

CHAPTER 1 : Finitely Generated Algebras

Throughout this book a ring will always mean a commutative ring with identity if not stated otherwise. The letter K will always denote a field and the letters A, B, C, R will be generally used for rings. As usual we use $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and \mathbb{C} to denote the ring of integers, the fields of rational, real and complex numbers respectively.

1.A. Algebras over a Ring

Let A be a ring. An A -algebra is a pair (B, φ) where B is a ring and $\varphi : A \rightarrow B$ is a ring homomorphism called the structure homomorphism of the A -algebra (B, φ) . We will often omit φ in the notation of (B, φ) and simply say that B is an A -algebra.

Note that an A -algebra B is also an A -module, where the scalar multiplication is defined via the structure homomorphism $\varphi : A \rightarrow B$ by $ax := \varphi(a)x$ for all $a \in A$ and $x \in B$. Conversely, if a ring B is an A -module with the property:

$$(ax)(by) = (ab)(xy) \quad \text{for all } a, b \in A \text{ and } x, y \in B,$$

then B is an A -algebra with structure homomorphism $\varphi : A \rightarrow B$ defined by $a \mapsto a1_B$.

Let (B, φ) and (C, ψ) be two A -algebras. An A -algebra homomorphism $\theta : B \rightarrow C$ is a ring homomorphism such that the diagram

$$\begin{array}{ccc} B & \xrightarrow{\theta} & C \\ \varphi \swarrow & & \nearrow \psi \\ & A & \end{array}$$

is commutative, that is, $\theta \circ \varphi = \psi$ or equivalently θ is A -linear.

1.A.1. Example (1) Let A be a subring of a ring B . Then B is an A -algebra with the natural inclusion $A \hookrightarrow B$ as the structure homomorphism.

(2) Let A be a ring and let \mathfrak{a} be an ideal in A . Then the residue class ring A/\mathfrak{a} is an A -algebra with the natural surjection $\pi : A \rightarrow A/\mathfrak{a}$ as the structure homomorphism.

(3) (Polynomial algebra) Let I be a set and let $X_i, i \in I$, be a family of indeterminates or variables over A . Then the polynomial ring $A[X_i \mid i \in I]$ in the indeterminates $X_i, i \in I$, is an A -algebra and the natural inclusion $A \hookrightarrow A[X_i \mid i \in I]$ is the structure homomorphism.

Polynomial algebras are the free objects (in the language of categories) in the category of (commutative) A -algebras with the following universal property:

1.A.2. Universal property of polynomial algebras Let B be an A -algebra and let $x_i, i \in I$, be a family of elements of B . Then there exists a unique A -algebra homomorphism $A[X_i \mid i \in I] \rightarrow B$ such that $X_i \mapsto x_i$ for every $i \in I$.

In particular, we can identify $\text{Hom}_{A\text{-alg}}(A[X_i \mid i \in I], B)$ with B^I . Further, if $I = \{1, 2, \dots, n\}$ then $\text{Hom}_{A\text{-alg}}(A[X_1, \dots, X_n], B)$ can be identified with B^n .

Let B be an A -algebra and let $x := (x_i)_{i \in I}$ be a family of elements of B . Then the unique A -algebra homomorphism $\varepsilon : A[X_i \mid i \in I] \rightarrow B$ with $\varepsilon(X_i) = x_i$ for every $i \in I$ is called the substitution homomorphism or the evaluation homomorphism defined by x . For $F \in A[X_i \mid i \in I]$, the image $\varepsilon(F)$ is denoted by $F(x)$ and is called the value of F at the point $x \in B^I$. Since ε is an A -algebra homomorphism, for $F, G \in A[X_i \mid i \in I]$ and $x \in B^I, a \in A$ we have

$$(F + G)(x) = F(x) + G(x), \quad (FG)(x) = F(x)G(x) \quad \text{and} \quad (aF)(x) = aF(x).$$

If $y \in B$ and $y = F(x)$, then x is called a y -place of F . In particular, $x \in B^I$ is called a 0-place or zero of F if $F(x) = 0$.

The image of ε is the smallest A -subalgebra of B containing $\{x_i \mid i \in I\}$ and is denoted by $A[x_i \mid i \in I]$. We call it the A -subalgebra generated by the family $x_i, i \in I$. We say that B is an A -algebra generated by the family $x_i, i \in I$, if $B = A[x_i \mid i \in I]$. Further, we say that B is a finitely generated A -algebra or an A -algebra of finite type if there exists a finite family x_1, \dots, x_n of elements of B such that $B = A[x_1, \dots, x_n]$. A ring homomorphism $\varphi : A \rightarrow B$ is called a homomorphism of finite type if B is an A -algebra of finite type with respect to φ .

The above discussions convey the fact that the residue class algebras $A[X_i \mid i \in I]/\mathfrak{a}$ represent all the A -algebras up to isomorphism and, therefore, a good understanding of the structure of the polynomial algebras over A is essential for the study of any A -algebra.

1.B. Factorization in Rings

We will begin by reviewing a study of division and factorization in rings. This study is modeled on properties of the ring of integers \mathbb{Z} .

Let R be a ring. An element $p \in R$ is called a prime element if it is a non-zero divisor in R and if the principal ideal Rp is a prime ideal or, equivalently, if the residue class ring R/Rp is an integral domain. A non-zero divisor $a \in R$ is called irreducible if a is a non-unit but not a product of two non-units. A prime element is always irreducible (but not conversely).

A ring R is called factorial (or a unique factorization domain (UFD)) if R is an integral domain and if every non-zero element $a \in R$ which is not a unit in R has a factorization $a = p_1 p_2 \cdots p_r$, where the elements $p_i \in R$ are prime elements for $i = 1, \dots, r$. In a factorial domain every irreducible element is prime.

It is easy to show that in a factorial ring R , for every non-zero element $a \in R$ which is not a unit in R , a factorization $a = p_1 p_2 \cdots p_r$ of a into prime factors is unique up to a permutation and up to multiplication by units. Every principal ideal domain R (in particular, \mathbb{Z}) is factorial.

1.B.1. Proposition *Let R be a ring. If R is factorial then $R[X_i \mid i \in I]$ is also factorial.*

For $R = \mathbb{Z}$ the above proposition is a theorem due to Gauss. One important observation for proving the above proposition is the following lemma.

1.B.2. Lemma (Gauss) *Let R be a ring and let $p \in R$ be a prime element. Then p is a prime element in $R[X_i \mid i \in I]$.*

PROOF. The rings $R[X_i \mid i \in I]/R[X_i \mid i \in I] \cdot p$ and $(R/Rp)[X_i \mid i \in I]$ are canonically isomorphic. •

1.B.3. Corollary *Let R be a ring. If R is factorial then so is the polynomial ring $R[X_1, \dots, X_n]$. In particular, the polynomial rings $K[X_1, \dots, X_n]$ with K a field and $\mathbb{Z}[X_1, \dots, X_n]$ are factorial.*

1.B.4. Example The following examples (besides (6)) are good to get a feeling about factoriality.

(1) Let $S \subseteq R$ be a multiplicatively closed set in the ring R not containing 0. Then every prime element $p \in R$ which is not a unit in $S^{-1}R$ is prime in $S^{-1}R$. Moreover, if R is factorial then so is $S^{-1}R$.

(2) Let R be a factorial domain and let $a \in R$ be either a prime element or a unit in R . Then $R[X, Y]/(XY + a)$ is a factorial domain.

(3) $\mathbb{R}[X, Y]/(X^2 + Y^2 - 1)$ is not factorial, but $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ is factorial.

(4) (Klein-Nagata) Let K be a field of characteristic $\neq 2$ and let $a_1, \dots, a_n, n \geq 5$, be non-zero elements of K . Then $K[X_1, \dots, X_n]/(a_1 X_1^2 + \cdots + a_n X_n^2)$ is factorial.

(5) Let K be a field of characteristic $\neq 2$ and let Q be a non-degenerate quadratic form in $K[X_1, \dots, X_n]$. If $n \geq 5$ then $K[X_1, \dots, X_n]/(Q)$ is factorial by (4) above.

(6) Let D be a square free integer $\neq 0, 1$ and let R_D be the ring of algebraic integers in the quadratic field $\mathbb{Q}(\sqrt{D})$. If $D < 0$ then R_D is factorial if and only if D belongs to $\{-1, -2, -3, -7, -11, -19, -43, -67, -163\}$.¹⁾

¹⁾ This is a very deep theorem. Gauss proved for these values of D that R_D is factorial. He also conjectured that there is no other. This much more difficult part of the theorem was finally proved in 1967, after the problem had been worked out for more than 150 years. In 1967 Stark found a proof of this theorem as did Baker soon after. The situation for positive D is not well understood. It is not known whether R_D is factorial (i.e. a principal ideal domain) for infinitely many $D > 0$.

1.B.5. Exercise (1) Let A denote a factorial domain and let K be the quotient field of A . Let $A[X_1, \dots, X_n]$ be the polynomial ring and let $F \in A[X_1, \dots, X_n]$ be a non-constant polynomial. Prove the following statements (use only simple arguments):

- Let $\varphi : A[X_1, \dots, X_n] \rightarrow A[X_1, \dots, X_n]$ be a ring isomorphism. Then F is prime if and only if $\varphi(F)$ is prime.
- Let B be an integral domain containing A . If the coefficients of F are relatively prime and if F is irreducible in $B[X_1, \dots, X_n]$ then F is prime in $A[X_1, \dots, X_n]$.
- If the degree form F_d of F is prime then so is F .
- F is prime if and only if its homogenization F^h is prime.
- Let \mathfrak{p} be a prime ideal in A . If the residue class \overline{F} of F in $(A/\mathfrak{p})[X_1, \dots, X_n]$ is irreducible of degree $\deg(F)$ and if the coefficients of F are relatively prime, then F is prime in $A[X_1, \dots, X_n]$.
- F is prime in $A[X_1, \dots, X_n]$ if and only if F is prime in $K[X_1, \dots, X_n]$ and the coefficients of F are relatively prime.

(2) Let A denote a factorial domain and let K be the quotient field of A . Show that the following polynomials are irreducible.

- $XY - a \in A[X, Y]$, $a \neq 0$; $(X - 1)^2(X^2 + Y^2) - X^2$, $\text{char} K \neq 2$;
 $(X^2 + Y^2)(X - 2) + X$, $\text{char} K \neq 2$; $X^3 + X^2 - Y^2$.
- $aX^m + bY^n$, $m, n \in \mathbb{N}^*$ relatively prime and $a, b \in A^* := A \setminus \{0\}$ relatively prime in A .
- $X^{2m} + Y^{2n} \in \mathbb{R}[X, Y]$, $m, n \in \mathbb{N}^*$ relatively prime. (**Hint:** Look at the prime factorization in $\mathbb{C}[X, Y]$.)
- $\det (X_{ij})_{1 \leq i, j \leq n} \in A[X_{ij} \mid 1 \leq i, j \leq n]$.
- $X^d - G(Z)/H(Z) \in K(Z)[X]$, $d \in \mathbb{N}^*$, where $G, H \in K[Z]$ are such that GH is non-constant and has no multiple factors.
- $a_1X_1^{v_1} + a_2X_2^{v_2} + \dots + a_nX_n^{v_n} \in A[X_1, \dots, X_n]$, $n \geq 3$, $v_1, \dots, v_n \in \mathbb{N}^*$ not all zero in A , $a_1, \dots, a_n \in A^*$ relatively prime. (**Hint:** One assumes $A = K$ and using Eisenstein's criterion reduces to the case $n = 3$. Then use the fact that $a_1X_1^{v_1} + a_2X_2^{v_2}$ has no multiple factors if either $v_1 \neq 0$ or $v_2 \neq 0$ in K .)
- $X_1^d + \dots + X_n^d + G \in A[X_1, \dots, X_n]$, $n \geq 3$, $d \neq 0$ in K and $G \in A[X_1, \dots, X_n]$ is any polynomial of degree $< d$. What about the case $n = 2$?
- $(X - a_1) \cdots (X - a_d) + 1 \in \mathbb{Z}[X]$, $d \geq 1$, where $a_1, \dots, a_d \in \mathbb{Z}$ are distinct.

1.C. Noetherian Rings and Modules

Let R be a ring and let M be an R -module. We say that M is Noetherian if it satisfies the equivalent conditions of the proposition below. A ring R is called a Noetherian ring if it is Noetherian as an R -module.

1.C.1. Proposition *Let R be a ring. Then for an R -module M the following three conditions are equivalent:*

- Every submodule of M is finitely generated.

(2) M satisfies the ascending chain condition for submodules, i.e., if $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ is any ascending sequence of submodules of M , then there exists a positive integer n such that $M_n = M_{n+1} = M_{n+2} = \cdots$.

(3) Every non-empty family of submodules of M has a maximal element.

PROOF. (1) \Rightarrow (2): Let $M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$ be an ascending sequence of submodules of M . Let $N = \bigcup_{i=1}^{\infty} M_i$. Then N is a submodule of M and is therefore generated by a finite number of elements, say x_1, \dots, x_r . There exists a positive integer n such that $x_1, \dots, x_r \in M_n$. Therefore we have $M_n = N$, so that $M_n = M_{n+1} = \cdots$.

(2) \Rightarrow (3): Let \mathcal{F} be a non-empty family of submodules of M . Suppose \mathcal{F} does not have a maximal element. Choose any $M_1 \in \mathcal{F}$. Suppose there exist $M_2, \dots, M_n \in \mathcal{F}$ such that $M_1 \subset M_2 \subset \cdots \subset M_n$. Then, since M_n is not maximal, there exists $M_{n+1} \in \mathcal{F}$ such that $M_n \subset M_{n+1}$. Therefore, recursively, we get an infinite sequence $M_1 \subset M_2 \subset M_3 \subset \cdots$ such that $M_n \subsetneq M_{n+1}$ for every n . This contradicts (2).

(3) \Rightarrow (1): Let N be a submodule of M . Let \mathcal{F} be the family of all finitely generated submodules of N . Since $0 \in \mathcal{F}$, \mathcal{F} is non-empty. Therefore \mathcal{F} has a maximal element, say N' . If $N' \neq N$ then there exists $x \in N$, $x \notin N'$. The submodule $N' + Rx$ of N is finitely generated and contains N' properly. This is a contradiction. Therefore $N' = N$ and N is finitely generated. \bullet

1.C.2. Example (1) A vector space V over a field K is Noetherian if and only if V is finite dimensional over K , that is, $\text{Dim}_K V < \infty$.

(2) Every principal ideal domain is Noetherian. In particular, \mathbb{Z} is Noetherian and, if K is a field, then the polynomial ring $K[X]$ and the formal power series ring $K[[X]]$ are Noetherian.

(3) If R is a Noetherian ring and \mathfrak{a} is an ideal in R , then R/\mathfrak{a} is a Noetherian ring.

We list some simple properties of Noetherian modules. The proofs are very easy.

1.C.3. Proposition *Let R be a ring.*

(1) *Let $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ be an exact sequence of R -modules. Then M is Noetherian if and only if both M' and M'' are Noetherian.*

(2) *Let N be a submodule of an R -module M . Then M is Noetherian if and only if both N and M/N are Noetherian R -modules.*

(3) *A finite direct sum of Noetherian modules is Noetherian.*

(4) *Suppose that R is a Noetherian ring. Let M be a finitely generated R -module. Then M is Noetherian.*

(5) *Let S be a multiplicatively closed subset of R and let M be a Noetherian R -module. Then $S^{-1}M$ is a Noetherian $S^{-1}R$ -module.*

(6) *Let S be a multiplicatively closed subset of a Noetherian ring R . Then $S^{-1}R$ is Noetherian. In particular, the localization $R_{\mathfrak{p}}$ of a Noetherian ring R at a prime ideal \mathfrak{p} is Noetherian.*

1.C.4. Hilbert's Basis Theorem *Let R be a Noetherian ring. Then the polynomial ring $R[X_1, \dots, X_n]$ in n variables over R is also Noetherian.*

PROOF. By induction on n , it is sufficient to prove the theorem for $n = 1$, i.e. that the polynomial ring $B := R[X]$ in one variable is Noetherian. Let \mathfrak{b} be any ideal of B . We will show that \mathfrak{b} is finitely generated. Suppose that \mathfrak{b} is not finitely generated. Then choose f_1, f_2, f_3, \dots inductively such that f_n is of smallest degree in $\mathfrak{b} \setminus \sum_{i=1}^{n-1} Bf_i$. Let $d_n := \deg(f_n)$ and let a_n be the leading coefficient of f_n . Then $d_1 \leq d_2 \leq \dots$. Since R is Noetherian, there exists a positive integer m such that $a_m \in \sum_{i=1}^{m-1} Ra_i$. Write $a_m = \sum_{i=1}^{m-1} \alpha_i a_i$ with $\alpha_i \in R$. Let $g := f_m - \sum_{i=1}^{m-1} \alpha_i X^{d_m-d_i} f_i$. Then $g \in \mathfrak{b} \setminus \sum_{i=1}^{m-1} Bf_i$ and $\deg(g) < d_m$. This contradicts the choice of f_m . Therefore \mathfrak{b} is finitely generated. •

This short proof is due to H. Sarges (see: Ein Beweis des Hilbertschen Basisatzes, J. Reine und Angew. Math. **283/284** (1976), 436-437). At the end of 1.D we give a more conceptual proof of Hilbert's basis theorem.

1.C.5. Corollary *Let R be a Noetherian ring and B a finitely generated R -algebra. Then B is Noetherian.*

PROOF. Since any finitely generated R -algebra is a quotient of a polynomial algebra $R[X_1, \dots, X_n]$, the corollary follows. •

1.C.6. Exercise Let R be a ring.

- (1) Let M be an R -module. Let B be a subring of R , so that M is also a B -module. If M is Noetherian as a B -module then M is Noetherian as an R -module.
- (2) Let M be a Noetherian R -module. Show that any surjective R -endomorphism of M is an isomorphism.
- (3) Let M be a Noetherian R -module and let $\mathfrak{a} := \text{Ann}_R M = \{a \in R \mid aM = 0\}$. Show that R/\mathfrak{a} is a Noetherian ring.
- (4) Let R be a non-Noetherian ring and let \mathcal{F} be the set of ideals in R which are not finitely generated. Show that \mathcal{F} has maximal elements and that the maximal elements of \mathcal{F} are prime ideals.
- (5) (I. S. Cohen) A ring R is Noetherian if and only if every prime ideal of R is finitely generated. (**Hint:** Use (4).)
- (6) Suppose that $R_{\mathfrak{p}}$ is Noetherian for every prime ideal $\mathfrak{p} \subseteq R$. Is R necessarily Noetherian?
- (7) Let B be a faithfully flat R -algebra. If B is Noetherian, show that R is Noetherian. More generally: Let $R \subseteq B$ be a ring extension with $(\mathfrak{a}B) \cap R = \mathfrak{a}$ for all finitely generated ideals $\mathfrak{a} \subseteq R$. If B is Noetherian, then R is Noetherian. (For example, if $R \subseteq B$ and R is a direct summand of B as an R -module, then R is Noetherian if B is Noetherian.)
- (8) Let \mathfrak{P} be a prime ideal in the formal power series ring $R[[X]]$ over R and let $\mathfrak{p} = \{f(0) \mid f \in \mathfrak{P}\}$. Show that \mathfrak{p} is a prime ideal of R and if \mathfrak{p} is generated by r elements then \mathfrak{P} can be generated by $r + 1$ elements.
- (9) If R is Noetherian then the formal power series ring $R[[X_1, \dots, X_n]]$ in n variables over R is also Noetherian. (**Hint:** Use (5) and (8).)

1.D. Graded Rings and Modules

A grading of type \mathbb{Z} or \mathbb{Z} -grading on a ring R is a sequence $(R_n)_{n \in \mathbb{Z}}$ of subgroups of R such that $R = \bigoplus_{n \in \mathbb{Z}} R_n$ and $R_m R_n \subseteq R_{m+n}$ for all $m, n \in \mathbb{Z}$. A ring with a \mathbb{Z} -grading is called a \mathbb{Z} -graded ring. A graded ring $R = \bigoplus_{n \in \mathbb{Z}} R_n$ of type \mathbb{Z} is called positively graded or \mathbb{N} -graded if $R_n = 0$ for all $n < 0$.

1.D.1. Example Let A be any ring.

(1) The grading $A_0 := A$, $A_n := 0$ for all $n \in \mathbb{Z}$, $n \neq 0$ on A is called the trivial grading on A .

(2) For $n \in \mathbb{Z}$, the subgroups

$$R_n := \{0\} \cup \{F \in A[X_1, \dots, X_r] \mid F \text{ is homogeneous of degree } n\}$$

define a grading on the polynomial ring $R := A[X_1, \dots, X_r]$. This grading is called the usual or standard grading on R .

(3) Let $r \in \mathbb{N}$ and $\gamma := (\gamma_1, \dots, \gamma_r) \in \mathbb{Z}^r$. For a monomial $X^m := X_1^{m_1} \cdots X_r^{m_r} \in R := A[X_1, \dots, X_r]$, let $\deg_\gamma X^m := m_1 \gamma_1 + \cdots + m_r \gamma_r$ be the so called γ -degree of X^m . For $n \in \mathbb{Z}$, let R_n be the A -submodule generated by all monomials of γ -degree n . Then $(R_n)_{n \in \mathbb{Z}}$ is a grading on R and is called the weighted grading corresponding to the weights $\gamma_1, \dots, \gamma_r$ on R or the γ -grading on R . If $\gamma_i = 1$ (respectively $\gamma_i = 0$) for all $i = 1, \dots, r$ then the corresponding weighted grading on R is the standard (respectively the trivial) grading on R .

Let $R = \bigoplus_{n \in \mathbb{Z}} R_n$ be a \mathbb{Z} -graded ring and let M be an R -module. A grading of type \mathbb{Z} or \mathbb{Z} -grading on M is a sequence $(M_n)_{n \in \mathbb{Z}}$ of subgroups of M such that $M = \bigoplus_{n \in \mathbb{Z}} M_n$ and $R_m M_n \subseteq M_{m+n}$ for all $m, n \in \mathbb{Z}$. An R -module M with a \mathbb{Z} -grading is called a \mathbb{Z} -graded R -module.

Let $R = \bigoplus_{n \in \mathbb{Z}} R_n$ be a graded ring and let $M = \bigoplus_{n \in \mathbb{Z}} M_n$ be a graded R -module. Then R_0 is a subring of R and R_n (respectively M_n) is an R_0 -submodule of R (respectively M) for every $n \in \mathbb{Z}$.

For $n \in \mathbb{Z}$, the elements of R_n (respectively M_n) are called the homogeneous elements of R (respectively M) of degree n . The zero element of R (respectively M) is homogeneous of degree n for every $n \in \mathbb{Z}$.

Every $x \in M$ can be written uniquely in the form $x = \sum_{n \in \mathbb{Z}} x_n$ with $x_n \in M_n$ for all $n \in \mathbb{Z}$ and $x_n = 0$ for almost all n . The x_n are called the homogeneous components of x of degree n .

For a non-zero element $x \in M$, the integers $\omega(x) := \inf \{n \in \mathbb{Z} \mid x_n \neq 0\}$ and $\deg(x) := \sup \{n \in \mathbb{Z} \mid x_n \neq 0\}$ are called the order and the degree of x , respectively. We put $\omega(0) := \infty$ and $\deg(0) := -\infty$. For $0 \neq x \in M$, the non-zero homogeneous elements $x_{\omega(x)}$ and $x_{\deg(x)}$ are called the initial form and the degree form of x respectively.

An R -submodule N of M is called a graded or homogeneous submodule of M if it satisfies the following equivalent conditions: (1) $N = \sum_{n \in \mathbb{Z}} (M_n \cap N)$.

(2) $N = \bigoplus_{n \in \mathbb{Z}} (M_n \cap N)$. (3) If $x \in N$ then every homogeneous component of x belongs to N . (4) N is generated by a set of homogeneous elements of M .

A graded R -submodule \mathfrak{a} of R is called a graded or homogeneous ideal of R .

Let $\mathfrak{a} \subseteq R$ be an ideal and let $L(\mathfrak{a})$ be the ideal generated by the degree forms $L(x) := x_{\deg(x)}$, $x \in \mathfrak{a}$, $x \neq 0$. Then $L(\mathfrak{a})$ is a homogeneous ideal in R . We say that the family f_j , $j \in J$, of elements of \mathfrak{a} is a Gröbner basis of \mathfrak{a} if $L(f_j)$, $j \in J$, generate $L(\mathfrak{a})$.

1.D.2. Lemma *Let $R = \bigoplus_{n \in \mathbb{N}} R_n$ be a positively graded ring and let $\mathfrak{a} \subseteq R$ be an ideal in R . If the family f_j , $j \in J$, of elements of \mathfrak{a} is a Gröbner basis of \mathfrak{a} then \mathfrak{a} is generated by f_j , $j \in J$.*

PROOF. Let $x \in \mathfrak{a}$, $x \neq 0$. We shall prove by induction on $\deg x$ that $x \in \sum_{j \in J} R f_j$. Write $x = x_0 + \dots + x_d$ with $d := \deg x$. Then $L(x) = x_d \in L(\mathfrak{a})$ and so there exist homogeneous elements $a_i \in R$, $i = 1, \dots, n$, such that $x_d = \sum_{i=1}^n a_i L(f_{j_i})$ and $\deg(a_i) = d - \deg(f_{j_i})$. In particular, $\deg(x - \sum_{i=1}^n a_i f_{j_i}) < d$. If $d = 0$ then $x = x_0 = \sum_{i=1}^n a_i f_{j_i} \in \sum_{j \in J} R f_j$, since R is positively graded. Now assume that $d \geq 1$. Then $x - \sum_{i=1}^n a_i f_{j_i} \in \sum_{j \in J} R f_j$ by induction and therefore $x \in \sum_{j \in J} R f_j$. •

We use the above lemma to give a conceptual proof of the Hilbert Basis Theorem, using the language of Gröbner bases: Let R be a Noetherian ring and let $\mathfrak{a} \subseteq R[X]$ be an ideal. Since $L(\mathfrak{a})$ is a homogeneous ideal in $R[X]$ (we take the standard grading on $R[X]$), we have $L(\mathfrak{a}) = \bigoplus_{m \in \mathbb{N}} \mathfrak{a}_m X^m$, where \mathfrak{a}_m , $m \in \mathbb{N}$, are ideals in R with $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \dots \subseteq \mathfrak{a}_n \subseteq \dots$. Now, since R is Noetherian, there exists an $m_0 \in \mathbb{N}$ such that $\mathfrak{a}_m = \mathfrak{a}_{m_0}$ for all $m \geq m_0$. Then $L(\mathfrak{a})$ is generated by $\mathfrak{a}_0, \mathfrak{a}_1 X, \dots, \mathfrak{a}_{m_0} X^{m_0}$ and since the ideals $\mathfrak{a}_0, \mathfrak{a}_1, \dots, \mathfrak{a}_{m_0}$ are finitely generated in R the ideal $L(\mathfrak{a})$ in $R[X]$ is finitely generated. This proves that \mathfrak{a} has a finite Gröbner basis and therefore \mathfrak{a} is finitely generated by the previous lemma. •

1.E. Integral Extensions

In this section we collect few basic facts on integral extensions which we will come across quite often in these lectures. Let R be an algebra over a ring A .

We say that R is a finite A -algebra if R is a finitely generated as an A -module, i.e. if there exist finitely many elements $x_1, \dots, x_n \in R$ such that $R = Ax_1 + \dots + Ax_n$. A ring homomorphism $\varphi : A \rightarrow R$ is called finite if R is a finite A -algebra with respect to φ .

Obviously, we have the transitivity of finiteness: *If R is a finite A -algebra and S is a finite R -algebra then S is a finite A -algebra.*

It is clear that a finite algebra is of finite type, but the converse is not true. For example, the polynomial algebra $A[X_1, \dots, X_n]$, $n \geq 1$, $A \neq 0$, is of finite type over A , but not a finite A -algebra.

An element x of an A -algebra R is said to be integral over A if it is a zero of a monic polynomial with coefficients in A , that is,

$$x^d + a_{d-1}x^{d-1} + \dots + a_0 = 0, \quad a_0, \dots, a_{d-1} \in A,$$

equivalently, the kernel of the substitution homomorphism $A[X] \rightarrow R$, $X \mapsto x$, contains a monic polynomial (in $A[X]$). Such a monic polynomial equation is called an integral equation of x over A . In case, A is a field, the concept of integral elements and the concept of algebraic elements are equivalent.

1.E.1. Example (1) (Theorem of Cayley–Hamilton) Let R be a finite free A -algebra of rank d with A -basis x_1, \dots, x_d and let $x \in R$. Consider the left translation $\lambda_x : R \rightarrow R$, $y \mapsto xy$. For each $j = 1, \dots, d$, write $xx_j = \sum_{i=1}^d a_{ij}x_i$ with $a_{ij} \in A$. Then $\sum_{i=1}^d (x\delta_{ij} - a_{ij})x_i = 0$ for all $j = 1, \dots, d$ and therefore, by Cramer's rule, we have $\det(x\mathfrak{E}_d - \mathfrak{A})x_i = 0$ for all $i = 1, \dots, d$, where \mathfrak{E}_d is the $d \times d$ identity matrix and \mathfrak{A} is the $d \times d$ matrix (a_{ij}) . Therefore $\chi_x(x) = \det(x\mathfrak{E}_d - \mathfrak{A}) = 0$ is a canonical integral equation of degree d of x over A , where $\chi_x = \det(X\mathfrak{E}_d - \mathfrak{A})$ is the characteristic polynomial of the A -linear endomorphism λ_x of R .

(2) Let b be a non-zero divisor in A which is not a unit. Then the element $1/b$ in the total quotient ring $Q = Q(A)$ of A is not integral over A . The kernel of the substitution homomorphism $A[X] \rightarrow Q$, $X \mapsto 1/b$, is generated by the linear polynomial $bX - 1$ and contains no monic polynomial.

The next proposition gives the connection between integral elements and finite algebras. First recall that an A -module M is said to be faithful if $\text{Ann}_A M = 0$.

1.E.2. Proposition Let R be an A -algebra and let $x \in R$. The following statements are equivalent:

- (1) x is integral over A .
- (2) $A[x]$ is a finite A -algebra.
- (3) $A[x]$ is contained in a finite A -subalgebra S of R .
- (4) There is a faithful $A[x]$ -module M which is finite as an A -module.

PROOF. (1) \Rightarrow (2): By (1) $x^d + a_{d-1}x^{d-1} + \dots + a_0 = 0$ for some $a_0, \dots, a_{d-1} \in A$. Then $x^d \in A + Ax + \dots + Ax^{d-1}$ and so by induction $x^m \in A + Ax + \dots + Ax^{d-1}$ for all $m \geq 0$. Therefore $A[x] = A + Ax + \dots + Ax^{d-1}$ is a finite A -algebra.

The implication (2) \Rightarrow (3) is trivial.

(3) \Rightarrow (4): Since $A[x]$ is a subring of S , the $A[x]$ -module S is faithful and therefore $M = S$ serves the purpose.

(4) \Rightarrow (1): Let $M = Ax_1 + Ax_2 + \dots + Ax_n$ be a faithful $A[x]$ -module. For each $j = 1, \dots, n$, write $xx_j = \sum_{i=1}^n a_{ij}x_i$ with $a_{ij} \in A$. Then $\sum_{i=1}^n (x\delta_{ij} - a_{ij})x_i = 0$

for all j and so $\det(x\delta_{ij} - a_{ij})M = 0$ by Cramer's rule. Therefore, since M is a faithful $A[x]$ -module, the equation $\det(x\delta_{ij} - a_{ij}) = 0$ is an integral equation of x over A (of degree n). •

1.E.3. Remark The proof of the implication (4) \Rightarrow (1) shows: *If $xM \subseteq aM$ for an ideal $a \subseteq A$, then there is an integral equation $x^n + a_{n-1}x^{n-1} + \dots + a_0 = 0$ with $a_j \in a^{n-j}$, $j = 0, \dots, n-1$.*

1.E.4. Corollary *Let R be an A -algebra and let $x_1, \dots, x_r \in R$. If x_1, \dots, x_n are integral over A , then $A[x_1, \dots, x_r]$ is a finite A -algebra.*

PROOF. We use induction on r . For $r = 1$ the assertion is a part of 1.E.2. For $r \geq 2$, $R' := A[x_1, \dots, x_{r-1}]$ is a finite A -algebra by induction hypothesis. Now x_r being integral over A , it is also integral over R' and so $R'[x_r] = A[x_1, \dots, x_r]$ is a finite R' -algebra by 1.E.2. Therefore $A[x_1, \dots, x_r]$ is a finite A -algebra, too. •

The set of elements of R which are integral over A is called the integral closure of A in R , and is usually denoted \bar{A} .

1.E.5. Corollary *For any A -algebra R , \bar{A} is a subalgebra of R .*

PROOF. For any $x, y \in \bar{A}$, $A[x, y] \subseteq R$ is a finite A -algebra by 1.E.4 and therefore $A[x, y] \subseteq \bar{A}$ by Proposition 1.E.2. •

1.E.6. Corollary *Let S be an R -algebra and R be an A -algebra. If S is integral over R and R is integral over A then S is integral over A .*

PROOF. Let $x \in S$ and let $x^d + b_{d-1}x^{d-1} + \dots + b_0 = 0$ be an integral equation of x over R . Then x is integral over $R' := A[b_0, \dots, b_{d-1}]$ and so $R'[x]$ is a finite R' -algebra by 1.E.2 and hence a finite A -algebra by 1.E.4. Therefore x is integral over A by 1.E.2.

1.E.7. Corollary *For an A -algebra R , the following statements are equivalent:*
(1) R is a finite A -algebra. (2) R is of finite type and integral over A .

1.E.8. Example (1) For a monic polynomial $F = X^d + a_{d-1}X^{d-1} + \dots + a_0 \in A[X]$ the A -algebra $R = A[X]/(F) = A[x]$ is a finite A -algebra. The residue class x of X is integral over A because $x^d + a_{d-1}x^{d-1} + \dots + a_0 = F(x) = 0$. In fact, R is a free A -algebra of rank d with A -basis $1, x, \dots, x^{d-1}$.

(2) Let $F \in A[X_1, \dots, X_n]$ be a monic polynomial in X_n , i.e., $F = X_n^d + F_{d-1}X_n^{d-1} + \dots + F_0$ with $F_i \in A[X_1, \dots, X_{n-1}]$ and x_1, \dots, x_n be the residue classes of X_1, \dots, X_n modulo the principal ideal (F) . Then $A[X_1, \dots, X_n]/(F) = A[x_1, \dots, x_n]$ is a finite free algebra of rank d over the polynomial algebra $A[X_1, \dots, X_{n-1}] \cong A[x_1, \dots, x_{n-1}]$. This is a special case of (1). In case $A = K$ is a field, every non-zero polynomial $G \in K[X_1, \dots, X_n]$, after a change of variables, can be expressed, up to a constant, as a monic polynomial in X_n . We prove this in the next section, see 1.F.1.

(3) (Normalisation) Let A be a ring and let $Q := Q(A)$ be its total quotient ring. Then the integral closure \bar{A} of A in Q is called the normalisation of A . An integral domain A is called normal if $\bar{A} = A$. The normalisation of an integral domain A is the smallest subring of its quotient field Q which is normal and contains A .

For example: Every factorial domain is normal. In particular, polynomial rings over \mathbb{Z} or a field K are normal. For the proof note that if $x = a/b \in Q$ with $\text{GCD}(a, b) = 1$ and x is a zero of a polynomial $a_n X^n + \dots + a_0 \in A[X]$ then a divides a_0 and b divides a_n . More generally, $bX - a$ is a generator of the kernel of the substitution homomorphism $A[X] \rightarrow Q, X \mapsto a/b$.

(4) (Conductor) Let $A \subseteq R$ be a ring extension. Then the ideal $\mathfrak{C}_{R|A} := \text{Ann}_A R/A = \{a \in A \mid aR \subseteq A\}$ is called the conductor of R over A . It is the largest ideal in A which is also an ideal in R . If $\mathfrak{C}_{R|A}$ contains a non-zero divisor of A then $R \subseteq Aa^{-1}$ can be embedded in the total quotient ring $Q(A)$ of A . Moreover, R is then finite over A if A is Noetherian. The conductor of A is the ideal $\mathfrak{C}_A := \mathfrak{C}_{\bar{A}|A}$ where \bar{A} is the normalisation of A (see (3)).

(5) The following lemma gives an important property of a normal domain.

1.E.9. Lemma *Let A be a normal domain with quotient field Q . If an element x of a Q -algebra L (not necessarily a field) is integral over A then the minimal polynomial μ_x of x over Q has coefficients in A .*

PROOF. By extending L , we may assume that μ_x splits into linear factors over L (see also Exercise 1.E.10 (1) below). Let $f(x) = 0, f \in A[X]$, be an integral equation of x over A . Then μ_x divides f in $Q[X]$ and so, every zero y of μ_x is integral over A (with integral equation $f(y) = 0$). Therefore the coefficients of μ_x are integral over A by 1.E.5 and hence elements of A , since A is normal. •

(6) Let M be a numerical monoid, i.e. M is a submonoid of $\mathbb{N} = (\mathbb{N}, +)$ such that $\mathbb{N} \setminus M$ is finite. Let $A = K[M] := \{\sum_{m \in M} a_m T^m \in K[T]\} \subseteq K[T]$ be the monoid algebra of M over a field K . Then the polynomial algebra $K[T]$ is finite over $K[M]$, indeed, $\text{Dim}_K K[T]/K[M] = \text{Card}(\mathbb{N} \setminus M)$, and so $K[T]$ is integral over $K[M]$. Since T belongs to the quotient field of $K[M]$ and $K[T]$ is normal, $K[T]$ is the normalisation of $K[M]$. The K -algebra $K[M]$ is called the coordinate algebra of the monomial curve over K defined by M . (See Exercise 2.B.14 (3).)

(7) Let K be a field and let A be a normal K -subalgebra of $K[T], A \neq K$. Then A is a polynomial algebra $K[f]$ for some $f \in A$. (f is necessarily a non-constant polynomial in A of least degree.) For the proof, let $\mu_T = X^n + f_{n-1}X^{n-1} + \dots + f_0 \in Q(A)[X]$ be the minimal polynomial of T over $Q(A)$. By the lemma in (5), the coefficients $f_0, \dots, f_{n-1} \in A$. But every non-constant coefficient f of μ_T generates the field $Q(A)$ over K (see the proof of Lüroth's theorem in van der Waerden, B. L.: Algebra, Part I, § 73, p. 222). Then $K[f] \subseteq A \subseteq Q(A) = K(f)$ and $K[f] = A$, since $K[T]$ and hence A is integral over $K[f]$ and $K[f]$ is normal. (For Lüroth's theorem see also the end of Example 7.E.18.) •

As a consequence we get: *Let A be a K -subalgebra of $K[T], A \neq K$. Then the normalisation \bar{A} of A is a polynomial algebra $K[f]$ for some non-constant polynomial $f \in K[T]$. (Note that every K -subalgebra of $K[T]$ is a K -algebra of finite type.)*

In general a K -algebra A of finite type is called rational if it is an integral domain and if the quotient field $Q(A)$ of A is K -isomorphic to a rational function field $K(T_1, \dots, T_m)$ in m variables T_1, \dots, T_m . The integer m is nothing but the transcendence degree of the field

extension $K \subseteq Q(A)$. By Lüroth's theorem, any K -subalgebra A of $K(T)$, $A \neq K$, of finite type is rational with $m = 1$.

As an example, consider the K -algebra homomorphism $\varphi : K[X, Y] \rightarrow K[T]$ defined by $x := \varphi(X) = T^2 - 1$ and $y := \varphi(Y) = T(T^2 - 1)$ and the K -subalgebra $A := \text{im } \varphi$ of $K[T]$. Obviously, if $f \in K[X, Y]$ with $f \neq 0$ and $\deg_y f \leq 1$ then $f \notin \text{Ker } \varphi$, therefore $\text{Ker } \varphi$ is the principal ideal generated by $Y^2 - X^2 - X^3$. Since $T = y/x$ belongs to the quotient field of A , the polynomial algebra $K[T]$ is the normalization of $A \cong K[X, Y]/(Y^2 - X^2(X + 1))$.

1.E.10. Exercise (1) Let $A \subseteq B$ be a ring extension and let $H, G \in B[X]$ be monic polynomials such that $HG \in A[X]$. Then the coefficients of H and G are integral over A . If A is integrally closed in B then $H, G \in A[X]$. (**Hint:** There is a finite ring extension C of B (even a free one) such that H and G factor into monic linear factors in $C[X]$.)

(2) Let R be an A -algebra. Then the integral closure of $A[T_1, \dots, T_n]$ in $R[T_1, \dots, T_n]$ is $\bar{A}[T_1, \dots, T_n]$, where \bar{A} is the integral closure of A in R . (**Hint:** Assume $n = 1$. Let $g \in R[T]$ be integral over $A[T]$ with integral equation $0 = f(g) = g^n + f_{n-1}g^{n-1} + \dots + f_1g + f_0$. Let r be an integer larger than n and the degrees of f_{n-1}, \dots, f_0 and let $g_1 := g - T^r$. From

$$(g_1 + T^r)^n + f_{n-1}(g_1 + T^r)^{n-1} + \dots + f_1(g_1 + T^r) + f_0 = 0$$

one gets $(-g_1)(g_1^{n-1} + h_{n-1}g_1^{n-2} + \dots + h_1) = (T^r)^n + (T^r)^{n-1}f_{n-1} + \dots + (T^r)f_1 + f_0$ which is a monic polynomial in $A[T]$. Now use (1) to conclude that g_1 and hence g has coefficients in \bar{A} . In particular, if A is a normal integral domain then $A[T_1, \dots, T_n]$ too.

(3) (Graded integral extensions) a) Let $A \subseteq B$ be an extension of \mathbb{Z} -graded rings. Then the integral closure \bar{A} of A in B is a graded A -subalgebra of B . (**Hint:** Note that, by (2), $\bar{A}[T, T^{-1}]$ is the integral closure of $A[T, T^{-1}]$ in $B[T, T^{-1}]$. Now, use the fact that, for any graded ring $C = \bigoplus_{m \in \mathbb{Z}} C_m$, the map $C \rightarrow C[T, T^{-1}]$, $\sum_m c_m \mapsto \sum_m c_m T^m$, is an injective graded ring homomorphism.)

b) Let A be a \mathbb{Z} -graded integral domain. Then the normalization \bar{A} of A is a graded subalgebra of $S^{-1}A$ where S is the multiplicative system of non-zero homogeneous elements in A . If A is positively graded (i. e. $A_m = 0$ for $m < 0$) then \bar{A} is also positively graded.

1.E.11. Exercise Let $A \subseteq B$ be an extension of integral domains such that A is a direct summand of B as an A -module. Show that:

(1) If B is normal, then A is normal too. (**Hint:** Let $f, g \in A, g \neq 0$, and let f/g be integral over A . Then $f \in A \cap Bg = Ag$.)

(2) $\bar{B} \cap Q(A) = \bar{A}$, where \bar{A} and \bar{B} are the normalizations of A and B respectively. (**Hint:** Let f, g be as in (1). If $f/g \in \bar{B}$, then $f^n \in A \cap (Bf^{n-1}g + \dots + Bfg^{n-1} + Bg^n) = Af^{n-1}g + \dots + Afg^{n-1} + Ag^n$ for some $n \in \mathbb{N}^*$.)

1.F. Noether's Normalization Lemma and Its Consequences

First we prove the classical version of Noether's normalization lemma.

1.F.1. Lemma Let K be a field and $F \in K[X_1, \dots, X_n]$ be a non-constant polynomial. Then there exists a K -automorphism $\varphi : K[X_1, \dots, X_n] \rightarrow K[X_1, \dots, X_n]$ such that $\varphi(X_n) = X_n$ and $F = aX_n^d + f_{d-1}X_n^{d-1} + \dots + f_0$ where $a \in K^\times$ and $f_j \in K[Y_1, \dots, Y_{n-1}]$, $0 \leq j \leq d - 1$, $Y_i := \varphi(X_i)$, $1 \leq i \leq n - 1$.

PROOF. First assume that K is infinite. Then there exist $a_1, \dots, a_{n-1} \in K$ such that $Y_i = \varphi(X_i) := X_i - a_i X_n, 1 \leq i \leq n - 1$, serves the purpose. To prove this let $F = F_0 + F_1 + \dots + F_d$, where $F_m \in K[X_1, \dots, X_n]$ is the homogeneous component of degree m of $F, 0 \leq m \leq d := \deg F$. For any $a_1, \dots, a_{n-1} \in K$, put $Y_i := X_i - a_i X_n, 1 \leq i \leq n - 1$. Then

$$\begin{aligned}
 F &= \sum_{m=0}^d F_m(Y_1 + a_1 X_n, \dots, Y_{n-1} + a_{n-1} X_n, X_n) \\
 &= \sum_{m=0}^d (F_m(a_1, \dots, a_{m-1}, 1) X_n^m + \sum_{j=0}^{m-1} f_{mj}(Y_1, \dots, Y_{n-1}) X_n^j)
 \end{aligned}$$

where $f_{mj} \in K[Y_1, \dots, Y_{n-1}]$ are homogeneous polynomials of degree $m - j$. Now, since $F_d(X_1, \dots, X_{n-1}, 1) \neq 0$ and K is infinite, we can choose $a_1, \dots, a_{n-1} \in K$ such that $a := F_d(a_1, \dots, a_{n-1}, 1) \neq 0$.

In the general case, there exist positive integers $\gamma_1, \dots, \gamma_{n-1}$ such that $Y_i = \varphi(X_i) := X_i - X_n^{\gamma_i}, 1 \leq i \leq n - 1$, serves the purpose. Let $F = \sum_{\alpha \in \Lambda} a_\alpha X^\alpha$ where Λ is a finite subset of \mathbb{N}^n and $a_\alpha \in K^\times$ for every $\alpha = (\alpha_1, \dots, \alpha_n) \in \Lambda$. For any positive integers $\gamma_1, \dots, \gamma_{n-1}$, put $Y_i := X_i - X_n^{\gamma_i}, 1 \leq i \leq n - 1$. Then

$$F = \sum_{\alpha \in \Lambda} a_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n} = \sum_{\alpha \in \Lambda} a_\alpha (Y_1 + X_n^{\gamma_1})^{\alpha_1} \dots (Y_{n-1} + X_n^{\gamma_{n-1}})^{\alpha_{n-1}} X_n^{\alpha_n}.$$

For $\gamma = (r, r^2, \dots, r^{n-1}, 1)$, where r is an integer bigger than all the components of all $\alpha = (\alpha_1, \dots, \alpha_n) \in \Lambda$, we have $\deg_\gamma X^\alpha \neq \deg_\gamma X^\beta$ for all $\alpha, \beta \in \Lambda, \alpha \neq \beta$. Therefore, there exists a unique $\nu \in \Lambda$ such that $d := \deg_\gamma F = \deg_\gamma X^\nu (> 0)$ and so $F = a_\nu X_n^d + f_{d-1} X_n^{d-1} + \dots + f_0, f_j \in K[Y_1, \dots, Y_{n-1}]$. •

An affine transformation of a polynomial algebra $A[X_1, \dots, X_n]$ is an A -algebra automorphism φ defined by $\varphi(X_j) = \sum_{i=1}^n a_{ij} X_i + b_j, 1 \leq j \leq n$, where $(a_{ij}) \in GL_n(A)$ and $(b_j) \in A^n$. If (a_{ij}) is the identity matrix then φ is called a translation, if $(b_j) = 0$ then φ is called linear. In the proof of Lemma 1.F.1 for an infinite field K , we have used a simple linear transformation of $K[X_1, \dots, X_n]$.

Now we prove Noether's normalization lemma with the help of the above lemma.

1.F.2. Noether's Normalization Lemma *Let K be a field and $R = K[x_1, \dots, x_n]$ be a K -algebra of finite type. Then there exist $z_1, \dots, z_m \in R$ which are algebraically independent over K such that R is integral (and hence finite) over the K -subalgebra $K[z_1, \dots, z_m]$. – If x_1, \dots, x_n are algebraically dependent over K then $m < n$.*

PROOF. We prove the assertion by induction on n . In case x_1, \dots, x_n are algebraically independent over K we are through. Otherwise, let $F \in K[X_1, \dots, X_n], F \neq 0$, be such that $F(x_1, \dots, x_n) = 0$. By the previous lemma, we can write

$$F = a X_n^d + f_{d-1} X_n^{d-1} + \dots + f_0$$

with $f_j \in K[Y_1, \dots, Y_{n-1}]$ and $a \in K^\times$, where Y_1, \dots, Y_{n-1} are as in 1.F.1. Therefore,

$$0 = a^{-1}F(x_1, \dots, x_n) = x_n^d + a^{-1} \sum_{j=1}^d f_{d-j}(y_1, \dots, y_{n-1})x_n^{d-j}$$

where $y_j := Y_j(x_1, \dots, x_n)$. This shows that x_n is integral over $K[y_1, \dots, y_{n-1}]$ and so $K[x_1, \dots, x_n] = K[y_1, \dots, y_{n-1}, x_n]$ is integral over $K[y_1, \dots, y_{n-1}]$. By induction hypothesis there exist $z_1, \dots, z_m \in K[y_1, \dots, y_{n-1}]$, $m \leq n-1$, which are algebraically independent over K such that $K[y_1, \dots, y_{n-1}]$ is integral over $K[z_1, \dots, z_m]$. Now, the assertion follows from Corollary 1.E.6. •

1.F.3. Remark If in Noether's normalization lemma R is an integral domain then m is the transcendence degree of the field of fractions $Q(R)$ over K and therefore uniquely determined. Even for an arbitrary K -algebra R of finite type, the non-negative integer m is uniquely determined. It is in fact the Krull-dimension of the (Noetherian) ring R . See Theorem 3.B.8 (and 3.B.14).

The normalization lemma has many consequences as we will see in these lectures. One example is the following:

1.F.4. Example A hypersurface algebra over a field K is a K -algebra of the form $K[X_1, \dots, X_n]/(f)$ for some $n \in \mathbb{N}$ and a non-constant polynomial $f \in K[X_1, \dots, X_n]$. Besides polynomial algebras these are the simplest K -algebras of finite type.

For any algebra R of finite type over a field K of characteristic zero which is an integral domain, there exists a hypersurface algebra $H \subseteq R$, $H \cong K[X_1, \dots, X_n]/(f)$, with quotient field $Q(R)$ and the same normalization as R , that is, $\bar{R} = \bar{H}$.

PROOF. Let $P = K[z_1, \dots, z_m] \subseteq R$ be a Noether's normalization of R as in 1.F.2. Since the characteristic of K is zero, the quotient field $Q(R)$ is finite separable over the function field $K(z_1, \dots, z_m)$. Therefore by the primitive element theorem, there exists an element $\alpha \in Q(R)$ such that $Q(R) = K(z_1, \dots, z_m)[\alpha]$. By the following Lemma 1.F.5 (2) $Q(R) = S^{-1}R$ where $S := K[z_1, \dots, z_m] \setminus \{0\}$ and hence we may assume that $\alpha \in R$. Then $H := P[\alpha] \cong K[z_1, \dots, z_m][X]/(\mu_\alpha)$ where μ_α is the minimal polynomial of α over $Q(P)$ (cf. Lemma 1.E.9) which is a hypersurface algebra contained in R with $Q(H) = Q(R)$. Further, $\bar{H} = \bar{R}$ is the integral closure of P in $Q(H) = Q(R)$. •

The above statement is also true for a perfect field K of characteristic $p > 0$. (Use 6.D.12 (3) and Exercise 6.D.26.)

1.F.5. Lemma Let $A \subseteq B$ be an algebraic extension of integral domains, i.e. the field extension $Q(A) \subseteq Q(B)$ is algebraic. Then:

- (1) If \mathfrak{b} is an ideal $\neq 0$ in B , then $\mathfrak{b} \cap A \neq 0$.
- (2) If A is a field, then B is a field.
- (3) If B is integral over A and if B is a field, then A is a field.

PROOF. (1) Let $b \in \mathfrak{b}$, $b \neq 0$, and $a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0 = 0$ be a non-trivial algebraic equation of b over A . If necessary, cancelling a power of b , we may assume that $a_0 \neq 0$. Then $a_0 \in (Bb) \cap A \subseteq \mathfrak{b} \cap A$.

(2) Let A be a field and let $b \in B$, $b \neq 0$. Then $(Bb) \cap A \neq 0$ by (1) and so $(Bb) \cap A = A$ and $Bb = B$.

(3) Let B be a field and let $a \in A$, $a \neq 0$. Then $a^{-1} \in B$ and therefore we have an equation $a^{-n} + a_{n-1} a^{-(n-1)} + \cdots + a_0 = 0$ for some $a_0, \dots, a_{n-1} \in A$. Multiplying by a^n , we get $1 = -(a_{n-1} + \cdots + a_0 a^{n-1}) a \in A$ and so $a^{-1} \in A$. •

Now we deduce the famous Hilbert's nullstellensatz from Noether's Normalization Lemma 1.F.2.

1.F.6. Hilbert's Nullstellensatz (algebraic version) *Let $K \subseteq L$ be a field extension. If L is a K -algebra of finite type then L is a finite extension of K .*

PROOF. By the normalization lemma there exist $z_1, \dots, z_m \in L$ which are algebraically independent over K such that $K[z_1, \dots, z_m] \subseteq L$ is a finite extension. We have to show that $m = 0$, which follows from 1.F.5 (3). •

A reformulation of 1.F.6 is the following corollary.

1.F.7. Corollary *Let K be a field and let R be a K -algebra of finite type. Then, for every maximal ideal $\mathfrak{m} \subseteq R$, the field R/\mathfrak{m} is a finite extension of K .*

For a ring R , the set of all maximal ideals of R is called the maximal spectrum of R and is denoted by

$$\text{Spm } R.$$

If $R \neq 0$ then $\text{Spm } R \neq \emptyset$. This is Krull's theorem which is an easy consequence of Zorn's lemma. Of course, in the Noetherian case, it is an immediate consequence of the Noetherian condition for the ideals of R .

For an algebraically closed field K , the maximal spectrum of a polynomial algebra over K has a simple description:

1.F.8. Corollary *Let K be an algebraically closed field. Then the map*

$$a = (a_1, \dots, a_n) \mapsto \mathfrak{m}_a := (X_1 - a_1, \dots, X_n - a_n)$$

from K^n to $\text{Spm } K[X_1, \dots, X_n]$ is bijective.

PROOF. For any $a \in K^n$, the ideal \mathfrak{m}_a is the kernel of the substitution homomorphism $K[X_1, \dots, X_n] \rightarrow K$, $X_i \mapsto a_i$, and therefore maximal.

For $\mathfrak{m} \in \text{Spm } K[X_1, \dots, X_n]$, $K[X_1, \dots, X_n]/\mathfrak{m} = K$ by Corollary 1.F.7. Therefore, there exists $a = (a_1, \dots, a_n) \in K^n$ such that $X_i \equiv a_i \pmod{\mathfrak{m}}$ for $i = 1, \dots, n$ and so $\mathfrak{m}_a \subseteq \mathfrak{m}$. Therefore $\mathfrak{m} = \mathfrak{m}_a$. •

Of course, if K is not algebraically closed and $n \geq 1$, then there are maximal ideals in $K[X_1, \dots, X_n]$ which are not point ideals \mathfrak{m}_a , $a \in K^n$. For example, the principal ideal $(X^2 + 1) \subseteq \mathbb{R}[X]$ is a maximal ideal in $\mathbb{R}[X]$, but not of the form $(X - a)$ for any $a \in \mathbb{R}$.

In general, the contraction $\varphi^{-1}(\mathfrak{m})$ of a maximal ideal $\mathfrak{m} \in \text{Spm } S$ with respect to a ring homomorphism $\varphi : R \rightarrow S$ is not a maximal ideal in R . However, for K -algebras of finite type, we have:

1.F.9. Theorem *Let K be a field and let $\varphi : R \rightarrow S$ be a homomorphism of K -algebras of finite type. Then, for every $\mathfrak{m} \in \text{Spm } S$, $\varphi^{-1}(\mathfrak{m}) \in \text{Spm } R$.*

PROOF. Since $K \hookrightarrow R/\varphi^{-1}(\mathfrak{m}) \hookrightarrow S/\mathfrak{m}$ and S/\mathfrak{m} is a finite field extension of K by 1.F.7, $R/\varphi^{-1}(\mathfrak{m})$ is also a field. •

1.F.10. Remark For an uncountable field, there is a very simple proof of 1.F.6, more precisely we prove:

1.F.11. Proposition *Let K be an uncountable field and let $K \subseteq L$ be a field extension. If L is countably generated as a K -algebra then L is algebraic over K .*

PROOF. If $x \in L$ is transcendental over K then $K(x) \subseteq L$ is a rational function field over K and the elements $1/(x - a)$, $a \in K$, in $K(x)$ are linearly independent over K . In particular, L is a K -vector space of uncountable dimension, but any countably generated K -algebra has countable K -vector space dimension. •

We have the following partial generalization of Noether's normalization lemma:

1.F.12. Proposition *Let $A \subseteq R$ be an extension of integral domains such that R is an A -algebra of finite type. Then there exist an element $f \in A$, $f \neq 0$, and elements $z_1, \dots, z_m \in R$ such that z_1, \dots, z_m are algebraically independent over A and R_f is finite over $A_f[z_1, \dots, z_m]$.*

PROOF. Let $R = A[x_1, \dots, x_n]$ and let $K := Q(A)$ and $L := Q(R)$ be the quotient fields of A and R respectively. By 1.F.2 there are elements $z_1, \dots, z_m \in K[x_1, \dots, x_n] \subseteq L$ which are algebraically independent over K such that the algebra $K[x_1, \dots, x_n]$ is finite over $K[z_1, \dots, z_m]$. We may assume that $z_1, \dots, z_m \in R$. If $f \in A$, $f \neq 0$, is a common denominator of the coefficients of integral equations of x_1, \dots, x_n over $K[z_1, \dots, z_m]$ then $R_f = A[x_1, \dots, x_n, 1/f] = A_f[x_1, \dots, x_n]$ is integral over $A_f[z_1, \dots, z_m]$. •

As an application, we consider the polynomial algebra $R := A[X_1, \dots, X_n]$, $n \geq 1$, over an integral domain A . Then there exists a maximal ideal $\mathfrak{M} \in \text{Spm } R$ with $\mathfrak{M} \cap A = 0$ if and only if $Q(A) = A_f$ for some $f \neq 0$ in A . Proof. If $Q(A) = A_f$ then $(fX_1 - 1, X_2, \dots, X_n)$ is such a maximal ideal. Conversely, if \mathfrak{M} is such a maximal ideal then by the proposition there exists an element $f \in A$, $f \neq 0$, and elements z_1, \dots, z_m in the field $L := R/\mathfrak{M}$ such that z_1, \dots, z_m are

algebraically independent over A and L is finite over $A_f[z_1, \dots, z_m]$. However, by 1.F.5 (3) $A_f[z_1, \dots, z_m]$ is also a field which means $m = 0$ and $A_f = Q(A)$.

For example, in a principal ideal domain A , there exists an element $f \in A$, $f \neq 0$, with $Q(A) = A_f$ if and only if A has only a finite number of prime ideals. Therefore we have: *Let A be a principal ideal domain with infinitely many prime ideals. Then for every maximal ideal $\mathfrak{M} \in \text{Spm}A[X_1, \dots, X_n]$ the ideal $\mathfrak{m} := \mathfrak{M} \cap A$ is maximal in A and $A[X_1, \dots, X_n]/\mathfrak{M}$ is finite over A/\mathfrak{m} .* In particular, for every maximal ideal \mathfrak{M} in $\mathbb{Z}[X_1, \dots, X_n]$, the residue class field $\mathbb{Z}[X_1, \dots, X_n]/\mathfrak{M}$ is finite. In other words, a field of characteristic zero is never a \mathbb{Z} -algebra of finite type.