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.

- 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

1.1. **Rings: Lecture Notes §0.1.**

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

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

1.2. **Ideals: Lecture Notes §0.1.**

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 $\mathbb{X}\mathbb{Y} - \mathbb{Y}\mathbb{X}$. 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 $1 \leq i, j \leq n$.

Key topics:

- Generating sets of algebras
- Presentation of an algebra

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

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 $n = 3$.

Key topics:

- Accessing M2
- Defining rings, ideals, maps

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

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.

Key topics:

- Generating set of a module
- Presentation of a module

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

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.

Key topics:

- Matrices and linear combinations
- The adjoint trick
- Ideals of minors

1.5. **Determinants.**

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

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

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

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 $n = 1$?

Key topics:

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

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

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 $r = ua_1 \cdots a_n$