Commutative Algebra and Algebraic Geometry

Miles Reid

Washington Directed Reading Program

Brian Nugent, Lukshya Ganjoo

March 06, 2024

Existence of maximal ideals

Definition 1

Given a commutative ring R and an ideal $I \subset R$, I is said to be **maximal** iff for any ideal $J \subseteq R$, where $I \subseteq J$; either $I = J$ or $J = R$.

Proposition 1

Suppose that Σ is a non-empty set with a partial order and that any totally ordered subset $S \subset \Sigma$ has an upper bound in Σ. Then Σ has a maximal element.

Proposition 2

Let A be a ring and $I \neq A$ an ideal; then there exists a maximal ideal of A containing I.

Intuitively the proof of this proposition essentially consists of saying that if I is not already maximal, then it is contained in a bigger ideal and so on. To make the "and so on" rigorous, we need **Zorn's Lemma**

Existence of maximal ideals

Proof.

Let us define the following set Σ

$$\Sigma = \{J_i \neq A \mid I \subseteq J_i \subset A\}$$

It is easy to see that $I \in \Sigma$ and therefore Σ is non-empty. Additionally, we note that set inclusion is a partial ordering on any collection of sets, and therefore we use inclusion as the partial ordering on Σ. We then note that if $\{J_\lambda\}_{\lambda \in \Lambda}$ is a totally ordered subset of Σ,

$$J^* = \bigcup_{\lambda \in \Lambda} J_\lambda \quad \text{is an ideal where } J^* \neq A$$

Indeed J^* is an upper bound of $\{J_\lambda\}_{\lambda \in \Lambda}$, and since all the conditions of **Zorn's Lemma** have been met, we can assert that Σ contains a maximal element. $\square$

Existence of maximal ideals

Proposition 3

For a ring A, an element $a \in A$ is either a unit, or is contained in a maximal ideal, and not both. If we define $A^\times$ as the set of units of A, then

$$A = A^\times \sqcup \bigcup_{m \in \mathcal{M}} m \quad \textit{where } \mathcal{M} \textit{ is the set of maximal ideals of } A$$

Proof.
$\implies$: Let $a \in A$ be contained in some maximal ideal m. We claim that a cannot be a unit. Indeed; suppose it was. If so, there exists a $u \in A$ such that $au = 1_A$. Since m is an ideal, it absorbs products; and therefore $1_A = au \in m$. This implies that $m = A$, a contradiction!

$\impliedby$: For this direction, we use **Zorn's Lemma**. Indeed if a is not a unit, then $1_A \notin (a)$, necessitating $(a) \neq A$. By **Proposition 2**, $a \in (a) \subseteq J$ for some maximal ideal J which completes the proof. $\square$

Definition 2

Given a ring A, M is said to be an A**-module** iff it is an abelian group with a multiplication map such that

$$A \times M \mapsto M \quad \text{written } (f, m) \mapsto fm$$

satisfying for all $f, g \in A$ and $m, n \in M$

1. $f(m \pm n) = fm \pm fn$
2. $(f + g)m = fm + gm$
3. $(fg)m = f(gm)$
4. $1_A m = m$

The intuition here is simply that **modules** over fields are vector spaces and all the stuff we do with modules can be thought of as linear algebra where scalar multiplication is with elements contained in A and linear combinations consist of coefficients in M.

Definition 3

A ring A is said to be **local** if it has a unique maximal ideal. We write this down as (A, m) where m denotes the aforementioned maximal ideal.

Definition 4

An A-module M is said to be **finite** or **finitely generated** if there exist $a_1, a_2, \ldots, a_n \in M$ such that for any $x \in M$,

$$x = \sum_{i=1}^{n} r_i a_i \quad \text{for some } \{r_i\}_{i=1}^{n}$$

The actually fun stuff (Nakayama's Lemma)

Proposition 4

Let (A, m) be a ***local ring*** *and M a finite A-module; then $M = mM$ implies that $M = 0$.*

Proof.

Let $(a_1, a_2, \ldots, a_n)$ be a minimal set of generators for M. Clearly $a_1 \in (a_1, a_2, \ldots, a_n) = M$. Since $M = mM$, there exist $\{m_i\}_{i=1}^{n}$ where $m_i \in m$ such that

$$\begin{aligned} a_1 &= m_1 a_1 + m_2 a_2 + \ldots m_n a_n \\ (1 - m_1) a_1 &= m_2 a_2 + \cdots + m_n a_n \\ a_1 &= \frac{1}{1 - m_1} (m_2 a_2 + \cdots + m_n a_n) \quad \text{since } 1 - m_1 \text{ is a unit} \end{aligned}$$

This is a contradiction since we assumed $(a_1, a_2, \ldots, a_n)$ was a minimal set of generators for M, thereby necessitating that $M = (0)$ and completing the proof. □

Proposition 5

Let (A, m) *be a local ring with* $m_1 \in m$*. Then* $1 - m_1$ *is a unit.*

Proof.

Since $m_1 \in m$, we claim that $1 - m_1$ is a unit. Assume not, then by **Proposition 3**, $1 - m_1 \in m$. Since ideals are closed under addition,

$$1_A = m_1 + (1 - m_1) \in m \implies m = A$$

which yields the desired contradiction. $\square$

Noetherian Rings (the best kind of rings)

Definition 5

A ring A is said to be **Noetherian** iff any one of the following three conditions are satisfied

- The set Σ of ideals of A has the **ascending chain condition**, i.e. for every increasing chain of ideals

  $$I_1 \subset I_2 \subset \cdots \subset I_k \subset \dots$$

  eventually stops, i.e. $I_n = I_{n+1}$ for some n.
- Every non-empty set $\mathcal{S}$ of ideals has a maximal element.
- Every ideal $I \subset A$ is finitely generated.

Note that the above conditions are equivalent conditions for a **Noetherian ring**.

Surjective homomorphism over Noetherian rings

Proposition 6

*If A is a **Noetherian ring**, then any subjective ring homomorphism $\varphi : A \to A$ is additionally injective.*

Proof.

We first claim that for $n \in \mathbb{N}$, $\mathbf{ker}(\varphi^n)$ is an ideal. Indeed we argue in the standard way

- **Closed under subtraction and products:** For $a, b \in \mathbf{ker}(\varphi^n)$, clearly

$$\varphi^n(a-b) = \underbrace{\varphi^n(a)}_{0} - \underbrace{\varphi^n(b)}_{0} \implies a - b \in \mathbf{ker}(\varphi^n)$$

and in much of the same way

$$\varphi^n(ab) = \varphi^n(a)\varphi^n(b) \implies ab \in \mathbf{ker}(\varphi^n)$$

where we make use of the fact that φ is a homomorphism.

Surjective homomorphisms over Noetherian rings

Proof.

- **Absorption of products:** Let $a \in A$ and $k \in \mathbf{ker}(\varphi^n)$, then

$$\varphi^n(ak) = \varphi^n(a)\underbrace{\varphi^n(k)}_{0} \implies ak \in \mathbf{ker}(\varphi^n)$$

Therefore $\mathbf{ker}(\varphi^n)$ is an ideal. Now we argue that the kernels of φ^n form an ascending chain of ideals of A. Indeed, let $a \in \mathbf{ker}(\varphi^n)$. Then

$$\varphi^n(a) = 0 \implies \varphi^{n+1}(a) = \varphi(\varphi^n(a)) = 0 \implies a \in \mathbf{ker}(\varphi^{n+1})$$

Now we proceed onto the main part of the proof. Since A is **Noetherian** and $\{\mathbf{ker}(\varphi^n)\}_{n\geq 1}$ is an ascending chain of ideals, there exists $m \in \mathbb{N}$ s.t. $\mathbf{ker}(\varphi^m) = \mathbf{ker}(\varphi^{m+1})$ $\square$

Proof.

Then let $a \in \mathbf{ker}(\varphi)$. Since φ is subjective, there exists $a_1 \in A$ s.t. $\varphi(a_1) = a$. Inductively, we can find $\{a_i\}_{i=1}^m \subset A$ where $\varphi(a_i) = a_{i-1}$. Therefore

$$\varphi^m(a_m) = a \implies \varphi^{m+1}(a_m) = 0$$

Since $a_m \in I_{m+1} = I_m$, we obtain $\varphi^m(a_m) = a = 0$, necessitating $\mathbf{ker}(\varphi) = \{0\}$. This completes the proof (a homomorphism f is said to be injective iff $\mathbf{ker}(f) = \{0\}$). □

Proposition 7

*For a **Noetherian ring** A, then $A[X]$ is also **Noetherian**.*

Okay so where's the geometry

Definition 6

The **prime spectrum** or $\mathrm{Spec}(A)$ is the set of prime ideals of A, i.e.

$$\mathrm{Spec}(A) = \{P \mid P \subset A \text{ is a prime ideal}\}$$

Definition 7

The **nilradical** of a ring A is defined as the set of all nilpotent elements of A, i.e.

$$\mathrm{nilrad}(A) = \{a \mid a^n = 0; a \in A, n > 0\}$$

Definition 8

The **radical** of an ideal I in a ring R is defined as

$$\sqrt{I} = \mathrm{rad}(I) = \{r \in R \mid r^n \in I; n > 0\}$$

Definition 9

Let k be a field. A **variety** $V \subset k^n$ is a subset of the form

$$V = V(J) = \{P = (a_1, \ldots, a_n) \in k^n \mid f(P) = 0 \text{ for all } f \in J\}$$

where $J \subset k[X_1, \ldots, X_n]$ is an ideal.

Since $k[X_1, \ldots, X_n]$ is a **Noetherian ring**, J is finitely generated, i.e. $J = (f_1, \ldots, f_m)$ and therefore a variety is defined by

$$f_1(P) = f_2(P) = \cdots = f_m(P) = 0$$

Intuitively a variety is simply a set of common zeros to a collection of polynomial equations.

The Nullstellensatz

Proposition 8

Let k be an algebraically closed field.

1. *If $J \subset k[X_1, \ldots, X_n]$, then $V(J) \neq \emptyset$*
2. *$I(V(J)) =$ rad(J), i.e. for $f \in k[X_1, \ldots, X_n]$,*

$$f(P) = 0 \text{ for all } P \in V \Leftrightarrow f^n \in J \text{ for some } n$$

where $I(U)$ is the ideal of all polynomials that vanish on the set U.

Consequence: *Gives a one-to-one correspondence between algebraic varieties and the radical ideals of a ring.*

Definition 10

A field k is said to be **algebraically closed** iff every non-constant polynomial in $k[X]$ has a root in k.

Corollary 1

Let k be an algebraically closed field, and let $I \subseteq k[X_1, \ldots, X_N]$ be an ideal such that $V(I) = \emptyset$. Then $I = k[X_1, \ldots, X_n]$

Corollary 2

The maximal ideals of $\mathbb{C}[X_1, \ldots, X_n]$ are precisely those maximal ideals that come from points, i.e. ideals of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for $a_1, \ldots, a_n \in \mathbb{C}$

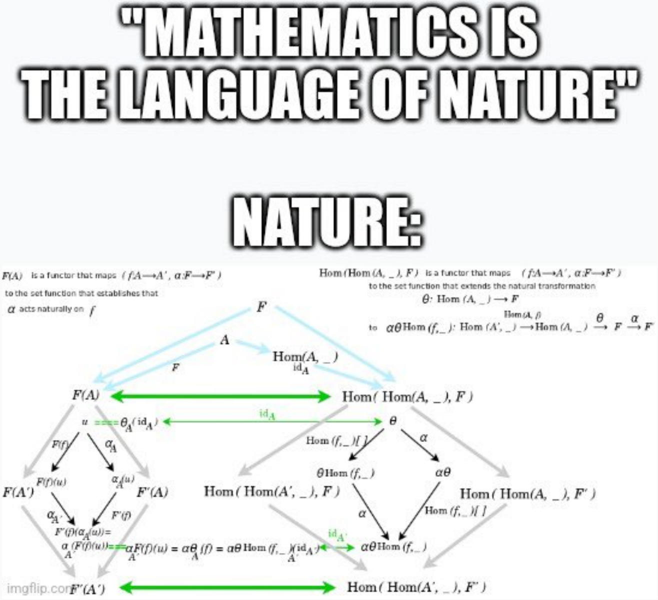
Applications

1. The Nullstellensatz shows up in Buchberger's algorithm in geometry, a technique used to transform a given set of polynomials into a Gröbner basis.
2. Used in the proof of Stickelberger's theorem which shows up in algebraic number theory and deals with annihilators in rings and ideals.
3. Determines whether a solution to polynomial problems exists when working within the framework of semi-definite programming problems.
4. Proof of Ax-Grothendieck theorem that discusses the relationship between a function's injective and bijective properties.

Lots we didn't talk about

1. **Localization:** A ring of fractions corresponds to restricting functions on the spectrum of said ring to a specific open subset.
2. **Primary decomposition:**
3. **Integral extensions and normalization**
4. **Discrete valuation rings:** The best kind of UFD's (the ones having only one prime).
5. **A noetherian normal ring is an intersection of DVR's**
6. **Finiteness of normalization**

Thank you!



"MATHEMATICS IS THE LANGUAGE OF NATURE"
NATURE:
F(A) is a functor that maps (f:A⟶A′, α:F⟶F′)
to the set function that establishes that
α acts naturally on f
Hom (Hom (A, _), F) is a functor that maps (f:A⟶A′, α:F⟶F′)
to the set function that extends the natural transformation
θ: Hom (A, _) ⟶ F
F
A
Hom(A, _)
F(A)
Hom(Hom(A, _), F)
θ
α
F(A′)
F′(A)
Hom (Hom(A′, _), F)
Hom (Hom(A, _), F′)
θHom (f, _)
αθ
αθHom (f, _)
F′(A′)
Hom (Hom(A′, _), F′)
imgflip.com