Kendig, Elementary Algebraic Geometry

lattices, it is natural to ask in specific cases if these lattices satisfy any chain conditions or are distributive. We can then formulate possible decomposition theorems. In this and the next section we do this for an important class of rings occurring in algebraic geometry.

Definition 3.1. Let R be a ring and suppose the associated p.o. set $(\mathscr{I}, \subset)$ satisfies the a.c.c.—that is, each strictly ascending chain of ideals of R, $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \dots$, terminates after finitely many steps. Then by abuse of language, we say that R **satisfies the** a.c.c. Similarly, R **satisfies the** d.c.c. if $(\mathscr{I}, \subset)$ does.

We now turn our attention to proving that the a.c.c. holds for polynomial rings over a field. We begin by giving an equivalent formulation of the a.c.c. on R (Lemma 3.3).

Definition 3.2. A **basis** (or **base**) **for an ideal** $\mathfrak{a}$ in R is any collection $\{a_\gamma\}$ of elements $a_\gamma \in \mathfrak{a}$ (γ in some indexing set Γ) such that

$$\mathfrak{a} = \{r_{\gamma_1}a_{\gamma_1} + \dots + r_{\gamma_k}a_{\gamma_k} \,|\, r_{\gamma_i} \in R \text{ and } \gamma_i \in \Gamma\}.$$

We write $\mathfrak{a} = (\{a_\gamma\})$, or $\mathfrak{a} = (a_1, a_2, \dots)$ if Γ is countable, and $\mathfrak{a} = (a_1, \dots, a_n)$ if Γ is finite. If we can write $\mathfrak{a} = (a_1, \dots, a_n)$, we say $\mathfrak{a}$ *has a finite basis.*

Lemma 3.3. *R satisfies the* a.c.c. *iff every ideal of R has a finite basis.*

Proof. $\Rightarrow$: Suppose some ideal $\mathfrak{a}$ did not have a finite basis. Then one could find a sequence of elements $a_1, a_2, \dots$ ($a_k \in \mathfrak{a}$) such that

$$(a_1) \subsetneqq (a_1, a_2) \subsetneqq \dots,$$

and R would not satisfy the a.c.c.

$\Leftarrow$: Suppose R did not satisfy the a.c.c.; let $\mathfrak{a}_1 \subsetneqq \mathfrak{a}_2 \subsetneqq \dots$ be an infinite strict sequence. Then $\mathfrak{a} = \bigcup_j \mathfrak{a}_j$ is an ideal. The ideal $\mathfrak{a}$ cannot have a finite basis $a_1, \dots, a_n$, since surely $a_1 \in \mathfrak{a}_{j_1}$ for some j_1, $a_2 \in \mathfrak{a}_{j_2}$ for some $j_2, \dots,$ and so on. This would mean $\bigcup_{k=1}^n \mathfrak{a}_{jk} = \mathfrak{a}$, so the ideals $\mathfrak{a}_j$ could strictly increase at most up to $\mathfrak{a}_{j_n}$. □

This explains the commonly-used alternate

Definition 3.4. A ring satisfying the a.c.c. is said to satisfy the **finite basis condition**; such a ring is further called **Noetherian**. (This term is named after the German mathematician Emmy Noether (1882–1935), the daughter of Max Noether (1844–1921). M. Noether was the "father of algebraic geometry." E. Noether was a central figure in the development of modern ideal theory.)

If R is any ring, then $R[X]$ as usual denotes the ring of all polynomials in X with coefficients in R.

Our main result of this section is

Theorem 3.5 (Hilbert basis theorem). *If R is Noetherian, so is $R[X]$.*

Before proving it, let us note

Corollary 3.6. *If k is a field, then $k[X_1, \dots, X_n]$ is Noetherian.*

Proof. Certainly k satisfies the a.c.c. since it has only two ideals. Then by repeated application of Theorem 3.5, $k[X_1]$, $k[X_1][X_2] = k[X_1, X_2], \dots,$ $k[X_1, \dots, X_{n-1}][X_n] = k[X_1, \dots, X_n]$ must all be Noetherian. □

Remark 3.7. In the next section we apply the Hilbert basis theorem to get at once decomposition into irreducibles in $\mathscr{I}$, and unique decomposition in $\mathscr{J}$ and in $\mathscr{V}$.

Remark 3.8. The Basis Theorem does not have a dual—that is, no polynomial ring $R[X_1, \dots, X_n]$ where $n \geqslant 1$ ever satisfies the d.c.c.; one strictly descending sequence is always

$$(X_1) \supsetneqq (X_1{}^2) \supsetneqq (X_1{}^3) \supsetneqq \dots.$$

Note on the Hilbert basis theorem

The basis theorem lies at the very foundations of algebraic geometry; it shows there are "fundamental building blocks," in the sense that each variety is uniquely the finite union of irreducible varieties (Theorem 4.4). This is very much akin to the fundamental theorem of arithmetic, which lies at the foundations of number theory; it says that every integer is a product of primes (the "building blocks"), and that this representation is unique (up to order and units.) The essential idea of the basis theorem, though couched in older language, led at once to a solution of one of the outstanding unsolved problems of mathematics in the period 1868–1888, known as "Gordan's problem" (in honor of Paul Gordan).

Gordan's computational abilities were recognized as a youth, and he became the world's leading expert in unbelievably extended algorithms in a field of mathematics called *invariant theory*. In 1868 he found a long, computational proof of the basis theorem for two variables which showed, in essence, how to construct a specific base for a given ideal. Proving the generalization to n variables defied the attempts of some of the world's most distinguished mathematicians. All their attempts were along the same basic path that Gordan followed and, one by one, they became trapped in a dense jungle of complicated algebraic computations.

Now it was Hilbert's belief that the trick in doing mathematics is to start at the right end, and there can hardly be a more beautiful example of this than Hilbert's own solution to Gordan's problem. He looked at it as an *existence* problem rather than as a *construction* problem (wherein a basis is actually produced). In a short notice submitted in 1888 in the *Nachrichten* he showed in the n-variable case the existence of a finite basis for any ideal. Many in the mathematical community reacted by doubting that this was even mathematics; the philosophy of their day was that if you want to prove that something exists, you must explicitly *find* it. Thus Gordan saw the proof as akin to those of theologians for the existence of God, and his comment has become forever famous: "Das ist nicht Mathematik. Das ist Theologie." However, later Hilbert was able to build upon his existence proof, and he actually found a general constructive proof. This served as a monumental vindication of Hilbert's outlook and began a revolution in mathematical thinking. Even Gordan had to admit that theology had its merits. Hilbert's philosophy, so simple, yet so important, may perhaps be looked at this way: If we see a fly in an airtight room and then it hides from us, we still know there is a fly in the room even though we cannot specify its coordinates. Acceptance of this broader viewpoint has made possible some of the most elegant and important contributions to mathematics, and mathematicians of today would find themselves hopelessly straitjacketed by a reversion to the attitude that you must *find* it to show it exists. (For an absorbing account of Hilbert's life and times, see [Reid].)

The following proof is essentially Hilbert's—his language was a bit different, and he took R to be the integers, but the basic ideas are all the same.

Proof of the Basis Theorem. We show that if R satisfies the finite basis condition, then so does $R[X]$. First, if $r_0 X^n + \ldots + r_n$ $(r_0 \neq 0)$ is any nonzero polynomial of $R[X]$, we call r_0 the **leading coefficient** of the polynomial. Now let $\mathfrak{A}$ be any ideal of $R[X]$. Then $\mathfrak{A}$ induces an ideal $\mathfrak{a}$ in R, as well as smaller ideals $\mathfrak{a}_k$ in R, as follows:

Let $\mathfrak{a}$ consist of 0 together with all leading coefficients of all polynomials in $\mathfrak{A}$. (We show that this is an ideal in a moment.) Since R is Noetherian, for some N, $\mathfrak{a} = (a_1, \ldots, a_N)$, where $a_i \in R$. Let $p_i(X) \in \mathfrak{A}$ have a_i as leading coefficient and let $m^* = \max(\deg p_1, \ldots, \deg p_N)$. Then for each $k < m^*$, let $\mathfrak{a}_k$ consist of 0 together with all leading coefficients of all polynomials in $\mathfrak{A}$ whose degree is equal to or less than k.

We now show $\mathfrak{a}$ is an ideal. (The proof for $\mathfrak{a}_k$ is similar.) First, $\mathfrak{a}$ is closed under subtraction, for $a, b \in \mathfrak{a}$ implies that there are polynomials $p(X) = aX^m + \sum_{i=1}^{m} c_i X^{m-i}$ and $q(X) = bX^n + \sum_{i=1}^{n} d_i X^{n-i}$ in $\mathfrak{A}$. Then $m \geqslant n$ implies that $p(X) - (X^{m-n}q(X)) \in \mathfrak{A}$; if $a = b$, then $a - b = 0 \in \mathfrak{a}$, and if $a \neq b$, then $a - b \in \mathfrak{a}$ since $a - b$ is then the leading coefficient of $p(X) - (X^{m-n}q(X))$.

Second, $\mathfrak{a}$ has the absorption property, for if $r \in R$, then $r \neq 0$ implies that the leading coefficient of $rp(X)$ is $ra \in \mathfrak{a}$, and $r = 0$ implies that $ra = 0 \in \mathfrak{a}$.

Now write $\mathfrak{a}_k = (a'_{k1}, \ldots, a'_{kn_k})$, and let $q_1(X), \ldots, q_M(X)$ be polynomials of $\mathfrak{A}$ whose leading coefficients are the basis elements a'_{kj} of the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_{m^*-1}$. We claim that

$$\mathfrak{A} = (p_1, \ldots, p_N, q_1, \ldots, q_M). \tag{5}$$

Let us denote $(p_1, \ldots, p_N, q_1, \ldots, q_M)$ by $\mathfrak{A}^\dagger$; we show $\mathfrak{A} = \mathfrak{A}^\dagger$. Since all polynomials p_i and q_j were chosen from $\mathfrak{A}$, obviously $\mathfrak{A}^\dagger \subset \mathfrak{A}$. We show $\mathfrak{A} = \mathfrak{A}^\dagger$ by assuming $\mathfrak{A}^\dagger \subsetneqq \mathfrak{A}$ and deriving a contradiction. Thus if $\mathfrak{A}^\dagger \subsetneqq \mathfrak{A}$, let p be any polynomial of lowest degree which is in $\mathfrak{A}$ but not in $\mathfrak{A}^\dagger$. We may write p's leading coefficient as $a = \sum_{i=1}^{N} r_i a_i$. Now surely either $\deg p \geqslant m^*$ or $\deg p < m^*$. Suppose first that $\deg p \geqslant m^*$. This would imply there are monomials $m_i(X) \in R[X]$ such that $\sum_i m_i p_i$ has the same leading term as p. (Specifically, if we take m_i to be $r_i(X^{\deg p - \deg p_i})$, then

$$\sum r_i(X^{\deg p - \deg p_i})p_i \tag{6}$$

has leading term $aX^{\deg p}$. The effect of $X^{\deg p - \deg p_i}$ is to "jack up" the degree of each p_i so that all the N summands in (6) have the same degree. This is possible since $\deg p - \deg p_i \geqslant 0$ for each $i = 1, \ldots, N$.) We thus get

$$\deg((\textstyle\sum m_i p_i) - p) < \deg p.$$

But p is a polynomial of lowest degree which is in $\mathfrak{A}$ and not in $\mathfrak{A}^\dagger$. Thus $(\sum m_i p_i) - p \in \mathfrak{A}^\dagger$. But surely also $\sum m_i p_i \in \mathfrak{A}^\dagger$, so $p \in \mathfrak{A}^\dagger$, a contradiction.

Now suppose $\deg p < m^*$. Now we may use the q_i! For some monomials $v_i(X) \in R[X]$, we have

$$\deg((\textstyle\sum v_i q_i) - p) < \deg p,$$

so as before, $p \in \mathfrak{A}^\dagger$.

Thus p cannot exist, (5) holds, and the basis theorem is proved. □

Exercises

3.1 Follow through the proof of the basis theorem for the ideal $\mathfrak{A} \subset \mathbb{Z}[X]$, where $\mathfrak{A}$ is generated by the set $\{2nX + 3m \mid n \text{ and } m \text{ positive integers}\}$ to arrive at $\mathfrak{A} = (2X, 3)$.

3.2 Let the ideal $\mathfrak{A} \subset \mathbb{C}[X]$ be generated by $\{n + X^n \mid n \in \mathbb{Z}^+\}$. Use the proof of the basis theorem to find a single generator of $\mathfrak{A}$.

4 Some basic decomposition theorems on ideals and varieties

Now that we have proved the Hilbert basis theorem we may apply it, together with the basic decomposition theorems of lattice theory, to reap some of the important decomposition results of algebraic geometry.