $\alpha$. $X$ endowed with this topology is called the Zariski topology. What is the Zariski topology on $X = Spec(Z)$. How about $Spec(C[t])$? How about $Spec(Q)$? $Spec(\{a/b : b \text{ odd}\})$?

Notice that $C_I \supseteq C_J$ if and only if $\sqrt{I} \subseteq \sqrt{J}$ and $C_I = C_{\sqrt{I}}$, so we'll only consider radical ideals. Recall that a topological space $X$ is disconnected if it can be written as a union of two disjoint closed sets.
Correspondence. $C_I$ inherits the subspace top. Then $C_I$ is homeomorphic to $Spec(R/I)$. Via the map $P \in C_I \mapsto P/I$ bijection. We just need to check that this is a continuous map with cts inverse. If $Y$ is a closed subset of $Spec(R/I)$ then $Y = C(J/I)$ for some ideal $J$ of $R$ that contains $I$. Then the pre image of $Y$ is $C_J$. Conversely, if $Y$ is a closed subset of $C_I$ then $Y = C_J$ for some radical ideal $J$ containing $I$. Then the forward image is just $C_{J/I}$.
Localization. $Spec(S^{-1}R) \to Spec(R)$ is a continuous injection.
$P \mapsto P \cap R$. Then this is injective. If $C_J$ is a closed subset of $Spec(R)$ then the pre image is all primes $P$ that contain $J$ and have the property that $S \cap P$ is empty. If $J \cap S$ is non-empty, $J$ radical, this is just an empty set. Otherwise we have $S^{-1}J$ and this is $C_{S^{-1}J}$. Notice that the image is an open subset when $S = \{1, f, \ldots\}$ : It is just $Spec(R) - C_{(f)}$.

## Lecture 18

Prop: 1) X=Spec(R) is disconnected if and only if 2) $R \cong R_1 \times R_2$ if and only if 3) $R$ has an idempotent $e \neq 0, 1$.

*Proof.* if (3) then $R \cong Re \times R(1-e)$. So (3) gives (2). If (2) then every prime contains $(1,0)$ or $(0,1)$ so $R = C_{(1,0)} \cup C_{(0,1)}$. Disjoint because if $P$ contains $(1,0)$ and $(0.1)$ then it contains $(1,1)$. Finally (1) implies (3). If $X = C \cup D$ then $C = C_I$ and $D = C_J$. Then disjoint says that $I + J = R$. (Why? maximal ideal otherwise). Also union says $P \supseteq IJ$ for all $P$, so $IJ$ is in the nil radical of $R$. Thus $1 = x + y$, $x \in I$ and $y \in J$ and $(xy)^m = 0$. Then let $e = \sum_{j=0}^{m} \binom{2m}{j} x^j y^{2m-j}$ and $1 - e = \sum_{j=m+1}^{2m}$. Then $e(1-e) = 0$. Why is $e \neq 0, 1$. Well, $e \in J$ so it can't be 1 and $1 - e \in I$ so it can't be 1. □

A topological space $X$ is reducible if and only if it can be written as $Y \cup Z$ with $Y, Z$ proper closed subsets not nec. disjoint. $X$ is irreducible if and only if $R$ is prime and $C_I$ is irreducible if and only if $\sqrt{I}$ is prime.

Prop: Let $R$ be a ring. Then $X = Spec(R)$ is quasi-compact. (In alt geom, it is normal to use the term quasi-compact and reserve compact for Hausdorff+quasi-compact)

*Proof.* Let $\cup U_\alpha$ be an open cover of $X$. Each $U_\alpha = X \setminus C_{I_\alpha}$. Then $\cap C_{I_\alpha} = \emptyset$. This means $\sum I_\alpha = R$. So $1 = x_1 + \cdots + x_d$, $x_i \in I_{\alpha_i}$. So $\sum_{j=1}^{d} I_{\alpha_j} = R$ thus ... □

Notice that $X = Spec(R)$ is rarely Hausdorff. In fact for a noetherian ring it occurs if and only if every prime is minimal. To see this, let $P$ be a prime and suppose that $P$ is not minimal. Then there is some prime $Q \subsetneq P$. If $X$ is Hausdorff, there are neighbourhoods $U_P$ and $U_Q$ disjoint. What does this mean? It means we have closed sets $C_I$ and $C_J$ such that $P \notin C_I$ and $Q \notin C_J$ such that $C_I \cup C_J = X$. But $Q$ doesn't contain $J$ so $P$ doesn't. Thus $P$ is not in $C_J$. This means $P$ is not in the union. Also: POINTS ARE CLOSED in hausdorff space. Maximal ideals are the only closed points.

If every prime is minimal then $R$ has only finitely many primes (noetherian ring). Why? Now these points are closed and open.

DIMENSION

This gets us to a notion of dimension of a topological space and dimension of a ring. Let $X$ be a topological space. Given a top space we say it is noetherian if every descending chain of closed sets terminates. Notice that if $R$ is noetherian then $Spec(R)$ is noetherian. Check it! We say that the dimension of $X$ is the sup over all strictly descending chains of irreducible closed subsets $C_0 \subseteq C_1 \subseteq C_2 \cdots C_n$. Notice that $C = C_I$ is irreducible if and only if $I$ is a prime ideal. So the dimension of $Spec(R)$ is the same as the sup over lengths of ascending chains of prime ideals of $R$. This is called the Krull dimension of $R$. So $Kdim(R)$ is the Krull dimension of $Spec(R)$.

Theorem: $R$ is noetherian and dim 0 if and only if $R$ is noetherian and $spec(R)$ is compact Hausdorff if and only if $R$ is noetherian and $spec(R)$ is finite and discrete if and only if $R/N$ is isomorphic to a product of fields, $N$ nil radical. Cor: If $R$ is a noetherian domain of Krull dimension 0 then $R$ is a field.

We'll see that zero dimensional noetherian rings are precisely those rings that are artinian; namely rings where every descending chain of ideals terminates. Let $R$ be a ring. We say that an $R$ is artinian if ... We say that an $R$-module $M$ is artinian if and only if every descending chain of $R$-submodules terminates. Notice $R$ is artinian if and only if $R$ is artinian as a module over itself.

$R$ is artinian if and only if every nonempty subset of ideals of $R$ has a minimal element. $M$ is artinian if and only if every nonempty subset of submodules has a minimal element.

If $0 \to M_1 \to M \to M_2 \to 0$ is a s.e.s. of $R$-modules then $M$ is artinian if and only if $M_1$ and $M_2$ are.

*Proof.* If $M_1$ and $M_2$ are artinian and we have a d.c. $N_i$ of submodules of $M$ then looking at the quotient it stabilize so $\bar{N}_i = \bar{N}_{i+1}$ and $N_i \cap M_1 = N_{i+1} \cap M_1$. Now we know. This is for noetherian too. □

## Lecture 19

Also if $R$ is artinian then every homomorphic image of $R$ is artinian.

**Corollary 0.1.** *If $R$ is a ring in which zero is a product of maximal ideals then $R$ is artinian if and only if $R$ is noetherian.*

*Proof.* Let $(0) = P_1 \cdots P_s$. Let $M_i = P_1 \cdots P_i$. We claim that each $M_i$ is artinian. Notice $M_s$ is artinian. We want to show $M_0$ is. If it's not, pick the smallest $i$ for which $M_i$ is not artinian. Then $M_{i+1} \to M_i \to M_i/M_{i+1}$. Notice $M_{i+1}$ is artinian. Also $M_i/M_{i+1}$ is an $R/P_{i+1}$-module spanned by images for generators for $M_1 \cdots M_i$. Thus it is finite-dimensional and hence artinian. Other direction is similar. □

**Theorem 0.1.** *Let $R$ be a ring. Then $R$ is artinian if and only if $R$ is noetherian and Krull zero.*

*Proof.* If noetherian and Kdim $= 0$ then $(0)$ is a product of maximal ideals. Done.

For the other direction, we'll do some structure theory.

Claim 1: If $R$ is artinian and Let $P$ be prime. We claim that $P$ is maximal. If not let $S = R/P$. This is an artinian domain. We claim $S$ is a field. Let $x \in S$ be nonzero. Let $I_n = x^n S$. Then $I_n = I_{n+1}$ so $x^n = x^{n+1}y$. Now we can cancel and we get $xy = 1$. Thus $P$ is maximal.

Claim 2: We claim we have only finitely many prime ideals. If we have $P_1, P_2, \ldots$. Let $I_n = P_1 \cap P_2 \cdots P_n$. Then $I_n \subseteq P_{n+1}$ by artinian property. So $P_{n+1} = P_i$ for some $i$.

Claim 3: $J(R)$ of $R$ artinian is nilpotent. Proof. By artinianness we have $J^n = J^{2n}$ for some $n$. Suppose that $J^n$ is nonzero. Let $S$ be the set of all ideals $I$ such that $J^n I \neq (0)$. Then $J \in S$. Pick $L$ minimal in $S$. Then there is some $x \in L$ such that $J^n x \neq (0)$. So $L = Rx$ by minimality. Then $J^n L \subseteq L$ and $J^n L \in S$ since $J^n J^n L = J^{2n} L = J^n L$. Thus $J^n L = L$. So $JL = L$ and $L$ is f.g. so by Nakayama we have $L = (0)$.

Thus we have that $(0)$ is a product of maximal ideals in an artinian ring and so $R$ is noetherian and Kdim is zero. □

## Lecture 20

Now we'll turn our attention to height one primes. To do this, we need some background. Primary decomposition.

**Definition 0.2.** *Let $R$ be a ring. We say that an ideal $I$ of $R$ is* primary. *If whenever $xy \in I$ we have either $x \in I$ or $y^n \in I$ for some $n \geq 1$. This means that if $xy \in I$ then either $x \in I$, $y \in I$ or there is some $n \geq 1$ such that both $x^n$ and $y^n$ are in $I$.*

Notice that any prime ideal is primary, by the definition (take $n = 1$). Notice that as a corollary, if $ab \in I$ and $a \notin \sqrt{I}$ then $b \in I$. Why? Take $y = a$ and $x = b$. Then $xy \in I$. If $x \notin I$ then $y^n \in I$, which means $a = y \in \sqrt{I}$.

**Lemma 0.3.** *Let $Q$ be a primary ideal. Then the radical ideal of $Q$ is a prime ideal.*

*Proof.* Suppose that $P = \sqrt{Q}$ is not prime. Then there exist $x, y \in R \setminus P$ such that $xy \in P$. Then $x^n y^n \in Q$. By the definition, either $x^n \in Q$ or there is some $m$ such that $y^{nm} \in Q$. Thus either way $x$ or $y$ is in $P$. □

**Definition 0.4.** *If $Q$ is primary and $P = \sqrt{Q}$, we say that $Q$ is $P$-primary.*

Example we did in class. The primary ideals of $\mathbb{Z}$ are precisely $(0)$ and $p^n\mathbb{Z}$. Prove it! Notice prime powers need not be primary. Example we did in class. If $A = \mathbb{C}[x, y, z]/(xy - z^2)$ then if $P$ is the ideal generated by the images of $x$ and $z$, then $A/P \cong \mathbb{C}[y]$, so $P$ is prime. We claim that $P^2$ is not $P$-primary. Notice that (the image of) $xy = z^2 \in P^2$ and so if $P^2$ is primary then either $x \in P^2$ (nope!—look at degees!) or $y^n \in P^2$ (nope!—this would mean $y^{2n} \in P$, which we know doesn't occur). We can say something in the case that the radical ideal is maximal.

**Proposition 0.5.** *Let $R$ be a ring and suppose that $Q$ is an ideal with $P := \sqrt{Q}$ a maximal ideal. Then $Q$ is $P$-primary.*

*Proof.* Look at $R/Q$. $R/Q$ is a local ring with maximal ideal $P/Q$ (why?). Thus every element in $R$ is either in $P/Q$ or is a unit. In particular, if $xy \in Q$ then $xy \in P$ so $x$ or $y$ is in $P$. If $y \in P$ then $y^n \in Q$ for some $n$ since $P$ is radical over $Q$. If $y \notin P$ then $y$ is a unit in $R/Q$ and so $xy \in Q$ gives $x \in Q$. □

We'll show that in a noetherian ring every ideal has a primary decomposition—this means that every ideal is the intersection of a finite set of primary ideals. This is a bit like how we showed that in a noetherian ring that every radical ideal is the intersection of prime ideals. To do this, we'll introduce the notion of irreducible ideals.

**Definition 0.6.** *Let $I$ be an ideal in a ring $R$. We say that $I$ is* irreducible *if $I = J \cap K$ implies $I = J$ or $I = K$. This is not to be confused with the notion of irreducibles in* Spec$(R)$.

Notice any prime ideal is irreducible.

**Lemma 0.7.** *In a noetherian ring every ideal is a finite intersection of irreducible ideals.*

*Proof.* Suppose not and let $I$ be the biggest ideal in $R$ that is not an intersection of finitely many irreducibles. Then obviously $I$ is not irreducible. So there exist $J, K \supsetneq I$ such that $J \cap K = I$. But now $J$ and $K$ are finite intersections. Done! □

**Lemma 0.8.** *In a noetherian ring every irreducible ideal is primary.*

*Proof.* Let $I$ be an irreducible ideal of $R$. Then passing to $R/I$, we see (0) is irreducible and so it is enough to show (0) is primary in $R/I$. So we replace $R$ by $R/I$ and assume (0) is irreducible. Suppose that $xy = 0$ but $x \neq 0$. We must show $y^n = 0$ for some $n$. Let $J_n = \{a \in R\colon ay^n = 0\}$. Then $J_1 \subseteq J_2 \subseteq \cdots$ is a chain of ideals. Since $R$ is noetherian, it terminates, say $J_n = J_{n+1}$. This means that $(x) \cap (y^n) = (0)$. Why? If $a \in (x)$ and $a \in y^n$ then $a = bx$ and so $ay = 0$. But $a = cy^n$ so $ay = cy^{n+1} = 0$ so $c \in J_{n+1} = J_n$ and so $cy^n = 0 = a$. But now since $(0) = (x) \cap (y^n)$ and (0) is irreducible and $(x) \neq (0)$ we see $(y^n) = (0)$. □

**Corollary 0.9.** *In a noetherian ring every ideal is a finite intersection of primary ideals.*

What about noetherian one-dimensional rings? These are rings in which every prime ideal that is not minimal is maximal. E.g. $Z, k[t]$.

## Lecture 21

Valuation rings

Let $K$ be a field. A map $\nu : R \to \mathbb{Z} \cup \{\infty\}$ is called a valuation if $\nu(a) = \infty$ if and only if $a = 0$; $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a + b) \geq \min(\nu(a), \nu(b))$.

Given a field $K$ with a valuation $\nu$, we define the valuation ring $R = O_\nu$ of $\nu$ to be the set of $x \in K$ such that $\nu(x) \geq 0$. Notice that $R$ is a local ring with unique maximal ideal $M_\nu$ all things with valuation $> 0$. Why is it unique. If $\nu(x) = 0$ then $\nu(1/x) = 0$. Well, we need to check that $\nu(1) = 0$, but this is fine: $\nu(1) = \nu(1^2) = \nu(1) + \nu(1)$. A ring $R$ is called a d.v.r if it is the valuation ring of some valuation on a field. Example, power series, $Z_{(p)}$.

Remark. A d.v.r. is a PID. Proof. Let $I$ be an ideal of $R$ that is nonzero. Then there is some smallest $m$ such that $\nu(x) = m$ for some $x \in I$. We claim that $I = (x)$. To see this, suppose that $y \in I$. Then $\mu(y) \geq m$ so $mu(y/x) \geq 0$ so it is in $R$. In particular, $R$ is noetherian.

Cor. $R$ has Kdim $\leq 1$.

Proof. Suppose that $P \subseteq Q$ are distinct nonzero primes. Then $Q = (x)$ for some $x$ and $P = (y)$; moreover $\nu(y)$ is minimal among all elements of $P$. Since $P$ is contained in $Q$, we have $y = xa$. Thus $x \in P$ or $a \in P$. By assumption, $x \notin P$ so $a \in P$—but this has smaller valuation.

Another nice fact. If $R$ is a d.v.r then $R$ is integrally closed. Proof. Let $x \in K$ be integral over $R$. Then $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, $a_i \in R$. If $x \notin R$ then $\nu(x) < 0$; but now $\nu(x^n) < \nu(-(a_{n-1}x^{n-1} + \cdots + a_0))$.

In fact, we'll soon see that dvrs are characterized by being noetherian local domains of Kdim 1 that are integrally closed. This means that if we start with an integrally closed noetherian domain $A$ and localize at a height one prime $P$ we'll get a dvr. Why? $A_P$ is local noetherian and Kdim 1. It is integrally closed because

Remark. If $A$ is an integrally closed domain then so is $S^{-1}A$. If $x \in Frac(S^{-1}A)$ is integral over $S^{-1}A$ then $x^n + \cdots + s_0^{-1}a_0 = 0$. Now multiply by $s^n = s_0 \cdots s_{n-1}$. Then $s^n x^n + b_{n-1}(sx)^{n-1} + \cdots + b_0 = 0$, $b_i \in A$. Since $A$ is integrally closed, $sx \in A$ so $x \in S^{-1}A$.

We are going to look at rings of Krull dimension one in this context. We need to begin with a lemma.

**Lemma 0.10.** *Let $A$ be a noetherian integral domain of Kdim 1. Then every nonzero ideal in $A$ can be expressed uniquely as a product of primary ideals whose radicals are pairwise distinct.*

To do this we need a remark. Let $P$ be a fixed prime. If $Q_1, \ldots, Q_r$ are $P$-primary ideals then so is $I := Q_1 \cap Q_2 \cdots \cap Q_r$. To see this notice that the radical of $I$ is $P$. If $xy \in I$. Then if $x \in I$, we are done. So $x \notin I$. Then $x \notin Q_i$. But this means that $y^n \in Q_i$ so $y \in P$. But now $y^N \in I$ since $P$ is the radical of $I$. As a corollary, we see that in a noetherian ring every ideal has a primary decomposition $Q_1 \cap \cdots \cap Q_s$ where the radicals of the $Q_i$ are distinct. Now we prove the lemma.

*Proof.* Let $I$ be a nonzero ideal of $A$. Then $I$ has a primary decomposition with distinct radicals, say $I = Q_1 \cap \cdots \cap Q_s$. Let $P_1, \ldots, P_s$ be the radicals of $Q_1, \ldots, Q_s$. Then Claim: $Q_i + I_i := \prod_{j \neq i} Q_j = A$.

To see this, notice that if not $Q_i + I_i$ must be contained in some maximal ideal $P$. But $P_i$ is the only max ideal above $Q_i$ since our ring is Kdim 1; If $I_i$ is in $P_i$ then some $Q_j$ must be in $P_i$, which is impossible.

Notice that $Q_1 \cap \cdots \cap Q_s = Q_1 \cdots Q_s$: one containment is clear. Notice that we have $Q_i + \prod_{j \neq i} Q_j = A$, too, so there is $x_i \in Q_i$ and $y_i \in I_i$ such that $x_i + y_i = 1$. Then If $z \in Q_1 \cap \cdots \cap Q_s$, we have $z = z(x_1 + y_1) \cdots (x_s + y_s) \in Q_1 \cdots Q_s$. Why? If we choose even one $y_j$, we're done since $z$ is in all the $Q_j$. So we only need to look at $zx_1 \cdots x_s$, but that is in the product too. □

Now we can study some local rings of Kdim 1.

**Proposition 0.11.** *Let $A$ be a noetherian local domain of Kdim 1 and let $P$ be its max ideal and $k = A/P$ its residue field. Then TFAE.*

(i) *$A$ is a d.v.r.*
(ii) *$A$ is integrally closed*
(iii) *$P$ is principal.*
(iv) *$dim_k(P/P^2) = 1$*
(v) *every nonzero proper ideal is a power of $P$*
(vi) *there is some $x$ such that every nonzero ideal is of the form $x^n$.*

*Proof.* We just saw $1- > 2$. For $2- > 3$, let $a \in P \setminus P^2$. Then $P$ is radical over $(a)$ and so $P^n \subseteq (a)$ since the radical ideal is nilpotent in a noetherian ring. Thus there is some smallest $n$ such that $P^n \subseteq (a)$. If $n = 1$, we're done. If not, pick $b \in P^{n-1} \setminus (a)$. Then look at $x = a/b$. Then $x^{-1} \notin A$ since $b \notin (a)$. Thus $x^{-1}$ is not integral over $A$ since $A$ is integrally closed. But notice that $Px^{-1} \subseteq A$ since $Pb$ is in $P^n$ and $a \supseteq P^n$. Thus $Px^{-1}$ is an ideal of $A$. Notice that if it is all of $A$, we get $Ax = P$, and so we are done. Otherwise we have $Px^{-1} \subseteq P$. But $P$ is a f.g. $A$-module with $Px^{-1} \subseteq P$ and this gives $x^{-1}$ integral over $A$, contradiction. $3 - - > 4$ is immediate: if $P = (x)$, then $P/P^2 = kx + P^2$. $4- > 5$ is OK too. If $P/P^2$ is 1-diml, then $P$ is principal by Nakayama: if $x \in P \setminus P^2$ then $Ax + P^2 = P$ and so we get $P = Ax$ by looking at $P/Ax$. If $I$ is a nonzero proper ideal then $I \subseteq P$. Pick the biggest $n$ for which $I \subseteq P^n$; then if $I \neq P^n$ there is some $y \in I$ such that $y = ax^n$ but $y \neq bx^{n+1}$. Thus $a \notin (x) = P$ and so $a$ is a unit. Thus $y = x^n$, so $I \supseteq (x^n)$. So $I = (x^n) = P^n$. To see $5- > 6$, let $x \in P \setminus P^2$. Then $(x) = P^k$. Since $x \notin P^2$, we see $k = 1$ and $(x) = P$. Now we get $I = P^k = (x^k)$. WAIT! We cheated. How do we know that $P$ is not $P^2$? If $P = P^2$ then $J(A)P = P \cdot P = P^2 = P$ and so $P = (0)$ by Nakayama's lemma!

Ok $6- > 1$ can't be hard, right? Let $K$ be the field of fractions of $A$. Let $\nu(a)$ for $a$ nonzero in $A$ be defined by $\nu(a) = m$ when $(a) = (x)^m$. Show this gives a valuation. □

## Dedekind domains

Let's recall that a Dedekind domain is an integrally closed noetherian domain of Krull dimension one.

Examples: $\mathbb{Z}, \mathbb{C}[t]$.

We showed UFDs are integrally closed and we showed that both rings are noetherian and of Kdim 1. Now we'll give a characterization of Dedekind domains. The next result shows that Dedekind domains can be characterized in terms of their local rings and in terms of their primary ideals.

**Proposition 0.12.** *Let $A$ be a noetherian domain of Krull dimension one. Then TFAE:*

(i) *$A$ is integrally closed (in particular, $A$ is a dedekind domain);*
(ii) *every primary ideal in $A$ is a prime power (we saw this in the special case when $A = \mathbb{Z}$);*
(iii) *Every local ring $A_P$ with $P$ a nonzero prime is a d.v.r.*

*Proof.* Let's show the equivalence of (i) and (iii). We know that if $A$ is an integrally closed domain then so is $S^{-1}A$ for any multiplicatively closed set of nonzero elements—we've shown this. Thus if $P$ is a nonzero prime ideal then $A_P$ is a noetherian local ring of Kdim 1 that is integrally closed. We showed last time that this is equivalent to being a d.v.r. To see the other direction, suppose that each $A_P$ is a d.v.r. when $P$ is a nonzero prime ideal. Then each $A_P$ is integrally closed. Now let $C$ be the integral closure of $A$ in its field of fractions. If $A = C$, we are done, so we'll show this. Since $A \subseteq C$, we have an inclusion map $f : A \to C$. We must show that $f$ is in fact onto.

We claim that $f$ is onto. Suppose not and let $c \in C \setminus A$. Notice that if we let $S = A \setminus P$ then $S$ is a multiplicatively closed subset of $A$ and $C$. We have $A_P = S^{-1}A$ and we define $C_P := S^{-1}C$. We can check that $C_P$ is contained in the integral closure of $A_P$—this is an easy exercise to leave to the students. Since $A_P$ is integrally closed, we have that $A_P = C_P$ for all maximal ideals $P$. Since $C \subseteq C_P$ we see that $c \in A_P$ for every maximal ideal $P$ of $A$. In particular, there is some $s \notin P$ and some $a \in A$ such that $c = as^{-1}$. In other words, $cs \in A$. Let $I = \{s \in A : cs \in A\}$. Then $I$ is an ideal. We claim $I = A$; if not, $I$ is contained in some maximal ideal $P$. But we just showed there was some $s \notin P$ such that $cs \in A$ and hence $s \in I$ and so $I \not\subseteq P$. It follows that $1 \cdot c \in A$ and so $A = C$. So we've shown (i) and (iii) are equivalent.

Now we'll show that (i) and (ii) are equivalent. Suppose first that (ii) holds. To do this, it suffices to show that $A_P$ is a d.v.r. whenever $P$ is a maximal ideal—we showed this characterizes Dedekind domains when $A$ is a noetherian domain of Krull dimension one. So consider the local ring $A_P$. Let $J$ be a nonzero ideal of $A_P$. Then the radical of $J$ is $PA_P$ since $A_P$ has only two prime ideals (0) and $PA_P$ and $J$ is nonzero. Since $A$ is noetherian, there is some $n \geq 1$ such that $(PA_P)^n = P^nA_P \subseteq J$. Now let $I = J \cap A$. Then $I \supseteq P^n$. It follows that $P$ is the radical of $I$ since $P^n \subseteq I$. Since $P$ is maximal, we see that $I$ is a primary ideal—we showed in class that any primary ideal whose radical is maximal is necessarily primary.

Now what? Since (ii) holds, $I$ is a prime power; moreover, since the radical of $I$ is $P$, we see that $I = P^m$ for some $m$. We know that $J = IA_P$ since $I = J \cap A$—**remark: we showed in class that if $J$ is an ideal of $S^{-1}A$ and $I = A \cap J$ then**

**$J = S^{-1}I$; doing it in the other order, namely starting with an ideal of $I$ then going to $S^{-1}I$ and intersecting down to $A$ doesn't necessarily return $I$—we showed this occurs if and only if $I$ is what we called $S$-saturated: namely, if $sx \in I$ and $s \in S$ then we must have $x \in I$.** This means that $J = IA_P = P^m A_P = (PA_P)^m$. This means that every nonzero ideal of $A_P$ is a power of $PA_P$ and so we see from a result last time that $A_P$ is a d.v.r. Since this holds for every nonzero $P$ and $A$ is a noetherian domain of Krull dimension one, we get that $A$ is a Dedekind domain, and so we get (i).

Suppose that (i) holds, so that $A$ is a Dedekind domain. Let $I$ be a primary ideal and let $P$ be its radical. Then we showed last time that $A_P$ is a d.v.r. Thus the ideal $IA_P$ is a power of $PA_P$, say $IA_P = (PA_P)^m = P^m A_P$. Now we want to show that $I$ is $P^m$, but that takes some arguing. We showed during the lectures on localization that if $S$ is a multiplicatively closed set, then there is a bijection between the $S$-saturated ideals (see above for definition) of $A$ and the ideals of $S^{-1}A$ given in one direction by $I \mapsto S^{-1}I$ and in the other by $J \mapsto J \cap A$. So to finish this proof, we'll show that any primary ideal with radical $P$ is $S$-saturated, where $S = A \setminus P$ (the set we invert to form the local ring $A_P$). Let $J$ be a primary ideal with radical $P$. Let's recall the definition of primary: if $xy \in J$ then either $x \in J$ or $y^n \in J$ for some $n \geq 1$. So let's show that a $P$-primary ideal is $S$ saturated when $S = A \setminus P$. Suppose that $xs \in J$ with $s \in S$. Then $s \notin P$ and so no power of $s$ can be in $J$ since if $s^n \in J$ then $s^n \in P$ since $P$ is the radical of $J$; since $P$ is prime, this gives $s \in P$, which cannot occur. It follows that $x \in J$, since $J$ is primary. Thus $J$ is $S$-saturated. Now $I$ and $P^n$ are both $P$-primary. ($P^n$ is $P$-primary, since its radical is $P$, which is a maximal ideal: we showed that ideals whose radical is maximal are primary.) Thus $I$ and $P^n$ are both $S$-saturated. It follows that

$$I = (IA_P) \cap A = (P^m A_P) \cap A = P^m.$$

Thus we get (ii). □

The next result shows that Dedekind domains, while not always UFDs, have something close to this property.

**Corollary 0.13.** *Let $A$ be a Dedekind domain. Then every nonzero ideal has a unique (up to ordering) factorization as a product of prime ideals.*

*Proof.* We showed last time that every nonzero ideal in a noetherian domain of Krull dimension one is a product of primary ideals with pairwise distinct radicals. We just showed that in a Dedekind domain every primary ideal is a prime power. This gives that if $I$ is a nonzero ideal then $I$ has a factorization $I = P_1^{m_1} \cdots P_k^{m_k}$ where $P_1, \ldots, P_k$ are distinct nonzero primes.

We'll now show uniqueness. Suppose that we have two factorizations: $I = P_1^{m_1} \cdots P_k^{m_k} = Q_1^{n_1} \cdots Q_j^{n_j}$ with the $P_i$ pairwise distinct and the $Q_j$ pairwise distinct and the $m_i, n_j$ all positive. We first note that $\{P_1, \ldots, P_k\} = \{Q_1, \ldots, Q_j\}$ since if $P_i \notin \{Q_1, \ldots, Q_j\}$ then $Q_1^{n_1} \cdots Q_j^{n_j} \subseteq P_i$. We have shown multiple times that this can only occur if $P_i$ contains some $Q_j$. Since all nonzero primes are maximal, we see that $P_i = Q_j$ for some $j$. Thus $\{P_1, \ldots, P_k\} \subseteq \{Q_1, \ldots, Q_j\}$. By symmetry we get the other inclusion. Thus $k = j$ and after ordering, we may assume that $P_i = Q_i$ for all $i$. From now on, we'll just take $j = k$ and write $P_i$ for $Q_i$. We must show that $n_i = m_i$ for all $i$.

Notice that if we pass to the local ring $A_P$, we have

$$(P_1 A_P)^{m_1} \cdots (P_k A_P)^{m_k} = (P_1 A_P)^{n_1} \cdots (P_k A_P)^{n_k}.$$

Now let's take $P = P_i$. Then the LHS becomes $(P_i A_{P_i})^{m_i}$ since $P_j$ contains a unit in $A_{P_i}$ for $j \neq i$. Similarly, the RHS becomes $(P_i A_{P_i})^{n_i}$. Thus $(P_i A_{P_i})^{m_i} = (P_i A_{P_i})^{n_i}$ in $A_{P_i}$. This then gives $m_i = n_i$. OR DOES IT?

Well, it does, but we need to show this. Now $A_{P_i}$ is a d.v.r., so to show this, it suffices to show the following claim.

Claim: Let $R$ be a d.v.r. of Krull dimension one (to rule out a field where all nonzero elements have zero valuation). Then if $P$ is the maximal ideal of $R$ then $P^m = P^n$ if and only if $m = n$.

Suppose that $P^m = P^n$ with $m < n$. Then $P^m = P^{m+1}$ since $P^m \supseteq P^{m+1} \supseteq P^n = P^m$. This means that $J(R)P^m = P \cdot P^m = P^{m+1} = P^m$, and so $P^m = (0)$. But now since $R$ is a domain, we see that $P^m = (0)$ implies that $P = (0)$ and so $R$ is a field, a contradiction.

From the claim, we see that $m_i = n_i$ for all $i$ and so we get unique factorization. □

As an important case, we look at number rings. Let $K$ be a field that is a finite extension of $\mathbb{Q}$. We say that $R \subseteq K$ is a *number ring* if $R$ is the integral closure of $\mathbb{Z}$ inside $K$.

Example. $\mathbb{Z}[\sqrt{2}]$ is the integral closure of $\mathbb{Z}$ in $\mathbb{Q}(\sqrt{2})$. Let's see why!

We know that $\sqrt{2}$ is integral over $\mathbb{Z}$ since it satisfies $x^2 - 2 = 0$. Since the integral elements form a ring, we see that $\mathbb{Z}[\sqrt{2}]$ is contained in the integral closure. On the other hand if $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, $a, b$ rational, is integral over $\mathbb{Z}$, then so is $a - b\sqrt{2}$ since any integer polynomial having $a + b\sqrt{2}$ as a root also has $a - b\sqrt{2}$ as a root (this is either an easy exercise or the students know enough Galois theory to know it is trivial). Since the integral elements form a ring, we have that $2a = (a + b\sqrt{2}) + (a - b\sqrt{2})$ is integral over $\mathbb{Z}$. Since $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$, we see that $2a$ is an integer. Similarly, $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 \in \mathbb{Z}$ and $4b = (a + b\sqrt{2})\sqrt{2} - (a - b\sqrt{2})\sqrt{2}$ is an integer. So we see that $a = a_0/2$ and $b = b_0/4$ for some integers $a_0, b_0$. Also, $a^2 - 2b^2 = a_0^2/4 - b_0^2/8$ is an integer. Multiplying by 4 we see that $b_0^2/2$ is an integer and so

$b_0$ is even. Thus we can write $b = b_1/2$. Then we have $a^2 - 2b^2 = (a_0^2 - 2b_1^2)/4$ is an integer. In particular, $a_0^2 - 2b_1^2$ must be even and so $a_0$ must be even. Thus $a \in \mathbb{Z}$. Hence $2b^2$ is an integer and so $b$ must be an integer too.

Let's notice that $R = \mathbb{Z}[\sqrt{2}]$ is a number ring and let's now show that $R$ is a Dedekind domain. Notice that $R$ is a finitely generated $\mathbb{Z}$-algebra—it's generated by $\sqrt{2}$ over $\mathbb{Z}$. Thus $R$ is noetherian by the Hilbert basis theorem; since $R$ is an integral extension of $\mathbb{Z}$, we see, from an earlier result from class, that $R$ and $\mathbb{Z}$ both have the same Krull dimension—in this case it is one; finally, we can check that $R$ is integrally closed in its field of fractions: leave this as an exercise to the students. If students ask whether it follows from the definition of $R$, then you can say 'yes', but it requires proof.

In fact, the following theorem holds, but this proof is done in Algebraic Number Theory, so we will not do it.

**Theorem 0.2.** *Let $R$ be a number ring. Then $R$ is a Dedekind domain.*

This gives the fact that we have unique factorization of nonzero ideals into prime ideals in a number ring.

Let's now tie up some loose ends with height one primes. There are two last results that we should touch upon, and this will conclude the course.

(i) Krull's principal ideal theorem: if $A$ is a noetherian ring and $f$ is a non-unit then any prime ideal $P$ that is minimal with respect to containing $Af$ is necessarily of height at most one;
(ii) (Characterization of UFDs). Let $A$ be a noetherian domain. Then $A$ is a UFD if and only if every height one prime is principal.

We will postpone the proof of Krull's PIT, but we will assume it when characterizing UFDs and then give its proof, which is technical, later.

Let's recall some facts about UFDs. Recall that if $R$ is an integral domain, then an element $f \in R$ is called prime if $(f) = Rf$ is a prime ideal; a nonzero, non-unit element $f$ of $R$ is irreducible, if whenever we have $f = ab$ with $a, b \in R$ then either $a$ or $b$ is a unit. We recall that in 347 we showed that in a UFD, irreducible elements and prime elements are the same and that in general, a prime element is irreducible, but an irreducible element need not be prime (look at $\mathbb{C}[t^2, t^3]$—$t^2$ is irreducible, but it is not prime since $t^3 \cdot t^3 \in (t^2)$ but $t^3 \notin (t^2)$). 0

We recall that if we have a ring $R$ in which every element factors into irreducibles and all irreducible elements are prime then $R$ is a UFD. That is:

**Theorem 0.3.** *Let $R$ be a domain in which every element factors into irreducibles and $f \in R$ is irreducible if and only if it is prime. Then $R$ is a UFD.*

*Proof.* Suppose that we have two factorizations of an element $x$. Recall that unique factorization is always up to associates (multiplication by units), for example, $2 \cdot 3 = (-2)(-3)$ are consider the same factorization. We have $x = u\pi_1^{i_1} \cdots \pi_k^{i_k} = v\rho_1^{j_1} \cdots \rho_\ell^{j_\ell}$ with $u, v$ units and the $\pi_i, \rho_j$ prime (or irreducible, if you prefer–we are assuming these are the same) elements and the $i_s, j_s > 0$ and the $(\pi_i)$ pairwise distinct and the $(\rho_i)$ pairwise distinct. First note that $\{(\pi_1), \ldots, (\pi_k)\} = \{(\rho_1), \ldots, (\rho_\ell)\}$. To see this, notice that

$$\prod_s (\rho_s)^{j_s} = (x) \subseteq (\pi_i).$$

Since $(\pi_i)$ is a prime ideal, by the same argument as before we see that $(\pi_i) \supseteq (\rho_s)$ for some $s$. Thus $\rho_s = \pi_i a$ for some $a \in R$. Since $\rho_s$ is prime, it is irreducible and since $\pi_i$ is not a unit, $a$ must be a unit. Hence $\rho_s = \pi_i$ up to associates. Thus $(\pi_i) = (\rho_s)$ for some $s$ and so we see $\{(\pi_1), \ldots, (\pi_k)\} \subseteq \{(\rho_1), \ldots, (\rho_\ell)\}$. By symmetry, $\{(\pi_1), \ldots, (\pi_k)\} = \{(\rho_1), \ldots, (\rho_\ell)\}$. Thus $\ell = k$ and so it is enough to look at a non-unique factorization with the same primes; that is:

$$x = u\pi_1^{i_1} \cdots \pi_k^{i_k} = v\pi_1^{j_1} \cdots \pi_k^{j_k}.$$

We now show that $i_s = j_s$ for all $s$. Suppose that $i_s < j_s$ for some $s$ (the other case, is identical). Then since $R$ is a domain, we can cancel $\pi_s^{i_s}$ and we get

$$u \prod_{t \neq s} \pi_t^{i_t} = v\pi_s^{j_s - i_s} \prod_{t \neq s} \pi_t^{j_t}.$$

Thus $\pi_s$ divides

$$u \prod_{t \neq s} \pi_t^{i_t}.$$

In other words, $u \prod_{t \neq s} \pi_t^{i_t} \in (\pi_s)$. Since $(\pi_s)$ is a prime ideal and $u$ is a unit, some $\pi_t$, $t \neq s$ is in $(\pi_s)$. But this gives $\pi_t = \pi_s a$ for some $a$ and so since $\pi_t$ is irreducible, $a$ is a unit. Thus $(\pi_t) = (\pi_s)$—this contradicts pairwise distinct. □

**Corollary 0.14.** *Let $R$ be a noetherian domain. Then $R$ is a UFD if and only if all height one primes are principal.*

*Proof.* Suppose that $R$ is a UFD. Let $P$ be a height one prime. We claim that $P$ contains an irreducible. Then $P$ is nonzero and so it contains some nonzero, non-unit $f_0$. If $f_0$ is irreducible, we're done; if not $f_0 = f_1 g_1$ with $f_1, g_1$ non-units. Since $P$ is prime and $f \in P$, we see either $f_1$ or $g_1$ is in $P$; WLOG $f_1 \in P$. Then $(f_0) \subsetneq (f_1)$. Continuing in this manner, we get an

ascending chain. This chain must terminate because $R$ is noetherian, so we arrive at an element $f = f_n$ that is irreducible. Since $R$ is a UFD, $f$ is prime. Thus $(0) \subsetneq (f) \subseteq P$. Since $P$ is height one, $P = (f)$ and so $P$ is principal.

Next suppose that all height one primes are principal. We need Krull's PIT. We first show that every element of $R$ factors into irreducibles. This is the same trick using noetherian. Let $S$ be the set of all ideals of the form $(f)$ where $f$ is nonzero, non-unit and does not factor into irreducibles. If $S$ is empty, we're done; if it is non-empty, we can pick a maximal element $(g)$ of $S$. Since $(g)$ is in $S$, $g$ cannot be irreducible. Thus $g = ab$ with $a, b$ non-units. But then $(g) \subsetneq (a)$ and $(g) \subsetneq (b)$ and so by maximality, $a$ and $b$ factor into irreducibles. But this gives that $g$ does since $g = ab$.

Now we must show that irreducible elements are prime (we know already that primes are irreducibles, since this always holds). Pick $f$ irreducible. Suppose that $f$ is not prime. Then since $R$ is noetherian, there is a finite set of minimal prime ideals $P_1, \ldots, P_s$ containing $Rf$. By Krull's PIT theorem, these are all principal, say $P_i = (g_i)$. Then $P_1 = (g_1) \supset (f)$ and so $f = g_1 a$ for some $a \in R$. But $f$ is irreducible and $g_1$ is not a unit, so $a$ must be a unit. Thus $(f) = (g_1)$ and so $f$ is prime, since it generates a prime ideal. □

## Krull's principal ideal theorem

Let's prove PIT now.

Given a prime ideal $P$ of $R$, we define the $n$-th symbolic power $P^{(n)}$ of $P$ to be $P^{(n)} = (PR_P)^n \cap R$.

Easy exercise: $P^{(n)}R_P = (PR_P)^n$ and $P^{(n)}$ is $P$-primary.

Now we assume $R$ is noetherian and $f$ is a non-unit.

Proof of PIT: Let $f$ be a non-unit and suppose there is a prime $Q$ of height $\geq 2$ above $Rf$. Then we have a chain $P_0 \subsetneq P \subsetneq Q$ with $f \notin P_1$. Passing to $R/P_0$, we may assume that (0) is prime. Passing to $R_Q$, we may assume that $R$ is a local ring of Kdim $\geq 2$ such that $Q$ is the unique maximal ideal and it is minimal above $Rf$. We also assume we have a chain $(0) \subsetneq P \subsetneq Q$. Then $R/Rf$ is artinian: $R$ is artinian and $Q$ is the only prime ideal above $Rf$ and so $R/Rf$ has Kdim 0. Thus $R/Rf$ is artinian. Now let $I_t := P^{(t)} + Rf$. Then $I_t$ gives a descending chain in $R/Rf$ and so there is some $n$ such that $I_n = I_{n+1} = \cdots$. That is $P^{(n)} + Rf = P^{(n+1)} + Rf$. This means that if $a \in P^{(n)}$, there is some $b \in P^{(n+1)}$ such that $a = b + fy$. So $fy = a - b \in P^{(n)} \subseteq P$. But $f \notin P$ and so no power of $f$ is in $P^{(n)}$. Thus $y \in P^{(n)}$ since $P^{(n)}$ is primary. This means that $fy \in fP^{(n)}$ and so we see that $P^{(n)} = P^{(n+1)} + P^{(n)}f$. In other words, $M = P^{(n)}/P^{(n+1)}$ satisfies $fM = M$ and so $QM = M$. By Nakayama, $M = 0$ so $P^{(t)} = P^{(n)}$ for all $t \geq n$. But this means that

$$(PR_P)^n = P^{(n)}R_P = \cap_t P^{(t)}R_P = \cap_t (PR_P)^t.$$

In particular, $(PR_P)^{n+1} = (PR_P)^n$. But now use Nakayama to get that $(PR_P)^n = (0)$. This means $P = (0)$ since $R$ is a domain. This is a contradiction.