Commutative Algebra

Alec Zabel-Mena

June 6, 2023

Contents

Chapter 1

Preliminaries

We assume that all rings are commutative, and have identity.

1.1 Multivariate Polynomial Rings

Theorem 1.1.1. *Let I be an ideal of R and $I[x]$ the ideal of $R[x]$ generated by I. Then*

$$R[x]/_{I[x]} \simeq R/_{I}[x]$$

Moreover, if I is a prime ideal in R, then $I[x]$ is a prime ideal in $R[x]$.

Proof. Consider the map $\pi : R[x] \to R/_{I}[x]$ given by $f \to f \mod I$. That is, reduce f modulo I. Then π is a ring homomorphism with kernel $\ker \pi = I[x]$. By the first isomorphism theorem, we get

$$R[x]/_{I[x]} \simeq R/_{I}[x]$$

Now, let I be a prime ideal in R, Then we have that $R/_{I}$ is an integral domain, hence, so is $R/_{I}[x]$, which makes $I[x]$ a prime ideal of $R[x]$. ■

Example 1.1. Consider the ideal $n\mathbb{Z}$ in $\mathbb{Z}$. By above, we have

$$\mathbb{Z}[x]/_{n\mathbb{Z}[x]} \simeq \mathbb{Z}/_{n\mathbb{Z}}[x]$$

with natural map reduction of polynomials modulo n. If n is composite, then the ring $\mathbb{Z}/_{n\mathbb{Z}}[x]$ is not an integral domain. If $n = p$ a prime, then $\mathbb{Z}/_{n\mathbb{Z}}[x]$ is an integral domain.

Definition. We define the **polynomial ring** in n **variables** $x_1, \dots, x_n$ with **coefficients** in R inductively to be

$$R[x_1, \dots, x_n] = R[x_1, \dots, x_{n-1}][x_n]$$

and is the set of all **multivariate polynomials** of the form $f(x_1, \dots, x_n) = \sum a x_1^{d_1} \dots x_n^{d_n}$. We call the monic term $x_1^{d_1} \dots x_n^{d_n}$ of f a **monomial**. We define the **degree** of a monomial to be $\deg x_1^{d_1} \dots x_n^{d_n} = d_1 + \dots + d_n$ and we define the **degree** of f to be $\deg f = \max \{\deg x_1^{d_1} \dots x_n^{d_n}\}$ (i.e. the maximum degree of all monomials of f). If all the monomials of f have the same degree, we call f **homogeneous**, or, a **form**.

Lemma 1.1.2. *Let R be a ring. Then $R[x_1, \ldots, x_n]$ is a ring.*

Example 1.2. (1) Consider the polynomial ring $\mathbb{Z}[x, y]$ in two variables x and y with integer coefficients. Then $p(x, y) = 2x^3 + xy - y^2$ and has $\deg p = 3$. The polynomial $q(x, y) = -3xy + 2y^2 + x^2y^3$ has $\deg q = 5$. The sum

$$p + q(x, y) = 2x^3 - 2xy + y^2 + x^2y^3 \text{ has degree } \deg p + q = 5$$

and the product

$$pq(x, y) = -6x^4y + 4x^3y^2 + 2x^5y^3 - 3x^2y^2 + 5xy^3 + x^3y^4 - 2y^4 - x^2y^5$$

had degree $\deg pq = 8$.

(2) The polynomial $p(x, y, z) = 4y^2z^5 - 3xy^3z + 2x^2y$ over $\mathbb{Z}[x, y, z]$ has degree $\deg p = 7$ and the polynomial $q(x, y, z) = 5x^2y^3z^4 - 9x^2z + 7x^2$ has degreee $\deg q = 9$. The polynomials

$$p + q(x, y, z) = 5x^2y^3z^4 + 4y^2z^5 - 3xy^3z + 2x^2y - 9x^2z + 7x^2$$

and

$$pq(x, y, z) = 20x^2y^5z^9 - 15x^3y^6z^5 + 10x^4y^4z^4 - 36x^2y^2z^6 + 28x^2y^2z^5 + 27x^3y^3z^2 - 21x^3y^3z - 18x^4yz + 14x^4y$$

have degrees $\deg(p + q) = 9$ and $\deg pq = 16$, respectively.

(3) Consider the polynomials p and q of the above example over $\mathbb{Z}/3\mathbb{Z}$, i.e. as polynomials in $\mathbb{Z}/3\mathbb{X}[x, y, z]$. Then we have

$$\begin{aligned} p(x, y, z) &= xy^2z^5 + 2x^2y \\ q(x, y, z) &= 2x^2y^3z^4 + x^2 \end{aligned}$$

which makes

$$p + q(x, y, z) = 2x^2y^3z^4 + y^2z^5 + 2x^2y + x^2$$

and

$$pq(x, y, z) = 2x^2y^5z^9 + 1x^4y^4z^4 + 1x^2y^2z^5 + 14x^4y$$

of degrees $\deg(p + q) = 9$ and $\deg pq = 16$, still.

Lemma 1.1.3. *Let R be a commutative ring, and π a permutation of the set $\{1, \ldots n\}$. Then $R[x_1, \ldots, x_n] \simeq R[x_{\pi(1)}, \ldots, x_{\pi(n)}]$. That is, multivariate polynomial rings are independent of the ordering of their variables.*

Proof. Define the map $\Pi : R[x_1, \ldots, x_n] \to R[x_{\pi(1)}, \ldots, x_{\pi(n)}]$ termwise by first sending $x_1 \ldots x_n \to x_{\pi(1)} \ldots x_{\pi(n)}$. Then notice that Π defines a ring homomorphism, and moreover, for any $f \in R[x_1, \ldots, x_n]$, Π permutes the terms of f. So that Π dictates the required isomorphism. ∎

Example 1.3. (1) Consider the ideals (x) and (x, y) in $\mathbb{Q}[x, y]$. We have that (x) is a prime ideal in $\mathbb{Q}[x, y]$, since $\mathbb{Q}[x, y] \simeq \mathbb{Q}[y, x] = \mathbb{Q}[y][x]$. Moreover, let $fg \in (x, y)$ so that $fg(x, y) = xyr(x, y)$ for some $r \in \mathbb{Q}[x, y]$. Then $xy|fg$ which makes $xy|f$ or $xy|g$, so that $f \in (x, y)$ or $g \in (x, y)$. This makes (x, y) a prime ideal. Notice, however, that $(x) \subseteq (x, y)$, so that (x) is not maximal. (x, y), however is a maximal ideal in $\mathbb{Q}[x, y]$.

(2) Notice that (x, y) is a prime ideal in $\mathbb{Z}[x, y]$, since $\mathbb{Z}[x, y]$ is a subring of $\mathbb{Q}[x, y]$, and (x, y) is prime in $\mathbb{Q}[x, y]$. Similarly, $(2, x, y)$ is prime in $\mathbb{Z}[x, y]$. Notice however that $(x, y) \subseteq (2, x, y)$ so that (x, y) is not maximal in $\mathbb{Z}[x, y]$; $(2, x, y)$ is maximal in $\mathbb{Z}[x, y]$.

(3) Notice that (x, y) is not a principle ideal in $\mathbb{Q}[x, y]$. Suppose that it were, then $(x, y) = (f)$ for some $f(x, y) \in \mathbb{Q}[x, y]$. Then we have that $x \in (f)$ and $y \in (f)$ so that $f|x$ and $f|y$. That is, $x = f(x, y)r(x, y)$ and $y = f(x, y)q(x, y)$. Then $x + y = f(x, y)(r(x, y) + q(x, y))$. Notice also that $\deg f \leq 1$. Then if $\deg f = 0$, f is a unit, and we get $(f) = \mathbb{Q}[x, y]$. On the other hand, if $\deg f = 1$, and since $x + y = f(x, y)(r(x, y) + q(x + y))$, we have that

1.2 Noetherian Rings

Definition. Let R be a ring. We call a nondecreasing sequence $\{I_n\}_{n \in \mathbb{Z}^+}$ of ideals of R an **ascending chain of ideals**. We call R **Noetherian** if it satisfies the **ascending chain considition**; that is, if $\{I_n\}$ is an ascending chain of ideals of R, then there exists an $m \in \mathbb{Z}^+$ for which $I_n = I_m$ for all $n \geq n$.

Lemma 1.2.1. *If I is an ideal of a Noetherian ring R, then the factor ring ${}^{R}\!/_{I}$ is also Noethrian. In particular, the image of a Noetherian ring under any ring homomorphism is Noetherian.*

Proof. This follows by the isomorphism theorems for ring homomorphisms. ∎

Theorem 1.2.2. *The following are equivalent for any ring R.*

(1) R is Noetherian.

(2) Every nonempty collection of ideals of R contains a maximal element under inclusion.

(3) Every ideal of R is finitelt generated.

Proof. Let R be Noetherian, and let $\mathcal{I}$ an nonempty collection of ideals of R. Choose an ideal $I_1 \in \mathcal{I}$. If I_1 is maximal, we are done. If not, then there is an ideal $I_2 \in \mathcal{I}$ for which $I_1 \subseteq I_2$. Now, if I_2 is maximal, we are done. Otherwise, proceeding inductively, if there are no maximal ideals of R in $\mathcal{I}$, then by the axiom of choice, construct the infinite strictly increasing chain

$$\dots \subseteq I_1 \subseteq I_2 \subseteq \dots$$

of ideal of R. This contradicts that R is Noetherian, so $\mathcal{I}$ must contain a maximal element.

Now, suppose that any nonempty collection of ideals of R contains a maximal element. Let $\mathcal{I}$ the collection of all finitely generated ideals of R, and let I be any ideal of R. By hypothesis, $\mathcal{I}$ has a maximal element I'. Now suppose that $I \neq I'$, and choose an $x \in I \backslash I'$, then the ideal generated by I' and x is finitely generated, and so is in $\mathcal{I}$; but that contradicts the maximality of I'. Therefore we must have $I = I'$.

Finally, suppose every ideal of R is finitely genrated, and let $I = (a_1, \dots, a_n)$. Let

$$I_1 \subseteq I_2 \subseteq \dots$$

an ascending chain of ideals of R for which

$$I = \bigcup_{n \in \mathbb{Z}^+} I_n$$

Since $a_i \in I$ for each $1 \leq j \leq n$, we have that $a_i \in I_{i_j}$ and $i \in \mathbb{Z}^+$. Now, let $m = \max\{j_1, \dots, j_n\}$ and coinsider the ideal I_m. Then $a_i \in I_m$ for each i, which makes $I \subseteq I_m$. That is, $I_n = I_m$ for some $n \geq m$; which makes R Noetherian. ■

Example 1.4. (1) Every principle ideal domain (PID) is Noetherian, since any collection of ideals has a maximal element.

(2) The rings $\mathbb{Z}$, $\mathbb{Z}[i]$, and $k[x]$ (where k is a field) are Noetherian.

(3) The multivariate polynomial ring $\mathbb{Z}[x_1, x_2, \dots]$ is not Noetheria, since the ideal $(x_1, x_2, \dots)$ is not finitely generated.

Theorem 1.2.3 (Hilbert's Basis Theorem)**.** *If R is a Noetherian ring, then so is the polynomial ring $R[x]$.*

Proof. Let I be an ideal of $R[x]$, and let L be the set of all leading coefficients of polyonimials in I. Notice that since $0 \in I$, then $0 \in L$, so that L is nonempty. Moreover, let $f(x) = ax^d + \dots$ and $g(x) = bx^e + \dots$ polynomials in I of degree $\deg f = d$ and $\deg g = e$, with leading coefficients $a, b \in R$. Then for any $r \in R$, we have the coefficient $ra - b = 0$, or $ra - b$ is the leading coefficient of the polynomial $rx^e f - x^d g \in I$. In either case, we get $ra - b \in L$. This makes L an ideal of R. Now, since R is Noetherian L is finitely generated ; let $L = (a_1, \dots, a_n)$. Then for every $1 \leq i \leq n$, let $f_i \in I$ the polynomial of degree $\deg f_i = e_i$ whose leading coefficient is a_i. Take, then $N = \max\{e_1, \dots, e_n\}$. Then for any $d \in \mathbb{Z}/N\mathbb{Z}$, let L_d be the set of all leading coefficients of polynomials in I, of degree d, together with 0. Let $f_{di} \in I$ a polynomial of degree $\deg f_{di} = d$ with leading coefficient b_{di}. We wish to show that

$$I = (f_1, \dots, f_n) \cup (f_{d1}, \dots f_{nd})$$

Let $I' = (f_1, \dots, f_n) \cup (f_{d1}, \dots f_{nd})$. By construction, since the generators were chosen from I, $I' \subseteq I$. Now, if $I \neq I'$. Then there is a nonzero polynomial $f \in I$ of minimum degree not contained in I' (i.e $f \notin I'$). Let $\deg f = d$, and let a be the leading coefficient of f. Suppose that $d \geq N$. Since $a \in L$, a is an R-linear combination of the generators of L; i.e.

$$a = r_1 a_1 + \dots + r_n a_n$$

where $r_1, \dots, r_n \in R$. Let

$$g = r_1 x^{d-e_1} f_1 + \dots + r_n x^{d-e_n} f_n$$

then $g \in I'$ and has degree $\deg g = d$ and leading coefficient a. Hence $f - g \in I'$ is of smaller degree, and by the minimality of f, $f - g = 0$, which makes $f = g \in I'$; a contradiction. THerefore $I = I'$

Now, if $d < N$, then $a \in L_d$, and so is an R-linear combniation of generators of L_d; that is

$$a = r_1 b_{d1} + \cdots + r_n b_{dn}$$

where $r_1, \ldots, r_n \in R$. Then let

$$g = r_1 f_{d1} + \cdots + r_n f_{dn}$$

then $g \in I'$ is a polynomial of degree $\deg g = d$ and leading coefficient a; which gives us the above contraditction.

Therefore, $I = I'$, and since I' is finitely generated, $R[x]$ is Noetherian. ■

Corollary. *Let k be a field. Then the polynomial ring in n variables $k[x_1, \ldots, x_n]$ is Noetherian.*

Definition. Let k be a field. We call a ring R a **k-algebra** if k is contained in the center of R (i.e. $k \subseteq Z(R)$), and $1_k = 1_R$. We call R a **finitely generated** k-algbera if R is generated by k together with a finite set $\{r_1, \ldots, r_n\}$ of elements of R.

Definition. Let k be a field and R and S k-algebras. We call a map $\phi : R \to S$ a **k-algebra homomorphism** if ϕ is a ring homomorphism, and ϕ is the identity on k.

Lemma 1.2.4. *Let k be a field. Then a ring R is a finitely generated k-algebra if, and only if there exists a k-algebra homomorphism $\phi : k[x_1, \ldots, x_n] \to R$ taking $k[x_1, \ldots, x_n]$ onto R.*

Proof. If R is generated by elements $r_1, \ldots, r_n$ as a k-algebra, then define the map $\phi : k[x_1, \ldots, x_n] \to R$ by taking $x_i \to r_i$, for all $1 \leq i \leq n$, and $\phi(a) = a$ for all $a \in k$. Then ϕ extends to a ring homomorphism of $k[x_1, \ldots, x_n]$ onto R.

Conversly, let ϕ be a k-algebra homomorphism of $k[x_1, \ldots, x_n]$ onto R, such that the images $\phi(x_1), \ldots \phi(x_r)$ generate R as a k-algebra. Then R is finitely generated, and since $k[x_1, \ldots, x_n]$ is Notherian by the corollory to Hilbert's basis theorem, R is a quotient of a Noetherian ring, and hence R is Noetherian. This makes R a finitely generated k-algebra. ■

Example 1.5. Let R be a k-algebra, for some field k, viewed as a finite dimensional vector space over k. In particular, let $R = {}^{k[x]}\!/_{(f(x))}$, where $f(x)$ is a nonzero polynomial over k. Then R is a finitely generated k-algebra, since it has a finite basis, and that basis serves as a generator for R as a k-algebra. Thus, we have the ideals of R are k-subspaces. Moreover, any ascending chain of ideals of R has at most $\dim_k R - 1$ distinct terms, which means that R satisfies the ascending chain condition.

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.