WORKSHEET #1.1: RINGS

EXAMPLE: The following are rings.

(1) Rings of numbers, like $\mathbb{Z}$ and $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z}\}$.
(2) Given a starting ring A, the polynomial ring in one indeterminate
$$A[X] := \{a_d X^d + \cdots + a_1 X + a_0 \mid d \geq 0, a_i \in A\},$$
or in a (finite or infinite![1]) set of indeterminates $A[X_1, \ldots, X_n]$, $A[X_\lambda \mid \lambda \in \Lambda]$.
(3) Given a starting ring A, the power series ring in one indeterminate
$$A[\![X]\!] := \left\{ \sum_{i \geq 0} a_i X^i \mid a_i \in A \right\},$$
or in a set of indeterminates $A[\![X_1, \ldots, X_n]\!]$.
(4) For a set X, $\mathrm{Fun}(X, \mathbb{R}) := \{\text{all functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.
(5) $\mathcal{C}([0,1]) := \{\text{continuous functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.
(6) $\mathcal{C}^\infty([0,1]) := \{\text{infinitely differentiable functions } f : [0,1] \to \mathbb{R}\}$ with pointwise $+$ and $\times$.
($\div$) Quotient rings: given a starting ring A and an ideal I, $R = A/I$.
($\times$) Product rings: given rings R and S, $R \times S = \{(r, s) \mid r \in R, s \in S\}$.

DEFINITION: An element x in a ring R is called a

- **unit** if x has an **inverse** $y \in R$ (i.e., $xy = 1$).
- **zerodivisor** if there is some $y \neq 0$ in R such that $xy = 0$.
- **nilpotent** if there is some $e \geq 0$ such that $x^e = 0$.
- **idempotent** if $x^2 = x$.

We also use the terms **nonunit, nonzerodivisor, nonnilpotent, nonidempotent** for the negations of the above. We say that a ring is **reduced** if it has no nonzero nilpotents.

(1) Warmup with units, zerodivisors, nilpotents, and idempotents.
(a) What are the implications between nilpotent, nonunit, and zerodivisor?
(b) What are the implications between reduced, field, and domain?
(c) What two elements of a ring are always idempotents? We call an idempotent **nontrivial** to mean that it is neither of these.
(d) If e is an idempotent, show that $e' := 1 - e$ is an idempotent[2] and $ee' = 0$.

(a) nilpotent $\Rightarrow$ zerodivisor $\Rightarrow$ nonunit
(b) reduced $\Leftarrow$ domain $\Leftarrow$ field
(c) 0 and 1
(d) $e'^2 = (1-e)(1-e) = 1 - 2e + e^2 = 1 - e = e'$ and $ee' = e(1-e) = e - e^2 = 0$.

(2) Elements in polynomial rings: Let $R = A[X_1, \ldots, X_n]$ a polynomial ring over a *domain* A.
(a) If $n = 1$, and $f, g \in R = A[X]$, briefly explain why the top degree[3] of fg equals the top degree of f plus the top degree of g. What if A is not a domain?

[1] Note: Even if the index set is infinite, by definition the elements of $A[X_\lambda \mid \lambda \in \Lambda]$ are finite sums of monomials (with coefficients in A) that each involve finitely many variables.

[2] We call e' the **complementary idempotent** to e.

[3] The **top degree** of $f = \sum a_i X^i$ is $\max\{k \mid a_k \neq 0\}$; we say **top coefficient** for a_k. We use the term top degree instead of degree for reasons that will come up later.

(b) Again if $n = 1$, briefly explain why $R = A[X]$ is a domain, and identify all of the units in R.
(c) Now for general n, show that R is a domain, and identify all of the units in R.

(a) If $f = a_m X_m +$ lower terms and $g = b_n X_n +$ lower terms , then $fg = \sum a_m b_n X^{m+n} +$ lower terms. If A is a domain, then $a_m, b_n \neq 0$ implies $a_m b_n \neq 0$, but if A is not a domain, the top degree may drop.
(b) By looking at the top degree terms as above, we see that the product of nonzero polynomials is nonzero. The units in R are just the units in A viewed as polynomials with no higher degree terms. Indeed, such elements are definitely units; on the other hand, if $fg = 1$ in R, then the top degree of f and g are both zero, so f and g are constant, which means f and g are in A, so a unit in R is a unit in A.
(c) The claim that R is a domain follows by induction on n, since $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$. The units in R are again the units in A. This also follows by induction on n: a unit in $A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$ is a unit in $A[X_1, \ldots, X_{n-1}]$, which by the induction hypothesis is constant.

(3) Elements in power series rings: Let A be a ring.
(a) Explain why the set of formal sums $\{\sum_{i \in \mathbb{Z}} a_i X_i \mid a_i \in A\}$ with arbitrary positive and negative exponents is *not* clearly a ring in the same way as $A[\![X]\!]$.
(b) Given series $f, g \in A[\![X]\!]$, how much of f, g do you need to know to compute the X^3-coefficient of $f + g$? What about the X^3-coefficient of fg?
(c) Find the first three coefficients for the inverse[4] of $f = 1 + 3X + 7X^2 + \cdots$ in $\mathbb{R}[\![X]\!]$.
(d) Does "top degree" make sense in $A[\![X]\!]$? What about "bottom degree"?
(e) Explain why[5] for a domain A, the power series ring $A[\![X_1, \ldots, X_n]\!]$ is also a domain.
(f) Show[6] that $f \in A[\![X_1, \ldots, X_n]\!]$ is a unit if and only if the constant term of f is a unit.

(a) To multiply two such formal sums, you would have to take an infinite sum in A to compute the coefficient of any X^i.
(b) To compute the X^3-coefficient of $f + g$, you just need to know the X^3-coefficients of f and g. To compute the X^3-coefficient of fg, you need to know the $1, X, X^2, X^3$ coefficients of f and g.
(c) $g = 1 - 3X - 2X^2 + \cdots$.
(d) No; yes.
(e) For $n = 1$, look at the bottom degree terms. The bottom degree term of the product is the product of the bottom degree terms; if A is a domain, this product is nonzero. The statement just follows by induction on n.
(f) If f is a unit, then the constant term is a unit, since the constant term of fg is the constant term of f times that of g.
For the other direction, first, take $n = 1$. Given $f = \sum_i a_i X^i$, construct $g = \sum_i b_i X^i$ by defining b_m recursively $b_0 = 1/a_0$ and that the X^m-coefficient of $(\sum_{i=0}^m a_i X^i)(\sum_{i=0}^m b_i X_i)$ is 0 for $m > 0$: we can do this since, given $b_0, \ldots, b_m$ that work in the mth step, in the next step we can the formula for the X^{m+1} coefficient is $a_0 b_{m+1} + a_1 b_m + \cdots + a_{m+1} b_0$, since a_0 is a unit, we can solve for b_{m+1} to make this equal

[4] It doesn't matter what the $\cdots$ are!
[5] You might want to start with the case $n = 1$.
[6] Hint: For $n = 1$, given $f = \sum_i a_i X^i$, construct $g = \sum_i b_i X^i$ by defining b_m recursively $b_0 = 1/a_0$ and that the X^m-coefficient of $(\sum_{i=0}^m a_i X^i)(\sum_{i=0}^m b_i X_i)$ is 0 for $m > 0$.

zero without changing the lower coefficients. Continuing this way, take $g = \sum_i b_i X^i$. Then for any k, the X^k-coefficient only depends on the $a_0, \ldots, a_k$ and $b_0, \ldots, b_k$ coefficients, and by construction, this coefficient is zero for $k \geq 1$. Thus, any such f has an inverse.

The general claim follows by induction on n: if $f \in A[\![X_1, \ldots, X_n]\!]$ has a unit constant term considered as a power series in $A[\![X_1, \ldots, X_n]\!]$, then its constant term in $(A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!]$ has a unit constant term, hence is a unit in $A[\![X_1, \ldots, X_{n-1}]\!]$, so f is a unit in $(A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!] = A[\![X_1, \ldots, X_n]\!]$.

(4) Elements in function rings.

(a) For $R = \mathrm{Fun}([0,1], \mathbb{R})$,

(i) What are the nilpotents in R?

(ii) What are the units in R?

(iii) What are the idempotents in R?

(iv) What are the zerodivisors in R?

(b) For $R = \mathcal{C}([0,1], \mathbb{R})$, $R = \mathcal{C}^\infty([0,1], \mathbb{R})$ same questions as above. When are there any/none?

(a) For $R = \mathrm{Fun}([0,1], \mathbb{R})$,

(i) There are no nilpotents, since for any $\alpha \in [0,1]$, $f(\alpha)^n = 0$ means that $f(\alpha) = 0$.

(ii) The units are the functions that are never zero, since the function $g(x) = 1/f(x)$ is then defined (and conversely).

(iii) $f(x)$ is idempotent if $f(\alpha) \in \{0, 1\}$ for all $\alpha \in [0,1]$.

(iv) Any function that is zero at some point is a zerodivisor: if $S = \{\alpha \in [0,1] \mid f(\alpha) = 0\}$ is nonempty, then let g be a nonzero function that vanishes on $[0,1] \smallsetminus S$, then $fg = 0$.

(b) For $R = \mathcal{C}([0,1])$ or $R = \mathcal{C}^\infty([0,1])$,

(i) Same

(ii) Same

(iii) There are no nontrivial idempotents: the same condition as above applies, but by continuity, f must either be identically 0 or identically 1.

(iv) The difference is that now there may not be a nonzero function that vanishes on $[0,1] \smallsetminus S$, e.g., if f vanishes at a single point. To be a zerodivisor, the set $[0,1] \smallsetminus S$ as above must be not be dense.

(5) Product rings and idempotents.

(a) Let R and S be rings, and $T = R \times S$. Show that $(1,0)$ and $(0,1)$ are nontrivial complementary idempotents in T.

(b) Let T be a ring, and $e \in T$ a nontrivial idempotent, with $e' = 1 - e$. Explain why $Te = \{te \mid t \in T\}$ and Te' are rings with the same addition and multiplication as T. Why didn't I say "subring"?

(c) Let T be a ring, and $e \in T$ a nontrivial idempotent, with $e' = 1 - e$. Show that $T \cong Te \times Te'$. Conclude that R has nontrivial idempotents if and only if R decomposes as a product.

(a) $(1,0)^2 = (1,0)$, $(0,1)^2 = (0,1)$, and $(1,0) + (0,1) = (1,1)$ is the "1" of $R \times S$.

(b) $re + se = (r+s)e$ and $(re)(se) = rse^2 = rse$. Same with e'.

(c) Define $\phi : T \to Te \times Te'$ by $\phi(t) = (te, te')$. The verification that this is a ring homomorphism essentially the content of (b). If $\phi(t) = (0,0)$, then $te = 0$ and $0 = te' = t(1-e) = t - te$, so $t = 0$, hence ϕ is injective. Given $(re, se') \in Te \times Te'$, we have $\phi(re + se') = ((re + se')e, (re + se')e') = (re, se')$, hence ϕ is surjective, as well.

(6) Elements in quotient rings:
   (a) Let K be a field, and $R = K[X, Y]/(X^2, XY)$. Find
      - a nonzero nilpotent in R
      - a zerodivisor in R that is not a nilpotent
      - a unit in R that is not equivalent to a constant polynomial
   (b) Find $n \in \mathbb{Z}$ such that
      - $[4] \in \mathbb{Z}/(n)$ is a unit
      - $[4] \in \mathbb{Z}/(n)$ is a nonzero nilpotent
      - $[4] \in \mathbb{Z}/(n)$ is a nonnilp. zerodivisor
      - $[4] \in \mathbb{Z}/(n)$ is a nontrivial idempotent

This solution is embargoed.

(7) More about elements.
   (a) Prove that a nilpotent plus a unit is always a unit.
   (b) Let A be an arbitrary ring, and $R = A[X]$. Characterize, in terms of their coefficients, which elements of R are units, and which elements are nilpotents.
   (c) Let A be an arbitrary ring, and $R = A[\![X]\!]$. Characterize, in terms of their coefficients, which elements of R are nilpotents.

§1.2: IDEALS

DEFINITION: Let S be a subset of a ring R. The **ideal generated by** S, denoted (S), is the smallest ideal containing S. Equivalently,

$$(S) = \left\{ \sum r_i s_i \mid r_i \in R, s_i \in S \right\} \quad \text{is the set of } R\text{-linear combinations}^1 \text{ of elements of } S.$$

We say that S **generates** an ideal I if $(S) = I$.

DEFINITION: Let I, J be ideals of a ring R. The following are ideals:

- $IJ := (ab \mid a \in I, b \in J)$.
- $I^n := \underbrace{I \cdot I \cdots I}_{n \text{ times}} = (a_1 \cdots a_n \mid a_i \in I)$ for $n \geq 1$.
- $I + J := \{a + b \mid a \in I, b \in J\} = (I \cup J)$.
- $rI := (r)I = \{ra \mid a \in I\}$ for $r \in R$.
- $I : J := \{r \in R \mid rJ \subseteq I\}$.

DEFINITION: Let I be an ideal in a ring R. The **radical** of I is $\sqrt{I} := \{f \in R \mid f^n \in I \text{ for some } n \geq 1\}$. An ideal I is **radical** if $I = \sqrt{I}$.

DIVISION ALGORITHM: Let A be a ring, and $R = A[X]$ be a polynomial ring. Let $g \in R$ be a **monic** polynomial; i.e., the leading coefficient of f is a unit. Then for any $f \in R$, there exist unique polynomials $q, r \in R$ such that $f = gq + r$ and the top degree of r is less than the top degree of g.

(1) Briefly discuss why the two characterizations of (S) in Definition 2.1 are equal.

The set of linear combinations of elements of S is an ideal:

- $0 = 0s_1$ (we also consider 0 to be the empty combination);
- given two linear combinations, by including zero coefficients, we can assume our combinations involve the same elements of S, and then $\sum_i a_i s_i + \sum_i b_i s_i = \sum_i (a_i + b_i) s_i$;
- $r(\sum_i a_i s_i) = \sum_i r a_i s_i$.

Any ideal that contains S must contain all of the linear combinations of S, using the definition of ideal. These two facts mean that the set of linear combinations is the smallest ideal containing S.

(2) Finding generating sets for ideals: Let S be a subset of a ring R, and I an ideal.

(a) To show that $(S) = I$, which containment do you think is easier to verify? How would you check?

(b) To show that $(S) = I$ given $(S) \subseteq I$, explain why it suffices to show that $I/(S) = 0$ in $R/(S)$; i.e., that every element of I is equivalent to 0 modulo S.

(c) Let K be a field, $R = K[U, V, W]$ and $S = K[X, Y]$ be polynomial rings. Let $\phi : R \to S$ be the ring homomorphism that is constant on K, and maps $U \mapsto X^2, V \mapsto XY, W \mapsto Y^2$. Show that the kernel ϕ is generated by $V^2 - UW$ as follows:

- Show that $(V^2 - UW) \subseteq \ker(\phi)$.
- Think of R as $K[U, W][V]$. Given $F \in \ker(\phi)$, use the Division Algorithm to show that $F \equiv F_1 V + F_0$ modulo $(V^2 - UW)$ for some $F_1, F_0 \in K[U, W]$ with $F_1 V + F_0 \in \ker(\phi)$.
- Use $\phi(F_1 V + F_0) = 0$ to show that $F_1 = F_0 = 0$, and conclude that $F \in \ker(\phi)$.

(a) Showing $(S) \subseteq I$ is the easier containment: it suffices to show that $S \subseteq I$.

(b) This follows from the Second Isomorphism Theorem.

[1] Linear combinations always means *finite* linear combinations: the axioms of a ring can only make sense of finite sums.

(c)
- We check $\phi(V^2 - UW) = (XY)^2 - X^2Y^2 = 0$, so $V^2 - UW \in \ker(\phi)$. This implies $(V^2 - UW) \subseteq \ker(\phi)$.
- By Division, we have $F = (V^2 - UW)Q + R$, with the top degree (in V) of R at most 1. Then $F \equiv R = F_1V + F_0$ modulo $(V^2 - UW)$. Since $F, V^2 - UW \in \ker(\phi)$, we must have $F_1V + F_0 \in \ker(\phi)$.
- We have $0 = \phi(F_1V + F_0) = F_1(X^2, Y^2)XY + F_0(X^2, Y^2)$. The $F_1(X^2, Y^2)XY$ terms only have monomials whose X-degree is odd, and the $F_0(X^2, Y^2)$ terms only have monomials whose X-degree is even, so none can cancel with each other. This means that $F_1(X^2, Y^2) = 0$ and $F_0(X^2, Y^2) = 0$, so $F_1(U, W) = F_0(U, W) = 0$. Thus, $F \equiv 0$ modulo $(V^2 - UW)$, and as above, we conclude $\ker(\phi) = (V^2 - UW)$.

(3) Radical ideals:

(a) Fill in the blanks and convince yourself:

- R/I is a field $\iff$ I is _____
- R/I is a domain $\iff$ I is _____
- R/I is reduced $\iff$ I is _____

(b) Show that the radical of an ideal is an ideal.

(c) Show that a prime ideal is radical.

(d) Let K be a field and $R = K[X, Y, Z]$. Find a generating set[2] for $\sqrt{(X^2, XYZ, Y^2)}$.

(a)
- R/I is a field $\iff$ I is maximal
- R/I is a domain $\iff$ I is prime
- R/I is reduced $\iff$ I is radical

(b) Let $f, g \in \sqrt{I}$. Then there are $m, n \geq 1$ such that $f^m, g^n \in I$. Then

$$(f + g)^{m+n-1} = \sum_{i+j=m+n-1} \binom{m+n-1}{i, j} f^i g^j,$$

and for each term in the sum either $i \geq m$ or $j \geq n$, so each term is in I, hence the whole sum is in I. Now let $r \in R$. Then $(rf)^m = r^m f^m \in I$.

(c) Suppose I is prime. If $x \in \sqrt{I}$, then $x^n \in I$ for some n. Then, by the definition of prime, $x \in I$. Thus, $\sqrt{I} = I$.

(d) Since X^2 and Y^2 are in (X^2, XYZ, Y^2), we have $X, Y \in \sqrt{(X^2, XYZ, Y^2)}$ by definition, so $(X, Y) \subseteq \sqrt{(X^2, XYZ, Y^2)}$. For the other containment, if $F(X, Y, Z) \notin (X, Y)$, consider F as a polynomial in X, Y with coefficients in $K[Z]$; the condition means that the top degree of F is zero, and hence the top degree of F^n is zero for all n, so $F \notin \sqrt{(X^2, XYZ, Y^2)}$.

(4) Evaluation ideals in polynomial rings: Let K be a field and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let $\alpha = (\alpha_1, \ldots, \alpha_n) \in K^n$.

(a) Let $\mathrm{ev}_\alpha : R \to K$ be the map of evaluation at α: $\mathrm{ev}_\alpha(f) = f(\alpha_1, \ldots, \alpha_n)$, or $f(\alpha)$ for short. Show that $\mathfrak{m}_\alpha := \ker \mathrm{ev}_\alpha$ is a maximal ideal and $R/\mathfrak{m}_\alpha \cong K$.

(b) Apply division repeatedly to show that $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.

(c) For $K = \mathbb{R}$ and $n = 1$, find a maximal ideal that is not of this form. Same question with $n = 2$.

(d) With K arbitrary again, show that every maximal ideal $\mathfrak{m}$ of R for which $R/\mathfrak{m} \cong K$ is of the form $\mathfrak{m}_\alpha$ for some $\alpha \in K^n$. Note: this is *not* a theorem with a fancy German name.

[2] Hint: To show your set generates, you might consider the bottom degree of F considered as a polynomial in X and Y.

(a) The evaluation map is surjective, since for any $k \in K$, the constant function k maps to k. By the First Isomorphism Theorem, $R/\mathfrak{m}_\alpha \cong K$, so $\mathfrak{m}_\alpha$ is maximal.

(b) We have $\mathrm{ev}_\alpha(X_i - \alpha_i) = \alpha_i - \alpha_i = 0$, so $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq \mathfrak{m}_\alpha$. Given some $F \in \mathfrak{m}_\alpha$, consider F as a polynomial in X_1 and apply division by $X_1 - \alpha_1$, to get $F \equiv F_1$ modulo $(X_1 - \alpha_1, \ldots, X_n - \alpha_n)$, for some F_1 not involving X_1. Continue with $X_2 - \alpha_2, \ldots$ to get the F is equivalent to a constant, which must be zero. This shows that $F \in (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$, so $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.

(c) $(X^2 + 1)$; $(X^2 + 1, Y)$.

(d) Let $\phi : R \to R/\mathfrak{m} \cong K$ be quotient map followed by the given isomorphism. Set $\alpha_i := \phi(X_i)$. Then $X_i - \alpha_i \in \ker(\phi)$, so $\mathfrak{m}_\alpha = (X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq \ker(\phi)$. Since $\mathfrak{m}_\alpha$ is maximal, we must have equality.

(5) Lots of generators:

(a) Let K be a field and $R = K[X_1, X_2, \ldots]$ be a polynomial ring in countably many variables. Explain[3] why the ideal $\mathfrak{m} = (X_1, X_2, \ldots)$ cannot be generated by a finite set.

(b) Show that the ideal $(X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n) \subseteq K[X, Y]$ cannot be generated by fewer than $n + 1$ generators.

(c) Let $R = \mathcal{C}([0, 1], \mathbb{R})$ and $\alpha \in (0, 1)$. Show that for any element $g \in (f_1, \ldots, f_n) \subseteq \mathfrak{m}_\alpha$, there is some $\varepsilon > 0$ and some $C > 0$ such that $|g| < C \max_i\{|f_i|\}$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$. Use this to show that $\mathfrak{m}_\alpha$ cannot be generated by a finite set.

(a) Suppose $\mathfrak{m} = (f_1, \ldots, f_m)$. Since each polynomial involves only finitely many variables, only finitely many variables occur in $\{f_1, \ldots, f_m\}$, and since each f_i has no constant term, these polynomials are linear combinations of those variables $X_1, \ldots, X_n$; i.e., $(f_1, \ldots, f_m) \subseteq (X_1, \ldots, X_n)$. It suffices to show that $\mathfrak{m} \neq (X_1, \ldots, X_n)$. To see it, take X_{n+1} and note that $X_{n+1} = \sum_{i=1}^n g_i X_i$ is impossible, since the monomial X_{n+1} can't occur in any summand of the right hand side.

(b) Note that this ideal is the set of all polynomial whose bottom degree is at least n. Given a generating set $f_1, \ldots, f_m$ for I, consider the degree n terms of the polynomials f_i. We claim that the degree n terms of $f_1, \ldots, f_m$ must span the space of degree n polynomials as a vector space. Indeed, given h of degree n, we have $h \in I$, so $h = \sum_i g_i f_i$. But every term of f_i has degree at least n, so the only things of degree n on the right hand side come from the degree n piece of f_i and the degree zero piece of g_i. This shows the claim. Then the statement is clear, since the degree n terms form an $n + 1$ dimensional vector space.

(c) Let $g = \sum g_i f_i \in (f_1, \ldots, f_n)$. By continuity, there is some $\varepsilon > 0$ and some $C > 0$ such that $|g_i| < C/n$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$, so $|g| < |\sum_i g_i f_i| \leq \sum_i |g_i||f_i| \leq \sum_i C/n \max_i\{|f_i|\} \leq C \max_i\{|f_i|\}$ on $(\alpha - \varepsilon, \alpha + \varepsilon)$.
Now, given $f_1, \ldots, f_n \in \mathfrak{m}_\alpha$, let $g = \sqrt{\max_i\{|f_i|\}}$. Then g is continuous and $g(\alpha) = 0$, so $g \in \mathfrak{m}_\alpha$, but $g/\max_i\{|f_i|\} = 1/g \to \infty$ as $x \to \alpha$, so there is no constant $C > 0$ and no interval $(\alpha - \varepsilon, \alpha + \varepsilon)$ on which $|g| < C \max_i\{|f_i|\}$. Thus, $\mathfrak{m}_\alpha$ is not finitely generated.

(6) Evaluation ideals in function rings: Let $R = \mathcal{C}([0, 1], \mathbb{R})$. Let $\alpha \in [0, 1]$.

(a) Let $\mathrm{ev}_\alpha : \mathcal{C}([0, 1]) \to \mathbb{R}$ be the map of evaluation at α: $\mathrm{ev}_\alpha(f) = f(\alpha)$. Show that $\mathfrak{m}_\alpha := \mathrm{ev}_\alpha$ is a maximal ideal and $R/\mathfrak{m}_\alpha \cong \mathbb{R}$.

(b) Show that $(x - \alpha) \subseteq \mathfrak{m}_\alpha$.

[3] Hint: You might find it convenient to show that $(f_1, \ldots, f_m) \subseteq (X_1, \ldots, X_n)$ for some n, and then show that $(X_1, \ldots, X_n) \subsetneq \mathfrak{m}$

(c) Show that every maximal ideal R is of the form $\mathfrak{m}_\alpha$ for some $\alpha \in [0,1]$. You may want to argue by contradiction: if not, there is an ideal I such that the sets $U_f := \{x \in [0,1] \mid f(x) \neq 0\}$ for $f \in I$ form an open cover of $[0,1]$. Take a finite subcover $U_{f_1}, \ldots, U_{f_t}$ and consider $f_1^2 + \cdots + f_t^2$.

(a) $\mathrm{ev}_\alpha : \mathcal{C}([0,1]) \to \mathbb{R}$ is a surjective ring homomorphism, since $\mathrm{ev}_\alpha(r) = r$ for any $r \in \mathbb{R}$. Thus, by the First Isomorphism Theorem, $R/\mathfrak{m}_\alpha \cong \mathbb{R}$, and hence $\mathfrak{m}_\alpha$ is a maximal ideal.
(b) It suffices to note that $\mathrm{ev}_\alpha(x - \alpha) = 0$.
(c) Argue by contradiction: if not, there is a proper ideal I that is not contained in some $\mathfrak{m}_\alpha$; this means that for every α, some element of I does not vanish at α. Since for any continuous f, the set $U_f := \{x \in [0,1] \mid f(x) \neq 0\}$ is open, the collection $\{U_f \mid f \in I\}$ is an open cover of $[0,1]$. Since $[0,1]$ is compact, there is a finite subcover $U_{f_1}, \ldots, U_{f_t}$. For these f_i's consider $h = f_1^2 + \cdots + f_t^2$. Each f_i^2 is nonnegative, and for any α, one of these is strictly positive at α. This means that $h(x) \neq 0$ for all $x \in [0,1]$, so h is a unit, and hence $I = R$, a contradiction.

(7) Division Algorithm.
(a) What fails in the Division Algorithm when g is not monic? Uniqueness? Existence? Both?
(b) Review the proof of the Division Algorithm.

(8) Let K be a field and $R = K[\![X_1, \ldots, X_n]\!]$ be a power series ring in n indeterminates. Let $R' = K[\![X_1, \ldots, X_{n-1}]\!]$, so we can also think of $R = R'[\![X_n]\!]$. In this problem we will prove the useful analogue of division in power series rings:

WEIERSTRASS DIVISION THEOREM: Let $r \in R$, and write $g = \sum_{i \geq 0} a_i X_n^i$ with $a_i \in R'$. For some $d \geq 0$, suppose that $a_d \in R'$ is a unit, and that $a_i \in R'$ *not* a unit for all $i < d$. Then, for any $f \in R$, there exist unique $q \in R$ and $r \in R'[X_n]$ such that $f = gq + r$ and the top degree of r as a polynomial in X_n is less than d.

(a) Show the theorem in the very special case $g = X_n^d$.
(b) Show the theorem in the special case $a_i = 0$ for all $i < d$.
(c) Show the uniqueness part of the theorem.[4]
(d) Show the existence part of the theorem.[5]

(a) Given f, write $f = \sum_{i \geq 0} b_i X_n^i$ with $b_i \in R'$. For existence, just take $r = \sum_{i=0}^{d-1} b_i X_n^i$ and $q = \sum_{i=d}^{\infty} b_i X_n^{i-d}$. For uniqueness, note that if $f = gq + r = gq' + r'$ with the top degree of r and r' as polynomials in X_n are less than d. Then $0 = g(q - q') + (r - r')$, so the uniqueness claim reduces to the case $f = 0$; we will use this in the other parts without comment. Every term of r has X_n-degree less than d, whereas every term of qg has X_n-degree at least d, so no terms can cancel. Thus $qg + r = 0$ implies $q = r = 0$ (here and henceforth, we assume r is as in the statement when we write $qg + r$).
(b) If $a_i = 0$ for $i < d$, then $g = X_n^d u$ where $u = \sum_{i \geq 0} a_{i-d} X_n^i$. Since the constant coefficient of u is a_d, which is a unit in R', u is a unit in R. Thus, we can apply (a) to f and X_n^d to get

[4]Hint: For an element of R' or of R, write ord' for the order in the $X_1, \ldots, X_{n-1}$ variables; that is, the lowest total $X_1, \ldots, X_{n-1}$-degree of a nonzero term (not counting X_n in the degree). If $qg + r = 0$, write $q = \sum_i b_i X_n^i$. You might find it convenient to pick i such that $\mathrm{ord}'(b_i)$ is minimal, and in case of a tie, choose the smallest such i among these.

[5]Hint: Write $g_- = \sum_{i=0}^{t-1} a_i X_n^i$ and $g_+ = \sum_{i=t}^{\infty} a_i X_n^i$. Apply (b) with g_+ instead of g, to get some q_0, r_0; write $f_1 = f - (q_0 g + r_0)$, and keep repeating to get a sequence of q_i's and r_i's. Show that $\mathrm{ord}'(q_i), \mathrm{ord}'(r_i) \geq i$, and use this to make sense of $q = \sum_i q_i$ and $r = \sum_i r_i$.

$f = q_0 X_n^d + r_0 = (q_0 u^{-1})g + r_0$; thus, $q = q_0 u^{-1}$ and $r = r_0$ satisfy the existence clause of the theorem. For uniqueness, if $f = q'g + r'$, then $f = q'uX_n^d + r'$, so by the uniqueness part of (a), we must have $q'u = q_0$ and $r' = r_0$, and thus $q' = q$ and $r' = r$.

(c) For an element of R' or of R, write ord' for the order in the $X_1, \ldots, X_{n-1}$ variables; that is, the lowest total $X_1, \ldots, X_{n-1}$-degree of a nonzero term (not counting X_n in the degree). Suppose that $qg + r = 0$, and write $q = \sum_i b_i X_n^i$. Suppose that q is nonzero, so $b_i \neq 0$ for some i. Pick i such that $\mathrm{ord}'(b_i) \leq \mathrm{ord}'(b_j)$ for all j with $b_j \neq 0$, and $\mathrm{ord}'(b_i) = \mathrm{ord}'(b_j)$ implies $i < j$; we can do this by well ordering of $\mathbb{N}$. Say $\mathrm{ord}'(b_i) = t$. Consider the coefficient of X_n^{d+i} in $0 = qg + r$. Byt he degree constraint on r, this is the same as the coefficient of X_n^{d+i} in qg. Multiplying out, this is $\sum_{j=0}^{d+i} a_{d+i-j} b_j$. For $j = i$, the order of $a_d b_i$ is t. For $j < i$, we have $\mathrm{ord}'(a_{d+i-j} b_j) \geq \mathrm{ord}'(b_j) > t$ by choice of i. For $j > i$, since $\mathrm{ord}'(a_{d+i-j}) > 0$ and ord'(b$_j$) $\geq t$, we have $\mathrm{ord}'(a_{d+i-j} b_j) > t$. Thus, the no term can cancel the $a_d b_i$ term, so $qg + r \neq 0$. On the other hand, if $q = 0$ and $r \neq 0$, clearly $qg + r \neq 0$. It follows there there are unique q, r such that $qg + r = 0$.

(d) First, we observe that in the context of (b), if $\mathrm{ord}'(f) = t$, then $\mathrm{ord}'(q), \mathrm{ord}'(r) \geq t$. This is clear in the setting of (a), and following the proof of (b), we just need to observe that if u is a unit in R, then $\mathrm{ord}'(q_0 u^{-1}) \geq \mathrm{ord}'(q_0)$, which is clear since any coefficient of the product $q_0 u^{-1}$ is a sum of multiples of the coefficients of q_0.

Now we begin the main proof. Write $g_- = \sum_{i=0}^{t-1} a_i X_n^i$ and $g_+ = \sum_{i=t}^{\infty} a_i X_n^i$. Apply (b) with g_+ to write $f = q_0 g_+ + r_0$, and set $f_1 = f - (q_0 g + r_0) = -q_0 g_-$. Repeat with f_1 to write $f_1 = q_1 g_+ + r_1$, and $f_2 = f_1 - (q_1 g + r_1) = -q_1 g_-$. Continue like so to obtain a sequence of series $q_0, q_1, \ldots$ and $r_0, r_1, \ldots$. From the observation above, we have that $\mathrm{ord}'(q_i), \mathrm{ord}'(r_i) \geq \mathrm{ord}'(f_i) \geq \mathrm{ord}'(q_{i_1}) + 1$, since the constant term of each coefficient of g_- vanishes. It follows that $\mathrm{ord}'(q_i), \mathrm{ord}'(r_i) \geq i$ for each i.

For a series h, write $[h]_i$ for the degree i part of h, and $[h]_{\leq i}$ for the sum of all parts of degree $\leq i$. Define q to be the series such that $[q]_i = \sum_{j=0}^{i} [q_j]_i$, and likewise with r. Note that r is a still a polynomial in X_n of top degree less than d. We claim that $f = qg + r$. To show this, it suffices to show that $[f]_i = [qg + r]_i$. Note that to compute $[qg + r]_i$, we can replace q, g, r by $[q]_{\leq i}$, and similarly for the others. But $[q]_{\leq i} = [\sum_{j=0}^{i} q_j]_{\leq i}$ (and likewise with r), so $[qg + r]_i = [(\sum_{j=0}^{i} q_j)g + (\sum_{j=0}^{i} r_j)]_i$. Then, by construction of the sequences $\{q_i\}, \{r_i\}, \{f_i\}$, we have $[f - (qg + r)]_i = [f_{i+1}]_i$ and since $\mathrm{ord}'(f_{i+1}) \geq i + 1$, we have $[f_{i+1}]_i = 0$. It follows that $f - (qg + r) = 0$; i.e., $f = qg + r$.

§1.3: ALGEBRAS

DEFINITION: Let A be a ring. An **A-algebra** is a ring R equipped with a ring homomorphism $\phi : A \to R$; we call ϕ the **structure morphism** of the algebra[1]. A **homomorphism** of A-algebras is a ring homomorphism that is compatible with the structure morphisms; i.e., if $\phi : A \to R$ and $\psi : A \to S$ are A-algebras, then $\alpha : R \to S$ is an A-algebra homomorphism if $\alpha \circ \phi = \psi$.

UNIVERSAL PROPERTY OF POLYNOMIAL RINGS: Let[2] A be a ring, and $T = A[X_1, \ldots, X_n]$ be a polynomial ring. For any A-algebra R, and any collection of elements $r_1, \ldots, r_n \in R$, there is a unique A-algebra homomorphism $\alpha : T \to R$ such that $\alpha(X_i) = r_i$.

DEFINITION: Let A be a ring, and R be an A-algebra. Let S be a subset of R. The **subalgebra generated by** S, denoted $A[S]$, is the smallest A-subalgebra of R containing S. Equivalently[3],

$$A[r_1, \ldots, r_n] = \left\{ \sum_{\text{finite}} a r_1^{d_1} \cdots r_n^{d_n} \mid a \in \phi(A) \right\}.$$

DEFINITION: Let R be an A-algebra. Let $r_1, \ldots, r_n \in R$. The ideal of **A-algebraic relations** on $r_1, \ldots, r_n$ is the set of polynomials $f(X_1, \ldots, X_n) \in A[X_1, \ldots, X_n]$ such that $f(r_1, \ldots, r_n) = 0$ in R. Equivalently, the ideal of A-algebraic relations on $r_1, \ldots, r_n$ is the kernel of the homomorphism $\alpha : A[X_1, \ldots, X_n] \to R$ given by $\alpha(X_i) = r_i$. We say that a set of elements in an A-algebra is **algebraically independent over** A if it has no nonzero A-algebraic relations.

DEFINITION: A **presentation** of an A-algebra R consists of a set of generators $r_1, \ldots, r_n$ of R as an A-algebra and a set of generators $f_1, \ldots, f_m \in A[X_1, \ldots, X_n]$ for the ideal of A-algebraic relations on $r_1, \ldots, r_n$. We call $f_1, \ldots, f_m$ a set of **defining relations** for R as an A-algebra.

PROPOSITION: If R is an A-algebra, and $f_1, \ldots, f_m$ is a set of defining relations for R as an A-algebra, then $R \cong A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$.

(1) Let R be an A-algebra and $r_1, \ldots, r_n \in R$.
- **(a)** Discuss why the equivalent characterizations in the definition of $A[r_1, \ldots, r_n]$ are equivalent.
- **(b)** Explain why $A[r_1, \ldots, r_n]$ is the image of the A-algebra homomorphism $\alpha : A[X_1, \ldots, X_n] \to R$ such that $\alpha(X_i) = r_i$.
- **(c)** Suppose that $R = A[r_1, \ldots, r_n]$ and let $f_1, \ldots, f_m$ be a set of generators for the kernel of the map α. Explain why $R \cong A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, i.e., why the Proposition above is true.
- **(d)** Suppose that R is generated as an A-algebra by a set S. Let I be an ideal of R. Explain why R/I is generated as an A-algebra by the image of S in R/I.
- **(e)** Let $R = A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, where $A[X_1, \ldots, X_n]$ is a polynomial ring over A. Find a presentation for R.

[1] Note: the same R with different ϕ's yield different A-algebras. Despite this we often say "Let R be an A-algebra" without naming the structure morphism.

[2] This is equally valid for polynomial rings in infinitely many variables $T = A[X_\lambda \mid \lambda \in \Lambda]$ with a tuple of elements of $\{r_\lambda\}_{\lambda \in \Lambda}$ in R in bijection with the variable set. I just wrote this with finitely many variables to keep the notation for getting too overwhelming.

[3] Again written with a finite set just for convenience.

(a) Clearly $\mathrm{im}(\alpha) \subseteq R$ is an A-subalgebra that contains $r_1, \ldots, r_n$, so $A[r_1, \ldots, r_n] \subseteq \mathrm{im}(\alpha)$. On the other hand, since $r_1, \ldots, r_n \in A[r_1, \ldots, r_n]$, we have $\alpha(X_i) \in A[r_1, \ldots, r_n]$, so we can consider α as an A-algebra homomorphism from $A[X_1, \ldots, X_n] \to A[r_1, \ldots, r_n]$, and hence $\mathrm{im}(\alpha) \subseteq A[r_1, \ldots, r_n]$.
(b) This is just another way of thinking about $\mathrm{im}(\alpha)$: $\alpha(\sum a_i X_1^{i_1} \cdots X_n^{i_n}) = \sum \phi(a_i) r_1^{i_1} \cdots r_n^{i_n}$.
(c) This is just the First Isomorphism Theorem applied along with (a).
(d) If $K[\{X_\lambda\}] \to R$ where the variables map to the elements of S is surjective, then composing with the quotient map gives a surjection $K[\{X_\lambda\}] \to R \to R/I$ where the variables map to the images of elements of S.
(e) R is generated by $[X_1], \ldots, [X_n]$, with defining relations $f_1, \ldots, f_m$.

(2) Presentations of some subrings:
(a) Consider the $\mathbb{Z}$-subalgebra of $\mathbb{C}$ generated by $\sqrt{2}$. Write the notation for this ring. Is there a more compact description of the set of elements in this ring? Find a presentation.
(b) Same as (a) with $\sqrt[3]{2}$ instead of $\sqrt{2}$.
(c) Let K be a field, and $T = K[X, Y]$. Come up with a concrete description of the ring $R = K[X^2, XY, Y^2] \subseteq T$, (i.e., describe in simple terms which polynomials are elements of R), and give a presentation as a K-algebra.

(a) $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^2 - 2)$
(b) $\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\} \cong \mathbb{Z}[X]/(X^3 - 2)$.
(c) $K[X^2, XY, Y^2]$ is the collection of polynomials that only have even degree terms. We computed the kernel of the presenting map last time, in slightly different words and letters, and saw that the kernel is generated by $X_2^2 - X_1X_3$.

(3) Infinitely generated algebras:
(a) Show that $\mathbb{Q} = \mathbb{Z}[1/p \mid p \text{ is a prime number}]$.
(b) True or false: It is a direct consequence of the conclusion of (a) and the fact that there are infinitely many primes that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.
(c) Given $p_1, \ldots, p_m$ prime numbers, describe the elements of $\mathbb{Z}[1/p_1, \ldots, 1/p_m]$ in terms of their prime factorizations. Can you ever have $\mathbb{Z}[1/p_1, \ldots, 1/p_m] = \mathbb{Q}$ for a finite set of primes?
(d) Show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-algebra.
(e) Show that, for a field K, the algebra $K[X, XY, XY^2, XY^3, \ldots] \subseteq K[X, Y]$ is not a finitely generated K-algebra.
(f) Show that, for a field K, the algebra $K[X, Y/X, Y/X^2, Y/X^3, \ldots] \subseteq K(X, Y)$ is not a finitely generated K-algebra.

(a) The $\supseteq$ containment is clear. For the other, take $a/b \in \mathbb{Q}$, and write $b = p_1^{e_1} \cdots, p_n^{e_n}$. Then $a/b = a(1/p_1)^{e_1} \cdots (1/p^n)^{e_n}$ exhibits a/b in the right hand side.
(b) False! There could be a different finite generating set.
(c) An element of $\mathbb{Z}[1/p_1, \ldots, 1/p_m]$ can be written as $\sum_\alpha a_\alpha (1/p_1)^{\alpha_1} \cdots (1/p_m)^{\alpha_m}$ so has a denominator that is a product of powers of p_i's. This can never equal $\mathbb{Q}$, since $1/(p_1 \cdots p_m + 1)$ can't be written in this form: if so, and in lowest terms with numerator

a, after clearing denominators we would have $p_1^{\alpha_1} \cdots p_n^{\alpha_n} = (p_1 \cdots p_m + 1)a$, which contradicts the expression in lowest terms.

(d) If $\mathbb{Q} = \mathbb{Z}[a_1/b_1, \ldots, a_n/b_n]$ (in lowest terms) let $p_1, \ldots, p_m$ be the prime factors of $b_1, \ldots, b_n$. Then $\mathbb{Z}[a_1/b_1, \ldots, a_n/b_n] \subseteq \mathbb{Z}[1/p_1, \ldots, 1/p_m]$, so $\mathbb{Z}[1/p_1, \ldots, 1/p_m] = \mathbb{Q}$ contradicting what we just showed.

(e) Suppose otherwise that $K[X, XY, XY^2, XY^3, \ldots] = K[f_1, \ldots, f_n]$. Since each f_i is a polynomial expression of $X, XY, XY^2, XY^3, \ldots$, and there are finitely many XY^j that appear in (fixed expressions for) each of the finitely many f_i, we have $K[X, XY, XY^2, XY^3, \ldots] \subseteq K[f_1, \ldots, f_n] \subseteq K[X, XY, \ldots, XY^m]$ for some m, and equality holds for this same m. We claim that $XY^{m+1} \notin K[X, XY, \ldots, XY^m]$, which will yield the desired contradiction. Indeed, one can see that every monomial in $K[X, XY, \ldots, XY^m]$ has its y-exponent is less than or equal to m times its x-exponent, which is not true of XY^{m+1}. This is the desired contradiction.

(f) Similar to the previous.

(4) More algebras:

(a) Give two different nonisomorphic $\mathbb{C}[X]$-algebra structures on $\mathbb{C}$.

(b) Find a $\mathbb{C}$-algebra generating set for the ring of polynomials in $\mathbb{C}[X, Y]$ that only have terms whose total degree (X-exponent plus Y-exponent) is a multiple of three (e.g., $X^3 + \pi X^5 Y + 5$ is in while $X^3 + \pi X^4 Y + 5$ is out).

(c) Find a $\mathbb{C}$-algebra presentation for $\mathbb{C} \times \mathbb{C}$.

(a) We can write $\mathbb{C} \cong \mathbb{C}[X]/(X)$ or $\mathbb{C} \cong \mathbb{C}[X]/(X-1)$, for example. These are not isomorphic as $\mathbb{C}[X]$-algebras, since such a morphism would send $[0]$ to $[0]$ and $[X]$ to $[X]$, but $[X] = [0]$ in $\mathbb{C}[X]/(X)$ while $[X] = [1]$ in $\mathbb{C}[X]/(X-1)$.

(b) The set X^3, X^2Y, XY^2, Y^3 works. We can write any polynomial in this ring as a sum of monomials of total degree three. From such a monomial, we can factor out powers of X^3 and Y^3 until we get either a constant or X^2Y, or XY^2. Then putting everything back together, we get that any polynomial in our ring is a polynomial expression in the four things we named.

(c) We need a generator for $(1, 0)$; then $(0, 1)$ comes for free as $1 - (1, 0)$, and we're set on generators. Let's map X to $(1, 0)$ for our presentation. Then $X(1 - X)$ maps to $(1, 0)(0, 1) = 0$ so this is in the kernel; one can show with a division argument along the lines of many we've discussed that this generates the kernel.

(5) Let K be a field. Describe which elements are in the K-algebra $K[X, X^{-1}] \subseteq K(X)$, and find an element of $K(X)$ not in $K[X, X^{-1}]$. Then compute[4] a presentation for $K[X, X^{-1}]$ as a K-algebra.

The elements of $K[X, X^{-1}]$ are rational functions that can be written with a power of X as a denominator. The rational function $1/(X-1)$ is not in this algebra.

We claim that $K[X, X^{-1}] \cong K[X_1, X_2]/(X_1X_2 - 1)$. Clearly $X_1X_2 - 1$ is a relation on X and X^{-1}. If it does not generate, take a relation not in the ideal among which has lowest X_2-degree. Let $f(X_1, X_2) = f_n(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1)$ be an algebraic relation,

[4]Hint: Note that Division does not apply. Say $X_1 \mapsto X$ and $X_2 \mapsto Y$. Show that the top X_2-degree coefficient of an algebraic relation is a multiple of X_1, and use this to set an induction on the top X_2-degree.

and consider the top X_2-degree coefficient $f_n(X_1)$ of f. Note that f_n is a multiple of X_1 since, mapping $X_1 \mapsto X$ and $X_2 \mapsto X^{-1}$, we get $f_n(X)X^{-n} + f_{n-1}(X)X^{-n+1} + \cdots + f_0(X) = 0$, so $f_n(X) = X(-f_{n-1}(X) - Xf_{n-2}(X) - \cdots - X^n f_0(X))$. Write $f_n = X_1 f_n'$. Then

$$\begin{aligned} f(X_1, X_2) &= f_n(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1) \\ &= X_1 f_n'(X_1)X_2^n + f_{n-1}(X_1)X_2^{n-1} + \cdots + f_0(X_1) \\ &= (X_1X_2 - 1)f_n'(X_1)X_2^{n-1} + (f_n'(X_1) + f_{n-1})X_2^{n-1} + \cdots + f_0(X_1). \end{aligned}$$

Subtracting off a multiple of $X_1X_2 - 1$, we obtain a relation of lower X_2-degree, contradicting the choice of our relation, and hence the existence of a relation that is not a multiple of $X_1X_2 - 1$.

(6) Can you guess defining relations for the ring in (4b)? Can you prove your guess?

Since $X^3, X^2Y, XY^2, Y^3 \in R$, we have $K[X^3, X^2Y, XY^2, Y^3] \subseteq R$. To show equality, note that we can write $f \in R$ as a sum of monomials of degree a multiple of three, so it suffices to show that any such monomial is in the algebra generated by X^3, X^2Y, XY^2, Y^3. Given X^iY^j, if $i \geq 3$ or $j \geq 3$, we can write $X^iY^j = X^3\mu$ or $Y^3\mu$ with μ a smaller monomial of degree a multiple of three. Continuing like so, we can assume $i, j < 3$, in which case we must have X^2Y or XY^2. Thus, $K[X^3, X^2Y, XY^2, Y^3] = R$.

Now we compute the ideal of relations. We can check directly that each relation is in the defining ideal. To see that they generate, we show that any polynomial in the kernel of the presenting map is equivalent to zero modulo the ideal generated by the given three. Write $T = X_1, U = X_2, V = X_3, W = Y^3$. Given a relation F, we think of it as a polynomial in V. We can use division via $V^2 - UW$ to get rid of the $V^{\geq 2}$ terms, and the other relations to rewrite the coefficient of the V^1 term as a polynomial in W alone, so $F \equiv f_1(W)V + f_0(T, U, W)$. Then we have $f_1(Y^3)XY^2 + f_0(X^3, X^2Y, Y^3) = 0$. The first term only produces Y^1-terms, while the second produces only other powers of Y, so the two parts must be zero. This implies that f_1 is the zero polynomial, and that f_0 is a relation on X^3, X^2Y, Y^3. A similar division argument shows that any polynomial in T, U, W that vanishes upon mapping $T \mapsto X^3$, $U \mapsto X^2Y$, $W \mapsto Y^3$ is a multiple of $U^3 - T^2W$, but $U^3 - T^2W = U(U^2 - TV) - T(TW - UV)$. This completes the proof.

EXAMPLE: For a ring R, the following are sources of modules:

(1) The free module of n-tuples R^n, or more generally, for a set Λ, the free module
$$R^{\oplus\Lambda} = \{(r_\lambda)_{\lambda\in\Lambda} \mid r_\lambda \neq 0 \text{ for at most finitely many } \lambda \in \Lambda\}.$$
(2) Every ideal $I \subseteq R$ is a submodule of R.
(3) Every quotient ring R/I is a quotient module of R.
(4) If S is an R-algebra, (i.e., there is a ring homomorphism $\alpha : R \to S$), then S is an R-module by **restriction of scalars**: $r \cdot s := \alpha(r)s$.
(5) More generally, if S is an R-algebra and M is an S-module, then M is also an R-module by **restriction of scalars**: $r \cdot m := \alpha(r) \cdot m$.
(6) Given an R-module M and $m_1, \ldots, m_n \in M$, the **module of R-linear relations** on $m_1, \ldots, m_n$ is the set of n-tuples $[r_1, \ldots, r_n]^{\text{tr}} \in R^n$ such that $\sum_i r_i m_i = 0$ in R.

DEFINITION: Let M be an R-module. Let S be a subset of M. The **submodule generated by** S, denoted[1] $\sum_{m\in S} Rm$, is the smallest R-submodule of M containing S. Equivalently,

$$\sum_{m\in S} Rm = \Big\{ \sum r_i m_i \mid r_i \in R, m_i \in S \Big\} \quad \text{is the set of } R\text{-linear combinations of elements of } S.$$

We say that S **generates** M if $M = \sum_{m\in S} Rm$.

DEFINITION: A[2] **presentation** of an R-algebra M consists of a set of generators $m_1, \ldots, m_n$ of M as an R-module and a set of generators $v_1, \ldots, v_m \in R^n$ for the submodule of R-linear relations on $m_1, \ldots, m_n$. We call the $n \times m$ matrix with columns $v_1, \ldots, v_m$ a **presentation matrix** for M.

LEMMA: If M is an R-module, and A an $n \times m$ presentation matrix[3] for M, then $M \cong R^n/\text{im}(A)$. We call the module $R^n/\text{im}(A)$ the **cokernel** of the matrix A.

(1) Let M be an R-module and $m_1, \ldots, m_n \in M$.
- **(a)** Briefly explain why the characterizations of the submodule generated by S are equivalent.
- **(b)** Briefly explain why $\sum_i Rm_i$ is the image of the R-module homomorphism $\beta : R^n \to M$ such[4] that $\beta(e_i) = m_i$.
- **(c)** Let I be an ideal of R. How does a generating set of I as an ideal compare to a generating set of I as an R-module?
- **(d)** Explain why the Lemma above is true.
- **(e)** If M has an $a \times b$ presentation matrix A, how many generators and how many (generating) relations are in the presentation corresponding to A?
- **(f)** What is a presentation matrix for a free module?

(a) ($\subseteq$) : The elements of the form $\sum r_i m_i$ form a submodule of M that contains S. ($\supseteq$) : A submodule that contains S must also contain the elements of the form $\sum r_i m_i$.

[1] If $S = \{m\}$ is a singleton, we just write Rm, and if $S = \{m_1, \ldots, m_n\}$, we may write $\sum_i Rm_i$.
[2] As written, there is a finite set of generators, and a finite set of generators for their relations. This is called a **finite presentation**. One could do the same thing with an infinite generating set and/or infinite generating set for the relations.
[3] $\text{im}(A)$ denotes the **image** or column space of A in R^n. This is equal to the module generated by the columns of A.
[4] where e_i is the vector with ith entry one and all other entries zero.

(b) This is just unpackaging $\mathrm{im}(\beta)$: $\beta((r_1,\ldots,r_n)) = \beta(\sum_i r_i e_i) = \sum_i r_i m_i$.
(c) They are the same.
(d) Follows from (b) and First Isomorphism Theorem.
(e) There are a generators and b relations.
(f) A matrix is free if and only if it has zero presentation matrix.

(2) Describe $\mathbb{Z}[\sqrt{2}]$ as a $\mathbb{Z}$-module.

$Z[\sqrt{2}]$ is a free $\mathbb{Z}$-module with basis $1, \sqrt{2}$.

(3) Module structure for polynomial rings and quotients:
- **(a)** Let $R = A[X]$ be a polynomial ring. Give a generating set for R as an A-module. Is R a free A-module?
- **(b)** Let $R = A[X,Y]$ be a polynomial ring. Give a generating set for R as an A-module. Is R a free A-module?
- **(c)** Let $R = A[X]/(f)$, where f is a monic polynomial of top degree d. Apply the Division Algorithm to show that R is a free A-module with basis $[1],[X],\ldots,[X^{d-1}]$.
- **(d)** Let $R = \mathbb{C}[X,Y]/(Y^3 - iXY + 7X^4)$. Describe R as a $\mathbb{C}[X]$-module, and then give a $\mathbb{C}$-vector space basis.

(a) R is free on basis $1, X, X^2, \ldots$.
(b) R is free on basis $1, X, X^2, \ldots, Y, XY, XY^2, \ldots, Y^2, XY^2, X^2Y^2, \ldots\ldots$.
(c) We need to show that any $[g] \in R$ has a unique expression as an A-linear combination of $[1],\ldots,[X^{d-1}]$. Given $[g]$, take a represenatative g; use the division algorithm to write $g = qf + r$ with top deg r ¡ d. Thus $[g] = [r]$, and since $r \in A1 + AX + \cdots + AX^{d-1}$, $[g] = [r] \in A[1] + \cdots + A[X^{d-1}]$. For uniqueness, it suffices to show linear independence of $[1],\ldots,[X^{d-1}]$; a nontrivial relation would yield a multiple of f in $A[X]$ of degree less than d, which cannot happen.
(d) R is free over $\mathbb{C}[X]$ on $[1],[Y],[Y^2]$. It has as a vector space basis $\{[X^iY^j] \mid i \geq 0, j \in \{0,1,2\}.\}$.

(4) Let $R = \mathbb{C}[X]$ and $S = \mathbb{C}[X,X^{-1}] \subseteq \mathbb{C}(X)$. Find a generating set for S as an R-module. Does there exist a finite generating set for S as an R-module? Is S a free R-module?

S is generated by $\{1/X^n \mid n \geq 0\}$. S cannot be generated by a finite set: if $S = Rf_1 + \cdots + Rf_n$, among $f_1,\ldots,f_n$ there is a largest power of X in the denominator, say m. Then $S \subseteq R\frac{1}{X^m}$, but $\frac{1}{X^{m+1}} \in S \setminus R\frac{1}{X^m}$. S is not free: if it were, there would be a basis element s, and $s \notin xS$, as this would lead to a nontrivial relation with other basis elements, but $S = xS$, so this is impossible.

(5) Presentations of modules: Let K be a field, and $R = K[X,Y]$ be a polynomial ring.
- (a) Consider the quotient ring $K \cong R/(X,Y)$ as an R-module. Find a presentation for K as an R-module.
- (b) Consider the ideal $I = (X,Y)$ as an R-module. Find a presentation for I as an R-module.
- (c) Consider the ideal $J = (X^2, XY, Y^2)$ as an R-module. Find a presentation for J as an R-module.

(a) $[1]$ generates K, and X, Y are the defining relations. So, a presentation matrix is $[X, Y]$.
(b) A generating set is $\{X, Y\}$. To find the relations, suppose that $fX + gY = 0$. Then $fX = -gY$. Writing out $f, -g$ in terms of monomials, one sees that $-g$ must be a multiple of X and f must be a multiple of Y so $f = hY, -g = jX$. Then $hXY = jXY$, so $j = h$. Thus, the relation $\begin{bmatrix} f \\ g \end{bmatrix}$ can be written as $h \begin{bmatrix} Y \\ -X \end{bmatrix}$. A defining relation (and hence the presentation matrix) is $\begin{bmatrix} Y \\ -X \end{bmatrix}$.
(c) A generating set is $\{X^2, XY, Y^2\}$. We have relations $\begin{bmatrix} Y \\ -X \\ 0 \end{bmatrix}$ and $\begin{bmatrix} 0 \\ Y \\ -X \end{bmatrix}$ corresponding to $Y(X^2) - X(XY) = 0$ and $Y(XY) - X(Y^2) = 0$. We claim that these generate. Suppose that $aX^2+bXY+CY^2 = 0$; we want to show that $\begin{bmatrix} a \\ b \\ c \end{bmatrix} \in \operatorname{im} \begin{bmatrix} Y & 0 \\ -X & Y \\ 0 & -X \end{bmatrix}$. We can write $a = a'Y + a''$ with $a'' \in K[X]$ and subtracting $a' \begin{bmatrix} Y \\ -X \\ 0 \end{bmatrix}$, we obtain a relation with $a \in K[X]$; similarly, we can assume $c \in K[Y]$. Then plugging in $a(X)X^2 + b(X, Y)XY + c(Y)Y^2$, since each sum has no possible monomials in common, we must have $a = b = c = 0$. This shows the claim.

(6) Let M be an R-module, $S \subseteq M$ a generating set, and $r \in R$. Show that $rM = 0$ if and only if $rm = 0$ for all $m \in S$.

The forward direction is clear. For the other, writing $m = \sum_i r_i m_i$ with $m_i \in S$, if $rm_i = 0$, then $rm = 0$.

(7) Let K be a field, $S = K[X, Y]$ be a polynomial ring, and $R = K[X^2, XY, Y^2] \subseteq S$. Find an R-module M such that $S = R \oplus M$ as R-modules. Given a presentations for S and M as R-modules.

We can take M to be the collection of polynomials all of whose terms have odd degree. Note that M is indeed closed under multiplication by R. A presentation matrix for M is $\begin{bmatrix} XY & Y^2 \\ -X^2 & -XY \end{bmatrix}$ and for S is $\begin{bmatrix} 0 & 0 \\ XY & Y^2 \\ -X^2 & -XY \end{bmatrix}$.

(8) Messing with presentation matrices: Let M be a module with an $n \times m$ presentation matrix A.
(a) If you add a column of zeroes to A, how does M change?
(b) If you add a row of zeroes to A, how does M change?
(c) If you add a row and column to A, with a 1 in the corner and zeroes elsewhere in the new row and column, how does M change?
(d) If A is a block matrix $\begin{bmatrix} B & 0 \\ 0 & C \end{bmatrix}$, what does this say about M?

(a) It doesn't.
(b) Corresponds to adding a free copy of R as a direct sum.
(c) It doesn't.
(d) $M \cong \operatorname{coker}(B) \oplus \operatorname{coker}(C)$

§1.5: DETERMINANTS

Recall that given matrices A and B, the matrix product AB consists of linear combinations, namely: Each column of AB is a linear combinations of the columns of A, with coefficients/weights coming from the corresponding columns of B. That is,

$$\big(\text{col } j \text{ of } AB\big) = \sum_{i=1}^{t} b_{ij} \cdot \big(\text{col } i \text{ of } A\big);$$

note that $b_{1j}, \ldots, b_{tj}$ is the j-th column of B.

PROPERTIES OF $\det$: For a ring R, the determinant is a function $\det : \mathrm{Mat}_{n\times n}(R) \to R$ such that:

(1) $\det$ is a polynomial expression of the entries of A of degree n.
(2) $\det$ is a linear function of each column.
(3) $\det(A) = 0$ if the columns are linearly dependent.
(4) $\det(AB) = \det(A)\det(B)$.
(5) $\det$ can be computed by Laplace expansion along a row/column.
(6) $\det(A) = \det(A^{\mathrm{tr}})$.
(7) If $\phi : R \to S$ is a ring homomorphism, and $\phi(A)$ is the matrix obtained from A by applying ϕ to each entry, then $\det(\phi(A)) = \phi(\det(A))$.

ADJOINT TRICK: For an $n \times n$ matrix A over R,

$$\det(A)\mathbb{1}_n = A^{\mathrm{adj}}A = A\,A^{\mathrm{adj}},$$

where $(A^{\mathrm{adj}})_{ij} = (-1)^{i+j}\det(\text{matrix obtained from } A \text{ by removing row } j \text{ and column } i)$.

EIGENVECTOR TRICK: Let A be an $n \times n$ matrix, $v \in R^n$, and $r \in R$. If $Av = rv$, then $\det(r\mathbb{1}_n - A)v = 0$. Likewise, if instead v is a row vector and $vA = rv$, then $\det(r\mathbb{1}_n - A)v = 0$.

DEFINITION: Given an $n \times m$ matrix A and $1 \leq t \leq \min\{m, n\}$ the **ideal of $t \times t$ minors of** A, denoted $I_t(A)$, is the ideal generated by the determinants of all $t \times t$ submatrices of A given by choosing t rows and t columns. For $t = 0$, we set $I_0(A) = R$ and for $t > \min\{m, n\}$ we set $I_t(A) = 0$.

LEMMA: If A is an $n \times m$ matrix, B is an $m \times \ell$ matrix, and $t \leq 1$, then

- $I_{t+1}(A) \subseteq I_t(A)$
- $I_t(AB) \subseteq I_t(A) \cap I_t(B)$.

PROPOSITION: Let M be a finitely presented module. Suppose that A is an $n \times m$ presentation matrix for M. Then $I_n(A)M = 0$. Conversely, if $fM = 0$, then $f \in I_n(A)^n$.

(1) Let M be a module. Suppose that $m_1, \ldots, m_n$ is a generating set with corresponding presentation matrix A. Which of the following is true:

$$A \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} \stackrel{?}{=} 0 \qquad\qquad \begin{bmatrix} m_1 & \cdots & m_n \end{bmatrix} A \stackrel{?}{=} 0.$$

Explain your answer in terms of the recollection on matrix multiplication above.

The second one!

(2) Eigenvector Trick:

(a) What familiar fact/facts from linear algebra (over fields) is/are related to the Eigenvector Trick?

(b) Use the Adjoint Trick to prove the Eigenvector Trick.

(a) Over a field, an eigenvalue of a matrix is a root of the characteristic polynomial.

(b) If $Av = rv$, then $(A - r\mathbb{1}_n)v = 0$, so multiply by $(A - r\mathbb{1}_n)^{\text{adj}}$ to get $\det(A - r\mathbb{1}_n)v = (A - r\mathbb{1}_n)^{\text{adj}}(A - r\mathbb{1}_n)v = 0$. Likewise on the other side.

(3) Show that a square matrix over a ring R is invertible if and only if its determinant is a unit.

If $AB = \mathbb{1}_n$, then $\det(A)\det(B) = \det(\mathbb{1}_n) = 1$, so $\det(A)$ is a unit. On the other hand, if $\det(A)$ is a unit, then $B = \det(A)^{-1}A^{\text{adj}}$ is an inverse of A by the adjoint trick.

(4) Proof of Proposition:

(a) First consider the case $m = n$. Show that $\det(A)$ kills each generator m_i, and conclude that $I_n(A)M = 0$.

(b) Now consider the case $n \leq m$. Show that for any $n \times n$ submatrix A' of A that $\det(A')M = 0$, and conclude that $I_n(A)M = 0$. What's the deal when $m < n$?

(c) For the "conversely" statement, show that if $fM = 0$ then there is some matrix B such that $AB = f\mathbb{1}_n$, and deduce that $f \in I_n(A)^n$.

(a) Since A is a presentation matrix for M, with the corresponding generating set $m_1, \ldots, m_n$, we have $\begin{bmatrix} m_1 & \ldots & m_n \end{bmatrix} A = 0$. By the adjoint trick, $\det(A) \begin{bmatrix} m_1 & \ldots & m_n \end{bmatrix} = 0$, so $\det(A)$ kills each generator of M. Thus, $\det(A)$ kills M. By definition $I_n(A) = (\det(A))$, so we are done.

(b) Suppose $n \leq m$ and fix m columns of A to form an $n \times n$ submatrix A'. The columns of A' are still relations on $m_1, \ldots, m_n$, so the same argument shows that $\det(A')$ kills M. Now, by definition, $I_n(A)$ is generated by the determinants of the submatrices A', so $I_n(A)M = 0$.
When $m < n$, $I_n(A) = 0$, which very much kills M.

(c) If $fM = 0$, then the vector with f in the ith entry and zeroes elsewhere is a relation on the generators, so by definition of presentation matrix, this vector is a linear combination of the columns of A. Thus each column $f\mathbb{1}_n$ is a linear combination of the columns of A, which means that we can write $f\mathbb{1}_n = AB$ for some matrix B following the discussion above. By the Lemma, we have $f^n = \det(f\mathbb{1}_n) \in I_n(AB) \subseteq I_n(A)$. This completes the proof.

(5) Prove the Lemma above.

The first statement follows from Laplace expansion. For the second, it suffices to show that the determinant of any $t \times t$ submatrix of AB is a linear combination of determinants of $t \times t$ submatrices of A; the claim for B follows by applying transposes. We can restrict to the relevant rows of A and columns of B, so we can assume that A is $t \times n$ and B is $n \times t$ for some $n \geq t$. Then AB is a matrix whose columns are linear combinations of the columns of A. Then using linearity of $\det$ in each column, we can write $\det(AB)$ as a linear combination of the determinants of matrices with columns from A, which shown the claim.

(6) Prove[1] FITTING'S LEMMA: If A and B are presentation matrices for the same R-module M of size $n \times m$ and $n' \times m'$ (respectively), and $t \geq 0$, then $I_{n-t}(A) = I_{n'-t}(B)$.

[1]Hint: First consider the case when the two presentations have the same generating sets, but different generating sets for the relations. Reduce to the case where $B = [A|v]$ for a single column v.

§2.6: ALGEBRA-FINITE AND MODULE-FINITE EXTENSIONS

DEFINITION: Let $\phi : R \to S$ be a ring homomorphism.

- We say that ϕ is **algebra-finite**, or S is **algebra-finite** over R, if S is a finitely generated R-algebra.
- We say that ϕ is **module-finite**, or S is **module-finite** over R, if S is a finitely generated R-module.

One also often encounters the less self-explanatory terms **finite type** for algebra-finite, and **finite** for module-finite, but we will avoid these.

LEMMA: A module-finite map is algebra-finite. The converse is false.

DEFINITION: Let R be an A-algebra. We say that an element $r \in R$ is **integral** over A if r satisfies a monic polynomial with coefficients in A.

PROPOSITION: Let R be an A-algebra. If $r_1, \ldots, r_n \in R$ are integral over A, then $A[r_1, \ldots, r_n]$ is module-finite over A.

(1) Algebra-finite vs module-finite: Let $\phi : A \to R$ be a ring homomorphism and $r_1, \ldots, r_n \in R$.
- **(a)** Agree or disagree: an A-linear combination of $r_1, \ldots, r_n$ is a special type of polynomial expression of $r_1, \ldots, r_n$ with coefficients in A.
- **(b)** Explain why $R = \sum_{i=1}^{n} Ar_i$ implies $R = A[r_1, \ldots, r_n]$. Explain why module-finite implies algebra-finite.
- **(c)** Let $R = A[X]$ be a polynomial ring in one variable over A. Is the inclusion map $A \subseteq A[X]$ algebra-finite? Module-finite?
- **(d)** Give an example of a map that is module-finite (and hence also algebra-finite).
- **(e)** Give an example of a map that is not algebra-finite (and hence also not module-finite).

- **(a)** Agree.
- **(b)** The first part follows from what you just agreed to.
- **(c)** Algebra-finite but not module-finite.
- **(d)** Possibilities include $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{2}]$, $\mathbb{R} \subseteq \mathbb{C}$
- **(e)** Possibilities include $\mathbb{Z} \subseteq \mathbb{Q}$, $K \subseteq K[X_1, X_2, \ldots]$.

(2) Integral elements: Use the definition of integral to determine whether each is integral or not.
- **(a)** An indeterminate X in a polynomial ring $A[X]$, over A.
- **(b)** $\sqrt[3]{2}$, over $\mathbb{Z}$.
- **(c)** $\frac{1}{2}$, over $\mathbb{Z}$.

- **(a)** No: X satisfies no polynomial over A.
- **(b)** Yes: $\sqrt[3]{2}$ is a root of $T^3 - 2$.
- **(c)** No: given $T^n + a_1 T^{n-1} + \cdots + a_n = 0$ with $a_i \in \mathbb{Z}$, plugging in $T = 1/2$ and clearing denominators gives $1 + 2a_1 + \cdots + 2^n a_n = 0$, which is impossible.

(3) Proof of Proposition: Let A be a ring.
- **(a)** Let $f \in A[X]$ be monic, and let $T = A[X]/(f)$. Explain why T is module-finite over A. What is a generating set?
- **(b)** Let $R = A[r]$ be an algebra generated by one element $r \in R$. Suppose that r satisfies a monic polynomial $f \in A[X]$. How is R related to the ring T as in part (a)? Must they be equal?
- **(c)** Show that R as in (b) is module-finite over A. What is a generating set?

(d) Let $S = A[r_1, \ldots, r_t]$ with $r_1, \ldots, r_t \in S$ integral over A. Use (c) and (4b) below to show that $A \to S$ is module-finite.

(a) We showed earlier that T is a free A-module with basis given by powers of $[X]$ of degree less than the top degree of f.
(b) R is a quotient of T, but could be smaller (a proper quotient). For example, take $R = \mathbb{Z}[X]/(X^2, 2X)$.
(c) It is generates by the powers of $[X]$ of degree than the top degree of f.
(d) This follows from (c), 2(b), and induction.

(4) Finiteness conditions and compositions: Let $R \subseteq S \subseteq T$ be rings.
(a) If $R \subseteq S$ and $S \subseteq T$ are algebra-finite, show[1] that the composition $R \subseteq T$ is algebra-finite.
(b) If $R \subseteq S$ and $S \subseteq T$ are module-finite, show[2] that the composition $R \subseteq T$ is module-finite.

(a) If $S = R[s_1, \ldots, s_m]$ and $T = S[t_1, \ldots, t_n]$. We claim that $T = R[s_1, \ldots, s_m, t_1, \ldots, t_n]$. Suppose that $T' \subseteq T$ is an R-subalgebra containing $s_1, \ldots, s_m, t_1, \ldots, t_n$. Since $s_1, \ldots, s_m \in T'$, we have $S \subseteq T'$ so T' is a S-subalgebra of T. But since $t_1, \ldots, t_n \in T'$ we then must have $T' = T$.
(b) If $S = \sum_i Ra_i$ and $T = \sum_j Sb_j$, we claim that $T = \sum_{i,j} Ra_ib_j$. Indeed, given $t \in T$, we can write $t = \sum_j s_jb_j$, and for each s_j we can write $s_j = \sum_i r_{i,j}a_i$, so $t = \sum_j(\sum_i r_{i,j}a_i)b_j$ is an R-linear combination of a_ib_j.

(5) Power series rings:
(a) Let $A \to R$ be algebra-finite. Show that R is a countably-generated A-module.
(b) Let A be a ring and $R = A[\![X]\!]$ be a power series ring over A. Show[3] that R is not a countably generated A-module. Deduce that R is not algebra-finite over A.

(a) If $R = A[X_1, \ldots, X_n]$, then R is a free A-module on basis given by monomials. This is a countable set, so R is a countably-generated A-module. In the general case of $A \to R$ be algebra-finite, R is a quotient of a polynomial ring in finitely many variable, so R is a countably-generated A-module.
(b) Suppose $R = \sum_{i=1}^{\infty} Af_i$ is countably generated. Write $[g]_{\leq j}$ for the sum of terms in g of degree at most j and similar things.
We claim that there is some $g \in R$ such that $[g]_{\leq n^2} \notin \sum_{i=1}^{n} A[f_i]_{\leq n^2}$. We construct such g recursively. Suppose we have such a g that satisfies the condition some n. We need to show that there are coefficients $a_{n^2+1}, \ldots, a_{(n+1)^2}$ such that $[g]_{\leq (n+1)^2} \notin \sum_{i=1}^{n+1} A[f_i]_{\leq (n+1)^2}$; we will choose these coefficients with the stronger property that $[g]_{>n\&\leq (n+1)^2} \notin \sum_{i=1}^{n+1} A[f_i]_{>n\&\leq (n+1)^2}$. To do this, just note that $\sum_{i=1}^{n+1} A[f_i]_{>n\&\leq (n+1)^2}$ is a submodule of A^{2n+1} with $n+1$ generators, so is a proper submodule; choose any element of the complement. Thus there exists a g as claimed.

[1]Hint: If $S = R[s_1, \ldots, s_m]$ and $T = S[t_1, \ldots, t_n]$, apply the definition of "algebra generated by" to $R[s_1, \ldots, s_m, t_1, \ldots, t_n] \subseteq T$. Why must the LHS contain S? After that, why must it contain T?
[2]Hint: If $S = \sum_i Rs_i$ and $T = \sum_j St_j$, use the "linear combinations" characterization of module generators to show $T = \sum_{i,j} Rs_it_j$.
[3]Hint: Write $[g]_{\leq j}$ for the sum of terms in g of degree at most j. Suppose $R = \sum_{i=1}^{\infty} Af_i$, and construct $g \in R$ such that $[g]_{\leq n^2} \notin \sum_{i=1}^{n} A[f_i]_{\leq n^2}$.

But then $g \notin \sum_{i=1}^{\infty} Af_i$, since if it were, g would be an A-linear combination of finitely many such f_i, so $g \in \sum_{i=1}^{N} Af_i$ for some N, and hence $[g]_{\leq N^2} \in \sum_{i=1}^{N} A[f_i]_{\leq N^2}$, a contradiction.
It follows from (1) that R is not a finitely-generated A-algebra.

(6) Let $R \subseteq S \subseteq T$ be rings.
   (a) If $R \subseteq T$ is algebra-finite, must $S \subseteq T$ be? What about $R \subseteq S$?
   (b) If $R \subseteq T$ is module-finite, must $S \subseteq T$ be? What[4] about $R \subseteq S$?

   (a) $S \subseteq T$ must be, as following immediately from the definition. $R \subseteq S$ need not, e.g., for $K[X] \subseteq K[X, XY, XY^2, \cdots] \subseteq K[X, Y]$.
   (b) $S \subseteq T$ must be, as following immediately from the definition. $R \subseteq S$ need not, e.g., for $K[X_1, X_2, \dots] \subseteq K[X_1, X_2, \dots] \ltimes (X_1, X_2, \dots) \subseteq K[X_1, X_2, \dots] \ltimes K[X_1, X_2, \dots]$.

(7) Let R be a ring, and M be an R-module. The **Nagata idealization** of M in R, denoted $R \ltimes M$, is the ring that
   - as a set and an additive group is just $R \times M = \{(r, m) \mid r \in R, m \in M\}$, and
   - has multiplication $(r, m)(s, n) = (rs, rn + sm)$.

   Convince yourself that $R \ltimes M$ is an R-algebra. Show that $R \subseteq R \ltimes M$ is module-finite if and only if M is a finitely generated R-module.

[4] Hint: Use a problem below.

§2.7: INTEGRAL EXTENSIONS

DEFINITION: Let $\phi : A \to R$ be a ring homomorphism. We say that ϕ is **integral** or that R is **integral over** A if every element of R is integral over A.

THEOREM: A homomorphism $\phi : A \to R$ is module-finite if and only if it is algebra-finite and integral. In particular, every module-finite extension is integral.

COROLLARY 1: An algebra generated (as an algebra) by integral elements is integral.

COROLLARY 2: If $R \subseteq S$ is integral, and x is integral over S, then x is integral over R.

PROPOSITION: Let $R \subseteq S$ be an integral extension of domains. Then R is a field if and only if S is a field.

DEFINITION: Let A be a ring, and R be an A-algebra. The **integral closure** of A in R is the set of elements in R that are integral over A.

(1) Proof of Theorem:

(a) Very briefly explain why, to prove that module-finite implies integral in general, it suffices to show the claim for an inclusion $A \subseteq R$.

(b) Take a module generating set $\{1, r_2, \ldots, r_n\}$ for R as an A-module, and write it as a row vector $v = \begin{bmatrix} 1 & r_2 & \cdots & r_n \end{bmatrix}$. Let $x \in R$. Explain why there is a matrix $M \in \mathrm{Mat}_{n\times n}(A)$ such that $vM = xv$.

(c) Apply a TRICK to obtain a monic polynomial over A that x satisfies.

(d) Combine the previous parts with results from last time to complete the proof of the Theorem.

(a) You can replace A by $\phi(A)$ for both.

(b) $xr_i \in R$ for each i, so each xr_i is an A-linear combination of $1, r_2, \ldots, r_n$. We can write these linear combinations using matrix multiplication.

(c) The eigenvector trick implies that $\det(M - x\mathbb{1}_n)$ kills v; since 1 is an entry of v, $\det(M - x\mathbb{1}_n) = 0$, so x is a root of the polynomial $\det(M - X\mathbb{1}_n) = 0$, which is monic.

(d) The previous part shows that module-finite implies integral. We already saw that module-finite implies algebra-finite. Also, if $R = A[r_1, \ldots, r_m]$ and R is integral over A, then each r_i is integral over R. We saw last time that R as above is module-finite over A.

(2) Let $R = \mathbb{C}[X, X^{1/2}, X^{1/3}, \ldots] \subseteq \overline{\mathbb{C}(X)}$, where $X^{1/n}$ is an nth root of X. Is $\mathbb{C}[X] \subseteq R$ integral[1]? Is it module-finite? Is it algebra-finite?

Each algebra generator $X^{1/n}$ satisfies a polynomial $T^n - X = 0$, so is integral over $\mathbb{C}[X]$. By the Corollary, R is integral over $\mathbb{C}[X]$. It is not algebra-finite or module-finite. The argument is similar to examples we have done before: if it was, it would be generated by a finite subset of $\{X^{1/n}\}$, but there would then be a largest denominator on the powers of X.

(3) Proof of Corollary 1: Let R be an A-algebra.

(a) If $x, y \in R$ are integral over A, explain why $A[x, y] \subseteq R$ is integral over A. Now explain why $x \pm y$ and xy are integral over A.

[1] You might find the Corollary helpful.

(b) Deduce that the integral closure of A in R is a ring, and moreover an A-subalgebra of R.
(c) Now let S be a set of integral elements. Apply (b) to the ring $R = A[S]$ in place of R. Complete the proof of the Corollary.

(a) $A[x, y]$ is module-finite over A, and $x \pm y$ and $xy \in A[x, y]$.
(b) This follows from (a) plus the fact that every element of A is obviously integral over A.
(c) The integral closure of A in $A[S]$ is a subalgebra of A that contains S, so by definition of generators must be all of $A[S]$. Thus $A[S]$ is integral over A.

(4) Proof of Proposition:
(a) First, assume that S is a field, and let $r \in R$ be nonzero. Explain why r has an inverse in S.
(b) Take an integral equation for $r^{-1} \in S$ over R, and solve for r^{-1} in terms of things in R. Deduce that R must also be a field.
(c) Now, assume that R is a field, and that S is a domain, and let $s \in S$ be nonzero. Explain why $R[s]$ is a finite-dimensional vector space.
(d) Explain why the multiplication by s map from $R[s]$ to itself is surjective. Deduce that S must also be a field.

(a) Because S is a field.
(b) Take $(r^{-1})^n + r_1(r^{-1})^{n-1} + \cdots + r_n = 0$. Multiplying through, $r^{-1} = -r_1 - r_2 r - \cdots - r_n r^{n-1} \in R$.
(c) $R[s]$ is module-finite over R; for a field, this means finite-dimensional.
(d) Since s is nonzero, and S is a domain, multiplication by s is injective. But this is an R-linear map from $R[s]$ to itself, and since $R[s]$ is a finite-dimensional vector space, this is also surjective. That means that $1 = ss'$ for some s', so s is a unit. Thus, S is also a field.

(5) Prove Corollary 2.

Let $R \subseteq S$ be integral and x be integral over S. Let $x^n + s_1 x^{n-1} + \cdots + s_n = 0$ with $s_i \in S$. Then x is integral over $R[s_1, \ldots, s_n]$, so $R[s_1, \ldots, s_n, x]$ is module-finite over $R[s_1, \ldots, s_n]$. But $R[s_1, \ldots, s_n]$ is module-finite over R, so $R[s_1, \ldots, s_n, x]$ is module-finite over R, and hence integral over R. In particular, x is integral over R.

(6) Let $A = \mathbb{C}[X, Y]$ be a polynomial ring, and $R = \dfrac{\mathbb{C}[X, Y, U, V]}{(U^2 - UX + 3X^3, V^2 - 7Y)}$. Find an equation of integral dependence for $U + V$ over A.

§2.8: UFDs and Normal Rings

DEFINITION: Let R be a domain. The **normalzation** of R is the integral closure of R in $\mathrm{Frac}(R)$. We say that R is **normal** if it is equal to its normalization, i.e., if R is integrally closed in its fraction field.

PROPOSITION: If R is a UFD, then R is normal.

LEMMA: A domain is a UFD if and only if
(1) Every nonzero element has a factorization[1] into irreducibles, and
(2) Every irreducible element generates a prime ideal.

THEOREM: If R is a UFD, then the polynomial ring $R[X]$ is a UFD.

(1) Use the results above to explain why $K[X_1, \ldots, X_n]$ (with K a field) and $\mathbb{Z}[X_1, \ldots, X_n]$ are normal.

Because fields and $\mathbb{Z}$ are UFDs, so $K[X_1, \ldots, X_n]$ and $\mathbb{Z}[X_1, \ldots, X_n]$ are UFDs, hence normal.

(2) Prove the Proposition above.

Let $k = a/b$ be in the fraction field of R written in lowest terms. Suppose that k is integral over R and take an equation $k^n + r_1 k^{n-1} + \cdots + r_n = 0$. Plugging in and clearing denominators gives $a^n + r_1 a^{n-1} b + \cdots + r_n b^n = 0$. Then a^n is a multiple of b, so any irreducible factor of b is an irreducible factor of a by unique factorization. The only possibility is that b admits no irreducible factors; i.e., b is a unit, so $k \in R$.

(3) Let K be a module-finite field extension of $\mathbb{Q}$. The **ring of integers** in K, sometimes denoted $\mathcal{O}_K$, is the integral closure of $\mathbb{Z}$ in K.
(a) What is the ring of integers in $\mathbb{Q}(\sqrt{2})$?
(b) For $L = \mathbb{Q}(\sqrt{-3})$, show that $\frac{1+\sqrt{-3}}{2} \in \mathcal{O}_L$. In particular, $\mathcal{O}_L \supsetneq \mathbb{Z}[\sqrt{-3}]$.
(c) Explain why $\mathcal{O}_K$ is normal.
(d) Explain why, if $\mathbb{Z} \subseteq \mathcal{O}_K$ is algebra-finite, then $\mathcal{O}_K \cong \mathbb{Z}^n$ as abelian groups for some $n \in \mathbb{N}$.
(e) Do we have a theorem that implies $\mathbb{Z} \subseteq \mathcal{O}_K$ is algebra-finite?

(a) $\mathbb{Z}[\sqrt{2}]$.
(b) If $\omega = \frac{1+\sqrt{-3}}{2}$, note that $\omega^2 = \frac{-1+1\sqrt{-3}}{2} = \omega - 1$, so $\omega^2 - \omega + 1 = 0$.
(c) If $k \in K$ is integral over $\mathcal{O}_K$, then k is integral over $\mathcal{O}_K$ and hence over $\mathbb{Z}$ (by Corollary 2 from last time). Then by definition, $k \in \mathcal{O}_K$.
(d) If $\mathbb{Z} \subseteq \mathcal{O}_K$ is algebra-finite, then since it is integral, it is also module-finite. $\mathcal{O}_K$ is definitely torsion free, since it's contained in a field, so by the structure theorem for fg abelian groups, it is isomorphic to a finite number of copies of $\mathbb{Z}$.
(e) Not yet!

(4) Discuss the proof of the Lemma above.

We show by induction on n, that for any element $r \in R$ that can has an irreducible factorization as a unit times a product on n irreducibles (counting repetitions), that any other irreducible

[1] i.e., for any $r \in R$, there exists a unit u and a finite (possibly empty) list of irreducibles $a_1, \ldots, a_n$ such that $r = u a_1 \cdots a_n$.

factorization agrees with the given one up to associates and reordering. If r is a unit, then any factorization only consists of units, since otherwise r is a divisible by prime element, contradicting that it is a unit.

Say that p is an irreducible in the first factorization of r, so $r = ps$ for some s. Then given any irreducible factorization of r, p must divide some irreducible factor since (p) is prime, and by definition, p must be associate to that irreducible. Then we can cancel p from both factorizations and apply the induction hypothesis to s.

(5) Let K be a field, and $R = K[X^2, XY, Y^2] \subseteq K[X, Y]$. Prove[2] that R is *not* a UFD, but R is normal.

This solution is embargoed.

(6) Prove the Theorem above. You might find it useful to recall the following:
GAUSS' LEMMA: Let R be a UFD and let K be the fraction field of R.
   (a) $f \in R[X]$ is irreducible if and only if f is irreducible in $K[X]$ and the coefficients of f have no common factor.
   (b) Let $r \in R$ be irreducible, and $f, g \in R[X]$. If r divides every coefficient of fg, then either r divides every coefficient of f, or r divides every coefficient of g.

(7) Let R be a normal domain, and s be an element of some domain $S \supseteq R$. Let K be the fraction field of R. Show that if s is integral over R, then the minimal polynomial of s has all of its coefficients in R.

[2]Hint: Use $K[X, Y]$ to your advantage.

§2.9: NOETHERIAN RINGS

DEFINITION: A ring R is **Noetherian** if every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ eventually stabilizes: i.e., there is some N such that $I_n = I_N$ for all $n \geq N$.

HILBERT BASIS THEOREM: If R is a Noetherian ring, then the polynomial ring $R[X]$ and power series ring $R[\![X]\!]$ are also Noetherian.

We will return to the proof of Hilbert Basis Theorem after discussing Noetherian modules next time.

COROLLARY: Every finitely generated algebra over a field is Noetherian.

(1) Equivalences for Noetherianity.

(a) Show[1] that R is Noetherian if and only if every ideal is finitely generated.

(b) Show[2] that R is Noetherian if and only if every nonempty collection of ideals has a maximal[3] element.

(a) ($\Leftarrow$) Suppose that every ideal is finitely generated, and take a chain $I_1 \subseteq I_2 \subseteq \cdots$. Consider $I = \bigcup_n I_n$. This is an ideal (it was important that we had a chain, not an arbitrary collection of ideals for this step), and by hypothesis we have $I = (f_1, \ldots, f_m)$. For each i, there is some n_i such that $f_i \in I_{n_i}$. Let $N = \max\{n_i\}$. Then $I = (f_1, \ldots, f_m) \subseteq I_N \subseteq I$, so equality holds, and the chain stabilizes at N.
($\Rightarrow$) Suppose that there is an ideal I that is not finitely generated. Then we construct an infinite chain as follows: let $f_1 \in I \smallsetminus 0$ (0 is finitely generated so $I \neq 0$), and set $I_1 = (f_1)$, and for each n take $f_{n+1} \in I \smallsetminus I_n = (f_1, \ldots, f_n)$, ($I_n$ is finitely generated so $I \neq I_n$).

(b) ($\Leftarrow$) Suppose that every nonempty collection of ideals has a maximal element. Then a chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ is, in particular, a nonempty collection of ideals, hence has a maximal element, say I_n. Then for $n \geq n$, $I_N \subseteq I_n$ and maximality of I_N imply $I_N = I_n$.
($\Rightarrow$) Suppose that there is a nonempty collection of ideals without a maximal element, say $\mathcal{S}$. Let I_1 be any element of $\mathcal{S}$. Then, by definition, there is some I_2 that properly contains I_1, and so on, yielding a chain that does not stabilize.

(2) Some Noetherian rings:

(a) Show that fields and PIDs are Noetherian.

(b) Show that if R is Noetherian and $I \subseteq R$, then R/I is Noetherian.

(c) Is[4] every subring of a Noetherian ring Noetherian?

(a) Every element of a field is generated by no elements; every element of a PID is generated by one element.

(b) The ideals of R/I are in containment-preserving bijection with ideals of R containing I. A chain of ideals in R containing I must stabilize, so the corresponding chain in R/I must stabilize as well.

---

[1] For the backward direction, consider $\bigcup_{n \in \mathbb{N}} I_n$

[2] Hint: For the forward direction, show the contrapositive.

[3] This means that if $\mathcal{S}$ is our collection of ideals, there is some $I \in \mathcal{S}$ such that no $J \in \mathcal{S}$ properly contains I. It does not mean that there is a maximal ideal in $\mathcal{S}$.

[4] Hint: Every domain has a fraction field, even the domain from (4a).

(c) No: $K[X_1, X_2, \dots]$ is not Noetherian, but it is a subring of its fraction field $K(X_1, X_2, \dots)$, which is a field, hence Noetherian.

(3) Use the Hilbert Basis Theorem to deduce the Corollary.

From the Hilbert Basis Theorem and induction, if R is Noetherian, then $R[X_1, \dots, X_n]$ is as well. In particular, if K is a field, then $K[X_1, \dots, X_n]$ is too. Since a finitely generated K-algebra is a quotient of some $K[X_1, \dots, X_n]$, then any such ring is Noetherian as well.

(4) Some nonNoetherian rings:
(a) Let K be a field. Show that $K[X_1, X_2, \dots]$ is not Noetherian.
(b) Let K be a field. Show that $K[X, XY, XY^2, \dots]$ is not Noetherian.
(c) Show that $\mathcal{C}([0, 1], \mathbb{R})$ is not Noetherian.

(a) The ideal $(X_1, X_2, \dots)$ is not finitely generated.
(b) The ideal $(X, XY, \dots)$ is not finitely generated.
(c) The ideal $\sqrt{(x)} = \mathfrak{m}_0$ is not finitely generated.

(5) Let R be a Noetherian ring. Show that for every ideal I, there is some n such that $\sqrt{I}^n \subseteq I$. In particular, there is some n such that for every nilpotent element z, $z^n = 0$.

Let $\sqrt{I} = (f_1, \dots, f_m)$. For each i, there is some n_i such that $f_i^{n_i} \in I$. Then for $n \geq n_1 + \cdots + n_m - m + 1$, any generator $f_1^{a_1} \cdots f_m^{a_m}$ with $\sum a_i = n$ must have $a_j \geq n_j$ for some j, and hence $f_1^{a_1} \cdots f_m^{a_m} \in I$.
For the particular case, we consider $\sqrt{0}$.

(6) Let R be Noetherian. Show that every element of R admits a decomposition into irreducibles.

We argue the contrapositive. Suppose that $r \in R$ does not admit a decomposition into irreducibles. Then in particular, r is reducible, so $r = r_1 r_1'$, with r_1' not a unit, so $(r) \subsetneqq (r_1)$. Likewise, r_1 is reducible, so $r_1 = r_2 r_2'$, with r_2' not a unit, so $(r_1) \subsetneqq (r_2)$. We can continue like this forever to obtain an infinite ascending chain of *principal* ideals even.

(7) Prove the principle of **Noetherian induction**: Let $\mathcal{P}$ be a property of a ring. Suppose that "For every nonzero ideal I, $\mathcal{P}$ is true for R/I implies that $\mathcal{P}$ is true for R" and $\mathcal{P}$ holds for all fields. Then $\mathcal{P}$ is true for every Noetherian ring.

(8) (a) Suppose that every maximal ideal of R is finitely generated. Must R be Noetherian?
(b) Suppose that every ascending chain of prime ideals stabilizes. Must R be Noetherian?
(c) Suppose that every prime ideal of R is finitely generated. Must R be Noetherian?

(a) No. One counterexample is $\mathcal{C}^\infty([0, 1], \mathbb{R})$. Prove it!
Here is another more algebraic example: Let K be a field, and R be the subring of $K(X, Y)$ consisting of elements that can be written as f/g with $f = aX^n + bY$ and $g = uX^n + cY$ for some $n \geq 0$, $a, b, c \in K[X, Y]$, and $u \in K[X, Y]$ with nonzero constant term. I leave it to you to show that

- R is indeed a subring of $K(X, Y)$,
- the ideal (X) is a maximal ideal,
- any $r \in R \setminus (X)$ is a unit, so (X) is the unique maximal ideal, and
- the ideal $(Y, Y/X, Y/X^2, \dots)$ is not finitely generated.

This example is not totally coming from nowhere; see if you can find the train of thought behind it.

(b) No.

(c) Yes.

§2.10: NOETHERIAN MODULES

DEFINITION: A module is **Noetherian** if every ascending chain of submodules $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ eventually stabilizes: i.e., there is some N such that $M_n = M_N$ for all $n \geq N$.

THEOREM: If R is a Noetherian ring, then an R-module M is Noetherian if and only M is finitely generated.

COROLLARY: If R is a Noetherian ring, then a submodule of a finitely generated R-module is finitely generated.

LEMMA: Let M be an R-module and $N \subseteq M$ a submodule. Let L, L' be two more submodules of M. Then $L = L'$ if and only if $L \cap N = L' \cap N$ and $\frac{L+N}{N} = \frac{L'+N}{N}$.

(1) Equivalences for Noetherianity.
- **(a)** Explain why M is Noetherian if and only if every submodule of M is finitely generated.
- **(b)** Explain why M is Noetherian if and only if every nonempty collection of submodules has a maximal element.

- **(a)** Analogous to what we did with ideals.
- **(b)** Analogous to what we did with ideals.

(2) Submodules and quotient modules: Let $N \subseteq M$.
- **(a)** Show that if M is a Noetherian R-module, then N is a Noetherian R-module.
- **(b)** Show that if M is a Noetherian R-module, then M/N is a Noetherian R-module.
- **(c)** Use the Lemma above to show that if N and M/N are Noetherian R-modules, then M is a Noetherian R-module.

- **(a)** A chain of submodules of N is a chain of submodules of M, so by hypothesis must stabilize.
- **(b)** The submodules of M/N are in containment-preserving bijection with the submodules of M that contain N, so a chain of submodules of M/N must stabilize.
- **(c)** Suppose we have a chain of submodules M_i of M. By intersecting with N, we get a chain of submodules of $M_i \cap N$ of N, which by hypothesis, must stabilize at some $n = a$. By taking images in M/N, we get a chain of submodules $\frac{M_i+N}{N}$ of M/N that must stabilize at some $n = b$. Then for $n \geq \max\{a, b\}$ by the Lemma, we must have that the chain M_i stabilizes.

(3) Proof of Theorem: Let R be a Noetherian ring.
- **(a)** Explain why R is a Noetherian R-module.
- **(b)** Show that R^n is a Noetherian R-module for every n.
- **(c)** Deduce the Theorem above.
- **(d)** Deduce the Corollary above.

- **(a)** The submodules of R are just the ideals of R.
- **(b)** There is a copy of R^{n-1} in R^n (where the last coordinate is zero) with quotient R^1, so it follows by induction on n.
- **(c)** If M is Noetherian, then every submodule of M including M itself is finitely generated. Conversely, if M is finitely generated, then M is a quotient of R^n for some n, so it follows from (3b) and (2b).
- **(d)** Follows from (3c) and (2a).

(4) Proof of Hilbert Basis Theorem for $R[X]$: Let R be a Noetherian ring.

(a) Let I be an ideal of $R[X]$. Given a nonzero element $f \in R[X]$, set $\mathrm{LT}(f)$ to be the leading coefficient[1] of f and $\mathrm{LT}(0) = 0$, and let $\mathrm{LT}(I) = \{\mathrm{LT}(f) \mid f \in I\}$. Is $\mathrm{LT}(I)$ an ideal of R?

(b) Let $f_1, \ldots, f_n \in R[X]$ be such that $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_n)$ generate $\mathrm{LT}(I)$. Let N be the maximum of the top degrees of f_i. Show that every element of I can be written as $\sum_i r_i f_i + g$ with $r_i, g \in R[X]$ and the top degree of $g \in I$ is less than N.

(c) Write $R[X]_{<N}$ for the R-submodule of $R[X]$ consisting of polynomials with top degree $< N$. Show that $I \cap R[X]_{<N}$ is a finitely generated R-module.

(d) Complete the proof of the Theorem.

(a) Yes; we just check the definition.

(b) We proceed by induction on top degree of $f \in I$. For f with top degree less than N, we just take $g = f$ and $r_i = 0$. For f with top degree $t \geq N$, write $f = aX^t +$ lower degree terms, and $a = \sum_i a_i \mathrm{LT}(f_i)$. Then $\sum_i a_i X^{t-n_i} f_i = aX^t +$ lower degree terms, so $f' = f - \sum_i a_i X^{t-n_i} f_i \in I$ is of lower degree. We can then write f' in the desired form by induction, and then the original f as well.

(c) $I \cap R[X]_{<N}$ is an R-submodule of $R[X]_{<N}$, which is generated by $1, X, \ldots, X^{N-1}$, whence finitely generated. Since R is Noetherian, this submodule is also Noetherian.

(d) Fix an R-module generating set $g_1, \ldots, g_s$ for $I \cap R[X]_{<N}$. We claim that $I = (f_1, \ldots, f_n, g_1, \ldots, g_s)$. By construction we have $\supseteq$. Then, given $f \in I$, we can write $f = \sum_i r_i f_i + g$ and $g = \sum_j a_j g_j$ with $a_j \in R$, so $f \in (f_1, \ldots, f_n, g_1, \ldots, g_s)$. Thus, I is finitely generated.

(5) Proof of Hilbert Basis Theorem for $R[\![X]\!]$: How can you modify the Proof of Hilbert Basis Theorem for $R[X]$ to work in the power series case? Make it happen!

We use lowest degree terms instead. Define $\mathrm{LT}(f)$ to be the bottom coefficient of f. Proceeding similarly, we can show that if $f_1, \ldots, f_n \in R[\![X]\!]$ are such that $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_n)$ generate $\mathrm{LT}(I)$, then and $f \in I$ can be written as $\sum_i r_i f_i + g$ with g a *polynomial* in X of top degree less than N, and continue as in the polynomial case.

(6) Prove the Lemma.

(7) Noetherianity and module-finite inclusions: Let $R \subseteq S$ be module-finite.

(a) Without using the Hilbert Basis Theorem, show that is R is Noetherian, then S is Noetherian.

(b) EAKIN-NAGATA THEOREM: Show that if S is Noetherian, then R is Noetherian.

[1] That is, if $f = \sum_i a_i X^i$ and $k = \max\{i \mid a_i \neq 0\}$, then $\mathrm{LT}(f) = a_k$.

§3.11: GRADED RINGS

DEFINITION:

(1) An $\mathbb{N}$**-grading** on a ring R is
- a decomposition of R as additive groups $R = \bigoplus_{d \geq 0} R_d$
- such that $x \in R_d$ and $y \in R_e$ implies $xy \in R_{d+e}$.

(2) An $\mathbb{N}$**-graded ring** is a ring with an $\mathbb{N}$-grading.

(3) We say that an element $x \in R$ in an $\mathbb{N}$-graded ring R is **homogeneous** of **degree** d if $x \in R_d$.

(4) The **homogeneous decomposition** of an element $r \neq 0$ in an $\mathbb{N}$-graded ring is the sum

$$r = r_{d_1} + \cdots + r_{d_k} \quad \text{where } r_{d_i} \neq 0 \text{ homogeneous of degree } d_i \text{ and } d_1 < \cdots < d_k.$$

The element r_{d_i} is the **homogeneous component** r **of degree** d_i.

(5) An ideal I in an $\mathbb{N}$-graded ring is **homogeneous** if $r \in I$ implies every homogenous component of r is in I. Equivalently, I is homogeneous if can be generated by homogeneous elements.

(6) A homomorphism $\phi : R \to S$ between $\mathbb{N}$-graded rings is **graded** if $\phi(R_d) \subseteq S_d$ for all $d \in \mathbb{N}$.

DEFINITION: For an abelian semigroup $(G, +)$, one defines G**-grading** as above with G in place of $\mathbb{N}$ and $g \in G$ in place of $d \geq 0$. The other definitions above make sense in this context.

DEFINITION: Let K be a field, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let G be a group acting on R so that for every $g \in G$, $r \mapsto g \cdot r$ is a K-algebra homomorphism. The **ring of invariants** of G is

$$R^G := \{r \in R \mid \text{for all } g \in G,\ g \cdot r = r\}.$$

(1) Basics with graded rings: Let R be an $\mathbb{N}$-graded ring.

(a) If $f \in R$ is homogeneous of degree a and $g \in R$ is homogeneous of degree b, what about $f + g$ and fg?

(b) Translate the definition of graded ring to explain why every nonzero element has a unique homogeneous decomposition.

(c) Does every element in R have a degree? What about "top degree" or "bottom degree"?

(d) What is the[1] degree of zero?

(e) Suppose that $r \in (s_1, \ldots, s_m)$, and r is homogeneous of degree d, and s_i is homogeneous of degree d_i. Explain why we can write $r = \sum_i a_i s_i$ with $a_i \in R$ *homogeneous* of degree $d - d_i$.

(a) $f+g$ is homogeneous if and only if $a = b$, in which case it has degree a; fg is homogeneous of degree $a + b$.

(b) The direct sum decomposition means that every element can be expressed in a unique way as a finite sum of elements from the components.

(c) No; only homogeneous elements have a degree. Any nonzero element has a top degree and a bottom degree.

(d) Zero is homogeneous of every degree, since each R_n is an additive group.

(e) We can write $r = \sum_i b_i s_i$ for some $b_i \in R$. Write $b_i = a_i + c_i$ where a_i is the homogeneous component of degree $d - d_i$ (or zero, if there is none) and c_i is the sum of the other components. Then $r = \sum_i a_i s_i + \sum_i c_i s_i$ where $\sum_i a_i s_i$ has degree d and $\sum_i c_i s_i$ lives entirely in other degrees. By comparing homogeneous components, we must have $\sum_i a_i s_i = r$ (and $\sum_i c_i s_i = 0$).

[1] Hint: This is a trick question, but specify exactly how.

(2) The **standard grading** on a polynomial ring: Let A be a ring.

(a) Let $R = A[X]$. Discuss: the decomposition $R_d = A \cdot X^d$ gives an $\mathbb{N}$-grading on R.

(b) Let $R = A[X_1, \ldots, X_n]$. Discuss: the decomposition

$$R_d = \sum_{d_1+\cdots+d_n=d} A \cdot X_1^{d_1} \cdots X_m^{d_m}$$

gives an $\mathbb{N}$-grading on R. What is the homogeneous decomposition of $f = X_1^3 + 2X_1X_2 - X_3^2 + 3$?

(c) Let $R = A[\![X]\!]$. Explain why $R_n = A \cdot X^n$ *does not* give an $\mathbb{N}$-grading on R.

(a) Agree.
(b) Agree. $f_3 = X_1^3$, $f_2 = 2x_1x_2 - x_3^2$, $f_0 = 3$.
(c) An element must be a finite sum of homogeneous elements.

(3) **Weighted gradings** on polynomial rings: Let A be a ring, $R = A[X_1, \ldots, X_n]$ and $a_1, \ldots, a_m \in \mathbb{N}$.

(a) Discuss: $R_n = \sum_{d_1a_1+\cdots+d_ma_m=n} A \cdot X_1^{d_1} \cdots X_m^{d_m}$ gives an $\mathbb{N}$-grading of R where the degree of X_i is a_i.

(b) Can you find a_1, a_2, a_3 such that $X_1^2 + X_2^3 + X_3^5$ is homogeneous? Of what degree?

(a) Yes. It is the truth.
(b) $a_1 = 15, a_2 = 10, a_3 = 6$ makes the element degree 30.

(4) The **fine grading** on polynomial rings: Let A be a ring and $R = A[X_1, \ldots, X_n]$. Discuss why

$$R_d = A \cdot X^d \quad \text{for } d = (d_1, \ldots, d_m) \in \mathbb{N}^n, \quad \text{where } X^d := X_1^{d_1} \cdots X_m^{d_m}$$

yields an $\mathbb{N}^m$-grading on R. What are the homogeneous elements?

Yes, every polynomial is a sum of monomials with coefficients in a unique way, and the exponent vectors add when we multiply. The homogeneous elements are monomials with coefficients.

(5) More basics with graded rings. Let R be $\mathbb{N}$-graded.

(a) Show[2] that if $e \in R$ is idempotent, then e is homogeneous of degree zero. In particular, 1 is homogeneous of degree zero.

(b) Show that R_0 is a subring of R, and each R_n is an R_0-module.

(c) Show that if I is homogeneous, then R/I is also $\mathbb{N}$-graded where $(R/I)_n$ consists of the classes of homogeneous elements of R of degree n.

(d) Show that I is homogeneous if and only if I is generated by homogeneous elements.

(e) Suppose that $\phi : R \to S$ is a homomorphism of K-algebras, and that R and S are $\mathbb{N}$-graded with K contained in R_0 and S_0. Show that ϕ is graded if ϕ preserves degrees for all of the elements in some homogeneous generating set of R.

(a) Suppose otherwise; then we can write $e = e_0 + e_d + X$ with e_0 the degree zero component (a priori possibly zero), $e_d \neq 0$ the lowest positive degree component, and X a sum of higher degree terms. Then $e^2 = e$ yields $e_0^2 + 2e_0e_d +$ higher degree terms $= e_0 + e_d +$ higher degree terms, and equating terms of the same degree, $e_0^2 = e_0$ and $2e_0e_d = e_d$. Multiplying the latter by e_0 and using the first gives $2e_0e_d = e_0e_d$, so $e_0e_d = 0$, so $e_d = 0$. This is a contradiction, so we must have $e = e_0$ is homogeneous of degree zero.

[2]Hint: If not, write $e = e_0 + e_d + X$ where e_0 has degree zero and e_d is the lowest nonzero positive degree component. Apply uniqueness of homogeneous decomposition to $e^2 = e$ and show that $2e_0e_d = e_0e_d \ldots$

(b) From the above, $1 \in R_0$; we also know that R_0 is closed under $\pm$ and $\times$, so it is a subring. For $r \in R_0$ and $s \in R_n$, $rs \in R_n$, and all the other module axioms follows from the ring axioms in R.

(c) We need to show that R/I has a unique expression as a sum of elements in distinct $(R/I)_n$ pieces. Let $\overline{r} \in R/I$, and write $r = \sum_i r_{d_i}$ as a sum of homogeneous components. Then $\overline{r} = \sum_i \overline{r_{d_i}}$ gives existence. For uniqueness, suppose that $\overline{0} = \sum_i \sum_i \overline{r_{d_i}}$ with $r_{d_i} \in R_{d_i}$ and d_i distinct. This just means that $\sum_i r_{d_i} \in I$, and by definition of homogeneous ideal, we must have $r_{d_i} \in I$, so $\overline{r_{d_i}}$=$\overline{0}$. This is the required uniqueness statement.

(d) ($\Rightarrow$) Suppose that I is homogeneous, and let S be a generating set for I. We claim that the set of homogeneous components S' of elements of S is a generating set for I. Indeed, each such component is in I, so $(S') \subseteq I$ and since each generator is a linear combination of said components, we have $I = (S) \subseteq (S')$, so $(S') = I$. ($\Leftarrow$) Suppose that I is generated by a set S of homogeneous elements. Then given $f \in I$, we can write $f = \sum_i r_i s_i$ for some $s_i \in S$ of degree d_i. Write each r_i as a sum of homogeneous elements $r_i = \sum_j r_{i,j}$ with $\deg(r_{i,j}) = j$. Then $f = \sum_i r_i s_i = \sum_i \sum_j r_{i,j} s_i$. Then the homogeneous components of f are $\sum_{i,j:j+d_i=t} r_{i,j} s_i$, which lie in I.

(e) Any homogeneous element can be written as a polynomial expression in the generators: $r = \sum_i k_i f_1^{d_1} \cdots f_t^{d_t}$. Each summand on the right hand side is homogeneous, so taking the homogeneous component of degree equal to that of r, we can assume that each term in the right hand side had degree equal to that of r. Then $\phi(r) = \phi\left(\sum_i k_i f_1^{d_1} \cdots f_t^{d_t}\right) = \sum_i k_i \phi(f_1)^{d_1} \cdots \phi(f_t)^{d_t}$. But since $\deg(f_i) = \deg(\phi(f_i))$ the right hand side has the same degree as that on the previous formula, so $\deg(\phi(r)) = \deg(r)$.

(6) Semigroup rings: Let S be a subsemigroup of $\mathbb{N}^n$ with operation $+$ and identity $(0, \ldots, 0)$. The **semigroup ring** of S is

$$K[S] := \sum_{\alpha \in S} K X^\alpha \subseteq R, \qquad \text{where } X^\alpha := X_1^{\alpha_1} \cdots X_n^{\alpha_n}.$$

(a) Show that $K[S]$ is a K-subalgebra that is a graded subring of R in the fine grading.

(b) Let $S = \langle 4, 7, 9 \rangle \subseteq \mathbb{N}$. Draw a picture of S. What is $K[S]$?

(c) Find a semigroup $S \subseteq \mathbb{N}^2$ such that $K[S]$ is Noetherian, and another such that $K[S]$ is not Noetherian. Draw pictures of these semigroups.

(d) Show that every K-subalgebra that is a graded subring of R in the fine grading is of the form $K[S]$ for some S.

(7) Homogeneous elements: Let R be an $\mathbb{N}$-graded ring.

(a) Show that R is a domain if and only if for all homogeneous elements x, y, $xy = 0$ implies $x = 0$ or $y = 0$.

(b) Show that the radical of a homogeneous ideal is homogeneous.

(8) In the setting of the definition of "ring of invariants" suppose that each $g \in G$ acts as a graded homomorphism. Show that R^G is an $\mathbb{N}$-graded K-subalgebra of R.

§3.12: GRADED MODULES

DEFINITION: Let R be an $\mathbb{N}$-graded ring with graded pieces R_i. A **$\mathbb{Z}$-grading** on an R-module M is

- a decomposition of M as additive groups $M = \bigoplus_{e \in \mathbb{Z}} M_e$
- such that $r \in R_d$ and $m \in M_e$ implies $rm \in M_{d+e}$.

An **$\mathbb{Z}$-graded module** is a module with a $\mathbb{Z}$-grading. As with rings, we have the notions of **homogeneous** elements of M, the **degree** of a homogeneous element, **homogeneous decomposition** of an arbitrary element of M. A homomorphism $\phi : M \to N$ between graded modules is **degree-preserving** if $\phi(M_e) \subseteq N_e$.

GRADED NAK 1: Let R be an $\mathbb{N}$-graded ring, and R_+ be the ideal generated by the homogeneous elements of positive degree. Let M be a $\mathbb{Z}$-graded module. Suppose that $M_{\ll 0} = 0$; that is, there is some $n \in \mathbb{Z}$ such that $M_t = 0$ for $t \leq n$. Then $M = R_+M$ implies $M = 0$.

GRADED NAK 2: Let R be an $\mathbb{N}$-graded ring and M be a $\mathbb{Z}$-graded module with $M_{\ll 0} = 0$. Let N be a graded submodule of M. Then $M = N + R_+M$ if and only if $M = N$.

GRADED NAK 3: Let R be an $\mathbb{N}$-graded ring and M be a $\mathbb{Z}$-graded module with $M_{\ll 0} = 0$. Then a set of homogeneous elements $S \subseteq M$ generates M if and only if the image of S in M/R_+M generates M/R_+M as a module over $R_0 \cong R/R_+$.

DEFINITION: Let R be an $\mathbb{N}$-graded ring with $R_0 = K$ a field. Let M be a a $\mathbb{Z}$-graded module with $M_{\ll 0} = 0$. A set S of homogeneous elements of M is a **minimal generating set** for M if the image of S in M/R_+M is an K-vector space basis.

(1) Warmup with minimal generating sets.

(a) Note that the definition of "minimal generating set" does not say that it is a generating set. Use Graded NAK 3 to explain why it is!

(b) Let K be a field and $S = K[X, Y]$. Verify that $\{X^2, XY, Y^2\}$ is a minimal generating set of the ideal I it generates in S.

(c) Let K be a field. Find a minimal generating set of $S = K[X, Y]$ as a module over the K-subalgebra $R = K[X + Y, XY]$.

(a) A basis is a generating set; it is then the $(\Leftarrow)$ of Graded NAK 3.

(b) We need to show that the images of X^2, XY, Y^2 form a basis for I/R_+I; write lowercase for images in this quotient. To see that they span, take $F \in I$, so $F = AX^2 + BXY + CY^2$ for $A, B, C \in R$; then going modulo R_+ we have $f = ax^2+bxy+cy^2$, so x^2, xy, y^2 span the quotient. For linear independence, $ax^2+bxy+cy^2 = 0$ implies $AX^2+BXY+CY^2 \in R_+I$, and by comparing degrees, A, B, C have bottom degree one, hence are in R_+, so $a, b, c = 0$. Alternatively, note that I consists of all polynomials of bottom degree at least two, and R_+I consists of all polynomials of bottom degree at least three. Then the quotient is isomorphic as a vector space to the collection of polynomials of degree two, and X^2, XY, Y^2 is indeed a basis.

(c) We compute $S/R_+S = K[X, Y]/(X + Y, XY) \cong K[Y]/(-Y^2) \cong K[Y]/(Y^2)$, so the classes of $1, Y$ generate. Thus $\{1, Y\}$ forms a minimal generating set.

(2) Proofs of graded NAKs:

(a) Prove Graded NAK 1.

(b) Use Graded NAK 1 to prove Graded NAK 2.
(c) Use Graded NAK 2 to prove Graded NAK 3.

(a) Suppose that $M \neq 0$. Take a nonzero homogeneous element m of minimal degree d in M, which exists by the hypothesis. Then since $m \in R_+M$, we can write $r = \sum_i r_i m_i$ with $r_i \in R_+$, so the bottom degree of r_i is at least one. Thus, we can take the top degree of m_i to be $< d$. But then each $m_i = 0$, so $m = 0$, a contradiction.
(b) The $(\Leftarrow)$ direction is clear. For the other, we can apply Graded NAK 1 to M/N since it is graded and its degrees are bounded below. We have $\frac{M}{N} = \frac{N+R_+M}{N} = R_+\frac{M}{N}$ so $M/N = 0$; i.e., $M = N$.
(c) Apply Graded NAK 2 to the submodule $N = \sum_{s\in S} Rs$: to do so, we need to note that a submodule generated by homogeneous elements is a graded submodule, which follows along similar lines to the corresponding statement we showed for ideals.

(3) The hypotheses:
(a) Examine your proofs from the previous problem and verify that one direction (each) of Graded NAK 2 and Graded NAK 3 hold without assuming that R or M is graded.
(b) Let K be a field and $R = K[X]$ with the standard grading. Let $M = K[X]/(X-1)$. Analyze the hypotheses and conclusion of Graded NAK 1 for this example.
(c) Let K be a field and $R = K[X]$ with the standard grading. Let $M = K[X, X^{-1}]$. Analyze the hypotheses and conclusion of Graded NAK 1 for this example.
(d) Find counterexamples to Graded NAK 3 with M is not graded or not bounded below in degree.

(a) The $(\Leftarrow)$ direction of Graded NAK 2 and the $(\Rightarrow)$ direction of Graded NAK 3 hold without assuming that R or M is graded.
(b) M is not a graded module; any element is of the form $\overline{\lambda}$ for $\lambda \in K$; if such an element was homogeneous, then

$$\deg(\overline{\lambda}) = \deg(\overline{X\lambda}) = \deg(X) + \deg(\overline{\lambda}) = 1 + \deg(\overline{\lambda}),$$

a contradiction. We also have $M = (X)M = R_+M$.
(c) M is graded, but not bounded below. We also have $M = (X)M = R_+M$.
(d) For a cheap example, take either of the previous with $S = \varnothing$.

(4) Minimal generating sets: Let R be an $\mathbb{N}$-graded ring with $R_0 = K$ a field. Let M be a a $\mathbb{Z}$-graded module with $M_{\ll 0} = 0$.
(a) Explain why every minimal generating set for M has the same cardinality.
(b) Explain why every homogeneous generating set for M contains a minimal generating set for M. Moreover, explain why any generating set (homogeneous or not) has cardinality at least that of a minimal generating set.
(c) Explain why "minimal generating set" is equivalent to "homogeneous generating set such that no proper subset generates".
(d) Give an example of a finitely generated module N over $K[X, Y]$ and two generating set S_1, S_2 for N such that no proper subset of S_i generates N, but $|S_1| \neq |S_2|$. Compare to the statements above.

(a) Because all bases of a vector space do.
(b) If S is a homogeneous generating set for M, then the images span M/R_+M, so the images must contain a basis; the elements of S that map to a basis form a minimal generating set. For a general generating set, its images still contain a basis of M/R_+M.

(c) This just follows from the fact that a basis of a vector space is the same as a minimal spanning set.
(d) One could take the two generating sets of the ideal $I = ((X-1)Y, XY) = (Y)$.

(5) Let R be an $\mathbb{N}$-graded ring with $R_0 = K$ a field. Suppose that $R_{\text{red}} = R/\sqrt{0}$ is a domain, and that $f \in R$ is a homogeneous nonnilpotent element of positive degree. Show that $R/(f)$ is reduced implies that R is a reduced, and hence a domain.

(6) Let $r \in \sqrt{0}$ be a homogeneous nilpotent element. Then for some $e \in \mathbb{N}$ we have $r^e = 0 \in (f)$, and since $R/(f)$ is reduced, $r \in (f)$. Thus, we can write $r = fs$ for some homogeneous s. But $r \in \sqrt{0}$, $f \notin \sqrt{0}$, and $\sqrt{0}$ prime implies that $s \in \sqrt{0}$. This implies that $\sqrt{0} = f\sqrt{0} \subseteq R_+\sqrt{0}$, so $\sqrt{0} = 0$; i.e., R is reduced.

§3.13: FINITENESS THEOREM FOR INVARIANT RINGS

HILBERT'S FINITENESS THEOREM: Let K be a field of characteristic zero, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let G be a finite group acting on R by degree-preserving K-algebra automorphisms. Then the invariant ring R^G is algebra-finite over K.

THEOREM: Let R be an $\mathbb{N}$-graded ring. Then R is Noetherian if and only if R_0 is Noetherian and R is algebra-finite over R_0.

DEFINITION: Let $R \subseteq S$ be an inclusion of rings. We say that R is a **direct summand** of S if there is an R-module homomorphism $\pi : S \to R$ such that $\pi|_R = \mathbb{1}_R$.

PROPOSITION: A direct summand of a Noetherian ring is Noetherian.

LEMMA: Let R be a polynomial ring over a field K. If G is a group acting on R by degree-preserving K-algebra automorphisms, then

(1) R^G is an $\mathbb{N}$-graded K-subalgebra of R with $(R^G)_0 = K$.
(2) If in addition, G is finite, and $|G|$ is invertible in K, then R^G is a direct summand of R.

(1) Use the Lemma, Proposition, and Theorem to deduce Hilbert's finiteness Theorem.

By the Lemma, R^G is a direct summand of R. Since R is Noetherian, so is R^G. By the Lemma, R^G is graded with $(R^G)_0 = K$. Then, by the Theorem, since R^G is Noetherian, and R^G is algebra-finite over $(R^G)_0$, and it remains to note that $(R^G)_0 = K$.

(2) Proof of Theorem:

(a) Explain the direction $(\Leftarrow)$.
(b) Show that R Noetherian implies R_0 is Noetherian.
(c) Let $f_1, \ldots, f_t$ be a homogeneous generating set for R_+, the ideal generated by positive degree elements of R. Show[1] by (strong) induction on d that every element of R_d is contained in $R_0[f_1, \ldots, f_t]$.
(d) Conclude the proof of the Theorem.

(a) This follows from the Hilbert Basis Theorem.
(b) $R_0 \cong R/R_+$.
(c) For $d = 0$ there is nothing to show. For $d > 0$, take $h \in R_d$. Since $R_d \subseteq R_+$, write $h = \sum_i r_i f_i$ for some $r_i \in R$. If we replace r_i by r_i' its homogeneous component of degree $d - \deg(f_i)$, we claim that $h = \sum_i r_i' f_i$. Indeed, writing each r_i as a sum of homogeneous components and multiplying out, all of the other terms are homogeneous of some other degree, so the claim follows by uniqueness of homogeneous decomposition. So suppose r_i is homogeneous of degree $d - \deg(f_i)$. By induction, we have $r_i \in R_0[f_1, \ldots, f_t]$. But then this plus $h = \sum_i r_i f_i$ show $h \in R_0[f_1, \ldots, f_t]$.
(d) If R is Noetherian then R_+ is finitely generated as an ideal; since R_+ is homogeneous, it is generated by the (fintely many) components of these generators so has a finite homogeneous generating set, and a such generating set of R_+ generates R as an algebra over R_0 by the previous part.

[1] Hint: Start by writing $h \in R_d$ as $h = \sum_i r_i f_i$ with $d = \deg(r_i) + \deg(f_i)$ for all i.

(3) Proof of Proposition:

(a) Show that if R is a direct summand of S, and I is an ideal of R, then $IS \cap R = I$.

(b) Complete the proof of the proposition.

(a) We always have $I \subseteq IS \cap R$. Let $f \in IS \cap R$, so $f = \sum_i a_i s_i$ with $a_i \in I$, $s_i \in S$. Apply the map π. Since $f \in R$, we have $\pi(f) = f$. Since π is R-linear, we also have $\pi\left(\sum_i a_i s_i\right) = \sum_i a_i \pi(s_i)$, with $\pi(s_i) \in R$. But this is an element of I, so $f \in I$.

(b) Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be a chain of ideals in R. Then $I_1 S \subseteq I_2 S \subseteq I_3 S \subseteq \cdots$ is a chain of ideals in S, which necessarily stabilizes. But the chain $(I_1 S \cap R) \subseteq (I_2 S \cap R) \subseteq (I_3 S \cap R) \subseteq \cdots$ stabilizes, but this is our original chain!

(4) Proof of Lemma part (2): Consider $r \mapsto \frac{1}{|G|} \sum_{g \in G} g \cdot r$.

One checks directly that this map is R^G-linear and restricts to the identity on R^G.

(5) Show that a direct summand of a normal ring is normal.

(6) Let $\mathcal{S}_3$ denote the symmetric group on 3 letters, and let $\mathcal{S}_3$ act on $R = \mathbb{C}[X_1, X_2, X_3]$ by permuting variables; i.e., σ is the $\mathbb{C}$-algebra homomorphism given by $\sigma \cdot X_i = X_{\sigma(i)}$. Find a $\mathbb{C}$-algebra generating set for $R^{\mathcal{S}_3}$. What about replacing 3 by n?

§3.14: Rees Rings and the Artin-Rees Lemma

DEFINITION: Let R be a ring and I be an ideal. The **Rees ring** of I is the $\mathbb{N}$-graded R-algebra

$$R[IT] := \bigoplus_{d\geq 0} I^d T^d = R \oplus IT \oplus I^2T^2 \oplus \cdots$$

with multiplication determined by $(aT^d)(bT^e) = abT^{d+e}$ for $a \in I^d$, $b \in I^e$ (and extended by the distributive law for nonhomogeneous elements). Here I^n means the nth power of the ideal I in R, and t is an indeterminate. Equivalently, $R[IT]$ is the R-subalgebra of the polynomial ring $R[T]$ generated by IT, with $R[T]$ is given the standard grading $R[T]_d = R \cdot T^d$.

DEFINITION: Let R be a ring and I be an ideal. The **associated graded ring** of I is the $\mathbb{N}$-graded ring

$$\mathrm{gr}_I(R) := \bigoplus_{d\geq 0} (I^d/I^{d+1})T^d = R/I \oplus (I/I^2)T \oplus (I^2/I^3)T^2 \oplus \cdots$$

with multiplication determined by $(a + I^{d+1}T^d)(b + I^{e+1}T^e) = ab + I^{d+e+1}\,T^{d+e}$ for $a \in I^d$, $b \in I^e$ (and extended by the distributive law). For an element $r \in R$, its **initial form** in $\mathrm{gr}_I(R)$ is

$$r^* := \begin{cases} (r + I^{d+1})T^d & \text{if } r \in I^d \smallsetminus I^{d+1} \\ 0 & \text{if } r \in \bigcap_{n\geq 0} I^n. \end{cases}$$

ARTIN-REES LEMMA: Let R be a Noetherian ring, I an ideal of R, M a finitely generated module, and $N \subseteq M$ a submodule. Then there is a constant[1] $c \geq 0$ such that for all $n \geq c$, we have $I^n M \cap N \subseteq I^{n-c}N$.

(1) Warmup with Rees rings:

(a) Let R be a ring and I be an ideal. Show that if $I = (a_1, \ldots, a_n)$, then $R[It] = R[a_1t, \ldots, a_nt]$.

(b) Let K be a field, $R = K[X, Y]$ and $I = (X, Y)$. Find K-algebra generators for $R[It]$, and find a relation on these generators.

(a) This follows from the Theorem we showed last time: given a (finite, though this isn't necessary) set of homogeneous elements that generate R_+ as an ideal, these elements generate R as an R_0-algebra.

(b) The elements X, Y, XT, YT generate. A relation is $X(YT) - Y(XT)$, or $X_1X_4 - X_2X_3$ in dummy variables. In fact, this is a defining set of relations.

(2) Warmup with associated graded rings:

(a) Convince yourself that the multiplication given in the definition of $\mathrm{gr}_I(R)$ is well-defined. After doing this, do *not* use coset notation for elements of $\mathrm{gr}_I(R)$ and instead write a typical homogeneous element as something like $\overline{r}\,T^d$.

(b) Let K be a field, $R = K[X, Y]$, and $\mathfrak{m} = (X, Y)$. Show that $\mathrm{gr}_{\mathfrak{m}}(R)_d \cong R_d$ as K-vector spaces, and construct a ring isomorphism $\mathrm{gr}_{\mathfrak{m}}(R) \cong R$.

(c) For the same R, show that the map $R \to \mathrm{gr}_{\mathfrak{m}}(R)$ given by $r \mapsto r^*$ is *not* a ring homomorphism.

(d) Let K be a field, $R = K[\![X, Y]\!]$, and $\mathfrak{m} = (X, Y)$. Show[2] that $\mathrm{gr}_{\mathfrak{m}}(R) \cong K[X, Y]$.

[1] The constant c depends on I, M, and N but works for all t.

[2] Yes, the brackets changed. This is not a typo!

(e) What happens in (b) and (d) if we have n variables instead of 2?

(a) Let $a \in I^d$ and $b \in I^e$. Then given $a' \in I^{d+1}$ and $b' \in I^{e+1}$, we have $(a+a')(b+b') = ab + a'b + ab' + a'b' \in ab + I^{d+e+1}$.
(b) Note that $\mathrm{gr}_I(R)_d$ is exactly the vector space fT^d with $f \in R_d$. So "ignoring" T is an isomorphism of vector spaces. One checks directly that it is compatible with multiplication by reducing to the case of homogeneous elements.
(c) For example, if $f = X - 1$ and $g = 1$, then $f^* = -1$, $g^* = 1$, but $(f+g)^* = X$.
(d) Note that $\mathrm{gr}_I(R)_d$ is again just the vector space fT^d with $f \in R_d$, and multiplication is the same as in the polynomial case.
(e) The same thing.

(3) Consider the special case of Artin-Rees where $M = R$, and $I = (f)$ and $N = (g)$.
(a) What does Artin-Rees say in this setting? Express your answer in terms of "divides".
(b) Take $R = \mathbb{Z}$. Does $c = 0$ "work" for every $f, g \in \mathbb{Z}$? Can you find a sequence of examples requiring arbitrarily large values of c?

(a) There is some c such that $f^n | h$ and $g | h$ implies $(f^{n-c}g) | h$.
(b) Take $f = 2$ and $g = 2^m$. Then $2^n | h$ and $2^m | h$ implies $2^{\max\{m,n\}} | h$. Then $f^{n-c}g = 2^{m+n-c}$. To guarantee this to divide h, we must have $c \geq m$.

(4) Proof of Artin-Rees: Let R be a Noetherian ring, and I be an ideal.
(a) Explain why $R[It]$ is a Noetherian ring.
(b) Let $M = \sum_i Rm_i$ be a finitely generated R-module. Set $\mathcal{M} := \bigoplus_{n \geq 0} I^n M t^n$. Show that this is a graded $R[It]$-module, and that $\mathcal{M} = \sum_i R[It] \cdot m_i$, where in the last equality we consider m_i as the element $m_i t^0 \in \mathcal{M}_0$.
(c) Given a submodule N of M, set $\mathcal{N} := \bigoplus_{n \geq 0} (I^n M \cap N) t^n \subseteq \mathcal{M}$. Show that $\mathcal{N}$ is a graded $R[It]$-submodule of $\mathcal{M}$.
(d) Show that there exist $n_1, \ldots, n_k \in N$ and $c_1, \ldots, c_k \geq 0$ such that $\mathcal{N} = \sum_j R[It] \cdot n_j t^{c_j}$.
(e) Show that $c := \max\{c_j\}$ satisfies the conclusion of the Artin-Rees Lemma.

(a) Since I is finitely generated, it is a finitely generated algebra over a Noetherian ring.
(b) First, we check that this is an $R[It]$-module. It is clearly an additive group. To check that it is closed under the $R[It]$-action and that this yields a graded action, it suffices to check that $R[It]_d \cdot \mathcal{M}_e \subseteq \mathcal{M}_{d+e}$. To see it, take rt^d with $r \in I^d$ and mt^e with $m \in I^e M$; then the action yields rmt^{d+e} and $rm \in I^d(I^e M) = I^{d+e}M$, so $rmt^{d+e} \in \mathcal{M}_{d+e}$, as required.
Clearly $m_i \in \mathcal{M}$, so $\sum_i R[It] \cdot m_i \subseteq \mathcal{M}$. Now we check that this generates. It suffices to check that any homogeneous element can be generated by this generating set, so take some $mt^d \in \mathcal{M}_d$ with $m \in I^d M$. This means we can write $m = \sum_j a_j u_j$ with $a_j \in I^d$ and $u_j \in M$. Then we can write $u_j = \sum b_{ij} m_i$ for some $b_{ij} \in R$, yielding an expression $m = \sum_i c_i m_i$ with $c_i \in I^d$. Thus, $m = \sum_i (c_i t^d) m_i \in R[It] \cdot m_i$.
(c) It suffices to check that $R[It]_d \cdot \mathcal{N}_e \subseteq \mathcal{N}_{d+e}$. Take rt^d with $r \in I^d$ and nt^e with $n \in (I^e M \cap N)$. Then $rn \in I^d(I^e M \cap N)$, so $rn \in I^d I^e M = I^{d+e}M$ and $rn \in I^d N \subseteq N$, and hence $rn \in I^{d+e}M \cap N$. Thus $(rt^d)(nt^e) \in \mathcal{N}_{d+e}$.

(d) Since $R[It]$ is Noetherian and $\mathcal{M}$ is finitely generated, so is $\mathcal{N}$. Since it is graded and finitely generated, it can be generated by finitely many homogeneous elements. The statement is just naming them.

(e) Let $c = \max\{c_j\}$. Take $u \in I^n M \cap N$. Then $ut^n \in \mathcal{N}_n = \sum_j R[It] \cdot n_j t^{c_j}$. We can then express u as a homogeneous linear combination of these generators, so $ut^n = \sum_j (r_j t^{n-c_j})(n_j t^{c_j})$. Since $n - c_j \geq n - c$, we have $r_j \in I^{n-c}$, and each $n_j \in N$, so $u = \sum_j r_j n_j \in I^{n-c}N$. Moving over the c, we obtain the statement.

(5) Presentations of associated graded rings: Let R be a ring and I, J be ideals. Set $\mathrm{in}_I(J)$ to be the ideal of $\mathrm{gr}_I(R)$ generated by $\{a^* \mid a \in J\}$.
   (a) Show that $\mathrm{gr}_I(R/J) \cong \mathrm{gr}_I(R)/\mathrm{in}(J)$.
   (b) If $J = (f)$ is a principal ideal, show that $\mathrm{in}_I(J) = (f^*)$.
   (c) Is $\mathrm{in}_I((f_1, \ldots, f_t)) = (f_1^*, \ldots, f_t^*)$ in general?
   (d) Compute $\mathrm{gr}_{(x,y,z)}(\frac{K[\![X,Y,Z]\!]}{(X^2+XY+Y^3+Z^7)})$.

(6) Properties of associated graded rings: Let R be a ring and I be an ideal such that $\bigcap_{n\geq 0} I^n = 0$.
   (a) Show that if $\mathrm{gr}_I(R)$ is a domain, then so is R.
   (b) Show that if $\mathrm{gr}_I(R)$ is reduced, then so is R.
   (c) What about the converses of these statements?

(7) Show that for the ideal $I = (X, Y)^2$ in $R = K[X, Y]$, the Rees ring $R[It]$ has defining relations of degree greater than one.

§4.15: NOETHER NORMALIZATION AND ZARISKI'S LEMMA

NOETHER NORMALIZATION: Let K be a field, and R be a finitely-generated K-algebra. Then there exists a finite[1] set of elements $f_1, \dots, f_m \in R$ that are algebraically independent over K such that $K[f_1, \dots, f_m] \subseteq R$ is module-finite; equivalently, there is a module-finite injective K-algebra map from a polynomial ring $K[X_1, \dots, X_m] \hookrightarrow R$. Such a ring S is called a **Noether normalization** for R.

LEMMA: Let A be a ring, and $F \in R := A[X_1, \dots, X_n]$ be a nonzero polynomial. Then there exists an A-algebra automorphism ϕ of R such that $\phi(F)$, viewed as a polynomial in X_n with coefficients in $A[X_1, \dots, X_{n-1}]$, has top degree term aX_n^t for some $a \in A \smallsetminus 0$ and $t \geq 0$.

- If $A = K$ is an infinite field, one can take $\phi(X_n) = X_n$ and $\phi(X_i) = X_i + \lambda_i X_n$ for some $\lambda_1, \dots, \lambda_{n-1} \in K$.
- In general, if the top degree of F (with respect to the standard grading) is D, one can take $\phi(X_n) = X_n$ and $\phi(X_i) = X_i + X_n^{D^{n-i}}$ for $i < n$.

ZARISKI'S LEMMA: An algebra-finite extension of fields is module-finite.

USEFUL VARIATIONS ON NOETHER NORMALIZATION:

- NN FOR DOMAINS: Let $A \subseteq R$ be an algebra-finite inclusion of domains[2]. Then there exists $a \in A \smallsetminus 0$ and $f_1, \dots, f_m \in R[1/a]$ that are algebraically independent over $A[1/a]$ such that $A[1/a][f_1, \dots, f_m] \subseteq R[1/a]$ is module-finite.
- GRADED NN: Let K be an infinite field, and R be a standard graded K-algebra. Then there exist algebraically independent elements $L_1, \dots, L_m \in R_1$ such that $K[L_1, \dots, L_m] \subseteq R$ is module-finite.
- NN FOR POWER SERIES: Let K be an infinite field, and $R = K[\![X_1, \dots, X_n]\!]/I$. Then there exists a module-finite injection $K[\![Y_1, \dots, Y_m]\!] \hookrightarrow R$ for some power series ring in m variables.

(1) Examples of Noether normalizations: Let K be a field.

(a) Show that $K[x, y]$ is a Noether normalization of $R = \dfrac{K[X, Y, Z]}{(X^3 + Y^3 + Z^3)}$, where x, y are the classes of X and Y in R, respectively.

(b) Show that $K[x]$ is *not* a Noether normalization of $R = \dfrac{K[X, Y]}{(XY)}$. Then show that $K[x + y] \subseteq R$ *is* a Noether normalization.

(c) Show that $K[X^4, Y^4]$ is a Noether normalization for $R = K[X^4, X^3Y, XY^3, Y^4]$.

(a) From the equation $z^3 + x^3 + y^3 = 0$, we have $K[x, y] \subseteq R$ is integral, and since z generates as an algebra, hence module-finite. We need to check that x, y are algebraically independent in R. Suppose that $p(x, y) = 0$ in R, so $p(X, Y) \in$

[1] Possibly empty!

[2] The assumption that R is a domain is actually not necessary, but can't quite state the general statement yet. We assume that R is a domain so that there is fraction field of R in which to take $R[1/a]$.

$(X^3 + Y^3 + Z^3)$ in $K[X, Y, Z]$. By considering $K[X, Y, Z] = K[X, Y][Z]$ as polynomials in Z, the Z-degree of such a p, which forces $p = 0$. Thus x, y are algebraically independent.

(b) y is not integral over $K[x]$: this would imply $Y^n + a_1(X)Y^{n-1} + \cdots a_n(X) = XYb(X, Y)$ in $K[X, Y]$, but no monomial from any term can cancel Y^n. Alternatively, if the inclusion is module-finite, go mod x to get $K \subseteq K[X, Y]/(XY, X) = K[Y]$ module-finite, which it isn't.

(c) It is easy to check that X^4, Y^4 are algebraically independent, and $(X^3Y)^4 = (X^4)^3Y^4$, $(XY^3)^4 = X^4(Y^4)^3$ give integral dependence relations for the algebra generators.

(2) Use Noether Normalization[3] to prove Zariski's Lemma.

Let $K \subseteq L$ be an algebra-finite extension of fields. Take a NN of L: say $K \subseteq K[\ell_1, \ldots, \ell_t] \subseteq L$, with ℓ_i algebraically independent and $R := K[\ell_1, \ldots, \ell_t] \subseteq L$ module-finite and a fortiori integral. From the Integral Extensions worksheet, since L and R are domains, the extension is integral, and L is a field, we know that R is a field. This means that $t = 0$, so $K \subseteq L$ is module-finite.

(3) Proof of Noether Normalization (using the Lemma): Proceed by induction on the number of generators of R as a K-algebra; write $R = K[r_1, \ldots, r_n]$.

(a) Deal with the base case $n = 0$.

(b) For the inductive step, first do the case that $r_1, \ldots, r_n$ are algebraically independent over K.

(c) Let $\alpha : K[X_1, \ldots, X_n] \to R$ be the K-algebra homomorphism such that $\alpha(X_i) = r_i$, and let ϕ be a K-algebra automorphism of $K[X_1, \ldots, X_n]$. Let $r_i' = \alpha(\phi(X_i))$ for each i. Explain[4] why $R = K[r_1', \ldots, r_n']$, and for any K-algebra relation F on $r_1, \ldots, r_n$, the polynomial $\phi^{-1}(F)$ is a K-algebra relation on $r_1', \ldots, r_n'$.

(d) Use the Lemma to find a K-subalgebra R' of R with $n - 1$ generators such that the inclusion $R' \subseteq R$ is module-finite.

(e) Conclude the proof.

(a) This means that R is a quotient of K, but K is a field, so $R = K$; the identity map is module-finite.

(b) If we have an algebraically independent set of generators for R, then R works: the identity map is module-finite.

(c) First we claim that $R = K[r_1', \ldots, r_n']$: indeed, the map $\alpha' = \alpha \circ \phi$ is the K-algebra map that sends X_i to r_i', and since α and ϕ are surjective, α' is surjective, verifying the claim. The relations on the r_i' are of the elements of the kernel of α'; if F is a relation on the originals, then $\alpha(F) = 0$, so $\alpha'(\phi^{-1}(F)) = 0$ as well.

[3] and a suitable fact about integral extensions...

[4] Say α' is the K-algebra map given by $\alpha'(X_i) = r_i'$. Observe that $\alpha' = \alpha \circ \phi$. Why is this surjective?

(d) Take a map ϕ as in the Lemma, and n generators $r_1, \ldots, r_n$. Set $r_i' = \phi^{-1}(r_i)$. By the previous part, these generate, and there is a relation on these that is monic in X_n, so $R' = K[r_1', \ldots, r_{n-1}'] \subseteq R$ is module-finite.

(e) Apply IH to R' to get $K[f_1, \ldots, f_t] \subseteq R'$ with f_i alg indep't and the inclusion module-finite. Then $K[f_1, \ldots, f_t]$ is a Noether normalization.

(4) Proof of the "general case" of the Lemma:
   (a) Where do "base D expansions" fit in this picture?
   (b) Consider the automorphism ϕ from the general case of the Lemma. Show that for a monomial, we have $\phi(aX_1^{d_1} \cdots X_n^{d_n})$ is a polynomial with unique highest degree term $aX_n^{d_1 D^{n-1} + d_2 D^{n-2} + \cdots + d_n}$.
   (c) Can two monomials μ, ν in F, have $\phi(\mu)$ and $\phi(\nu)$ with the same highest degree term?
   (d) Complete the proof.

(5) Variations on NN.
   (a) Adapt the proof of NN to show Graded NN.
   (b) Adapt the proof of NN to show NN for domains.
   (c) Adapt the proof of NN to show NN for power series.

§4.16: NULLSTELLENSATZ

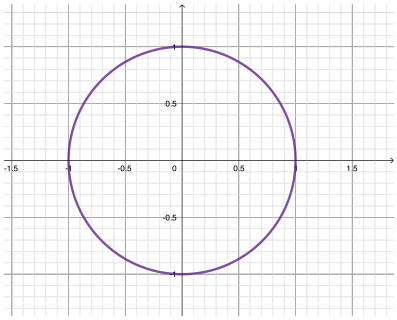
DEFINITION: Let K be a field and $R = K[X_1, \ldots, X_n]$. For a set of polynomials $S \subseteq R$, we define the **zero-set** of **solution set** of S to be

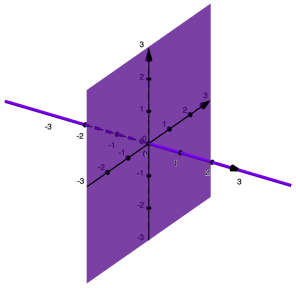
$$\mathcal{Z}(S) := \{(a_1, \ldots, a_n) \in K^n \mid F(a_1, \ldots, a_n) = 0 \text{ for all } F \in S\}.$$

NULLSTELLENSATZ: Let K be an algebraically closed field, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let $I \subseteq R$ be an ideal. Then $\mathcal{Z}(I) = \varnothing$ if and only if $I = R$ is the unit ideal. Put another way, a set S of multivariate polynomials has a common zero unless there is a "certificate of infeasibility" consisting of $f_1, \ldots, f_t \in S$ and $r_1, \ldots, r_t \in R$ such that $\sum_i r_i s_i = 1$.

PROPOSITION: Let K be an algebraically closed field, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Every maximal ideal of R is of the form $\mathfrak{m}_\alpha = (X_1 - a_1, \ldots, X_n - a_n)$ for some point $\alpha = (a_1 \ldots, a_n) \in K^n$.

(1) Draw the "real parts" of $\mathcal{Z}(X^2 + Y^2 - 1)$ and of $\mathcal{Z}(XY, XZ)$.





(2) Explain why the Nullstellensatz is definitely false if K is assumed to *not* be algebraically closed.

To not be algebraically closed means that there is a nonconstant polynomial in one variable that has empty solution set; such a polynomial generates a proper ideal.

(3) Basics of $\mathcal{Z}$: Let $R = K[X_1, \ldots, X_n]$ be a polynomial ring.

- **(a)** Explain why, for any system of polynomial equations $F_1 = G_1, \ldots, F_m = G_m$, the solution set can be written in the form $\mathcal{Z}(S)$ for some set S.
- **(b)** Let $S \subseteq T$ be two sets of polynomials. Show that $\mathcal{Z}(S) \supseteq \mathcal{Z}(T)$.
- **(c)** Let $I = (S)$. Show that $\mathcal{Z}(I) = \mathcal{Z}(S)$. Thus, every solution set system of any polynomial equations can be written as $\mathcal{Z}$ of some ideal.
- **(d)** Explain the following: every system of equations over a polynomial ring is equivalent to a *finite* system of equations.

- **(a)** Take $S = \{F_1 - G_1, \ldots, F_m - G_m\}$.
- **(b)** $\alpha \in \mathcal{Z}(T)$ implies $F(\alpha) = 0$ for all $F \in T$ implies $F(\alpha) = 0$ for all $F \in S$ implies $\alpha \in \mathcal{Z}(S)$.

(c) Since $S \subseteq I$ we have $\mathcal{Z}(S) \supseteq \mathcal{Z}(I)$. On the other hand, if $\alpha \in \mathcal{Z}(S)$ and $F \in I$, then $F = \sum_i r_i s_i$ with $s_i \in S$, and $F(\alpha) = \sum_i r_i(\alpha) s_i(\alpha) = \sum_i r_i(\alpha) \cdot 0 = 0$. Thus $\alpha \in \mathcal{Z}(I)$.

(d) We can write any system as $\mathcal{Z}(I)$. By the Hilbert Basis Theorem, $I = (f_1, \ldots, f_m)$, and $\mathcal{Z}(I) = \mathcal{Z}(f_1, \ldots, f_m)$, which is equivalent to the system $f_1 = 0, \ldots, f_m = 0$.

(4) Proof of Proposition and Nullstellensatz: Let K be an algebraically closed field, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring.

(a) Use Zariski's Lemma to show that for every maximal ideal $\mathfrak{m} \subseteq R$, we have $R/\mathfrak{m} \cong K$.

(b) Reuse some old work to deduce the Proposition.

(c) Deduce the Nullstellensatz from the Proposition.

(d) Convince yourself that the "certificate of infeasibility" version follows from the other one.

(a) The ring $R/\mathfrak{m}$ is a finitely generated K-algebra and a field, so $K \subseteq R/\mathfrak{m}$ is module-finite by Zariski's Lemma. Since K is algebraically closed, we must have $K \cong R/\mathfrak{m}$.

(b) From worksheet #2, we know that any maximal ideal in a polynomial ring with $R/\mathfrak{m} \cong K$ is of the form $\mathfrak{m}_\alpha$ for some α.

(c) If I is a proper ideal, then $I \subseteq \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, and from above $I \subseteq \mathfrak{m}_\alpha$ for some α. Then $\mathcal{Z}(I) \supseteq \mathcal{Z}(\mathfrak{m}_\alpha) = \{\alpha\}$ is nonempty!

(d) This is just unpackaging what it means for (S) to be the unit ideal.

(5) Given a system of polynomial equations and inequations

$$(\star) \qquad F_1 = 0, \ldots, F_m = 0 \qquad G_1 \neq 0, \ldots, G_\ell \neq 0$$

come up with a system[1] of equations $(\dagger)$ *in one extra variable* such that $(\star)$ has a solution if and only if $(\dagger)$ has a solution. Thus every equation-and-inequation feasibility problem is equivalent to a question of the form $\mathcal{Z}(I) \stackrel{?}{=} \varnothing$.

We can take $F_1 = 0, \ldots, F_m = 0, G_1 G_2 \ldots G_\ell Y - 1 = 0$: a solution of this must consist of a solution of $(\star)$ for the X's and the inverse of the product of the $G_i(X)$ for Y.

(6) Show that any system of multivariate polynomial equations (or equations and inequations) over a field K has a solution in some extension field of L if and only if it has a solution over $\overline{K}$.

(7) Let K be a field and $R = K[X_1, \ldots, X_n]$. Let $L \supseteq K$ and $S = L[X_1, \ldots, X_n]$.

(a) Find some f that is irreducible in R but reducible in S for some choice of $K \subseteq L$.

(b) Show that if K is algebraically closed and $f \in R$ is irreducible, then it is irreducible in S.

(c) Show that if K is algebraically closed and $I \subseteq R$ is prime, then IS is prime.

(8) Show that the statement of the Nullstellensatz holds for the ring of continuous functions from $[0, 1]$ to $\mathbb{R}$.

[1] Hint: $\lambda \in K$ is nonzero if and only if there is some μ such that $\lambda\mu = 1$.

§4.17: Strong Nullstellensatz

Strong Nullstellensatz: Let K be an algebraically closed field, and $R = K[X_1, \dots, X_n]$ be a polynomial ring. Let $I \subseteq R$ be an ideal and $f \in R$ a polynomial. Then

$$f \text{ vanishes at every point of } \mathcal{Z}(I) \text{ if and only if } f \in \sqrt{I}.$$

Definition: Let K be a field and $R = K[X_1, \dots, X_n]$. A **subvariety** of K^n is a set of the form $\mathcal{Z}(S)$ for some set of polynomials $S \subseteq R$; i.e., a solution set of some system of polynomial equations.

Corollary: Let K be an algebraically closed field. There is a bijection

$$\{\text{radical ideals in } K[X_1, \dots, X_n]\} \longleftrightarrow \{\text{subvarieties of } K^n\}.$$

(1) Proof of Strong Nullstellensatz:

- **(a)** Show that $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$, and deduce the ($\Leftarrow$) direction.
- **(b)** Let Y be an extra indeterminate. Show that f vanishes on $\mathcal{Z}(I)$ implies that
$$\mathcal{Z}\big(I + (Yf - 1)\big) = \varnothing \quad \text{in } K^{n+1}.$$
- **(c)** What does the Nullstellensatz have to say about that?
- **(d)** Apply the R-algebra homomorphism $\phi : R[Y] \to \operatorname{frac}(R)$ given by $\phi(Y) = \frac{1}{f}$ and clear denominators.

- **(a)** Since $I \subseteq \sqrt{I}$, we have $\mathcal{Z}(\sqrt{I}) \subseteq \mathcal{Z}(I)$. On the other hand, if $\alpha \in \mathcal{Z}(I)$ and $f^n \in I$, then $f^n(\alpha) = 0$, so $f(\alpha) = 0$, so $\alpha \in \mathcal{Z}(\sqrt{I})$. In particular, the ($\Leftarrow$) direction of the statement holds.
- **(b)** If there was a solution (α, a), this would mean $\alpha \in \mathcal{Z}(I)$ and $af(\alpha) - -1 = 0$, so $f(\alpha) \neq 0$, contradicting that $\alpha \in \mathcal{Z}(f)$.
- **(c)** We can write $1 = \sum_i r_i(\underline{X}, Y) g_i(\underline{X}) + s(\underline{X}, Y)(Yf(\underline{X}) - 1)$ for some $r_i, s \in R[Y]$ and $g_i \in I$.
- **(d)** We get $1 = \sum_i r_i(\underline{X}, 1/f) g_i(\underline{X}) + s(\underline{X}, 1/f)(1/f \cdot f(\underline{X}) - 1)$. The last term dies so $1 = \sum_i r_i(\underline{X}, 1/f) g_i(\underline{X})$. We can clear denominators to get $f^n = \sum r_i'(\underline{X}) g_i(\underline{X})$ in R, so $f^n \in I$.

(2) Strong Nullstellensatz warmup:

- **(a)** Consider the ideal $I = (X^2 + Y^2) \in \mathbb{R}[X, Y]$ and $f = X$. Discuss the hypotheses and conclusion of Strong Nullstellensatz in this example.
- **(b)** Show that[1] no power of $F = X^2 + Y^2 + Z^2$ is in the ideal
$$I = (X^3 - Y^2 Z, Y^7 - XZ^3, 3X^5 - XYZ - 2Z^{19}) \quad \text{in the ring} \quad \mathbb{C}[X, Y, Z].$$

- **(a)** $\mathcal{Z}(I) = \{(0, 0)\}$ and X vanishes along $\mathcal{Z}(I)$, but $(X^2 + Y^2)$ is prime and hence radical. The conclusion of Strong Nullstellensatz fails. Of course, $\mathbb{R}$ is not algebraically closed.
- **(b)** $F(1, 1, 1) = 3 \neq 0$ but $(1, 1, 1) \in \mathcal{Z}(I)$, since it is in the zero-set of each generator.

(3) Prove the Corollary.

[1] Hint: You just need to find one point. *One*, *one*, *one*…

We have a map from radical ideals to subvarieities given by $I \mapsto \mathcal{Z}(I)$. This is surjective by definition and the first part of the proof of Strong Nullstellensatz. It is injective too: if I and J are distinct radical ideals, without loss of generality there is some $f \in J$ such that $f \notin \sqrt{I}$; then $f(\alpha) \neq 0$ for some $\alpha \in \mathcal{Z}(I)$, so $\mathcal{Z}(I) \not\subseteq \mathcal{Z}(J)$.

(4) Let $R = \mathbb{C}[T]$ be a polynomial ring. In this problem, we will show that the ideal of $\mathbb{C}$-algebraic relations on the elements $\{T^2, T^3, T^4\}$ is $I = (X_1^2 - X_3, X_2^2 - X_1X_3)$.

(a) Let $\phi : \mathbb{C}[X_1, X_2, X_3] \to \mathbb{C}[T]$ be the $\mathbb{C}$-algebra map $X_1 \mapsto T^2, X_2 \mapsto T^3, X_3 \mapsto T^4$. Show that $I \subseteq \ker(\phi)$.

(b) Show that $\mathcal{Z}(I) \subseteq \{(\lambda^2, \lambda^3, \lambda^4) \in \mathbb{C}^3 \mid \lambda \in \mathbb{C})\} \subseteq \mathcal{Z}(\ker(\phi))$, and deduce that $\ker(\phi) \subseteq \sqrt{I}$.

(c) Show that I is prime[2], and complete the proof.

(a) The generators map to 0 under ϕ.

(b) For the first containment, let $(\alpha, \beta, \gamma) \in \mathcal{Z}(I)$. From the first equation, we can write $\gamma = \alpha^2$. From the second, we have $\beta^2 = \alpha^3$. If $\alpha = 0$, we must have $(0, 0, 0)$. Otherwise, α has two square roots. Take λ to be one of these. Then $\alpha = \lambda^2$ and $\beta^2 = \lambda^6$. This means $\beta = \pm\lambda^3$. If $\beta = -\lambda^3$, replace λ by $-\lambda$; this does not change $\alpha = \lambda^2$ or $\gamma = \lambda^4$. So, we obtain λ such that $(\alpha, \beta, \gamma) = (\lambda^2, \lambda^3, \lambda^4)$.
For the second, if $F(X_1, X_2, X_3) \in \ker(\phi)$, then $F(T^2, T^3, T^4) = 0$, so $F(\lambda^2, \lambda^3, \lambda^4) = 0$.

(c) Using the first relation and an isomorphism theorem, $\mathbb{C}[X_1, X_2, X_3]/I \cong \mathbb{C}[X_1, X_2]/(X_2^2 - X_1^3)$. The element $X_2^2 - X_1^3$ is irreducible by Eisenstein's criterion, so I is prime.

(5) Let K be an algebraically closed field and $R = K\begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$ be a polynomial ring. Use the Strong Nullstellensatz to show that any polynomial $F(X_{11}, X_{12}, X_{21}, X_{22})$ that vanishes on every matrix of rank at most one is a multiple of $\det \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$.

(6) We say that a subvariety of K^n is **irreducible** if it cannot be written as a union of two proper subvarities. Show that the bijection from the Corollary restricts to a bijection

$$\{\text{prime ideals in } K[X_1, \ldots, X_n]\} \longleftrightarrow \{\text{irreducible subvarieties of } K^n\}.$$

Let I be a radical ideal. We need to show that $\mathcal{Z}(I)$ is irreducible if and only if I is prime.

Suppose that I is not prime, so one has $f, g \notin I$ with $fg \in I$. Since I is radical, $f, g \notin \sqrt{I}$, so $\mathcal{Z}(f), \mathcal{Z}(g) \not\supseteq \mathcal{Z}(I)$. This means that $\mathcal{Z}(I + (f))$ and $\mathcal{Z}(I + (g))$ are proper subvarieties of $\mathcal{Z}(I)$. But $\alpha \in \mathcal{Z}(I)$ and $fg \in I$ implies $f(\alpha)g(\alpha) = 0$ so $f(\alpha) = 0$ or $g(\alpha) = 0$, which means $\mathcal{Z}(I) = \mathcal{Z}(I + (f)) \cup \mathcal{Z}(I + (g))$.

Conversely, suppose that $\mathcal{Z}(I) = \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$, with J_1, J_2 radical and not equal to I. Since $\mathcal{Z}(I) \supseteq \mathcal{Z}(J_i)$ we have $J_i \supsetneq I$. We can take $f \in J_1 \smallsetminus J_2$ and $g \in J_2 \smallsetminus J_1$. Since $f(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(J_1)$, $g(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(J_2)$, and $\mathcal{Z}(I) = \mathcal{Z}(J_1) \cup \mathcal{Z}(J_2)$, we have $fg(\alpha) = 0$ for all $\alpha \in \mathcal{Z}(I)$, so $fg \in I$, and I is not prime.

[2]Show $\mathbb{C}[X_1, X_2, X_3]/I$ is a domain by simplifying the quotient.

(7) Use the Strong Nullstellensatz to show that, in a finitely generated algebra over an algebrically closed field, every radical ideal can be written as an intersection of maximal ideals.

§4.18: SPECTRUM OF A RING

DEFINITION: Let R be a ring, and $I \subseteq R$ an ideal of R.

- The **spectrum** of a ring R, denoted $\operatorname{Spec}(R)$, is the set of prime ideals of R.
- We set $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \subseteq \mathfrak{p}\}$, the set of primes containing I.
- We set $D(I) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid I \not\subseteq \mathfrak{p}\}$, the set of primes *not* containing I.
- More generally, for any subset $S \subseteq R$, we define $V(S)$ and $D(S)$ analogously.

DEFINITION/PROPOSITION: The collection $\{V(I) \mid I \text{ an ideal of } R\}$ is the collection of closed subsets of a topology on R, called the **Zariski topology**; equivalently, the open sets are $D(I)$ for I an ideal of R.

DEFINITION: Let $\phi : R \to S$ be a ring homomorphism. Then the **induced map on Spec** corresponding to ϕ is the map $\phi^* : \operatorname{Spec}(S) \to \operatorname{Spec}(R)$ given by $\phi^*(\mathfrak{p}) := \phi^{-1}(\mathfrak{p})$.

LEMMA: Let $\mathfrak{p}$ be a prime ideal. Let I_λ, J be ideals.

(1) $\sum_\lambda I_\lambda \subseteq \mathfrak{p} \iff I_\lambda \subseteq \mathfrak{p}$ for all λ.
(2) $IJ \subseteq \mathfrak{p} \iff I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$
(3) $I \cap J \subseteq \mathfrak{p} \iff I \subseteq \mathfrak{p}$ or $J \subseteq \mathfrak{p}$
(4) $I \subseteq \mathfrak{p} \iff \sqrt{I} \subseteq \mathfrak{p}$

(1) The spectrum of some reasonably small rings.

(a) Let $R = \mathbb{Z}$ be the ring of integers.

(i) What are the elements of $\operatorname{Spec}(R)$? Be careful not to forget (0)!

(ii) Draw a picture $\operatorname{Spec}(R)$ (with $\cdots$ since you can't list everything) with a line going up from $\mathfrak{p}$ to $\mathfrak{q}$ if $\mathfrak{p} \subset \mathfrak{q}$.

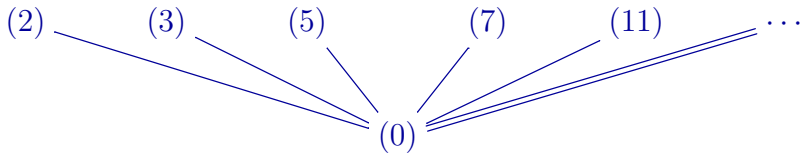
(iii) Describe the sets $V(I)$ and $D(I)$ for any ideal I.

(b) Same questions for $R = K$ a field.

(c) Same questions for the polynomial ring $R = \mathbb{C}[X]$.

(d) Same questions[1] for the power series ring $R = K[\![X]\!]$ for a field K.

(a) The spectrum of $\mathbb{Z}$ is, as a poset:

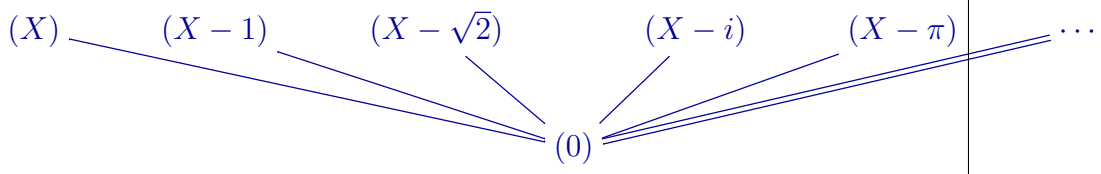


The sets $D((n))$ are the whole space when $n = 1$, the empty set with $n = 0$, and any complement of finite union of things in the top row otherwise. The sets $V((n))$ are the whole space when $n = 0$, the empty set with $n = 1$, and any finite union of things in the top row otherwise.

(b) The spectrum of a field is just $\{(0)\}$.

[1] Spoiler: The only primes are (0) and (X). To prove it, show/recall that any nonzero series f can be written as $f = X^n u$ for some unit $u \in K[\![X]\!]$.

(c) The spectrum of $\mathbb{C}[X]$ is, as a poset:



For an element f, $V((f))$ corresponds to the irreducible factors of f. The sets $D((f))$ are the whole space when $f = 1$, the empty set with $f = 0$, and any complement of finite union of things in the top row otherwise. The sets $V((f))$ are the whole space when $f = 0$, the empty set with $f = 1$, and any finite union of things in the top row otherwise.

(d)

The sets V are $\varnothing$, $\{(X)\}$, and $\{(0),(X)\}$. The sets D are $\varnothing$, $\{(0)\}$, and $\{(0),(X)\}$.

(2) More Spectra.

(a) Let $R = \mathbb{C}[X,Y]$ be a polynomial ring in two variables. Find some maximal ideals, the zero ideal, and some primes that are neither. Draw a picture like the ones from the previous problem to illustrate some containments between these.

(b) Let R be a ring and I be an ideal. Use the Second Isomorphism Theorem to give a natural bijection between $\mathrm{Spec}(R/I)$ and $V(I)$.

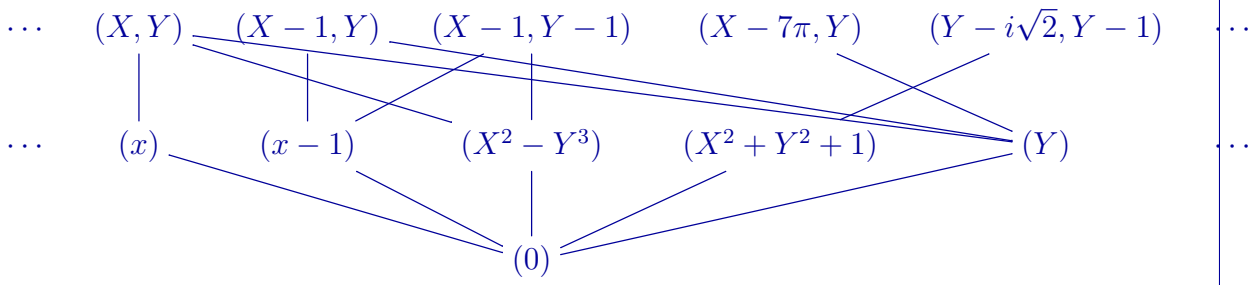
(c) Let $R = \dfrac{\mathbb{C}[X,Y]}{(XY)}$. Let $x = [X]$ and $y = [Y]$.

(i) Use the definition of prime ideal to show that $\mathrm{Spec}(R) = V(x) \cup V(y)$.

(ii) Use the previous problem to completely describe $V(x)$ and $V(y)$.

(iii) Give a complete description/picture of $\mathrm{Spec}(R)$.

(a)

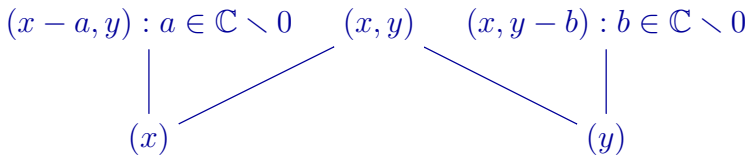


(b) $\mathfrak{p} \in V(I)$ maps to $\mathfrak{p}/I \in \mathrm{Spec}(R/I)$.

(c) **(i)** Since $xy = 0$, if $\mathfrak{p}$ is prime, we must have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

(ii) $V(x) \cong \mathrm{Spec}(R/(x)) \cong \mathrm{Spec}(\mathbb{C}[Y])$ and $V(y) \cong \mathrm{Spec}(R/(y)) \cong \mathrm{Spec}(\mathbb{C}[X])$.

(iii)



(3) Let R be a ring.

(a) Show that for any subset S of R, $V(S) = V(I)$ where $I = (S)$.

(b) Translate the lemma to fill in the blanks:

$V(I) \_\_ V(\sqrt{I})$	$D(I) \_\_ D(\sqrt{I})$
$V(\sum_\lambda I_\lambda) \_\_\_\_ V(I_\lambda)$	$D(\sum_\lambda I_\lambda) \_\_\_\_ D(I_\lambda)$
$V(f_1,\dots,f_n) \_\_ V(f_1) \_\_ \cdots \_\_ V(f_n)$	$D(f_1,\dots,f_n) \_\_ D(f_1) \_\_ \cdots \_\_ D(f_n)$
$V(IJ) \_\_\_ V(I) \_\_\_ V(J)$	$D(IJ) \_\_\_ D(I) \_\_\_ D(J)$
$V(I \cap J) \_\_\_ V(I) \_\_\_ V(J)$	$D(I \cap J) \_\_\_ D(I) \_\_\_ D(J)$

(c) Use the above to verify that the Zariski topology indeed satisfies the axioms of a topology.

(a) This follows from definition of generating set of an ideal.

(b)

$V(I) = V(\sqrt{I})$	$D(I) = D(\sqrt{I})$
$V(\sum_\lambda I_\lambda) = \bigcap_\lambda V(I_\lambda)$	$D(\sum_\lambda I_\lambda) = \bigcup_\lambda D(I_\lambda)$
$V(f_1,\dots,f_n) = V(f_1) \cap \cdots \cap V(f_n)$	$D(f_1,\dots,f_n) = D(f_1) \cup \cdots \cup D(f_n)$
$V(IJ) = V(I) \cup V(J)$	$D(IJ) = D(I) \cap D(J)$
$V(I \cap J) = V(I) \cup V(J)$	$D(I \cap J) = D(I) \cap D(J)$

(c) The D's are closed under arbitrary unions and finite intersection; we also have $\mathrm{Spec}(R) = D(1)$ and $\varnothing = D(0)$.

---

(4) The induced map on Spec: Let $\phi : R \to S$ be a ring homomorphism.

(a) Show that for any prime ideal $\mathfrak{q} \subseteq S$, the ideal $\phi^*(\mathfrak{q}) = \phi^{-1}(\mathfrak{q})$ is a prime ideal of R.

(b) Show that for any ideal $I \in R$, we have

$$(\phi^*)^{-1}(V(I)) = V(IS) \text{ and } (\phi^*)^{-1}(D(I)) = D(IS).$$

(c) Show that ϕ^* is continuous.

(d) If $\phi : R \to R/I$ is quotient map, describe ϕ^*.

(a) $\phi^{-1}(\mathfrak{q})$ is the kernel of the map $R \xrightarrow{\phi} S \to S/\mathfrak{q}$, so by the First Isomorphism Theorem, $R/\phi^{-1}(\mathfrak{q})$ is isomorphic to a subring of $S/\mathfrak{q}$. Since $S/\mathfrak{q}$ is a domain, so is $R/\phi^{-1}(\mathfrak{q})$, so $\phi^{-1}(\mathfrak{q})$ is a prime ideal.
(b) Let $\mathfrak{q} \in \operatorname{Spec}(S)$. We claim that $\mathfrak{q} \in V(IS)$ if and only if $\mathfrak{p} := \phi^*(\mathfrak{q}) \in V(I)$, which shows both statements. Indeed, $\mathfrak{q} \in V(IS)$ is equivalent to $\mathfrak{q}$ contains IS. Since IS is generated by $\phi(I)$, this is equivalent to $\mathfrak{q} \supseteq \phi(I)$, which is equivalent to $\phi^{-1}(\mathfrak{q}) \supseteq I$. But this is the same as $\phi^{-1}(\mathfrak{q}) \in V(I)$.
(c) Follows from the previous.
(d) This corresponds to the embedding $V(I) \subseteq \operatorname{Spec}(R)$.

(5) Let R and S be rings. Describe $\operatorname{Spec}(R \times S)$ in terms of $\operatorname{Spec}(R)$ and $\operatorname{Spec}(S)$.

(6) Properties of $\operatorname{Spec}(R)$.
(a) Show that for any ring R, the space $\operatorname{Spec}(R)$ is compact.
(b) Show that if $\operatorname{Spec}(R)$ is Hausdorff, then every prime of R is maximal.
(c) Show that $\operatorname{Spec}(R) \cong \operatorname{Spec}(R/\sqrt{0})$.

(7) Let K be a field, and $R = \dfrac{K[X_1, X_2, \dots]}{(\{X_i - X_i X_j \mid 1 \leq i \leq j\})}$. Describe $\operatorname{Spec}(R)$ as a set and as a topological space.

§4.19: SPECTRUM OF A RING

FORMAL NULLSTELLENSATZ: Let R be a ring, I an ideal, and $f \in R$. Then $V(f) \supseteq V(I)$ if and only if $f \in \sqrt{I}$.

COROLLARY 1: Let R be a ring. There is a bijection

$$\{\text{radical ideals in } R\} \longleftrightarrow \{\text{closed subsets of } \mathrm{Spec}(R)\}.$$

DEFINITION: Let R be a ring and I an ideal. A **minimal prime** of I is a prime $\mathfrak{p}$ that contains I, and is minimal among primes containing I. We write $\mathrm{Min}(I)$ for the set of minimal primes of I.

LEMMA: Every prime that contains I contains a minimal prime of I.

COROLLARY 2: Let R be a ring and I be an ideal. Then

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in \mathrm{Min}(I)} \mathfrak{p}.$$

DEFINITION: A subset W of a ring R is **multiplicatively closed** if $1 \in W$ and $u, v \in W$ implies $uv \in W$.

PROPOSITION: Let R be a ring and W be a multiplicatively closed subset. Then every ideal I such that $I \cap W = \varnothing$ is contained in a prime ideal $\mathfrak{p}$ such that $\mathfrak{p} \cap W = \varnothing$.

(1) Proof of Formal Nullstellensatz and Corollaries.
- **(a)** Show the direction $(\Leftarrow)$ of Formal Nullstellensatz.
- **(b)** Verify that $W = \{f^n \mid n \geq 0\}$ is a multiplicatively closed set. Then apply the Proposition to prove the direction $(\Rightarrow)$ of Formal Nullstellesatz.
- **(c)** Prove Corollary 1.
- **(d)** Prove the Lemma.
- **(e)** Prove Corollary 2.
- **(f)** What does Corollary 2 say in the special case $I = (0)$?

- **(a)** Suppose that $f \in \sqrt{I}$, so $f^n \in I$. If $\mathfrak{p} \in V(I)$, then $I \subseteq \mathfrak{p}$, and $f^n \in \mathfrak{p}$ implies $f \in \mathfrak{p}$, so $\mathfrak{p} \in V(f)$.
- **(b)** Yes, it is a multiplicatively closed set. If $f \notin \sqrt{I}$, then $W \cap I = \varnothing$, so there is some prime $\mathfrak{p}$ such that $W \cap \mathfrak{p} = \varnothing$. In particular, $f \notin \mathfrak{p}$, so $V(f) \not\supseteq V(I)$.
- **(c)** We map a radical ideal I to the closed set $V(I)$. This is surjective since $V(J) = V(\sqrt{J})$. If I, J are distinct radical ideals, then take some $f \in J \smallsetminus I$. Then $V(f)$ contains $V(I)$ but not $V(J)$, so $V(I) \neq V(J)$.
- **(d)** Usual Zorn's Lemma argument.
- **(e)** If $f \in \sqrt{I}$, then $f \in V(\mathfrak{p})$ for all $\mathfrak{p}$ containing I, so f is in every minimal prime of I. On the other hand, if f is in every minimal prime of I, then it is in every prime containing I, so $V(f) \supseteq V(I)$, which implies $f \in \sqrt{I}$.
- **(f)** An element is nilpotent if and only if it is in every minimal prime of the ring.

(2) Use the Formal Nullstellensatz to fill in the blanks:

$$f \text{ is nilpotent} \iff V(f) = \_\_\_\_ \iff D(f) = \_\_\_\_.$$

What property replaces "nilpotent" if you swap the blanks for V and D above?

$$f \text{ is nilpotent} \iff V(f) = \operatorname{Spec}(R) \iff D(f) = \varnothing.$$

The opposite property is unit.

(3) Prove[1] the Proposition.

Given an increasing union of ideals that don't intersect I, the union is an ideal and does not intersect I, so by Zorn's Lemma, there is an ideal maximal among those that don't intersect I; call it J. Let $ab \in J$ with $a, b \notin J$. Then $(J + (a)) \cap W$ and $(J + (b)) \cap W$ are nonempty. Say u, v are elements in the respective intersections. Then $u = j_1 + ar_1$ and $v = j_2 + br_2$, and $uv = j_1 j_2 + j_1 b r_2 + j_2 a r_2 + ab r_1 r_2 \in J$.

(4) Let R be a ring. Show[2] that $\operatorname{Spec}(R)$ is connected as a topological space if and only if $R \ncong S \times T$ for rings[3] S, T.

First, suppose that $R \cong S \times T$. Then any prime ideal of R is of the form $\mathfrak{p} \times T$ for $\mathfrak{p} \in \operatorname{Spec}(S)$ or $S \times \mathfrak{q}$ for $\mathfrak{q} \in \operatorname{Spec}(T)$. So, as sets, there is a bijection $\operatorname{Spec}(R) \leftrightarrow \operatorname{Spec}(S) \coprod \operatorname{Spec}(T)$. Moveover, this is a homeomorphism: the ideals in $S \times T$ are of the form $I \times J$, and $V(I \times J) \subseteq \operatorname{Spec}(S \times T)$ corresponds to $V(I) \coprod V(J) \subseteq \operatorname{Spec}(S) \coprod \operatorname{Spec}(T)$, so this is the disjoint union topology. In particular, $\operatorname{Spec}(S)$ and $\operatorname{Spec}(T)$ are form a disconnection.

From above, we know that $\operatorname{Spec}(S \times T) \cong \operatorname{Spec}(S) \coprod \operatorname{Spec}(T)$ so it suffices to show that $\operatorname{Spec}(R)$ disconnected implies that R has a nontrivial idempotent. Applying the definition of disconnected, there exists some closed sets $V(I), V(J)$ such that $V(I) \cup V(J) = \operatorname{Spec}(R)$ and $V(I) \cap V(J) = \varnothing$. Thus $\sqrt{I + J} = R$, so $I + J = R$ and $\sqrt{I \cap J} = \sqrt{0}$, so $I \cap J$ consists of nilpotents. By CRT, we have $R/(I \cap J) \cong R/I \times R/J$. Set $N = I \cap J$. We have that there is a nontrivial idempotent in R/N but $e, 1 - e \notin N$. So there is some $e \in R$ such that $e - e^2 \in N$ so $e^n(1-e)^n = 0$ for some n. Set $I' = (e^n)$ and $J' = (1 - e)^n$. We claim that $I' + J' = R$ and $I' \cap J' = 0$. Indeed, in R/I', $\overline{e}$ is nilpotent, so $\overline{1 - e}$ is a unit, as is $(1 - e)^n$. Thus, we can write $(1 - e)^n u = 1 + e^n f$ for some $u, f \in R$, and hence $1 \in I' + J'$; then $I' \cap J' = I'J' = 0$. By CRT we have $R \cong R/I' \times R/J'$. Finally, it remains to note that $I', J' \neq 0$ to see that this is proper: we have $0 \neq \overline{e} = \overline{e^2} = \cdots = \overline{e^n}$ in R/N, so we must have $e^n \neq 0$ and likewise $(1-e)^n \neq 0$.

[1] Hint: Take an ideal maximal among those that don't intersect W.

[2] Start with the $(\Rightarrow)$ direction. For the other direction, use CRT.

[3] Recall that the zero ring is not a ring.

§5.20: LOCAL RINGS AND NAK

DEFINITION: A ring is **local** if it has a unique maximal ideal. We write $(R, \mathfrak{m})$ for a local ring to denote the ring R and the maximal ideal $\mathfrak{m}$; we many also write $(R, \mathfrak{m}, k)$ to indicate the residue field $k := R/\mathfrak{m}$.

GENERAL NAK: Let R be a ring, I an ideal, and M be a finitely generated module. If $IM = M$, then there is some $a \in R$ such that $a \equiv 1 \bmod I$ and $aM = 0$.

LOCAL NAK 1: Let $(R, \mathfrak{m})$ be a local ring and M be a finitely generated module. If $M = \mathfrak{m}M$, then $M = 0$.

LOCAL NAK 2: Let $(R, \mathfrak{m})$ be a local ring and M be a finitely generated module. Let N be a submodule of M. Then $M = N + \mathfrak{m}M$ if and only if $M = N$.

LOCAL NAK 3: Let $(R, \mathfrak{m}, k)$ be a local ring and M be a finitely generated module. Then a set of elements $S \subseteq M$ generates M if and only if the image of S in $M/\mathfrak{m}M$ generates $M/\mathfrak{m}M$ as a k-vector space.

DEFINITION: Let $(R, \mathfrak{m}, k)$ be a local ring and M be a finitely generated module. A set of elements S of M is a **minimal generating set** for M if the image of S in $M/\mathfrak{m}M$ is a basis for $M/\mathfrak{m}M$ as a k-vector space.

(1) Local rings.

(a) Show that for a ring R the following are equivalent:
- R is a local ring.
- The set of all nonunits forms an ideal.
- The set of all nonunits is closed under addition.

(b) Show that if A is a domain then $A[X]$ is *not* a local ring.

(c) Show that if K is a field, the power series ring $R = K[\![X_1, \ldots, X_n]\!]$ is a local ring.

(d) Let $p \in \mathbb{Z}$ be a prime number, and $\mathbb{Z}_{(p)} \subseteq \mathbb{Q}$ be the set of rational numbers that can be written with denominator *not* a multiple of p. Show that $(\mathbb{Z}_{(p)}, p\mathbb{Z}_{(p)})$ is a local ring.

(e) Show that any quotient of a local ring is also a local ring.

(a) Since any element times a nonunit is a nonunit, the last two are equivalent. Recall that an element is a unit if and only if it is not in any maximal ideal. So, if $(R, \mathfrak{m})$ is local, the nonunits are the elements of $\mathfrak{m}$, which is an ideal; conversely, if the nonunits form an ideal, then this ideal must be the unique maximal ideal.

(b) X and $X + 1$ are nonunits, but $1 = (X + 1) - X$ is a unit.

(c) The set of nonunits is the elements with zero constant term, which is the ideal $(X_1, \ldots, X_n)$.

(d) First, check that this is a ring. Then note that the units in this ring are the fractions a/b with $p \nmid a, b$, which is complement of the ideal $p\mathbb{Z}_{(p)}$.

(e) This follows from the Lattice Isomorphism Theorem.

(2) General NAK implies Local NAKs

(a) Show that General NAK implies Local NAK 1.

(b) Briefly[1] explain why Local NAK 1 implies Local NAK 2.
(c) Briefly[2] explain why Local NAK 2 implies Local NAK 3.
(d) Use Local NAK 3 to briefly explain why a minimal generating set is a generating set, and that, in this setting, any generating set contains a minimal generating set.

(a) If $\mathfrak{m}M = M$, then by General NAK, there is some $a \in \mathfrak{m}$ such that $a \equiv 1 \bmod \mathfrak{m}$ and $aM = 0$. But a must be a unit, so $M = 0$!
(b) Same as the graded case: apply NAK 1 to M/N.
(c) Same as the graded case: apply NAK 2 to $N = \sum_{s \in S} Rs$.
(d) Same as the graded case: a k-basis for $M/\mathfrak{m}M$ is a k-spanning set for $M/\mathfrak{m}M$, and any k-spanning set for $M/\mathfrak{m}M$ contains a k-basis.

(3) Proof of General NAK: Let $M = \sum_{i=1}^{n} Rm_i$. Set v to be the row vector $[m_1, \ldots, m_n]$.
(a) Suppose that $IM = M$. Explain why there is an $n \times n$ matrix A with entries in I such that $vA = v$.
(b) Apply a TRICK and complete the proof.

(a) Each m_i is an element of IM, so we can write $m_i = \sum_j b_j n_j$ with $n_j \in M$ and $b_j \in I$. We can then write n_j as a linear combination of the m_i's. Combining all together, we can write $m_i = \sum_j a_j m_j$ with $a_j \in I$. These linear combinations are the columns of a matrix A as desired.
(b) By the Eigenvector trick, $\det(A - \mathbb{1})$ kills v, so kills M. Going mod I we have $\det(A - \mathbb{1}) \equiv \det(-\mathbb{1}) \equiv \pm 1$; up to sign, $a = \det(A - \mathbb{1})$ is the element we seek.

(4) Let $(R, \mathfrak{m})$ be a local ring, $f \in R$ not a unit, and M be a nonzero finitely generated module. Show that there is some element of M that is *not* a multiple of f.

Suppose otherwise. Then $M = fM$. We have $f \in \mathfrak{m}$, so $M = fM \subseteq \mathfrak{m}M \subseteq M$, so $M = \mathfrak{m}M$. But by NAK, we then have $M = 0$, a contradiction.

(5) Applications of NAK.
(a) Let R be a ring and I be a finitely generated ideal. Show that if $I^2 = I$ then there is some idempotent e such that $I = (e)$.
(b) Find a counterexample to (a) if I is *not* assumed to be finitely generated.
(c) Let $(R, \mathfrak{m})$ be a Noetherian local ring and M be a finitely generated module. Show that $\bigcap_{n \geq 1} \mathfrak{m}^n M = 0$.
(d) Find a counterexample to (c) if $(R, \mathfrak{m})$ is still Noetherian local but M is not finitely generated.
(e) Find a counterexample to (c) if $(R, \mathfrak{m})$ with $M = R$, $\mathfrak{m}$ is a maximal ideal, but R is not necessarily Noetherian and local.
(f) Let R be a Noetherian ring, and M a finitely generated module. Let $\phi : M \to M$ be a surjective R-module homomorphism. Show[3] that ϕ must also be injective.
(g) Let $(R, \mathfrak{m})$ be a local ring. Suppose that $R_{\text{red}} := R/\sqrt{0}$ is a domain, and that there is some $f \in R$ such that R/fR is reduced (and nonzero). Show that R is reduced (and hence a domain).

[1] Reuse an old argument in a similar setting.
[2] It's déjà vu all over again.
[3] Hint: Take a page from the 818 playbook and give M an $R[X]$-module structure.

§5.21: LOCALIZATION OF RINGS

DEFINITION: Let R be a ring and W a multiplicatively closed subset with $0 \notin W$. The **localization** $W^{-1}R$ is the ring with

- elements equivalence classes of $(r, w) \in R \times W$, with the class of (r, w) denoted as $\dfrac{r}{w}$.
- with equivalence relation $\dfrac{s}{u} = \dfrac{t}{v}$ if there is some $w \in W$ such that $w(sv - tu) = 0$,
- addition given by $\dfrac{s}{u} + \dfrac{t}{v} = \dfrac{sv + tu}{uv}$, and
- multiplication given by $\dfrac{s}{u}\dfrac{t}{v} = \dfrac{st}{uv}$.

(If $0 \in W$, then $W^{-1}R := 0$, which by our convention is not a ring.)

DEFINITION: Let R be a ring.

- If $f \in R$ is nonnilpotent[1], then $R_f := \{1, f, f^2, \dots\}^{-1}R$.
- If $\mathfrak{p} \subseteq R$ is a prime ideal then $R_{\mathfrak{p}} := (R \smallsetminus \mathfrak{p})^{-1}R$.
- The **total quotient ring** of R is $\mathrm{Frac}(R) := \{w \in R \mid w \text{ is a nonzerodivisor}\}^{-1}R$.

For a ring R, multiplicative set $W \not\ni 0$, and an ideal I, we define

$$W^{-1}I := \left\{ \frac{a}{w} \in W^{-1}R \mid a \in I \right\}.$$

THEOREM: Let R be a ring and W be a multiplicatively closed subset. Then the map induced on Spec corresponding to the natural map $R \to W^{-1}R$ yields a homeomorphism into its image:

$$\mathrm{Spec}(W^{-1}R) \cong \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}.$$

LEMMA: Let R be a ring and W be a multiplicatively closed subset.

(1) For any ideal $I \subseteq R$, $W^{-1}I = I(W^{-1}R)$.
(2) For any ideal $I \subseteq R$, $W^{-1}I \cap R = \{r \in R \mid \exists w \in W : wr \in I\}$.
(3) For any ideal $J \subseteq W^{-1}R$, $W^{-1}(J \cap R) = J$.
(4) For any prime ideal $\mathfrak{p} \subseteq R$ with[2] $\mathfrak{p} \cap W = \varnothing$, $W^{-1}\mathfrak{p}$ is prime.

(1) Computing localizations

(a) What is the natural ring homomorphism $R \to W^{-1}R$?
(b) Show that the kernel of $R \to W^{-1}R$ is ${}^{W}0 := \{r \in R \mid \exists w \in W : wr = 0\}$.
(c) If every element of W is a nonzerodivisor, explain why the equivalence relation on $W^{-1}R$ simplifies to $\frac{s}{u} = \frac{t}{v}$ if and only if $sv = tu$.
(d) If R is a domain, explain why $\mathrm{Frac}(R)$ is the usual fraction field of R.
(e) If R is a domain, explain why $W^{-1}R$ is a subring of the fraction field of R. Which subring?
(f) Let $\overline{R} = R/{}^{W}0$ and $\overline{W}$ be the image of W in $\overline{R}$. Show that $W^{-1}R \cong \overline{W}^{-1}\overline{R}$.

[1] If f is nilpotent, $0 \in \{1, f, f^2, \dots\}$ so $R_f = 0$.
[2] If $W \cap \mathfrak{p} \ni a$, then $W^{-1}\mathfrak{p} \ni \frac{a}{a} = \frac{1}{1}$, so $W^{-1}\mathfrak{p} = W^{-1}R$ is the improper ideal!

(a) $r \mapsto \frac{r}{1}$.
(b) $\frac{r}{1} = \frac{0}{1}$ if and only if $\exists w \in W : rw = w(1r - 0) = 0$.
(c) $w(sv - tu) = 0$ and w a nonzerdivisor implies $sv - tu = 0$; i.e., $sv = tu$.
(d) In light of the above, it's just the definition.
(e) The equivalence relation on the fractions is the same as that in the fraction field, so the map is injective; the operations are definitely the same. It is the subring consisting of fractions that can be written with denominator in W.
(f) We define a map from $W^{-1}R \to \overline{W}^{-1}\overline{R}$ by $\frac{r}{w} \mapsto \frac{\overline{r}}{\overline{w}}$. It is clear from the construction that this is a surjective homomorphism. Suppose that $\frac{r}{w}$ is in the kernel, so $\frac{\overline{r}}{\overline{w}} = \frac{\overline{0}}{\overline{1}}$. This means that there is some $\overline{v} \in \overline{W}$ such that $\overline{vr} = \overline{0}$; i.e., $vr \in {}^{W}0$ for some $v \in W$. Then there is some $u \in W$ such that $uvr = 0$, but $uv \in W$, so $\frac{r}{w} = \frac{0}{1}$ in $W^{-1}R$.

(2) Ideals in localizations: Let R be a ring and W a multiplicatively closed set.
(a) Use the Theorem to show that, if $f \in R$ is nonnilpotent, then

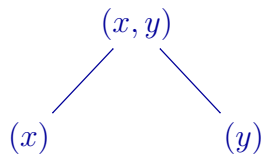
$$\mathrm{Spec}(R_f) \cong D(f) \subseteq \mathrm{Spec}(R).$$

(b) Use the Theorem to show that, if $\mathfrak{p} \subseteq R$ is prime, then

$$\mathrm{Spec}(R_{\mathfrak{p}}) \cong \{\mathfrak{q} \in \mathrm{Spec}(R) \mid \mathfrak{q} \subseteq \mathfrak{p}\} =: \Lambda(\mathfrak{p}).$$

Deduce that $R_{\mathfrak{p}}$ is always a *local* ring.
(c) Draw[3] a picture of $\mathrm{Spec}(\frac{\mathbb{C}[X,Y]}{(XY)_{(x,y)}})$.
(d) Use Part (3) of the Lemma to show that every ideal of $W^{-1}R$ is of the form $W^{-1}I$ for some ideal $I \subseteq R$.
(e) Use Part (3) of the Lemma to show that any localization of a Noetherian ring is Noetherian.

(a) The condition $\mathfrak{p} \cap \{1, f, f^2, \dots\} = \varnothing$ is equivalent to $f \notin \mathfrak{p}$; i.e., $f \in D(\mathfrak{p})$.
(b) The condition $\mathfrak{q} \cap (R \setminus \mathfrak{p}) = \varnothing$ is equivalent to $\mathfrak{q} \subseteq \mathfrak{p}$; i.e., $\mathfrak{q} \in \Lambda(\mathfrak{p})$. There is a unique maximal element in this set, namely $\mathfrak{p}$, so $R_{\mathfrak{p}}$ is local.
(c)



(d) Clear.
(e) Given an ideal of $W^{-1}R$, write it as $I(W^{-1}R)$ for some ideal I of R. Then $I = (f_1, \dots, f_t)$ by Noetherianity, whence $I(W^{-1}R)$ is generated by the images $\frac{f_1}{1}, \dots, \frac{f_t}{1}$.

(3) Examples of localizations
(a) Describe as concretely as possible the rings $\mathbb{Z}_2$ and $\mathbb{Z}_{(2)}$ as defined above.
(b) Describe as concretely as possible the rings $K[X]_X$ and $K[X]_{(X)}$.
(c) Describe as concretely as possible the rings $K[X,Y]_X$ and $K[X,Y]_{(X)}$.
(d) Describe as concretely as possible the rings $\left(\frac{K[X,Y]}{(XY)}\right)_x$ and $\left(\frac{K[X,Y]}{(XY)}\right)_{(x)}$.

[3]Recall that $\mathrm{Spec}(\frac{\mathbb{C}[X,Y]}{(XY)})$ consists of $\{(x), (y), (x, y - \alpha), (x - \beta, y) \mid \alpha, \beta \in \mathbb{C}\}$.

(e) Describe as concretely as possible $\left(\frac{K[X,Y]}{(X^2)}\right)_x$ and $\left(\frac{K[X,Y]}{(X^2)}\right)_{(x)}$.

(a) $\mathbb{Z}_2 = \{a/b \in \mathbb{Q} \mid b = 2^n\}$ and $\mathbb{Z}_{(2)} = \{a/b \in \mathbb{Q} \mid 2 \nmid b\}$.
(b) $K[X]_X = \{f/g \in K(X) \mid g = X^n\}$ and $K[X]_{(X)} = \{f/g \in K(X) \mid X \nmid g\}$.
(c) $K[X,Y]_X = \{f/g \in K(X,Y) \mid g = X^n\}$
and $K[X,Y]_{(X)} = \{f/g \in K(X,Y) \mid X \nmid g\}$.
(d) $\left(\frac{K[X,Y]}{(XY)}\right)_x \cong K[X,X^{-1}]$ and $\left(\frac{K[X,Y]}{(XY)}\right)_{(x)} \cong K(Y)$.
(e) $\left(\frac{K[X,Y]}{(X^2)}\right)_x \cong K[Y]$ and $\left(\frac{K[X,Y]}{(X^2)}\right)_{(x)} \cong K(Y)[X]/(X^2)$.

(4) Prove the Lemma and the Theorem.

Lemma:
(a) For the containment $\subseteq$, we have $\frac{a}{w} = \frac{a}{1}\frac{1}{w}$. For the other, given $\sum_i \frac{a_i}{1}\frac{r_i}{w_i}$, take $w = w_1 \cdots w_t$ and w_i' to be the product of all w's except w_i; then

$$\sum_i \frac{a_i}{1}\frac{r_i}{w_i} = \sum_i \frac{a_i}{1}\frac{w_i' r_i}{w} = \sum_i \frac{a_i w_i' r_i}{w} \in W^{-1}I.$$

(b) We have $r \in W^{-1}I \cap R$ if and only if $\frac{r}{1} \in W^{-1}I$, so $\frac{r}{1} = \frac{a}{w}$ some $a \in I, w \in W$. Then there is some $u \in W$ such that $u(wr - a) = 0$, so $(uw)r \in I$, as claimed.
(c) Let $j = \frac{r}{w} \in J$. Then $\frac{r}{1} = wj \in J \cap R$, $\frac{r}{w} = \frac{1}{w}\frac{r}{1} \in W^{-1}(J \cap R)$. Conversely, if $\frac{a}{w} \in W^{-1}(J \cap R)$ so $a \in J \cap R$, then $\frac{a}{1} \in J$, and $\frac{a}{w} = \frac{1}{w}\frac{a}{1} \in J$.
(d) Let $\frac{a}{u}, \frac{b}{v} \in W^{-1}R$, and $\frac{ab}{uv} \in W^{-1}\mathfrak{p}$. Then there are some $w \in W$ and $p \in \mathfrak{p}$ such that $\frac{ab}{uv} = \frac{p}{w}$, so there is $t \in W$ with $t(wab - uvp) = 0$, so $(tw)ab \in \mathfrak{p}$. Since $W \cap \mathfrak{p} = \varnothing$, $tw \notin \mathfrak{p}$ so $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, and hence $\frac{a}{u} \in W^{-1}\mathfrak{p}$ or $\frac{b}{v} \in W^{-1}\mathfrak{p}$.

Theorem: Suppose that $\mathfrak{q}$ is a prime ideal in $W^{-1}R$ and $\mathfrak{q} \cap R = \mathfrak{p}$. Then $W^{-1}\mathfrak{p} = W^{-1}(\mathfrak{q} \cap R) = \mathfrak{q}$. This shows that the only ideal (in particular, the only prime ideal) that contracts to $\mathfrak{p}$ is $W^{-1}\mathfrak{p}$, so this map is injective. Since $W^{-1}\mathfrak{p}$ is prime for any $\mathfrak{p} \cap W = \varnothing$, and is the bogus ideal otherwise, the image is exactly the primes with $\mathfrak{p} \cap W = \varnothing$. To see that it induces a homeomorphism onto its image, it suffices to show that the image of a closed set is closed. One checks from the definition that the image of $V(W^{-1}I)$ is $V(I) \cap \{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}$.

(5) Prove the following LEMMA: If V, W are multiplicatively closed sets, then $(VW)^{-1}R \cong (\frac{V}{1})^{-1}(W^{-1}R)$, where $(\frac{V}{1})^{-1}$ is the image of V in $W^{-1}R$.

Check that the map $(r/w)/(v/1) \mapsto r/(wv)$ is an isomorphism: it is clearly a ring homomorphism, and clearly surjective. If $r/(wv)$ is zero, then there is some $u \in VW$ with $ur = 0$. We can write $u = st$ with $s \in V$ and $t \in W$, so $str = 0$. But this implies that $s(r/w) = 0$ in $W^{-1}R$ (because there is some $t \in W$ such that $str = 0$), and this means that $(r/w)/(v/1) = 0$.

(6) Minimal primes.
   (a) Let $\mathfrak{p}$ be a minimal prime of R. Show that for any $a \in \mathfrak{p}$, there is some $u \notin \mathfrak{p}$ and $n \geq 1$ such that $ua^n = 0$.
   (b) Show that the set of minimal[4] primes $\mathrm{Min}(R)$ with the induced topology from $\mathrm{Spec}(R)$ is Hausdorff.
   (c) Let $R = K[X_1, X_2, X_3, \dots]/(\{X_i X_j \mid i \neq j\})$. Describe $\mathrm{Min}(R)$ as a topological space.

[4] $\mathrm{Min}(R)$ denotes the set of primes of R that are minimal. This is the same as $\mathrm{Min}(0)$ in our notation of minimal primes of an ideal; this conflict of notation is standard.

§5.22: LOCALIZATION OF MODULES

DEFINITION: Let R be a ring, M an R-module, and W a multiplicatively closed subset. The **localization** $W^{-1}M$ is the $W^{-1}R$-module[1] with

- elements equivalence classes of $(m, w) \in M \times W$, with the class of (m, w) denoted as $\frac{m}{w}$.
- with equivalence relation $\frac{m}{u} = \frac{n}{v}$ if there is some $w \in W$ such that $w(vm - un) = 0$,
- addition given by $\frac{m}{u} + \frac{n}{v} = \frac{vm + un}{uv}$, and
- action given by $\frac{r}{u}\frac{m}{v} = \frac{rm}{uv}$.

If $\alpha : M \to N$ is a homomorphism of R-modules, then the $W^{-1}R$-module homomorphism $W^{-1}\alpha : W^{-1}M \to W^{-1}N$ is defined by $W^{-1}\alpha(\frac{m}{w}) = \frac{\alpha(m)}{w}$.

DEFINITION: Let R be a ring and M a module.

- If $f \in R$, then $M_f := \{1, f, f^2, \dots\}^{-1}M$.
- If $\mathfrak{p} \subseteq R$ is a prime ideal then $M_{\mathfrak{p}} := (R \smallsetminus \mathfrak{p})^{-1}M$.

PROPOSITION: Let R be a ring, W a multiplicatively closed set, and $N \subseteq M$ be modules. Then

- $W^{-1}N$ is a submodule of $W^{-1}M$, and
- $W^{-1}(M/N) \cong \dfrac{W^{-1}M}{W^{-1}N}$.

COROLLARY: Let R be a ring, I an ideal, and W a multiplicatively closed subset. Then the map $R \to W^{-1}(R/I)$ induces an order preserving bijection

$$\operatorname{Spec}(W^{-1}(R/I)) \xrightarrow{\sim} \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p} \supseteq I \text{ and } \mathfrak{p} \cap W = \varnothing\}.$$

(1) Let M be an R-module and W be a multiplicatively closed set.

(a) What is the natural map from $M \to W^{-1}M$?

(b) If S is a generating set for M, explain why $\frac{S}{1} = \{\frac{s}{1} \mid s \in S\}$ is a generating set for $W^{-1}M$.

(c) Let $m \in M$. Show that $\frac{m}{u}$ is zero in $W^{-1}M$ if and only if there is some $w \in W$ such that $wm = 0$ in M.

(d) Let $m_1, \dots, m_t \in M$ be a finite set of elements. Show that $\frac{m_1}{u_1}, \dots, \frac{m_t}{u_t} \in W^{-1}M$ are all zero if and only if there is some $w \in W$ that such that $wm_i = 0$ in M for all i.

(e) Let M be a finitely generated module. Show that $W^{-1}M = 0$ if and only if $M_w = 0$ for some $w \in W$.

(f) Let $m \in M$ and $\mathfrak{p}$ be a prime ideal. Show that $\frac{m}{1} \neq 0$ in $M_{\mathfrak{p}}$ if and only if $\mathfrak{p} \supseteq \operatorname{ann}_R(m)$.

(a) $m \mapsto \frac{m}{1}$

(b) We can write $\frac{m}{w} = \frac{\sum_i r_i m_i}{w} = \sum_i \frac{r_i}{w}\frac{m_i}{1}$.

(c) $\frac{m}{u} = \frac{0}{1}$ iff $\exists w$ such that $0 = w(1m - 0u) = wm$.

(d) The "if" is clear; for the only if, we have $w_1 m_1 = \cdots w_t m_t = 0$ so we can take $w = w_1 \cdots w_t$.

[1] If $0 \in W$, then $W^{-1}R = 0$ is not a ring.

(e) Take a finite generating set for M. Then $W^{-1}M = 0$ iff each generator maps to 0 iff there is a w that kills each m_i iff the corresponding $M_w = 0$.
(f) $\frac{m}{1} = 0$ if and only if there is some $w \notin \mathfrak{p}$ with $wm = 0$, which happens if and only if $\mathfrak{p} \not\supseteq \operatorname{ann}_R(m)$.

(2) Prove the Proposition.

For the first part, we need to show that a nonzero element in $W^{-1}N$ is nonzero in $W^{-1}M$. If $\frac{n}{u} \neq 0$, in $W^{-1}M$ then there is some $w \in W$ such that $wn = 0$, which is the same as the condition to be zero in $W^{-1}N$.

For the second part, consider the map from $W^{-1}M$ to $W^{-1}(M/N)$ given by $\frac{m}{u} \mapsto \overline{m}u$. Clearly, $W^{-1}N$ is contained in the kernel. An element is in the kernel if and only if there is some $w \in W$ such that $w\overline{m} = 0$ in M/N, which means $wm \in N$. Then $\frac{m}{u} = \frac{wm}{wu} \in W^{-1}N$.

(3) Corollary.
(a) Rewrite the Corollary in the special case $W = R \setminus \mathfrak{p}$ for some prime $\mathfrak{p}$.
(b) Use the Proposition[2] to justify the Corollary.

(a) There is a bijection between $\operatorname{Spec}((R/I)_{\mathfrak{p}})$ and primes of R containing I but also contained in $\mathfrak{p}$.
(b) We have $W^{-1}(R/I) \cong W^{-1}R/W^{-1}I$. Fromt he Proposition, this is an isomorphism of R-modules, but it is easy to see that the map is in fact a ring isomorphism. The primes in $W^{-1}R$ are of the form $W^{-1}\mathfrak{p}$ for $\mathfrak{p} \in \operatorname{Spec}(R)$ such that $\mathfrak{p} \cap W = \varnothing$. By the lattice isomorphism theorem, the primes in $W^{-1}R/W^{-1}I$ correspond to primes $W^{-1}\mathfrak{p}$ that contain $W^{-1}I$. But if $\mathfrak{p} \supseteq I$ then $W^{-1}\mathfrak{p} \supseteq W^{-1}I$, and if $W^{-1}\mathfrak{p} \supseteq W^{-1}I$, then since $W^{-1}\mathfrak{p} \cap R = \mathfrak{p}$ (from definition of prime) $I \subseteq W^{-1}I \cap R \subseteq W^{-1}\mathfrak{p} \cap R = \mathfrak{p}$. Thus, there is a bijection between primes containing I and not intersecting W with primes of $W^{-1}(R/I)$.

(4) Invariance of base: Let $\phi : R \to S$ be a ring homomorphism, and $V \subseteq R$ and $W \subseteq S$ be multiplicatively closed sets such that $\phi(V) = W$. Show that for any S-module M, $V^{-1}M \cong W^{-1}M$.

(5) I'm already local!
(a) Suppose that the action of each $w \in W$ on M is invertible: for every $w \in W$ the map $m \mapsto mw$ is bijective. Show that $M \cong W^{-1}M$ via the natural map.
(b) Let R be a ring, $\mathfrak{m}$ a maximal ideal (so $R/\mathfrak{m}$ is a field), and M a module such that $\mathfrak{m}M = 0$. Show that $M \cong M_{\mathfrak{m}}$ by the natural map.
(c) More generally, show that[3] if for every $m \in M$ there is some n such that $\mathfrak{m}^n m = 0$, then $M \cong M_{\mathfrak{m}}$.

[2]Hint: You may want to show that, for $W \cap \mathfrak{p} = \varnothing$, $I \subseteq \mathfrak{p}$ if and only if $W^{-1}I \subseteq W^{-1}\mathfrak{p}$. For this, it may help to observe that $W^{-1}\mathfrak{p} \cap R = \mathfrak{p}$. You can also use that the isomorphism from the Proposition is a ring isomorphism when R is a ring and I is an ideal.
[3]Hint: Note that $R/\mathfrak{m}^n$ is local with maximal ideal (the image of) $\mathfrak{m}$.

(a) The map is injective, since $wm = 0$ implies $m = 0$, and surjective since $\frac{m}{w} = \frac{m'w}{w} = \frac{m'}{1}$ for some m'.
(b) Let $u \in R \setminus \mathfrak{m}$. Then since $R/\mathfrak{m}$ is a field, there is some $v \in R$ such that $uv \equiv 1 \mod \mathfrak{m}$. Then for any $m \in M$, we have $uvm = (1+a)m = m$ for some $a \in \mathfrak{m}$. In particular the action of v is the inverse of u.
(c) Because $R/\mathfrak{m}^n$ is local with maximal ideal $\mathfrak{m}$, every element not in $\mathfrak{m}$ in this ring is a unit. Thus, given $u \in R \setminus \mathfrak{m}$, there is some $v \in R$ such that $uv \equiv 1 \mod \mathfrak{m}^n$. This shows that the action of u on M is bijective and the first part applies.

(6) Prove the following:
LEMMA: Let R be a ring, W a multiplicatively closed set. Let M be a finitely presented[4] R-module, and N an arbitrary R-module. Then for any homomorphism of $W^{-1}R$-modules $\beta : W^{-1}M \to W^{-1}N$, there is some $w \in W$ and some R-module homomorphism $\alpha : M \to N$ such that $\beta = \frac{1}{w}W^{-1}\alpha$.
(a) Given β, show that there exists some $u \in W$ such that for every $m \in M$, $\frac{u}{1}\beta(\frac{M}{1}) \subseteq \frac{N}{1}$.
(b) Let $m_1, \ldots, m_a$ be a (finite) set of generators for M, and $A = [r_{ij}]$ be a corresponding (finite) matrix of relations. Let $n_1, \ldots, n_a$ be an a-tuple of elements of N. Justify: There exists an R-module homomorphism $\alpha : M \to N$ such that $\alpha(m_i) = n_i$ if and only if $[n_1, \cdots, n_a]A = 0$.
(c) Complete the proof.

(a) Let $m_1, \ldots, m_a$ be a (finite) set of generators for M. We have $\beta(\frac{m_i}{1}) = \frac{t_i}{w_i}$ for some $t_i \in N$ and $w_i \in W$. Take $u = w_1 \cdots w_a$.
(b) For α to be well-defined means that relations map to zero; it suffices to show that any defining relation maps to zero, and the condition above just says this.
(c) In the notation of the above, let $\frac{n_i'}{u} = \beta(m_i)$. Note that

$$[\frac{n_1'}{u}, \cdots, \frac{n_a'}{u}]A = [\beta m_1, \cdots, \beta m_a]A = \beta([m_1, \ldots, m_a]A) = 0 \qquad \text{in } W^{-1}N.$$

But this just means that there is some $v \in W$ such that v kills each entry of $[\frac{n_1'}{u}, \cdots, \frac{n_a'}{u}]A$. But then

$$[vn_1', \cdots, vn_a']A = (uv)[\frac{n_1'}{u}, \cdots, \frac{n_a'}{u}]A = 0.$$

This means that the map α given by $\alpha(m_i) = vn_i'$ is well defined, and $\beta = \frac{1}{uv}W^{-1}\alpha$ since it is true for each generator m_i.

[4]This means that M admits a finite generating set for which the module of relations is also finitely generated.

§5.23: Local Properties and Support

DEFINITION: Let $\mathcal{P}$ be a property[1] of a ring. We say that

- $\mathcal{P}$ is **preserved by localization** if

  $\mathcal{P}$ holds for $R \implies$ for every multiplicatively closed set W, $\mathcal{P}$ holds for $W^{-1}R$.

- $\mathcal{P}$ is a **local property** if

  $\mathcal{P}$ holds for $R \iff$ for every prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$, $\mathcal{P}$ holds for $R_{\mathfrak{p}}$.

One defines **preserved by localization** and **local property** for properties of modules in the same way, or for properties of a ring element (where one considers $\frac{r}{1} \in W^{-1}R$ or $R_{\mathfrak{p}}$ in the right-hand side) or module element.

DEFINITION: The **support** of a module M is

$$\{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}.$$

PROPOSITION: If M is a finitely generated module, then $\operatorname{Supp}(M) = V(\operatorname{ann}_R(M))$.

(1) Let R be a ring, M be a module, and $m \in M$.

(a) Show that[2] the following are equivalent:

(i) $m = 0$ in M;
(ii) $\frac{m}{1} = 0$ in $W^{-1}M$ for all multiplicatively closed $W \subseteq R$;
(iii) $\frac{m}{1} = 0$ in $M_{\mathfrak{p}}$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$;
(iv) $\frac{m}{1} = 0$ in $M_{\mathfrak{m}}$ for all $\mathfrak{m} \in \operatorname{Max}(R)$.

(b) Deduce that "$= 0$" (as a property of a module element) is preserved by localization, and a local property.

(c) Show that the "$= 0$" locus (as a property of a module element) of $m \in M$ is $D(\operatorname{ann}_R(m))$.

(a) The implication (i)⇒(ii) is clear from the definition of localization, and (ii)⇒(iii)⇒(iv) are tautologies. Suppose that $m \neq 0$. Then $\operatorname{ann}_R(m)$ is a proper ideal, so it is contained in some maximal ideal $\mathfrak{m}$. We claim that $m/1$ is nonzero in $M_{\mathfrak{m}}$. Indeed, $m/1$ is zero if and only if there is some $w \in R \smallsetminus \mathfrak{m}$ such that $wm = 0$, but by assumption this is impossible.

(b) The implication (i)⇒(ii) means preserved by localization, while (i)⇔(iii) means local property.

(c) Reviewing the argument from (a), we have $\frac{m}{1} = 0$ if and only if there is some $w \in W$ with $wm = 0$, which happens if and only if $R \smallsetminus \mathfrak{p} \cap \operatorname{ann}_R(m) = \varnothing$, which is equivalent to $\operatorname{ann}_R(m) \subseteq \mathfrak{p}$.

(2) Let R be a ring, M be a module.

(a) Show that the following are equivalent, and deduce that "$= 0$" (as a property of a module) is preserved by localization, and a local property.

(i) $M = 0$
(ii) $W^{-1}M = 0$ for all multiplicatively closed $W \subseteq R$;
(iii) $M_{\mathfrak{p}} = 0$ for all $\mathfrak{p} \in \operatorname{Spec}(R)$;
(iv) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \in \operatorname{Max}(R)$.

[1] For example, two properties of a ring are "is reduced" or "is a domain".

[2] Hint: Go (i)⇒(ii)⇒(iii)⇒(iv)⇒(i). For the last, If $m \neq 0$, consider a maximal ideal containing $\operatorname{ann}_R(m)$.

(b) Prove[3] the Proposition.

> **(a)** Again (i)⇒(ii)⇒(iii)⇒(iv) are clear. If $M \neq 0$, take some nonzero $m \in M$. Then there is some $\mathfrak{m}$ such that $m/1$ is nonzero in $M_{\mathfrak{m}}$ so $M_{\mathfrak{m}} \neq 0$.
> **(b)** Let $M = \sum_i Rm_i$. Since $M_{\mathfrak{p}} = \sum_i R_{\mathfrak{p}} \frac{m_i}{1}$, we have $M_{\mathfrak{p}} = 0$ if and only each $\frac{m_i}{1} = 0$, which happens if and only if $\mathfrak{p} \in \cap_i D(\mathrm{ann}_R(m_i))$. This equals $D(\cap_i D\mathrm{ann}_R(m_i)) = D(\mathrm{ann}_R(M))$. Then, we are considering the complement.

(3) More local properties

(a) Let R be a ring and $N \subseteq M$ modules. Show[4] that the following are equivalent, and deduce that $M = N$ for a submodule N is preserved by localization and a local property:

(i) $M = N$.
(ii) $W^{-1}M = W^{-1}N$ for all multiplicatively closed $W \subseteq R$;
(iii) $M_{\mathfrak{p}} = N_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathrm{Spec}(R)$;
(iv) $M_{\mathfrak{m}} = N_{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Max}(R)$.

(b) Let R be a ring. Show that the following are equivalent:

(i) R is reduced
(ii) $W^{-1}R$ is reduced for all multiplicatively closed $W \subseteq R$;
(iii) $R_{\mathfrak{p}}$ is reduced for all $\mathfrak{p} \in \mathrm{Spec}(R)$.
(iv) $R_{\mathfrak{m}}$ is reduced for all $\mathfrak{m} \in \mathrm{Max}(R)$.

> **(a)** Again (i)⇒(ii)⇒(iii)⇒(iv) are clear. If $N \subsetneq M$, then $M/N \neq 0$, and by the above there is some $\mathfrak{m}$ such that $(M/N)_{\mathfrak{m}} \neq 0$. But $(M/N)_{\mathfrak{m}} \cong M_{\mathfrak{m}}/N_{\mathfrak{m}}$ so $N_{\mathfrak{m}} \subsetneq M_{\mathfrak{m}}$.
> **(b)** Suppose that R is reduced and let $W \subseteq R$ be multiplicatively closed. Take a nilpotent element r/w. Then $(r/w)^n = 0$ implies there is some $v \in W$ with $vr^n = 0$. Then $(vr)^n = 0$ so $vr = 0$ and $r/w = 0$ in $R_{\mathfrak{p}}$. Again (ii)⇒(iii)⇒(iv) are tautologies. Suppose that R is not reduced and take $r^n = 0$ with $r \neq 0$. By part (a), for every maximal ideal $\mathfrak{m}$ in $R_{\mathfrak{m}}$ we have $(r/1)^n = 0$, and for some maximal ideal we have $r/1 \neq 0$, so $R_{\mathfrak{m}}$ is not reduced.

(4) Not so local.

(a) Show that the property R is a domain is preserved by localization.
(b) Let K be a field and $R = K \times K$. Show that $R_{\mathfrak{p}}$ is a field for all $\mathfrak{p} \in \mathrm{Spec}(R)$. Conclude that the property that R is a domain (or R is a field) is not a local property.

> **(a)** Suppose that R is a domain and $(a/u)(b/v) = 0$ in some $R_{\mathfrak{p}}$. Then there is some $w \notin \mathfrak{p}$ such that $wab = 0$, so $a = 0$ or $b = 0$, whence $a/u = 0$ or $b/v = 0$, so $R_{\mathfrak{p}}$ is a domain.
> **(b)** The ring $K \times K$ has two prime ideals $0 \times K$ and $K \times 0$. The kernel of the localization map $(K \times K)_{0\times K}$ is the set of elements that are killed by some element not in $0 \times K$; i.e., the set of (a, b) such that there is some $(c, d) \in K^\times \times K$ with $(ac, bd) = (0, 0)$. This forces $a = 0$ and conversely, for an element $(0, b)$ we have $(0, b)(1, 0) = (0, 0)$, so this kernel is exactly $0 \times K$. Thus
>
> $$(K \times K)_{0\times K} \cong \left(\frac{K \times K}{0 \times K}\right)_{\overline{0\times K}} \cong K_0 \cong K.$$
>
> Similarly for the other prime.

[3]Recall that if $M = \sum_i Rm_i$ is finitely generated then $W^{-1}M = \sum_i W^{-1}R\frac{m_i}{1}$ and that an element annihilates a module if and only if it annihilates every generator in a generating set.
[4]Hint: Consider M/N.

(5) More local properties, or not.
   (a) Let M be an R-module. Show that the property that M is finitely generated is preserved by localization but is not[5] a local property.
   (b) Let $R \subseteq S$ be an inclusion of rings. Show that the properties that $R \subseteq S$ is algebra-finite/integral/module-finite are preserved by localization on R: i.e., if one of these holds, the same holds for $W^{-1}R \subseteq W^{-1}S$ for any $W \subseteq R$ multiplicatively closed.
   (c) Let $R \subseteq S$ be an inclusion of rings, and $s \in S$. Show that the property that $s \in S$ is integral over R is a local property on R: i.e., this holds if and only if it holds for $\frac{s}{1} \in S_{\mathfrak{p}}$ over $R_{\mathfrak{p}}$ for each $\mathfrak{p} \in \mathrm{Spec}(R)$.
   (d) Is the property that $r \in R$ is a unit a local property?
   (e) Is the property that $r \in R$ is a zerodivisor a local property?
   (f) Is the property that $r \in R$ is nilpotent a local property?
   (g) Let $R \subseteq S$ be an inclusion of rings. Are the properties $R \subseteq S$ is algebra-finite/module-finite local properties on R?

(6) Let $\mathcal{P}$ be a local property of a ring, and $f_1, \ldots, f_t \in R$ such that $(f_1, \ldots, f_t) = R$. Show that if $\mathcal{P}$ holds for each R_{f_i}, then $\mathcal{P}$ holds for R.

[5]Hint: Consider $\bigoplus_{\alpha \in \mathbb{C}} \mathbb{C}[X]/(X - \alpha)$