WORKSHEET PREVIEWS FOR MATH 905

TABLE OF CONTENTS

INTRODUCTION

What am I? The majority of this document consists of the 1–2 page daily quick summaries that you should read before each class. These will include some reminders of things from previous algebra courses that we will use, as well as the statements of definitions and theorems we will encounter in class, so that we aren't just wasting class time reading a definition or theorem for the first time. We will not follow any textbook directly, but most of the material will overlap with the recommended text Atiyah-MacDonald and Grifo's Fall 2022 905 notes, the latter of which is available here:

`https://eloisagrifo.github.io/Teaching/ca1/CA1notes.pdf`

Each course preview references the relevant sections of the sources in this case. Some previews also have a "Just for fun" at the end: this is either an open question or easily stated fact requiring deeper techniques. This part of the reading is optional and can be skipped if you don't like fun.

Mathematical ground rules. In this class, all rings are commutative with $1 \neq 0$, and all modules are unital, meaning $1m = m$ for all $m \in M$. We are assuming as background knowledge the content covered in the first year algebra sequence Math 817–818.

Using these worksheets.

- To complete a problem on a worksheet means to discuss as a group until every member of the group understands the solution. I envision solving a "Prove" or "Show that" problem as meaning to know how to fill in all of the details of a proof (though you might not find it practical to write out a full proof of everything starting from ZFC), whereas an "Explain" or "Discuss" might not require as rigorous a solution or might not even be a completely precise question. If you do not understand your solution or are unsure of something, let your group know: they are probably missing something or could understand some detail better. Conversely, if someone in your group doesn't understand the solution, you should thank them for the opportunity to understand the problem better, as you may have missed something, or you might understand better by explaining your thoughts if you think you haven't.
- The worksheets have some problems numbered in bold **(1)**, some in standard font (2), and some in italics *(3)*. Those marked in bold **(1)** you should think of as mandatory, either in class, or after class if you didn't get to them. Those in standard font (2) are recommended. Those in italics *(3)* are somewhat more for adventure seekers.
- As noted above, the assumed background is Math 817–818. If you've taken a Homological Algebra or Commutative Algebra 2 course or a reading on related topics like Gröbner bases, you might find that some questions are an easy consequence of some fact about faithfully flat modules, Ext-modules, regular sequences, or regular rings. You should feel free to enjoy your knowledge in such cases, but every problem has a solution only using material the background sequence, and you should find a solution of that type: this is both so that you develop mastery of the notions of basic commutative algebra and to avoid any logical circularities!

Why are you doing this to me? Math is learned by working through proofs and examples, not by watching someone else do the work. I could tell you about all of the interesting commutative algebra I know, and I could mix it in with funny anecdotes and obscure puns, but my algebra will never be your own until you do it. So we will just skip the step where I read to you: you know how to read anyway. This style of class may stretch our comfort zone more than a conventional lecture, but it's a much better approximation of doing research and writing a thesis than the latter.

1. Rings, Ideals, and Modules

1.1. Rings: Lecture Notes §0.1.

- Key examples of rings: polynomial rings, power series rings, and function rings
- Key constructions of rings: quotient rings, product rings, and subrings
- Special elements in rings: units, zerodivisors, nilpotents, and idempotents

Special elements in rings.

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 $x^2 = x$.

Polynomial rings. Polynomial rings, and quotients of polynomial rings, will be ubiquitous in this class. Recall: Given a ring A, the polynomial ring $A[X]$ in one indeterminate X is

$$A[X] := \{a_d X^d + \cdots + a_1 X + a_0 \mid d \geq 0, a_i \in A\}.$$

We can also form the polynomial ring in finitely many indeterminates $A[X_1, \ldots, X_n]$, which is the same as the polynomial ring in one variable X_n with coefficients in $A[X_1, \ldots, X_{n-1}]$. We can even take a polynomial ring in an arbitrary set of indeterminates $A[X_\lambda \mid \lambda \in \Lambda]$, whose elements are *finite* sums of terms of the form $aX_{\lambda_1}^{d_1} \cdots X_{\lambda_k}^{d_k}, a \in A$. It is often convenient to break up polynomials by **degree**: the degree t part of a polynomial is the sum of all of the terms as above with $d_1 + \cdots + d_k = t$. In particular, for a polynomial in one variable, the degree t part is the X^t term (with its coefficient). We will say **top degree** of a polynomial to refer to the highest degree term if terms of different degrees occur.

Power series rings. Power series rings, and quotients of power series rings, will also be a main source of examples for us. Recall: Given a ring A, the power series ring $A[\![X]\!]$ in one indeterminate X is

$$A[\![X]\!] := \Big\{ \sum_{i \geq 0} a_i X^i \mid a_i \in A \Big\}.$$

The "infinite summation" is to be thought of formally; infinite addition is not a well-defined operation in this ring as one cannot make sense of things like $X + X + X + \cdots$. If you get disoriented with a power series, it is best to proceed one coefficient at a time, going from **lowest** up towards infinity. For example, two series $f = \sum_i a_i X^i$ and $g = \sum_i b_i X^i$, are the same if and only if $a_i = b_i$ for all i, and to compute fg, compute the zeroth coefficient $a_0 b_0$, then the first coefficient $a_1 b_0 + a_0 b_1$, and so on[1]. We'll also consider multivariate power series rings

$$A[\![X_1, \ldots, X_n]\!] := \{ \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n} \mid a_{i_1, \ldots, i_n} \in A\} = (A[\![X_1, \ldots, X_{n-1}]\!])[\![X_n]\!].$$

[1]The only problem is that if you want to write everything out concretely, you have to do this forever.

Function rings. Various natural collections of functions form rings with pointwise operations $+$ and $\times$; i.e., $f + g$ is the function whose value at x is $f(x) + g(x)$. For example:

- $\mathrm{Fun}([0,1], \mathbb{R})$, the set for all functions from $[0,1]$ to $\mathbb{R}$.
- $\mathcal{C}([0,1], \mathbb{R})$, the set of continuous functions from $[0,1]$ to $\mathbb{R}$.
- $\mathcal{C}^\infty([0,1], \mathbb{R})$, the set of infinitely differentiable functions from $[0,1]$ to $\mathbb{R}$.
- $\mathcal{C}^{\mathrm{an}}([0,1], \mathbb{R})$, the set of analytic[2] functions from $[0,1]$ to $\mathbb{R}$.

Product rings. Recall that given two rings R, S we can form the product ring $R \times S$. We can recognize product rings in many situations:

CHINESE REMAINDER THEOREM: Let R be a ring, and I, J be two ideals such $I+J = R$. Then $IJ = I \cap J$ and $R/IJ \cong R/I \times R/J$.

PROPOSITION: A ring T is isomorphic to a product $R \times S$ of two rings if and only if there is an idempotent $e \in T$ with $e \neq 0, 1$.

Just for fun. There are lots of things we don't know even about polynomials in one variable over a field. Here is an open problem:

CASAS-ALVERO CONJECTURE: Let K be a field of characteristic zero. Suppose that $f(X) \in K[X]$ is a monic polynomial of top degree n such that for each $i \in \{1, \ldots, n-1\}$, f and $\dfrac{d^i f}{dx^i}$ have a common root. Then $f = (X - a)^n$ for some $a \in K$.

For a warmup, can you show that the conclusion holds if all of these derivatives have a common root?

[2] i.e., functions that agree with a power series on some neighborhood of any point

1.2. **Ideals: Lecture Notes §0.1.**

- Generating set of an ideal
- Radical of an ideal
- Division Algorithm

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

$$(S) = \left\{ \sum r_i s_i \mid r_i \in R, s_i \in S \right\} \quad \text{is the set of } R\text{-linear combinations}^3 \text{ of elements of } S.$$

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

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

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

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

- If J is an ideal of S, then $\phi^{-1}(J) := \{r \in R \,|\phi(r) \in J\}$ is an ideal of R, often denoted $J \cap R$.
- If I is an ideal of R, then $IS := (\phi(I))$ is an ideal of S.

Radical ideals.
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 $I = \sqrt{I}$.

PROPOSITION: The radical of an ideal is an ideal.

Division Algorithm. You are certainly familiar with the division algorithm in $K[X]$ when K is a field. For an arbitrary ring in place of K, we can do the same thing as long as we divide by a **monic** polynomial:

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

The division algorithm is often useful for finding generators of an ideal. One can use it in a multivariate polynomial ring $A[X_1, \ldots, X_n]$ by thinking of it as a polynomial ring in one variable X_n with coefficients in $A[X_1, \ldots, X_{n-1}]$.

Just for fun. It can be very hard to tell whether an ideal is radical. Here is a well-known open question:

COMMUTING MATRIX PROBLEM: Let K be a field. Let $\mathbb{X} = [X_{i,j}]_{1 \leq i,j \leq n}$ and $\mathbb{Y} = [Y_{i,j}]_{1 \leq i,j \leq n}$ be two $n \times n$ matrices of indeterminates, and $R = K[\mathbb{X}, \mathbb{Y}]$ be a polynomial ring in $2n^2$ variables. Let I be ideal generated by the entries[4] of the commutator matrix $\mathbb{XY} - \mathbb{YX}$. Is I reduced?

[4] I.e., there are n^2 generators of the form $X_{i,1}Y_{1,j} + \cdots + X_{i,n}Y_{n,j} - Y_{i,1}X_{1,j} + \cdots + Y_{i,n}X_{n,j}$ for $1 \leq i, j \leq n$.

1.3. **Algebras: Lecture Notes §1.2.**

Key topics:
- Generating sets of algebras
- Presentation of an algebra

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. Note: the same ring R with different ϕ's are different A-algebras. Despite this we often say "Let R be an A-algebra" without naming the structure morphism. If R is an A-algebra with structure map ϕ, then $\phi(A) \subseteq R$. We often consider the special case when ϕ is an inclusion map, so $A \subseteq R$.

DEFINITION: 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 $\alpha \circ \phi = \psi$. When ϕ and ψ are inclusion maps $A \subseteq R$ and $A \subseteq S$, this just says[5] $\alpha|_A = \mathbb{1}_A$.

The mapping property of polynomial rings is best expressed in the language of algebras:

UNIVERSAL PROPERTY OF POLYNOMIAL RINGS: Let[6] 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 $\alpha(X_i) = r_i$.

Algebra generators.

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

$$A[S] = \{ \text{ sums of elements of the form } \phi(a) r_1^{i_1} \cdots r_t^{i_t} \mid a \in A, r_j \in S, i_j \geq 0 \},$$

where ϕ is the map from A to R.

It may be helpful to think of an A-algebra R as a ring built from A, and a generating set as a collection of building blocks that one can use to build R from A with the ring operations.

WARNING: We have used the notation $A[\text{stuff}]$ both for polynomial rings in the "stuff" variables and the algebra generated by "stuff" in some other algebra. It is best practice to make clear which you mean when there is risk of any confusion. We will also generally use capital letters X_i, X, Y, Z for indeterminates (i.e., polynomial and power series variables).

PROPOSITION: Let[7] A be a ring, and R be an A-algebra. Then $A[r_1, \ldots, r_n]$ is the image of the A-algebra homomorphism $\alpha : A[X_1, \ldots, X_n] \to R$ such that $\alpha(X_i) = r_i$.

[5] We use $\mathbb{1}$ for the identity map, and later on, for the identity matrix.

[6] 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.

[7] This is also equally valid for infinite sets.

Algebra presentations.

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 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 $R \cong A[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$.

It may be helpful to think of a presentation as a recipe for building R as a ring starting from A. The proposition above says that a presentation (or just a set of defining relations) is sufficient information to determine an algebra up to isomorphism.

Just for fun. The most notorious open problem in commutative algebra is easy to state:

JACOBIAN CONJECTURE: Let K be a field of characteristic zero, and $R = K[X_1, \ldots, X_n]$ be a polynomial ring over K. Let $f_1, \ldots, f_n \in R$. Then

$$R = K[f_1, \ldots, f_n] \quad \text{if and only if} \quad \det \begin{bmatrix} \frac{\partial f_1}{\partial X_1} & \cdots & \frac{\partial f_n}{\partial X_1} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_1}{\partial X_n} & \cdots & \frac{\partial f_n}{\partial X_n} \end{bmatrix} \in K^\times.$$

Can you see which direction is the hard one? This is open even for $n = 3$.

1.m Macaulay2 Introduction: Lecture Notes §A.1.

Key topics:

- Accessing M2
- Defining rings, ideals, maps

Running Macaulay2. Macaulay2 is a computer algebra system with a wide range of functions implemented for commutative algebra and algebraic geometry. You can run it online at

`https://www.unimelb-macaulay2.cloud.edu.au/`

You can also install it on your machine, but that isn't necessary at first. You many want to click the "Editor" tab, so you can type your commands on the left-side pane. You can execute a line with `SHIFT+ENTER`.

Basic commands. Here are enough commands to get started.

- Starting rings: Try `K=QQ`, `K=ZZ`, or `K=ZZ/13`
- Polynomial rings: After fixing a starting ring, try `R=K[X,Y]` or `S=K[X_1 .. X_4]`
- Ideals: With R as above, try `I=ideal(X^2,X*Y)` or `J=ideal(X^3-2*X^2*Y+7*Y^5)`
- Ideal containment: With I as above, try `(2*X^3-X*Y^2)%I` or `(2*Y^3-X*Y^2)%I`
- Ideal operations: With I and J as above, try `I+J`, `I*J`, `I:J`, `I^4`, or `intersect(I,J)`
- Radicals: With I and J as above, try `radical I` or `radical J`
- Homomorphisms: With R and S as above, try `f=map(R,S,{X^3,X^2*Y,X*Y^2,Y^3})`
- Kernels: With f as above, try `ker f`
- Quotient rings: With R and I as above, try `R/I`

Learning more. Go to `https://macaulay2.com/` if you want to learn more.

1.4. **Modules: Lecture Notes §0.2, §1.1.**

Key topics:
- Generating set of a module
- Presentation of a module

Sources of modules. Here are a few sources of modules:

(1) Every ideal $I \subseteq R$ is a submodule of R.
(2) Every quotient ring R/I is a quotient module of R.
(3) 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**: $r \cdot s := \alpha(r)s$.
(4) 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**[8]: $r \cdot m := \alpha(r) \cdot m$.
(5) Given an $n \times m$ matrix A, its image $\mathrm{im}(A)$, is the module generated by its columns in R^n.

Free modules. Recall that a module is **free** if it admits a **free basis**: a generating set (see below for refresher) that is linearly independent. Every free module with a basis of n elements is isomorphic to the module R^n of n-tuples of elements of R. The module R^n has a **standard basis** $e_1, \ldots, e_n$ where e_i is the tuple with i-th entry equal to 1 and every other entry equal to 0. More generally, every free module with a basis that is bijective to some index set Λ is isomorphic to

$$R^{\oplus\Lambda} = \{(r_\lambda)_{\lambda\in\Lambda} \mid r_\lambda \neq 0 \text{ for at most finitely many } \lambda \in \Lambda\}.$$

UNIVERSAL PROPERTY OF FREE MODULES: Let R be a ring, and R^n be a free module. For any A-module M, and any collection[9] of elements $m_1, \ldots, m_n \in M$, there is a unique R-module homomorphism $\beta : R^n \to M$ such that $\beta(e_i) = m_i$.

Generating sets.
DEFINITION: Let M be an R-module. Let S be a subset of M. The **submodule generated by** S, denoted[10] $\sum_{s\in S} Rs$, is the smallest R-submodule of M containing S. Equivalently,

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

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

PROPOSITION: Let[11] R be a ring, and M be an R-module. Then $\sum_i Rm_i$ is the image of the R-module homomorphism $\beta : R^n \to M$ such that $\beta(e_i) = m_i$.

Module presentations.
DEFINITION: Let M be an R-module. Let $m_1, \ldots, m_n \in M$. The **module of R-linear relations** on $m_1, \ldots, m_n$ is the set of n-tuples $[r_1, \ldots, r_n]^{\mathrm{tr}} \in R^n$ such that $\sum_i r_i m_i = 0$ in R. Equivalently, the submodule of R-linear relations is the kernel of the homomorphism $\beta : R^n \to M$ such that $\beta(e_i) = m_i$.

DEFINITION: A (finite[12]) **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.

PROPOSITION: If M is an R-module, and A is an $n \times m$ presentation matrix for M, then $M \cong R^n/\mathrm{im}(A)$.

[8] Note that if $R \subseteq S$, then the name "restriction of scalars" is spot-on; we are literally restricting which scalars can be used.
[9] This is equally valid for free modules in infinitely basis elements $R^{\oplus\Lambda}$ with a tuple of elements $\{m_\lambda\}_{\lambda\in\Lambda}$ in M in bijection with the free basis. I just wrote this with finitely many basis elements to keep the notation for getting too overwhelming.
[10] If $S = \{m\}$ is a singleton, we just write Rm, and if $S = \{m_1, \ldots, m_n\}$, we may write $\sum_i Rm_i$.
[11] This is also equally valid for infinite sets.
[12] We leave it to you to state the definition of an infinite presentation.

1.5. **Determinants.**

Key topics:
- Matrices and linear combinations
- The adjoint trick
- Ideals of minors

Matrices and linear combinations. 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. This makes sense whenever one of our matrices has entries in a ring R and the other has entries in a module M. In particular, given $m_1, \ldots, m_n \in M$, we can write $\begin{bmatrix} m_1 & \cdots & m_n \end{bmatrix} B$, for some $n \times m$ matrix B with entries in R, as a recipe for b linear combinations of our starting elements, with coefficients/weights given by the columns of B. Note that there is no difference between $\sum_j m_j b_{i,j}$ and $\sum_j b_{i,j} m_j$: over a commutative ring, acting on the left and acting on the right makes no difference.

Determinants. Recall that, 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 $\det(\phi(A)) = \phi(\det(A))$.
($\star$) $\det(A)\mathbb{1}_n = A^{\mathrm{adj}}A = A\,A^{\mathrm{adj}}$, where

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

Property ($\star$) is sometimes called the ADJOINT TRICK.

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, for a row vector w, if $wA = rw$, then $\det(r\mathbb{1}_n - A)w = 0$.

Ideals of minors.
DEFINITION: Given an $n \times m$ matrix A and $1 \le t \le \min\{m, n\}$ the ideal of $t \times t$ minors of 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 $I_t(A) = 0$.

PROPOSITION: Let A be an $n \times m$ matrix and B be an $m \times \ell$ matrix over R.

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

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

2.6. **Algebra-finite and module-finite maps: Lecture Notes §1.3, 1.4.**

Key topics:
- Algebra-finite and module-finite maps
- Module-finite $\Longrightarrow$ algebra-finite
- Integral elements

Algebra-finite and module-finite maps.

DEFINITION: Let $\phi : R \to S$ be a ring homomorphism.
- We say that ϕ is **algebra-finite**, or that S is **algebra-finite** over R, if S is a finitely generated R-algebra.
- We say that ϕ is **module-finite**, or that S is **module-finite** over R, if S is a finitely generated R-module.

These are *relative* finiteness conditions for a ring S.

We have already seen examples of maps that are algebra-finite, and examples that are not algebra-finite; likewise for module-finite. A map $\phi : R \to S$ is algebra-finite (or module-finite) if and only if $\phi(R) \subseteq S$ is algebra-finite (respectively, module-finite), so we will sometimes just focus on inclusion maps.

PROPOSITION: Let $R \to S$ and $S \to T$ be ring homomorphisms.
- If $R \to S$ and $S \to T$ are algebra-finite, then the composition $R \to T$ is algebra-finite.
- If $R \to S$ and $S \to T$ are module-finite, then the composition $R \to T$ is module-finite.

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

Integral elements.

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; that is, there exists $n > 0$ and $a_1, \ldots, a_n \in A$ such that

$$r^n + a_1 r^{n-1} + \cdots + a_n = 0.$$

An integral element is algebraic over A (i.e., $\{r\}$ is not algebraically independent over A), but integral is a stronger condition than algebraic. Note that r is integral over A if and only if it is integral over the image of A in R.

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.

Just for fun. Questions about algebra-finiteness can be incredibly difficult. Among Hilbert's highly influential list of twenty three problems posed at the beginning of the twentieth century is the following:

HILBERT'S 14TH PROBLEM: Let K be a field and $R = K[X_1, \ldots, X_n]$ be a polynomial ring. Let L be a subfield of the rational function field $K(X_1, \ldots, X_n)$ (i.e., the fraction field of R). Is $R \cap L$ algebra-finite over K?

The first counterexample to this well-known problem was given *sixty* years later by Nagata. Is it any easier if $n = 1$?

2.7. **Integral extensions: Lecture Notes §1.4.**

Key topics:
- Integral extensions
- Module-finite $\Longleftrightarrow$ algebra-finite & integral
- Integral closure of a ring
- Integral extension and fields

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.

This is another *relative* finiteness condition for a ring R.

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 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.

Integral extensions force rings to be closely related. This is a theme that will be important for us later on. As a first case of this principle, we have:

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

Integral closure.

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.

It is not obvious from the definition, but the integral closure of A in R is a ring.

Just for fun. Here is an innocuous looking fact:

THEOREM: Let K be a field, and $f_1, \ldots, f_{n+1} \in K[X_1, \ldots, X_n]$ be $n+1$ polynomials in n variables. Then $f_1^n \cdots f_{n+1}^n \in (f_1^{n+1}, \ldots, f_{n+1}^{n+1})$.

For example, if $f, g, h \in K[X, Y]$, then $f^2 g^2 h^2 \in (f^3, g^3, h^3)$.

The only proof of this fact that I know of uses deep facts about integral closure! Is it easy when $n = 1$? What about when $n = 2$?

2.8. **UFDs and integral closure.**

Key topics:
- Normal rings
- UFD $\Longrightarrow$ normal
- Polynomial rings are UFDs

DEFINITION: Let R be a domain. The **normalization** 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.

DEFINITION: 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.

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[13] 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.

The proof of the previous theorem largely follows from the following fact from Math 818:

GAUSS' LEMMA: Let R be a UFD and K be the fraction field of R.
(1) $f \in R[X]$ is irreducible if and only if f is irreducible in $K[X]$ and the coefficients of f have no common factor.
(2) 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.

[13] That is, 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 $r = ua_1 \cdots a_n$

2.9. **Noetherian rings: Lecture Notes §1.6.**

Key topics:
- Noetherian rings: definition and equivalences
- Hilbert Basis Theorem

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 $n \geq N$.

Here are some equivalent conditions for a ring to be Noetherian:
- R is Noetherian if and only if every nonempty collection of ideals has a maximal[14] element.
- R is Noetherian if and only if every ideal is finitely generated.

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.

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". Then $\mathcal{P}$ is true for every Noetherian ring.

[14]Warning: 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 $\mathcal{S}$.

2.10. **Noetherian modules: Lecture Notes §1.6.**

Key topics:
- Noetherian modules
- Noetherianity vs finite generation
- Proof of Hilbert Basis Theorem

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 $n \geq N$.

Here are some equivalent conditions for a module to be Noetherian:
- M is Noetherian if and only if every nonempty collection of submodules has a maximal[15] element.
- M is Noetherian if and only if every submodule is finitely generated.

THEOREM: If R is a Noetherian ring, then a 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 module is finitely generated.

LEMMA: Let M be a 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 $\dfrac{L+N}{N} = \dfrac{L'+N}{N}$.

[15]This means that if $\mathcal{S}$ is our collection of submodules, there is some $L \in \mathcal{S}$ such that no $L' \in \mathcal{S}$ properly contains L.

3. GRADED RINGS

3.11. **Graded rings: Lecture Notes §2.1.**

Key topics:
- Definition of graded ring, homogeneous element, homogeneous ideal
- Examples of graded rings

Graded rings, homogeneous elements and ideals. Some rings have a notion of "degree" that behaves analogously to degree in polynomial rings. This ends up being very useful for multiple reasons. It comes with an unescapable list of definitions though.

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** n if $x \in R_n$.

(4) The **homogeneous decomposition** of an nonzero[16] element r in an $\mathbb{N}$-graded ring is the sum

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

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 that every homogenous component of r is in I. (Equivalently, I is 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.

Examples of graded rings:

- The main example of a graded ring is a polynomial ring $R = K[X_1, \ldots, X_n]$ with the **standard grading**, where R_d is the K-vector space with basis given by monomials $X_1^{d_1} \cdots X_n^{d_n}$ such that $d_1 + \cdots + d_n = d$.
- There are also **weighted gradings** on R: given $a_1, \ldots, a_n \in \mathbb{N}$, instead take R_d to be the K-vector space with basis given by monomials $X_1^{d_1} \cdots X_n^{d_n}$ such that $a_1 d_1 + \cdots + a_n d_n = d$.
- One also has the **fine grading** on R. This is the $\mathbb{N}^n$-grading where $R_{(d_1,\ldots,d_n)} = K \cdot X_1^{d_1} \cdots X_n^{d_n}$.
- Quotients of graded rings by homogeneous ideals are graded: If R is a G-graded ring and $I \subseteq R$ is homogeneous, then R/I is G-graded with $(R/I)_g = \{\overline{r} \mid r \in R_g\}$.
- Let $R = K[X_1, \ldots, X_n]$ be a polynomial ring over a field, considered with the fine grading. The homogeneous ideals of R in the *fine grading* are exactly the **monomial ideals**—ideals generated by monomials.
- Let $R = K[X_1, \ldots, X_n]$ be a polynomial ring over a field. Let S be a subs4migroup of $\mathbb{N}^n$ with operation $+$ and identity $\mathbf{0}$. The **semigroup ring** of S is

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

[16] If we must speak of the homogeneous decomposition of 0, it would be the empty sum.

The graded K-subalgebras of R in the *fine grading* are exactly the semigroup rings for semigroups of $\mathbb{N}^n$.

- 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

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

Suppose that G acts by graded homomorphisms (thinking of R with the standard grading); equivalently, $g \cdot X_i$ is homogeneous of degree one for each i. Then R^G is an $\mathbb{N}$-graded K-subalgebra of R.

3.12. **Graded modules: Lecture Notes §2.1.**

Key topics:

- Basic terminology of graded modules
- Graded NAK
- Minimal generating sets

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. 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.

3.13. **Finiteness theorem for invariant rings: Lecture Notes §2.2, §2.3.**

Key topics:
- Hilbert's finiteness theorem and its proof
- Structure theorem for Noetherian graded rings
- Direct summands

Our goal is to prove the following Theorem, which was the main theorem in Hilbert's 1890 paper that is considered by many to be the starting point of Commutative Algebra.

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 automorphisms. Then the invariant ring R^G is algebra-finite over K.

The theorem has two main ingredients that are interesting in their own right:

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.

To use apply these, the following will obviously be relevant:

LEMMA: In the setting of Hilbert's finiteness Theorem,
(1) R^G is $\mathbb{N}$-graded with $(R^G)_0 = K$.
(2) R^G is a direct summand of R.

3.14. **Rees rings and Artin-Rees.**

Key topics:
- Rees ring of an ideal
- Associated graded ring of an ideal
- 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

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

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 $\operatorname{gr}_I(R)$ 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[17] $c \geq 0$ such that for all $n \geq c$, we have $I^n M \cap N \subseteq I^{n-c}N$.

4.15. **Noether normalization: Lecture Notes §7.3.**

Key topics:
- Noether normalization
- Zariski's Lemma
- Useful variants on Noether normalization

NOETHER NORMALIZATION: Let K be a field, and R be a finitely-generated K-algebra. Then there exists a finite[18] set of elements $f_1, \dots, f_m \in R$ that are algebraically independent over K such that $K[f_1, \dots, f_m] \subseteq R$ is module-finite; equivalently, there is a module-finite injective K-algebra map from a polynomial ring $K[X_1, \dots, X_m] \hookrightarrow R$. Such a ring S is called a **Noether normalization** for R.

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

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

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

USEFUL VARIATIONS ON NOETHER NORMALIZATION:

- NN FOR DOMAINS: Let $A \subseteq R$ be a module-finite inclusion of domains[19]. Then there exists $a \in A \smallsetminus 0$ and $f_1, \dots, f_m \in R[1/a]$ that are algebraically independent over $A[1/a]$ such that $A[1/a][f_1, \dots, f_m] \subseteq R[1/a]$ is module-finite.
- GRADED NN: Let K be an infinite field, and R be a standard graded K-algebra. Then there exist algebraically independent elements $L_1, \dots, L_m \in R_1$ such that $K[L_1, \dots, L_m] \subseteq R$ is module-finite.
- NN FOR POWER SERIES: Let K be an infinite field, and $R = K[\![X_1, \dots, X_n]\!]/I$. Then there exists a module-finite injection $K[\![Y_1, \dots, Y_m]\!] \hookrightarrow R$ for some power series ring in m variables.

4.16. **Nullstellensatz: Lecture Notes §4.3.**

Key topics:

- Zero-set of an ideal
- Nullstellensatz
- Maximal ideals in polynomial rings over algebraically closed fields

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 $\alpha = (a_1 \ldots, a_n) \in K^n$.

4.17. **Strong Nullstellensatz: Lecture Notes §4.3.**

Key topics:

- Strong Nullstellensatz
- Correspondence between radical ideals and subvarieties

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. Then f vanishes at every point of $\mathcal{Z}(I)$ 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

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

4.18. **Spectrum of a ring: Lecture Notes §3.2.**

Key topics:

- Spectrum of a ring as a set
- Zariski topology on $\mathrm{Spec}(R)$
- Properties of $VI(I)$ and $D(I)$
- Induced map on Spec

DEFINITION: Let R be a ring, and $I \subseteq R$ a subset 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) $I \subseteq \mathfrak{p} \iff \sqrt{I} \subseteq \mathfrak{p}$

4.19. **Spectrum and radical ideals: Lecture Notes §3.2.**

Key topics:

- Correspondence between radical ideals and closed subsets
- Multiplicatively closed subsets
- Minimal primes

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 $\mathfrak{p} \cap W = \varnothing$.

5.20. **Local rings and NAK: Lecture Notes §5.1.**

Key topics:
- Definitions of local ring
- General NAK
- Local NAK
- Minimal generating sets

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.

Note: Any of the four NAK statements above would generally be referred to as NAK or Nakayama's Lemma. The "General" vs "local" and the numbers are just there for our own convenience to reference.

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.

5.21. **Localization of rings: Lecture Notes §5.2.**

Key topics:

- Localization of a ring
- The key localizations R_f, $R_{\mathfrak{p}}$, and the total quotient ring.
- Correspondence between primes in localizations and primes in the original ring.

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[20], 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 $W^{-1}I := \left\{\dfrac{a}{w} \in W^{-1}R \mid a \in I\right\}$.

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 $\mathfrak{p} \cap W = \varnothing$, $W^{-1}\mathfrak{p}$ is prime.
(5) The map $\mathrm{Spec}(W^{-1}R) \to \mathrm{Spec}(R)$ is injective with image $\{\mathfrak{p} \in \mathrm{Spec}(R) \mid \mathfrak{p} \cap W = \varnothing\}$.

[20] If f is nilpotent, $0 \in \{1, f, f^2, \dots\}$ so $R_f = 0$.

5.22. **Localization of modules: Lecture Notes §5.2.**

Key topics:
- Localization of a module
- Localization & subs and quotients
- Spectrum of localization & quotient

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[21] 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

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

[21] If $0 \in W$, then $W^{-1}R$ is zero, which is not a ring; $W^{-1}M$ is also zero.

5.23. **Local Properties: Lecture Notes §5.2, §6.1.**

Key topics:
- Preserved by localization
- Local property
- Support of a module

DEFINITION: Let $\mathcal{P}$ be a property[22] of a ring. We say that

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

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

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

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

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.

The point is that many properties are local properties, and we can reduce many statements to the case where R is a local ring. In this setting, we have extra tools, like NAK.

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

$$\operatorname{Supp}_R(M) := \{\mathfrak{p} \in \operatorname{Spec}(R) \mid M_{\mathfrak{p}} \neq 0\}.$$

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

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

6. Decompositions of ideals and modules

6.24. **Minimal primes: Lecture Notes §6.1.**

Key topics:
- Minimal primes in Noetherian rings
- Minimal primes and radical ideals

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 $\operatorname{Min}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_t\}$.

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.

6.25. **Associated primes: Lecture Notes §6.2.**

Key topics:

- Associated primes and witnesses
- Associated primes and Noetherian rings
- Associated primes and zerodivisors
- Associated primes and localization

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 $\operatorname{Min}(I) \subseteq \operatorname{Ass}_R(R/I)$.

6.26. **Associated primes: Lecture Notes §6.2, §3.3.**

Key topics:
- Prime filtrations
- Finiteness of associated primes
- Prime avoidance

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 $Im = 0$.

6.27. **Primary decomposition: Lecture Notes §6.3.**

Key topics:

- Primary ideals
- Primary ideals vs prime ideals
- Irreducible ideals vs prime ideals
- Primary decompositions
- Existence of primary decompositions

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.

6.28. **Primary decomposition and uniqueness: Lecture Notes §6.3.**

Key topics:

- Minimal primary decompositions
- Uniqueness theorems for primary decomposition
- Primary decomposition and associated primes
- Minimal components in 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

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

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) $\operatorname{Ass}_R\left(R/\bigcap_{i=1}^t I_i\right) \subseteq \bigcup_{i=1}^t \operatorname{Ass}_R(R/I_i)$.