446/646 COURSE NOTES

BACKGROUND

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, which I assume you can look up somewhere. 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; it contains zero, it's closed under addition and under multiplication by R;
(ii) what the quotient ring R/I is for a ring R and an ideal I.
(iii) What a unit, zero divisor, idempotent, nilpotent element, integral domain, field, PID, and UFD are.
(iv) What a prime ideal is. For commutative rings $ab \in P$ if and only if $a \in P$ or $b \in P$. Also, P is prime if and only if R/P is an integral domain.
(v) What a maximal ideal is. An ideal 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 vector space 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 we can give M the structure of an R/I-module since $r \cdot m = r' \cdot m$ whenever $r - r' \in I$; thus, 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 vector space is an F-module. The annihilator of V is (0) unless $V = (0)$.
(ii) Let $R = \mathbb{Z}$ and let M be an abelian group. Then M is an R-module. $n \in \mathbb{Z}$ and $x \in M$ then $nx = x + x + \cdots + x$ if $n > 0$ and $-x + \cdots - x$ $|n|$ times if $n < 0$. If $M = \mathbb{Z}_3 \oplus \mathbb{Z}_{10}$ 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 vector space E.g., If $R = \mathbb{Z}$ and $M = \mathbb{Q}$ then M is not finitely generated.

Proof. If $\mathbb{Q} = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha_d$ then pick a common denominator for $\alpha_1, \ldots, \alpha_d \in \mathbb{Q}$, call it N. Then $\mathbb{Q} \subseteq \mathbb{Z}[1/N]$, which is impossible. □

E.g., $R = \mathbb{Z}$, $M = \mathbb{Z}_2 \times \mathbb{Z}_3$ is finitely generated. 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 it 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-vector space then f is an F-module homomorphism. Any homomorphism of abelian groups is a $\mathbb{Z}$-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 α. 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**. $R = \mathbb{Z}$ show that $\mathbb{Z} \oplus \mathbb{Z} \cdots$ is not isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots$.) 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^ω 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 vector space Since every vector space has a basis (**Exercise. Zorn!**) we see that $V = F^X$. E.g. if $R = \mathbb{Z}$ and $M = \mathbb{Z}/2\mathbb{Z}$ then M is not free. Let $R = \mathbb{Z}$ and let $M = \prod_{i=1}^\infty \mathbb{Z}$. Show that M is not free **Tricky exercise!** If M is a finitely generated free module, then we call the *rank* of R the cardinality of $|X|$, where $M \cong R^X$.

Question 0.1. *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 vector space has a basis and all bases have the same cardinality **Exercise.** In general, the rank is not well-defined if R is not commutative. E.g., x, y, x^*, y^* relations $x^*x = y^*y = 1$, $x^*y = y^*x = 0$, $xx^* + yy^* = 1$. Then $R \cong R \oplus R$. (Why? Let $\phi : R^2 \to R$ be defined by $\phi(a,b) = ax^* + by^*$. Then $\phi(rx, ry) = r$ and so ϕ is onto. Also the kernel of ϕ is zero, since $ax^* + by^* = 0$ gives that $ax^*x = 0$ and so $a = 0$. Similarly, $b = 0$. This is a homomorphism, too!) For now we will just assume this, but we'll see how to derive this from the vector space case after we do tensor products.

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 $g \circ \tau = \mathrm{id}_{M'}$.

The Splitting Lemma

Lemma 0.2. *Let*

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

be a short exact sequence with maps $f : M'' \to M$ and $g : M \to M'$. The splitting lemma says that the following are equivalent (notice condition 1 is a bit subtle, but it shows that (2) and (3) imply that M is isomorphic to a direct sum):

1. *there exists an isomorphism $\theta : M \cong M'' \oplus M'$ such that $\theta \circ f(m'') = (m'', 0)$ for every $m'' \in M''$ and $\pi_2(\theta(m)) = g(m)$ for every $m \in M$, where $\pi_2 : M'' \oplus M' \to M'$ is the natural projection onto M';*
2. *there exists $\tau : M' \to M$ with $g \circ \tau = \mathrm{id}_{M'}$;*
3. *there exists $\sigma : M \to M''$ with $\sigma \circ f = \mathrm{id}_{M''}$.*

Proof. To see the proof, notice that we showed in class that (2) implies (1) except for the extra conditions added in (1). We defined a map $k : M'' \oplus M' \to M$ via $k(m'', m') = f(m'') + \tau(m')$. Notice that if $\theta = k^{-1}$ then $\theta \circ f(m'') = (m'', 0)$ and if $\theta(m) = (m'', m')$ then $\pi_2(\theta(m)) = m'$. Since $m = f(m'') + \tau(m')$, we see that applying g gives $g(m) = m'$ as required.

Notice we also have (3) implies (1) as follows. We define $h : M \to M'' \oplus M'$ via $h(m) = (\sigma(m), g(m))$. Then it is easy to check that h is a homomorphism. Also h is 1-to-1, since $g(m) = 0$ only if m is in the image of f, which means that $m = f(x)$ and so $\sigma(m) = x$. Thus if $h(m) = 0$, we must have $\sigma(m) = x = 0$ and so $m = f(x) = 0$. To see that h is onto, notice that g is onto, so given m' there is some y such that $g(y) = m'$. Since the image of f is the kernel of g, we have $g(y + f(x)) = m'$ for all $x \in M'$. Thus it is enough to show that there is some x such that $\sigma(y + f(x)) = m''$. Notice, however, that $\sigma(f(x)) = x$

and so we can take $x = m'' - \sigma(y)$ to get $h(y + f(x)) = (m'', m')$. It is straightforward to check that $\theta = h$ has the extra properties. Since $h \circ f(m'') = (\sigma \circ f(m''), f \circ g(m'')) = (m'', 0)$ and $\pi_2(h(m)) = g(m)$.

It remains to show that (1) implies (2) and (3). This is actually easy. We take $\tau(m') = \theta^{-1}((0, m'))$. Then $g = \pi_2 \circ \theta$ and so $g \circ \tau(m') = \pi_2 \circ \theta \circ \theta^{-1}((0, m')) = m'$. We take $\sigma(m) = \pi_1(\phi(m))$. Then $\sigma \circ f(m'') = \pi_1 \circ \theta \circ f(m'') = \pi_1(m'', 0) = m''$.

We note that condition (1) is best appreciated by drawing a diagram, which is left to you. Here is what's interesting: although some books (and wikipedia) state the splitting lemma without the extra conditions, they are in fact necessary. To see this, let $R = \mathbb{Z}$ and let $M'' = \mathbb{Z}$, $M = \mathbb{Z} \oplus (\bigoplus_{i=1}^{\infty} \mathbb{Z}_2)$ and let $M' = \bigoplus_{i=1}^{\infty} \mathbb{Z}_2$. Let $f : M'' \to M$ be the map given by $f(n) = (2n, 0, 0, 0, \ldots)$ and let $g : M \to M'$ be given by $g(n, \epsilon_1, \epsilon_2, \ldots) = ([n]_2, \epsilon_1, \epsilon_2, \ldots)$. Then f is one-to-one, g is onto and the kernel of g is exactly the image of f. Notice that $M \cong M'' \oplus M'$ but there cannot exist $\sigma : M \to M''$ with $\sigma \circ f = \mathrm{id}_{M''}$. Why? Since $f(1) = (2, 0, \ldots)$ we have $\sigma(2, 0, 0, \ldots) = 1$. But what is $\sigma(1, 0, 0, \ldots)$? It has to be $1/2$, which is impossible. Similarly, we can't have $\tau : M' \to M$ with $g \circ \tau = \mathrm{id}_{M'}$. Why? Think about it! □

Structure theorem for finitely generated modules over a PID

If R is a PID and M is a finitely generated R-module then we have a nice structure theorem for finitely generated modules. Thm: Structure theorem for finitely generated 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 $I = (a) = (p_1^{j_1} \cdots p_m^{j_m})$. Use the Chinese remainder theorem! (Remark: this gives a ring isomorphism, but it is easily checked to give a module isomorphism.)

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 if we don't know that PIDs are noetherian). 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 $asm_1 + \cdots + bsm_i + \cdots = 0$. 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 $as(cm_1' + bm_i') + bs(dm_1' - am_i') + \cdots = sm_1' + \cdots +$ so this contradicts minimality. So if we let $m_1'' = m_1' + \cdots$ 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 $M = \langle m_1 \rangle \oplus N$, N is $d - 1$ generated and $\langle m_1 \rangle$ 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 universal property.

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 isomorphism) module with this universal property. Let's see why. Suppose that A and B both have the universal property for $M \times N$. Then we have bilinear maps $\phi : M \times N \to A$ and $\psi : M \times N \to B$ that give the universal property. Now using the universal property with A (and bilinear map to B) gives that there is a homomorphism $\tilde{\psi} : A \to B$ and using it with B (and bilinear map to A) gives a homomorphism $\tilde{\phi} : B \to A$. Notice that $\tilde{\psi} \circ \tilde{\phi} \circ \psi = \tilde{\psi} \circ \phi = \psi$. But using the universal property with B and bilinear map to B gives that the identity is the unique homomorphism with $\mathrm{id} \circ \psi = \psi$ and so the homomorphisms are inverses.

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

We have $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathbb{Z}_3 = 0$. Proof. F is $\mathbb{Z}^6$. $(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)$. 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.

What is $\mathbb{Z}_2 \otimes \mathbb{Z}_2$? 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 $\mathbb{Z}_2$. Well, it is $\mathbb{Z}_2$. Let $f : \mathbb{Z}_2 \otimes \mathbb{Z}_2 \to \mathbb{Z}_2$ 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.

What is $\mathbb{Z}_2 \otimes \mathbb{Z}_4$? 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 $\mathbb{Z}_2$. Define $m \otimes n = mf(n)$, where $f : \mathbb{Z}_4 \to \mathbb{Z}_2$ is the natural map. In general, $\mathbb{Z}_n \otimes \mathbb{Z}_m = \mathbb{Z}_d$, $d = gcd(m,n)$. Proof. Well, let's see that it has size at most d. We have a map $f : \mathbb{Z}_n \otimes \mathbb{Z}_m \to \mathbb{Z}_d$ 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 $\mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_d$ by $(m,n) \to g(m)h(n)$. If we have a bilinear map $h : \mathbb{Z}_m \times \mathbb{Z}_n \to P$ 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 $\mathbb{Z}_d \to P$ given by $i \to i(1,1)$. Then this works.

Properties of Tensor products

Proposition 0.3. *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 follows from the universal property since $M \times N \cong N \times M$. For associativity, notice that a bilinear map on $(M \otimes N) \otimes P \cong M \otimes (N \otimes P)$ gives a trilinear map on $M \times N \times P$. □

If $f : M \to N$ and $g : P \to Q$ then we have a bilinear map $h : M \times P \to N \otimes Q$ given by $h(m,p) = f(m) \otimes g(p)$. The universal property then gives a homomorphism $f \otimes g : M \otimes P \to N \otimes Q$ satisfying $f \otimes g(m \otimes p) = f(m) \otimes g(p)$. If $P = Q = C$ and g is the identity on C then we have a homomorphism $f \otimes id : M \otimes C \to N \otimes C$ by $f(m \otimes c) = n \otimes c$.

Right exactness

Next we'll discuss an important property, called *right exactness.*

Proposition 0.4. *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 from the above. □

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 $M = N = \mathbb{Z}$, f is multiplication by 2, and $C = \mathbb{Z}_2$? 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 $\mathbb{Z}_2$ is not flat as a $\mathbb{Z}$-module. So, a module is called *flat* if it it preserves injections under tensoring; the module C is called *faithfully flat* if it is flat and if M is nonzero then so is $M \otimes C$. What is a faithful and flat module that is not faithfully flat? How about $\mathbb{Q}$ as a $\mathbb{Z}$-module. Notice that $\mathbb{Q} \otimes \mathbb{Z}_2 = (0)$. But $\mathbb{Q}$ is certainly faithful and we can show this is flat later in the course.

Proposition 0.5. $R \otimes_R M = M$.

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. □

Proposition 0.6. *(direct sums)* $(M \oplus N) \otimes C \cong M \otimes C \oplus N \otimes C$. *Same proof works for arbitrary direct sums.*

Proof. Just use the natural maps $i : M \to M \oplus N$ and $\pi : M \oplus N \to M$, as follows. We have a bilinear map from $(M \oplus N) \times C \to M \otimes C \oplus N \otimes C$ given by $((m,n),c) \mapsto (m \otimes c, n \otimes c)$. The universal property then gives a homomorphism $h : (M \oplus N) \otimes C \cong M \otimes C \oplus N \otimes C$ that satisfies $h((m,n) \otimes c) = (m \otimes c, n \otimes c)$. Similarly, the inclusions i_M and i_N for M and N into $M \oplus N$ give a map $g : M \otimes C \oplus N \otimes C \to (M \oplus N) \otimes C$ given by $g(m \otimes c, n \otimes c) = (m,0) \otimes c + (0,n) \otimes c = (m,n) \otimes c$. Notice $h \circ g$ and $g \circ h$ agree with the identity maps on generating sets and so they are inverses.

□

What about direct products? It doesn't work in general for infinite direct products. Consider $R = \mathbb{Z}$, $C = \mathbb{Q}$, and $M_i = \mathbb{Z}/i\mathbb{Z}$ for $i = 2,3,\ldots$. Then one has $M_i \otimes C = (0)$ for all i. But $\prod M_i \otimes C$ is nonzero. Why? Use (and prove!) the following general fact. If A is an abelian group that has an element of infinite order then $A \times \mathbb{Q}$ is nonzero. (Hint: we showed that $\mathbb{Q}$ is flat (but not faithfully flat). If A is not torsion then we have an embedding $\mathbb{Z} \to A$ and flatness gives the result.) Notice that $(1,1,1,\ldots)$ has infinite order in the direct product!

Proposition 0.7. *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 $V = F \otimes_R M \cong F \otimes_R R^X \cong (F \otimes_R R)^X \cong F^X$ and $V = F^Y$. So $F^X \cong F^Y$, which means that $|X| = |Y|$. □

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 $\mathbb{Z}$-algebra, $\alpha(n) = n \cdot 1_R$. We usually suppress α 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. E.g. $\mathbb{C}$ is a $\mathbb{Q}$-algebra. Notice if S is an R-algebra then S is also an R-module.

Base change/extension of scalars

If S is an R-algebra and M is an R-module, sometimes we'd rather work with an S-module. (Think of vector space over Q v.s. vector space 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 $(s_1 + s_2)(s' \otimes m) = (s_1 s' + s_2 s') \otimes m$.

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.

Proposition 0.8. *The noetherian property is equivalent to every non-empty set of ideals having a maximal element and to every ideal being finitely generated as an ideal.*

Example 0.9. If R is a PID, then R is noetherian; $R = k[x_1, x_2, \ldots]$ 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 finitely generated and equivalent to every non-empty set of submodules having a maximal element.

Example 0.10. $R = \mathbb{Z}$, $M = \mathbb{Q}$ is not noetherian.

We note that if R noetherian then R is noetherian as an R-module.

Proposition 0.11. *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 implies that M/N noetherian. Any chain in N is also a chain in M so M noetherian implies N noetherian. Let's do the other direction now.

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?

Proposition 0.12. *Let R be a noetherian ring and let M be a finitely generated R-module. Then M is noetherian.*

Proof. M is finitely generated 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.

Pay attention to the fact that the primes contain I in the proposition below!

Proposition 0.13. *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! □

As a nice corollary notice that we get that in a noetherian ring R there are only finitely many primes that are minimal with respect to containing I.

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.

Proposition 0.14. *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 0.15. We can get this proof to work for general commutative rings using Zorn's lemma to produce a maximal element of $\mathcal{S}$.

Corollary 0.16. *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.

Proposition 0.17. *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.)

Corollary 0.18. *If R is noetherian then so is $R[x_1, \ldots, x_d]$ for $d < \infty$.*

Corollary 0.19. *If R is noetherian and S is a finitely generated R algebra then S is noetherian.*

Let's give the argument in the Hilbert basis theorem in steps we can understand. Let R be a noetherian ring. Recall that given $p(x) \in R[x]$, we let $\deg(p(x))$ denote its degree and we let $\mathrm{in}(p(x))$ denote the coefficient of the highest power of x that occurs in $p(x)$ with nonzero coefficient. So $\mathrm{in}(p(x)) \in R$.

Key steps in the argument

(i) We start with a nonzero ideal I in $R[x]$. Our goal is to show that I is finitely generated. Our first step is that we take f_1 in $I \setminus 0$ of smallest degree. We let $I_1 = f_1 R[x]$ and we let $a_1 = \mathrm{in}(f_1)$ and $J_1 = a_1 R$.

(ii) At step $n+1$, having found $f_1, \ldots, f_n$ in I and $a_1, \ldots, a_n \in R$, and ideals $I_n = f_1 R[x] + \cdots + f_n R[x]$ and $J_n = a_1 R + \cdots + a_n R$, we pick $f_{n+1} \in I \setminus I_n$ of minimal degree (if we cannot do this, we stop and we have $I = I_n$ and so I is finitely generated). We let $a_{n+1} = \mathrm{in}(f_{n+1})$ and we let $I_{n+1} = I_n + f_{n+1} R[x]$ and $J_{n+1} = J_n + a_n R$.

(iii) Since R is noetherian, there is some n such that

$$J_n = J_{n+1} = \cdots .$$

We claim that $I = I_n$.

(iv) To see this, if it is not the case then the algorithm does not terminate at the $n+1$-st step and so $f_{n+1} \in I \setminus I_n$.

(v) By minimality, we have that the degree of f_{n+1} is at least as big as the degrees of $f_1, \ldots, f_n$. Also, since $a_{n+1} = \mathrm{in}(f_{n+1}) \in J_{n+1} = J_n$, we have $a_{n+1} = r_1 a_1 + \cdots + r_n a_n$ for some $r_1, \ldots, r_n \in R$.

(vi) Let $d_i = \deg(f_i)$ for $i = 1, \ldots, n+1$. Since $\deg(f_{n+1}) \geq \deg(f_i)$ for $i \leq n$, we have

$$h := f_{n+1} - r_1 x^{d_{n+1} - d_1} f_1 - \cdots - r_n x^{d_{n+1} - d_n} f_n$$

is in I and has degree strictly less than d_{n+1}. So by minimality of $\deg(f_{n+1})$ we must have that $h \in I_n$.

(vii) Now what? if $h \in I_n$ then so is f_{n+1} since

$$f_{n+1} = h + r_1 x^{d_{n+1} - d_1} f_1 + \cdots + r_n x^{d_{n+1} - d_n} f_n$$

and every term in the RHS is in I_n. This is a contradiction!

(viii) Conclusion $I = I_n$ as claimed and so I is generated by $f_1, \ldots, f_n$. Since every ideal is finitely generated, we see that $R[x]$ is noetherian.

The Jacobson radical

The intersection of all maximal ideals is the Jacobson radical. Note that the Jacobson radical need not be nil. E.g. $R = \{a/b : b \text{ odd}\}$. What is $J(R)$? A ring is a Jacobson ring if R/P has Jacobson radical zero for every prime P. This is the same as saying that if S is a homomorphic image of R then the Jacobson radical is equal to the nil radical. (In the noetherian case, this says that the Jacobson radical of any homomorphic image is nilpotent.)

Example 0.20. $\mathbb{Z}$, a field F, $F[x]$ are all Jacobson.

Notice that the following holds:

Proposition 0.21. *$x \in J(R)$ if and only if $1 + ax$ 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.

Theorem 0.1. *(Nakayama's lemma.) Let R be a ring and let M be a finitely generated R-module. Suppose that $J(R)M = M$. Then $M = (0)$.*

Why is finitely generated needed? What if $R = \{a/b : b \text{ odd}\}$? Then $J(R) = 2R$. Take $M = \mathbb{Q}$. Then $J(R)M = M$. Notice that M not finitely generated. Why is Nakayama's lemma useful? Often one has a finitely generated module M and one wants to say it is generated by some subset $\{m_1, \ldots, m_d\}$. Of course, proving that elements generate a module is not always so easy. The way one does it in a ring with a big Jacobson radical is as follows. First, let $N = \langle m_1, \ldots, m_d \rangle$. Then if $J(R)L = L$ where $L = M/N$, then Nakayama's lemma says that $L = (0)$ and so $M = N$ and we are done. This can be checked by showing $J(R)M + N = M$, which is often not so hard when $J(R)$ is big, such as in a local ring. So for a local ring, where the Jacobson radical is maximal and $R/J(R)$ is a field, we can say that if images of $m_1, \ldots, m_d$ span $M/J(R)M$ as an $R/J(R)$-vector space, then we are done!

Proof of Nakayama's lemma. Suppose M is nonzero. Then a minimal generating set has size at least 1. Let $\{m_1, \ldots, m_d\}$ be a set of generators for M of smallest possible size. Since $J(R)M = M$, we have $m_1 = j_1 m_1 + \cdots + j_d m_d$ with the $j_i \in J(R)$. Now we rewrite this as $(1 - j_1)m_1 = j_2 m_2 + \cdots + j_d m_d$. But notice that $1 - j_1$ is a unit in R since $j_1 \in J(R)$. Thus $m_1 = (1 - j_1)^{-1} j_2 m_2 + \cdots + (1 - j_1)^{-1} j_d m_d$. But this means that we do not need m_1 in our generating set, contradicting the minimality of our choice of generating set. □

Localization

Let R be a ring. We say that a subset S of R is multiplicatively closed if $1 \in S$ and whenever $s_1, s_2 \in S$ we have $s_1 s_2 \in S$. (We can think of 1 as being the empty product and then we really just want S to be closed under all finite, possibly empty, products.) Because we don't want to deal with the zero ring in this class, we'll assume that $0 \notin S$ throughout the course.

We make a ring $S^{-1}R = R \times S/\sim = \{(r, s) \colon r \in R, s \in S\}/\sim$, which is called the *localization of R with respect to S*. Our model will be the rational numbers, where we invert the nonzero integers to obtain this ring.

Using this as our intuition, we define an equivalence relation on pairs $(r, s) \in R \times S$ Where

$$(r_1, s_1) \sim (r_2, s_2) \iff (r_1 s_2 - r_2 s_1)s_3 = 0$$

for some $s_3 \in S$. Notice that when you defined the rational numbers you didn't need this s_3. This is an extra subtlety that is added to deal with the fact that you might want to "invert" zero divisors in general.

Let's check that it is an equivalence relation. It's clearly reflexive and symmetric, so let's check transitivity. Suppose that $(r_1, s_1) \sim (r_2, s_2)$ and $(r_2, s_2) \sim (r_3, s_3)$. Then there are $s, s' \in S$ such that $(r_1 s_2 - r_2 s_1)s = 0$ and $(r_2 s_3 - r_3 s_2)s' = 0$. Thus

$$0 = s_3 s'(r_1 s_2 - r_2 s_1)s - s_1 s(r_2 s_3 - r_3 s_2)s' = (r_1 s_3 - r_3 s_1)s' s.$$

Since $ss' \in S$ we see that $(r_1, s_1) \sim (r_3, s_3)$. We can then give $S^{-1}R$ a ring structure. Rather than write $[(r, s)]$ for the equivalence class of $(r, s) \in R \times S$, we instead simply write $s^{-1}r$, much as we do with the rational numbers.

We can then define addition and multiplication as follows:

$$s_1^{-1} r_1 \cdot s_2^{-1} r_2 = (s_1 s_2)^{-1}(r_1 r_2)$$

and

$$s_1^{-1} r_1 + s_2^{-1} r_2 = (s_1 s_2)^{-1}(r_1 s_2 + r_2 s_1).$$

As always, one should check these are well-defined, because we are using equivalence class representatives and once can check the ring axioms, if one likes. If you have done this for the construction of the rationals, the same arguments go through here.

There is one additional subtlety. We know that $\mathbb{Z}$ is a subring of $\mathbb{Q}$. In general, however, R need not embed, as a ring, into $S^{-1}R$.

For example, let $R = \mathbb{Z}\times\mathbb{Z}$, $S = \{\mathbb{Z}\backslash(0)\}\times 0)$. Then S does not contain zero. Let's look at equivalence. For $(a,b),(c,d) \in R$ and $(s,0),(s',0) \in S$ we have

$$((a,b),(s,0)) \sim ((c,d),(s',0))$$

if and only if $(a,b)(s',0)(t,0) = (c,d)(s,0)(t,0)$ for some $(t,0) \in S$. This holds if and only if $as' = bs$. Thus $S^{-1}R = \mathbb{Q}$, with isomorphism given by $(s,0)^{-1}(a,b) \mapsto s^{-1}a$. If S consists of regular elements (non-zero divisors) then it is straightforward to see that the map $R \to S^{-1}R$ given by $r \mapsto 1^{-1}r$ is an embedding: if $1^{-1}r = 1^{-1}r'$ then we have $s(r-r') = 0$ for some $s \in S$. But s is a non-zero divisor and so $r = r'$. We'll mostly focus on this case in the course.

We note that if I is an ideal of R and S is a multiplicatively closed subset of R then we can make an ideal $S^{-1}I := \{s^{-1}r\colon r \in I\}$ of $S^{-1}R$.

Universal property of localization

Let S be a multiplicatively closed set of non-zero divisors of R. Then localization has the following universal property.

Proposition 0.22. *(Universal property of localization) If R is a ring and S is a multiplicatively closed subset of R not containing any zero divisors. Then if T is a ring and $\phi : R \to T$ is a ring homomorphism such that $\phi(S) \subseteq T^*$, the units of T, then ϕ extends to a homomorphism from $S^{-1}R$ to T, and moreover this extension is unique and if ϕ is one-to-one then the unique extension is one-to-one as well.*

Proof. Define a map $\psi : S^{-1}R \to T$ via the rule $\psi(s^{-1}r) = \phi(s)^{-1}\phi(r)$. Observe that since $\phi(s)$ is a unit in T, we can invert $\phi(s)$. We note that since there may be multiple ways to express a fraction in $S^{-1}R$, we must check that this map is well-defined. Let us suppose then that $s_1^{-1}r_1 = s_2^{-1}r_2$ with $r_1, r_2 \in R$ and $s_1, s_2 \in S$. Then by the definition we have that there is some $s_3 \in S$ such that $s_3(s_1r_2 - s_2r_1) = 0$ (we don't really need s_3 in this case, because we are using non-zero divisors in S). Now apply the homomorphism ϕ to obtain

$$\phi(s_3)(\phi(s_1)\phi(r_2) - \phi(s_2)\phi(r_1)) = 0.$$

Since $\phi(s_3)$ is a unit, we then have $\phi(s_1)\phi(r_2)-\phi(s_2)\phi(r_1) = 0$. Multiplying by $\phi(s_1)^{-1}\phi(s_2)^{-1}$ we now see that $\phi(s_1)^{-1}\phi(r_1) = \phi(s_2)^{-1}\phi(r_2)$, and so the map ψ is well-defined. Once we have that it is well-defined, we immediately see that its restriction to R is equal to ϕ, since $\psi(r) = \psi(s^{-1}(sr)) = \phi(r)$.

We now claim that ψ is a homomorphism from $S^{-1}R$ to T. To see this, we just check that

$$\psi(s_1^{-1}r_1 \cdot s_2^{-1}r_2) = \psi((s_1s_2)^{-1}(r_1r_2)) = \phi(s_1)^{-1}\phi(r_1) \cdot \phi(s_2)^{-1}\phi(r_2).$$

Also,

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

We note that ψ is also the unique extension of ϕ to a homomorphism, because if f is an extension of ϕ then we must have $\phi(1) = f(1) = f(s^{-1}s) = f(s^{-1})\phi(s)$, so $f(s^{-1}) = \phi(s)^{-1}$ and so $f(s^{-1}r) = \psi(s^{-1}r)$.

As before, uniqueness gives that localization is the unique—up to isomorphism—ring with this property. If B_1 and B_2 both have this property (for a fixed set S) then if we take $T = B_2$ and $\phi : R \to B_2$ to be the inclusion map $r \mapsto 1^{-1}r$, we see that we get a map from B_1 to B_2 and similarly we get a map from B_2 to B_1. Now the composition of these maps must be the identity by the universal property: if we work with B_1 and take $T = B_1$ we see that there is only one extension of the inclusion map to B_1 and it is the identity map.

Finally, suppose that ϕ is one-to-one. We claim that the extension ψ is also one-to-one. To see this, suppose that $s^{-1}r$ is in the kernel of ψ. Then $\phi(s)^{-1}\phi(r) = 0 \implies \phi(r) = 0$ since $\phi(s)$ is a unit. But since ϕ is one-to-one this gives that $r = 0$ and so the kernel of ψ is trivial. □

Example 0.23. If f is non-nilpotent and $S = \{1, f, f^2, \ldots\}$ then we define $R_f := S^{-1}R$. Let P be a prime ideal and let $S = R \setminus P$ be its complement in R. Then we have that S is multiplicatively closed, contains 1, and has no zero divisors. We define $R_P := S^{-1}R$.

We notice that R_P has an ideal $PR_P := \{s^{-1}r : s \notin P, r \in P\}$. Let's show that PR_P is a prime ideal of R_P. Let $\mathrm{Frac}(R/P)$ denote the field of fractions of R/P. We construct a homomorphism $\phi : R \to T := \mathrm{Frac}(R/P)$ via the rule $\phi(r) = (r + P)$. Notice that if $s \in S = R \setminus P$, then $\phi(s) \neq 0$ and so it is sent to a unit of T. By the universal property ϕ extends uniquely to a homomorphism $\psi : S^{-1}R \to T = \mathrm{Frac}(R/P)$. Then it is straightforward to see that ψ is onto since if $x = (b+P)^{-1}(a+P)$ is in T then $b \in S$ and so $\psi(b^{-1}a) = x$. Then the kernel of ψ is a maximal ideal since the image is a field. The kernel is precisely the elements of the form $s^{-1}r$ with $s \in S$ and $r \in P$. Thus PR_P is a maximal ideal. We'll show that it is in fact the *only* maximal ideal in R_P.

We recall that a ring R is a *local ring* if it has a unique maximal ideal. Notice that a field is a local ring, but $\mathbb{Z}$ is not. There is a nice criterion to show that a ring R with maximal ideal M is a local ring. You simply show that $1 + x$ is a unit for every $x \in M$. To see this, suppose that there is some maximal ideal $Q \neq M$. Then $Q + M = R$, since M and Q are both maximal and are not equal. Now pick $q \in Q$ and $x \in M$ such that $q + x = 1$. By assumption $1 + (-x)$ is a unit, since $-x \in M$. Thus $q = 1 - x$ is a unit, which is a contradiction since it is contained in a proper ideal.

Proposition 0.24. *Let R be a ring and let P be a prime ideal of R. Then the ring R_P is a local ring whose unique maximal ideal is the ideal PR_P.*

Proof. It suffices to show that if $x \in PR_P$ then $1+x$ is a unit in R_P. To see this, notice that $1+x \notin PR_P$ since if $x, 1+x \in PR_P$ then we would have $1 \in PR_P$. Thus $1+x = s^{-1}a$ for some $s \in S$ and $a \notin P$; i.e., $a \in S$. But then $a^{-1}s \in R_P$, too, and so $1+x$ has an inverse in R_P. □

Let R be a ring and let S be a multiplicatively closed set of regular elements (non-zero divisors) of R. We say that an ideal J of R is *S-saturated* if whenever $s \in S$ and $x \in R$ has the property that $sx \in J$, we then have $x \in J$. The structure of the poset of ideals in $S^{-1}R$ can be understood in terms of the saturated ideals of R.

Theorem 0.2. *Let R be a ring and let S be a multiplicatively closed set of regular elements. Then we have an inclusion-preserving bijection between the poset of proper ideals of $S^{-1}R$ and the poset of S-saturated ideals of R that intersect S. In one direction, this is given by $I \leq S^{-1}R \mapsto f(I) := I \cap R$; in the other direction, we take $J \leq R \mapsto g(J) := S^{-1}J$.*

Proof. We first show that if I is an ideal of $S^{-1}R$ then $g \circ f(I) = S^{-1}(I \cap R) = I$. To see this, observe that if $x \in I$ then $x = s^{-1}a$ for some $s \in S$ and some $a \in R$. So $a = sx \in I \cap R$. Then $x = s^{-1}a \in S^{-1}(I \cap R)$. Thus $I \subseteq g \circ f(I)$. Conversely, if $x \in g \circ f(I)$ then $x = s^{-1}a$ for some $s \in S$ and some $a \in I \cap R$. but then $a \in I$ so $x \in I$.

In the other direction, If J is a saturated ideal of R then we can show that $S^{-1}J \cap R = J$. To see this, observe that if $x = s^{-1}j \in S^{-1}J \cap R$ with $s \in S$ and $j \in J$ then $sx \in J$ and since J is saturated and $x \in R$ we see that $x \in J$. To get the other containment, observe that $S^{-1}J \supseteq J$ and so $S^{-1}J \cap R \supseteq J$.

Now let's put it together. Notice that if I is an ideal of $S^{-1}R$ then $f(I) = I \cap R$ is an S-saturated ideal of R since if $sx \in I \cap R$ with $s \in S$ and $x \in R$ then $x = s^{-1}sx \in I$ and since $x \in R$ it is also in $I \cap R$. Thus f gives a map from the ideals of $S^{-1}R$ to the S-saturated ideals of R. If we look at the map g on the S-saturated ideals of R then we have shown that $g \circ f$ and $f \circ g$ are both the identity maps on their respective domains. Furthermore, it is straightforward to see that f and g are inclusion preserving. The result follows. □

Corollary 0.25. *Let R be a noetherian ring and let S be a multiplicatively closed set of regular elements. Then $S^{-1}R$ is noetherian.*

Proof. Using the bijection described in Theorem 0.2, we see that an ascending chain of ideals in $S^{-1}R$ corresponds (via the map f) to an ascending chain of S-saturated ideals in R. Since the chain of ideals we produce in R must terminate, the original chain of ideals in $S^{-1}R$ must terminate too. The result follows. □

Notice that if S is a multiplicatively closed set consisting of regular elements and P is a prime ideal of R with $P \cap S = \emptyset$ then P is automatically S-saturated. To see this, notice that if $x \in R$ and $s \in S$ and $sx \in P$ then we must have $s \in P$ or $x \in P$, but by assumption $s \notin P$ and so P is indeed S-saturated. We claim that this bijection restricts to a bijection on prime ideals which we can describe as follows

$$\{\text{prime ideals of } S^{-1}R\} \longleftrightarrow \{\text{prime ideals of } R \text{ with } P \cap S = \emptyset\}.$$

To see this, let P be a prime ideal of $S^{-1}R$. Then since S consists of regular elements we have that the map $r \mapsto 1^{-1}r \in S^{-1}R$ is an embedding. Then if ϕ is the composition of the embedding $R \to S^{-1}R$ and the canonical surjection $S^{-1}R \to S^{-1}R/P$ then the kernel of ϕ is $P \cap R = f(P)$. Then $f(P)$ is prime since $R/f(P)$ is isomorphic to the image of ϕ and ϕ maps into an integral domain. Similarly, if I is not a prime ideal then $f(I)$ is not prime since if $ab \in I$ and $a, b \notin I$ then we can "clear denominators" and assume without loss of generality that $a, b \in R$. Then $ab \in f(I)$ and $a, b \notin f(I)$.

We also have that $f(P) \cap S = \emptyset$, since if this were not the case then there would be some $s \in S \cap P$ and so $1 = s^{-1}s \in P$, too, a contradiction. Now if Q is a prime of R with $P \cap S = \emptyset$ then we saw that Q is S-saturated and $f(g(Q)) = Q$. Thus Q is in the image of f and we saw that $g(Q)$ must be prime since $f(g(Q))$ is prime. Thus we have this bijection.

Let's look at a few special cases.

Example 0.26. Let R be a ring, let f be a non-zero divisor and let $S = \{1, f, f^2, \ldots\}$. Then the prime ideals in $S^{-1}R$ correspond to prime ideals of R that do not contain f. In the ring R_P, we are taking $S = R \setminus P$. Then the primes in R_P correspond to primes Q of R such that $Q \cap \emptyset$. This is the same assaying that $Q \subseteq P$. Thus the primes of R_P are in bijection with the prime ideals that are contained in P—this again shows that R_P is local.

Compare this last example with the correspondence theorem: the prime ideals of R_P correspond bijectively to the prime ideals of R that are contained in P; the prime ideals of R/P correspond bijectively to the prime ideals that contain P.

Remark 0.27. 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 $(S \otimes T)^{-1}(A \otimes_R B) \cong S^{-1}A \otimes S^{-1}B$.

Proof. To see this, use the universal property of localization (we already used the universal property of tensors to get homomorphisms of this type in Assignment 2). We have an injective homomorphism $f \otimes g : A \otimes_R B \to S^{-1}A \otimes T^{-1}B$, where $f : A \to S^{-1}A$ and $g : B \to T^{-1}B$ are the canonical injections given by $a \mapsto 1^{-1}a$ and $b \mapsto 1^{-1}b$. There's an important question here: Why is $f \otimes g$ 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 $\mathbb{Z}_2 \otimes \mathbb{Z}_2 \mapsto \mathbb{Z}_4 \otimes \mathbb{Z}_4$ with the map being $a \otimes b \mapsto 2a \otimes 2b$. Then $1 \otimes 1 \mapsto 2 \otimes 2 = 4 \otimes 1 = 0$. When we take the tensor product over a field, however, it is fine. We can pick bases for A and B over F, say $\{a_\alpha\}$ and $\{b_\beta\}$

respectively. Then since A and B are free F-modules (well, they're vector spaces), we see that $\{a_\alpha \otimes b_\beta\}$ forms a basis for $A \otimes_F B$. Now if $f \otimes g$ is not injective then there is some finite F-linear combination

$$\sum c_{\alpha,\beta} a_\alpha \otimes b_\beta$$

that is in the kernel of $f \otimes g$. But $f \otimes g$ sends this to the element

$$\sum c_{\alpha,\beta} 1^{-1} a_\alpha \otimes 1^{-1} b_\beta.$$

Since A injects into $S^{-1}A$, $\{1^{-1}a_\alpha\}$ is linearly independent over F; similarly, $\{1^{-1}b_\beta\}$ is linearly independent over F and so the set $\{1^{-1}a_\alpha \otimes 1^{-1}b_\beta\}$ is linearly independent over F by the assignment. This gives injectivity.

Moreover the elements of $S \otimes T$ get sent to units so by the universal property of localization, $f \otimes g$ extends to an injective homomorphism $(S \otimes T)^{-1}(A \otimes_R B) \to S^{-1}A \otimes S^{-1}B$. The map is easily seen to be onto since $s^{-1}a \otimes t^{-1}b$ generate $S^{-1}A \otimes S^{-1}B$ and they are in the image of $f \otimes g$. □

Corollary 0.28. *Let F be a field and let K be a finitely generated extension of F. Then $K \otimes_F K$ is noetherian. In particular, every subfield of K that contains F is finitely generated by the assignment.*

Proof. We have $K = \mathrm{Frac}(A)$, the field of fractions of A, where A is a finitely generated F-algebra that is an integral domain. By the second assignment $A \otimes_F A$ is finitely generated as an F-algebra and so it is also noetherian by the Hilbert Basis Theorem. 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 of $A \otimes_K A$. □

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.

Theorem 0.3. *(Nullstelensatz) Let R be a Jacobson ring and let S be a finitely generated 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 α need not be injective, but we may assume that it is—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 0.29. *If $S = \mathbb{C}[t_1, \ldots, t_m]$ then S/M is $\mathbb{C}$ so every maximal ideal is of the form $(t_1 - \alpha_1, \ldots, t_m - \alpha_m)$.*

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

We recall that a ring R has an ideal, $J(R)$, called the *Jacobson radical*. It is the intersection of all maximal ideals. A ring is a *Jacobson ring* if $J(R/P) = (0)$ for every prime ideal P of R. We've already seen some examples of Jacobson rings: $\mathbb{Z}$, $k[x]$, k a field (why? think about it!). We note that if R is Jacobson then the correspondence theorem immediately gives that R/I is Jacobson for every proper ideal I of R.

We will prove a very general version of the Nullstellensatz. Before we do this, recall that if R is a ring, then S is an *R-algebra* if S is a ring and there is a ring homomorphism $\alpha : R \to S$ sending 1_R to 1_S. In general, α need not be injective (for fields it is, however). Thus $\alpha(R)$, the image of R under α is in general a homomorphic image of R; i.e., it is isomorphic to $R/\mathrm{Ker}(\alpha)$. Nevertheless, when we speak of R we will mean $\alpha(R)$, even though it is not necessarily isomorphic to R. This will not create any problems, since we will be concerned with maximal ideals of $\alpha(R)$ and by the correspondence theorem maximal ideals of $\alpha(R)$ correspond to maximal ideals of R that contain the kernel of α. Thus we will assume without loss of generality that α is injective and we will identify R with $\alpha(R) \subseteq S$.

Theorem: (General form of Nullstellensatz) Let R be a Jacobson ring and let S be a finitely generated R-algebra. Then S is a Jacobson ring and if M is a maximal ideal of S then $N := M \cap R$ is a maximal ideal of R and S/M is a finite field extension of R/N.

Before we continue, we note that $R \subseteq S$ and if we look at the composition of the injection $R \to S$ with the surjection $S \to S/M$, then N is in the kernel of this and so we get an injective map from R/N into S/M. Thus we can regard R/N as a subfield of S/M.

The Rabinowitch trick

The Rabinowitch trick is often stated in forms that make it look like more of a trick. We use the following version from Eisenbud, which simply gives a reformulation of the Jacobson property.

Theorem: Let R be a ring. Then R is a Jacobson ring if and only if whenever P is a prime ideal of R and $T := R/P$ has the property that T_b is a field for some nonzero $b \in T$ then T is a field.

Proof. Suppose first that R is Jacobson and P is a prime ideal of R. Let $T = R/P$ and suppose that T_b is a field. Since the prime ideals of T_b are in bijective correspondence with the prime ideals of T that do not contain b, we see that every nonzero prime ideal of T contains b. It follows that if T is not a field then every maximal ideal of T contains b and so the Jacobson radical of T contains b; a contradiction, since $J(T) = (0)$, since R is Jacobson.

Suppose next that whenever P is a prime ideal of R and $T := R/P$ has the property that T_b is a field for some nonzero $b \in T$ then T is a field. Let P be a prime ideal of R. We claim that $S := R/P$ has zero Jacobson radical. To see this, suppose not. Then there is some nonzero $b \in S$ such that every maximal ideal contains b. Then there is a bijection between prime ideals of S_b and prime ideals of S that do not contain b. Let Q' be a maximal ideal of S_b. Then there is a prime ideal Q of S that does not contain b with $QS_b = Q'$. Let $T = S/Q$. By construction, every nonzero prime ideal of T contains the image of b in T. Thus T_b has only the zero prime ideal and hence it is a field. It follows that T is a field. But this is a contradiction since every maximal ideal of S is a nonzero maximal ideal of T that contains b. □

Strategy of proof of Nullstellensatz

The main steps are as follows.

(i) Show that the Nullstellensatz holds when $S = R[x]$;
(ii) Use induction to show that it holds for $S = R[x_1, \ldots, x_n]$;
(iii) Show that the Nullstellensatz holds for homomorphic images of $R[x_1, \ldots, x_n]$.

Every finitely generated R-algebra is isomorphic to an algebra of the form $R[x_1, \ldots, x_n]/I$ for some ideal I (a homomorphic image) and so we get the result from (1)–(3).

We observe that (1) is the only difficult step. Let's see this now.

Proof of (2) and (3) from (1). (2): Suppose that the Nullstellensatz holds for $S = R[x_1, \ldots, x_d]$ with $d < n$. Let $T = R[x_1, \ldots, x_{n-1}]$. Then by the inductive hypothesis T is Jacobson. Thus $S = R[x_1, \ldots, x_n] = T[x_n]$ is Jacobson by applying step (1) using $R = T$ (which is Jacobson). Thus if M is a maximal ideal of S then $N := M \cap T$ is a maximal ideal of T and S/M is a finite extension of T/N. But by the inductive hypothesis, $N' := N \cap R$ is a maximal ideal of R and T/N is a finite extension of R/N' and hence S/M is a finite extension of T/N.

(3): If $S = R[x_1, \ldots, x_n]/I$ then by (2) and the remarks we made at the beginning S is Jacobson. We may assume that $I \cap R = (0)$ or else we would work with $R/(I \cap R)$ instead at the beginning. If M is a maximal ideal of S then M corresponds to a maximal ideal M' of $R[x_1, \ldots, x_n]$ that contains I. Then $N := M \cap R = M' \cap R$ and by (2), N is a maximal ideal of R and $S/M \cong R[x_1, \ldots, x_n]/M'$ is a finite extension of R/N. The result follows. □

To prove (1), there are two parts: We must show that if R is Jacobson then $R[x]$ is Jacobson. We must then show that if M is a maximal ideal of $R[x]$ then $M \cap R$ is a maximal ideal of R and $R[x]/M$ is a finite extension of $R/(R \cap M)$. So we do these now. We show that R Jacobson $\implies$ $R[x]$ Jacobson. This is the hardest part and we will notice that if we pay attention to the proof, that the second part falls out for free. There is one extra ingredient that we need that will appear on the third assignment. For now we will call it the black box.

Black box: If $R \subseteq S$ are rings and S is a finite R-module then if S is a field then R is a field.

For now we will assume this and we will come back to this at the end. Now let's do step (1)—this is the trickiest part of the argument.

Step (1) of Nullstellensatz. By the Rabinowitch trick it is enough to show that if $T = R[x]/P$ has the property that T_b is a field then T is a field. We let $R' = R/(P \cap R)$. Then R' is Jacobson since R is Jacobson and R' can be regarded as a subring of T and we may regard $T = R'[x]/Q$ where Q is a prime ideal of $R'[x]$ with $Q \cap R' = (0)$. We first note that Q is not the zero ideal: if it were, we would have $T = R'[x]$ and so T would be a subring of $K[x]$, where K is the field of fractions of $R'[x]$. But then $T_b = R'[x]_b$ would be a subring of $K[x]_b$. Since T_b is a field and it contains K, we see that $R'[x]_b = K[x]_b$ and so $K[x]_b$ is a field. But $K[x]$ is a Jacobson ring (polynomial ring in one variable over a field, which we know is a Jacobson ring) and it is not a field and so $K[x]_b$ cannot be a field by the Rabinowitch trick. Thus Q is nonzero.

Since $(R'[x]/Q)_b$ is a field and $Q \cap R'$ is zero, it contains K. Thus we see that $T_b = (K[x]/QK[x])_b$. Notice that $K[x]/QK[x]$ is a finite extension of K since it is a nonzero prime ideal and hence it is a finite field extension of K. Thus T_b is a finite extension of K. We will show that R' must be equal to K and so $T = K[x]/Q$ with Q nonzero and so T is a field!

Let $f(x) = a_n x^n + \cdots + a_0$ be an element of Q with $a_0, \ldots, a_n \in R'$ and a_n not equal to zero. Then notice that we have $x^n + (a_{n-1}/a_n)x^{n-1} + \cdots + (a_0/a_n) = 0 \bmod Q' := QR'[x]_{a_n}$. Thus the image of x in$T_{a_n} = R'_{a_n}[x]/Q'$ satisfies a monic polynomial. It follows that T_{a_n} is a finite R'_{a_n}-module (with spanning set given by the images of $1, x, x^2, \ldots, x^{n-1}$). Now if T_b is a field then certainly $T_{a_n b}$ is a field, since inverting $a_n b$ is the same as inverting both a_n and b. Now since T_{a_n} is a finite R'_{a_n}-module, it follows that there is a non-trivial relation (why? think about it!)

$$c_m b^m + \cdots + c_0 = 0$$

with $c_0, \ldots, c_m \in R'_{a_n}$. By clearing denominators, we can assume that the c_i are all in R. Since T is an integral domain, we may divide by a power of b if necessary to assume that $c_0 c_m \neq 0$. Then consider the localization $T_{a_n c_0}$. This is a finite $R'_{a_n c_0}$-module (think about it!). Also, we notice that b is invertible in $T_{a_n c_0}$ since we have

$$c_m b^m + \cdots + c_0 = 0 \implies 1 = b(-c_1/c_0 + \cdots - c_m/c_0 b^{m-1})$$

and so b h as an inverse in $T_{a_n c_0}$. Thus $T_{a_n c_0}$ contains T_b. Since it sits between T_b and the field of fractions of T and T_b is a field, we see that $T_{a_n c_0}$ is a field. Also $T_{a_n c_0}$ is a finite $R'_{a_n c_0}$-module. It follows from the black box that $R'_{a_n c_0}$ is also a field. Since R' is Jacobson, the Rabinowitch trick gives that R' is a field and so $T = R'[x]/Q = K[x]/Q$ is a field since Q is a nonzero prime ideal.

For the remaining part, above we showed that if $T = R[x]/Q$ is a field then $R' = R/Q \cap R$ is a field. Thus $P := Q \cap R$ is a maximal ideal of R. We also showed that $T \cong R'[x]/Q'$ with Q' a nonzero ideal and so T is a finite extension of R'. Thus we get the second part for free from the first part. □

This just leaves the black box, and you will see this on the assignment.

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.

Example 0.30. $\mathbb{Q}$ is not an integral extension of $\mathbb{Z}$. $\mathbb{Z}[\sqrt{2}]$ is an integral extension of $\mathbb{Z}$.

Remark 0.31. 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 0.4. *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:

Proposition 0.32. *TFAE: $x \in S$ is integral over R*
there is a finitely generated 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 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 finitely generated R-module that works. □

The integral closure of an integral domain R is the integral closure relative to the field of fractions of R.

Example 0.33. What is the integral closure of $\mathbb{C}[t^2, t^3]$?

If R is equal to its integral closure we say it is *integrally closed* or we say it is a *normal* domain.

Theorem 0.5. *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. □

Lying over and going up

Theorem 0.6. *If $R \subseteq S$ is an integral extension, if $P \in \operatorname{Spec}(R)$ then there is $Q \in \operatorname{Spec}(S)$ with $Q \cap R = P$. Moreover, we may find $Q \supseteq Q_1$ whenever $Q_1 \in \operatorname{Spec}(S)$ 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 $r_0 \neq 0$.

Krull dimension

Given a ring R, we let $\mathrm{Kdim}(R)$ denote the supremum over lengths of ascending chains of prime ideals of R (starting the count from 0).

Example 0.34. $\mathrm{Kdim}(F) = 0$, $\mathrm{Kdim}(F[x]) = 1$, $\mathrm{Kdim}(\mathbb{C}[x, y]) = 2$.

Theorem 0.7. *If $R \subseteq S$ is an integral extension then* $\mathrm{Kdim}(S) = \mathrm{Kdim}(R)$*.*

For now we will restrict to noetherian rings.

A noetherian ring R has Krull dimension zero if and only if R/N is a finite product of fields, where N is the nil radical of R. A ring R has Krull dimension 1 if every non minimal prime is maximal. A *Dedekind domain* is a normal noetherian domain of Krull dim 1.

Krull dimension of polynomial rings

Lemma 0.35. *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 Krull dimension 1. So we get the upper bound. The lower bound is easy. □

Noether normalization

Let R be a finitely generated k-algebra and then there is a polynomial subalgebra S in $d = \mathrm{Kdim}(R)$ variables with R a finite S-module.

Proof. (Induction on number of generators.) Suppose that R is generated by one element, say $R = k[a]$. If a is algebraic over k then we take $S = k$; otherwise, we take $S = R \cong k[x]$.

Assume true for $< m$ generators. Suppose $R = k[a_1, \ldots, a_m]$. If $a_1, \ldots, a_m$ are algebraically independent, then R is a polynomial ring in m variables and we take $S = R$ and we are done. If not, there is some nonzero polynomial relation $P(a_1, \ldots, a_m) = 0$. Exercise: There is a substitution $a_i = u_i + u_m^{A_i}$ for $i < m$ and $a_m = u_m$. Such that

$$P(u_1 + u_m^{A_1}, ..., u_m) = u_m^D + \text{stuff of lower degree in } u_m$$

Then $R = k[u_1, \ldots, u_m]$. Then R is a finite T-module, where $T = k[u_1, \ldots, u_{m-1}]$. By the inductive hypothesis, T is integral over S, a polynomial subring in d variables. Since R is finite over T and T is finite over S, R is finite over S. The result follows. □

We've just shown that if A is a finitely generated k-algebra then A is a finite free module over a polynomial ring $B = k[y_1, \ldots, y_d]$. Moreover, A is integral over B so $\mathrm{Kdim}(A) = \mathrm{Kdim}(B)$. We'll show that $\mathrm{Kdim}(B) = d$—we'll use an indirect proof. This gives a strengthened version of Noether normalization theorem: A is a finitely generated module over a polynomial ring in $d = \mathrm{Kdim}(A)$ variables. Right now all we know, however, is that $\mathrm{Kdim}(K[x_1, \ldots, x_d[) \geq d$ by using the polynomial extension estimates for Krull dimension.

Combinatorial Krull dimension

Let A be a finitely generated k-algebra. Given a k-subspace V of A, we say V is a *frame* for A if V is finite-dimensional, V generates A as a k-algebra and $1 \in V$. Then given two subspaces V and W of A we define VW to be the span of all products of vw with $v \in V$ and $w \in W$. If V and W are finite-dimensional then so is VW as it is spanned by products of basis elements. Since A is associative we see that if V, W, U are subspaces then $(VW)U = V(WU)$ and so we can speak unambiguously about VWU.

If V is a frame then we have

$$V \subseteq V^2 \subseteq \cdots \subseteq \bigcup_n V^n = A.$$

We define the dimension function $d_V(n) = \dim(V^n)$. We then define the combinatorial Krull dimension (Gelfand-Kirillov dimension) to be

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

Notice that $\mathrm{GKdim}(A)$ is independent of choice of generating space V. To see this observe that if V and W are two frames for A, then we have $V \subseteq W^p$ and $W \subseteq V^q$ for some $p, q \geq 1$. Thus $V^n \subseteq W^{pn}$ and so

$$\limsup_n \log(\dim(V^n))/\log n \leq \limsup_n \log(\dim(W^{pn}))/\log n = \limsup_n \log(\dim(W^{pn}))/\log(pn) \leq \limsup_n \log(\dim(W^n))/\log n.$$

Similarly,

$$\limsup_n \log(\dim(W^n))/\log n \leq \limsup_n \log(\dim(V^n))/\log n.$$

So we see that we get the same result regardless of choice of frame.

Remark 0.36. If V is a frame for A and $\dim(V^n) \sim Cn^d$ for some $C > 0$ and some $d \geq 0$ then $\mathrm{GKdim}(A) = d$.

Remark 0.37. $\mathrm{GKdim}(k[x_1, \ldots, x_d]) = d$.

Proof. Let $V = k + kx_1 + \cdots + kx_d$. Then V is a frame for $k[x_1, \ldots, x_d]$ and V^n has a basis consisting of monomials $\{x_1^{i_1} \cdots x_d^{i_d}\}$ with $i_1 + \cdots + i_d \leq n$. Notice there is a bijection between this set and all ways of placing d copies of the letter x into $n + d$ slots. We describe the bijection briefly. Given $x_1^{i_1} \cdots x_d^{i_d}$, we put an x in the $i_1 + 1$, $i_1 + i_2 + 2, \ldots, i_1 + \cdots + i_d + d$ slots. This is clearly reversible and so we see that V^n has dimension $\binom{n+d}{d} \sim n^d/d$. Thus $\mathrm{GKdim}(k[x_1, \ldots, x_d]) = d$. □

Lemma 0.38. *Suppose that A is a finitely generated k-algebra and B is a finitely generated k-subalgebra of A. If A is a finitely generated B-module then* $\mathrm{GKdim}(A) = \mathrm{GKdim}(B)$.

Proof. **Exercise on Assignment 4.** □

Corollary 0.39. *If A is a finitely generated k-algebra then the Gelfand-Kirillov dimension of A is a nonnegative integer.*

Proof. By Noether normalization, there is some subalgebra B of A such that $B \cong k[x_1, \ldots, x_d]$ for some d and such that A is a finitely generated B-module. Since A is a finitely generated B-module, they have the same GK dimension, which we saw was equal to d for a polynomial ring in d variables. □

Corollary 0.40. *If A is a finitely generated k-algebra then* $\mathrm{GKdim}(A) = \mathrm{Kdim}(A)$.

Proof. We'll prove this by induction on $\mathrm{Kdim}(A)$. We first remark that we have $\mathrm{Kdim}(A) \geq \mathrm{GKdim}(A)$. To see this, observe that by Noether normalization, there is some subalgebra B of A such that $B \cong k[x_1, \ldots, x_d]$ for some d and such that A is a finitely generated B-module. Since A is a finitely generated B-module, B is integral over A. It follows that A and B have the same Krull dimension. Since A is a finitely generated B-module, we also have that they have the same GK dimension, which we saw was equal to d. Since we have shown that a polynomial ring in d variables has Krull dimension at least d, we get the inequality stated above. We have now shown that it suffices to prove the equality in the case of a polynomial ring. Suppose that the claim does not hold. Then pick the smallest $d \geq 0$ for which $\mathrm{Kdim}(k[x_1, \ldots, x_d]) > \mathrm{GKdim}(k[x_1, \ldots, x_d]) = d$. Then $d > 1$, since we have shown the equality holds in the cases when $d = 0$ or $d = 1$.

Then by assumption there is some chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_{d+1}$ in $k[x_1, \ldots, x_d]$. Then $\mathrm{Kdim}(A/P_1) \geq d$ by correspondence. We now use the following claim.

Lemma 0.41. *If A is an integral domain and I is nonzero then* $\mathrm{GKdim}(A/I) \leq \mathrm{GKdim}(A) - 1$.

Let's first see how this claim finishes this for us. $\mathrm{GKdim}(A/P_1) \leq \mathrm{GKdim}(A) - 1 = d - 1 < d \leq \mathrm{Kdim}(A/P_1)$. By Noether normalization, there is some polynomial ring in e variables with $e < d$ such that A/P_1 is integral over a polynomial subring in e variables. Moreover, the Krull dimension of A/P_1 is equal to the Krull dimension of B. But by minimality of d, $e = \mathrm{GKdim}(A/P_1) = \mathrm{Kdim}(A/P_1) \geq d$, a contradiction. □

It only remains to prove the lemma, which we do now.

Proof of Lemma. 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 sum is easily seen to be direct. Finally, if $\mathrm{GKdim}(A/I) > \mathrm{GKdim}(A) - 1$. Then let $d = \mathrm{GKdim}(A)$. Then $\dim(W^n) > n^{d-1+\epsilon}$ for infinitely many n. This means $dim(V^{2n}) \geq n \cdot \dim(W^n) > n^{d+\epsilon}$ for infinitely many n. So $\mathrm{GKdim}(A) > d$. Contradiction. □

Corollary 0.42. *Let A be a finitely generated k-algebra. Then* $\mathrm{Kdim}(A[x]) = \mathrm{Kdim}(A) + 1$.

Proof. By Noether Normalization, A is a finite $k[x_1, \ldots, x_d]$-module. So $A[x]$ is a finite $k[x_1, \ldots, x_d, x]$-module. If V is 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 $\mathrm{GKdim}(A[x]) \leq \mathrm{GKdim}(A) + 1$. So $\mathrm{Kdim}(A[x]) \leq \mathrm{Kdim}(A) + 1$. But we saw the other inequality already. □

Transcendence degree

Let F be an extension of a field K. We define $\mathrm{trdeg}_K(F)$ to be the sup over the cardinality of sets of algebraically independent elements of F over K (possibly can be infinite).

We can define $\mathrm{GKdim}(A)$ when A is a not necessarily finitely generated k-algebra to be the supremum of the GK dimensions of finitely generated subalgebras of A. Notice $\mathrm{GKdim}(A)$ is still either infinity or a nonnegative integer. GK dim gives us a nice connection between trdeg and Kdim.

Proposition 0.43. *Let K be an extension of a field F. Then $\mathrm{GKdim}_F(K) = \mathrm{trdeg}_F(K)$. That is GK dimension of K as an F-algebra is the same as its transcendence degree.*

Proof. If $x_1, \ldots, x_d$ are algebraically independent then K contains $F[x_1, \ldots, x_d]$ so $\mathrm{GKdim}(K) \geq d$. Thus $GK \geq$ trdeg. Next suppose that K has GK dimension m. Then if $m < \infty$, m is an integer and K has a finitely generated subalgebra B of GK dimension m. It follows that B contains a polynomial subalgebra on m generators and so K has trdeg $\geq m$. Thus transcendence degree is greater than or equal to the GK dimension. If m is infinite then we get infinite transcendence degree too. □

Lemma 0.44. . *If A is a finitely generated k-algebra that is an integral domain and K is its field of fractions then* $\mathrm{GKdim}_k(K) = \mathrm{GKdim}(A)$.

Proof. Let B be a finitely generated subalgebra of K. Then B is generated by $s^{-1}a_1, \ldots, s^{-1}a_m$. So B is contained in the subalgebra A_s. So $\mathrm{GKdim}(B) \leq \mathrm{GKdim}(A_s)$. Next notice that $A_s \cong A[x]/(xs-1)$. So $\mathrm{GKdim}(A_s) \leq \mathrm{GKdim}(A[x]) - 1$. Finally, $\mathrm{GKdim}(A[x]) = \mathrm{Kdim}(A[x]) = \mathrm{Kdim}(A) + 1$. So $\mathrm{GKdim}(A_s) \leq \mathrm{GKdim}(A)$. So $\mathrm{GKdim}(K) \leq \mathrm{GKdim}(A)$. On the other hand, A is a finitely generated subalgebra of K so the other inequality is immediate. □

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.

Spec and M-Spec

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-$\mathrm{Spec}(R)$ denote the set of maximal ideals of R. We can actually turn $\mathrm{Spec}(R)$ 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 $b \in J$. Do the rest! Arbitrary intersections. $\cap C_{I_\alpha} = C_{\sum I_\alpha}$. Why? If $P \supseteq I_\alpha$ for all α then it contains I_α. Conversely, if $P \supseteq \sum I_\alpha$ then $P \supseteq I_\alpha$ for all α. X endowed with this topology is called the Zariski topology. What is the Zariski topology on $X = \mathrm{Spec}(\mathbb{Z})$. How about $\mathrm{Spec}(C[t])$? How about $\mathrm{Spec}(Q)$? $\mathrm{Spec}(\{a/b : b \text{ odd}\})$?

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 topology. Then C_I is homeomorphic to $\mathrm{Spec}(R/I)$. Via the map $P \in C_I \mapsto P/I$ bijection. We just need to check that this is a continuous map with continuous inverse. If Y is a closed subset of $\mathrm{Spec}(R/I)$ 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. $\mathrm{Spec}(S^{-1}R) \to \mathrm{Spec}(R)$ is a continuous injection.
$P \mapsto P \cap R$. Then this is injective. If C_J is a closed subset of $\mathrm{Spec}(R)$ 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 $\mathrm{Spec}(R) - C_{(f)}$.

Proposition 0.45. *The following are equivalent:*

(i) $X = \mathrm{Spec}(R)$ *is disconnected;*
(ii) $R \cong R_1 \times R_2$, *with* R_1, R_2 *nonzero rings;*
(iii) R *has an idempotent* $e \neq 0, 1$.

Proof. If (3) holds then $R \cong Re \times R(1-e)$. So (3) gives (2). If (2) holds then we may take $R = R_1 \times R_2$. Then every prime contains $(1,0)$ or $(0,1)$ so $R = C_{(1,0)} \cup C_{(0,1)}$. These are disjoint because if P contains $(1,0)$ and $(0,1)$ then it contains $(1,1)$. Finally we show that (1) implies (3). If $X = C \cup D$ with C, D proper and closed and disjoint then we have $C = C_I$ and $D = C_J$ with I and J proper ideals. Then disjointness says that $I + J = R$. The fact that the union is $\mathrm{Spec}(R)$ 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 $e(1-e) = 0$. Finally $e \in J$ so it can't be 1 since J is proper and $1 - e \in I$ so e can't be 0 since I is proper. □

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 necessarily disjoint. X is irreducible if and only if R is prime and C_I is irreducible if and only if $\sqrt{I}$ is prime.

Proposition 0.46. *Let R be a ring. Then $X = \mathrm{Spec}(R)$ is quasi-compact. (In algebraic geometry, it is normal to use the term quasi-compact and reserve compact for Hausdorff and 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 $\sum_{j=1}^{d} I_{\alpha_j} = R$. What does this mean? □

Notice that $X = \mathrm{Spec}(R)$ 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. Even more simply: *points are closed in a Hausdorff space!* In $\mathrm{Spec}(R)$ the maximal ideals are the only closed points.

If every prime is maximal (and hence minimal too!) and R is noetherian then R has only finitely many primes by Noether's trick! 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 $\mathrm{Spec}(R)$ is noetherian (**Exercise on Assignment 4**!). 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 $\mathrm{Spec}(R)$ 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 $\mathrm{Spec}(R)$.

Theorem 0.8. *Let R be a noetherian ring. Then the following are equivalent:*

(i) *R has Krull dimension zero;*
(ii) $\mathrm{Spec}(R)$ *is compact Hausdorff;*
(iii) $\mathrm{Spec}(R)$ *is finite and discrete;*
(iv) *R/N is isomorphic to a finite product of fields, where N is the radical of* (0).

Proof. Suppose that R has Krull dimension zero. We've shown that $\mathrm{Spec}(R)$ is quasi-compact, so we only have to show Hausdorff. We know that $\mathrm{Spec}(R)$ is finite by Noether's trick and all points are closed so we see that (1) implies (2) and (3). Also (3) implies (2) and and if $\mathrm{Spec}(R)$ is Hausdorff then points are closed and so all primes are maximal and so (2) implies (1). It remains to show the equivalence with (4). If R/N is a finite product of fields, then R has Krull dimension zero. Conversely if R has Krull dimension zero then R has finitely many prime ideals $P_1, \ldots, P_r$, all of which are maximal and hence comaximal. Also $N = \cap P_i$ and so the Chinese remainder theorem gives that $R/N \cong \prod R/P_i$, which is a finite product of fields. □

As an immediate corollary we see that if R is a noetherian integral domain of Krull dimension 0 then R is a field.

Artinian rings

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 a ring R is Artinian if whenever $I_1 \supseteq I_2 \supseteq \cdots$ is a descending chain of ideals, we have $I_n = I_{n+1} = \cdots$ for some n. 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.

Just as with the noetherian case, we have that R is Artinian if and only if every nonempty subset of ideals of R has a minimal element and an R-module 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. □

Also if R is Artinian then every homomorphic image of R is Artinian.

Corollary 0.47. *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 0.9. *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: the ideal $J(R)$ of R Artinian is nilpotent.

Proof. By the Artinian property 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 finitely generated 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 its Krull dimension is equal to zero. □

Primary decomposition

Definition 0.48. *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 $b \in I$. To see this, 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 0.49. *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 0.50. *If Q is primary and $P = \sqrt{Q}$, we say that Q is P-primary.*

The primary ideals of $\mathbb{Z}$ are precisely (0) and $p^n\mathbb{Z}$. Prove it!

Notice prime powers need not be primary. 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 $x \in P^2$ or $y^n \in P^2$. But if $x \notin P^2$ because every element of P^2 has degree at least 2 in the generators and if $y^n \in P^2$ then we would have $y^{2n} \in P$, which we know doesn't occur.

We can say something in the case that the radical ideal is maximal.

Proposition 0.51. *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. Observe that R/Q is a local ring with maximal ideal P/Q by correspondence. Thus every element in R is either in P/Q or it 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, so one can regard this as a generalization of Noether's result.

To do this, we'll introduce the notion of irreducible ideals.

Definition 0.52. *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 0.53. *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 0.54. *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 0.55. *In a noetherian ring every ideal is a finite intersection of primary ideals.*

What does this say about noetherian rings of Krull dimension one? These are rings in which every prime ideal that is not minimal is maximal. For example, the rings $\mathbb{Z}$ and $k[t]$ with k a field. In such a ring a nonzero ideal is primary precisely if and only if its radical is prime (since its radical will be a maximal ideal). Primary decomposition show that every nonzero ideal in a noetherian ring of Krull dimension one is a finite intersection of ideals $I_1 \cap \cdots \cap I_r$ with the I_j having radical equal to a maximal ideal.

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 ν, we define the valuation ring $R = O_\nu$ of ν 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_ν all things with valuation > 0. Why is it unique. If $\nu(x) = 0$ then $\nu(1/x) = 0$. 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 *discrete valuation ring* (d.v.r. for short) if it is the valuation ring of some valuation on a field. Example, power series in one variable, $\mathbb{Z}_{(p)}$.

Remark 0.56. A d.v.r. is a PID. In particular a discrete valuation ring is noetherian.

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. □

Corollary 0.57. *R has Krull dimension ≤ 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. □

Here is another nice fact, which shows that discrete valuations are especially nice rings.

Proposition 0.58. *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 discrete valuation rings are characterized by being noetherian local domains of Krull dimension 1 that are integrally closed. This means that if we start with an integrally closed noetherian integral domain A and localize at a height one prime P we'll get a discrete valuation ring. To see this, observe that A_P is a local noetherian integral domain and has Krull dimension 1 by our choice of P. It is integrally closed, which follows from the following remark.

Remark 0.59. If A is an integrally closed domain then so is $S^{-1}A$.

Proof. 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 begin with a lemma.

Lemma 0.60. *Let A be a noetherian integral domain of Krull dimension* 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 0.61. *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 $1 \implies 2$. For $2 \implies 3$, 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 finitely generated A-module with $Px^{-1} \subseteq P$ and this gives x^{-1} integral over A, contradiction. $3 \implies 4$ is immediate: if $P = (x)$, then $P/P^2 = kx + P^2$. $4 \implies 5$ 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 $I \neq P^n$ then 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 $\implies$ 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 $\implies$ 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. □

Last time, we had begun proving the following proposition.

Proposition 0.62. *Let A be a noetherian local domain of Kdim 1 and let P be its maximal ideal and let $k = A/P$ 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).*

In addition, we had proved that $(i) \implies (ii) \implies (iii) \implies (iv)$.

Proof. Let's do the rest. OK, so we need $(iv) \implies (v)$. If P/P^2 is 1-dimensional as a k-vector space then P is principal by Nakayama's lemma, since if $x \in P \setminus P^2$ then $Ax + P^2 = P$ since P/P^2 is 1-dimensional and the image of x spans. This means that if we look at $M = P/Ax$, then $PM = (P^2 + Ax)/Ax = P/Ax = M$. Nakayama gives $M = (0)$ and so $P = Ax$. If I is a nonzero proper ideal then $I \subseteq P$. Let n be the largest natural number for which $I \subseteq P^n = (x^n)$. Since I is not contained in $(x^{n+1}) = P^{n+1}$, there is some $y \in I$ such that $y = ax^n$ but $y \notin P^{n+1} = (x^{n+1})$. 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 $(v) \implies (vi)$, 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 just cheated on the first set when we picked $x \in P \setminus P^2$. How do we know that P is not equal to P^2? If $P = P^2$ then $J(A)P = P \cdot P = P^2 = P$ and so $P = (0)$ by Nakayama's lemma!

Finally, we'll do $(vi) \implies (i)$. Let K be the field of fractions of A. Define $\nu(a)$ for a nonzero in A by $\nu(a) = m$ when $(a) = (x)^m$. The Nakayama argument we did before shows that this m is unique. We extend this to K^* via $\nu(a/b) = \nu(a) - \nu(b)$. We leave it as an exercise to the class to show that ν is indeed 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 0.63. *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 $I = \{s \in A\colon cs \in A\}$. 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 $(PA_P)^n = P^n A_P \subseteq J$. 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 0.64. *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 0.10. *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

A few facts on UFDs

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 0.11. *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 π_i, ρ_j prime (or irreducible, if you prefer–we are assuming these are the same) elements and the $i_s, j_s > 0$ and the (π_i) pairwise distinct and the (ρ_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 (π_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 ρ_s is prime, it is irreducible and since π_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 π_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 (π_s) is a prime ideal and u is a unit, some π_t, $t \neq s$ is in (π_s). But this gives $\pi_t = \pi_s a$ for some a and so since π_t is irreducible, a is a unit. Thus $(\pi_t) = (\pi_s)$—this contradicts pairwise distinct. □

Corollary 0.65. *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 ≥ 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 ≥ 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.

Regular local rings

Recall that a noetherian ring R of finite Krull dimension is *regular* if the dimension of M/M^2 as an R/M-vector space is equal to the Krull dimension of R for every maximal ideal M of R. regular local rings (which are taken to be noetherian) are very well-behaved. We note that they always have finite Krull dimension too even without the regular hypothesis: one always has $\mathrm{Kdim}(R) \leq \dim(M/M^2) < \infty$. We begin with a result showing a nice property of regular local rings.

Proposition 0.66. *A regular local ring is an integral domain.*

Proof. We prove this by induction on d, the Krull dimension of R. Let P be the maximal ideal of R. If the Krull dimension is zero then P/P^2 is zero-dimensional and hence $P = P^2$ and so $P = (0)$ by Nakayama's lemma and so R is a field. Thus we may assume that $d \geq 1$ and that the claim holds whenever the Krull dimension is strictly less than d.

Since R is noetherian, there is a finite set of minimal primes (the primes above (0))—let's write them as $Q_1, \ldots, Q_m$. Then if $I \subseteq Q_1 \cup Q_2 \cup \cdots \cup Q_d \cup P^2$ then I is contained in one of the Q_i or in P^2 (exercise). If P is contained in some $Q_j$then this would give $P = Q_j$ and so the Krull dimension would be zero. Similarly, if P is in P^2 then Nakayama gives that the Krull dimension is zero. Thus there is some $x \in P$ that is not in P^2 and not in the Q_j. Let $S = R/xR$. By our choice of x we see that the Krull dimension of S is strictly less than the Krull dimension of R, so $\mathrm{Kdim}(S) \leq d-1$. Let $Q = P/xR$ denote the maximal ideal of S. Then $Q/Q^2 = P/(P^2 + (x))$ is clearly generated by $d-1$ elements. By Nakayama's lemma, the dimension is exactly $d-1$: if not there would be $y_1, \ldots, y_e$ with $e < d-1$ such that the images in Q/Q^2 span. Then by Nakayama's lemma $Q = (y_1, \ldots, y_e, x)$ and so $y_1, \ldots, y_e, x$ would span P/P^2. We note that the Krull dimension of S is exactly $d-1$ by Theorem 0.12.

Thus S is a regular local ring and so it is an integral domain by the induction hypothesis. This means that (x) is a prime ideal. Thus (x) contains some Q_j. By our choice of x, we have $x \notin Q_j$. Let $y \in Q_j$ then $y = ax$ and so $a \in Q_j$. This means that $xQ_j = Q_j$ and so $PQ_j = Q_j$. Since R is noetherian, Nakayama's lemma gives that $Q_j = (0)$ and so (0) is prime and R is a domain. □

We require the following result to complete the proof of the preceding theorem. This can be seen as a converse to Krull's principal ideal theorem.

Theorem 0.12. *If R is a noetherian local ring of Krull dimension d with maximal ideal P and if $x \in P$ then the Krull dimension of R/xR is at least $d-1$.*

Proof. Exercise. □

Projectives are free in local rings

In this section, we'll be looking at projective modules in local rings. We begin with a lemma.

Lemma 0.67. *Let R be a local ring with maximal ideal P and let M be a finitely generated R-module and let N be a direct summand of M such that $N \subseteq PM$. Then $N = (0)$.*

Proof. Write $M = N \oplus C$. Then $PM + C = M$ since $PM \supseteq N$. Hence $P(M/C) = (M/C)$ and so $M = C$ by Nakayama's lemma. Thus $N = (0)$. □

Lemma 0.68. *Let R be a noetherian local ring with maximal idea P and let M be a finitely generated R-module with $m_1, \ldots, m_d$ a minimal set of generators for M. Let F be a free R-module on d generators $x_1, \ldots, x_d$ and consider the R-module homomorphism sending x_i to m_i. Then the kernel of this map is contained in PF.*

Proof. Suppose that $\sum c_i x_i$ is in the kernel and not all c_i are in P. Then without loss of generality $c_1 \notin P$ and so c_1 is a unit and so we can take it to be one by multiplying by the inverse of c_1. Then $m_1 + \sum_{i>1} c_i m_i = 0$ and so we can express m_1 in terms of the other generators, contradicting minimality of our generating set. □

Theorem 0.13. *Let R be a local ring with maximal ideal P. Then any finitely generated projective module is free.*

Proof. Let M be a finitely generated projective module. Map a free module F onto M as in the preceding lemma. Then the kernel is in PF. By projectivity, we have $F = M \oplus N$, where N is the kernel of the map. Then $N \subseteq PF$ and so $N = (0)$ by the other lemma. Hence $M = F$ and M is free. □

We remark that this holds for all projective modules and not just finitely generated ones, although the proof is more difficult.

Global dimension of regular local rings

We define the *projective dimension* of a module as follows. Let R be a noetherian ring and let M be a finitely generated R-module. Then the projective dimension, $d(M)$, is defined to be the infimum over all n for which there is a projective resolution of M of the form

$$0 \to P_n \to P_{n-1} \to \cdots \to P_0 \to M \to 0$$

with each P_i finitely generated and projective. If no such n exists then we take $d(M) = \infty$. The *global dimension* of R, denoted $d(R)$, is then taken to be the supremum of all $d(M)$ as M ranges over all finitely generated modules of R. When there is some ambiguity as to which ring we are working over, we'll use d_R instead of d.

We're going to show that regular local rings have finite free resolutions—we'll do this by induction on the Krull dimension. To do this, we need the following result which will serve as our "induction" step

Theorem 0.14. *Let R be a noetherian local ring with maximal ideal P and let $x \in P$ be a non-zero divisor. Let M be a finitely generated R module and suppose that if $m \in M$ has the property that $xm = 0$ then $m = 0$. If $d_{R/xR}(M/xM) < \infty$ then $d_{R/xR}(M/xM) \geq d_R(M)$.*

Proof. Let $d_{R/xR}(M/xM) = n$. We'll prove this by induction on n. We first do the base case. When $d_{R/xR}(M/xM) = 0$, we have M/xM is a projective R/xR module. We have to show that M is projective as an R-module in this case. Since R is local, so is R/xR and so M/xM is a free R/xR-module. Pick a basis $v_1, \ldots, v_d$ for M/xM as an R/xR-module. Then there exist $u_1, \ldots, u_d$ in M that map onto $v_1, \ldots, v_d$ under the natural map $M \to M/xM$. We claim that $M = Ru_1 + \cdots + Ru_d$ and that the sum is direct. To see this, first let $N = Ru_1 + \cdots + Ru_d$. Then since M/PM is a quotient of M/xM we see that $N + PM = M$ and so $P(M/N) = 0$, which gives $M = N$ by Nakayama's lemma. If $\sum c_i u_i = 0$ in M then $\sum c_i v_i = 0$ in M/xM and so each c_i is in xR. Since M has the property that if $xm = 0$ then $m = 0$ we see that we must have $\sum c_i' u_i = 0$ where $c_i' \in R$ satisfies $c_i = c_i' x$. But now each c_i' is divisible by x since $\sum c_i' v_i = 0$. Continuing in this manner, we get a sequence $c_i^{(m)}$ with $c_i^{(0)} = c_i$ and $c_i^{(m+1)} x = c_i^{(m)}$. But notice that we get an ascending chain of left ideals

$$(c_i^{(0)}) \subseteq c_i^{(1)} \subseteq \cdots,$$

which must terminate since R is noetherian. This gives $c_i^{(m+1)} \in Rc_i^{(m)} = Rc_i^{(m+1)} x$ for some m. In particular if $I = Rc_i^{(m+1)})$ then $Ix = I$ and so $IP \supseteq Ix = I$ and so $I = (0)$ by Nakayama's lemma. But since x is a non-zero divisor we see that each $c_i = 0$ and so M is free.

Now assume that $n > 0$ and that the claim is true for finitely generated modules K whenever $d_{R/xR}(K/xK) < n$. Map a finitely generated free module F onto M with kernel K. Then we get an induced map from F/xF onto M/xM with kernel K/xK. (This isn't hard, but let's see why. First, we map F onto M/xM by composing the map from F onto M with the quotient map $M \to M/xM$. The kernel of this map is $K + xF$ and since the kernel contains xF this map factors through F/xF with new kernel given by $(K + xF)/xF$. By the second isomorphism theorem we have that this is isomorphic to $K/(K \cap xF)$. Finally, $K \cap xF = xK$. The containment $K \cap xF \supseteq xK$ is easy. Conversely, if $m \in K \cap xF$ then $m = xu$ for some $u \in F$. Let $\bar{u}$ be the image of u in M. Then $x\bar{u} = 0$ in M and so $\bar{u} = 0$ and so $u \in K$, giving us the other containment.) Then by the generalized Schanuel lemma exercise, $d_{R/xR}(K/xK) = n - 1$. Then K is finitely generated and if $xm = 0$ with $m \in K$ then $m = 0$ since K is a submodule of a free module and x is a non-zero divisor. Thus by the induction hypothesis $d_R(K) \leq d_{R/xR}(K) = n$, and so $d_R(M) \leq n + 1$.

□

We note that one can in fact show with a bit more work that the inequality is always an equality and it holds even when $d_{R/xR}(M/xM) = \infty$.

Theorem 0.15. *Let R be a noetherian local ring with maximal ideal P and suppose that $x \in P$ is not a zero divisor. If $D(R/xR) = n < \infty$ then $D(R) \leq n + 1$.*

Proof. Let M be a finitely generated R-module with $d(M) = k$. We must show that $k < n + 1$. If $k = 0$ then clearly $d(M) < n + 1$ and so this is fine. Thus we may assume that $k > 0$. Then there is a finitely generated free module F that maps onto M with kernel K. Then K is finitely generated since R is noetherian and F is finitely generated. Observe that $d(K) = k - 1$ (where $\infty - 1 = \infty$, of course). (This follows from the generalized Schanuel lemma exercise.) Notice that if $m \in K$ and $xm = 0$ then $m = 0$, since x is a nonzero divisor and K lives inside a free module. Thus by the preceding theorem we have that $d_R(K) = d_{R/xR}(K/xK)$. Since $D(R/xR) \leq n$, we see that $d_R(K) \leq n$ and so $d(M) \leq n + 1$. □

Corollary 0.69. *Let R be a noetherian local ring of Krull dimension d with maximal ideal P. Then $D(R) \leq d$.*

Proof. We prove this by induction on d. We note that R is an integral domain. If $d = 0$ then R is a field and the claim is immediate. If R is not a field then P is nonzero and so by Nakayama's lemma we can pick $x \in P$ that is not in P^2. Then x is not a zero divisor since R is a domain. Then $S = R/xR$ is a local ring of Krull dimension $\leq d - 1$. By Theorem 0.12 it has Krull dimension exactly $d - 1$. Notice that $Q := P/xR$ is our maximal ideal and $Q/Q^2 \cong P/(P^2 + xR)$, which has dimension $d - 1$ as an $S/Q = R/P$-vector space (this requires Nakayama's lemma as we did before). Also, S is regular. Thus by the induction hypothesis, $D(R/xR) \leq d - 1$ and so $D(R) \leq d$ by the preceding theorem. □

Corollary 0.70. *Let R be a regular local ring of Krull dimension d. Then every finitely generated R-module has a free resolution of length at most d.*

We'll next show that a noetherian domain having the property that every finitely generated module has a finite free resolution is a UFD. As a corollary we obtain the famous Auslander-Buchsbaum theorem.

Theorem 0.16. *(Auslander-Buchsbaum) A regular local ring is a UFD.*

Before we prove this, we'll prove a few basic results.

Lemma 0.71. *Let R be a noetherian ring and let M be a finitely generated R-module. Then M has a filtration $M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = (0)$ such that $M_i/M_{i+1} \cong R/P_i$ for some $P_i \in \operatorname{Spec}(R)$.*

Proof. Suppose not. Let N be maximal with respect to M/N not having this property and replace M by M/N. Let P_0 be maximal among all annihilators of nonzero elements of M. Then P_0 is prime by the standard noetherian trick. Then P_0 is the annihilator of some $m \in M$. Consider the ideal $Rm \cong R/P$. Then we look at M/Rm, which by induction has this property. The result follows. □

One way of saying this is that in a noetherian ring the family of modules generated by modules isomorphic to R/P is equal to all finitely generated R-modules. Here we recall that a family of modules is a collection with the property that if two members from the family are in a short exact sequence then the third module in the short exact sequence is too. Notice that by induction the Lemma gives this result. We also remark that if a family in a noetherian ring is generated by a collection of finitely generated modules with the property that every element in the set of generators has a finite free resolution then the entire family has this property. To see this we just note that if we have a short exact sequence and two modules have a finite free resolution then so does the third—thus the set of finitely generated modules with an FFR forms a family.

Proposition 0.72. *If R is a noetherian ring with the property that every finitely generated R-module has an FFR then $S = R[x]$ has this property too.*

Proof. Let $\mathcal{S}$ denote the family of all modules generated by a module isomorphic to a module of the form $M \otimes_R R[x]$ where M ranges over finitely generated R-modules. If we can show that every finitely generated $R[x]$-module is in $\mathcal{S}$ then we'll be done. So we may first reduce to the case where we may assume that any $R[x]$-module whose R-annihilator is nonzero is in $\mathcal{S}$: we do this by at the beginning replacing R by R/I where I is maximal with respect to having the property that the statement of the proposition doesn't hold for R/I. Now finitely generated S modules are generated by modules of the form S/P with P a prime ideal, so it suffices to show that such modules are in $\mathcal{S}$. By assumption, we then have that $P \cap R$ is zero and so R is an integral domain. Let $f(x) \in P$ be a nonzero polynomial of smallest degree (at least degree 1). Then the principal ideal $f(x)S \cong S$ and hence is in $\mathcal{S}$. At the same time, $P/f(x)S$ has nonzero annihilator in R—this follows since $P \cap R = (0)$ and so if $g(x) \in P$ then $rg(x)$ must be a multiple of $f(x)$ and now we just take the product of r's as we range over a generating set for P—and so it is $\mathcal{S}$ too.

□

Theorem 0.17. *Let R be a noetherian integral domain and let $\{P_i\}$ be a collection of principal prime ideals and let S be the multiplicatively closed set that they generate; i.e., each $P_i = (f_i)$ and we let S be all finite products of f_i's. Then if $S^{-1}R$ is a UFD then so is R.*

Proof. Let Q be a nonzero height one prime ideal in R. We'll show that Q is principal. If Q contains some f_i then $Q = P_i$ and we're done. By assumption, $S^{-1}R$ is a noetherian UFD and since $S^{-1}Q$ is a height one prime ideal of R we see that $S^{-1}Q$ is principal. We write it as $S^{-1}Q = (q/s)$ where $q \in R$ and $s \in S$. Notice that $q \in Q$ and we may assume without loss of generality that not f_i divides q—if it did, we could divide it out and continue doing so; this process would have to terminate by the noetherian hypothesis. We now claim that with this extra condition, the ideal (q) in R is prime. Once we show this, we'll have $Q = (q)$ since Q is height one and we'll be done. So now suppose that $ab \in (q)$ with $a, b \in R$. Then $ab \in S^{-1}(q) = S^{-1}Q$ and so either $a \in S^{-1}(q)$ or $b \in S^{-1}(q)$. So let's suppose that it is a that is in the ideal and write $a = s^{-1}rq$. So by multiplying through by s we get that $as = rq$ with $s = f_{i_1} \cdots f_{i_d}$, where the i_j need not be distinct. But now f_{i_j} divides rq. Since (f_{i_j}) is prime, we see it must divide r and so by cancelling the f_{i_j} in succession, we see that we can reduce to an equation of the form $a = r'q$, which gives that $a \in (q)$, as required. □

We also need the following local characterization of UFDs. We recall that an ideal I is invertible if it is projective of rank one.

Theorem 0.18. *Let R be a noetherian integral domain. Suppose that R_P is a UFD for every maximal ideal P and suppose that every invertible ideal in R is principal. Then R is a UFD.*

Proof. Let Q be a height one prime ideal of R. Let P be a maximal ideal of R above Q. Then R_P is a UFD and hence QR_P is a height one prime of R_P and so it is principal. If, on the other hand, P is maximal and does not contain Q then $QR_P = R_P$ and so again QR_P is principal. Either way, we see that Q is invertible and so Q is principal by hypothesis. The result follows. □

We can now prove a general result about UFDs.

Theorem 0.19. *Let R be a noetherian integral domain. Suppose that each prime ideal P of grade one has the property that R_P is a UFD and that in any localization of $R[x]$ all invertible ideals are principal. Then $R[x]$ is a UFD and so in particular R is a UFD too.*

Proof. Let $T = R[x]$ and let S be the set of finite products of principal primes in T; that is, products of elements f where (f) is a height one prime ideal of R. Then it is sufficient to show that $U := S^{-1}T$ is a UFD. We'll do this with the preceding theorem. We already have that every invertible ideal in U is principal by hypothesis. Thus we just need to show that U_P is a UFD for every maximal ideal P of U. Now $P = S^{-1}Q$ for some prime ideal Q of T that is disjoint from S. Let $I = Q \cap R$. Then I is a prime ideal of R. We claim that I is either equal to zero or has grade one. Otherwise, there exist a, b in I such that a is a nonzero and such that the image of b in R/aR is not a zero divisor. But now we claim that $(a - bx)$ is a principal prime ideal of T and hence is a unit in U, which is a contradiction. Once we have this we're done: by hypothesis R_I is a UFD since I is either (0) or a prime ideal of grade 1 and so T_Q, which is a localization of $R_P[x]$ is a UFD, and so U, which is a localization of T_Q is a UFD too. Thus it remains to show that $(a - bx)$ is a prime ideal of T. We have a homomorphism $\phi : T \to R[1/b]$ given by $x \mapsto a/b$. Since the image is a domain, the kernel is a prime ideal that contains $(a - bx)$. We claim that this is the entire kernel. To see this, suppose that this is not the case and let $p(x) = p_0 + p_1x + \cdots + p_mx^m$ be in the kernel of ϕ and not in $(a-bx)$ with m minimal. Then we have $p_0b^m + p_1ab^{m-1} + \cdots + p_ma^m = 0$. Since b is not a zero divisor mod a, we see that $p_0 = aq_0$. Thus $p(x) - (a + bx)q_0 =: q_1x + \cdot + q_mx^m$ is in the kernel. Since the kernel is a prime ideal and x is not in the kernel, we see by minimality of m that $q_1 + \cdots + q_mx^{m-1} \in (a - bx)$ and so $p(x)$ is too, a contradiction. The result follows. □

Corollary 0.73. *If R is a regular local ring then R is a UFD.*

Proof. Let P be a prime ideal of grade one. Then P is height one and so R_P is a regular local ring of Krull dimension one, which means that R_P is a discrete valuation ring. Since R is regular local, every finitely generated module has a finite free resolution. Hence $R[x]$ has this property and thus so does any localization of it, since localization is flat. Let T be a localization of $R[x]$. If I is an invertible ideal of T then I is a rank one projective module with a finite free resolution. Hence by the assignment we have that $I \oplus T^n \cong T^{n+1}$ for some n and so $I \cong T$ by the assignment; i.e., I is principal.

□

We can even prove more!

Corollary 0.74. *Let R be a regular noetherian domain in which every invertible ideal is principal. Then R is a UFD.*

In fact, the converse holds too—this is similar to the argument we did before about height one primes being principal.

Proof. We just showed that R_P is a UFD for all maximal ideals P and this gives the result. □

We can even show that if R is a regular UFD then so is $R[[x]]$. Notice that if $R = \mathbb{C}[x, y, z]/(x^2 + y^3 + z^7)$ and S is R localized at the ideal (x, y, z) then R is a local ring but is not regular since $(0, 0, 0)$ is not a smooth point of the corresponding variety. Now R is a UFD but $S[[t]]$ is not a UFD, so the regular hypothesis is needed.

Theorem 0.20. *Let R be a regular UFD. Then $R[[x]]$ is a regular UFD.*

Proof. (Quick sketch) To see that $R[[x]]$ is regular, notice that x is in the Jacobson radical of $R[[x]]$ (use the usual criterion) and is not in the square of any maximal ideal. It follows that every maximal ideal P of $R[[x]]$ contains x and $x \notin P^2$ so P/P^2 has an $R[[x]]/P$-basis that contains x. Moreover, we can find a basis in which the remaining elements of the basis are in R—think about it! Now let d be the Krull dimension of R. Then the Krull dimension of $R[[x]]$ is at least $d + 1$. So it is sufficient to show that P/P^2 has dimension at most $d + 1$. By assumption there is a basis $\{x, r_1, \ldots, r_m\}$ for P/P^2 as an $R[[x]]/P$-vector space. Let Q be a maximal ideal in R above $P \cap R$. Then $Q = P \cap R$ since $QR[[x]] + xR[[x]]$ is proper and contains P. Then $r_1, \ldots, r_m$ are linearly independent in Q/Q^2 and so $m \leq d$, which gives the result about regularity.

To show it is a UFD, we must show that invertible ideals are principals. So let I be an invertible ideal in $R[[x]]$. Then $I \oplus Q = F$ for some finitely generated free module F and some module Q and I has rank 1. Then $(I/xI) \oplus (Q/xQ) = (F/xF)$ and F/xF is a free R-module. Hence I/xI is R-projective as it is a direct summand of a free module. In particular, I/xI is torsion free and has a well-defined rank (**see exercise**). We claim that the rank of I/xI is at most one. To see this, if $u_1, u_2 \in I/xI$ then there are $v_1, v_2 \in I$ that map onto u_1, u_2. Then v_1, v_2 are dependent and so we have $a_1v_1 + a_2v_2 = 0$, we may assume that a_1, a_2 are not both in (x). Then we reduce mod x and get a relation involving u_1, u_2. Similarly, the R-rank of Q/xQ is at most the $R[[x]]$-rank of Q. Since the R-rank of F/xF is equal to the $R[[x]]$-rank of F, we see that the ranks of all the involved modules are equal to the ranks of their reductions mod x.

A projective module of rank one is isomorphic to an invertible ideal in R. The idea is as follows: let P be a rank one projective module. Then $S^{-1}P \cong S^{-1}R$, where S is the set of nonzero elements of R (in general we'd use nonzero divisors). This means $P_s \cong R_s$ for some fixed element $s \in R$, since we just have to look at an element that gets sent to one under the isomorphism. But now by clearing denominators we can construct an injective map from P into R and the image is obviously a rank one projective ideal of R.

Thus $I/xI \cong J$ for some invertible ideal of R. So since R is a UFD, we see that J is principal. Now we lift J to a principal ideal $JR[[x]]$. We'd like to show that $JR[[x]] \cong I$ and then we'll have that I is principal. To do this, we use the fact that we have a map $f : JR[[x]] \to I/xI$, given by reducing first mod x to get J and then applying the isomorphism between J and I/xI. Since I is projective, the map $I \to I/xI$ lifts to a map $g : I \to JR[[x]]$. Similarly, $JR[[x]]$ is projective since J is principal and so we get a map $h : JR[[x]] \to I$. We'd just like to show that g and h are bijective. To see this, observe that $h \circ g : I \to I$ by construction induces the identity map on I/xI. Consider the map $\phi := (h \circ g, \mathrm{id}_Q) : P \oplus Q \to P \oplus Q$. This induces a map from F to itself that is the identity mod x. Thus we can regard ϕ as an $R[[x]]$ linear map from some $R[[x]]^d$ to itself that is the identity mod x; i.e., we can view it as a $d \times d$ matrix with entries in $R[[x]]$ that is the identity mod x.

Now x is in the Jacobson radical and use the usual trick to show that $I + xA$ is invertible. This gives that ϕ is a bijection and so $h \circ g$ is a bijection. Similarly, $g \circ h$ is a bijection. □