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.** Grifo §0.1; Atyiah-MacDonald §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 $A[X_1, \dots, X_n]$, which is the same as the polynomial ring in one variable X_n with coefficients in $A[X_1, \dots, X_{n-1}]$. 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

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

[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: Ket 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 $i\in\{1,\dots,n-1\}$, 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.** Grifo §0.1; Atyiah-MacDonald §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 $\phi^{-1}(J) := \{r \in R \mid \phi(r) \in J\}$ 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 $A[X_1, \dots, X_n]$ by thinking of it as a polynomial ring in one variable X_n with coefficients in $A[X_1, \dots, X_{n-1}]$.

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 $\underline{\mathrm{X}} = [X_{i,j}]_{1 \leq i,j \leq n}$ and $\underline{\mathrm{Y}} = [Y_{i,j}]_{1 \leq i,j \leq n}$ be two $n \times n$ matrices of indeterminates, and $R = K[\underline{\mathrm{X}}, \underline{\mathrm{Y}}]$ be a polynomial ring in $2n^2$ variables. Let I be ideal generated by the entries[4] of the commutator matrix $\underline{\mathrm{X}}\underline{\mathrm{Y}} - \underline{\mathrm{Y}}\underline{\mathrm{X}}$. 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 $1 \leq i, j \leq n$.

1.3. **Algebras.** Grifo §1.2; Aityah-MacDonald §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 $T = A[X_1, \dots, X_n]$ be a polynomial ring. For any A-algebra R, and any collection of elements $r_1, \dots, r_n \in R$, 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[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 $A[r_1, \dots, r_n]$ is the image of the A-algebra homomorphism $\alpha : A[X_1, \dots, X_n] \to R$ 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 $r_1, \dots, r_n \in R$. The ideal of **A-algebraic relations** on $r_1, \dots, r_n$ is the set of polynomials $f(X_1, \dots, X_n) \in A[X_1, \dots, X_n]$ such that $f(r_1, \dots, r_n) = 0$ in R. Equivalently, the ideal of A-algebraic relations is the kernel of the homomorphism $\alpha : A[X_1, \dots, X_n] \to R$ 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 $r_1, \dots, r_n$ of R as an A-algebra and a set of generators $f_1, \dots, f_m \in A[X_1, \dots, X_n]$ for the ideal of A-algebraic relations on $r_1, \dots, r_n$. We call $f_1, \dots, f_m$ a set of **defining relations** for R as an A-algebra.

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

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 $R = K[X_1, \dots, X_n]$ be a polynomial ring over K. Let $f_1, \dots, f_n \in R$. Then

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

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

1.m Macaulay2 Introduction. Grifo §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=(X^2,X*Y)` or `J=(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.