A QUICK REVIEW OF COMMUTATIVE ALGEBRA

SUDHIR R. GHORPADE

Department of Mathematics, Indian Institute of Technology, Mumbai 400 076, India
E-Mail : srg@math.iitb.ac.in

Abstract. These notes attempt to give a rapid review of the rudiments of Classical Commutative Algebra. Proofs of several of the results are also outlined.

Contents

Date: Ferbruary 2, 2000.

This is a slightly revised and expanded version of the first chapter of the Lecture Notes of the NBHM sponsored Instructional Conference on Combinatorial Topology and Algebra, held at IIT Bombay in December 1993. The subsequent chapters in the Algebra part consisted of the following topics: Primary Decompositions of Modules (S. R. Ghorpade and J. K. Verma), Dimension Theory (Balwant Singh), Cohen-Macaulay Modules (Vijaylaxmi Trivedi), Face Rings of Simplicial Complexes (J. K. Verma) and Upper Bound Theorem (R. C. Cowsik). Comments, corrections and criticism regarding these notes are most welcome and may please be communicated to the author.

1. Basic Constructions

Polynomials are among the most basic objects in Algebra. So let us talk about them first. Given a ring[1] A, we denote by $A[X_1, \ldots, X_n]$ the ring of all polynomials in the variables $X_1, \ldots, X_n$ with coefficients in A. Elements of $A[X_1, \ldots, X_n]$ look like

$$f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}, \qquad a_{i_1 \ldots i_n} \in A,$$

where $(i_1, \ldots, i_n)$ vary over a finite set of nonnegative integral n–tuples. A typical term (excluding the coefficient), viz., $X_1^{i_1} \ldots X_n^{i_n}$, is called a *monomial*; its (usual) *degree* is $i_1 + \cdots + i_n$. Such a monomial is said to be *squarefree* if $i_r \leq 1$ for $1 \leq r \leq n$. If $f \neq 0$, then the (total) *degree* of f is defined by $\deg f = \max\{i_1 + \cdots + i_n : a_{i_1 \ldots i_n} \neq 0\}$. Usual convention is that $\deg 0 = -\infty$. A *homogeneous polynomial* of degree d in $A[X_1, \ldots, X_n]$ is simply a finite A–linear combination of monomials of degree d. The set of all homogeneous polynomials of degree d is denoted by $A[X_1, \ldots, X_n]_d$. Note that any $f \in A[X_1, \ldots, X_n]$ can be uniquely written as $f = f_0 + f_1 + \ldots$, where $f_i \in A[X_1, \ldots, X_n]_i$ and $f_i = 0$ for $i > \deg f$; we may call f_i's to be the *homogeneous components* of f. If $f \neq 0$ and $d = \deg f$, then clearly $f_d \neq 0$ and $f = f_0 + f_1 + \cdots + f_d$. An ideal I of $A[X_1, \ldots, X_n]$ is said to be a *homogeneous ideal* (resp: *monomial ideal*) if it is generated by homogeneous polynomials (resp: monomials). Lastly, we remark that when we use a notation such as $k[X_1, \ldots, X_n]$, it will be tacitly assumed that k denotes a field and $X_1, \ldots, X_n$ are independent indeterminates over k (and, of course, n denotes a nonnegative integer).

(1.1) Exercise: Show that the monomials of degree d in $k[X_1, \ldots, X_n]$ form a k–vector space basis of $k[X_1, \ldots, X_n]_d$. Further, show that $\dim_k k[X_1, \ldots, X_n]_d = \binom{n+d-1}{d}$.

Forming rings of polynomials over a given ring is one of the three fundamental processes in Algebra of constructing new rings from given rings. The other two are as follows.

Quotient Ring: That is, the residue class ring A/I obtained by 'moding out' an ideal I from a ring A. This is same as taking a homomorphic image. Passing to A/I from A has the effect of making I the null element. We have a natural surjective homomorphism $q : A \to A/I$ given by $q(x) = x + I$ for $x \in A$. There is a one-to-one correspondence between the ideals of A containing I and the ideals of A/I given by $J \mapsto q(J) = J/I$ and $J' \mapsto q^{-1}(J')$.

Localisation: That is, the ring of fractions $S^{-1}A$ of a ring A w.r.t. a multiplicatively closed (m. c.) subset S of A [i.e., a subset S of A such that $1 \in S$ and $a, b \in S \Rightarrow ab \in S$]. Elements of $S^{-1}A$ are, essentially, fractions of the type $\frac{a}{s}$, where $a \in A$ and $s \in S$; the notion of equality in $S^{-1}A$ is understood as follows. $\frac{a}{s} = \frac{b}{t} \Leftrightarrow u(at - bs) = 0$, for some $u \in S$. Quite often, we consider $S^{-1}A$ when A is a domain and $0 \notin S$; in this case, the notion of equality (or, if you like, equivalence) is simpler and more natural. Note that if A is a domain and $S = A \setminus \{0\}$, then $S^{-1}A$ is nothing but the quotient field of A. Important instance of localisation is when $S = A \setminus \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A; in this case $S^{-1}A$ is customarily denoted by $A_\mathfrak{p}$. Passing from A to $A_\mathfrak{p}$ has the effect of making $\mathfrak{p}$ into a maximal ideal that consists of all nonunits; indeed, $A_\mathfrak{p}$ is a *local ring* [which means, a ring with a unique maximal ideal] with $\mathfrak{p}A_\mathfrak{p}$ as its unique maximal ideal. In general, we have a natural homomorphism

[1] here, and hereafter, by a ring we mean a commutative ring with identity.

$\phi : A \to S^{-1}A$ defined by $\phi(x) = \frac{x}{1}$. This is injective if S consists of nonzerodivisors, and in this case A may be regarded as a subring of $S^{-1}A$. Given an ideal I of A, the ideal of $S^{-1}A$ generated by $\phi(I)$ is called the *extension* of I, and is denoted by $IS^{-1}A$ or by $S^{-1}I$. For an ideal J of $S^{-1}A$, the inverse image $\phi^{-1}(J)$ is an ideal of A and is called the contraction of J to A. By abuse of language, the contraction of J is sometimes denoted by $J \cap A$. We have $S^{-1}(J \cap A) = J$ and $S^{-1}I \cap A \supseteq I$, and the last inclusion can be strict. This implies that there is a one-to-one correspondence between the ideals J of $S^{-1}A$ and the ideals I of A such that $\{a \in A : as \in I \text{ for some } s \in S\} = I$. This, in particular, gives a one-to-one correspondence between the prime ideals of $S^{-1}A$ and the prime ideals P of A such that $P \cap S = \emptyset$.

(1.2) Exercise: Show that localisation commutes with taking homomorphic images. More precisely, if I is an ideal of a ring A and S is a m. c. subset of A, then show that $S^{-1}A/S^{-1}I \simeq \bar{S}^{-1}(A/I)$, where $\bar{S}$ denotes the image of S in A/I.

Given ideals I_1 and I_2 in a ring A, their *sum* $I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1,\ a_2 \in I_2\}$, their *product* $I_1I_2 = \{\sum a_ib_i : a_i \in I_1,\ b_i \in I_2\}$, and intersection $I_1 \cap I_2$ are all ideals. Analogue of division is given by the *colon ideal* $(I_1 : I_2)$, which is defined to be the ideal $\{a \in A : aI_2 \subseteq I_1\}$. If I_2 equals a principal ideal (x), then $(I_1 : I_2)$ is often denoted simply by $(I_1 : x)$. We can also consider the *radical* of an ideal I, which is defined by $\sqrt{I} = \{a \in A : a^n \in I \text{ for some } n \geq 1\}$, and which is readily seen to be an ideal (by Binomial Theorem!). One says that I is a *radical ideal* if $\sqrt{I} = I$. Note that the notions of sum and intersections of ideals extend easily to arbitrary families of ideals.

(1.3) Exercise: Show that colon commutes with intersections. That is, if $\{I_i\}$ is a family of ideals of a ring A, then for any ideal J of A, we have $\cap(I_i : J) = (\cap I_i : J)$. Further, if $\{I_i\}$ is a finite family, then show that $\sqrt{\cap I_i} = \cap\sqrt{I_i}$. Give examples to show that these results do not hold (for finite families) if intersections are replaced by products.

(1.4) Exercise: Let $A = k[X_1, \ldots, X_n]$ and I be an ideal of A. Show that I is a homogeneous ideal iff I contains the homogeneous components of f, for each $f \in I$. Also show that I is a monomial ideal iff I contains all the monomials occurring in f, for each $f \in I$. Further show that if I is generated by monomials $m_1, \ldots, m_r$ and u is any monomial in A, then $u \in I$ iff u is divisible by m_i for some i. Use the fact that A is a UFD to deduce that a monomial ideal is a radical ideal iff it is generated by squarefree monomials.

Here is a prime fact about ideals whose mention can not be avoided.

(1.5) Prime Avoidance Lemma. Let I, $P_1, \ldots, P_n$ be ideals in a ring A such that $P_1, \ldots, P_n$ are prime and $I \subseteq \cup_{j=1}^{n} P_j$. Then $I \subseteq P_j$ for some j.

Proof: Suppose $n > 1$. If there exist $x_i \in I \setminus \cup_{j \neq i} P_j$ for $1 \leq i \leq n$, then we have a contradiction since $x_1 + x_2x_3 \ldots x_n \in I \setminus \cup_i P_i$. Thus $I \subseteq \cup_{j \neq i} P_j$, for some i. The case of $n = 1$ being trivial, the result now follows using induction on n. □

Remark: An easy alteration of the above proof shows that (1.5) holds under the weaker hypothesis that I is a subset of A closed under addition and multiplication, and $P_1, \ldots, P_n$ are ideals of A such that at least $n-2$ of them are prime. In the case A contains a field, then

(1.5) can be proved, using elementary vector space arguments, without assuming any of the P_i's to be prime.

2. Noetherian Rings

A ring A is said to be *noetherian* if every ideal of A is finitely generated. It is easy to see that this condition equivalent to either of the two conditions below.

1. (Ascending Chain Condition or a.c.c.) If $I_1, I_2, \ldots$ are ideals of A such that $I_1 \subseteq I_2 \subseteq \ldots$, then there exists $m \geq 1$ such that $I_n = I_m$ for $n \geq m$.
2. (Maximality Condition) Every nonempty set of ideals of A has a maximal element.

The class of noetherian rings has a special property that it is closed w.r.t. each of the three fundamental processes. Indeed, if A is a noetherian ring, then it is trivial to check that both A/I and $S^{-1}A$ are noetherian, for any ideal I of A and any m. c. subset S of A; moreover, the following basic result implies, using induction, that $A[X_1, \ldots, X_n]$ is also noetherian.

(2.1) Hilbert Basis Theorem. *If A is a noetherian ring, then so is $A[X]$.*

Proof: Let I be any ideal of $A[X]$. For $0 \neq f \in I$, let $\mathrm{LC}(f)$ denote the leading coefficient of f, and $J = \{0\} \cup \{LC(f) : f \in I,\ f \neq 0\}$. Then J is an ideal of A and so we can find $f_1, \ldots, f_r \in I \setminus \{0\}$ such that $J = (\mathrm{LC}(f_1), \ldots, \mathrm{LC}(f_r))$. Let $d = \max\{\deg f_i : 1 \leq i \leq r\}$. For $0 \leq i < d$, let $J_i = \{0\} \cup \{LC(f) : f \in I,\ \deg f = i\}$; then J_i is an ideal of A and so we can find $f_{i1}, \ldots, f_{ir_i} \in I$ such that $J_i = (\mathrm{LC}(f_{i1}), \ldots, \mathrm{LC}(f_{ir_i}))$. Now if I' is the ideal of $A[X]$ generated by $\{f_1, \ldots, f_r\} \cup \{f_{ij} : 0 \leq i < d,\ 1 \leq j \leq r_i\}$, then $I' \subseteq I$ and for any $0 \neq f \in I$, there is $f' \in I'$ such that $\deg(f - f') < \deg f$. Thus an inductive argument yields $I = I'$. $\square$

A field as well as a PID (e.g., $\mathbb{Z}$, the ring of integers) is clearly noetherian, and constructing from these, using combinations of the three fundamental processes, we obtain a rather inexhaustible source of examples of noetherian rings. Especially important among these are finitely generated algebras over a field or, more generally, over a noetherian ring. Let us recall the relevant definitions.

Definition: Let B be a ring and A be a subring of B. Given any $b_1, \ldots, b_n \in B$, we denote by $A[b_1, \ldots, b_n]$ the smallest subring of B containing A and the elements $b_1, \ldots, b_n$. This subring consists of all polynomial expressions $f(b_1, \ldots, b_n)$ as f varies over $A[X_1, \ldots, X_n]$. We say that B is a *finitely generated* (f. g.) *A–algebra* or an *A–algebra of finite type* if there exist $b_1, \ldots, b_n \in B$ such that $B = A[b_1, \ldots, b_n]$. Finitely generated k–algebras, where k is a field, are sometimes called *affine rings*.

Ideals in noetherian rings admit a decomposition which is somewhat similar, though much cruder, to the decomposition of positive integers into prime–powers.

Definition: An ideal $\mathfrak{q}$ in a ring A is said to be *primary* if $\mathfrak{q} \neq A$ and for any $a, b \in A$,

$$ab \in \mathfrak{q} \text{ and } b \notin \mathfrak{q} \Longrightarrow a^n \in \mathfrak{q} \text{ for some } n \geq 1.$$

If $\mathfrak{q}$ is a primary ideal, then, clearly, its radical $\sqrt{\mathfrak{q}}$ is prime; if $\mathfrak{p} = \sqrt{\mathfrak{q}}$, then we say that $\mathfrak{q}$ is $\mathfrak{p}$–primary or that $\mathfrak{q}$ is a primary ideal belonging to $\mathfrak{p}$ or that $\mathfrak{q}$ is primary to $\mathfrak{p}$.

Remark: If $\mathfrak{q}$ is an ideal such that $\sqrt{\mathfrak{q}}$ is prime, then $\mathfrak{q}$ needn't be primary; in fact, even a power of a prime ideal can fail to be primary [Example: $\mathfrak{p}^2$, where $\mathfrak{p}$ is the image in $k[X,Y,Z]/(XY-Z^2)$ of (X,Z)]. However, if $\sqrt{\mathfrak{q}}$ is a maximal ideal $\mathbf{m}$, then $\mathfrak{q}$ is easily seen to be $\mathbf{m}$–primary. On the other hand, if $\mathfrak{q}$ is $\mathfrak{p}$–primary, then $\mathfrak{q}$ needn't be a power of $\mathfrak{p}$, even when $\mathfrak{p}$ is maximal [Example: $\mathfrak{q}=(X^2,Y)$ in $k[X,Y]$]. It may be noted, however, that if A is a noetherian ring and $\mathfrak{q}$ is a $\mathfrak{p}$–primary ideal of A, then $\mathfrak{q}$ does contain some power of $\mathfrak{p}$.

(2.2) Theorem. *Let A be a noetherian ring and I be any ideal of A with $I \neq A$. Then we have the following.*

(i) *There exist primary ideals $\mathfrak{q}_1,\ldots,\mathfrak{q}_h$ in A such that $I=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_h$.*

(ii) *In* (i) *above, $\mathfrak{q}_1,\ldots,\mathfrak{q}_h$ can be chosen such that $\mathfrak{q}_i \not\supseteq \cap_{j\neq i}\mathfrak{q}_j$ for $1\leq i\leq h$, and $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$ are distinct, where $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}$.*

(iii) *If $\mathfrak{q}_i$ and $\mathfrak{p}_i$ are as in* (ii) *above, then $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$ are unique; in fact, $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_h\}$ is precisely the set of prime ideals among the ideals $(I:x)$ where x varies over elements of A. Moreover, if $\mathfrak{p}_i$ is minimal among $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$, i.e. $\mathfrak{p}_i\not\supseteq\mathfrak{p}_j$ for $j\neq i$, then the corresponding primary ideal $\mathfrak{q}_i$ is also unique.*

Proof: Classical proof of (i) is in two steps. First, one considers *irreducible ideals*, viz., nonunit ideals that are not finite intersections of strictly larger ideals. The maximality condition readily implies that every ideal of A is a finite intersection of irreducible ideals. Next, if I is irreducible and $ab\in I$ are such that $b\notin I$ and no power of a is in I, then we consider the chain $(I:a)\subseteq(I:a^2)\subseteq\ldots$. By a.c.c., $(I:a^n)=(I:a^{n+1})$ for some n and now it is easy to verify that $I=(I+Aa^n)\cap(I+Ab)$, which is a contradiction. Thus I is primary and (i) is proved. Proving (ii) is easy since if $\mathfrak{p}_i=\mathfrak{p}_j$, then $\mathfrak{q}_i\cap\mathfrak{q}_j$ is primary and it can replace both $\mathfrak{q}_i$ and $\mathfrak{q}_j$ in the decomposition. To prove (iii), let $i\in\{1,\ldots,h\}$. Find $c_i\in(\cap_{j\neq i}\mathfrak{q}_j)\setminus\mathfrak{q}_i$. Then $\mathfrak{q}_i\subseteq(I:c_i)\subseteq\mathfrak{p}_i$, and so there is $k\geq 1$ such that $\mathfrak{p}_i^k\subseteq(I:c_i)$ and $\mathfrak{p}_i^{k-1}\not\subseteq(I:c_i)$. Choose $y\in\mathfrak{p}_i^{k-1}\setminus(I:c_i)$, and let $x_i=yc_i$. Then $\mathfrak{p}_i\subseteq(I:x_i)$ and

$$x\in(I:x_i)\setminus\mathfrak{p}_i\Rightarrow xyc_i\in I\subseteq\mathfrak{q}_i \text{ and } x\notin\mathfrak{p}_i\Rightarrow yc_i\in\mathfrak{q}_i\Rightarrow yc_i\in I\Rightarrow y\in(I:c_i).$$

It follows that $\mathfrak{p}_i=(I:x_i)$. Conversely, if $(I:x)$ is a prime $\mathfrak{p}$ for some $x\in A$, then $\mathfrak{p}=(\cap\mathfrak{q}_i:x)=\cap(\mathfrak{q}_i:x)$, and thus $(\mathfrak{q}_i:x)\subseteq\mathfrak{p}$ for some i. In particular, $x\notin\mathfrak{q}_i$ and $\mathfrak{p}_i=\sqrt{\mathfrak{q}_i}\subseteq\sqrt{(\mathfrak{q}_i:x)}\subseteq\mathfrak{p}$. Also, $a\in\mathfrak{p}\Rightarrow ax\in I\subseteq\mathfrak{q}_i\Rightarrow a\in\mathfrak{p}_i$. Thus $\mathfrak{p}=\mathfrak{p}_i$. Finally, the uniqueness of the primary component $\mathfrak{q}_i$ corresponding to a minimal prime $\mathfrak{p}_i$ can be proved by localising at $\mathfrak{p}_i$. □

Definition: A decomposition $I=\mathfrak{q}_1\cap\cdots\cap\mathfrak{q}_h$, as in (i) above is called a *primary decomposition* of I. If $\mathfrak{q}_1,\ldots,\mathfrak{q}_h$ satisfy the conditions in (ii), then it is called an *irredundant (primary) decomposition* of I; the uniquely determined primes $\mathfrak{p}_1,\ldots,\mathfrak{p}_h$ are called the *associated primes* of I (in A) and the set $\{\mathfrak{p}_1,\ldots,\mathfrak{p}_h\}$ is denoted by $\mathrm{Ass}(A/I)$. An associated prime $\mathfrak{p}_i$ is called a *minimal prime* of I if $\mathfrak{p}_i\not\supseteq\mathfrak{p}_j$ for all $j\neq i$; otherwise $\mathfrak{p}_i$ is called an *embedded prime* of I.

Note that primary decompositions are neatly preserved under the fundamental processes of forming polynomial rings, quotient rings (by smaller ideals), and localisations w.r.t. m. c. subsets that are disjoint from all associated primes. If S is an arbitrary m. c. subset of A and

$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$, then $S^{-1}I = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} S^{-1}\mathfrak{q}_i$ and $S^{-1}I \cap A = \bigcap_{\mathfrak{p}_i \cap S = \emptyset} \mathfrak{q}_i$. Note also that the minimal primes of an ideal I of A are precisely the minimal elements (w.r.t. inclusion) of the set of prime ideals of A containing I.

Example: Let $A = k[X, Y]$ and $I = (X^2, XY)$. Then $I = (X) \cap (X^2, Y)$ gives an irredundant primary decomposition of I. The associated primes of I are $\mathfrak{p}_1 = (X)$ and $\mathfrak{p}_2 = (X, Y)$; clearly, $\mathfrak{p}_1$ is a minimal prime and $\mathfrak{p}_2$ is an embedded prime. Observe that $I = (X) \cap (X^2, Y + cX)$ is also an irredundant primary decomposition of I, for any $c \in k$.

(2.3) Exercise: Let I be a radical ideal and $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h$ be an irredundant primary decomposition of I, where $\mathfrak{q}_i$ is $\mathfrak{p}_i$–primary. Show that $I = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_h$. Deduce that I has no embedded component, and that $\mathfrak{q}_i = \mathfrak{p}_i$ for $1 \leq i \leq h$.

(2.4) Exercise: Let $\mathcal{Z}(A)$ be the set of all zerodivisors of the ring A. Show that $\mathcal{Z}(A) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A/(0))} \mathfrak{p}$. More generally, if I is any ideal of A, then show that $\mathcal{Z}(A/I) = \bigcup_{\mathfrak{p} \in \mathrm{Ass}(A/I)} \mathfrak{p}$, where $\mathcal{Z}(A/I) = \{x \in A : (I : x) \neq I\} \cup \{0\}$.

(2.5) Exercise: Let A be a noetherian ring, n be a nonnegative integer, and $\mathfrak{p}$ be a prime ideal of A. Show that $\mathfrak{p}^n A_\mathfrak{p}$ is a primary ideal of $A_\mathfrak{p}$ and $\mathfrak{p}^n A_\mathfrak{p} \cap A$ is a primary ideal of A. The ideal $\mathfrak{p}^n A_\mathfrak{p} \cap A$ is denoted by $\mathfrak{p}^{(n)}$ and is called the n-th *symbolic power* of $\mathfrak{p}$. Prove that $\mathfrak{p}^n$ has $\mathfrak{p}$ as its unique minimal prime and the (unique) primary component of $\mathfrak{p}^n$ corresponding to $\mathfrak{p}$ is precisely $\mathfrak{p}^{(n)}$.

(2.6) Exercise: Let Δ be a simplicial complex with vertex set $V = \{1, 2, \ldots, n\}$, and let $F_1, F_2, \ldots, F_m$ be the facets (i.e., maximal faces) of Δ. Let I_Δ be the ideal of $k[X_1, \ldots, X_n]$ generated by the squarefree monomials $X_{i_1} \ldots X_{i_r}$ for which $\{i_1, \ldots, i_r\} \notin \Delta$. And for any face F of Δ, let P_F be the ideal of $k[X_1, \ldots, X_n]$ generated by the variables $X_{j_1}, \ldots, X_{j_s}$, where $\{j_1, \ldots, j_s\} = V \setminus F$. Prove that each P_F is a prime ideal and $I_\Delta = P_{F_1} \cap \cdots \cap P_{F_m}$ gives the irredundant primary decomposition of I_Δ.

Reversing the inclusion signs in the definition of noetherian rings, we can consider rings satisfying the descending chain condition (d.c.c.); these are called *artinian rings*. It is easy to see that d.c.c. is equivalent to the condition that every nonempty set of ideals has a minimal element. Also it can readily be seen that quotient rings and localisations of artinian rings are artinian. Unlike a.c.c., the d.c.c. turns out to be a very restrictive condition. Indeed, it can be shown that a ring is artinian iff it is noetherian and every prime ideal is maximal (cf. [AM, p.90]). In particular, an artinian local ring has only one prime ideal and an artinian local domain has to be a field. Note also that an artinian ring has only finitely many prime ideals because each of them must be an associated prime of the minimal radical ideal. Further, it can be seen (from Chinese Remainder Theorem!) that every artinian ring is a direct product of artinian local rings. Basic example of an artinian local ring is $A/\mathfrak{q}$, where A is a noetherian ring and $\mathfrak{q}$ is primary to a maximal ideal of A. To obtain a more specific example, let $f, g \in k[X, Y]$ be polynomials with a common zero, say $P = (\alpha, \beta)$, such that no nonconstant polynomial in

$k[X,Y]$ divides both f and g. Take $A = k[X,Y]_{\mathfrak{p}}$, where $\mathfrak{p} = (X-\alpha, Y-\beta)$ and $\mathfrak{q} = (f,g)A$. Then $\mathfrak{q}$ is primary to the maximal ideal of A, and $A/\mathfrak{q}$ is artinian (verify!).

3. Modules

Let A be a ring. An A–module is simply a vector space except that the scalars come from the ring A instead of a field. Some examples of A–modules are: ideals I of A, quotient rings A/I, localisations $S^{-1}A$, and f. g. A–algebras $A[x_1,\ldots,x_n]$. The notions of submodules, quotient modules, direct sums of modules and isomorphism of modules are defined in an obvious fashion. The concept of localisation (w.r.t. m. c. subsets of A) also carries to A–modules, and an analogue of (1.2) can be verified easily. Direct sum of (isomorphic) copies of A is called a free A–module; $A^n = \underbrace{A \oplus \cdots \oplus A}_{n \text{ times}}$ is referred to as the free A–module of rank n.

Let M be an A–module. Given submodules $\{M_i\}$ of M, their sum

$$\sum M_i = \{\sum x_i : x_i \in M_i \text{ and all except finitely many } x_i\text{'s are } 0\}$$

and their intersection $\cap M_i$ are also submodules of M. Products of submodules doesn't make sense but the colon operation has an interesting and important counterpart. If M_1, M_2 are submodules of M, we define $(M_1 : M_2)$ to be the ideal $\{a \in A : aM_2 \subseteq M_1\}$ of A. The ideal $(0 : M)$ is called the *annihilator* of M and is denoted by $\mathrm{Ann}(M)$; for $x \in M$, we may write $\mathrm{Ann}(x)$ for the ideal $(0 : x)$, i.e., for $\mathrm{Ann}(Ax)$. Note that if I is an ideal of A, then $\mathrm{Ann}(A/I) = I$ and if $\mathrm{Ann}(M) \supseteq I$, then M may be regarded as an A/I–module. Let us also note that for any submodules M_1, M_2 of M, we always have the isomorphisms $(M_1+M_2)/M_2 \simeq M_1/(M_1 \cap M_2)$, and, if $M_2 \subseteq M_1$ and N is a submodule of M_2, $(M_1/N)/(M_2/N) \simeq M_1/M_2$.

We say that M is *finitely generated* (f. g.) or that M is a *finite A–module* if there exist $x_1,\ldots,x_n \in M$ such that $M = Ax_1 + \cdots + Ax_n$. Note that in this case M is isomorphic to a quotient of A^n. We can, analogously, consider the a.c.c. for submodules of M, and in the case it is satisfied, we call M to be *noetherian*. Artinian modules are defined similarly. Observe that M is noetherian iff every submodule of M is finitely generated. In general, if M is f. g., then a submodule of M needn't be f. g., i.e., M needn't be noetherian. However, the following basic result assures that 'most' f. g. modules are noetherian.

(3.1) Lemma. *Finitely generated modules over noetherian rings are noetherian.*

Proof (Sketch)**:** First note that given a submodule N of M, we have that M is noetherian iff both N and M/N are noetherian. Use this and induction to show that if A is noetherian, then so is A^n, and, hence, any of its quotient modules. □

Remark: The above lemma as well as the statements in its proof carry over verbatim if the word *noetherian* is replaced throughout by *artinian*.

Another basic fact about modules is the following.

(3.2) Nakayama's Lemma. Let M be a f. g. A–module and I be an ideal of A such that $IM = M$. Then there exists $a \in I$ such that $(1-a)M = 0$. In particular, if $I \neq A$ and A is a domain or a local ring, then $M = 0$.

Proof: Write $M = Ax_1 + \cdots + Ax_n$. Then $x_i = \sum_{j=1}^{n} a_{ij}x_j$, for some $a_{ij} \in I$. Let $d = \det(\delta_{ij} - a_{ij})$. Then $d = 1 - a$, for some $a \in I$, and, by Cramer's rule, $dx_j = 0$ for all j. □

Remark: The 'determinant trick' in the above proof shows more generally that if M and I are as in (3.2) above and $\phi : M \to M$ is an A–linear map such that $\phi(M) \subseteq IM$, then there exist $a_1, \ldots, a_n \in I$ such that $\phi^n + a_1\phi^{n-1} + \cdots + a_n = 0$. Thus Nakayama's Lemma may be considered as an analogue of Cayley–Hamilton Theorem of Linear Algebra.

Here is a nice application of Nakayama's Lemma and primary decomposition.

(3.3) Krull's Intersection Theorem. *Suppose A is noetherian and I is any ideal of A. Then there exists $a \in I$ such that $(1-a)\cap_{n=0}^{\infty} I^n = 0$. In particular, if $I \neq A$, and A is a local ring, then $\cap_{n=0}^{\infty} I^n = 0$.*

Proof: Let $J = \cap_{n=0}^{\infty} I^n$. Write $IJ = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r \cap \mathfrak{q}_{r+1} \cap \cdots \cap \mathfrak{q}_h$, where $\mathfrak{q}_i$ are $\mathfrak{p}_i$–primary ideals with $\mathfrak{p}_i \supseteq I$ for $1 \leq i \leq r$ and $\mathfrak{p}_j \not\supseteq I$ for $r < j \leq h$. Fix some $y_j \in I \setminus \mathfrak{p}_j$ for $r < j \leq h$. Then $x \in J \Rightarrow xy_j \in IJ \Rightarrow xy_j \in \mathfrak{q}_j \Rightarrow x \in \mathfrak{q}_j$. Thus $J \subseteq \mathfrak{q}_{r+1} \cap \cdots \cap \mathfrak{q}_h$. Also, since $I \subseteq \mathfrak{p}_i$ for $1 \leq i \leq r$, there exists $m \geq 1$ such that $I^m \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_r$. Since $J \subseteq I^m$, it follows that $J \subseteq \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_h = IJ$. Thus $IJ = J$. Now apply Nakayama's Lemma. □

If M satisfies both a.c.c. and d.c.c., then, clearly, any chain of submodules of M is finite; two such maximal chains can be shown to have the same length (as in Jordan–Hölder Theorem of Group Theory), which is called the *length* of M and denoted by $\ell(M)$. Note that the length of a module behaves in much the same way as the vector space dimension; for example, if N is a submodule of M, then $\ell(M) = \ell(N) + \ell(M/N)$. Basic examples of modules satisfying a.c.c. and d.c.c. are: (i) f.g. modules over artinian rings (in particular, finite dimensional vector spaces, for which length equals the dimension) (ii) A–modules of the type $\mathfrak{q}^n M/\mathfrak{q}^{n+1}M$, where A is noetherian, $\mathfrak{q}$ is primary to a maximal ideal of A, and M is a f. g. A–module (in particular, the artinian ring $A/\mathfrak{q}$).

4. Integral Extensions

The theory of algebraic field extensions has a useful analogue to ring extensions, which is discussed in this section.

Let B be a ring and A be a subring of B. We may express this by saying that B is a (ring) extension of A or that B is an overring of A.

Definition: An element $x \in B$ is said to be *integral* over A if it satisfies a monic polynomial with coefficients in A, i.e., $x^n + a_1x^{n-1} + \cdots + a_n = 0$ for some $a_1, \ldots, a_n \in A$. If every element of B is integral over A, then we say that B is an *integral extension* of A or that B is *integral* over A.

Evidently, if $x \in B$ satisfies an integral equation such as above, then $1, x, x^2, \ldots, x^{n-1}$ generate $A[x]$ as an A–module. And if B' is a subring of B containing $A[x]$ such that $B' = Ax_1 + \cdots + Ax_n$, then for any $b \in B'$, $bx_i = \sum a_{ij}x_j$ for some $a_{ij} \in A$ so that b satisfies the

monic polynomial $\det(X\delta_{ij} - a_{ij}) \in A[X]$. Thus we obtain the following criteria.

$$\begin{aligned} x \in B \text{ is integral over } A &\Leftrightarrow A[x] \text{ is a finite } A\text{–module} \\ &\Leftrightarrow \text{a subring } B' \text{ of } B \text{ containing } A[x] \text{ is a finite } A\text{–module.} \end{aligned}$$

In particular, if B is a finite A–module, then B is integral over A. The converse is true if we further assume (the necessary condition) that B is a f. g. A–algebra. This follows by observing that the above criteria implies, using induction, that if $x_1, \ldots, x_n \in B$ are integral over A, then $A[x_1, \ldots, x_n]$ is a finite A–module. This observation also shows that the elements of B which are integral over A form a subring, say C, of B. If $C = B$, we say that A is *integrally closed* in B. A domain is called *integrally closed* or *normal* if it is integrally closed in its quotient field. Note that if S is a m. c. subset of A, B is integral over A, and J is an ideal of B, then $S^{-1}B$ (resp: B/J) is integral over $S^{-1}A$ (resp: $A/J \cap A$); moreover, if A is a normal domain and $0 \notin S$, then $S^{-1}A$ is also a normal domain.

(4.1) Exercise: Show that a UFD is normal. Also show that if A is a domain, then A is normal iff $A[X]$ is normal. Further, show that if A is a normal domain, K is its quotient field, and x is an element of a field extension L of K, then x is integral over A implies that the minimal polynomial of x over K has its coefficients in A.

Example: Let $B = k[X, Y]/(Y - X^2)$, and let x, y denote the images of X, Y in B so that $B = k[x, y]$. Let $A = k[y]$. Then x is integral over A, and hence B is integral over A. On the other hand, if $B = k[X, Y]/(XY - 1) = k[x, y]$, then x is not integral over $A = k[y]$. It may be instructive to note, indirectly, that $B \simeq k[Y, 1/Y]$ is not a finite $k[Y]$–module. These examples correspond, roughly, to the fact that the projection of parabola along the x–axis onto the y–axis is a 'finite' map in the sense that the inverse image of every point is at 'finite distance', whereas in the case of hyperbola, this isn't so. Similar examples in "higher dimensions" can be constructed by considering projections of surfaces onto planes, solids onto 3–space, and so on. Examples of integral (resp: non–integral) extensions of $\mathbb{Z}$ are given by subrings B of number fields (viz., subfields of $\mathbb{C}$ of finite degree over $\mathbb{Q}$) such that $B \subseteq \mathcal{O}_K$ (resp: $B \not\subseteq \mathcal{O}_K$), where $\mathcal{O}_K$ denotes the ring of integers in K. Indeed, $\mathcal{O}_K$ is nothing but the integral closure of $\mathbb{Z}$ in K.

A precise definition of dimension for arbitrary rings can be given as follows.

Definition: $\dim A = \max\{\operatorname{ht} \mathfrak{p} : \mathfrak{p} \text{ a prime ideal of } A\}$, where for any prime ideal $\mathfrak{p}$ of A,

$$\operatorname{ht} \mathfrak{p} = \max\{n : \exists \text{ distinct primes } \mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n \text{ of } A \text{ such that } \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n = \mathfrak{p}\}.$$

We often call $\operatorname{ht} \mathfrak{p}$ to be the *height* of $\mathfrak{p}$, and $\dim A$ to be the *Krull dimension* of A.

Remark: Observe that a field, and more generally an artinian ring has dimension 0. A PID which is not a field, in particular $\mathbb{Z}$ as well as $k[X]$, is clearly of dimension 1. It is proved later in this section that $\dim k[X_1, \ldots, X_n] = n$. If A is noetherian and $x \in A$ is a nonzero nonunit, then by a famous result of Krull, called the Principal Ideal Theorem or the Hauptidealsatz, every minimal prime belonging to (x) has height ≤ 1 [and the equality holds, by (2.4), if x is a nonzerodivisor]. More generally, every minimal prime of an ideal generated by m elements has height $\leq m$. It follows that the height of any ideal in a noetherian ring is finite and a

noetherian local ring is of finite dimension. For a classical proof of Krull's Principal Ideal Theorem, see [N1] or [ZS] and for a more modern approach, using the so called Dimension Theorem, see [AM], [M2] or Chapter 3 of the ICCTA Lecture Notes.

(4.2) Exercise: Suppose A is noetherian and I is any ideal of A. Show that $\dim A/I = \max\{\dim A/\mathfrak{p} : \mathfrak{p} \in \mathrm{Ass}(A/I)\} = \max\{\dim A/\mathfrak{p} : \mathfrak{p}$ is a minimal prime of $I\}$. Use the above remark to deduce that $\dim R_\Delta = d+1$, where Δ, I_Δ are as in (2.5), R_Δ is the *face ring* of Δ, i.e., $R_\Delta = k[X_1, \ldots, X_n]/I_\Delta$, and d is the (topological) dimension of Δ.

Basic results about integral extensions are as follows. In the seven results given below, B denotes an integral extension of A and $\mathfrak{p}$ denotes a prime ideal of A.

(4.3) Theorem. *A is a field iff B is a field. Also, if $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, then $\mathfrak{p}$ is maximal iff $\mathfrak{q}$ is maximal. Moreover, if $\mathfrak{q}'$ is any prime ideal of B such that $\mathfrak{q} \subset \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{p}$, then $\mathfrak{q} = \mathfrak{q}'$.*

(4.4) Lying Over Theorem. *There exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$. In particular, $\mathfrak{p}B \cap A = \mathfrak{p}$.*

(4.5) Corollary. $\dim B \leq \dim A$. *In particular, if B is a domain and* $\dim A \leq 1$, *then* $\dim A = \dim B$.

(4.6) Going Up Theorem. *If $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, and $\mathfrak{p}'$ is a prime ideal of A such that $\mathfrak{p} \subseteq \mathfrak{p}'$, then there exists a prime ideal $\mathfrak{q}'$ of B such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap A = \mathfrak{p}$.*

(4.7) Corollary. $\dim A = \dim B$.

(4.8) Going Down Theorem. *Assume that A and B are domains and A is normal. If $\mathfrak{q}$ is a prime ideal of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, and $\mathfrak{p}'$ is a prime ideal of A such that $\mathfrak{p}' \subseteq \mathfrak{p}$, then there exists a prime ideal $\mathfrak{q}'$ of B such that $\mathfrak{q}' \subseteq \mathfrak{q}$ and $\mathfrak{q}' \cap A = \mathfrak{p}$.*

(4.9) Corollary. *Assume that A and B are domains and A is normal. Then for any prime ideal $\mathfrak{q}$ of B such that $\mathfrak{q} \cap A = \mathfrak{p}$, we have* $\mathrm{ht}\,\mathfrak{p} = \mathrm{ht}\,\mathfrak{q}$.

Proofs (Sketch). Easy manipulations with integral equations of relevant elements proves the first assertion of (4.3); the second and third assertions follow from the first one by passing to quotient rings and localisations respectively. To prove (4.4), first localise at $\mathfrak{p}$ and, then, note that if $\mathfrak{p}B_0 = B_0$, where $B_0 = (A \setminus \mathfrak{p})^{-1}B$, then $\mathfrak{p}B' = B'$ for some f. g. A–algebra B'; now B' is a finite A–module and Nakayama's Lemma applies. (4.6) follows by applying (4.4) to appropriate quotient rings. To prove (4.8), consider the multiplicatively closed subset $S = (A \setminus \mathfrak{p}')(B \setminus \mathfrak{q}) = \{ab : a \in A \setminus \mathfrak{p}',\ b \in B \setminus \mathfrak{q}\}$ of B and note that it suffices to prove $\mathfrak{p}'B \cap S = \emptyset$ [because, then there exists a prime ideal $\mathfrak{q}'$ of B such that $\mathfrak{p}'B \subseteq \mathfrak{q}'$ and $\mathfrak{q}' \cap S = \emptyset$, and this will have the desired properties]. To this end, let $x \in \mathfrak{p}'B \cap S$. Let K and L denote the quotient fields of A and B respectively. Let $\bar{L}$ be a normal extension of K containing L and $\bar{B}$ be the integral closure of A in $\bar{L}$. Since $\mathfrak{p}' \subseteq A$ and $x \in \mathfrak{p}'B$, all the conjugates of x w.r.t L/K are in $\mathfrak{p}'\bar{B}$, and hence the coefficients of the minimal polynomial, say $f(X)$, of x over K are in $\mathfrak{p}'\bar{B} \cap A = \mathfrak{p}'$ (since A is normal!). Write $f(X) = X^d + c_1X^{d-1} + \cdots + c_d$, and

$x = ab$, where $c_1, \ldots, c_d \in \mathfrak{p}'$, $a \in A \setminus \mathfrak{p}'$ and $b \in B \setminus \mathfrak{q}$. Clearly, $X^d + (c_1/a)X^{d-1} + \cdots + (c_d/a^d)$ is the minimal polynomial of b over K. But A is normal and b is integral over A implies that $c_i = c_i' a^i$ for some $c_i' \in A$ $(1 \leq i \leq d)$. Since $c_i \in \mathfrak{p}'$ and $a \notin \mathfrak{p}'$, we have $c_i' \in \mathfrak{p}'$ for $1 \leq i \leq d$. Hence $b^d \in \mathfrak{p}'B \subseteq \mathfrak{p}B \subseteq \mathfrak{q}$, and so $b \in \mathfrak{q}$, which is a contradiction. □

For a more leisurely proof of the results above, see [AM, pp. 61–64] or [ZS, pp. 257–264].

(4.10) Exercise. Prove the three corollaries above using the results preceding them.

Remark: It may be noted that (4.7) is an analogue of the simple fact that if L/K is an algebraic extension of fields containing a common subfield k, then $\text{tr.deg.}_k L = \text{tr.deg.}_k K$. Recall that if K is a ring containing a field k, then elements $\theta_1, \ldots, \theta_d$ of K are said to be *algebraically independent* over k if they do not satisfy any algebraic relation over k, i.e., $f(\theta_1, \ldots, \theta_d) \neq 0$ for any $0 \neq f \in k[X_1, \ldots, X_n]$. A subset of K is *algebraically independent* if every finite collection of elements in it are algebraically independent. If K is a field then any two maximal algebraically independent subsets have the same cardinality, called the *transcendence degree* of K/k and denoted by $\text{tr.deg.}_k K$; such subsets are then called *transcendence bases* of K/k; note that an algebraically independent subset S is a transcendence basis of K/k iff K is algebraic over $k(S)$, the smallest subfield of K containing k and S. If B is a domain containing k and K is its quotient field, then one sets $\text{tr.deg.}_k B = \text{tr.deg.}_k K$. Finally, note that $k[X_1, \ldots, X_n]$ and its quotient field $k(X_1, \ldots, X_n)$ are clearly of transcendence degree n over k. A good reference for this material is Chapter 2 of [ZS].

We shall now proceed to prove a basic result in Dimension Theory, known as Noether's Normalisation Lemma. The proof is based on the following lemma. The key idea here may be explained by revisiting the example of hyperbola for which the projection onto the y–axis is not 'finite'; however, if we tilt the axes a bit, e.g., via the coordinate change $X' = X$, $Y' = Y - cX$ for some $c \neq 0$, then the projection becomes a 'finite' map .

(4.11) Lemma. *Let k be a field and $f \in B = k[X_1, \ldots, X_n]$ be a nonconstant polynomial. Then there exist $X_2', \ldots, X_n' \in B$ such that $f, X_2', \ldots, X_n'$ are algebraically independent and*

$$f = cX_1^m + g_1 X_1^{m-1} + \cdots + g_m \quad \text{for some } c \in k,\ c \neq 0 \text{ and } g_1, \ldots, g_m \in k[X_2', \ldots, X_n'].$$

Moreover, $X_2', \ldots, X_n'$ can be chosen such that $X_i' = X_i - X_1^{m_i}$ for some $m_i \geq 1$ $(2 \leq i \leq n)$. In case k is infinite, we can choose $X_2', \ldots, X_n'$ to be of the form $X_i' = X_i - c_i X_1$ for suitable $c_i \in k$ $(2 \leq i \leq n)$. In particular, B is integral over $A = k[f, X_2', \ldots, X_n']$. Also, $fB \cap A = fA$ and B/fB is integral over A/fA.

Proof: Let e be an integer greater than any of the exponents of $X_1, \ldots, X_n$ appearing in f, and let $m_i = e^{i-1}$ for $2 \leq i \leq n$. In the 'new variables' X_1 and $X_i' = X_i - X_1^{m_i}$ $(2 \leq i \leq n)$, a monomial $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ appearing in f becomes $X_1^{i_1} (X_2' + X_1^{m_2})^{i_2} \cdots (X_n' + X_1^{m_n})^{i_n}$, and this is clearly monic in X_1 of degree $i_1 + i_2 e + \cdots + i_n e^{n-1}$. By our choice of e, these degrees are distinct for different values of $(i_1, \ldots, i_n)$, and if m is the maximum of these degrees, then f clearly has the desired form. In case k is infinite, we let $m = \deg f$ and write $f = f_0 + f_1 + \cdots + f_m$, where $f_i \in k[X_1, \ldots, X_n]_i$. Since $f_m \neq 0$, we can find $c_2, \ldots, c_n \in k$ such that $f_m(1, c_2, \ldots, c_n) \neq 0$. Now with $X_i' = X_i - c_i X_1$, for $2 \leq i \leq m$, we have

$f = f_m(1, c_2, \ldots, c_n)X_1^m + g_1X_1^{m-1} + \cdots + g_m$ for some $g_1, \ldots, g_m \in k[X_2', \ldots, X_n']$. Finally, since $B = k[X_1, X_2', \ldots, X_n']$, it follows that B is integral over $A = k[f, X_2', \ldots, X_n']$. In particular, $\text{tr.deg.}_k A = n$, and hence $f, X_2', \ldots, X_n'$ are algebraically independent over k, and A is isomorphic to a polynomial ring in n variables over k. This implies that A is a normal domain and thus if $fh \in A$ for some $h \in B$, then $h \in A$, being in the quotient field of A and integral over A. Thus $fB \cap A = fA$ and consequently, B/fB is integral over A/fA. □

(4.12) Corollary. $\dim k[X_1, \ldots, X_n] = n$. *In particular,* $\text{ht}\,(X_1, \ldots, X_i) = i$, *for* $1 \le i \le n$.

Proof: Let $B = k[X_1, \ldots, X_n]$. Since $(X_1) \subset (X_1, X_2) \subset \cdots \subset (X_1, \ldots, X_n)$ is a chain of prime ideals of B of length n, we have $\dim B \ge n$. We prove $\dim B \le n$ by induction on n. The case of $n = 0$ is obvious. For the inductive step, let $P_0 \subset P_1 \subset \cdots \subset P_r$ be a chain of prime ideals of B of length r. Choose $0 \ne f \in P_1$. By (4.11), we obtain $X_2', \ldots, X_n' \in B$ such that B is integral over $A = k[f, X_2', \ldots, X_n']$. Hence by (4.3), $A \cap P_1 \subset \cdots \subset A \cap P_r$ is a chain of prime ideals of A of length $r - 1$, containing fA. Passing to A/fA and using the induction hypothesis, we see that $r - 1 \le n - 1$. Hence $r \le n$. □

(4.13) Noether's Normalisation Lemma. *Let* $B = k[x_1, \ldots, x_n]$ *be a* f. g. *algebra over a field* k *and* $J_1 \subseteq \cdots \subseteq J_m$ *be a chain of nonunit ideals of* B. *Then there exist* $\theta_1, \ldots, \theta_d \in B$ *and nonnegative integers* $r_1 \le \cdots \le r_m$ *such that (i)* $\theta_1, \ldots, \theta_d$ *are algebraically independent over* k, *(ii)* B *is integral over* $A = k[\theta_1, \ldots, \theta_d]$; *in particular,* B *is a finite* A*–module, and (iii)* $J_i \cap A = (\theta_1, \ldots, \theta_{r_i})A$ *for* $1 \le i \le m$. *Moreover, if* k *is infinite, then* $\theta_1, \ldots, \theta_d$ *can be chosen to be* k*–linear combinations of* $x_1, \ldots, x_n$.

Proof: It suffices to prove the result when B is the polynomial ring $k[X_1, \ldots, X_n]$ (because in general, $B \simeq B'/J_0'$ where $B' = k[X_1, \ldots, X_n]$ and J_0' is an ideal of B'; now if $J_1', \ldots, J_m'$ are the ideals of B', containing J_0', corresponding to $J_1', \ldots, J_m$ respectively, then applying the result to B' and the chain $J_0' \subseteq J_1' \subseteq \cdots J_m'$, we obtain $\theta_1', \ldots, \theta_n'$ and $r_0', r_1', \ldots, r_m'$, and it is easily seen that the images $\theta_1, \ldots, \theta_d$ of $\theta'_{r_0'+1}, \ldots, \theta_n'$ in B and the integers $r_1, \ldots, r_m$ defined by $r_i = r_i' - r_0'$ have the desired properties). Thus we now assume that $B = k[X_1, \ldots, X_n]$. Induct on m. The case of $m = 0$ is obvious.

Consider the case when $m = 1$. Here, we induct on n. The case of $n = 0$ being trivial, assume that $n \ge 1$. We may also assume that $J_1 \ne 0$. Let $0 \ne f \in J_1$. Then we can find $X_2', \ldots, X_n'$ as in (4.11). By induction hypothesis, there exist $\theta_2, \ldots, \theta_n \in A' = k[X_2', \ldots, X_n']$ such that $\theta_2, \ldots, \theta_n$ are algebraically independent over k, A' is integral over $k[\theta_2, \ldots, \theta_n]$, and $J_1 \cap k[\theta_2, \ldots, \theta_n] = (\theta_2, \ldots, \theta_r)$, for some $r \ge 1$. Hence $A = A'[f]$ is integral over $k[f, \theta_2, \ldots, \theta_n]$, and therefore so is B. Consequently, $\text{tr.deg.}_k k[f, \theta_2, \ldots, \theta_n] = \text{tr.deg.}_k B = n$, and so if we let $\theta_1 = f$, then $\theta_1, \ldots, \theta_n$ are algebraically independent over k. Moreover, since $f \in J_1$. and $J_1 \cap k[\theta_1, \ldots, \theta_n] = (\theta_1) + J_1 \cap k[\theta_2, \ldots, \theta_n] = (\theta_1, \ldots, \theta_r)$.

If $m > 1$ and the result is assumed for $m - 1$, then for the chain $J_1 \subseteq \cdots \subseteq J_{m-1}$, there exist $\theta_1', \ldots, \theta_n' \in B$ and nonnegative integers $r_1', \ldots, r_{m-1}'$ satisfying conditions such as (i), (ii) and (iii). Let $r = r_{m-1}'$. Using the previous case (of $m = 1$), we can find $\theta''_{r+1}, \ldots, \theta''_n$ in $B'' = k[\theta'_{r+1}, \ldots, \theta_n']$, and an integer $s \ge r$ such that $\theta''_{r+1}, \ldots, \theta''_n$ are algebraically independent over k, B'' is integral over $A'' = k[\theta'_{r+1}, \ldots, \theta_n']$, and $J_m \cap A'' = (\theta''_{r+1}, \ldots, \theta''_s)$. Define $\theta_i = \theta_i'$ if $1 \le i \le r$ and $\theta_i = \theta_i''$ if $r + 1 \le i \le n$; also $r_i = r_i'$ if $1 \le i \le m - 1$ and $r_m = s$. Now B'' is

integral over A'' implies that $B''[\theta'_1, \ldots, \theta'_r]$ is integral over $A''[\theta'_1, \ldots, \theta'_r]$. Also, B is integral over $k[\theta'_1, \ldots, \theta'_n] = B''[\theta'_1, \ldots, \theta'_r]$, and hence over $A''[\theta'_1, \ldots, \theta'_r] = k[\theta_1, \ldots, \theta_n]$. Consequently, $\text{tr.deg.}_k k[\theta_1, \ldots, \theta_n] = \text{tr.deg.}_k B = n$, and hence $\theta_1, \ldots, \theta_n$ are algebraically independent over k. Checking that $J_i \cap k[\theta_1, \ldots, \theta_n] = (\theta_1, \ldots, \theta_{r_i})$ is an easy exercise. □

(4.14) Corollary. *If B is domain and a* f. g. *k–algebra, then* $\dim B = \text{tr.deg.}_k B$. *Consequently,* $\dim B[X_1, \ldots, X_n] = \dim B + n$.

Proof: Apply (4.13) for the singleton chain (0), and use (4.7) and (4.12). □

(4.15) Corollary. *If B is a* f. g. *algebra over a field k, and P is a prime ideal of B, then* $\dim B = \text{ht}\, P + \dim B/P$.

Proof: Apply (4.13) for the singleton chain P, and use (4.7) and (4.9). □

(4.16) Hilbert's Nullstellensatz. *Let k be a field. Then we have*

(i) *If K is a field and a* f. g. *k–algebra, then K is algebraic over k.*

(ii) *If k is algebraically closed, and $\mathbf{m}$ is a maximal ideal of $k[X_1, \ldots, X_n]$, then there exist $\alpha_1, \ldots, \alpha_n \in k$ such that $\mathbf{m} = (X_1 - \alpha_1, \ldots, X_n - \alpha_n)$.*

(iii) *If k is algebraically closed, and I is a nonunit ideal of $k[X_1, \ldots, X_n]$, then there exists $(\alpha_1, \ldots, \alpha_n) \in k^n$ such that $f(\alpha_1, \ldots, \alpha_n) = 0$, for each $f \in I$.*

Proof: By (4.13), K is integral over a polynomial ring $k[\theta_1, \ldots, \theta_d]$, and, by (4.3), the latter is a field. Hence $d = 0$ and thus K is algebraic over k. To prove (ii), let $K = k[X_1, \ldots, X_n]/\mathbf{m}$. Then by (i) and the assumption on k, we find that $K \simeq k$. Let $\alpha_1, \ldots, \alpha_n$ be the unique elements of k corresponding to the images of $X_1, \ldots, X_n$ in K. Now $(X_1 - \alpha_1, \ldots, X_n - \alpha_n) \subseteq \mathbf{m}$, and the former is clearly a maximal ideal of $k[X_1, \ldots, X_n]$. This proves (ii). Finally, if I is as in (iii), then $I \subseteq \mathbf{m}$, for some maximal ideal $\mathbf{m}$ of $k[X_1, \ldots, X_n]$. Now apply (ii). □

Exercise 4.17: Suppose k is an algebraically closed field and $f, g \in k[X, Y]$. Determine a primary decomposition of $(f, g)k[X, Y]$. Show that if f and g are not divisible by any nonconstant polynomial in $k[X, Y]$, then they have only finitely many common zeros in k^2.

References

[Ab] S. S. Abhyankar, *Algebraic Geometry for Scientists and Engineers*, American Math. Society, 1990.

[AM] M. Atiyah and I. G. MacDonald, *Introduction to Commutative Algebra*, Addison–Wesley, 1969.

[Bo] N. Bourbaki, *Commutative Algebra*, Hermann, 1972.

[BH] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, 1993.

[Ei] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer–Verlag, 1995.

[Ka] I. Kaplansky, *Commutative Rings*, The University of Chicago Press, 1974.

[KS] A. I. Kostrikin and I. R. Shafarevich (Eds), *Algebra I : Basic Notions of Algebra*, Springer–Verlag, 1990.

[Ku] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, 1985.

[M1] H. Matsumura, *Commutative Algebra*, Benjamin, 1970.

[M2] H. Matsumura, *Commutative Ring Theory*, Cambridge University Press, 1986.

[N1] D. G. Northcott, *Ideal Theory*, Cambridge University Press, 1953.

[N2] D. G. Northcott, *Lessons on Rings, Modules and Multiplicities*, Cambridge University Press, 1968.

[Sh] R. Y. Sharp, *Steps in Commutative Algebra*, Cambridge University Press, 1990.

[ZS] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1, Van Nostrand, 1958.