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 $ee' = 0$.

(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?

(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.

[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.

(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.

(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?

(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.

(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

(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.

---

[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 $m > 0$.

§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.

(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 $F \in \ker(\phi)$.

(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 $\sqrt{(X^2, XYZ, Y^2)}$.

---

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

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

(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.

(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.

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

(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 $f_1^2 + \cdots + f_t^2$.

(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 $a_i \in R'$ is *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]

---

[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 $(X_1, \ldots, X_n) \subsetneq \mathfrak{m}$

[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 $r = \sum_i r_i$.

§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.

(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.

(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.

(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., $X^3+\pi X^5Y+5$ is in while $X^3 + \pi X^4Y + 5$ is out).

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

(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.

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

[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.

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?

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

---

[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.

(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.

(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?

(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.

(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 $m \in S$.

(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.

(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?

§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.

(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.

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

(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 $f \in I_n(A)^n$.

(5) Prove the Lemma above.

(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).

(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 $\mathbb{Z}$.

(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.

(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.

[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 $T = \sum_{i,j} Rs_it_j$.

(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.

(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 $R \subseteq S$?

(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.

[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 $[g]_{\leq n^2} \notin \sum_{i=1}^{n} A[f_i]_{\leq n^2}$.
[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.

(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?

(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.
- **(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.

(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.

(5) Prove Corollary 2.

[1] You might find the Corollary helpful.

(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.

(2) Prove the Proposition above.

(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?

(4) Discuss the proof of the Lemma above.

(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.

(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.

[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 $r = ua_1 \cdots a_n$.
[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.

(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?

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

(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.

(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, $z^n = 0$.

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

(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?

---

[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).

§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.

(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.

(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.

(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.

(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!

(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 $d - d_i$.

(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.

(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: $R_n = \sum_{d_1 a_1 + \cdots + d_m a_m = n} A \cdot X_1^{d_1} \cdots X_m^{d_m}$ 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?

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

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

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

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

(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.

(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.

[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 $2e_0e_d = e_0e_d \ldots$

§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 $R = K[X + Y, XY]$.

(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.

(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.

(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.

(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.

§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.

(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.

(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.

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

(5) 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 $\sigma \cdot X_i = X_{\sigma(i)}$. Show[2] that

$$R^{\mathcal{S}_3} = \mathbb{C}[X_1 + X_2 + X_3, X_1X_2 + X_1X_3 + X_2X_3, X_1X_2X_3]$$

and that $X_1 + X_2 + X_3, X_1X_2 + X_1X_3 + X_2X_3, X_1X_2X_3$ are algebraically independent over $\mathbb{C}$. What about replacing 3 with n?

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

[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.

[2] Hint: Order the monomials of R by lexicographic (dictionary) order. Given a homogeneous invariant, can you find an element of $\mathbb{C}[X_1 + X_2 + X_3, X_1X_2 + X_1X_3 + X_2X_3, X_1X_2X_3]$ with the same "first" monomial in that order?

§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.

(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 $\mathrm{gr}_{\mathfrak{m}}(R) \cong K[X, Y]$.
- **(e)** What happens in (b) and (d) if we have n variables instead of 2?

(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?

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

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

(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.

(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 $\mathrm{gr}_{(x,y,z)}\left(\dfrac{K[\![X,Y,Z]\!]}{(X^2 + XY + Y^3 + Z^7)}\right)$.

(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 $f_1, \ldots, f_m \in R$ that are algebraically independent over K such that $K[f_1, \ldots, f_m] \subseteq R$ is module-finite; equivalently, there is a module-finite injective K-algebra map from a polynomial ring $K[X_1, \ldots, X_m] \hookrightarrow R$. Such a ring S is called a **Noether normalization** for R.

LEMMA: Let A be a ring, and $F \in R := A[X_1, \ldots, X_n]$ 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 $A[X_1, \ldots, X_{n-1}]$, 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 $\lambda_1, \ldots, \lambda_{n-1} \in K$.
- 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 $f_1, \ldots, f_m \in R[1/a]$ that are algebraically independent over $A[1/a]$ such that $A[1/a][f_1, \ldots, f_m] \subseteq R[1/a]$ 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 $L_1, \ldots, L_m \in R_1$ such that $K[L_1, \ldots, L_m] \subseteq R$ is module-finite.
- NN FOR POWER SERIES: Let K be an infinite field, and $R = K[\![X_1, \ldots, X_n]\!]/I$. Then there exists a module-finite injection $K[\![Y_1, \ldots, Y_m]\!] \hookrightarrow R$ 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 $R = K[X^4, X^3Y, XY^3, Y^4]$.

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

---

[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 $R[1/a]$.

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

(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.

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

§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.

(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.

(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.

(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 $\mathcal{Z}(I) \stackrel{?}{=} \varnothing$.

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

(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 $\mathbb{R}$.

§4.17: STRONG NULLSTELLENSATZ

STRONG 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 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 $R = K[X_1, \ldots, X_n]$. 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

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

(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.

(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

$$I = (X^3 - Y^2Z, Y^7 - XZ^3, 3X^5 - XYZ - 2Z^{19}) \quad \text{in the ring} \quad \mathbb{C}[X, Y, Z].$$

(3) Prove the Corollary.

(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.

(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 $\det \begin{bmatrix} X_{11} & X_{12} \\ X_{21} & X_{22} \end{bmatrix}$.

---

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

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

(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

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

(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 $\mathrm{Spec}(R)$, is the set of prime ideals of R.
- We set $V(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \subseteq \mathfrak{p}\}$, the set of primes containing I.
- We set $D(I) := \{\mathfrak{p} \in \mathrm{Spec}(R) \mid I \not\subseteq \mathfrak{p}\}$, 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 $\phi^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ 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 $\mathrm{Spec}(R)$? Be careful not to forget (0)!
  - **(ii)** Draw a picture $\mathrm{Spec}(R)$ (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.

(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 $\mathrm{Spec}(R)$.

[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 $u \in K[\![X]\!]$.

(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:

$V(I)$ ___ $V(\sqrt{I})$	$D(I)$ ___ $D(\sqrt{I})$
$V(\sum_\lambda I_\lambda)$ _____ $V(I_\lambda)$	$D(\sum_\lambda I_\lambda)$ _____ $D(I_\lambda)$
$V(f_1, \ldots, f_n)$ __ $V(f_1)$ __ $\cdots$ __ $V(f_n)$	$D(f_1, \ldots, f_n)$ __ $D(f_1)$ __ $\cdots$ __ $D(f_n)$
$V(IJ)$___$V(I)$___$V(J)$	$D(IJ)$___$D(I)$___$D(J)$
$V(I \cap J)$___$V(I)$___$V(J)$	$D(I \cap J)$___$D(I)$___$D(J)$

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

(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^*.

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

(6) Properties of $\mathrm{Spec}(R)$.

(a) Show that for any ring R, the space $\mathrm{Spec}(R)$ is compact.

(b) Show that if $\mathrm{Spec}(R)$ is Hausdorff, then every prime of R is maximal.

(c) Show that $\mathrm{Spec}(R) \cong \mathrm{Spec}(R/\sqrt{0})$.

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

§4.19: SPECTRUM AND RADICAL IDEALS

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 $I = (0)$?

(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?

(3) Prove[1] the Proposition.

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

[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.

(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.

(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.

[1] Reuse an old argument in a similar setting.
[2] It's déjà vu all over again.

(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.

(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).

[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!

(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.

(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 $\left(\frac{K[X,Y]}{(XY)}\right)_{(x)}$.

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

(4) Prove the Lemma and the Theorem.

(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 $W^{-1}R$.

(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 $R = K[X_1, X_2, X_3, \ldots]/(\{X_i X_j \mid i \neq j\})$. Describe $\mathrm{Min}(R)$ as a topological space.

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

[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 $\mathfrak{p} \supseteq \operatorname{ann}_R(m)$.

(2) Prove the Proposition.

(3) Corollary.

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

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

[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.

(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 $M \cong M_{\mathfrak{m}}$.

(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.

[3]Hint: Note that $R/\mathfrak{m}^n$ is local with maximal ideal (the image of) $\mathfrak{m}$.

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

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

  $\mathcal{P}$ holds for $R \Longleftrightarrow$ for every prime ideal $\mathfrak{p} \in \mathrm{Spec}(R)$, $\mathcal{P}$ 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

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

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

(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 $\mathfrak{p} \in \mathrm{Spec}(R)$;
(iv) $\frac{m}{1} = 0$ in $M_{\mathfrak{m}}$ for all $\mathfrak{m} \in \mathrm{Max}(R)$.

(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 $D(\mathrm{ann}_R(m))$.

(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 $\mathfrak{p} \in \mathrm{Spec}(R)$;
(iv) $M_{\mathfrak{m}} = 0$ for all $\mathfrak{m} \in \mathrm{Max}(R)$.

(b) Prove[3] the Proposition.

(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 $\mathfrak{m} \in \mathrm{Max}(R)$.

---

[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 $\mathrm{ann}_R(m)$.

[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.

(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 $\mathfrak{m} \in \mathrm{Max}(R)$.

(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.

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

§6.24: MINIMAL PRIMES

THEOREM: Let R be a Noetherian ring. Every ideal of R has finitely many minimal primes.

LEMMA: Let R be a ring, I an ideal, and $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ a finite set of incomparable prime ideals; i.e., $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ for any $i \neq j$. If $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_t$, then $\mathrm{Min}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$.

COROLLARY: Let R be a Noetherian ring. Every radical ideal of R can be written as a finite intersection of primes in a unique way such that no term can be omitted.

(1) Minimal primes review:
- **(a)** What is the intersection of all minimal primes of R?
- **(b)** What is the intersection of all minimal primes of I?
- **(c)** Explain why an arbitrary intersection of prime ideals is radical.
- **(d)** Explain why any radical ideal is an intersection of prime ideals.

(2) Proof of Theorem: Let R be a Noetherian ring.
- **(a)** Suppose the conclusion is false. Explain why[1] the set of ideals that do not have finitely many minimal primes has a maximal element J.
- **(b)** Explain why J is not prime.
- **(c)** Explain why, if $ab \in J$, $V(J) = V(J + (a)) \cup V(J + (b))$; i.e., every prime that contains J either contains $J + (a)$ or $J + (b)$.
- **(d)** Conclude the proof.

(3) In this problem, we will show that the minimal primes of $R = \mathbb{Q}[X, Y, Z, W]/(X^2 - Z^2, XY - ZW, Y^2 - W^2)$ are $(x-z, y-w)$ and $(x+z, y+w)$. Equivalently, we show that the minimal primes of $I = (X^2 - Z^2, XY - ZW, Y^2 - W^2)$ are $(X + Z, Y - W)$ and $(X + Z, Y + W)$.
- **(a)** Factor the first and last relations to show that any prime containing I contains either $X - Z$ or $X + Z$, and also contains either $Y - W$ or $Y + W$.
- **(b)** Show[2] that $(X - Z, Y - W) \supseteq I$ and $(X + Z, Y + W) \supseteq I$.
- **(c)** Show that $XY \in (X - Z, Y + W) + I$. Deduce that any prime that contains $(X - Z, Y + W)$ and I also contains either $(X - Z, Y - W)$ or $(X + Z, Y + W)$.
- **(d)** Deduce the claim.

(4) (a) Use the Theorem to show that, if R is Noetherian, a subset of $\mathrm{Spec}(R)$ is closed if and only if it is a finite union of "upward intervals" $V(\mathfrak{p}_i)$.
(b) Use the Theorem to show that, if R is Noetherian, then $\mathrm{Min}(R)$ is discrete.
(c) Prove the Lemma.
(d) Prove the Corollary.

(5) (a) Compute the minimal primes of $R = \mathbb{Q}[X, Y, Z]/(XY, XZ, YZ)$.
(b) Compute the minimal primes of $R = \mathbb{Q}[X, Y, Z]/(X^2 - X^3, XY^3, XZ^4 - Z^4)$.

[1] Warning: this looks like cause to apply Zorn's Lemma, but that is not why.
[2] Hint: Sometimes if you want to show $f \in J$ it is cleanest to show $f \equiv 0 \mod J$.

(6) Let K be a field. Let $R = \dfrac{K[X_1, X_2, X_3, \dots, Y_1, Y_2, Y_3, \dots]}{(\{X_i Y_i \mid i \geq 1\})}$. Compute $\mathrm{Min}(R)$, and show that $(x_1, x_2, x_3, \dots)$ is not open in $\mathrm{Min}(R)$; in particular, $\mathrm{Min}(R)$ is not discrete.

(7) Let K be a field. Let $R = \dfrac{K[X_1, X_2, X_3, \dots]}{(\{X_i X_j - X_j \mid 1 \leq i \leq j\})}$. Compute $\mathrm{Min}(R)$, and show that $(x_1, x_2, x_3, \dots)$ is not open in $\mathrm{Min}(R)$; in particular, $\mathrm{Min}(R)$ is not discrete.

§6.25: ASSOCIATED PRIMES

DEFINITION: Let R be a ring and M be a module. A prime ideal $\mathfrak{p}$ of R is an **associated prime** of M if $\mathfrak{p} = \operatorname{ann}_R(m)$ for some $m \in M$. The element m is called a **witness** for the associated prime $\mathfrak{p}$. We write $\operatorname{Ass}_R(M)$ for the set of associated primes of a module.

LEMMA: Let R be a Noetherian ring and M be a module. For any nonzero element $m \in M$, the ideal $\operatorname{ann}_R(m)$ is contained in an associated prime of M. In particular, if $M \neq 0$, then M has an associated prime.

DEFINITION: Let R be a ring and M be an R-module. We say that an element $r \in R$ is a **zerodivisor** on M if there is some $m \in M \smallsetminus 0$ such that $rm = 0$.

PROPOSITION: Let R be a Noetherian ring and M an R-module. The set of zerodivisors on M is the union of the associated primes of M.

THEOREM: Let R be a Noetherian ring, W be a multiplicatively closed set, and M be a module. Then

$$\operatorname{Ass}_{W^{-1}R}(W^{-1}M) = \{W^{-1}\mathfrak{p} \mid \mathfrak{p} \in \operatorname{Ass}_R(M), \mathfrak{p} \cap W = \varnothing\}.$$

COROLLARY: Let R be a Noetherian ring and I be an ideal. Then $\operatorname{Min}(I) \subseteq \operatorname{Ass}_R(R/I)$.

(1) Proof of Lemma and Proposition: Let R be a Noetherian ring and M be a nonzero module.
- **(a)** Let $\mathcal{S} = \{\operatorname{ann}_R(m) \mid m \in M \smallsetminus 0\}$. Explain why $\mathcal{S}$ has a maximal element J.
- **(b)** Let $J = \operatorname{ann}_R(m)$ and suppose that $rs \in J$ but $s \notin J$. Explain why $J = \operatorname{ann}_R(sm)$.
- **(c)** Conclude the proof of the Lemma.
- **(d)** Deduce the Proposition from the Lemma.
- **(e)** What does the Proposition say in the special case when $M = R$?

(2) Working with associated primes.
- **(a)** Let R be a domain and M be a torsionfree module. Show that $\operatorname{Ass}_R(M) = \{(0)\}$.
- **(b)** Let R be a ring and $\mathfrak{p}$ be a prime ideal. Show that for any nonzero element $\overline{r} \in R/\mathfrak{p}$ that $\operatorname{ann}_R(\overline{r}) = \mathfrak{p}$ and use the definition to deduce that $\operatorname{Ass}_R(R/\mathfrak{p}) = \{\mathfrak{p}\}$.
- **(c)** Let K be a field and $R = K[X,Y]/(X^2Y, XY^2)$. Use[1] the definition to show that (x,y), (x), and (y) are associated primes of R.
- **(d)** Let M be a module. Explain why $\mathfrak{p} \in \operatorname{Ass}_R(M)$ if and only if there is an injective R-module homomorphism $R/\mathfrak{p} \hookrightarrow M$.

(3) Using the Theorem. Let R be a Noetherian ring.
- **(a)** Restate the Theorem in the special case $W = R \smallsetminus \mathfrak{p}$ with our standard notation for this setting.
- **(b)** Show (either using the Theorem or 2(d) above) that $\operatorname{Ass}_R(M) \subseteq \operatorname{Supp}_R(M)$.
- **(c)** Use the Theorem (and the previous part or otherwise) to prove the Corollary.
- **(d)** Show the more general statement: if M is a nonzero module, then the primes that are minimal within the support of I are associated to M.

[1] Hint: Consider xy and y^2.

(4) Lemma 1:

(a) Let K be a field and $R = K[X]$. Explain why

- $\mathrm{Ass}_R(R) = \{(0)\}$
- $(X) \cong R$, so $\mathrm{Ass}_R((X)) = \{(0)\}$,
- $\mathrm{Ass}_R(R/(X)) = \{(X)\}$.

Does this contradict the Lemma?

(b) Show that $\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M)$.

(c) Suppose that $\mathfrak{p} \in \mathrm{Ass}_R(M) \smallsetminus \mathrm{Ass}_R(N)$ with witness m. Show[2] that $Rm \cap N = 0$, so the map $Rm \to M/N$ is injective. Deduce that $\mathfrak{p} \in \mathrm{Ass}_R(M/N)$ and complete the proof.

(5) Prove[3] the prime avoidance lemma.

(6) Let K be a field and $R = K[X^2, XY, Y^2] \subseteq K[X, Y]$.

(a) Mark all[4] of the points in the plane corresponding to exponent vectors of elements of R.

(b) Is $I = (X^2)$ a prime ideal? Is $J = (X^2, XY)$?

(c) Mark all of the points in the plane corresponding to exponent vectors of elements of $(X^2) \subseteq R$.

(d) Find and illustrate a prime filtration of R/I. Compute $\mathrm{Ass}_R(R/I)$.

(e) Find and illustrate a prime filtration of R/J^2. Compute $\mathrm{Ass}_R(R/J^2)$.

(7) More facts about associated primes: Let R be a Noetherian ring.

(a) Let $I \subseteq J$ be ideals. Show that $I = J$ if and only if $IR_\mathfrak{p} = JR_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}_R(R/I)$.

(b) Let I, J be ideals. Show that $I \subseteq J$ if and only if $IR_\mathfrak{p} \subseteq JR_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Ass}_R(R/J)$.

(c) Let r be a nonzerodivisor. Show that $\mathrm{Ass}_R(R/r^n) = \mathrm{Ass}_R(R/r)$ for all $n \geq 1$.

---

[2] Note that $Rm \cong R/\mathfrak{p}$ so every nonzero element has annihilator $\mathfrak{p}$.

[3] By induction, you can find elements $a_i \in J \smallsetminus \bigcup_{j \neq i} I_j$. Now consider $x = a_n + a_1 \cdots a_{n-1}$.

[4] Well, enough to get the pattern at least...

(4) The ring of Puiseux series is $R = \bigcup_{n \geq 1} \mathbb{C}[\![X^{1/n}]\!]$: elements consist of power series with fractional exponents that have a common denominator (though different elements can have different common denominators).
   (a) Show that every nonzero element of R can be written in the form $X^{m/n} \cdot u$ for some unit u.
   (b) Show that the R-module $R/(X)$ is nonzero but has no associated primes.

(5) Proof of Theorem: Let R be a Noetherian ring, W be a multiplicatively closed set, and M be a module.
   (a) Suppose that $\mathfrak{p}$ is an associated prime of M with $W \cap \mathfrak{p} = \varnothing$, and let m be a witness for $\mathfrak{p}$ as an associated prime of M. Show that $W^{-1}\mathfrak{p}$ is an associated prime of $W^{-1}M$ with witness $\frac{m}{1}$.
   (b) Suppose that $W^{-1}\mathfrak{p} \in \operatorname{Spec}(W^{-1}R)$ is an associated prime of $W^{-1}M$. Explain why there is a witness of the form $\frac{m}{1}$.
   (c) Let $\mathfrak{p} = (f_1, \ldots, f_t)$. Explain why there exist $w_1, \ldots, w_t \in W$ such that $w_i f_i m = 0$ in M for all i.
   (d) Show that $w_1 \cdots w_t m$ is a witness for $\mathfrak{p}$ as an associated prime of M.

(6) Let R be a Noetherian ring and M be a module. Show that $\mathfrak{p} \in \operatorname{Ass}_R(M)$ if and only if for every $r \in \mathfrak{p}$ and every nonzero $m \in M$, there exists some $u \notin \mathfrak{p}$ such that $urm = 0$.

(7) Let R be a Noetherian ring. Is every minimal prime of a zerodivisor a minimal prime of R?

§6.26: MORE ASSOCIATED PRIMES

LEMMA: Let R be a ring, and $N \subseteq M$ be modules. Then

$$\mathrm{Ass}_R(N) \subseteq \mathrm{Ass}_R(M) \subseteq \mathrm{Ass}_R(N) \cup \mathrm{Ass}_R(M/N).$$

EXISTENCE OF PRIME FILTRATIONS: Let R be a Noetherian ring and M be a finitely generated module. Then there exists a finite chain of submodules

$$M = M_t \supsetneq M_{t-1} \supsetneq \cdots \supsetneq M_1 \supsetneq M_0 = 0$$

such that for each $i = 1, \ldots, t$, there is some $\mathfrak{p}_i \in \mathrm{Spec}(R)$ such that $M_i/M_{i-1} \cong R/\mathfrak{p}_i$. Such a chain of submodules is called a **prime filtration** of M.

COROLLARY 1: Let R be a Noetherian ring and M be a finitely generated module. Then for any prime filtration of M, $\mathrm{Ass}_R(M)$ is a subset of the prime factors that occur in the filtration. In particular, $\mathrm{Ass}_R(M)$ is finite.

PRIME AVOIDANCE: Let R be a ring, J an ideal, and $I_1, I_2, I_3, \ldots, I_t$ a finite collection of ideals with I_i prime for $i > 2$ (that is, *at most* two I_i are not prime). If $J \not\subseteq I_i$ for all i, then $J \not\subseteq \bigcup_i I_i$.

COROLLARY 2: Let R be a Noetherian ring, M a finitely generated module, and I an ideal. If every element of I is a zerodivisor on M, then there is some nonzero $m \in M$ such that $Im = 0$.

(1) Let $R = K[X, Y]$ and $M = R/(X^2Y, XY^2)$.
- **(a)** Verify that $0 \subseteq Rxy \subseteq Rx \subseteq M$ is a prime filtration of M.
- **(b)** In an earlier problem, we more or less showed that $\{(x), (y), (x, y)\} \subseteq \mathrm{Ass}_R(M)$. Use Corollary 1 to deduce that this is an equality.

(2) Proving some Corollaries:
- **(a)** Show that Corollary 1 follows from the Lemma (and Existence of Prime Filtrations).
- **(b)** Write the contrapositive of the conclusion of Prime Avoidance.
- **(c)** Show that Corollary 2 follows from Prime Avoidance and Corollary 1.

(3) Proof of Existence of Prime Filtrations: Let R be a Noetherian ring and M a finitely generated R-module.
- **(a)** If $M \neq 0$, explain why you can always choose $M \supseteq M_1$ with $M_1 \cong R/\mathfrak{p}$ for some prime $\mathfrak{p}$.
- **(b)** If $M \neq M_1$, explain why[1] you can always choose $M \supseteq M_2 \supseteq M_1$ with $M_2/M_1 \cong R/\mathfrak{p}$ for some prime $\mathfrak{p}$.
- **(c)** If $M \neq M_{i-1}$ and you already have $M_1, \ldots, M_{i-1}$, explain why you can always choose $M \supseteq M_i \supsetneq M_{i-1}$ with $M_i/M_{i-1} \cong R/\mathfrak{p}$ for some prime $\mathfrak{p}$.
- **(d)** Explain why this process has to stop, and if it stops at $i = t$, we must have $M_t = M$.

[1] Hint: Consider M/M_1 and go back to the previous step.

§6.27: PRIMARY IDEALS

DEFINITION: A proper ideal I is **primary** if $rs \in I$ implies $r \in \sqrt{I}$ or $s \in I$. We say that I is $\mathfrak{p}$**-primary** if it is primary and $\sqrt{I} = \mathfrak{p}$.

LEMMA: Let R be a Noetherian ring and I an ideal. The following are equivalent:

(i) I is primary;
(ii) Every zerodivisor on R/I is nilpotent;
(iii) $\mathrm{Ass}_R(R/I)$ is a singleton.

DEFINITION: A **primary decomposition** of an ideal I is an expression of the form

$$I = Q_1 \cap \cdots Q_n$$

where each Q_i is a primary ideal.

DEFINITION: A proper ideal I is **irreducible** if $I = J_1 \cap J_2$ for some ideals J_1, J_2 implies $I = J_1$ or $I = J_2$.

THEOREM (EXISTENCE OF PRIMARY DECOMPOSITION): Let R be a Noetherian ring.

(1) Every irreducible ideal I is primary.
(2) Every ideal can be written as a finite intersection of irreducible ideals.

Hence, every ideal can be written as a finite intersection of primary ideals.

(1) Primary ideals
- **(a)** Use the definition to show that a prime ideal is primary.
- **(b)** Use the definition to show that the radical of a primary ideal is prime.
- **(c)** Use the definition to show that for the ideal $I = (X^2, XY)$ in $R = \mathbb{Q}[X, Y]$, $\sqrt{I}$ is prime but I is not primary.
- **(d)** Use the definition and part (b) above to show that if R is a UFD, then a proper principal ideal (f) is primary if and only if it is not generated[1] by a power of a prime element.
- **(e)** Use the Lemma to show that if $\sqrt{I} = \mathfrak{m}$ is a maximal ideal, then I is $\mathfrak{m}$-primary.

(2) Primary decompositions
- **(a)** Let n be an integer. Show that if $n = \pm p_1^{e_1} \cdots p_m^{e_m}$ is the prime factorization of n, then

$$(n) = (p_1^{e_1}) \cap \cdots \cap (p_m^{e_m})$$

  is a primary decomposition of (n) in $\mathbb{Z}$.
- **(b)** Let R be a Noetherian ring and I be a radical ideal. Give a recipe for a primary decomposition of I in terms of other named things pertaining to I.

(3) Prove[2] the Lemma.

[1] Note that if (f) is not generated by a power of a prime element, then f has nonassociate irreducible factors.

[2] Hint: For (ii)⇔(iii), recall that the set elements of R that are zerodivisors modulo I is the union of the associated primes of R/I and the set of elements that are nilpotent modulo I is the intersection of minimal primes of I.

(4) Proof of Existence of Primary Decompositions:

(a) Prove[3] part (2) of the Theorem.

(b) Suppose that $xy \in Q$ with $x \notin Q$ and $y \notin \sqrt{Q}$. Explain why the there is some $n \geq 1$ such that $(Q : y^n) = (Q : y^{n+1})$.

(c) Show that $Q = (Q, x) \cap (Q, y^n)$ and deduce part (1) of the Theorem.

(5) More examples: Let K be a field.

(a) Show that $(X^2, XY, Y^2) \subseteq K[X, Y]$ is primary but not irreducible.

(b) Show that (X^2, XY, Y^3) is primary, but not a power of a prime.

(c) Show that $(X^2, XY)^2 \subseteq K[X^2, XY, Y^2]$ is a power of a prime but not primary.

(6) Let R be a Noetherian ring and $\mathfrak{p}$ a prime ideal. Show that there is an order-preserving bijection

$$\{\mathfrak{p}\text{-primary ideals of } R\} \leftrightarrow \{\text{ideals of } (R_\mathfrak{p}, \mathfrak{p}R_\mathfrak{p}) \text{ with radical } \mathfrak{p}R_\mathfrak{p}\}.$$

(7) Let R be a Noetherian ring. Show that I is irreducible if and only if it is primary (with radical $\mathfrak{p}$) and $\dfrac{IR_\mathfrak{p} : \mathfrak{p}R_\mathfrak{p}}{IR_\mathfrak{p}}$ is a one-dimensional $R_\mathfrak{p}/\mathfrak{p}R_\mathfrak{p}$-vectorspace.

[3] Imitate the proof of finiteness of minimal primes.

§6.28: UNIQUENESS OF PRIMARY DECOMPOSITIONS

DEFINITION: A **minimal primary decomposition** of an ideal I is a primary decomposition

$$I = Q_1 \cap \cdots \cap Q_n$$

such that $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$, and $\sqrt{Q_i} \neq \sqrt{Q_j}$ for $i \neq j$.

THEOREM (FIRST UNIQUENESS THEOREM FOR PRIMARY DECOMPOSITION): Let R be a Noetherian ring and I an ideal. Let

$$I = Q_1 \cap \cdots \cap Q_n$$

be a minimal primary decomposition of I. Then

$$\{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\} = \mathrm{Ass}_R(R/I).$$

In particular, the set of primes occurring as the radicals of the primary components are uniquely determined.

THEOREM (SECOND UNIQUENESS THEOREM FOR PRIMARY DECOMPOSITION): Let R be a Noetherian ring and I an ideal. Let

$$I = Q_1 \cap \cdots \cap Q_n$$

be a minimal primary decomposition of I. Suppose that $\mathfrak{p} = \sqrt{Q_i}$ is a *minimal* prime of I. Then $Q_i = IR_{\mathfrak{p}} \cap R$. In particular, the primary components corresponding to the minimal primes are uniquely determined.

LEMMA: Let $I_1, \ldots, I_t$ be ideals. Then

(1) for any multiplicatively closed set W, $W^{-1}(I_1 \cap \cdots \cap I_t) = W^{-1}I_1 \cap \cdots \cap W^{-1}I_t$.
(2) $\mathrm{Ass}_R\left(R/\bigcap_{i=1}^t I_i\right) \subseteq \bigcup_{i=1}^t \mathrm{Ass}_R(R/I_i)$.

(1) Uniqueness theorems:

(a) Let K be a field, $R = K[X, Y]$ a polynomial ring, and $I = (X^2, XY)$. Verify[1] that $I = (X) \cap (X^2, Y) = (X) \cap (X^2, XY, Y^2)$ gives two different minimal primary decompositions of I.

(b) In the previous part, which aspects of the decomposition are the same, and which are different. Compare with the uniqueness theorems.

(c) Use the uniqueness theorems to explain why, for $n \in \mathbb{Z}$ with prime factorization $n = \pm p_1^{e_1} \cdots p_m^{e_m}$, the *only*[2] minimal primary decomposition of (n) is

$$(n) = (p_1^{e_1}) \cap \cdots \cap (p_m^{e_m}).$$

(2) Minimal primary decompositions: Let R be a Noetherian ring.

(a) Use the Lemma to explain why a finite intersection of $\mathfrak{p}$-primary ideals is $\mathfrak{p}$-primary.

(b) Explain how to turn a general $I = Q_1 \cap \cdots \cap Q_m$ primary decomposition into a minimal primary decomposition.

[1] You can take for granted that in each case the intersection is I, but explain why the ideals are primary and the minimality hypotheses hold.

[2] We don't care about the order.

(3) Proof of Second Uniqueness Theorem:

- **(a)** Use the definition of primary to show that if Q is $\mathfrak{p}$-primary, then $QR_{\mathfrak{p}} \cap R = Q$.
- **(b)** Show[3] that if Q is $\mathfrak{q}$-primary and $\mathfrak{q} \not\subseteq \mathfrak{p}$, then $QR_{\mathfrak{p}} = R_{\mathfrak{p}}$.
- **(c)** Let R be Noetherian and $I = Q_1 \cap \cdots \cap Q_n$ be a minimal primary decomposition, and $\mathfrak{p} = \sqrt{Q_i}$ a minimal prime of I. Use the Lemma to show that $IR_{\mathfrak{p}} = Q_i R_{\mathfrak{p}}$.
- **(d)** Complete the proof.

(4) Proof of First Uniqueness Theorem: Let R be Noetherian and $I = Q_1 \cap \cdots \cap Q_n$ be a minimal primary decomposition.

- (a) Use the Lemma to prove that $\mathrm{Ass}_R(R/I) \subseteq \{\sqrt{Q_1}, \ldots, \sqrt{Q_n}\}$.
- (b) Set $J_i = \bigcap_{j \neq i} Q_j$. Explain why it suffices to show that $\mathrm{Ass}_R(J_i/I) = \{\sqrt{Q_i}\}$ to establish the other containment.
- (c) Let $\mathfrak{q}$ be an associated prime of J_i/I and $r \in R$ such that $\overline{r} \in J_i/I$ is a witness (and in particular, nonzero). Show that $Q_i \subseteq \mathfrak{q}$ and deduce that $\sqrt{Q_i} \subseteq \mathfrak{q}$.
- (d) Use the definition of primary to show that $\mathfrak{q} \subseteq \sqrt{Q_i}$, and conclude the proof.

(5) Prove the Lemma.

(6) Let R be a Noetherian ring, and I be an ideal. Consider a collection of minimal primary decompositions of I:

$$I = \mathfrak{q}_{1,\alpha} \cap \cdots \cap \mathfrak{q}_{s,\alpha}, \quad \alpha \in \Lambda$$

where, for each α, $\sqrt{\mathfrak{q}_{i,\alpha}} = \mathfrak{p}_i$.

- (a) Suppose that $\mathfrak{p}_j$ is not contained in any other associated prime of I, and let $W = R \setminus \bigcup_{i \neq j} \mathfrak{p}_i$. Find some minimal primary decompositions of $I(W^{-1}R) \cap R$.
- (b) Show (by induction on s) that if we take components $\mathfrak{q}_{1,\alpha_1}, \ldots, \mathfrak{q}_{s,\alpha_s}$ from different primary decompositions of I, that we can put them together to get a primary decomposition of I; namely $I = \mathfrak{q}_{1,\alpha_1} \cap \cdots \cap \mathfrak{q}_{s,\alpha_s}$.

[3] One possibility is to consider the support of R/Q.

§7.29: DIMENSION AND HEIGHT

DEFINITION: Let R be a ring.

- A **chain of primes of length** n is
$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n \qquad \text{with } \mathfrak{p}_i \in \operatorname{Spec}(R).$$
We may say this chain is **from** $\mathfrak{p}_0$ and/or **to** $\mathfrak{p}_n$ to indicate the minimal and/or maximal elements.
- A chain of primes as above is **saturated** if for each i, there is no prime $\mathfrak{q}$ such that $\mathfrak{p}_i \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{p}_{i+1}$.
- The **dimension** of R is
$$\dim(R) := \sup\{n \geq 0 \mid \text{there is a chain of primes of length } n \text{ in } \operatorname{Spec}(R)\}.$$
- The **height** of a prime ideal $\mathfrak{p} \in \operatorname{Spec}(R)$ is
$$\operatorname{height}(\mathfrak{p}) := \sup\{n \geq 0 \mid \text{there is a chain of primes to } \mathfrak{p} \text{ of length } n \text{ in } \operatorname{Spec}(R)\}.$$
- The **height** of an arbitrary proper ideal $I \subseteq R$ is
$$\operatorname{height}(I) := \inf\{\operatorname{height}(\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Min}(I)\}.$$

(1) Let K be field. Use the definition of dimension to prove the following:
- **(a)** $\dim(K) = 0$.
- **(b)** If R is a PID, but not a field, then $\dim(R) = 1$.
- **(c)** $\dim(K[X_1, \ldots, X_n]) \geq n$.
- **(d)** $\dim(K[\![X_1, \ldots, X_n]\!]) \geq n$.
- **(e)** $\dim(K[X_1, X_2, X_3, \ldots]) = \infty$.

(2) Let R be a ring, I an ideal, and $\mathfrak{p}$ a prime ideal. Use the definitions to prove the following:
- **(a)** $\operatorname{height}(\mathfrak{p}) = 0$ if and only if $\mathfrak{p} \in \operatorname{Min}(R)$.
- **(b)** $\operatorname{height}(I) = 0$ if and only if $I \subseteq \mathfrak{p}$ for some $\mathfrak{p} \in \operatorname{Min}(R)$.
- **(c)** If R is a domain and $I \neq 0$, then $\operatorname{height}(I) > 0$.
- **(d)** $\dim(R/\mathfrak{p}) = \sup\{n \geq 0 \mid \text{there is a chain of primes of length } n \text{ in } V(\mathfrak{p})\}$.
- **(e)** $\dim(R/I) = \sup\{n \geq 0 \mid \text{there is a chain of primes of length } n \text{ in } V(I)\}$.
- **(f)** If R is a domain and $I \neq 0$, and $\dim(R) < \infty$, then $\dim(R/I) < \dim(R)$.
- **(g)** $\dim(R) = \sup\{\dim(R/\mathfrak{p}) \mid \mathfrak{p} \in \operatorname{Min}(R)\}$.
- **(h)** $\dim(R_{\mathfrak{p}}) = \operatorname{height}(\mathfrak{p})$.
- **(i)** $\dim(R) = \sup\{\dim(R_{\mathfrak{m}}) \mid \mathfrak{m} \in \operatorname{Max}(R)\}$.
- **(j)** $\operatorname{height}(\mathfrak{p}) + \dim(R/\mathfrak{p}) = \sup\left\{ n \geq 0 \;\middle|\; \begin{array}{l}\text{there is a chain of primes of length } n \\ \text{in } \operatorname{Spec}(R) \text{ such that } \mathfrak{p}_i = \mathfrak{p} \text{ for some } i\end{array} \right\}$
- **(k)** $\operatorname{height}(\mathfrak{p}) + \dim(R/\mathfrak{p}) \leq \dim(R)$.
- **(l)** $\operatorname{height}(I) + \dim(R/I) \leq \sup\left\{ n \geq 0 \;\middle|\; \begin{array}{l}\text{there is a chain of primes of length } n \\ \text{in } \operatorname{Spec}(R) \text{ such that } \mathfrak{p}_i \in \operatorname{Min}(I) \text{ for some } i\end{array} \right\}$.
- **(m)** $\operatorname{height}(I) + \dim(R/I) \leq \dim(R)$.

(3) Dimension vs height
- (a) Let K be a field and $R = K[X, Y, Z]/(XY, XZ)$. Let $\mathfrak{p} = (y, z)$. Compute $\dim(R/\mathfrak{p})$ and $\operatorname{height}(\mathfrak{p})$, and show that $\dim(R) \geq 2$.
- (b) Let $R = \mathbb{Z}_{(2)}[X]$. Let $\mathfrak{p} = (2X - 1)$. Compute $\dim(R/\mathfrak{p})$ and[1] $\operatorname{height}(\mathfrak{p})$, and show that $\dim(R) \geq 2$.

(4) Let R be a domain. Show that R is a UFD if and only if every prime ideal of height one is principal.

[1] You can use the next problem if you like.

(5) Does it follow from the definition that in a Noetherian ring, every prime has finite height?

(6) In this problem we will construct a Noetherian ring of infinite dimension. Let K be a field, $S = K[X_{1,1}, X_{2,1}, X_{2,2}, X_{3,1}, X_{3,2}, X_{3,3}, \dots]$, and $W = S \setminus \bigcup_t (X_{t,1}, \dots, X_{t,t})$.
   (a) Let A be a ring. Suppose that $\mathrm{Max}(A)$ is finite, $A_{\mathfrak{m}}$ is Noetherian for every $\mathfrak{m} \in \mathrm{Max}(A)$, and every nonzero element is contained in finitely many maximal ideals. Show that A is Noetherian.
   (b) Let $\mathfrak{p}_t = (X_{t,1}, \dots, X_{t,t},)$ for $t \geq 1$. Let I be an ideal. Show that if $I \subseteq \bigcup_{t \geq 1} \mathfrak{p}_t$, then there is[2] some $t \geq 1$ such that $I \subseteq \mathfrak{p}_t$.
   (c) Show that $R := W^{-1}S$ is Noetherian and infinite dimensional.

[2]Note that this looks similar to prime avoidance, but with an infinite set of primes. For $f \in S$, let $v(f) := \{t \mid f \in \mathfrak{p}_t\}$. Show that for any $f, g \in I$, there is some $h \in I$ with $v(h) \subseteq v(f) \cup v(g)$. Then apply prime avoidance.

§7.30: COHEN-SEIDENBERG THEOREMS: APPLICATIONS

LYING OVER: Let $R \subseteq S$ be an integral inclusion. Then the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective. That is, for any prime $\mathfrak{p} \in \mathrm{Spec}(R)$, there is a prime $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$; i.e., a prime *lying over* $\mathfrak{p}$.

INCOMPARABILITY: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathrm{Spec}(S)$ such[1] that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$, we have $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$. That is, any two primes lying over the same prime are *incomparable*.

GOING UP: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{Q} \cap R = \mathfrak{P}$.

GOING DOWN: Let $R \subseteq S$ be an integral inclusion of domains, and assume that R is normal. Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{Q} \cap R = \mathfrak{P}$, there is some $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{q} \cap R = \mathfrak{p}$.

COROLLARY: Let $R \to S$ be integral.

(1) If S is Noetherian, then for any $\mathfrak{p} \in \mathrm{Spec}(R)$, the set of primes in S that contract to $\mathfrak{p}$ is finite.
(2) If $R \subseteq S$ is an inclusion, and S is Noetherian, then for any $\mathfrak{p} \in \mathrm{Spec}(R)$, the set of primes in S that contract to $\mathfrak{p}$ is nonempty and finite.
(3) For any $\mathfrak{q} \in \mathrm{Spec}(S)$, we have $\mathrm{height}(\mathfrak{q}) \leq \mathrm{height}(\mathfrak{q} \cap R)$.
(4) $\dim(S) \leq \dim(R)$.
(5) If $R \subseteq S$ is an inclusion, then $\dim(R) = \dim(S)$.
(6) If $R \subseteq S$ is an inclusion, R is a normal domain, and S is a domain, then for any $\mathfrak{q} \in \mathrm{Spec}(S)$, we have $\mathrm{height}(\mathfrak{q}) = \mathrm{height}(\mathfrak{q} \cap R)$.

(1) Hypotheses of Lying Over and Incomparability:

(a) Consider the inclusion map $\mathbb{Z} \subseteq \mathbb{Q}$. Show that the conclusion of Lying Over fails. Which hypotheses are true?

(b) Consider the quotient map $\mathbb{C}[X] \to \mathbb{C}[X]/(X) \cong \mathbb{C}$. Show that the conclusion of Lying Over fails. Which hypotheses are true?

(c) Consider the inclusion map $\mathbb{C} \subseteq \mathbb{C}[X]$. Show that the conclusion of Incomparability fails. Which hypotheses are true?

(d) Consider the inclusion map $R := \mathbb{C}[X^2] \subseteq S := \mathbb{C}[X]$. Describe all of the primes $\mathfrak{q}_i$ that contract to $\mathfrak{p} := (X^2 - 1)R$. Verify the conclusions on Incomparability and Lying Over for $\mathfrak{p}$ and the $\mathfrak{q}_i$.

[1] Reminder: by abuse of notation, even when $\phi : R \to S$ is not injective, we write $\mathfrak{q} \cap R$ for $\phi^{-1}(\mathfrak{q}) \subseteq R$.

(2) Proof of Corollary using the theorems: Let $R \to S$ be integral.

(a) Use one of the Theorems above to show that for any chain of primes

$$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_n = \mathfrak{q} \qquad \text{in } \operatorname{Spec}(S)$$

the containments

$$(\mathfrak{q}_0 \cap R) \subseteq (\mathfrak{q}_1 \cap R) \subseteq \cdots \subseteq (\mathfrak{q}_n \cap R) = (\mathfrak{q} \cap R) \quad \text{in } \operatorname{Spec}(R)$$

are proper. Explain why this implies Part (3).

(b) Deduce part (4) from part (3).

(c) Let $R \subseteq S$ be an inclusion, and take a chain of primes

$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_n \qquad \text{in } \operatorname{Spec}(R).$$

Use Lying Over and Going up to find a chain of primes

$$\mathfrak{q}_0 \subsetneqq \mathfrak{q}_1 \subsetneqq \cdots \subsetneqq \mathfrak{q}_n \qquad \text{in } \operatorname{Spec}(S)$$

such that $\mathfrak{q}_i \cap R = \mathfrak{p}_i$ for all i. Deduce part (5).

(d) Prove part (6).

(e) Let $\mathfrak{q} \in \operatorname{Spec}(S)$ and $\mathfrak{p} \in \operatorname{Spec}(R)$. Show that if $\mathfrak{q} \cap R = \mathfrak{p}$, then $\mathfrak{q} \supseteq \mathfrak{p}S$, and if $\mathfrak{q}_0$ is some prime of S such that $\mathfrak{p}S \subseteq \mathfrak{q}_0 \subseteq \mathfrak{q}$, then $\mathfrak{q}_0 \cap R = \mathfrak{p}$ also.

(f) Show that every prime that contracts to $\mathfrak{p}$ is a minimal prime of $\mathfrak{p}S$, and deduce parts (1) and (2).

(3) Hypotheses of Going Down:

(a) Consider the inclusion map $\mathbb{C}[X] \subseteq \mathbb{C}[X,Y]/(XY, Y^2 - Y)$. Show that[2] the conclusion of Going Down fails. Which hypotheses are true?

(b) Consider the inclusion map $\mathbb{C}[X(1-X), X^2(1-X), Y, XY] \subseteq \mathbb{C}[X,Y]$. Show that[3] the conclusion of Going Down fails. Which hypotheses are true?

[2]Consider $(1-y)$, (X), and (0).

[3]Consider $(1-X, Y)$, $(X(1-X), X^2(1-X), Y, XY)$, and $(1-X, Y) \cap R$.

§7.31: COHEN-SEIDENBERG THEOREMS: PROOFS

LYING OVER: Let $R \subseteq S$ be an integral inclusion. Then the induced map $\mathrm{Spec}(S) \to \mathrm{Spec}(R)$ is surjective. That is, for any prime $\mathfrak{p} \in \mathrm{Spec}(R)$, there is a prime $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$; i.e., a prime *lying over* $\mathfrak{p}$.

INCOMPARABILITY: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{q}_1, \mathfrak{q}_2 \in \mathrm{Spec}(S)$ such that $\mathfrak{q}_1 \cap R = \mathfrak{q}_2 \cap R$, we have $\mathfrak{q}_1 \not\subseteq \mathfrak{q}_2$. That is, any two primes lying over the same prime are *incomparable*.

GOING UP: Let $R \to S$ be integral (but not necessarily injective). Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \cap R = \mathfrak{p}$, there is some $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{Q} \cap R = \mathfrak{P}$.

GOING DOWN: Let $R \subseteq S$ be an integral inclusion of domains, and assume that R is normal. Then for any $\mathfrak{p} \subsetneq \mathfrak{P}$ in $\mathrm{Spec}(R)$ and $\mathfrak{Q} \in \mathrm{Spec}(S)$ such that $\mathfrak{Q} \cap R = \mathfrak{P}$, there is some $\mathfrak{q} \in \mathrm{Spec}(S)$ such that $\mathfrak{q} \subseteq \mathfrak{Q}$ and $\mathfrak{q} \cap R = \mathfrak{p}$.

LEMMA: Let $R \subseteq S$ be an integral inclusion and I an ideal of R. Then any element of $s \in IS$ satisfies a monic equation over R of the form[1]

$$s^n + a_1 s^{n-1} + \cdots + a_n = 0 \qquad \text{with } a_i \in I \text{ for all } i.$$

(1) Proof of Lying Over from the Lemma: Let $R \subseteq S$ be an integral inclusion.
- **(a)** Use the Lemma to show that if $\mathfrak{p}$ is prime, then $\mathfrak{p}S \cap R = \mathfrak{p}$.
- **(b)** Show that $(R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$ is not the zero "ring".
- **(c)** Deduce[2] the Theorem.

(2) Proof of Lemma: Let $R \subseteq S$ be an integral inclusion and I an ideal of R.
- **(a)** Show that if $s \in IS$, then there is a module-finite R-subalgebra of S, say T, such that $s \in IT$, so we can assume that S is module-finite.
- **(b)** Write $S = \sum_i Rs_i$ and $v = [s_1, \ldots, s_t]$. Show that there is some $t \times t$ matrix A with entries in I such that $rv = vA$.
- **(c)** Apply a TRICK and conclude the proof.

(3) Proof of Incomparability: Let $R \to S$ be integral.
- **(a)** Explain[3] why the Theorem is true when R is a field.
- **(b)** Let $\mathfrak{p}$ in $\mathrm{Spec}(R)$. Use the definition to explain why the map $R/\mathfrak{p} \to S/\mathfrak{p}S$ is integral, and why the map $(R \smallsetminus \mathfrak{p})^{-1}(R/\mathfrak{p}) \to (R \smallsetminus \mathfrak{p})^{-1}(S/\mathfrak{p}S)$ is integral.
- **(c)** Use the previous parts (plus an old bijection) to prove the Theorem.

(4) Proof of Going Up: Show that $R/\mathfrak{p} \to S/\mathfrak{q}$ is an integral inclusion, apply Lying Over, and deduce the Theorem.

---

[1] In fact, one can take $a_i \in I^i$ for each i by the same proof, which is often useful.

[2] The old bijection $\mathrm{Spec}(W^{-1}(T/J)) \longleftrightarrow \{\mathfrak{q} \in \mathrm{Spec}(T) \mid \mathfrak{q} \cap W = \varnothing \text{ and } J \subseteq \mathfrak{q}\}$ may come in handy.

[3] Hint: Recall an old fact about integral extensions of domains…

(5) Proof of Going Down.
   (a) Explain why it suffices to show that $(S \smallsetminus \mathfrak{Q})(R \smallsetminus \mathfrak{p}) \cap \mathfrak{p}S$ is empty.
   (b) Let x be an element of the intersection. Show that[4] the minimal monic polynomial $f(x)$ of x over $\mathrm{Frac}(R)$ has all nonleading coefficients in $\mathfrak{p}$.
   (c) Write $x = rs$ with $r \in R \smallsetminus \mathfrak{p}$ and $s \in S \smallsetminus \mathfrak{Q}$. Show that $g(s) = f(rs)/r^n$ is the minimal polynomial of s over $\mathrm{Frac}(R)$.
   (d) Show that $g(s)$ has coefficients in R, and obtain a contradiction to the assumption that x was an element of the intersection.

(6) (a) Show that if S is module-finite over R with t generators, then for every $\mathfrak{p} \in \mathrm{Spec}(R)$, at most t distinct primes of S contract to $\mathfrak{p}$.
   (b) Give an example of an integral inclusion $R \subseteq S$ such that there are primes of R with arbitrarily many primes contracting to it.

[4]Hint: First show all the coefficients are in R. For this, note that every coefficient of the minimal polynomial is a polynomial expression of the roots of f in an algebraic closure of $\mathrm{Frac}(R)$.

§7.32: NOETHER NORMALIZATION AND DIMENSION

THEOREM: Let K be a field, and R be a domain that is algebra-finite over K. Let $K[f_1, \ldots, f_n]$ be a Noether normalization of R. Any saturated chain of primes from 0 to a maximal ideal $\mathfrak{m}$ of R has length n.

COROLLARY: Let K be a field, and R be a finitely generated K-algebra. Then

(1) For any primes $\mathfrak{p} \subseteq \mathfrak{q}$ of R, every saturated chain of primes from $\mathfrak{p}$ to $\mathfrak{q}$ has the same length. (That is, R is **catenary**).
(2) If R is a domain, and I is an arbitrary ideal, then $\dim(R) = \dim(R/I) + \text{height}(I)$.

(1) Consequences of the Theorem: Let K be a field.

(a) Use the Theorem to deduce that $\dim(K[X_1, \ldots, X_n]) = n$.

(b) Use the Theorem to deduce that every Noether normalization has the same number of elements.

(c) Use part (a) above to show that the dimension of a K-algebra is at most the number of generators in an K-algebra generating set.

(d) Use the Theorem to prove part (1) of the Corollary.

(2) Let K be a field. Use the Theorem and previous computations to compute the dimension of each of the following rings:

(a) $\dfrac{K[X, Y, Z]}{(X^3 + Y^3 + Z^3)}$.

(b) $\dfrac{K[X, Y]}{(XY)}$.

(c) $K[X^4, X^3Y, XY^3, Y^4]$.

(3) Proof of Theorem: Induce on the number of elements n in a Noether normalization.

(a) Explain the case $n = 0$.

(b) For the general case, let $A = K[z_1, \ldots, z_n] \subseteq R$ be a Noether normalization, and take a saturated chain of primes of R:

$$(0) = \mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_s = \mathfrak{m}.$$

Explain why $\mathfrak{p}_1$ has height 1.

(c) Explain why $\mathfrak{p}_1 \cap A$ has height 1.

(d) Explain why $\mathfrak{p}_1 \cap A$ is principal.

(e) Explain why, after a change of coordinates, we can assume that $K[z_1, \ldots, z_{n-1}]$ is a Noether normalization of $R/\mathfrak{p}_1$.

(f) Finish the proof.

(4) Use the Theorem to prove part (2) of the Corollary.

(5) Let $R = K[X_1, \ldots, X_n]$ and $f_{m+1}, \ldots, f_n$ be polynomials such that $f_{m+1} \in K[X_1, \ldots, X_{m+1}]$ is monic in X_{m+1}, …, $f_n \in K[X_1, \ldots, X_n]$ is monic in X_n. Show that $K[x_1, \ldots, x_m]$ is a Noether normalization for $S = R/(f_{m+1}, \ldots, f_n)$, and deduce that $\dim(S) = m$, and that $\text{height}(f_{m+1}, \ldots, f_n) = n - m$.

(6) Let K be a field, and let $R \subseteq S$ be an inclusion of finitely generated K-algebras that are both domains. Show that for any $\mathfrak{q} \in \mathrm{Spec}(S)$, $\mathrm{height}(\mathfrak{q}) = \mathrm{height}(\mathfrak{q} \cap R)$.

(7) Let K be a field. Show that $K[\![X_1, \ldots, X_n]\!]$ is a domain of dimension n.

§7.33: TRANSCENDENCE DEGREE AND DIMENSION

DEFINITION: Let $K \subseteq L$ be an extension of fields and let S be a subset of L.

(1) The **subfield of L generated by K and S**, denoted $K(S)$, is the smallest subfield of L containing K and S. Equivalently, $K(S)$ is the set of elements in L that can be written as rational function expressions in S with coefficients in K.

(2) We say that S is **algebraically independent** over K if there are nonzero polynomial relations on any finite subset of S. Equivalently, S is algebraically independent over K if, for a set of indeterminates $X = \{X_s \mid s \in S\}$, there is an isomorphism of field extensions of K between the field of rational functions $K(S)$ and $K(X)$ via $s \mapsto X_s$.

(3) We say that S is a **transcendence basis** for L over K if S is algebraically independent over K and the field extension $K(S) \subseteq L$ is algebraic.

LEMMA: Let $K \subseteq L$ be an extension of fields.

(1) Every K-algebraically independent subset of L is contained in a transcendence basis. In particular, there exists a transcendence basis for L over K.

(2) Every transcendence basis for L over K has the same cardinality.

DEFINITION: Let $K \subseteq L$ be an extension of fields. The **transcendence degree** of L over K is the cardinality of a transcendence basis for L over K.

THEOREM: Let K be a field, and R be a domain that is algebra-finite over K. Then, the dimension of R is equal to the transcendence degree of $\mathrm{Frac}(R)$ over K.

(1) Let K be a field, and R be a domain that is algebra-finite over K.

(a) Explain why, if $R = K[f_1, \ldots, f_m]$, then $\mathrm{Frac}(R) = K(f_1, \ldots, f_m)$.

(b) Show[1] that if $A = K[z_1, \ldots, z_t]$ is a Noether normalization for R, then $\{z_1, \ldots, z_t\}$ forms a transcendence basis for $\mathrm{Frac}(R)$.

(c) Deduce the Theorem.

(2) Let K be a field. Use the Theorem to compute the dimension of

$$R = K[UX, UY, UZ, VX, VY, VZ] \subseteq K[U, V, X, Y, Z].$$

(3) Let $R \subseteq S$ be domains.

(a) Use the Theorem to prove that if $R \subseteq S$ are finitely generated algebras over some field K, then $\dim(R) \leq \dim(S)$.

(b) Give an example where $\dim(R) > \dim(S)$.

[1] Hint: Recall that every nonzero $r \in R$ has a nonzero multiple in A.

(4) Proof of Lemma: Let $K \subseteq L$ be fields, and S a subset of L.
   (a) Show that S is a transcendence basis for L over K if and only if it is a maximal K-algebraically independent subset of L.
   (b) Deduce part (1) of the Lemma.
   (c) Show that, to prove part (2) (in the case of two finite transcendence bases), it suffices to show the following
   EXCHANGE LEMMA: If $\{x_1, \ldots, x_m\}$ and $\{y_1, \ldots, y_n\}$ are two transcendence bases, then there is some j such that
   $\{x_j, y_2, \ldots, y_n\}$ is a transcendence basis.
   (d) In the setting of the Exchange Lemma, explain why for each j, there is some nonzero $p_j(t) \in K[y_1, \ldots, y_n][t]$ such that $p_j(x_j) = 0$.
   (e) In the setting of the previous part, explain why there is some j such that $p_j(t) \notin K[y_2, \ldots, y_n][t]$.
   (f) Show that the conclusion of the Exchange Lemma holds for j as in the previous part.

§8.34: SIMPLE MODULES AND LENGTH

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

(1) M is **simple** if it is nonzero and M has no nontrivial proper submodules.
(2) A **composition series** for M of length n is a chain of submodules
$$M = M_n \supsetneqq M_{n-1} \supsetneqq \cdots \supsetneqq M_1 \supsetneqq M_0 = 0$$
with M_i/M_{i-1} simple for all $i = 1, \ldots, n$. The
(3) M has **finite length** if it admits a composition series. The **length** of M, denoted $\ell_R(M)$ is the minimal length n of a composition series for M.

JORDAN-HÖLDER THEOREM: Let R be a ring, and M a module *of finite length*. Let $N \subseteq M$ be a submodule.

(1) Any descending chain of submodules of M can be refined[1] to a composition series for M.
(2) Every composition series for M has the same length.
(3) If $N \subseteq M$ is any submodule, then
  (a) N and M/N have finite length, and $\ell_R(N), \ell_R(M/N) \leq \ell_R(M)$,
  (b) $\ell_R(N), \ell_R(M/N) < \ell_R(M)$ unless $M = N$ or $N = 0$ respectively, and
  (c) $\ell_R(N) + \ell_R(M/N) = \ell_R(M)$.

COROLLARY: If M has finite length, then M is Noetherian and any descending chain of submodules of M stabilizes.

LEMMA: Let R be a ring. A module M is simple if and only if $M \cong R/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$.

PROPOSITION: Let R be a Noetherian ring, and M be a module. The following are equivalent:

(1) M has finite length,
(2) M is finitely generated and $\mathrm{Supp}_R(M) \subseteq \mathrm{Max}(R)$,
(3) M is finitely generated and $\mathrm{Ass}_R(M) \subseteq \mathrm{Max}(R)$.

(1) Working with length: Let $R = \mathbb{R}[X, Y]$.
  (a) Compute a composition series and find the R-module length of $M = R/(X^2 + 1, Y)$.
  (b) Compute a composition series and find the R-module length of $M = R/(X^2 + X, Y)$.
  (c) Compute a composition series and find the R-module length of $M = (X, Y)/(X^2, Y^2)$.

(2) Use the Jordan-Hölder Theorem to prove the Corollary.

(3) Proof of Proposition: Let R be a Noetherian ring.
  (a) How do the concepts of "composition series" and "prime filtration" compare?
  (b) Why does having finite length imply that M is finitely generated[2]? What can one deduce about the associated primes of M? Deduce (1)⇒(3).
  (c) Use the definition of support to explain why, if $R/\mathfrak{p}$ is a factor in a prime filtration for M, then $\mathfrak{p} \in \mathrm{Supp}_R(M)$. Deduce (2)⇒(1).
  (d) Show (3)⇒(2) to complete the proof.

[1] That is, terms can be inserted in between others in the chain to get a composition series.
[2] The Corollary is fair game.

(4) Show that if R is a finitely generated algebra of an algebraically closed field K, then the length of an R-module M is equal to the dimension of M as a K-vector space.

(5) Proof of Jordan-Hölder: We will show (3a), (3b) directly, then deduce (1), (2), and (3c).
   (a) Let's start with deducing the other parts from (3a) and (3b). Show that (3a)+(3b)⇒(1) by inducing on length.
   (b) Show that (3a)⇒(2) by induction on length: given another composition series
   $$M = N_m \supsetneq N_{m-1} \supsetneq \cdots \supsetneq N_1 \supsetneq N_0 = 0,$$
   consider the case $N_{m-1} = M_{n-1}$, and in the other case, consider $K = N_{m-1} \cap M_{n-1}$.
   (c) Show that (1)+(2)⇒(3c).
   (d) Now we start on (3a) and (3b). Use the Second Isomorphism Theorem to show that
   $$\frac{M_i \cap N}{M_{i-1} \cap N} \cong \frac{M_i \cap N + M_{i-1}}{M_{i-1}}.$$
   (e) Show that N has a composition series of length at most n.
   (f) Show that if the composition series you just found for N has length n, then $N = M$, so if $N \subsetneq M$, then $\ell_R(N) < \ell_R(M)$.
   (g) Use the Second Isomorphism Theorem to show that
   $$\frac{(M_i + N)/N}{(M_{i-1} + N)/N} \cong \frac{M_i}{M_i \cap (M_{i-1} \cap N)}.$$
   (h) Show that M/N has a composition series of length at most n.
   (i) Show that if the composition series you just found for M/N has length n, then $N = 0$, so if $N \neq 0$, then $\ell_R(M/N) < \ell_R(M)$. Deduce (3a) and (3b) to finish the proof.

§8.36: KRULL HEIGHT THEOREM

PRINCIPAL IDEAL THEOREM: Let R be a Noetherian ring and $f \in R$. Then every minimal prime of (f) has height at most one.

KRULL'S HEIGHT THEOREM: Let R be a Noetherian ring and $I = (f_1, \ldots, f_n)$. Then every minimal prime of I has height at most n.

(1) Use Krull's Height Theorem to deduce the following:
- **(a)** Every ideal in a Noetherian ring has finite height.
- **(b)** Every Noetherian local ring has finite dimension.
- **(c)** If R is a finitely generated algebra over a field that is a domain, and $I = (f_1, \ldots, f_t)$ is a proper ideal, then $\dim(R/I) \geq \dim(R) - t$.

(2) Proof of Principal Ideal Theorem:
- **(a)** Suppose that the Theorem is false, so there is some Noetherian ring S, some $g \in S$, and some prime $\mathfrak{q}$ such that $\mathfrak{q} \in \mathrm{Min}((g))$ with $\mathrm{height}(\mathfrak{q}) > 1$. Show that we can then find a Noetherian local domain $(R, \mathfrak{m})$ of dimension greater than one and some $f \in R$ such that $\mathrm{Min}((f)) = \{\mathfrak{m}\}$. Henceforth, we continue with this notation.
- **(b)** Explain why $R/(f)$ is Artinian.
- **(c)** Let $\mathfrak{q}$ be a prime between (0) and $\mathfrak{m}$. Let $\mathfrak{q}^{(n)} = \mathfrak{q}^n R_{\mathfrak{q}} \cap R$; recall that, by the Second Uniqueness Theorem for Primary Decomposition, this[1] is the $\mathfrak{q}$-primary component of $\mathfrak{q}^n$ in R in any primary decomposition. Explain why there exists some n such that $\mathfrak{q}^{(n)}R/(f) = \mathfrak{q}^{(n+k)}R/(f)$ for all $k > 0$.
- **(d)** Show[2] that $\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+k)} = f(\mathfrak{q}^{(n)}/\mathfrak{q}^{(n+k)})$ for all $k > 0$.
- **(e)** Show that $\mathfrak{q}^{(n)} = \mathfrak{q}^{(n+k)}$ for all $k > 0$.
- **(f)** Show that $0 \neq \bigcap_{n>0} \mathfrak{q}^{(n)}$ from above and $\bigcap_{n>0} \mathfrak{q}^{(n)} \subseteq \bigcap_{n>0} \mathfrak{q}^n R_{\mathfrak{q}} = 0$ from another Theorem to obtain the decisive contradiction.

(3) Proof of Krull Height Theorem: We induce on t.
- **(a)** Dispatch with the base case.
- **(b)** Fix a chain of primes
$$\mathfrak{p}_0 \subsetneqq \mathfrak{p}_1 \subsetneqq \cdots \subsetneqq \mathfrak{p}_h = \mathfrak{p}$$
with $\mathfrak{p}$ a minimal prime $\mathfrak{p}$ of $I = (f_1, \ldots, f_t)$. Suppose that $f_1 \in \mathfrak{p}_1$. Apply the inductive hypothesis to $I/(f_1)$ in $R/(f_1)$ and complete the inductive step in this case.
- **(c)** Use the Principal Ideal Theorem to prove the following:
LEMMA: Let R be a Noetherian ring, $\mathfrak{p} \subsetneqq \mathfrak{q} \subsetneqq \mathfrak{r}$ be primes and $f \in \mathfrak{r}$. Then there exists some prime $\mathfrak{q}'$ such that $\mathfrak{p} \subsetneqq \mathfrak{q}' \subsetneqq \mathfrak{r}$ and $f \in \mathfrak{q}'$.
- **(d)** Use the Lemma to complete the inductive step in the case $f_1 \notin \mathfrak{p}_1$.

(4) Let K be a field, and $R = K[X, XY, XY^2, \ldots] \subseteq S = K[X, Y]$. Show that the height of $(X)R$ is two. Compare this to Krull's Height Theorem.

(5) Let R be a Noetherian ring, I be an ideal, and $f \in R$. Must one have $\mathrm{height}(I + (f)) \leq \mathrm{height}(I) + 1$?

(6) Let R be a Noetherian ring and $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals. Show that if there exists some prime strictly between $\mathfrak{p}$ and $\mathfrak{q}$, then there exist infinitely many primes between $\mathfrak{p}$ and $\mathfrak{q}$.

[1] This is known as the nth *symbolic power* of $\mathfrak{q}$.

[2] Use the fact that $f \notin \mathfrak{q}$ and $\mathfrak{q}^{(n)}$ is primary.