Commutative Algebra

October 12, 2020

0 Introduction

Commutative Algebra is the study of commutative rings and the spaces on which those rings act, namely modules. It was developed from two key sources: algebraic geometry, and algebraic number theory.

In algebraic geometry we are focused on polynomial rings over a field k, whilst in number theory we are focused on $\mathbb{Z}$, the ring of rational integers. Much of this work was done by Grothedieck, but the subject goes back much further, at least to Hilbert who wrote a series of papers on polynomial invariant theory in the late nineteenth century.

As an example, take Σ_n, the symmetric group on the set $\{1, 2, \ldots, n\}$. Σ_n acts on $k[x_1, \ldots, x_n]$ by permuting the variables, so that $(\sigma f)(x_1, \ldots, x_n) = f(x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$. σ_n acts here via ring automorphisms, and it is then natural to consider the ***ring of invariants***, given by $\{f \in k[\mathbf{x}] : \sigma f = f \ \ \forall \sigma \in \Sigma_n] \coloneqq S$. S is a ring, ***the ring of symmetric polynomials***. We can consider the elementary symmetric functions, which are:

$$\begin{aligned}
e_1(x_1, \ldots, x_n) &= x_1 + \ldots + x_n \\
e_2(x_1, \ldots, x_n) &= \sum_{i<j} x_i x_j \\
&\vdots \\
e_n(x_1, \ldots, x_n) &= x_1 \ldots x_n
\end{aligned}$$

In fact, S is generated as a ring by these e_i, and there are canonical maps $k[y_1, \ldots, y_n] \to S$ such that $Y_i \mapsto e_i$, which is a ring isomorphism.

Hilbert showed that S is finitely generated, and moreover for many other groups, not just symmetric groups.

Along the way, he proved four very deep theorems:

- Basis theorem
- Nullstellensatz
- The polynomial nature of the Hilbert function (leading to the beginnings of dimension theory)
- The syzygy theorem (leading to the beginnings of homological theory of polynomial rings)

In 1921 Emmy Noether extracted the key property that made the basis theorem, namely that a commutative ring is ***noetherian*** if every ideal is finitely generated (there are several equivalent definitions).

Theorem 0.1 (Hilbert's Basis Theorem)**.** *If R is a commutative noetherian ring, then $R[x]$ is also noetherian.*

Corollary 0.2. *If k is a field, then $k[x_1, \dots, x_n]$ is noetherian.*

Noether developed a theory of ideals for noetherian rings, for example the existence of primary decomposition, which generalises factorisation into primes in noetherian rings.

Link between Commutative Algebra and Algebraic Geometry

The starting point for this link is the ***fundamental theorem of algebra***, which says that $f \in \mathbb{C}[x]$ is determined up to scalar multiples by its zeros up to multiplicity. Given $f \in \mathbb{C}[x_1, \dots, x_n]$, there is a polynomial function $\mathbb{C}^n \to \mathbb{C}$ given by $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$.

Different polynomials will yield different functions, and so $\mathbb{C}[x_1, \dots, x_n]$ can be viewed as a ring of polynomial functions on complex affine n-space.

More specifically, given $I \subseteq \mathbb{C}[x_1, \dots, x_n]$, we can define the ***set of common zeros***, $Z(I) = \{(a_1, \dots, \_n) \in \mathbb{C}^n : f(a_1, \dots, a_n) = 0 \ \ \forall f \in I\}$, called an ***(affine) algebraic set***.

<u>Remarks:</u>

- One can replace I by the ideal generated by I, and you get the same algebraic set. Similarly, replacing an ideal by a generating set of the ideal leaves the algebraic set. The basis theorem asserts that any algebraic set is the set of common zeros of some ***finite*** set of polynomials.
- $\bigcap_j Z(I_j) = Z(\bigcup_j I_j), \bigcup_{j=1}^n Z(i_j) = Z(\prod_{j=1}^n I_j)$, for ideal I_j. If we define a topology on $\mathbb{C}^n$ by calling these algebraic sets the closed sets, we get the ***Zariski toplogy***, which is a rather coarser topology on $\mathbb{C}^n$ than the usual topology.
- For $S \subseteq \mathbb{C}^n$, we can define $I(S) = \{f \in \mathbb{C}[x_1, \dots, x^n] : f(a_1, \dots, a_n) = 0 \ \ \forall (a_1, \dots, a_n) \in S\}$. This is an ***ideal*** of $\mathbb{C}[x_1, \dots, x_n]$, and it is ***radical***, i.e. $f^r \in I(s) \implies f \in I(S)$. The Nullstellensatz is a family of results asserting that the correspondence

$$\begin{aligned} I &\mapsto Z(I) \\ I(S) &\leftarrow\!\shortmid S \end{aligned}$$

gives a bijection between the radical ideals in $\mathbb{C}[x_1, \dots, x_n]$ and the algebraic subsets of $\mathbb{C}^n$. In particular, the maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ correspond to points in $\mathbb{C}^n$

Dimension

A large portion of the course deals with the dimension of rings. We can define it in three main ways:

- The maximal length of a chain of prime ideals.
- In a geometric context in terms of growth rates.
- The transcendence degree of a field of fractions.

For commutative rings, all three give the same answer. There is in fact a fourth method, using homological algebra, which in the case of "nice" noetherian rings also gives the same answer.

Most of this theory dates back to 1920-1950. Rings of dimension 0 are called ***artinian*** rings, and in dimension 1 there are special properties which are important in number theory, particularly in the study of algebraic curves.

1 Noetherian Rings: Definitions and Examples

Throughout this section, R is a commutative ring with a 1.

Lemma 1.1. *Let M be a (left) R-module. The following are equivalent:*

1. *All submodules of M (including M itself) are finitely generated.*
2. *The ascending chain condition (ACC) holds: there are no strictly increasing infinite chains of submodules.*
3. *The maximum condition of submodules holds: any nonempty set S of submodules of M has a maximal element L, i.e. $L \subseteq L', L' \in S \implies L = L'$.*

Proof.
1. $\implies$ 2. Suppose there is a strictly increasing chain $N_1 \subsetneq N_2 \subsetneq \ldots$, and let $N = \bigcup_{i=1}^{\infty} N_i$. By *1* N is finitely generated, say by $m_1, \ldots, m_r$. Each m_i lies in some N_{n_i}. Then let $n = \max_i n_i$, so that $m_i \in N_n$. Then $N_n = M$, contradicting strict ascent.

2. $\implies$ 3. Assume ACC. Pick $M_1 \in S$. If it is the maximal member then we're done. If not, there is $M_2 \supsetneq M_1$. If M_2 is maximal, then we're done, otherwise there is some $M_3 \supsetneq M_2$, and so on. By ACC this process terminates, and we get a maximal element.

3. $\implies$ 1. Let $N \triangleleft M$, and let S be the collection of all finitely generated submodules of N. Then $S \neq \emptyset$ since it contains the 0 submodule. So S contains a maximal member, say L. We then claim $N = L$. If $x \in N$ then $L + Rx \in S$, and by maximality of L, $x \in L$. □

Definition 1.2. *An R-module satisfying 1, 2, 3 is* **noetherian**.

Lemma 1.3. *Let $N \triangleleft M$. Then M is noetherian if and only if N and M/N are noetherian.*

Proof.
$\implies$ Let M be noetherian, so that all its submodules are finitely generated. This property is inherited by N. Also, the submodules of M/N are all of the form Q/N with $Q \triangleleft M$ containing N. If M is noetherian, then Q is finitely generated, say by $x_1, \ldots, x_r$. Then $x_1 + N, \ldots, x_r + N$ generates Q/N.

$\impliedby$ Let $N, M/N$ be noetherian, and let $L_1 \subset L_2 \subset L_3 \subset \ldots$ be a strictly increasing chain of submodules of M. Set $Q_i/N = (L_i + N)/N$, and $N_i = L_i \cap N$. These give ascending chains of submodules of M/N and N respectively. By ACC there are r, s with $Q_i/N = Q_r/N$ for $i \geq r$, $N_i = N_s$ for $i \geq s$. Let $k = \max\{r, s\}$. Then we claim $L_i = L_k$ for $i \geq k$. Pick $\ell \in L_i$, $i \geq k$. Then $\ell + N \in Q_k/N$, and so there is some $\ell' \in L_k$ such that $\ell - \ell' \in N \cap L_i = N \cap L_k$. So $\ell \in L_k$, and the claim is proved. Hence our original ascending chain was not strictly increasing, $\lightning$. □

Lemma 1.4.
1. *If M, N are R-modules, then $M \oplus N$ is noetherian iff M and N are noetherian.*

2. *If $M_1, \ldots, M_n$ are R-modules then $M_1 \oplus \ldots \oplus M_n$ is noetherian iff each M_i is noetherian.*

3. *If M is noetherian then every homomorphic image of M is noetherian.*

4. *Suppose M can be expressed as a sum of finitely many submodules (not necessarily as a direct sum) $M = M_1 + \ldots + M_n$. Then M is noetherian iff each M_i is.*

Proof. 1. $M \cong N/N$, so this follows by **1.3**.

2. Apply *1* and induction on n.

3. If $\theta : M \to N$ then $\operatorname{im}\theta \cong M/\ker\theta$, so apply **1.3**.

4. The forwards direction follows as $M_i \lhd M$. For the reverse, there is a map from $M_1 \oplus \ldots \oplus M_n \to M$, $(m_1, \ldots, m_n) \mapsto m_1 + \ldots + m_n$, and then apply *2* and *3*.

□

Definition 1.5. *A ring R is* **noetherian** *if it is noetherian as a (left) R-module*

Remark: Submodules of R as an R-module are the same as ideals of R as a ring, and so the ACC for modules gives us the ACC for ideals.

Lemma 1.6. *Let R be a noetherian ring. Then any finitely generated R-module M is noetherian.*

Proof. Suppose $M = Rm_1 + \ldots + Rm_n$. There exist R-module epimorphisms:

$$\begin{aligned} R &\to Rm_i \\ r &\mapsto rm_i \end{aligned}$$

R is noetherian, so Rm_i is as the homomorphic image of R. Then, by **1.4** *(4)*, so is M. □

Theorem 1.7 (Hilbert Basis Theorem)**.** *Let R be a noetherian ring. Then the polynomial ring $R[x]$ is noetherian.*

Proof. We show that every ideal of $R[x]$ is finitely generated. Let I be an ideal. We define $I(n) = \{f \in I : \deg f \leq n\}$. Then $I(n) \neq \emptyset$ as $0 \in I(n)$, and $I(0) \subseteq I(1) \subseteq I(2) \subseteq \ldots$.

Let $R(n) = \{\text{Coefficient of } x^n \text{ in } f : f \in I(n)\} \subseteq R$. We claim $R(n) \lhd R$, and $R(n) \subseteq R(n+1)$.

To see this, suppose $a, b \in R(n)$. Then there are polynomials $f(x) = ax^n + \ldots, g(x) = bx^n + \ldots$ in I, where $\ldots$ indicates lower order terms. Since $I \lhd R$, $f \pm g \in I$, $rf \in I$ for all $r \in R$, and $xf \in I$.

Hence $a \pm b \in R(n), ra \in R(n)$, and $a \in R(n+1)$, and the claim is proved.

So then we have a chain $R(0) \subseteq R(1) \subseteq R(2) \subseteq \ldots$ terminates, so we may say $R(n) = R(N)\ \forall n \geq N$. Each of $R(0), \ldots, R(N)$ is a finitely generated ideal of R, say $R(j) = (a_{j,i}, \ldots, a_{j,k_j})$.

Then by definition of $R(j)$, we may take polynomials $f_{j,1}, \ldots, f_{j,k_j}$ in $I(j)$ which have the $a_{j,i}$ as their leading coefficients.

Clearly $I \supseteq (f_{j,k} : 0 \leq j \leq N, 1 \leq k \leq k_j) =: J$ - it remains to show that equality holds, then we will have found a finite generating set of I. So pick $f \in I$, then we claim $f \in J$, and prove this by induction on the degree of f.

If $\deg f = 0$, then $f(x) = a$, say. But then $a \in R(0)$, and so $a = \sum_i r_i a_{0,i}$ for some $r_i \in R$. Since $f_{0,i}$ has $a_{0,i}$ as its leading coefficient and has degree zero, $f_{0,i}(x) = a_{0,i}$, and $f = \sum_i r_i f_{0,i} \in J$.

If instead $\deg f = n$, with $0 < n \leq N$, and the claim holds for all g with $\deg g < n$, then write $f(x) = ax^n + \ldots$. $a \in R(n)$ then by definition, so $a = \sum_i r_{n,i} a_{n,i}$ for some $r_{n,i} \in R$. Then define $g(x) = f(x) - \sum_i r_{n,i} f_{n,i}(x)$. $g(x)$ has degree $\leq n$, and the coefficient of x^n is $a - a = 0$, hence $\deg g < n$. Since $f_{n,i} \in I$, we have $g \in I$, and hence by induction $g \in J$. But $f_{n,i} \in J$ as well, so $f \in J$.

Finally if $\deg f = n$, with $n > N$, and the claim holds for all g with $\deg g < n$, again write $f(x) = ax^n + \ldots$. Then $a \in R(n) = R(N)$, so $a = \sum r_{N,j} a_{N,j}$ for $r_{N,j} \in R$. We may then define $g(x) = f(x) - \sum_i x^{n-N} r_{N,j} f_{N,j}(x)$, and use the same argument as in the previous paragraph to deduce that $f \in J$.

Hence $I \subseteq J$, and so $I = J$ and I is finitely generated. But I was an arbitrary ideal of $R[x]$, so $R[x]$ is noetherian. □

In practice, one uses ***Gröbner bases*** for ideals - these are generating sets with extra properties that make algorithms more efficient.

Examples:

- Fields are noetherian.
- Principle Ideal Domains (PIDs) are noetherian.
- $\{q \in Q : q = \frac{m}{n}, m, n \in \mathbb{Z}, p \nmid n$ for some fixed prime $p\}$, an example of a *localisation* of $\mathbb{Z}$. All localisations of noetherian rings are noetherian - we will see this later.
- $k[x_1, x_2, \ldots]$ is not noetherian: $(x_1) \subsetneq (x_1, x_2) \subsetneq$ is an infinite strictly increasing chain.
- $k[x_1, x_2, \ldots, x_n]$ is noetherian - this follows by induction using the Hilbert basis theorem.
- $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ is noetherian, so any finitely generated commutative ring is noetherian: if R is generated by $r_1, \ldots, r_n$, then there is an epimorphism $\mathbb{Z}[x_1, \ldots, x_n] \to R$ given by $x_i \mapsto r_i$, and R is the homomorphic image of a noetherian ring.
- If A is a free abelian group, write $\mathbb{Z}A$ for its group algebra, which is the set of formal linear combinations of elements of A, i.e. terms of the form $\sum_{\alpha \in A} \lambda_\alpha \alpha$ where $\lambda_\alpha \in \mathbb{Z}$ and only finitely many of the λ_α are nonzero.

  If A is generated as a group by $g_1, \ldots, g_n$, then its group algebra is generated as a ring by $g_1, g_1^{-1}, \ldots, g_n, g_n^{-1}$.
- $k[[x]]$, the ring of formal power series with coefficients in k, is noetherian.

There are also some non-commutative examples that are both left and right noetherian:

- Enveloping algebras of a finite dimensional Lie algebra.
- Iwasawa algebras of compact p-adic groups.

Theorem 1.8. *If R is noetherian, then $R[[x]]$ is noetherian.*

Proof 1. As in **1.7**, consider $R(n) =$ the set of trailing coefficients a_n, for elements $a_n x^n +$ higher order terms, and mimic the proof. This is on example sheet 1. □

We will give a second proof, which uses

Theorem 1.9 (Cohen's Theorem)**.** *If every prime ideal in a ring R is finitely generated, then R is noetherian.*

Proof. If R is not noetherian, then there is a family of non-finitely generated ideals. Call it $\mathscr{S}$. By assumption, $\mathscr{S} \neq \emptyset$. Partially order $\mathscr{S}$ by inclusion.

Suppose $I_1 \subseteq I_2 \subseteq \dots$ is a chain of non-finitely generated ideals. Then we claim $\bigcup_i I_i$ is also non-finitely generated.

If it were, say by $(a_1, \dots, a_k)$, then $a_i \in I_{n(i)}$ for some finite integer $n(i)$, and so, if $N = max\{n(i) : 1 \leq i \leq k\}$, N is also finite and $a_i \in I_N$ for all i. But then $I_N = I_n$ for all $n \geq N$, and in particular I_N is finitely generated $\lightning$.

So $\mathscr{S}$ has upper bounds to its chains, and so we may apply Zorn's lemma to get a maximal element of $\mathscr{S}$, say I, so that I is not finitely generated but any ideal containing I is finitely generated.

We now claim I must be prime. Suppose aI, bI, but $ab \in I$. Then $I + (a) \supsetneq I$, so $I + (a)$ is finitely generated, say by $i_1 + r_1 a, \dots, i_n + r_n a$. Define $J = \{s \in R : sa \in I\} \supseteq I + (b) \supsetneq I$. Again, J is finitely generated.

Take $t \in I \subset I + (a)$, so $t = u_1(i_1 + r_1 a) + \dots + u_n(i_n + r_n a)$ for some $u_i \in R$. So $t = u_1 i_1 + \dots + u_n i_n + (u_1 r_1 + \dots + u_n r_n)a \in (i_1) + (i_2) + \dots + (i_n) + Ja$.

Hence $I \subseteq (i_1) + \dots + (i_n) + Ja$, so $I = (i_1) + \dots + (i_n) + Ja$, so I is finitely generated $\lightning$.

So I must be prime, but then by our hypothesis I is still finitely generated $\lightning$. So R must be noetherian. $\square$

We will also use the following lemma:

Lemma 1.10. *Let P be a prime ideal of $R[[x]]$ and $\theta : R[[x]] \to R$, $x \mapsto 0$. Then P is finitely generated if and only if $\theta(P)$ is a finitely generated ideal of R.*

Proof. Clearly if P is finitely generated then $\theta(P)$ is.

Conversely, suppose $\theta(P) = Ra_1 + \dots + Ra_n$.

If $x \in P$, then $P = (a_1, \dots, a_n, x)$.

This is immediate - if $g \in P$, $g = a+$ higher order terms. Now $a \in (a_1, \dots, a_n)$, so $g = \sum_i r_i a_i + xg'$ as required.

If xP, then let $f_1, \dots, f_n$ be power series with constant terms $a_1, \dots, a_n$ respectively. Then $P = (f_1, \dots, f_n)$.

Take $g \in p$, say $g = b+$ higher terms, with b the constant term. Then $b = \sum b_i a_i$, so $g - \sum b_i f_i = g_1 x$ for some g_1. Note that $g_1 x \in P$, P is prime, and xP, so $g_1 \in P$. Similarly, $g_1 = \sum c_i f_i + g_2 x$, and $g_2 \in P$. Continuing, we get $h_1, \dots, h_n \in R[[x]]$, where $h_i = b_i + c_i x + \dots$ with $g = h_1 f_1 + \dots + h_n f_n$. $\square$

We are now ready to give the second proof the R noetherian implies $R[[x]]$ noetherian:

Proof 2. Suppose P is a prime ideal of $R[[x]]$. Then P is finitely generated iff $\theta(P)$ is. But R is noetherian, so $\theta(P)$ is finitely generated, so P was finitely generated. Then we apply Cohen's theorem to get $R[[x]]$ noetherian. □

1.1 Ideal Structure

Here, we assume R is a commutative ring with a 1, not necessarily noetherian.

Lemma 1.11. *The set $N(R)$ of all nilpotent[1] elements of R is an ideal, and $R/N(R)$ has no nonzero nilpotent elements.*

Proof. If $x \in N(R)$, then $x^m = 0$ for some m. Hence $(rx)^m = 0$ for all $r \in R$, and so $rx \in N(R)$.

If $x, y \in N(R)$, then $x^n = 0, y^m = 0$ for some n, m. Then $(x+y)^{n+m-1}$ expands to give terms $\lambda x^s y^t$ where $s + t = m + n - 1$. So either $s \geq n$ or $y \geq m$, so all the terms are zero, and $x + y \in N(R)$.

So $N(R) \lhd R$.

Finally, if $s \in R/N(R)$ then $s = x + N(R)$. Note that $s^n = x^n + N(R)$ for all n. If $x + N(R)$ is nilpotent then $(x + N(R))^m = N(R)$ for some m, and hence $x^m \in N(R)$. So x^m is nilpotent, and $(x^m)^n = x^{mn} = 0$ for some n. But then x is nilpotent, so $x + N(R) = 0 + N(R)$. □

Definition 1.12. *$N(R)$ is called the* **nilradical** *of R.*

[1]An element x of a ring is called nilpotent if there is some integer m such that $x^m = 0$.