4. Noether normalisation

We shall say that a ring R is an *affine ring* (or *affine k-algebra*) if R is isomorphic to a polynomial ring over a field k with finitely many indeterminates modulo an ideal, i.e., $R \simeq k[T_1, \ldots, T_n]/I$. According to Hilbert's Basis Theorem any affine ring is Noetherian. In his early algebra work in the 1890's Hilbert gave a structure theorem for affine algebras over a field k (at least in the graded case over an infinite field), generalized later by Noether and Nagata, and nowadays called *Noether normalization.* It says that any affine algebra R over a field k has a subring S, which is isomorphic with a polynomial ring $k[X_1, \ldots, X_d]$ and such that R is finitely generated when considered as an S-*module*, see [2, §. 15.3]. We prove a slighly more general result in this section. The integer d does not depend on the choice of S and will be called the *dimension* of the affine k-algebra R. It is an important integer related to the more familiar notion of dimension of a manifold or of a vector space.

4.1. **Field extensions.** Hilbert was motivated by a well-known result in the theory of field extensions. Let $k \subset K$ be a field extension. If $x_1, \ldots, x_n$ is any collection of elements of K, we denote by $k(x_1, \ldots, x_n)$ the *subfield* of K generated by k and $\{x_1, \ldots, x_n\}$.

We say $x_1, \ldots, x_d \in K$ are *algebraically independent* over k, if there is no non-zero polynomial $F(X_1, \ldots, X_d) \in k[X_1, \ldots, X_d]$ such that $F(x_1, \ldots, x_d) = 0$. Or, equivalently, the k-algebra homomorphism $k[X_1, \ldots, X_d] \to K$ obtained by substituting x_i for X_i is injective.

We say $x \in K$ is *algebraic* over k if there is a non-zero polynomial $F(X) \in k[X]$ such that $F(x) = 0$, i.e., the kernel of $k[X] \to K : X \mapsto x$ is non-zero. Since the ring $k[X]$ is a principal domain, there is unique monic (or unitary) polynomial that generates this kernel. This polynomial is called the *minimal polynomial* of x over k and is an important tool in field theory. We recall that any polynomial ring over a field with finitely many variables is a factorial domain; in particular a polynomial is irreducible if and only if it is a prime element, see [2, §. 9.3].

We say that the field extension $k \subset K$ has finite *transcendence degree* d if d is minimal for the property that there are elements $x_1, \ldots, x_d$ in K that are algebraically independent over k and such that any element of K is algebraic over the subfield $k(x_1, \ldots, x_d)$. Such collection of elements $x_1, \ldots, x_d$ is then called a *transcendence basis* for the extension.

Suppose $K = k(y_1, \ldots, y_n)$, i.e., K is finitely generated by $\{y_1, \ldots, y_n\}$ as a field extension of k. By permuting the generators if necessary we can arrange that $y_1, \ldots, y_\delta$ are algebraically independent over k, and each y_i is algebraic over $k(y_1, \ldots, y_\delta)$. Then from the next lemma it follows easily that necessarily $\delta = d$ is the transcendence degree of the extension $k \subset K$ and so $y_1, \ldots, y_d$ is necessarily already a transcendence basis.

Lemma 4.1 (Replacement Lemma)**.** *Let $k \subset K$ be a field extension with finite transcendence degree d and let $x_1, \ldots, x_d$ be a transcendence basis. Suppose $y_1, y_2, \ldots, y_n \subset K$ are algebraically independent over k. Then $n \leq d$, and there is a reordering of the x_i's such that $y_1, \ldots, y_n, x_{n+1}, \ldots, x_d$ is also a transcendence basis for $k \subset K$.*

Proof. We remark that this result is mentioned in [2, §14.9], but not proved there. The proof is nevertheless a bit tricky, so we shall give it here.

Since $x_1, \ldots, x_d$ is a transcendence basis, any element of K is algebraic over $k(x_1, \ldots, x_d)$. Let

$$F_{\min} = Y^r + \phi_1 Y^{r-1} + \ldots + \phi_r$$

be the minimum polynomial of y_1, where each ϕ_i is an element of $k(x_1, \ldots, x_d)$, i.e. a rational function in the algebraically independent variables $\{x_1, \ldots, x_d\}$ with coefficients in k. Let $f_0 \in k[x_1, \ldots, x_d]$ be a common denominator of all the coefficients of $F_{\min}$, then the product $f_0 \cdot F_{\min} \in k[x_1, \ldots, x_d][Y] = k[x_1, \ldots, x_d, Y]$, i.e. is a polynomial. Since $k[x_1, \ldots, x_d, Y]$ is a polynomial ring there is a factorisation of $f_0 \cdot F_{\min}$ into a product of irreducible polynomials. If we substitute $Y := y_1$ we obtain 0, hence there must be an irreducible factor, say F, that also becomes 0 when we make the substitution $Y := y_1$. Necessarily F contains the variable Y. If we see F as an element of $k(x_1, \ldots, x_d)[Y]$ it has at most degree r in the variable Y, since it divides $f_0 \cdot F_{\min}$. On the other hand, since it vanishes at $Y := y_1$ it is divisible by the minimum polynomial $F_{\min}$, so the degree in the variable Y is at least r, hence exactly r. It follows that we can write $f_0 \cdot F_{\min} = g \cdot F$, where $g \in k[x_1, \ldots, x_d]$ and $F \in k[x_1, \ldots, x_d, Y]$ irreducible. Say

$$F = h_0 Y^r + h_1 Y^{r-1} + \ldots + h_r$$

where each $h_i \in k[x_1, \ldots, x_d]$ and $h_0 \neq 0$. Notice that in fact $\frac{1}{h_0} F = F_{\min}$. So in fact we get that

$$F = h_0 F_{\min}$$

is irreducible in $k[x_1, \ldots, x_d, Y]$ and vanishes when we substitute $Y := y_1$.

Let $G = g_0 Y^e + g_1 Y^{e-1} + \ldots + g_e$ in $k[x_1, \ldots, x_d, Y]$ (where each $g_i \in k[x_1, \ldots, x_d]$) be another polynomial that vanishes when we substitute $Y := y_1$. Then we claim that F divides G in the polynomial ring $k[x_1, \ldots, x_d, Y]$. At least $F_{\min}$ divides G in the ring $k(x_1, \ldots, x_d)[Y]$, by the fundamental property of the minimal polynomial. So, by getting rid of denominators, we get that there are $p, q \in k[x_1, \ldots, x_d]$ and $H \in k[x_1, \ldots, x_d, Y]$ such that $pG = qFH$. So F divides pG in $k[x_1, \ldots, x_d, Y]$, and does not divide p (since p does not contain the variable Y). So F divides G, since F is irreducible and therefore a prime element in $k[x_1, \ldots, x_d, Y]$; which proves the claim.

In the polynomial F one of the variables $x_1, \ldots, x_d$ must occur non-trivially, say x_1, since otherwise y_1 would be even algebraic over k, which it isn't by assumption. So we can write

$$F = p_0 x_1^a + p_1 x_1^{a-1} + \ldots + p_a, \tag{1}$$

where each $p_i \in k[x_2, \ldots, x_d, Y]$, $p_0 \neq 0$ and $a \geq 1$.

Suppose the coefficient p_0 vanishes after substitution $Y := y_1$. Then we proved before that F necessarily divides p_0. In particular x_1 occurs in p_0; which is a contradiction. So $p_0(x_2, \ldots, x_d, y)) \neq 0$ and it follows from equation (1) that x_1 is algebraic over the subfield $k(x_2, \ldots, x_d, y_1)$ (hence any element of K too, the argument for this will be seen later this section). By minimality of d it follows that $y_1, x_2, \ldots x_d$ are algebraically independent over k and also form a transcendence basis of K over k.

We repeat the argument with y_2 and $k(y_1, x_2, \ldots, x_d)$ and get again an irreducible polynomial F in $k[y_1, x_2, \ldots, x_d, Y]$ that can be expanded as

$$F = h_0 Y^r + h_1 Y^{r-1} + \ldots + h_d,$$

with $h_i \in k[y_1, x_2, \ldots, x_d]$, $h_0 \neq 0$ and such that F vanishes after substitution $Y := y_2$. In the polynomial F one of the variables $x_2, \ldots, x_d$ must occur non-trivially, say x_2, since otherwise y_1 and y_2 would not be algebraically independent over k. So we have an expansion

$$F = p_0 x_2^a + p_1 x_2^{a-1} + \ldots + p_a,$$

where each coefficient $p_i \in k[y_1, x_3, \ldots, x_d, Y]$, $p_0 \neq 0$ and $a \geq 1$.

Suppose the polynomial p_0 vanishes after substitution $Y := y_2$. Then F divides p_0, so x_2 occurs in p_0; which is a contradiction. So $p_0(y_1, x_3, \ldots, x_d, y_2) \neq 0$ and it follows that x_2 (hence K) is algebraic over $k(y_1, y_2, x_3, \ldots, x_d)$. By minimality of d it follows that $y_1, y_2, d_3 \ldots x_d$ are algebraically independent over k and also form a transcendence basis.

We proceed in a similar fashion, to complete the proof. □

4.2. **Integral extensions.** To generalize we need to modify some notions of field extensions to ring extensions. Let $R \subset S$ be a subring. An element $s \in S$ is *integral* over R (see [2, §15.3]) if there is a unitary polynomial $F(X) = X^n + r_1 X^{n-1} + \ldots + r_n \in R[X]$ such that $F(s) = 0$. If every element of S is integral over R we say that S is *integral over* R.

There is a big difference with field theory, in that there is no minimal such polynomial. Let $\mathrm{ev}_s : R[X] \to S$ be the ring homomorphism obtained by substituting $X := s$, with kernel I say. Then s is integral over R if I contains a monic polynomial. In general it is no longer true that I is a principal ideal, or if so it need not be generated by a monic polynomial!

For example, if the extension is $\mathbb{Z} \subset \mathbb{Q}$ and $s = \frac{1}{2}$ then the kernel is principal generated by $2X - 1$, but it does not contain a monic polynomial. So $\frac{1}{2}$ is not integral over $\mathbb{Z}$. Or, in the situation of the extension $\mathbb{Q}[U] \subset \mathbb{Q}[U, W]/(UW, W^2)$ and $s = \overline{W}$, then the kernel is not a principal ideal and generated by XU and X^2 (monic!). This time $\overline{W}$ is integral over $\mathbb{Q}[U]$.

Proposition 4.1. *Let $R \subset S$ be an extension of rings. The following are equivalent:*

(i) $s \in S$ is integral over R;

(ii) $R[s]$ is finitely generated as an R-module;

(iii) $R[s]$ is contained in a subring B of S, such that B is finitely generated as an R-module.

(iv) There is an $R[s]$-module with trivial annihilator, that is finitely generated as R-module.

Proof. (i) implies (ii): Suppose $s \in S$ is integral over R, hence there is a relation

$$s^n = -(r_1 s^{n-1} + \ldots + r_n),$$

so $R[s]$ is generated as R-module by $\{1, s, s^2, \ldots, s^{n-1}\}$.

(ii) implies (iii): Trivial: take $B = R[s]$.

(iii) implies (iv): Let $F \in R[s]$ be in the annihilator of B, as in the assumption of (iii). Then in particular $F = F \cdot 1 = 0$. So the annihilator of B as $R[s]$-module is trivial.

(iv) implies (i): Let M be an $R[s]$-module with trivial annihilator and finitely generated as R-module, say by $m_1, \ldots, m_n$. Put $\delta_{ij} = 0$ if $i \neq j$ and $\delta_{ij} = 1$ if $i = j$. There is an $n \times n$ matrix B of coefficients r_{ij} in R such that $s \cdot m_j = \sum_{i=1}^n r_{ij} m_i$, so $\sum_{i=1}^n (s\delta_{ij} - r_{ij}) m_i = 0$. Consider the $n \times n$ matrix A with coefficients $A_{ij} = s\delta_{ji} - r_{ji}$. It has an adjoint matrix A^* also with coefficients in $R[s]$, such that $A^* A = \det(A)\mathbf{1}$, where $\mathbf{1}$ is the $n \times n$ identity matrix. This is a consequence of

the Laplace expansion of the determinant in linear algebra. Or

$$\sum_k A^*_{ik}A_{kj} = \sum_k A^*_{ik}(s\delta_{jk} - r_{jk}) = \det(A)\delta_{ij}.$$

So

$$0 = \sum_k A^*_{jk} \sum_i (s\delta_{ik} - r_{ik})m_i = \sum_{i,k} A^*_{jk}A_{ki}m_i = \sum_i \det(A)\delta_{ji}m_i = \det(A)m_j$$

So $\det(A)$ annihilates M, hence $\det(A) = 0$. The characteristic polynomial of the matrix B is the determinant of $X\mathbf{1} - B$, so by substituting $X := s$ we get $\det A$, hence 0. The characteristic polynomial is of the form

$$s^n + r_1 s^{n-1} + r_2 X^{n-2} + \ldots + r_n$$

where the coefficients are some polynomials in the coefficients of B, hence are elements of R. We found a monic polynomial with coefficients in R that has s as zero. So s is integral over R. □

Remark. In the proof above we used a generalization of the Cayley-Hamilton theorem of linear algebra, that says that if $f(X)$ is the characteristic polynomial of square matrix A over a field, then $f(A)$ is the zero matrix.

If M is a finitely generated module over a ring R and $\phi : M \to M$ an R-homomorphism, then there is a monic polynomial $F(X) \in R[X]$ such that the endomorphism $F(\phi)$ acts trivially on M. The proof is the same as the proof in the proposition above.

Corollary 4.1. *(i) Let $s_1, \ldots, s_n$ elements of S that are integral over R, then $R[s_1, \ldots, s_n]$ is a subring that is finitely generated as an R-module.*

(ii) Let C be the collection of elements in S that are integral over R. Then C is a subring of S.

(iii) If $R \subset S \subset T$ are rings such that S is integral over R and T integral over S, then T is integral over R.

Proof. Suppose T is a finite S-module (say generated by $t_1, \ldots, t_n$), and S a finite R-module (say by $s_1, \ldots, s_m$). Then the $s_i t_j$'s generate T as R-module.

(i) $R[s_1]$ is finitely generated as R-module, and $R[s_1, s_2]$ is finitely generated as $R[s_1]$- module, hence also as R-module. Etcetera.

(ii) Let s_1, s_2 be integral over R, then $s_1 - s_2$ and $s_1 s_2$ are contained in $R[s_1, s_2]$, which is finite;y generated as R-module. Then apply the proposition.

(iii) Let $t \in T$. It is integral over S, say with integral equation

$$t^n + s_1 t^{n-1} + s_2 t^{n-2} + \ldots + s_n,$$

with each $s_i \in S$. So t is also integral over the subring $R[s_1, \ldots, s_n]$ and therefore $R[s_1, \ldots, s_n, t]$ is finitely generated as a module over $R[s_1, \ldots, s_n]$ (by the powers $1, t, \ldots, t^{n-1}$). Each s_i is integral over R, hence by (i) $R[s_1, \ldots, s_n]$ is finitely generated as R-module. Combining we get that $R[s_1, \ldots, s_n, t]$ is also finitely generated as R-module. So by Proposition 4.1, t is integral over R. □

The ring C in (ii) is called the *integral closure* of R in S. If $R = C$, then R is called *integrally closed* in S. In particular C is integrally closed in S. For example, $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Now a version of the Noether normalization is as follows.

Theorem 4.1 (Noether normalization)**.** *Let $S := k[X_1, \ldots, X_n]$ be a polynomial ring over a field k and let $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_m \neq S$ be a sequence of ideals in S.*

There exist $x_1, \ldots, x_n$ in S that are algebraically independent over k (put $R := k[x_1, \ldots, x_n]$), such that

(i) the ring extension $R \subset S$ is integral (or equivalently, such that S is a finitely generated module over R)

(ii) and there is a sequence of integers $d_1 \geq d_2 \geq \ldots \geq d_m$ such that

$$I_i \cap R = (x_{d_i+1}, x_{d_i+2}, \ldots, x_n) \lhd R.$$

The proof will use a repeated application of the following special case.

Lemma 4.2 (Nagata)**.** *Let $S := k[X_1, \ldots, X_n]$ be a polynomial ring over a field k and $F \in S$ a non-constant polynomial.*

There exist $x_1, \ldots, x_{n-1}$ in S, such $x_1, \ldots, x_{n-1}, F$ are algebraically independent over k, and such that

(i) for some fixed e each x_i is of the form $x_i = X_i - X_n^{e^i}$;

(ii) the ring extension $R := k[x_1, \ldots, x_{n-1}, F] \subset S$ is integral (or equivalently, S is a finitely generated module over R)

(iii) and $F \cdot S \cap R = F \cdot R$.

Proof. Let $e \geq 1$ be any integer that is larger than any of the exponents of the X_i that occur in F. Put $x_i := X_i - X_n^{e^i}$, or $X_i = x_i + X_n^{e^i}$, for $1 \leq i < n$. Any monomial we can expand as polynomial in X_n with coefficients in $k[x_1, \ldots, x_{n-1}]$:

$$\begin{aligned} X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n} &= (x_1 + X_n^e)^{a_1} (x_2 + X_n^{e^2})^{a_2} \cdots (x_{n-1} + X_n^{e^{n-1}})^{a_{n-1}} X_n^{a_n} \\ &= X_n^{a_n + a_1 e + a_2 e^2 + \ldots + a_{n-1} e^{n-1}} + \text{lower order terms} \end{aligned}$$

Now in elementary number theory, if $(a_1, a_2, \ldots, a_n) \neq (b_1, b_2, \ldots, b_n)$ and each a_i and b_i is a non-negative integer smaller than e, then also

$$a_n + a_1 e + a_2 e^2 + \ldots + a_{n-1} e^{n-1} \neq b_n + b_1 e + b_2 e^2 + \ldots + b_{n-1} e^{n-1}.$$

Among all monomials $X_1^{a_1} X_2^{a_2} \cdots X_n^{a_n}$ appearing in F there is therefore a unique one where $d := a_n + a_1 e + a_2 e^2 + \ldots + a_{n-1} e^{n-1}$ is maximal, say with coefficient $c_0 \in k$. Then we can expand F as polynomial in X_n with coefficients in $k[x_1, \ldots, x_{n-1}]$ and get

$$F = c_0 X_n^d + \text{lower order terms} ,$$

say $c_0^{-1} F = X_n^d + c_1 X_n^{d-1} + \ldots, + c_d$ for some $c_i \in k[x_1, \ldots, x_{d-1}]$. Since F is non-constant $d \geq 1$. Hence we get a integrality relation

$$X_n^d + c_1 X_n^{d-1} + \ldots, + c_{d-1} X_n + (c_d - c_0^{-1} F)$$

for X_n over $k[x_1, \ldots, x_{n-1}, F]$. It follows that S is integral over $k[x_1, \ldots, x_{n-1}, F]$. If $x_1, \ldots, x_{n-1}, F$ are not algebraically independent, then the transcendence degree of the quotient field of R over k, (and hence also of $k(X_1, \ldots, X_n)$ over k) is less than n, contradiction.

We still have to show (iii). Of course $F \cdot R \subseteq F \cdot S \cap R$. Any $f \in F \cdot S \cap R$ can be written as $f = F \cdot G$ with $G \in S$. We have an integrality relation

$$G^e + b_1 G^{e-1} + \ldots + b_e = 0$$

with $b_i \in R$. So multiplying by F^e we get

$$f^e + b_1 F f^{e-1} + \ldots + b_e F^e = 0$$

inside the polynomial ring R. From which it follows that F divides f inside R, or $f \in F \cdot R$. □

Remark. There is a different version of this lemma (due to Noether) that works when the field is infinite. In that case we can assume that each x_i is a k-linear combination of the X_j's, see [3, Lemma 13.2].

Proof of Theorem 4.1. We shall use induction on n starting from the trivial case $n = 0$. Suppose the result is true for less than n variables. We can also suppose that all ideals are non-zero.

Let F be a non-zero element of I_1. Since $I_m \neq S$, F is not a constant and we can apply Lemma 4.2 to get $x_1, \ldots, x_{n-1}, x_n$ in S that are algebraically independent over k, with $F = x_n$, and such that the ring extension $R := k[x_1, \ldots, x_n] \subset S$ is integral and $F \cdot S \cap R = F \cdot R$. From this it is no loss of generality to suppose that the variable X_n is contained in all the ideals.

Now consider the sequence of ideals $J_i := I_i \cap k[X_1, \ldots, X_{n-1}]$. By induction, there are exist $x_1, \ldots, x_{n-1}$ in $k[X_1, \ldots, X_{n-1}]$ that are algebraically independent over k such that

(i) the ring extension $k[x_1, \ldots, x_{n-1}] \subset k[X_1, \ldots, X_{n-1}]$ is integral

(ii) and there is a sequence of integers $d_1 \geq d_2 \geq \ldots \geq d_m$ such that

$$I_i \cap k[x_1, \ldots, x_{n-1}] = J_i \cap k[x_1, \ldots, x_{n-1}] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_{n-1}) \lhd k[x_1, \ldots, x_{n-1}].$$

It follows that the ring extension $k[x_1, \ldots, x_{n-1}, X_n] \subset k[X_1, \ldots, X_{n-1}, X_n]$ is also integral, so $x_1, \ldots, x_{n-1}, X_n$ are also algebraically independent (by Lemma 4.1). Since $X_n \in I_i \cap k[x_1, \ldots, x_{n-1}, X_n]$ any $f \in I_i \cap k[x_1, \ldots, x_{n-1}, X_n]$ can be written uniquely as

$$f = f_1 + f_2 X_n,$$

where $f_1 \in I_i \cap k[x_1, \ldots, x_{n-1}]$ and $f_2 \in k[x_1, \ldots, x_{n-1}, X_n]$. Since

$$I_i \cap k[x_1, \ldots, x_{n-1}] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_{n-1})$$

it follows that $I_i \cap k[x_1, \ldots, x_{n-1}, X_n] = (x_{d_i+1}, x_{d_i+2}, \ldots, x_{n-1}, X_n)$. Hence the theorem is proved. □

Corollary 4.2. *Let R be an affine algebra over a field k. There are elements $y_1, \ldots, y_d \in R$ that are algebraically independent over k and such that R is finitely generated as a $k[y_1, \ldots, y_d]$-module.*

Proof. There is a polynomial ring $k[X_1, \ldots, X_n]$ with an ideal I such that R is isomorphic to $k[X_1, \ldots, X_n]/I$. By the theorem there are elements $x_1, \ldots, x_n \in k[X_1, \ldots, X_n]$ that are algebraically independent over k, such that $k[X_1, \ldots, X_n]$ is finitely generated as $k[x_1, \ldots, x_n]$-module. Furthermore $I \cap k[x_1, \ldots, x_n] = (x_{d+1}, \ldots, x_n)$ for some d. Hence we have an inclusion

$$k[x_1, \ldots, x_n]/(x_{d+1}, \ldots, x_n) \subseteq k[X_1, \ldots, X_n]/I \simeq R,$$

and $k[X_1, \ldots, X_n]/I$ is integral over $k[x_1, \ldots, x_n]/(x_{d+1}, \ldots, x_n)$. Let y_i be the image of the class of x_i, for $1 \leq i \leq d$. So $k[y_1, \ldots, y_d]$ is isomorphic to $k[x_1, \ldots, x_n]/(x_{d+1}, \ldots, x_n) \simeq k[x_1, \ldots, x_d]$, and so $y_1, \ldots, y_d$ are algebraically independent over k and R is integral over $k[y_1, \ldots, y_d]$. $\square$

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA