DRAFT NOTES 0.085: SOLUTIONS TO PROBLEMS IN COMMUTATIVE ALGEBRA

LEAN TOLENTINO: TOLENTIJ@TCD.IE

1. Prelimanaries: Motivation and References

The central motivation behind our study of commutative algebra is to develop tools to handle algebraic geometry. For example, of central importance is Hilbert's Nullstellensatz,

Theorem 1.1. If a field $\mathbb{K}$ is algebraically closed, then for any ideal I in $K[x_1, ..., x_n]$, we have $I(Z(I)) = \sqrt{I}$

Here Z is a variety, $Z(I) = \{(a_1, ..., a_n) \in \mathbb{K}^n | f(a_1, ..., a_n) = 0 \, \forall f \in I\}$, and $\sqrt{I}$ refers to the radical of I, that is $\{a \in A | a^n \in I \, \exists n > 0\}$. You might notice that this appears to be a generalisation of the fundamental theorem of Algebra - in fact if we consider the field $\mathbb{K} = \mathbb{C}$ it is just the fundamental theorem of algebra for arbitrary polynomials. This is therefore a very useful tool, recall for example, the circle is the zero-set of $x^2 + y^2 - 1$, or the hyperboloid is the zero-set of $x^2 + y^2 - z^2 - 1$. In Algebraic geometry, we are particularly fascinated with the *loci* (that is the zero-sets of polynomials). There are many more tools that will be formed from our future study, but hopefully, this short example sets some inspiration.

More will be explained in my 'comments on Mozgovoy's Lecture Notes', but worth keeping in mind, for now, is that in commutative algebra, we often consider two types of rings: co-ordinate rings, and rings of algebraic integers in number fields. Throughout these notes, I will do my best to intervene with geometric examples, or better motivation for the given examples when possible, and hopefully, then the precise reasoning for each aspect of this course will reveal itself to you over time.

There are a total of six key texts that I have read (parts of, or all of) as part of writing these complementary notes, they are provided in order of familiarity with them (earlier = most familiar):
Atiyah and Macdonald: Introduction to commutative algebra
Eisenbud: Commutative algebra
Bourbaki: Commutative algebra
Matsumura: Commutative algebra
Cox, Little, O'Shea: Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra
Liu: Algebraic Geometry and Arithmetic Curves

Date: March 4, 2024.

2. Solutions to Mozgovoy's Exercises

Exercise 1.5. Assume p = (x) is in some (y) = m, then $x^n = y^m \; \exists m, n...$

Remark. I also have solved all the exercises in class, but I am positive at least some of these are going to be homework, and I'd like to avoid being disciplined over that! If you need advice just email me. I also have typed up notes on Mozgovoy's but these notes are personalised, and really only useful except for me explaining things, I might try to elaborate on them if I have time.

3. The Big Bag of Commutative Algebra Tricks

Remark 3.1. Maximal Ideals
1: When you try to show existence of some type of maximal ideal, the first thing that jumps to mind should be Zorn's Lemma

Remark 3.2. Jacobson Radical
1: When trying to show something is in the Jacobson radical it is often handy to consider the theorem: $a \in \mathcal{R}(A) \Leftrightarrow 1 - ab$ is invertible for arbitrary b. We find it is sometimes nicer to show the latter. In other cases this theorem is used in it's own right to derive a property, after showing something is in $\mathcal{R}(A)$

Remark 3.3. Local Rings
1: When trying to show there is a unique maximal ideal it is sometimes useful to think about the invertible, and non-invertible elements.

Remark 3.4. Radicals
1: When trying to get a specific minimum exponent on a bivariate polynomial, binomial expansion is often handy - and this is sometime used in elementary questions about radicals

Remark 3.5. Noetherian Modules
1: It is usually easiest to work with the ascending chain property, and in a close second, the fact that the module is finitely generated.

4. Solutions To Mozgovoy's Bonus Problems

5. Solutions To Problems in Atiyah's Introduction To Commutative Algebra

5.1. Chapter 1.

Exercise 1.1. On first glance one should hopefully see 2 options: either we prove this directly or equivalently show that $(1 + x) = A = (1) \Leftrightarrow 1 + x \in A^x$. It turns out, both ways are nice, though the first is hardly anything instructive. Proving the first we use that $(1 + x)(1 + (-1)^1x^1 + ... + (-1)^{n-1}x^{n-1}) = 1$, it is boring... Let us now use the second method: $x \in \mathcal{R} \Rightarrow x \in N(A) \subseteq J(A)$... Remark 1.22 of Sergey Mozgovoy's notes, and then: $\Rightarrow x \in J(A) \Rightarrow (1 + x) = A$... Lemma 1.24 of Sergey Mozgovoy's notes

Exercise 1.2. For the base case: r = 0 as $f \cdot f^{-1} = 1$, we have that $a_n b_m = 0$. Let us now consider arbitrary r ensures that $a_n^r b_{m-r+1} = 0$, it must then be that the coefficient of x^{m-n+r} in $f \cdot f^{-1}$ vanishes when $m - n + r \geq r$, that is to say: $a_n b_{m-r} + a_{n-1} b_{m-r+1} + ... = 0$, and multiplying with a_n^r, we have then that $a_n^{r+1} b_{m+r} + a_n^r a_{n-1} b_{m-r+1} + ... = 0$, by the inductive hypothesis all other elements are killed off, and so $a_n^{r+1} b_{m-r} = 0$, setting $r = m$, we have that a_n is nilpotent. The ($\Leftarrow$) side is immediate by exercise 1., we use induction on n for the ($\Rightarrow$) side, we know that a_n is nilpotent, and it must therefore be that $a_n x^n$ is nilpotent, and hence via exercise 1: $f - a_n x^n$ is invertible as well, then by the induction hypothesis (that it holds for those of a degree less), a_0 is invertible, and $a_1, ..., a_{n-1}$ are all nilpotent.
ii ($\Leftarrow$) If we have n elements, then f is nilpotent of degree $n(m-1)$, where m is such that $a_i^m = 0 \, \forall i$. It is nilpotent because, to ensure we have every element has degree 1 at least, this requires f^1 clearly. To ensure degree 2 is essentially a combinatorial question, we just need to eliminate all possible degree 1 combinations (this will require putting it to the n-th power as the maximal combination is always when you just have all n elements multiplied together), so doing this just $m - 1$ times will be sufficient. ($\Rightarrow$) This follows by induction, when $n = 1$, it is quite immediate.$f - a_{N+1} x^{N+1}$ is nilpotent as well (as per ($\Leftarrow$) and the fact that the leading co-efficient must be nilpotent), and so invoking the induction hypothesis we have the $N + 1$ case.
iii We have that $fg = 0$ for some polynomial g, we pick g such that it's degree m is minimal. $a_n b_m = 0$ as we consider the leading co-efficients, so then $a_n g f = 0$, but $a_n g$ is of degree less than m - so no such minimal m can exist, so m must be equal to zero.
iv ($\Rightarrow$) $a_i b_j y$ can be generated by $a_i y$ or $b_j y$, we can then see that $(1) = (a_1 b_1, ... a_n b_m)$ which is a subset of $(a_1, ..., a_n)$ and $(b_1, ..., b_n)$. ($\Leftarrow$) The contrapositive follows by the same technique we used in the other direction. This is an extension of Gauss' Lemma (see Mozgovoy's FRM notes).

Exercise 1.4. This follows from $A[x]$ being a finitely generated algebra. (See theorem 5.26 in Mozgovoy's Notes). We provide an alternative proof using exercise 2: We have that $\mathcal{J} \supset \mathcal{R}$ (see Mozgovoy Remark 1.22), so we only need prove $\mathcal{R} \supset \mathcal{J}$. Assume $f(x) \in \mathcal{J}$, then $1 - f(x)g(x)$ is invertible, for all $g(x) \in A[x]$, let $g(x) = x$, i.e. $1 - f(x)x$ is a unit, and then by exercise 2.1 we can assume that $a_1, ... a_n$ are nilpotent. This means all the co-efficients of f are nilpotent, which means by exercise 2.2 we have that f itself is nilpotent.

Exercise 1.5. ($\Rightarrow$) $\sum_{i=1}^{\infty} \sum_{j=1}^{\infty} a_i b_j x^{i+j}$ - this direction should be clear. ($\Leftarrow$) The inverse can be derived by long-division (divide 1 by our polynomial, the only inverse we require is an inverse of a_0) - there are (I would assume) other ways to find this fact, but this is the most elementary.
ii No, consider the counter-example: $f = \sum_i a_i x^i$ s.t. for each i we have $a_i^i = 0$ and $j < i \Rightarrow a_i^j \neq 0$.
iii This follows as per proposition 1.9 in Atiyah, combined with 5.i. The intuition behind this is that in the context of 5.i one may naturally consider that proper ideals consist of non-invertibles. Proposition 1.9 is also a commonly used one, the identity $1 - r$ or $1 - xy$ is also commonly considered regarding rings.
v The mapping is a ring homomorphism, hence by lemma 1.14 (Mozgovoy) is prime

Exercise 1.6. I have still to solve this

Exercise 1.7. This is an exercise in Sergey's Notes, my solution is provided in the commentary

Exercise 1.8. This is just applying Zorn's lemma on decreasing chains rather than increasing chains (see Mozgovoy's proof of existence of maximal ideals)

Exercise 1.9. ($\Leftarrow$) Let us assume $x^m \in a, p_1, p_2, ... \Rightarrow x^m \in r(a)$. Let us assume $x^m \in r(a), p_1, p_2, ...$, so then $x^m x^n \in a$ by induction on n we have that $x^m \in r(a)$, so then $a = r(a)$. ($\Rightarrow$) Proposition 1.14 (Atiyah)

Exercise 1.10. ($i \Rightarrow ii$) If $x \notin p$, then the maximal ideal containing x is not p, which is equivalent to saying that the sky has fallen because the only maximal ideal is the prime ideal, so x is a unit, suppose x $\in p$, then as $p = \mathcal{R}$, $x \in \mathcal{R}$ i.e., x is nilpotent. ($ii \Rightarrow iii$) $A/\mathcal{R} = A/p$, where p is maximal by uniqueness ($iii \Rightarrow i$) the intersection of all prime ideals is an ideal, and it must be maximal because it gives us a field, so it is unique because there are no prime ideals containing it.

Exercise 1.11. $(x+1)^2 = x+1 \Rightarrow x = 0, \vee x+1 = 0 \Rightarrow 2x = 0$
ii Suppose $x \in m$, and $p \subseteq m$, we have $x^2 \in p$, i.e. $x \in p$. It is reasonable to see that the only two elements are $0, x$ - as $x_{p_1} - x_{p_2}$ is still a second-degree nilpotent. iii It is also reasonable for arbitrary $x \in A$, Ax is generally an ideal because by definition: $0, -a, ab \in A$, and also that $2xa_i - xa_i = xa_i \Rightarrow -xa_i \in Ax$.

Exercise 1.12. Consider $x(x-1) = 0$, if x or $x-1$ are units, x must be 0 or 1, as x is not a zero-divisor. So we assume x is not a unit, but then $x, x-1 \in m \Rightarrow 1 \in m \Rightarrow 1 \in m \Rightarrow m = A$, a contradiction.

Exercise 1.14. This is another application of zorn's lemma, we can check it's well-defined, it is not hard. Now if we assume $xy \in m_i$, $x, y \in m_i$, as they are zero-divisors, and $m_i \subseteq (m_i, x)$, which consists solely of zero-divisors, a contradiction.

Exercise 1.16. First: prime numbers, Second: irreducibles (only degree one polynomials, Third/Fourth: irreducibles

Chapter 2.

Exercise 2.1. Let us consider arbitrary, $x \otimes y \in (\mathbb{Z}/m\mathbb{Z}) \otimes_z (\mathbb{Z}/n\mathbb{Z})$. Since x, y are co-prime, we can apply Bezout's lemma for (d = 1), then we have $x \otimes y = am(x \otimes y) + bn(x \otimes y) = a(mx \otimes y) + b(x \otimes ny) = a(0 \otimes y) + b(x \otimes 0) = 0$, this is for all elements. So then: $(\mathbb{Z}/m\mathbb{Z}) \otimes_z (\mathbb{Z}/n\mathbb{Z}) = 0$

Remark 2.1. We can find a stronger result than Exercise 2.1: we find that, when $d = gcd(m,n)$, $\mathbb{Z}_n \bigotimes \mathbb{Z}_m = \mathbb{Z}_d$, consider problem 1 from HW 2. We can hence deduce: $(\mathbb{Z}/m\mathbb{Z}) \bigotimes_Z (\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}/((m\mathbb{Z})(\mathbb{Z}_n)) = \mathbb{Z}/n\mathbb{Z}/((m\mathbb{Z})(\mathbb{Z}/n\mathbb{Z})) = \mathbb{Z}/n\mathbb{Z}/(((m\mathbb{Z})\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}/((m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z}) = \mathbb{Z}/((m\mathbb{Z} + n\mathbb{Z})) = \mathbb{Z}/d\mathbb{Z}$. The above seems convoluted - it is quite simple really, most of it is manipulating notation. All that is necessary to know is that $I\frac{M}{N} = \frac{IM+IN}{N}$ via the homomorphism theorem (take the mapping: $f : [im]_N \mapsto im + in$), you could perhaps just think for a second about what the definition of the two are in contrast. Regardless, this is the non-trivial part.

Exercise 2.2. Tensoring what we are given we have $a \bigotimes_A M \to A \bigotimes_A M \to (A/a) \bigotimes_A M \to 0$, and as per a Lemma from Mozgovoy's lectures (not in his notes)/Result 3 in Exact Sequences from Atiyah Chapter 2 (Appendices: 0.1) of these notes, we have that $A \bigotimes_A M/a \bigotimes_A M \cong (A/a) \bigotimes_A M \Rightarrow$ (Lemma 2.17 2 in Mozgovoy's notes) $M/a \bigotimes_A M \cong (A/a) \bigotimes_A M \Rightarrow$ (As a corollary of that lemma) $M/aM \cong (A/a) \bigotimes_A M$

Exercise 2.3. Firstly we show: $k \bigotimes_A M \cong M/(m) = 0 \Rightarrow M = (m) \Rightarrow M = 0$ (Nakayama's Lemma).
$M \bigotimes_A N = 0 \Rightarrow k \bigotimes_A (M \bigotimes_A N) = 0 \Rightarrow (k \bigotimes_A M) \bigotimes_k (k \bigotimes_A N) = 0$, but $k \bigotimes_A M$ and $k \bigotimes_A N$ are both vector spaces over the field k, i.e.
$dim_k((k \bigotimes_A M) \bigotimes_k (k \bigotimes_A N)) = dim_k(k \bigotimes_A M)(k \bigotimes_A N)$, $\Rightarrow k \bigotimes_A M = 0$ or $k \bigotimes_A N = 0$, so then $M = 0$ or $N = 0$

6. Solutions To Problems to Eisenbud's: Commutative Algebra With A View to Algebraic Geometry

6.1. **Chapter 1.**

Exercise 1.1. ($1 \Rightarrow 2 \Rightarrow 1$) This is in Mozgovoy's notes (Lemma 3.3)
($2 \Rightarrow 3$) Suppose we have a set of submodules of M we call S. We assume that S contains no elements that are maximal under conclusion, that means $\forall M_i \exists M_{i+1} \supset M_i$, that allows us to create a non-terminating ascending chain - this is a contradiction to the assumption our module is Noetherian.
($3 \Rightarrow 2$) Every ascending chain of submodules of M generates a set wherein which maximal elements exist with respect to inclusion - a chain is totally ordered, so the the chain terminates at these maximal "elements" (they equal each other)
($3 \Rightarrow 4$) Consider the chain generated by the submodules generated by each $f_1, ...f_i$. Eventually the chain terminates.
($4 \Rightarrow 3$) Every ascending chain of submodules can be expressed as a chain of generated submodules, eventually the sequence terminates.

Exercise 1.2. Mozgovoy proved this in class

Exercise 1.3. REMINDER: (**Proofread**)
(*A somewhat technical proof*)
($\Rightarrow$) If M is Noetherian, then M' is immediately noetherian. M/M' is also noetherian since there is an order-preserving correspondence between it, and modules in M containing M' (from Atiyah Chapter 2 - page 18, note that there's a typo. A non-typoed statement is available as Theorem 3.4 at https://mathstat.dal.ca/~yanghs/notes.php?name=Module), meaning we can associate a chain in M/M' with a chain in M that terminates.
($\Leftarrow$) Suppose that M is not Noetherian. Let us consider an ascending chain of modules $M_1, ...$ that does not terminate. We can then construct $M_1/M', ...,$ and $M_1 \cap M', ...$ which both terminate. Let us note then that $\forall i, \exists x \in M_{i+1}, x \notin M_i$. If $x \in M'$, this couldn't be the case, because M' is noetherian. Let us then assume that $x \in M_{i+1} \backslash M'$. We now note that $[x] \in M_{i+1}/M'$. So let us then assume $i > N$, where N is where the sequence (M_j/M') terminates. We have that

$M_{i+1}/M' \ni x = y+m, y \in M_N, m \in M'$. So then $M_{i+1} = M_N \cup N_1^* \cup L_1^*$[1], where N_1^*, L_1^* are chosen as arbitrary submodules of M', we have L_1^* (the extra M' submodule) from the scenario where $x \in M'$. We then have, $M_{i+2} = M_N \cup N_2^* \cup L_2^*, ...$, where $N_{i+1}^* \supseteq N_i^* \forall i$, and similarly for L. Since we had assumed that M' is Noetherian, the sequence of (N_i^*) must terminate at some J_1, and (L_i^*) at some J_2. We then find $M_i = M_{i-1} \forall i > \max J_1, J_2$. So our sequence actually terminates.
(*A rather simple proof*)
($\Leftarrow$) The same
($\Rightarrow$) We shall use the fact we have an order-preserving correspondence between $A \subseteq M$, s.t. $M' \subseteq A$, and modules of M/M'. We take an arbitrary ascending chain, and suppose $A_i \supset M' \exists i$, then what we require is immediate, since we have assumed an order-preserving correspondence, and $f^{-1}(A)_j/M'$ eventually terminates. Let us also note that $(A_1 \cap M') \leq M'$ is also Noetherian as a submodule of M'. So then we can apply the same trick on $(A_1 \cap M')$ instead of M'.

7. Further Resources For Learning Commutative Algebra

8. Appendices

Lemma 0.1. A sequence $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ is exact (at L, M, N) $\Leftrightarrow gf = 0$ and g induces an isomorphism $\underbrace{M/Imf}_{\cong M/L} \xrightarrow{\sim} N$

Proof of Claim: ($\Rightarrow$) N = Im(g) $\Rightarrow$ (By homomorphism theorem) $N = Im(g) \cong M/Ker(g)$, and by exactness $Im(f) = Ker(g) (\Rightarrow gf = 0) \Rightarrow N = M/Im(f)$ then, the other direction is similar $\square$

[1]Implicitly, I am using the fact that $y \in M_{i+1}, x \in M_{i+1} \Rightarrow m \in M_{i+1}$, which then allows for the manipulation: $(m) \cap M_{i+1} = N_1^*$, which must be a submodule of M_{i+1}, similar holds for L_1^*, which is why we have equality rather than just a subset