Algebra IV - 2024

Lecturer John Bourke
bourkej@math.muni.cz

Course
- Commutative algebra (app 4 wks)
- Homological algebra (app 6 wks)
- Representation theory (app 4 wks)

Structure: 3 marked assignments (30%)
+ oral exam (70%)

Notes uploaded to IS weekly

Lecture 1 - Commutative Algebra

This week we will look at polynomial rings (commutative algebras), Noetherian modules & rings, Hilbert's basis theorem & how it was introduced in context of invariant theory.

Commutative R-algebras

Let R be a commutative ring.
We are interested in the set $R[x_1, \dots, x_n]$ of polynomials in n variables with coefficients in R:

$$\text{eg. } r x_1 x_2^3 + s x_n^7$$

What sort of structure do they form?

- An R-module (add, action of elts of R)
- A comm ring (add, multiply polys)

such that multiplication is R-bilinear

(eg. $r(fg) = (rf)g = f(rg)$ etc ...)

Def) An R-algebra is an R-mod $(A, +, \cdot)$ with ring structure $(A, +, \times)$ for which $\times : A \times A \to A$ is R-bilinear.

It is a commutative R-alg if A is a commutative ring.

- With their homomorphisms, obtain categories R-Alg & c-R-Alg.

Remarks

① Recall from Alg3 that $(R\text{-Mod}, \otimes_R, R)$ is a monoidal cat -

a R-alg $\equiv$ a monoid $A \otimes_R A \xrightarrow{\cdot} A \longleftarrow R$ in R-Mod

comm R-alg $\equiv$ comm monoid.

② A comm. R-alg $\equiv$ comm. ring A with a ring homomorph $R \longrightarrow A$

Pf) Given A as above define ring homomorph $R \longrightarrow A$
$r \longmapsto r.1$.

Conversely, given $f : R \longrightarrow A$ a hom of c. rings, define R-mod str by
$r.a = f(r).a$.

Check operations inverse!

As anticipated at the start

Prop^n) $R[x_1,\dots,x_n]$ is the free comm. R-alg on n elements $x_1,\dots,x_n$.

Proof) Given a function $f:\{x_1,\dots,x_n\}\to A$ a comm. R-alg, must show $\exists!$ $\bar{f}: R[x_1,\dots,x_n]\to A \in$ c-R-Alg such that

$$\begin{tikzcd}
\{x_1,\dots,x_n\} \arrow[r, hook] \arrow[dr, "f"'] & R[x_1,\dots,x_n] \arrow[d, "\bar{F}"] \\
& A
\end{tikzcd}$$

This says $\bar{F}(x_i)=F(x_i)$ but then to have a homomorphism, we are forced to define

$$\sum_{m_1,\dots,m_n\in\mathbb{N}} r_{(m_1,\dots,m_n)} x_1^{m_1}\cdots x_n^{m_n} \overset{\bar{F}}{\longmapsto} \sum_{m_1,\dots,m_n\in\mathbb{N}} r_{(m_1,\dots,m_n)} \bar{F}(x_1)^{m_1}\cdots\bar{F}(x_n)^{m_n}$$

$$= \sum_{m_1,\dots,m_n\in\mathbb{N}} r_{(m_1,\dots,m_n)} F(x_1)^{m_1}\cdots F(x_n)^{m_n}$$

which is clearly a homomorphism.

Finitely generated structures

Def) An R-algebra A is finitely generated if $\exists a_1, \ldots, a_n$ st each element of A is a R-linear comb. of products of the a_i

eg. $r_1 a_1 a_2 + r_5 a_4 a_7^6 \ldots$

For a commutative R-algebra A, this is equiv. to saying that $\exists$ surj. homomorphism

$$R[x_1, \ldots, x_n] \twoheadrightarrow A \quad \text{for some } n.$$

$$x_i \longmapsto a_i$$

Def) An R-module M is finitely generated if $\exists a_1, \ldots, a_n$ st. each $a \in M$ is of form

$a = r_1 a_1 + \ldots + r_n a_n$.

· Equivalently, if $\exists n \in \mathbb{N}$ & surjective hom.

$$R^n \twoheadrightarrow M$$

free R-mod on n elements

Remark) A is finitely gen as R-module $\Rightarrow$ it is f.g. as R-algebra.

But $R[x]$ is f.g. algebra but not as R-module : $1, x, x^2, x^3, \ldots$ no finite basis.

Noetherian modules & rings

Def^n) **Let R be a commutative ring.**

An R-module M is finitely generated if $\exists a_1, \dots, a_n$ st. each $a \in M$ is of form $a = r_1 a_1 + \dots + r_n a_n$.

- Equivalently, if $\exists n \in \mathbb{N}$ & surjective hom.

$$R^n \twoheadrightarrow M$$

free R-mod on n elements

Def^n) An R-module M is Noetherian if all its submodules are f.g.

Remark) In partic., M itself must be f.g.

Proposition

TFAE

1. M is Noetherian
2. M satisfies ascending chain cond. (ACC):

each sequence $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq M$ stabilises - ie. $\exists k \in \mathbb{N}$ st $M_k = M_{k+i}$ $\forall i \in \mathbb{N}$.

3. Every non-empty set $\mathcal{F}$ of submodules of M has a maximal element.

~~Proof~~ $1 \Rightarrow 2$) $\bigcup_{i \in \mathbb{N}} M_i \subseteq M$ is a submodule. Hence by 1 it is f.g. by $a_1, \dots, a_n$.

Since each $a_i \in \bigcup M_i$ belongs to some M_{k_i}, then $a_1, \dots, a_n \in M_{\max(k_1, \dots, k_n)}$ so

$$M_{\max(k_1,\dots,k_n)} = M_i \text{ all } i \geq k.$$

$2 \Rightarrow 3$) Proof by contradiction.

Suppose $\mathcal{F}$ has no max^l elt.

- As non-empty, $\exists M_0 \in \mathcal{F}$. By assumption M_0 not max^l, so $\exists M_0 \subset M_1 \in \mathcal{F}$.
- Continue to get $M_0 \subset M_1 \subset \dots \subset M_n \subset \dots \in \mathcal{F}$ which does not stabilise. Contradiction.

Proposition

TFAE

① M is Noetherian

② M satisfies ascending chain cond. (ACC):

each sequence $M_0 \subseteq M_1 \subseteq \dots \subseteq M_n \subseteq \dots \subseteq M$ stabilises - ie. $\exists k \in \mathbb{N}$ st $M_k = M_{k+i}$ $\forall i \in \mathbb{N}$.

③ Every non-empty set $\mathcal{F}$ of submodules of M has a maximal element.

Proof continued

$3 \Rightarrow 1$) Let $N \subseteq M$.

Let $\mathcal{F}$ be set of f.g. submodules of N.

Then $\{0\} \in \mathcal{F}$, so $\mathcal{F}$ has max^{l} element

$A = \langle a_1, \dots, a_n \rangle$.

We claim $A = N$.

If not, $\exists\, b \in N \setminus A$, but then

$A < \langle a_1, \dots, a_n, b \rangle \subseteq N$ contradicting

maximality of A.

Hence $A = N$ is f.g. $\square$

Properties of Noetherian modules

① Let M be an R-mod & $N \leq M$. Then
M is Noetherian $\Leftrightarrow$ N is Noeth. & M/N is Noeth.

② If M, N Noetherian, so is $M \oplus N$.

~~Proof~~

① Suppose M Noetherian.

- If $N \leq M$ & $A \leq N$, then $A \leq M$ so A is f.g.
  Hence N is Noetherian.
- Consider $p: M \longrightarrow M/N : m \longmapsto m + N$.
  Given $A \leq M/N$, $p^{-1}A \leq M$ so
  $p^{-1}A = \langle a_1, \ldots, a_n \rangle$.
  Then $A = pp^{-1}A = \langle pa_1, \ldots, pa_n \rangle$ is f.g.
  Hence M/N Noetherian.

Conversely suppose N & M/N Noetherian.

$$A_0 \leq \cdots \leq A_i \leq \cdots M.$$

Then $(A_i \cap N)_{i \in \mathbb{N}} \leq N$ stabilises @ $A_k \cap N$
$(pA_i)_{i \in \mathbb{N}} \leq M/N$ stab @ pA_k.

Given $x \in A_{k+1}$, then $x + N = y + N$ for $y \in A_k$.
Then $x - y \in N \cap A_{k+1} = N \cap A_k$ so
$x = y + (x-y) \in A_k$. So $A_k = A_{k+1} \ldots$
& M Noetherian.

Properties of Noetherian modules

① Let M be an R-mod & $N \leq M$. Then M is Noetherian $\iff$ N is Noeth. & M/N is Noeth.

② If M, N are Noetherian, so is $M \oplus N$.

Proof continued.

② Note that $\ker(p : M \oplus N \longrightarrow N) = M$.
Hence by the first iso theorem
$$N \cong M \oplus N / M$$
so the result follows from ①.

$\square$

Noetherian rings

Def^n) A commutative ring R is Noetherian if it is Noetherian as an R-module.

Since a submodule of R is precisely an ideal I of R, this says that each ideal I is finitely gen.

Examples

- If R is a field, its only ideals are $\{0\}$ & R – hence R is Noetherian.

- If R is a principal ideal domain – eg. $\mathbb{Z}$ – all of its ideals are gen by a single element. Therefore R is Noetherian.

Non-example

- Note R is free R-module on 1 - $r = r.1$ - & so finitely generated.

Hence a non-Noetherian ring gives an example of a f.g. module **with a non f.g. submodule.**

- An example of such a ring is $R[x_1, x_2, \ldots, x_n, \ldots]$ the ring of polys in inf. many variables.

It has sequence of ideals

$\langle x_1 \rangle \subset \langle x_1, x_2 \rangle \subset \langle x_1, x_2, x_3 \rangle \subset \ldots R[x_1, \ldots, x_n]$

which never stabilises so this is a non-Noeth. ring;

indeed the non f.g. ideal

$$\bigcup_{n \in \mathbb{N}} \langle x_1, \ldots, x_n \rangle = \text{ideal of polynomials with no scalar term.}$$

Theorem (Hilbert's basis Theorem)

Suppose R is a commutative Noetherian ring. Then so is $R[x_1, \dots, x_n]$.

Remark

- Hilbert proved this result, 1890 in the context of proving the Fundamental theorem of invariant theory, which we will discuss below.
- It is not constructive, using contradiction & does not produce explicit set of generators of an ideal.
- Disturbed mathematical world at time: the leader of invariant theory at the time, Paul Gordan, said

"This is not mathematics, it is theology!"

Theorem (Hilbert's basis Theorem)

Suppose R is a commutative Noetherian ring. Then so is $R[x_1, \dots, x_n]$.

Proof

- Since $R[x_1, x_2] = R[x_1][x_2] \dots$ it suffices, by induction, to show that $R[x]$ is Noeth if R is.
- Suppose $I \subseteq R[x]$ which is not f.g. – we will derive a contradiction.
- Given a poly. $c_n x^n + \dots + c_1 x + c_0$ we say its degree is n & leading term is c_n.
- Choose $f_0 \in I$ of minimal degree. As I is not f.g. $\exists$ $f_1 \in I - \langle f_0 \rangle$ of min. degree.
- Continuing in this way, we obtain

  $f_{n+1} \in I - \langle f_0, \dots, f_n \rangle$ of min deg. for each n.

- By construction $\deg(f_0) \leq \deg(f_1) \leq \deg(f_2) \leq \dots$
- Let a_i be leading term of f_i.
- Then we have chain of ideals of R $\langle a_0 \rangle \subset \langle a_0, a_1 \rangle \subseteq \dots$
- As R is Noetherian, it stabilises at $\langle a_0, a_1, \dots, a_m \rangle$.

Then

$a_{m+1} = r_0 a_0 + \dots + r_m a_m$ for some $r_i \in R$.

- Since $\deg(f_{m+1}) \geq \deg(f_i)$ all $i \leq m$, we can form the polynomial

$$g = \sum_{i=0}^{m} r_i \, x^{(d(f_{m+1}) - d(f_i))} f_i \in \langle f_0, \dots, f_m \rangle$$

- This poly. is a sum of polys of degree $d(f_{m+1})$ & so g has deg $d(f_{m+1})$.
- If $f_{m+1} - g \in \langle f_0, \dots, f_m \rangle$ then we would have $f_{m+1} = (f_{m+1} - g) + g \in \langle f_0, \dots, f_m \rangle$ too as ideal closed under sums, which is false.

Hence $f_{m+1} - g \in I - \langle f_0, \dots, f_m \rangle$.

- Therefore its degree $\geq$ degree $\langle f_{m+1} \rangle$.
- However,

$$f_{m+1} - g = f_{m+1} - \left(\sum_{i=0}^{m} r_i \, x^{(d(f_{m+1}) - d(f_i))} f_i \right)$$

has term of top degree $d(f_{m+1})$ & this is $a_{m+1} - \sum_{i=0}^{m} r_i a_i = 0$.

Therefore $f_{m+1} - g$ has lower degree than f_{m+1}, which is a contradiction. $\square$

Prop^n Let $f: R \to S$ be a surjective homomorphism of commutative rings. If R is Noetherian, so is S.

Proof

For $I \subseteq S$ an ideal, then $f^{-1}(I) \subseteq R$ an ideal with $f(f^{-1}I) = I$

As R is Noeth, $f^{-1}I = \langle a_1, \ldots, a_n \rangle$.

Therefore $I = f(f^{-1}I) = f\langle a_1, \ldots, a_n \rangle$
$= \langle fa_1, \ldots, fa_n \rangle$. $\square$

Theorem

Let R be a commutative Noetherian ring. Then each f.g. commutative R-algebra A is Noetherian ring.

~~Proof~~ $\exists$ $R[x_1, \ldots, x_n] \twoheadrightarrow A$ surjective hom. of rings.

By Hilbert's basis thm, $R[x_1, \ldots, x_n]$ is Noetherian.

By previous result, so is A.

Invariant theory

Problem : understand functions invariant under action of a group G.

- We will look at the case K a field & G acting on comm. K-alg

$$P = K[x_1, \ldots, x_n] :$$

that is, we have a group hom

$$G \longrightarrow c\text{-}K\text{-}Alg(P,P)$$
$$g \longmapsto g.- : P \longrightarrow P$$

a K-alg hom

st. $e.f = f$ where $e \in G$ is unit &
$(g.h).f = g.(h.f)$ for $g,h \in G$.

- The invariants of the action are its fixpoints : those polys f s.t.
$$g.f = f \quad \forall g \in G.$$
- These form a subalgebra $P^G \overset{i}{\hookrightarrow} P$

Example - symmetric Functions

Symmetric group S_n acts on $\{x_1, \dots, x_n\}$ by permuting elements.

Induces action of S_n on $k[x_1, \dots, x_n]$ by permuting variables eg.

eg. $(12)(2x_1x_2^2 + 3) = 2x_2x_1^2 + 3$.

- Then P^{S_n} = k-alg. of symmetric functions.

Examples are the elementary symm. functions

$f_0 = 1$

$f_1 = x_1 + \dots + x_n$

$f_2 = \sum_{1 \leq i \leq j \leq n} x_i x_j$

$\vdots$

$f_n = x_1 . x_2 \dots x_n$

In fact, P^{S_n} is f.g. as a k-alg by the el. s.f.'s : in fact, each $f \in P^{S_n}$ is uniquely a lin comb of multiples of the esf.

Fundamental problem of invariant theory

- Determine whether P^G has a finite set of generators (i.e. is a f.g. K-algebra).

We will show this is true in wide generality.