Commutative Algebra: G0A82a

Lael John

March 15, 2023

Preface

These notes for the course on commutative algebra are to serve as a reference point for all future work in algebraic geometry, and the larger realm of algebra in general. From what I can gather, we begin with a basic overview of ring theory, and then proceed to study modules and tensor products, before finally arriving at an introduction to category theory.

13th March 2023

After having finished one semester of study in commutative algebra, these notes must take up a larger mandate. Commutative Algebra as a subject serves as the basis for understanding rings and their actions on groups (much like groups act on sets). These newly constructed modules give rise to much more "concrete" structures (still very much in the realm of abstraction). Proceeding further into this jungle of theory, localisations appear as a way of formally defining the existence of rational numbers as being the multiplicative extension of the integers, and then extending that conception to the modules previously encountered. The penultimate stage of this journey deals with understanding the importance of tensor products, their existence and use, before finally arriving at the land of category theory: where we go "beyond" abstract algebra, and take a peek behind the curtain of almost all mathematics. (or rather, the mathematics that I have encountered so far.)

Contents

Chapter 1

Rings

We begin by going over what we already know about rings, and use this knowledge as a springboard to dive into other complex (both in terms of difficulty and in the regular mathematical sense) algebraic structures.

1.1 Definitions

Definition. A *ring* is an algebraic structure $(R, +, \bullet)$, where under the operation $+, (R, +)$ forms an abelian group, and under the operation $\bullet, (R, \bullet)$ forms a semigroup (only closed and associative).

Remark. Here we call the ring *commutative*, if the $\bullet$ operation is abelian. Similarly we can also talk about the existence of a *unity* in the ring for that same operation.

NOTE: The only ring where the unity is not distinct from the identity (used to denote additive identity) is the 0 ring, or the ring $(\{0\}, +, .)$. This ring is generally treated as an edge case, even though trivially, it is a field (a commutative division ring).

For most rings that we talk about in the following sections, it is assumed that they are commutative (otherwise the course name would be redundant, and that they all have a unity.)

Definition. A *ring homomorphism* $f : R \to R$ is a mapping from one ring to another satisfying the following properties

1. $f(x+y) = f(x) + f(y)$, which basically means that the images in the target ring share the same structure under addition.

2. $f(xy) = f(x)f(y)$, again, meaning that the images in the target share the same structure under multiplication.

3. Finally, $f(1_R) = 1_S$. The unity from one ring, under a homomorphism, must be mapped to the unity in the other.

Remark. A subring is a subset of a ring that has a ring structure (closed under addition and multiplication, identity and unity, commutativity, and additive inverses) with respect to the parent operations. A homomorphism (injective) exists between such a subring and its parent. Homomorphisms can be treated like a special class of functions, and thus their composition is similar to the composition of functions, with the additional restrictions preserving their homomorphism-ness.

Definition. An *ideal* I of a ring R is a subring of R that is also has the following property, namely that $RI \subset I$ or equivalently,

$$\forall r \in R, i \in I, ri \in I$$

This is akin to saying an ideal "absorbs" the entire ring.

With this sort of substructure, we can then begin to talk about R/I or the quotient ring, i.e. $\{x + I | x \in R\}$ with operations of $\oplus, \odot$ defined slightly differently on this ring. This allows us to view the ring as two kinds of structure, both the regular, and a certain meta-ring structure, as larger sets (or cosets in this case) also can be used to represent elements in the quotient ring.
Thus, given an ideal a quotient ring generated by it, one can find a canonical homomorphism $\pi : R \to R/I, \pi(x) \mapsto x + I$.

Let me be clear here, whenever one uses the word canonical, it simply means "natural" or "obvious", and most mathematics professors/textbooks don't seem to explain this clearly enough/explicitly enough to students. If something is canonical, but doesn't appear obvious, then it might be a good idea to check your understanding of the underlying concept. (Very rarely is it the case that such a function appears out of thin air to confuse a student.)

Thoughts. Consider a ring R and an ideal I. Considering the set of ideals in R containing I, they are also ideals, say $\{I_a\}_{a\in A}$. Also now considering the set of ideals in the quotient ring R/I, we see that they are subrings such that $(x+I)\mathcal{I} \subset \mathcal{I}$. This ends up leading to the correspondence theorem for rings (according to Rotman). We are able to find a bijection between the ideals in R containing I, and the ideals in R/I

Definition. When we talk about a ring homomorphism (ring map in future), we can think about the elements in the domain that map to the identity in the target, i.e. $\{x \in R | f(x) = 0\}$. This set is so important in our study, we term it ker F or the *kernel* of f, denoted by $f^{-1}(0)$. In a similar vein, the image of f, denoted im $f = f(R)$

Thoughts. Now when we consider a ring map, the kernel of f is an ideal of the domain ring, (trivial to prove). However, when we consider the image of the map (in R_2) then we cannot directly say that it is an ideal, merely that it is a subring (because it does map all of R_1's structure into R_2). Now that we have those two observations, when thinking about the quotient ring of $R_1/\ker f = R_1/K$, we know that all the elements are of the form $r + K$. This new quotient ring is apparently isomorphic to the image of f. Which should be easy enough to see, a well defined function $\phi : R_1/K \to \text{im} f$ where each element in the quotient ring is mapped to its corresponding image. i.e. $\phi(r + K) = f(r)$. Now clearly we can see that ϕ is a homomorphism, and it remains to be proved as to whether it is a bijection (which it clearly is, with a bit of definition chasing). Thus we gain an understanding of the first ring isomorphism theorem.

Definition. Pivoting slightly, we define a *zero-divisor* in R to be a non-zero element such that, when operated upon with another non-zero element, it results in the identity. $xy = 0; x, y \neq 0$. (both are zero divisors of each other in this example). If a ring has no zero divisors, it is called an *Integral domain.* A related term *nilpotent*, refers to an element $x \in R$ such that $\exists\, n \in \mathbb{N}; x^n = 0$. Finally, units in R are those elements that have inverses.

Thoughts. A nilpotent element x is always going to be a zero divisor (think about breaking down $x^n = x^{n-1}x$). The converse though, is not always true. The nilpotents of a ring are also closed under multiplication (taking the required n to be the LCM of the corresponding "elementary" exponenets.) The units of a ring behave even better, forming an abelian group $(R^\times)$ with

respect to the multiplication operation (the shoes-and-socks property plays a role here). How do nilpotents and units combine? If $x \in R^\times$, and y nilpotent, is it possible to find an inverse for $x + y$, or is this resultant element nilpotent?. Clearly it is not nilpotent (for every value of n, and by the binomial expansion, there is always a non-zero term).

We now discuss the types of ideals, and see where each of those definitions leads us in our understanding of rings.

Definition. A *principal ideal*, is one that can be generated by a single element within it. $I \subset R; I =< x >, x \in R$. (Very clearly we can see that R itself is a principal ideal, generated by 1.)

Proposition 1.1.1. *The folowing are equivalent*

1. *R is a field*
2. *R has only the trivial ideals*
3. *$\forall f : R \to R'$, f is either injective or im $f = 0$.*

Proof. We go from 1 to 2, 2 to 3 and then 3 to 1. If we assume R is a field, then we can immediately see that it contains the ideals generated by 1 and 0. Now for any other ideal that could possibly exist (say I), there is at least one non-zero, non-unity element in it. BUT because R is a field, when multiplying with elements from R, since I is an ideal we get $1 \in I \implies I = R$.
IF we assume R has only trivial ideals, and consider a ring map to R', then since ker f needs to be an ideal, thus it must be either $< 0 >$ or $< 1 >$. But if it is the former, then it only maps the zero of one ring to the zero in the other, hence the function is injective (characterisation). If the latter, then all elements are mapped to the zero of the other ring.
Finally, assume that f maps $R \to R' \neq \emptyset$. This takes care of the situation where ker $f = R$. Since f is injective, assume that there is a non-unit element $x \in R$. This element generates an ideal $(x) \subset R$, which is non-trivial. Now seeing f as a particular homomorphism between R and $R'/(x)$, since it must be injective, ker $f = (x)$ must equal 0. Thus $x = 0$, and we are done, because the only non-unit is 0 □

Definition. A *prime* ideal in R is one such that for any product of 2 elements that lies within the ideal, one of them must be originally part of the ideal. (similar to how we define prime numbers dividing products)

Definition. A *maximal* ideal is one which does not have any ideal larger than it, other than the ring itself.

Example 1.1. Here, a classic example. if K is a field, and $K[x_1, x_2 \dots x_n]$ the ring of polynomials generated, then $(x_1 - a_1)(x_2 - a_2) \dots (x_n - a_n)$ generates a maximal ideal.

Proposition 1.1.2. *A ring map preserves the property of primeness of ideals, but not the property of maximalness.*

Remark. The proof that every ring has at least 1 maximal ideal stems from using Zorn's lemma, which is as follows: Given any non-empty partially ordered set such that every chain has an upper bound, such a set is guaranteed to have maximal element.

We embark on our last two definitions:

Definition. R is a *local* ring, if it has a unique maximal ideal. In particular, if we consider such a local ring, then the quotient ring generated by such a maximal ideal is called the *residue field*

1.2 Operations on Ideals

. Now that we've built up the groundwork and background regarding rings and their ideals, we consider the operations possible when dealing with two or more ideals. This section should be relatively short, but may cover some interesting edge cases.

Definition. The *sum* of two ideals is defined to be the resulting set of all the sums of elements within each. As expected, such a sum is also guaranteed to be an ideal. This ideal is trivially also the smallest one containing the two component ideals. In fact, that is true for all finite sums. However once we deal with infinite families of ideals (yes such exist/must be taken into account) we define the sume $\sum_{a \in A} I_a$ as $\sum_{a \in A} x_a$ where finitely many x_a's are non-zero.

Trivially, intersection is also an operation on ideals that results in an ideal (both in the finite case, and infinite case).

Definition. We consider the *product* of two ideals to be the set **generated** by all the individual products formed pairwise between the two. Naturally, this set is also an ideal (Think about it for a minute.) This definition of a product can be used to think about the n-th power of an ideal, (for a positive integer n). This is then the set generated by all the pairwise multiplications of elements in the ideal. (consider this like a $\binom{n}{2}$ set of generators.)

Definition. Two ideals are *coprime* if their sum is the ring itself.

Remark. If I, J coprime, then $I \cap J = (I+J)(I \cap J) = I(I+J) \cap J(I+J) \subset IJ$

Now in building up all this theory, as an interesting side note, we can prove the Chinese remainder theorem (which states that given a set of congruences 3 or more if I remember correctly,$x \cong a_i \mathrm{mod} n_i$ each saying then there existed a unique solution mod $n_1 n_2 \ldots$, where each n_i is pairwise coprime). Our proof hinges on this co-prime assumption, constructing a ring map between the ring and n quotient rings, each modulo ideals that taken pairwise are coprime. We finally move on to our last two operations,

Definition. The *ideal quotient* is defined as being

$$(I : J) = \{x \in R | xJ \subset I\}$$

. (confusing, requires some thought.) In particular if we take the quotient $(0 : J)$, that is the same as the annihilator of J.

Definition. Let R be a ring and I an ideal. Then the *radical* of I, denoted by $\sqrt{I} = \{x \in R | x^n \in I, n \in \mathbb{N}\}$. A radical ideal therefore, is an ideal I, where $I = \sqrt{I}$. (Note, usually the radical is a superset of the ideal.)

Proposition 1.2.1. *If R is a ring, and I an ideal, then $\sqrt{I}$ is a radical ideal.*

Proof. We first prove that $\sqrt{I}$ is an ideal, and then go on to show that it is radical. Let $x \in \sqrt{I}, r \in R$. Now we know that $\exists m \in \mathbb{N}$ such that $x^m \in I$. Now consider $r^m x^m \in I \iff (rx)^m \in I$ (we are dealing with commutative rings). Thus $rx \in \sqrt{I}$. Now to show $\sqrt{I}$ is closed under addition. let $x, y \in \sqrt{I}$, and thus there are 2 different m, n such that $x^m, y^n \in I$. Then we can also see that if we consider $(x+y)^{m+n}$, we find it to be an element of I. Thus the sum of elements in the radical of an ideal exists in the radical. Now to show that such an ideal is in fact, a radical ideal, consider elements

in $\sqrt{I}$. We look for all the elements in R such that one of their powers is in $\sqrt{I}$. But then that is precisely the definition of $\sqrt{I}$. Thus the readical of an ideal is a radical ideal. □

Definition. The *nilradical* of R is the the radical corresponding to $\sqrt{0}$.

One proposition that we can consider is that the radical of an ideal is simply the intersection of all the prime ideals that contain it. In particular, the nilradical seems to be the intersection of all the prime ideals of the ring itself.

Definition. The *Jacobson radical* of a ring, is the intersection of all the maximal ideals of the ring. (since all maximal ideals are prime, the proof follows from the previous proposition.)

1.3 Factorisation

We begin this section with a basic definition of divisibility, and then go on to discuss Euclidean domains, principal ideal domains and unique factorisation domains.

Definition. When we consider two elements of R, x, y, we say that $x|y$ read x divides y, whenever $\exists u \in R$ s.t $y = ux$.

Remark. x, y are termed associates if $y|x$ and $x|y$. If suppose they are associates in an integral domain, R, then there must exist a unit in R such that $x = uy$ or $y = ux$. Since u^{-1} also exists, this makes sense.

Definition. We term an element of a ring R to be irreducible, if for $x \in R, x$ not a unit, $x = uy$ where either of u, y is a unit.

Definition. Finally, an element $x \in R$ is **prime** if $x|yz \implies x|y$ or $x|z$. Here we can say that x when non-zero generates a non-zero prime ideal.

Definition. When we talk about *principal ideal domains*, we consider R an integral domain where every ideal I can be generated by a single element it contains.

If we consider $p \in R$ a PID to be irreducible, that means that it is not zero or a unit, and its factorisation into two different element involves one of them

being a unit. Therefore when we consider the ideal generated by p, we can see that at once, such an ideal is maximal (because R a PID, when you consider a ring containing $< p >$, that ring must necessarily also be generated by p). Furthermore, consider $q, r \in R$, such that $p|qr$. (COMPLETE LATER)

Definition. R is said to be a Euclidean domain when it is an integral domain, combined with a functiond $\phi : R \{0\} \to \mathbb{Z}^+$ known as a degree function, with the following properties

1. $x, y \neq 0 \in R, x|y \implies \phi(x) \leq \phi(y)$
2. $x, y \neq 0 \in R, \exists q \neq 0, r \in R$ such that $x = qy + r$ where $\phi(r) < \phi(y)$ or $r = 0$.

It follows very conventiently that every Euclidean Domain is a Principal Ideal Domain.

Definition. R an integral domain is called a *Unique Factorisation Domain*, if for every non-zero, non-unit in R, it $x = up_1p_2 \dots p_n$ for each p_i irreducible in R and u a unit.

Remark. As a remark, it can be clear to see that every euclidean domain is a principal ideal domain, and every principal ideal domain is a unique factorisation domain.

As a final proposition to this section, (and an apology to my future self for not completing the proofs right now,)

Proposition 1.3.1. *If R is a unique factorisation domain, then the polynomial ring generated by R is also one, and as a corollary, $R[x_1, x_2, \dots x_n]$ is also a unique factorisation domain.*

Chapter 2

Modules

Chapter 3

Finiteness and Order in Modules

Chapter 4

Linear Algebra in the context of Modules

Chapter 5

Localisation

Chapter 6

Tensor Products

Chapter 7

Category Theory