Notes on Atiyah-MacDonald

(Intro to Commutative Algebra)

Kat Watson

`https://pqcfox.dev`

Abstract

These notes are from late 2024, and are intended as a review of commutative algebra in preparation to cover more of the in-depth sections of Hartshorne. In these notes, I make arguments from the text as explicit as possible, even when they may be "obvious" in order to get additional practice–it's been a while since my undergrad. Exercise solutions are included, and are selected to cover the material as well as possible.

※ ※ ※

1. Rings and ideals

1.1. Prime and maximal ideals (page 3)

The claim is made that for a ring A with $\mathfrak{p}$ and $\mathfrak{m}$ ideals of A,

> $\mathfrak{p}$ is prime $\Leftrightarrow A/\mathfrak{p}$ is an integral domain;
> $\mathfrak{m}$ is maximal $\Leftrightarrow A/\mathfrak{m}$ is a field (by (1.1) and (1.2)).

Indeed, $A/\mathfrak{p}$ is a domain iff for all $x, y \in A$, $\overline{xy} = 0$ implies either $\overline{x} = 0$ or $\overline{y} = 0$. Since

$$\overline{xy} = 0 \Leftrightarrow xy \in \mathfrak{p}, \quad \overline{x} = 0 \Leftrightarrow x \in \mathfrak{p}, \quad \overline{y} = 0 \Leftrightarrow y \in \mathfrak{p}$$

we have that this is equivalent to $\mathfrak{p}$ being prime.

For the other claim, (1.2) states that $A/\mathfrak{m}$ is a field iff the only ideals in A are 0 and (1). By (1.1), there is a one-to-one order-preserving correspondence between the ideals of $A/\mathfrak{m}$ and the ideals of A containing $\mathfrak{m}$ sending $0, (1) \subseteq A/\mathfrak{m}$ to $\mathfrak{m}, (1) \subseteq A$ respectively. Thus, we have

$$\begin{aligned} A/\mathfrak{m} \text{ is a field} &\Leftrightarrow \text{the only ideals of } A/\mathfrak{m} \text{ are } 0 \text{ and } (1) \\ &\Leftrightarrow \text{the only ideals of } A \text{ containing } \mathfrak{m} \text{ are } \mathfrak{m} \text{ and } (1) \\ &\Leftrightarrow \mathfrak{m} \text{ is maximal.} \end{aligned}$$

1.2. Pullbacks of prime ideals (page 3)

The claim is also made that

> If $f : A \to B$ is a ring homomorphism and $\mathfrak{q}$ is a prime ideal in B, then $f^{-1}(q)$ is a prime ideal in A, for $A/f^{-1}(\mathfrak{q})$ is isomorphic to a subring of $B/\mathfrak{q}$ and hence has no zero-divisor $\neq 0$.

First, to construct this isomorphism, compose f with the quotient map $\pi : B \to B/\mathfrak{q}$ to get $\pi \circ f : A \to B/\mathfrak{q}$ and note that $\ker(\pi \circ f)$ is precisely $f^{-1}(\mathfrak{q})$, so that by the first isomorphism theorem, we have an injective map $\overline{\pi \circ f} : A/f^{-1}(\mathfrak{q}) \to B/\mathfrak{q}$. Since the image of any ring homomorphism is a subring of the codomain, this map makes $A/f^{-1}(\mathfrak{q})$ isomorphic to a subring of $B/\mathfrak{q}$ as desired.

1.3. Every non-zero ring has a maximal ideal (Proposition 1.3)

As part of the proof, it is claimed that for a chain $(\mathfrak{a}_\alpha)$ in Σ, $\mathfrak{a} := \cup_\alpha \mathfrak{a}_\alpha$ is an ideal. Indeed, take $x, y \in \mathfrak{a}$. We have that for some α and β, $x \in \mathfrak{a}_\alpha$ and $y \in \mathfrak{a}_\beta$. WLOG, assume $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$. Then $x, y \in \mathfrak{a}_\beta$, meaning $x + y \in \mathfrak{a}_\beta \subseteq \mathfrak{a}$.

Similarly, if $a \in A$ is a general element of A and $x \in \mathfrak{a}_\alpha$, then we have $ax \in \mathfrak{a}_\alpha \subseteq \mathfrak{a}$, so that $\mathfrak{a}$ is an ideal of A.

1.4. Every ideal is contained in a maximal ideal (Corollary 1.4)

In the proof of Corollary 1.4, the full argument is

> Apply (1.3) to $A/\mathfrak{a}$, bearing in mind (1.1). Alternatively, modify the proof of (1.3).

We expand on this: applying (1.3) to $A/\mathfrak{a}$, we get a maximal ideal of $A/\mathfrak{a}$, which by the correspondence in (1.1) corresponds to a maximal ideal of A containing $\mathfrak{a}$.

1.5. Criterion for a ring to be local (Proposition 1.6(ii))

The proof elides the detail that for any $x, y \in A$, if xy is a unit then x is a unit. This follows from definition: if xy is a unit, then there exists $z \in A$ such that $(xy)z = 1$, but then $x(yz) = 1$, meaning x is a unit.

1.6. Irreducible polynomials generate prime ideals (Example 1, page 4)

As an example of a prime ideal, page 4 gives

> $A = k[x_1, ..., x_n]$, k a field. Let $f \in A$ be an irreducible polynomial. By unique factorization, the ideal (f) is prime.

Making this explicit, assume that we have $g, h \in A$ such that $gh \in f$, i.e. $f \mid gh$. Then since f is irreducible, we have by unique factorization that either $f \mid g$ or $f \mid h$, i.e. $g \in (f)$ or $h \in (f)$, meaning (f) is prime.

1.7. Ideals of $\mathbb{Z}$ are all principal (Example 2, page 4)

As another example on page 4, there is a claim that

> Every ideal in $\mathbb{Z}$ is of the form (m) for some $m \geq 0$.

Indeed, take an arbitrary non-zero ideal $\mathfrak{a} \subseteq \mathbb{Z}$, and take the smallest positive element of $\mathfrak{a}$: denote this as m. Clearly $(m) \subseteq \mathfrak{a}$. Now, take any $n \in \mathfrak{a}$. By Bezout's identity, we have $\gcd(m, n) \in \mathfrak{a}$. Since $\gcd(m, n) \leq m$, but m is the smallest positive element of $\mathfrak{a}$, we have $\gcd(m, n) = m$, i.e. $m \mid n$. Thus $\mathfrak{a} \subseteq (m)$, and the two ideals are equal.

As implicitly noted in the text, a similar argument can be applied to show that $k[x]$ is a principal ideal domain, based on the Euclidean algorithm for univariate polynomials.

1.8. The modular law for ideals (page 6)

The following is stated as the closest approximate we have in general to $\cap$ and $+$ distributing over each other in a general ring:

$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ if $\mathfrak{a} \supseteq \mathfrak{b}$ or $\mathfrak{a} \supseteq \mathfrak{c}$

To see this, WLOG let $\mathfrak{a} \supseteq \mathfrak{b}$. We show each side of the desired equality contains the other.

$\subseteq$: By definition, we have $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{a}$, and since $\mathfrak{b} \subseteq \mathfrak{a}$, we have $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \subseteq \mathfrak{b} + \mathfrak{c} \subseteq \mathfrak{a} + \mathfrak{c}$. This means that any $x \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$ both lies in $\mathfrak{a}$ and can be written as $x = y + z$ for some $y \in \mathfrak{a}$ and some $z \in \mathfrak{c}$. But then, $z = x - y \in \mathfrak{a}$, meaning $z \in \mathfrak{a} \cap \mathfrak{c}$ and therefore

$$x = y + z \in \mathfrak{a} + \mathfrak{a} \cap \mathfrak{c} = \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}.$$

$\supseteq$: Any element $x \in \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ can be written as $x = y + z$ for $y \in \mathfrak{a} \cap \mathfrak{b}$ and z in $\mathfrak{a} \cap \mathfrak{c}$. Since $y, z \in \mathfrak{a}$, $x = y + z \in \mathfrak{a}$, and since $y \in \mathfrak{b}$ and $z \in \mathfrak{c}$, we have $x = y + z \in \mathfrak{b} + \mathfrak{c}$ as well, meaning $x \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$ as desired. $\square$

1.9. Ideals lying in the union of prime ideals (Proposition 1.11(i))

The part of the proof beginning with "...then for each i there exists $x_i \in \mathfrak{a}$ such that $x_i \notin \mathfrak{p}_j$ whenever $j \neq i$..." could use clarification. We paraphrase the argument below.

If $n > 1$ and the result is true for $n - 1$, assume the premise $\mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$ $(1 \leq i \leq n)$ and note that for each $1 \leq j \leq n$ we then have $\mathfrak{a} \not\subseteq \mathfrak{p}_i$ for $1 \leq i \leq n$, $i \neq j$.

Since our desired result holds for $n - 1$, this in turn implies $\mathfrak{a} \not\subseteq \bigcup_{1 \leq i \leq n;\, i \neq j} \mathfrak{p}_i$ for each such j, meaning that for each j we have some $x_j \notin \mathfrak{a}$ such that $x_j \notin \mathfrak{p}_k$ when $j \neq k$.

Now, if by chance we also have $x_j \notin \mathfrak{p}_j$ for some j, then $x_j \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$ meaning $\mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$, our desired result. Otherwise, i.e. if $x_j \in \mathfrak{p}_j$ for every j, then we consider

$$y = \sum_{i=1}^{n} x_1 x_2 \cdots \widehat{x_i} \cdots x_n$$

where the "hat" indicates the omission of x_i from the product, i.e. each summand is missing one of $\{x_1, x_2, \cdots x_n\}$. For each j, we note that all summands but one will contain x_j and thus lie in $\mathfrak{p}_j$. The remaining summand is a product of elements not in $\mathfrak{p}_j$ and thus by primality doesn't lie in $\mathfrak{p}_j$, meaning the whole sum doesn't lie in $\mathfrak{p}_j$. Since this argument applies for all j, we have $y \notin \bigcup_{i=1}^{n} \mathfrak{p}_i$, meaning that $\mathfrak{a} \not\subseteq \bigcup_{i=1}^{n} \mathfrak{p}_i$. $\square$

1.10. TODO: continue from Proposition 1.11(b).

1.11. End of chapter exercises

1.11.1. Exercise 1

Take $n > 0$ such that $x^n = 0$. Then $(1 + x)(1 - x + x^2 - x^3 + \cdots \pm x^{n-1}) = 1 \pm x^n = 1$. $\square$

1.11.2. Exercise 6

By Proposition 1.9, it suffices to show that for any $x \in A$, if $1 - xy$ is a unit for every $y \in A$, then x lies in the nilradical. Assume to a contraction that some such x is not in the nilradical. By the premise of the problem, (x) would then contain some non-zero idempotent e. Take y such that $e = xy$. Then $1 - xy = 1 - e$, which is idempotent: $(1 - e)^2 = 1 - 2e + e^2 = 1 - e$.

If $1 - e$ was a unit, then multiplying both sides of the previous equality by its inverse would give $1 - e = 1$, i.e. $e = 0$, contradicting our choice of e. $\Rightarrow\Leftarrow$ $\square$

1.11.3. Exercise 7

Fix an arbitrary prime ideal $\mathfrak{p} \subseteq A$, and take $x \in A - \mathfrak{p}$ with image $\overline{x} \in A/\mathfrak{p}$. Since $x^n = x$ for some $n > 1$, we have $(x^{n-1} - 1)x = 0$. Passing to the quotient, this gives $(\overline{x}^{n-1} - 1)\overline{x} = 0$.

Since $x \notin \mathfrak{p}$, we have $\overline{x} \neq 0$. Because $A/\mathfrak{p}$ is an integral domain, this means $\overline{x}^{n-1} - 1 = 0$, implying that $\overline{x}$ is a unit. As $x \in A - \mathfrak{p}$ was arbitrary, this means that any nonzero element of $A/\mathfrak{p}$ is a unit, i.e. $A/\mathfrak{p}$ is a field and thus $\mathfrak{p}$ is maximal. $\square$

1.11.4. Exercise 8

Let Σ be the set of all prime ideals in A, ordered by reverse inclusion. Σ is non-empty, since $0 \in \Sigma$. Moreover, if $(\mathfrak{a}_\alpha)$ is a chain of ideals in Σ, we claim that $\cap_\alpha \mathfrak{a}_\alpha$ is an upper (or rather, lower) bound to $(\mathfrak{a}_\alpha)$. It suffices to show that $\mathfrak{a} := \cap_\alpha \mathfrak{a}_\alpha$ is prime, and indeed if $x, y \notin \mathfrak{a}_\alpha$, then we have that there are some α, β such that $x \notin \mathfrak{a}_\alpha$ and $y \notin \mathfrak{a}_\beta$. Since $(\mathfrak{a}_\alpha)$ is a chain, we can assume WLOG that $\mathfrak{a}_\alpha \subseteq \mathfrak{a}_\beta$. Thus, $x, y \notin \mathfrak{a}_\beta$, meaning $xy \notin \mathfrak{a}_\beta$ and thus $xy \notin \mathfrak{a}$, showing that $\mathfrak{a}$ is prime.

1.11.5. Exercise 9

We handle both directions separately:

$\Rightarrow$: If $\mathfrak{a} = r(\mathfrak{a})$, then any $x \in A$ such that $x^n \in \mathfrak{a}$ for some $n > 0$ must lie in $\mathfrak{a}$. Thus, for any $\overline{x} \in A/\mathfrak{a}$ such that $\overline{x}^n = 0$, we have $\overline{x} = 0$, meaning in $A/\mathfrak{a}$ that the nilradical is the zero ideal, i.e. $\bigcap_{\mathfrak{p} \in \mathcal{F}} \mathfrak{p} = 0$ for a family of prime ideals $\mathcal{F}$ in $A/\mathfrak{a}$. Now, take $\pi : A \to A/\mathfrak{a}$ to be the natural projection of A onto $A/\mathfrak{a}$. Because taking preimages preserves intersections and sends prime ideals to prime ideals, we have that $\pi^{-1}\mathcal{F}$ is a family of prime ideals whose intersection is $\pi^{-1}(0) = \mathfrak{a}$, i.e. $\mathfrak{a}$ is an intersection of prime ideals.

$\Leftarrow$: Let $\mathfrak{a}$ be the intersection of some family $\mathcal{F}$ of prime ideals in A. If $x^n \in \mathfrak{a}$ for some $n > 0$, then $x^n \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{F}$. Since prime ideals are radical, this means that $x \in \mathfrak{p}$ for each $\mathfrak{p} \in \mathcal{F}$, and thus $x \in \mathfrak{a}$ as desired. $\square$

1.11.6. Exercise 10

We prove a cycle of implications.

(i) $\Rightarrow$ (ii): If A has exactly one prime ideal, then it must equal $\mathfrak{N}$, being the intersection of every prime ideal. Because $\mathfrak{N}$ is the maximal ideal in a local ring, every element not in $\mathfrak{N}$ must be a unit, i.e. every element is nilpotent or a unit.

(ii) $\Rightarrow$ (iii): Since every non-nilpotent element of A is a unit, we have that $\mathfrak{N}$ is maximal by Proposition 1.6(i) and thus $A/\mathfrak{N}$ is a field.

(iii) $\Rightarrow$ (i): If $A/\mathfrak{N}$ is a field, then $\mathfrak{N}$ is maximal. For any prime ideal $\mathfrak{p} \subseteq A$, we have $\mathfrak{N} \subseteq \mathfrak{p}$ as the nilpotent is the intersection of all prime ideals, but then by maximality of $\mathfrak{N}$ we must have $\mathfrak{N} = \mathfrak{p}$. Thus, there can only be one prime ideal in A. $\square$

1.11.7. Exercise 11

(i) For any $x \in A$, we have $x + 1 = (x+1)^2 = x^2 + 2x + 1 = 3x + 1$, meaning $2x = 0$.

(ii) For a given prime ideal $\mathfrak{p} \subseteq A$, take any $\overline{x} \in A/\mathfrak{p}$. Since $x^2 = x$ in A, i.e. $x(x-1) = 0$, we have $\overline{x}(\overline{x} - 1) = 0$ in $A/\mathfrak{p}$, meaning either $\overline{x} = 0$ or $\overline{x} = 1$ as $A/\mathfrak{p}$ is a domain. Thus, $A/\mathfrak{p}$ is a field with two elements, implying $\mathfrak{p}$ is maximal.

(iii) Take an arbitrary finitely generated ideal $\mathfrak{a} = (x_1, x_2, ..., x_n) \subseteq A$. Let $y = ...$

TODO: finish this!

1.11.8. Exercise 12

Let $\mathfrak{m}$ be the maximal ideal of a local ring A. Note that any $x \notin \mathfrak{m}$ must be a unit, otherwise by Corollary 1.5 it would lie in a maximal ideal distinct from $\mathfrak{m}$.

We show that the only idempotent element of $\mathfrak{m}$ is 0. Assume some $e \in \mathfrak{m}$ satisfies $e^2 = e$. Then $1 - e \notin \mathfrak{m}$, otherwise we would have $1 - e + e = 1 \in \mathfrak{m}$. Thus $1 - e$ is a unit. But $(1-e)^2 = 1 - 2e + e^2 = 1 - e$, so then multiplying both sides by $(1-e)^{-1}$, we get $1 - e = 1$, i.e. $e = 0$.

The only idempotent $e \notin \mathfrak{m}$ is 1, since $e \notin \mathfrak{m}$ implies e is a unit, meaning $e^2 = e$ implies $e = 1$. Since either $e \in \mathfrak{m}$ or $e \notin \mathfrak{m}$, our only options for an idempotent $e \in A$ are 0 and 1. □

2. Modules