# CHAPTER IX

# Algebraic Spaces

This chapter gives the basic results concerning solutions of polynomial equations in several variables over a field $k$. First it will be proved that if such equations have a common zero in some field, then they have a common zero in the algebraic closure of $k$, and such a zero can be obtained by the process known as specialization. However, it is useful to deal with transcendental extensions of $k$ as well. Indeed, if $\mathfrak{p}$ is a prime ideal in $k[X] = k[X_1, \ldots, X_n]$, then $k[X]/\mathfrak{p}$ is a finitely generated ring over $k$, and the images $x_i$ of $X_i$ in this ring may be transcendental over $k$, so we are led to consider such rings.

Even if we want to deal only with polynomial equations over a field, we are led in a natural way to deal with equations over the integers $\mathbf{Z}$. Indeed, if the equations are homogeneous in the variables, then we shall prove in §3 and §4 that there are universal polynomials in their coefficients which determine whether these equations have a common zero or not. "Universal" means that the coefficients are integers, and any given special case comes from specializing these universal polynomials to the special case.

Being led to consider polynomial equations over $\mathbf{Z}$, we then consider ideals $\mathfrak{a}$ in $\mathbf{Z}[X]$. The zeros of such an ideal form what is called an algebraic space. If $\mathfrak{p}$ is a prime ideal, the zeros of $\mathfrak{p}$ form what is called an arithmetic variety. We shall meet the first example in the discussion of elimination theory, for which I follow van der Waerden's treatment in the first two editions of his *Moderne Algebra*, Chapter XI.

However, when taking the polynomial ring $\mathbf{Z}[X]/\mathfrak{a}$ for some ideal $\mathfrak{a}$, it usually happens that such a factor ring has divisors of zero, or even nilpotent elements. Thus it is also natural to consider arbitrary commutative rings, and to lay the foundations of algebraic geometry over arbitrary commutative rings as did Grothendieck. We give some basic definitions for this purpose in §5. Whereas the present chapter gives the flavor of algebraic geometry dealing with specific polynomial ideals, the next chapter gives the flavor of geometry developing from commutative algebra, and its systematic application to the more general cases just mentioned.

The present chapter and the next will also serve the purpose of giving the reader an introduction to books on algebraic geometry, notably Hartshorne's systematic basic account. For instance, I have included those results which are needed for Hartshorne's Chapter I and II.

## §1. HILBERT'S NULLSTELLENSATZ

The Nullstellensatz has to do with a special case of the extension theorem for homomorphisms, applied to finitely generated rings over fields.

**Theorem 1.1.** *Let $k$ be a field, and let $k[x] = k[x_1, \ldots, x_n]$ be a finitely generated ring over $k$. Let $\varphi : k \to L$ be an embedding of $k$ into an algebraically closed field $L$. Then there exists an extension of $\varphi$ to a homomorphism of $k[x]$ into $L$.*

*Proof.* Let $\mathfrak{M}$ be a maximal ideal of $k[x]$. Let $\sigma$ be the canonical homomorphism $\sigma : k[x] \to k[x]/\mathfrak{M}$. Then $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ is a field, and is in fact an extension field of $\sigma k$. If we can prove our theorem when the finitely generated ring is in fact a field, then we apply $\varphi \circ \sigma^{-1}$ on $\sigma k$ and extend this to a homomorphism of $\sigma k[\sigma x_1, \ldots, \sigma x_n]$ into $L$ to get what we want.

Without loss of generality, we therefore assume that $k[x]$ is a field. If it is algebraic over $k$, we are done (by the known result for algebraic extensions). Otherwise, let $t_1, \ldots, t_r$ be a transcendence basis, $r \geqq 1$. Without loss of generality, we may assume that $\varphi$ is the identity on $k$. Each element $x_1, \ldots, x_n$ is algebraic over $k(t_1, \ldots, t_r)$. If we multiply the irreducible polynomial $\mathrm{Irr}(x_i, k(t), X)$ by a suitable non-zero element of $k[t]$, then we get a polynomial all of whose coefficients lie in $k[t]$. Let $a_1(t), \ldots, a_n(t)$ be the set of the leading coefficients of these polynomials, and let $a(t)$ be their product,

$$a(t) = a_1(t) \cdots a_n(t).$$

Since $a(t) \neq 0$, there exist elements $t_1', \ldots, t_r' \in k^a$ such that $a(t') \neq 0$, and hence $a_i(t') \neq 0$ for any $i$. Each $x_i$ is integral over the ring

$$k\left[t_1, \ldots, t_r, \frac{1}{a_1(t)}, \ldots, \frac{1}{a_r(t)}\right].$$

Consider the homomorphism

$$\varphi : k[t_1, \ldots, t_r] \to k^a$$

such that $\varphi$ is the identity on $k$, and $\varphi(t_j) = t_j'$. Let $\mathfrak{p}$ be its kernel. Then $a(t) \notin \mathfrak{p}$.

Our homomorphism $\varphi$ extends uniquely to the local ring $k[t]_{\mathfrak{p}}$ and by the preceding remarks, it extends to a homomorphism of

$$k[t]_{\mathfrak{p}}[x_1, \ldots, x_n]$$

into $k^a$, using Proposition 3.1 of Chapter VII. This proves what we wanted.

**Corollary 1.2.** *Let $k$ be a field and $k[x_1, \ldots, x_n]$ a finitely generated extension ring of $k$. If $k[x]$ is a field, then $k[x]$ is algebraic over $k$.*

*Proof.* All homomorphisms of a field are isomorphisms (onto the image), and there exists a homomorphism of $k[x]$ over $k$ into the algebraic closure of $k$.

**Corollary 1.3.** *Let $k[x_1, \ldots, x_n]$ be a finitely generated entire ring over a field $k$, and let $y_1, \ldots, y_m$ be non-zero elements of this ring. Then there exists a homomorphism*

$$\psi : k[x] \to k^a$$

*over $k$ such that $\psi(y_j) \neq 0$ for all $j = 1, \ldots, m$.*

*Proof.* Consider the ring $k[x_1, \ldots, x_n, y_1^{-1}, \ldots, y_m^{-1}]$ and apply the theorem to this ring.

Let $S$ be a set of polynomials in the polynomial ring $k[X_1, \ldots, X_n]$ in $n$ variables. Let $L$ be an extension field of $k$. By a **zero** of $S$ in $L$ one means an $n$-tuple of elements $(c_1, \ldots, c_n)$ in $L$ such that

$$f(c_1, \ldots, c_n) = 0$$

for all $f \in S$. If $S$ consists of one polynomial $f$, then we also say that $(c)$ is a zero of $f$. The set of all zeros of $S$ is called an **algebraic set** in $L$ (or more accurately in $L^{(n)}$). Let $\mathfrak{a}$ be the ideal generated by all elements of $S$. Since $S \subset \mathfrak{a}$ it is clear that every zero of $\mathfrak{a}$ is also a zero of $S$. However, the converse obviously holds, namely every zero of $S$ is also a zero of $\mathfrak{a}$ because every element of $\mathfrak{a}$ is of type

$$g_1(X)f_1(X) + \cdots + g_m(X)f_m(X)$$

with $f_j \in S$ and $g_i \in k[X]$. Thus when considering zeros of a set $S$, we may just consider zeros of an ideal. We note parenthetically that every ideal is finitely generated, and so every algebraic set is the set of zeros of a finite number of polynomials. As another corollary of Theorem 1.1, we get:

**Theorem 1.4.** *Let $\mathfrak{a}$ be an ideal in $k[X] = k[X_1, \ldots, X_n]$. Then either $\mathfrak{a} = k[X]$ or $\mathfrak{a}$ has a zero in $k^a$.*

*Proof.* Suppose $\mathfrak{a} \neq k[X]$. Then $\mathfrak{a}$ is contained in some maximal ideal $\mathfrak{m}$, and $k[X]/\mathfrak{m}$ is a field, which is a finitely generated extension of $k$, because it is generated by the images of $X_1, \ldots, X_n \bmod \mathfrak{m}$. By Corollary 2.2, this field is algebraic over $k$, and can therefore be embedded in the algebraic closure $k^a$. The homomorphism on $k[X]$ obtained by the composition of the canonical map mod $\mathfrak{m}$, followed by this embedded gives the desired zero of $\mathfrak{a}$, and concludes the proof of the theorem.

In §3 we shall consider conditions on a family of polynomials to have a common zero. Theorem 1.4 implies that if they have a common zero in some field, then they have a common zero in the algebraic closure of the field generated by their coefficients over the prime field.

**Theorem 1.5. (Hilbert's Nullstellensatz).** *Let $\mathfrak{a}$ be an ideal in $k[X]$. Let $f$ be a polynomial in $k[X]$ such that $f(c) = 0$ for every zero $(c) = (c_1, \ldots, c_n)$ of $\mathfrak{a}$ in $k^a$. Then there exists an integer $m > 0$ such that $f^m \in \mathfrak{a}$.*

*Proof.* We may assume that $f \neq 0$. We use the Rabinowitsch trick of introducing a new variable $Y$, and of considering the ideal $\mathfrak{a}'$ generated by $\mathfrak{a}$ and $1 - Yf$ in $k[X, Y]$. By Theorem 1.4, and the current assumption, the ideal $\mathfrak{a}'$ must be the whole polynomial ring $k[X, Y]$, so there exist polynomials $g_i \in k[X, Y]$ and $h_i \in \mathfrak{a}$ such that

$$1 = g_0(1 - Yf) + g_1h_1 + \cdots + g_rh_r.$$

We substitute $f^{-1}$ for $Y$ and multiply by an appropriate power $f^m$ of $f$ to clear denominators on the right-hand side. This concludes the proof.

For questions involving how effective the Nullstellensatz can be made, see the following references also related to the discussion of elimination theory discussed later in this chapter.

## Bibliography


[BeY 91] C. BERENSTEIN and A. YGER, Effective Bezout identities in $\mathbf{Q}[z_1, \ldots, z_n]$, *Acta Math.* **166** (1991), pp. 69–120

[Br 87] D. BROWNAWELL, Bounds for the degree in Nullstellensatz, *Ann. of Math.* **126** (1987), pp. 577–592

[Br 88] D. BROWNAWELL, Local diophantine nullstellen inequalities, *J. Amer. Math. Soc.* **1** (1988), pp. 311–322

[Br 89] D. BROWNAWELL, Applications of Cayley-Chow forms, *Springer Lecture Notes* **1380:** *Number Theory, Ulm 1987*, H. P. Schlickewei and E. Wirsing (eds.), pp. 1–18

[Ko 88] J. KOLLAR, Sharp effective nullstellensatz, *J. Amer. Math. Soc.* **1 No. 4** (1988), pp. 963–975

## §2. ALGEBRAIC SETS, SPACES AND VARIETIES

We shall make some very elementary remarks on algebraic sets. Let $k$ be a field, and let $A$ be an algebraic set of zeros in some fixed algebraically closed extension field of $k$. The set of all polynomials $f \in k[X_1, \ldots, X_n]$ such that $f(x) = 0$ for all $(x) \in A$ is obviously an ideal $\mathfrak{a}$ in $k[X]$, and is determined by $A$. We shall call it the ideal **belonging** to $A$, or say that it is **associated** with $A$. If $A$ is the set of zeros of a set $S$ of polynomials, then $S \subset \mathfrak{a}$, but $\mathfrak{a}$ may be bigger than $S$. On the other hand, we observe that $A$ is also the set of zeros of $\mathfrak{a}$.

Let $A$, $B$ be algebraic sets, and $\mathfrak{a}$, $\mathfrak{b}$ their associated ideals. Then it is clear that $A \subset B$ if and only if $\mathfrak{a} \supset \mathfrak{b}$. Hence $A = B$ if and only if $\mathfrak{a} = \mathfrak{b}$. This has an important consequence. Since the polynomial ring $k[X]$ is Noetherian, it follows that algebraic sets satisfy the dual property, namely every descending sequence of algebraic sets

$$A_1 \supset A_2 \supset \cdots$$

must be such that $A_m = A_{m+1} = \cdots$ for some integer $m$, i.e. all $A_v$ are equal for $v \geqq m$. Furthermore, dually to another property characterizing the Noetherian condition, we conclude that every non-empty set of algebraic sets contains a minimal element.

**Theorem 2.1.** *The finite union and the finite intersection of algebraic sets are algebraic sets. If $A$, $B$ are the algebraic sets of zeros of ideals $\mathfrak{a}$, $\mathfrak{b}$, respectively, then $A \cup B$ is the set of zeros of $\mathfrak{a} \cap \mathfrak{b}$ and $A \cap B$ is the set of zeros of $(\mathfrak{a}, \mathfrak{b})$.*

*Proof.* We first consider $A \cup B$. Let $(x) \in A \cup B$. Then $(x)$ is a zero of $\mathfrak{a} \cap \mathfrak{b}$. Conversely, let $(x)$ be a zero of $\mathfrak{a} \cap \mathfrak{b}$, and suppose $(x) \notin A$. There exists a polynomial $f \in \mathfrak{a}$ such that $f(x) \neq 0$. But $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$ and hence $(fg)(x) = 0$ for all $g \in \mathfrak{b}$, whence $g(x) = 0$ for all $g \in \mathfrak{b}$. Hence $(x)$ lies in $B$, and $A \cup B$ is an algebraic set of zeros of $\mathfrak{a} \cap \mathfrak{b}$.

To prove that $A \cap B$ is an algebraic set, let $(x) \in A \cap B$. Then $(x)$ is a zero of $(\mathfrak{a}, \mathfrak{b})$. Conversely, let $(x)$ be a zero of $(\mathfrak{a}, \mathfrak{b})$. Then obviously $(x) \in A \cap B$, as desired. This proves our theorem.

An algebraic set $V$ is called ***k*-irreducible** if it cannot be expressed as a union $V = A \cup B$ of algebraic sets $A$, $B$ with $A$, $B$ distinct from $V$. We also say irreducible instead of ***k*-irreducible**.

**Theorem 2.2.** *Let $A$ be an algebraic set.*

(i) *Then $A$ can be expressed as a finite union of irreducible algebraic sets $A = V_1 \cup \ldots \cup V_r$.*

(ii) *If there is no inclusion relation among the $V_i$, i.e. if $V_i \not\subset V_j$ for $i \neq j$, then the representation is unique.*

(iii) *Let $W, V_1, \ldots, V_r$ be irreducible algebraic sets such that*

$$W \subset V_1 \cup \ldots \cup V_r.$$

*Then $W \subset V_i$ for some $i$.*

*Proof.* We first show existence. Suppose the set of algebraic sets which cannot be represented as a finite union of irreducible ones is not empty. Let $V$ be a minimal element in its. Then $V$ cannot be irreducible, and we can write $V = A \cup B$ where $A, B$ are algebraic sets, but $A \neq V$ and $B \neq V$. Since each one of $A, B$ is strictly smaller than $V$, we can express $A, B$ as finite unions of irreducible algebraic sets, and thus get an expression for $V$, contradiction.

The uniqueness will follow from (iii), which we prove next. Let $W$ be contained in the union $V_1 \cup \ldots \cup V_r$. Then

$$W = (W \cap V_1) \cup \ldots \cup (W \cap V_r).$$

Since each $W \cap V_i$ is an algebraic set, by the irreducibility of $W$ we must have $W = W \cap V_i$ for some $i$. Hence $W \subset V_i$ for some $i$, thus proving (iii).

Now to prove (ii), apply (iii) to each $W_j$. Then for each $j$ there is some $i$ such that $W_j \subset V_i$. Similarly for each $i$ there exists $\nu$ such that $V_i \subset W_\nu$. Since there is no inclusion relation among the $W_j$'s, we must have $W_j = V_i = W_\nu$. This proves that each $W_j$ appears among the $V_i$'s and each $V_i$ appears among the $W_j$'s, and proves the uniqueness of the representation. It also concludes the proof of Theorem 2.2.

**Theorem 2.3** *An algebraic set is irreducible if and only if its associated ideal is prime.*

*Proof.* Let $V$ be irreducible and let $\mathfrak{p}$ be its associated ideal. If $\mathfrak{p}$ is not prime, we can find two polynomials $f, g \in k[X]$ such that $f \notin \mathfrak{p}$, $g \notin \mathfrak{p}$, but $fg \in \mathfrak{p}$. Let $\mathfrak{a} = (\mathfrak{p}, f)$ and $\mathfrak{b} = (\mathfrak{p}, g)$. Let $A$ be the algebraic set of zeros of $\mathfrak{a}$, and $B$ the algebraic set of zeros of $\mathfrak{b}$. Then $A \subset V$, $A \neq V$ and $B \subset V$, $B \neq V$. Furthermore $A \cup B = V$. Indeed, $A \cup B \subset V$ trivially. Conversely, let $(x) \in V$. Then $(fg)(x) = 0$ implies $f(x)$ or $g(x) = 0$. Hence $(x) \in A$ or $(x) \in B$, proving $V = A \cup B$, and $V$ is not irreducible. Conversely, let $V$ be the algebraic set of zeros of a prime ideal $\mathfrak{p}$. Suppose $V = A \cup B$ with $A \neq V$ and $B \neq V$. Let $\mathfrak{a}, \mathfrak{b}$ be the ideals associated with $A$ and $B$ respectively. There exist polynomials $f \in \mathfrak{a}, f \notin \mathfrak{p}$ and $g \in \mathfrak{b}, g \notin \mathfrak{p}$. But $fg$ vanishes on $A \cup B$ and hence lies in $\mathfrak{p}$, contradiction which proves the theorem.

**Warning.** Given a field $k$ and a prime ideal $\mathfrak{p}$ in $k[X]$, it may be that the ideal generated by $\mathfrak{p}$ in $k^a[X]$ is not prime, and the algebraic set defined over $k^a$ by $\mathfrak{p}k^a[X]$ has more than one component, and so is not irreducible. Hence the prefix referring to $k$ is really necessary.

It is also useful to extend the terminology of algebraic sets as follows. Given an ideal $\mathfrak{a} \subset k[X]$, to each field $K$ containing $k$ we can associate to $\mathfrak{a}$ the set

$\mathfrak{Z}_{\mathfrak{a}}(K)$ consisting of the zeros of $\mathfrak{a}$ in $K$. Thus $\mathfrak{Z}_{\mathfrak{a}}$ is an association

$$\mathfrak{Z}_{\mathfrak{a}} : K \mapsto \mathfrak{Z}_{\mathfrak{a}}(K) \subset K^{(n)}.$$

We shall speak of $\mathfrak{Z}_{\mathfrak{a}}$ itself as an **algebraic space**, so that $\mathfrak{Z}_{\mathfrak{a}}$ is not a set, but to each field $K$ associates the set $\mathfrak{Z}_{\mathfrak{a}}(K)$. Thus $\mathfrak{Z}_{\mathfrak{a}}$ is a functor from extensions $K$ of $k$ to sets (functorial with respect to field isomorphisms). By a $k$-**variety** we mean the algebraic space associated with a prime ideal $\mathfrak{p}$.

The notion of associated ideal applies also to such $\mathfrak{Z}_{\mathfrak{a}}$, and the associated ideal of $\mathfrak{Z}_{\mathfrak{a}}$ is also $\mathrm{rad}(\mathfrak{a})$. We shall omit the subscript $\mathfrak{a}$ and write simply $\mathfrak{Z}$ for this generalized notion of algebraic space. Of course we have

$$\mathfrak{Z}_{\mathfrak{a}} = \mathfrak{Z}_{\mathrm{rad}(\mathfrak{a})}.$$

We say that $\mathfrak{Z}_{\mathfrak{a}}(K)$ is the set of **points of** $\mathfrak{Z}_{\mathfrak{a}}$ **in** $K$. By the Hilbert Nullstellensatz, Theorem 1.1, it follows that if $K \subset K'$ are two algebraically closed fields containing $k$, then the ideals associated with $\mathfrak{Z}_{\mathfrak{a}}(K)$ and $\mathfrak{Z}_{\mathfrak{a}}(K')$ are equal to each other, and also equal to $\mathrm{rad}(\mathfrak{a})$. Thus the smallest algebraically closed field $k^{\mathrm{a}}$ containing $k$ already determines these ideals. However, it is also useful to consider larger fields which contain transcendental elements, as we shall see.

As another example, consider the polynomial ring $k[X_1, \ldots, X_n] = k[X]$. Let $\mathbf{A}^n$ denote the algebraic space associated with the zero ideal. Then $\mathbf{A}^n$ is called **affine** $n$-space. Let $K$ be a field containing $k$. For each $n$-tuple $(c_1, \ldots, c_n) \in K^{(n)}$ we get a homomorphism

$$\varphi : k[X_1, \ldots, X_n] \to K$$

such that $\varphi(X_i) = c_i$ for all $i$. Thus points in $\mathbf{A}^n(K)$ correspond bijectively to homomorphisms of $k(X)$ into $K$.

More generally, let $V$ be a $k$-variety with associated prime ideal $\mathfrak{p}$. Then $k[X]/\mathfrak{p}$ is entire. Denote by $\xi_i$ the image of $X_i$ under the canonical homomorphism $k[X] \to k[X]/\mathfrak{p}$. We call $(\xi)$ **the generic point** of $V$ over $k$. On the other hand, let $(x)$ be a point of $V$ in some field $K$. Then $\mathfrak{p}$ vanishes on $(x)$, so the homomorphism $\varphi : k[X] \to k[x]$ sending $X_i \mapsto x_i$ factors through $k[X]/\mathfrak{p} = k[\xi]$, whence we obtain a natural homomorphism $k[\xi] \to k[x]$. If this homomorphism is an isomorphism, then we call $(x)$ **a generic point** of $V$ in $K$.

Given two points $(x) \in \mathbf{A}^n(K)$ and $(x') \in \mathbf{A}^n(K')$, we say that $(x')$ is a **specialization** of $(x)$ (over $k$) if the map $x_i \mapsto x_i'$ is induced by a homomorphism $k[x] \to k[x']$. From the definition of a generic point of a variety, it is then immediate that:

*A variety $V$ is the set of specializations of its generic point, or of a generic point.*

In other words, $V(K)$ is the set of specializations of $(\xi)$ in $K$ for every field $K$ containing $k$.

Let us look at the converse construction of algebraic sets. Let $(x) = (x_1, \ldots, x_n)$ be an $n$-tuple with coordinates $x_i \in K$ for some extension field $K$ of $k$. Let $\mathfrak{p}$ be the ideal in $k[X]$ consisting of all polynomials $f(X)$ such that

$f(x) = 0$. We call $\mathfrak{p}$ the ideal **vanishing** on $(x)$. Then $\mathfrak{p}$ is prime, because if $fg \in \mathfrak{p}$ so $f(x)g(x) = 0$, then $f \in \mathfrak{p}$ or $g \in \mathfrak{p}$ since $K$ has no divisors of 0. Hence $\mathfrak{X}_\mathfrak{p}$ is a $k$-variety $V$, and $(x)$ is a generic point of $V$ over $k$ because $k[X]/\mathfrak{p} \approx k[x]$.

For future use, we state the next result for the polynomial ring over a factorial ring rather than over a field.

**Theorem 2.4.** *Let $R$ be a factorial ring, and let $W_1, \ldots, W_m$ be $m$ independent variables over its quotient field $k$. Let $k(w_1, \ldots, w_m)$ be an extension of transcendence degree $m - 1$. Then the ideal in $R[W]$ vanishing on $(w)$ is principal.*

*Proof.* By hypothesis there is some polynomial $P(W) \in R[W]$ of degree $\geqq 1$ vanishing on $(w)$, and after taking an irreducible factor we may assume that this polynomial is irreducible, and so is a prime element in the factorial ring $R[W]$. Let $G(W) \in R[W]$ vanish on $(w)$. To prove that $P$ divides $G$, after selecting some irreducible factor of $G$ vanishing on $(w)$ if necessary, we may assume without loss of generality that $G$ is a prime element in $R[W]$. One of the variables $W_i$ occurs in $P(W)$, say $W_m$, so that $w_m$ is algebraic over $k(w_1, \ldots, w_{m-1})$. Then $(w_1, \ldots, w_{m-1})$ are algebraically independent, and hence $W_m$ also occurs in $G$. Furthermore, $P(w_1, \ldots, w_{m-1}, W_m)$ is irreducible as a polynomial in $k(w_1, \ldots, w_{m-1})[W_m]$ by the Gauss lemma as in Chapter IV, Theorem 2.3. Hence there exists a polynomial $H(W_m) \in k(w_1, \ldots, w_{m-1})[W_m]$ such that

$$G(W) = H(W_m)P(W).$$

Let $R' = R[w_1, \ldots, w_{m-1}]$. Then $P$, $G$ have content 1 as polynomials in $R'[W_m]$. By Chapter IV Corollary 2.2 we conclude that $H \in R'[W_m] \approx R[W]$, which proves Theorem 2.4.

Next we consider homogeneous ideals and projective space. A polynomial $f(X) \in k[X]$ can be written as a linear combination

$$f(X) = \sum c_{(\nu)} M_{(\nu)}(X)$$

with monomials $M_{(\nu)}(X) = X_1^{\nu_1} \cdots X_n^{\nu_n}$ and $c_{(\nu)} \in k$. We denote the **degree** of $M_{(\nu)}$ by

$$|\nu| = \deg M_{(\nu)} = \sum \nu_i.$$

If in this expression for $f$ the degrees of the monomials $X^{(\nu)}$ are all the same (whenever the coefficient $c_{(\nu)}$ is $\neq 0$), then we say that $f$ is a **form**, or also that $f$ is a **homogeneous** (of that degree). An arbitrary polynomial $f(X)$ in $K[X]$ can also be written

$$f(X) = \sum f^{(d)}(X),$$

where each $f^{(d)}$ is a form of degree $d$ (which may be 0). We call $f^{(d)}$ the **homogeneous part** of $f$ of degree $d$.

An ideal $\mathfrak{a}$ of $k[X]$ is called **homogeneous** if whenever $f \in \mathfrak{a}$ then each homogeneous part $f^{(d)}$ also lies in $\mathfrak{a}$.

**Proposition 2.5.** *An ideal* $\mathfrak{a}$ *is homogeneous if and only if* $\mathfrak{a}$ *has a set of generators over* $k[X]$ *consisting of forms.*

*Proof.* Suppose $\mathfrak{a}$ is homogeneous and that $f_1, \ldots, f_r$ are generators. By hypothesis, for each integer $d \geqq 0$ the homogeneous components $f_i^{(d)}$ also lie in $\mathfrak{a}$, and the set of such $f_i^{(d)}$ (for all $i$, $d$) form a set of homogeneous generators. Conversely, let $f$ be a homogeneous element in $\mathfrak{a}$ and let $g \in K[X]$ be arbitrary. For each $d$, $g^{(d)}f$ lies in $\mathfrak{a}$, and $g^{(d)}f$ is homogeneous, so all the homogeneous components of $gf$ also lie in $\mathfrak{a}$. Applying this remark to the case when $f$ ranges over a set of homogeneous generators for $\mathfrak{a}$ shows that $\mathfrak{a}$ is homogeneous, and concludes the proof of the proposition.

An algebraic space $\mathfrak{X}$ is called **homogeneous** if for every point $(x) \in \mathfrak{X}$ and $t$ transcencental over $k(x)$, the point $(tx)$ also lies in $\mathfrak{X}$. If $t$, $u$ are transcendental over $k(x)$, then there is an isomorphism

$$k[x, t] \xrightarrow{\approx} k[x, u]$$

which sends $t$ on $u$ and restricts to the identity on $k[x]$, so to verify the above condition, it suffices to verify it for some transcendental $t$ over $k(x)$.

**Proposition 2.6.** *An algebraic space* $\mathfrak{X}$ *is homogeneous if and only if its associated ideal* $\mathfrak{a}$ *is homogeneous.*

*Proof.* Suppose $\mathfrak{X}$ is homogeneous. Let $f(X) \in k[X]$ vanish on $\mathfrak{X}$. For each $(x) \in \mathfrak{X}$ and $t$ transcendental over $k(x)$ we have

$$0 = f(x) = f(tx) = \sum_d t^d f^{(d)}(x).$$

Therefore $f^{(d)}(x) = 0$ for all $d$, whence $f^{(d)} \in \mathfrak{a}$ for all $d$. Hence $\mathfrak{a}$ is homogeneous. Conversely, suppose $\mathfrak{a}$ homogeneous. By the Hilbert Nullstellensatz, we know that $\mathfrak{X}$ consists of the zeros of $\mathfrak{a}$, and hence consists of the zeros of a set of homogeneous generators for $\mathfrak{a}$. But if $f$ is one of those homogeneous generators of degree $d$, and $(x)$ is a point of $\mathfrak{X}$, then for $t$ transcendental over $k(x)$ we have

$$0 = f(x) = t^d f(x) = f(tx),$$

so $(tx)$ is also a zero of $\mathfrak{a}$. Hence $\mathfrak{X}$ is homogeneous, thus proving the proposition.

**Proposition 2.7.** *Let* $\mathfrak{X}$ *be a homogeneous algebraic space. Then each irreducible component* $V$ *of* $\mathfrak{X}$ *is also homogeneous.*

*Proof.* Let $V = V_1, \ldots, V_r$ be the irreducible components of $\mathfrak{X}$, without inclusion relation. By Remark 3.3 we know that $V_1 \not\subset V_2 \cup \ldots \cup V_r$, so there is a point $(x) \in V_1$ such that $(x) \notin V_1$ for $i = 2, \ldots, r$. By hypothesis, for $t$ transcendental over $k(x)$ it follows that $(tx) \in \mathfrak{X}$ so $(tx) \in V_i$ for some $i$. Specializing to $t = 1$, we conclude that $(x) \in V_i$, so $i = 1$, which proves that $V_1$ is homogeneous, as was to be shown.

Let $V$ be a variety defined over $k$ by a prime ideal $\mathfrak{p}$ in $k[X]$. Let $(x)$ be a generic point of $V$ over $k$. We say that $(x)$ is **homogeneous** (**over** $k$) if for $t$

transcendental over $k(x)$, the point $(tx)$ is also a point of $V$, or in other words, $(tx)$ is a specialization of $(x)$. If this is the case, then we have an isomorphism

$$k[x_1, \ldots, x_n] \approx k[tx_1, \ldots, tx_n],$$

which is the identity on $k$ and sends $x_i$ on $tx_i$. It then follows from the preceding propositions that the following conditions are equivalent for a variety $V$ over $k$:

*$V$ is homogeneous.*
*The prime ideal of $V$ in $k[X]$ is homogeneous.*
*A generic point of $V$ over $k$ is homogeneous.*

A homogeneous ideal always has a zero, namely the origin (0), which will be called the **trivial zero**. We shall want to know when a homogeneous algebraic set has a non-trivial zero (in some algebraically closed field). For this we introduce the terminology of projective space as follows. Let $(x)$ be some point in $\mathbf{A}^n$ and $\lambda$ an element of some field containing $k(x)$. Then we denote by $(\lambda x)$ the point $(\lambda x_1, \ldots, \lambda x_n)$. Two points $(x), (y) \in \mathbf{A}^n(K)$ for some field $K$ are called equivalent if not all their coordinates are 0, and there exists some element $\lambda \in K$, $\lambda \neq 0$, such that $(\lambda x) = (y)$. The equivalence classes of such points in $\mathbf{A}^n(K)$ are called the points of **projective space** in $K$. We denote this projective space by $\mathbf{P}^{n-1}$, and the set of points of projective space in $K$ by $\mathbf{P}^{n-1}(K)$. We define an **algebraic space in projective space** to be the non-trivial zeros of a homogeneous ideal, with two zeros identified if they differ by a common non-zero factor.

## Algebraic spaces over rings

As we shall see in the next section, it is not sufficient to look only at ideals in $k[X]$ for some field $k$. Sometimes, even often, one wants to deal with polynomial equations over the integers $\mathbf{Z}$, for several reasons. In the example of the next sections, we shall find universal conditions over $\mathbf{Z}$ on the coefficients of a system of forms so that these forms have a non-trivial common zero. Furthermore, in number theory—diophantine questions—one wants to consider systems of equations with integer coefficients, and to determine solutions of these equations in the integers or in the rational numbers, or solutions obtained by reducing mod $p$ for a prime $p$. Thus one is led to extend the notions of algebraic space and variety as follows. Even though the applications of the next section will be over $\mathbf{Z}$, we shall now give general definitions over an arbitrary commutative ring $R$.

Let $f(X) \in R[X] = R[X_1, \ldots, X_n]$ be a polynomial with coefficients in $R$. Let $R \to A$ be an $R$-algebra, by which for the rest of this chapter we mean a homomorphism of commutative rings. We obtain a corresponding homomorphism

$$R[X] \to A[X]$$

on the polynomial rings, denoted by $f \mapsto f_A$ whereby the coefficients of $f_A$ are the images of the coefficients of $f$ under the homomorphism $R \to A$. By a **zero** of $f$ in $A$ we mean a zero of $f_A$ in $A$. Similarly, let $S$ be a set of polynomials in $R[X]$. By a **zero** of $S$ in $A$ we mean a common zero in $A$ of all polynomials $f \in S$. Let $\mathfrak{a}$ be the ideal generated by $S$ in $R[X]$. Then a zero of $S$ in $A$ is also

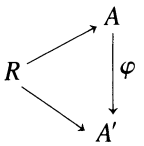
a zero of $\mathfrak{a}$ in $A$. We denote the set of zeros of $S$ in $A$ by $\mathfrak{Z}_S(A)$, so that we have

$$\mathfrak{Z}_S(A) = \mathfrak{Z}_{\mathfrak{a}}(A).$$

We call $\mathfrak{Z}_{\mathfrak{a}}(A)$ an **algebraic set** over $R$. Thus we have an association

$$\mathfrak{Z}_{\mathfrak{a}}: A \mapsto \mathfrak{Z}_{\mathfrak{a}}(A)$$

which to each $R$-algebra associates the set of zeros of $\mathfrak{a}$ in that algebra. We note that $R$-algebras form a category, whereby a morphism is a ring homomorphism $\varphi: A \to A'$ making the following diagram commutative:




Then it is immediately verified that $\mathfrak{Z}_{\mathfrak{a}}$ is a functor from the category of $R$-algebras to the category of sets. Again we call $\mathfrak{Z}_{\mathfrak{a}}$ an **algebraic space** over $R$.

If $R$ is Noetherian, then $R[X]$ is also Noetherian (Chapter IV, Theorem 4.1), and so if $\mathfrak{a}$ is an ideal, then there is always some finite set of polynomials $S$ generating the ideal, so $\mathfrak{Z}_S = \mathfrak{Z}_{\mathfrak{a}}$.

The notion of **radical** of $\mathfrak{a}$ is again defined as the set of polynomials $h \in R[X]$ such that $h^N \in \mathfrak{a}$ for some positive integer $N$. Then the following statement is immediate:

*Suppose that $R$ is entire. Then for every $R$-algebra $R \to K$ with a field $K$, we have*

$$\mathfrak{Z}_{\mathfrak{a}}(K) = \mathfrak{Z}_{\mathrm{rad}(\mathfrak{a})}(K).$$

We can define **affine space** $\mathbf{A}^n$ over $R$. Its points consist of all $n$-tuples $(x_1, \ldots, x_n) = (x)$ with $x_i$ in some $R$-algebra $A$. Thus $\mathbf{A}^n$ is again an association

$$A \mapsto \mathbf{A}^n(A)$$

from $R$-algebras to sets of points. Such points are in bijection with homormorphisms

$$R[X] \to A$$

from the polynomial ring over $R$ into $A$. In the next section we shall limit ourselves to the case when $A = K$ is a field, and we shall consider only the functor $K \mapsto \mathbf{A}^n(K)$ for fields $K$. Furthermore, we shall deal especially with the case when $R = \mathbf{Z}$, so $\mathbf{Z}$ has a unique homomorphism into a field $K$. Thus a field $K$ can always be viewed as a $\mathbf{Z}$-algebra.

Suppose finally that $R$ is entire (for simplicity). We can also consider projective space over $R$. Let $\mathfrak{a}$ be an ideal in $R[X]$. We define $\mathfrak{a}$ to be homogeneous just as before. Then a homogeneous ideal in $R[X]$ can be viewed as defining an algebraic subset in projective space $\mathbf{P}^n(K)$ for each field $K$ (as an $R$-algebra). If $R = \mathbf{Z}$,

then $\mathfrak{a}$ defines an algebraic subset in $\mathbf{P}^n(K)$ for every field $K$. Similarly, one can define the notion of a homogeneous algebraic space $\mathfrak{X}$ over $R$, and over the integers $\mathbf{Z}$ *a fortiori*. Propositions 2.6 and 2.7 and their proofs are also valid in this more general case, viewing $\mathfrak{X} = \mathfrak{X}_{\mathfrak{a}}$ as a functor from fields $K$ to sets $\mathbf{P}^n(K)$.

If $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$, then we call $\mathfrak{X}_{\mathfrak{p}}$ an $R$-**variety** $V$. If $R$ is Noetherian, so $R[X]$ is Noetherian, it follows as before that an algebraic space $\mathfrak{X}$ over $R$ is a finite union of $R$-varieties without inclusion relations. We shall carry this out in §5, in the very general context of commutative rings. Just as we did over a field, we may form the factor ring $\mathbf{Z}[X]/\mathfrak{p}$ and the image $(x)$ of $(X)$ in this factor ring is called a **generic point** of $V$.

## §3. PROJECTIONS AND ELIMINATION

Let $(W) = (W_1, \ldots, W_m)$ and $(X) = (X_1, \ldots, X_n)$ be two sets of independent variables. Then ideals in $k[W, X]$ define algebraic spaces in the product space $\mathbf{A}^{m+n}$. Let $\mathfrak{a}$ be an ideal in $k[W, X]$. Let $\mathfrak{a}_1 = \mathfrak{a} \cap k[W]$. Let $\mathfrak{X}$ be the algebraic space of zeros of $\mathfrak{a}$ and let $\mathfrak{X}_1$ be the algebraic space of zeros of $\mathfrak{a}_1$. We have the projection

$$\mathrm{pr}: \mathfrak{X}^{m+n} \to \mathfrak{X}^m \quad \text{or} \quad \mathrm{pr}: \mathbf{A}^{m+n} \to \mathbf{A}^m$$

which maps a point $(w, x)$ to its first set of coordinates $(w)$. It is clear that $\mathrm{pr}\,\mathfrak{X} \subset \mathfrak{X}_1$. In general it is not true that $\mathrm{pr}\,\mathfrak{X} = \mathfrak{X}_1$. For example, the ideal $\mathfrak{p}$ generated by the single polynomial $W_1^2 - W_2X_1 = 0$ is prime. Its intersection with $k[W_1, W_2]$ is the zero ideal. But it is not true that every point in the affine $(W_1, W_2)$-space is the projection of a point in the variety $\mathfrak{X}_{\mathfrak{p}}$. For instance, the point $(1, 0)$ is not the projection of any zero of $\mathfrak{p}$. One says in such a case that the projection is **incomplete**. We shall now consider a situation when such a phenomenon does not occur.

In the first place, let $\mathfrak{p}$ be a prime ideal in $k[W, X]$ and let $V$ be its variety of zeros. Let $(w, x)$ be a generic point of $V$. Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$. Then $(w)$ is a generic point of the variety $V_1$ which is the algebraic space zeros of $\mathfrak{p}_1$. This is immediate from the canonical injective homomorphism

$$k[W]/\mathfrak{p}_1 \to k[W, X]/\mathfrak{p}.$$

Thus the generic point $(w)$ of $V_1$ is the projection of the generic point $(w, x)$ of $V$. The question is whether a special point $(w')$ of $V_1$ is the projection of a point of $V$.

In the subsequent applications, we shall consider ideals which are homogeneous only in the $X$-variables, and similarly algebraic subsets which are homogeneous in the second set of variables in $\mathbf{A}^n$.

An ideal $\mathfrak{a}$ in $k[W, X]$ which is homogeneous in $(X)$ defines an algebraic space in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. If $V$ is an irreducible component of the algebraic set defined by $\mathfrak{a}$, then we may view $V$ as a subvariety of $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Let $\mathfrak{p}$ be the prime ideal associated with $V$. Then $\mathfrak{p}$ is homogeneous in $(X)$. Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$. We shall see that the situation of an incomplete projection mentioned previously is eliminated when we deal with projective space.

We can also consider the product $\mathbf{A}^m \times \mathbf{P}^n$, defined by the zero ideal over $\mathbf{Z}$. For each field $K$, the set of points of $\mathbf{A}^m \times \mathbf{P}^n$ in $K$ is $\mathbf{A}^m(K) \times \mathbf{P}^n(K)$. An ideal $\mathfrak{a}$ in $\mathbf{Z}[W, X]$, homogeneous in $(X)$, defines an algebraic space $\mathfrak{Z} = \mathfrak{Z}_\mathfrak{a}$ in $\mathbf{A}^m \times \mathbf{P}^n$. We may form its projection $\mathfrak{Z}_1$ on the first factor. This applies in particular when $\mathfrak{a}$ is a prime ideal $\mathfrak{p}$, in which case we call $\mathfrak{Z}_\mathfrak{a}$ an **arithmetic subvariety** of $\mathbf{A}^m \times \mathbf{P}^n$. Its projection $V_1$ is an arithmetic subvariety of $\mathbf{A}^m$, associated with the prime ideal $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbf{Z}[W]$.

**Theorem 3.1.** *Let $(W) = (W_1, \ldots, W_m)$ and $(X) = (X_1, \ldots, X_n)$ be independent families of variables. Let $\mathfrak{p}$ be a prime ideal in $k[W, X]$* (resp. $\mathbf{Z}[W, X]$) *and assume $\mathfrak{p}$ is homogeneous in $(X)$. Let $V$ be the corresponding irreducible algebraic space in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Let $\mathfrak{p}_1 = \mathfrak{p} \cap k[W]$* (resp. $\mathfrak{p} \cap \mathbf{Z}[W]$), *and let $V_1$ be the projection of $V$ on the first factor. Then $V_1$ is the algebraic space of zeros of $\mathfrak{p}_1$ in $\mathbf{A}^m$.*

*Proof.* Let $V$ have generic point $(w, x)$. We have to prove that every zero $(w')$ of $\mathfrak{p}_1$ in a field is the projection of some zero $(w', x')$ of $\mathfrak{p}$ such that not all the coordinates of $(x')$ are equal to 0. By assumption, not all the coordinates of $(x)$ are equal to 0, since we viewed $V$ as a subset of $\mathbf{A}^m \times \mathbf{P}^{n-1}$. For definiteness, say we are dealing with the case of a field $k$. By Chapter VII, Proposition 3.3, the homomorphism $k[w] \to k[w']$ can be extended to a place $\varphi$ of $k(w, x)$. By Proposition 3.4 of Chapter VII, there is some coordinate $x_j$ such that $\varphi(x_i/x_j) \neq \infty$ for all $i = 1, \ldots, n$. We let $x_i' = \varphi(x_i/x_j)$ for all $i$ to conclude the proof. The proof is similar when dealing with algebraic spaces over $\mathbf{Z}$, replacing $k$ by $\mathbf{Z}$.

**Remarks.** Given the point $(w') \in \mathbf{A}^m$, the point $(w', x')$ in $\mathbf{A}^m \times \mathbf{P}^{n-1}$ may of course not lie in $k(w')$. The coordinates $(x')$ could even be transcendental over $k(x')$. By any one of the forms of the Hilbert Nullstellensatz, say Corollary 1.3 of Theorem 1.1, we do know that $(x')$ could be found algebraic over $k(w')$, however. In light of the various versions of the Nullstellensatz, if a set of forms has a non-trivial common zero in some field, then it has a non-trivial common zero in the algebraic closure of the field generated by the coefficients of the forms over the prime field. In a theorem such as Theorem 1.2 below, the conditions on the coefficients for the forms to have a non-trivial common zero (or a zero in projective space) are therefore also conditions for the forms to have such a zero in that algebraic closure.

We shall apply Theorem 3.1 to show that given a finite family of homogeneous polynomials, the property that they have a non-trivial common zero in some

algebraically closed field can be expressed in terms of a finite number of universal polynomial equations in their coefficients. We make this more precise as follows.

Consider a finite set of forms $(f) = (f_1, \ldots, f_r)$. Let $d_1, \ldots, d_r$ be their degrees. *We assume* $d_i \geqq 1$ *for* $i = 1, \ldots, r$. Each $f_i$ can be written

$$f_i = \sum w_{i,(\nu)} M_{(\nu)}(X) \tag{1}$$

where $M_{(\nu)}(X)$ is a monomial in $(X)$ of degree $d_i$, and $w_{i,(\nu)}$ is a coefficient. We shall say that $(f)$ has a **non-trivial zero** $(x)$ if $(x) \neq (0)$ and $f_i(x) = 0$ for all $i$. We let $(w) = (w)_f$ be the point obtained by arranging the coefficients $w_{i,(\nu)}$ of the forms in some definite order, and we consider this point as a point in some affine space $\mathbf{A}^m$, where $m$ is the number of such coefficients. This integer $m$ is determined by the given degrees $d_1, \ldots, d_r$. In other words, given such degrees, the set of all forms $(f) = (f_1, \ldots, f_r)$ with these degrees is in bijection with the points of $\mathbf{A}^m$.

**Theorem 3.2. (Fundamental theorem of elimination theory.)** *Given degrees* $d_1, \ldots, d_r$, *the set of all forms* $(f_1, \ldots, f_r)$ *in n variables having a non-trivial common zero is an algebraic subspace of* $\mathbf{A}^m$ *over* $\mathbf{Z}$.

*Proof.* Let $(W) = (W_{i,(\nu)})$ be a family of variables independent of $(X)$. Let $(F) = (F_1, \ldots, F_r)$ be the family of polynomials in $\mathbf{Z}[W, X]$ given by

$$F_i(W, X) = \sum W_{i,(\nu)} M_{(\nu)}(X) \tag{2}$$

where $M_{(\nu)}(X)$ ranges over all monomials in $(X)$ of degree $d_i$, so $(W) = (W)_F$. We call $F_1, \ldots, F_r$ **generic forms**. Let

$$\mathfrak{a} = \text{ideal in } \mathbf{Z}[W, X] \text{ generated by } F_1, \ldots, F_r.$$

Then $\mathfrak{a}$ is homogeneous in $(X)$. Thus we are in the situation of Theorem 3.1, with $\mathfrak{a}$ defining an algebraic space $\mathfrak{A}$ in $\mathbf{A}^m \times \mathbf{P}^{n-1}$. Note that $(w)$ is a specialization of $(W)$, or, as we also say, $(f)$ is a specialization of $(F)$. As in Theorem 3.1, let $\mathfrak{A}_1$ be the projection of $\mathfrak{A}$ on the first factor. Then directly from the definitions, $(f)$ has a non-trivial zero if and only if $(w)_f$ lies in $\mathfrak{A}_1$, so Theorem 3.2 is a special case of Theorem 3.1.

**Corollary 3.3.** *Let* $(f)$ *be a family of n forms in n variables, and assume that* $(w)_f$ *is a generic point of* $\mathbf{A}^m$, *i.e. that the coefficients of these forms are algebraically independent. Then* $(f)$ *does not have a non-trivial zero.*

*Proof.* There exists a specialization of $(f)$ which has only the trivial zero, namely $f_1' = X_1^{d_1}, \ldots, f_n' = X_n^{d_n}$.

Next we follow van der Waerden in showing that $\mathfrak{A}$ and hence $\mathfrak{A}_1$ are irreducible.

**Theorem 3.4.** *The algebraic space* $\mathfrak{A}_1$ *of forms having a non-trivial common zero in Theorem 3.2 is actually a* $\mathbf{Z}$*-variety, i.e. it is irreducible. The prime ideal*

$\mathfrak{p}$ *in* $\mathbf{Z}[W, X]$ *associated with* $\mathfrak{A}$ *consists of all polynomials* $G(W, X) \in \mathbf{Z}[W, X]$ *such that for some index* $j$ *there is an integer* $s \geqq 0$ *satisfying*

$(*)_j$ $\quad X_j^s G(W, X) \equiv 0 \bmod (F_1, \ldots, F_r)$; *that is,* $X_j^s G(W, X) \in \mathfrak{a}$.

*If relation* (*) *holds for one index* $j$, *then it holds for every* $j = 1, \ldots, n$. (*Of course, the integer* $s$ *depends on* $j$.)

*Proof.* We construct a generic point of $\mathfrak{A}$. We select any one of the variables, say $X_q$, and rewrite the forms $F_i$ as follows:

$$F_i(W, X) = F_i^* + Z_i X_q^{d_i}$$

where $F_i^*$ is the sum of all monomials except the monomial containing $X_q^{d_i}$. The coefficients $(W)$ are thereby split into two families, which we denote by $(Y)$ and $(Z)$, where $(Z) = (Z_1, \ldots, Z_r)$ are the coefficients of $(X_q^{d_1}, \ldots, X_q^{d_r})$ in $(F_1, \ldots, F_r)$, and $(Y)$ is the remaining family of coefficients of $F_1^*, \ldots, F_r^*$. We have $(W) = (Y, Z)$, and we may write the polynomials $F_i$ in the form

$$F_i(W, X) = F_i(Y, Z, X) = F_i^*(Y, X) + Z_i X_q^{d_i}.$$

Corresponding to the variables $(Y, X)$ we choose quantities $(y, x)$ algebraically independent over $\mathbf{Z}$. We let

$$z_i = -F_i^*(y, x)/x_q^{d_i} = -F_i^*(y, x/x_q). \tag{3}$$

We shall prove that $(y, z, x)$ is a generic point of $\mathfrak{A}$.

From our construction, it is immediately clear that $F_i(y, z, x) = 0$ for all $i$, and consequently if $G(W, X) \in \mathbf{Z}[W, X]$ satisfies (*), then $G(y, z, x) = 0$.

Conversely, let $G(Y, Z, X) \in \mathbf{Z}[Y, Z, X] = \mathbf{Z}[W, X]$ satisfy $G(y, z, x) = 0$. From Taylor's formula in several variables we obtain

$$\begin{aligned} G(Y, Z, X) &= G(Y, \ldots, -F_i^*/X_q^{d_i} + Z_i + F_i^*/X_q^{d_i}, \ldots, X) \\ &= G(Y, -F_i^*/X_q^{d_i}, X) + \sum (Z_i + F_i^*/X_q^{d_i})^{\mu_i} H_{\mu_i}(Y, Z, X), \end{aligned}$$

where the sum is taken over terms having one factor $(Z_i + F_i^*/X_q^{d_i})$ to some power $\mu_i > 0$, and some factor $H_{\mu_i}$ in $\mathbf{Z}[Y, Z, X]$. From the way $(y, z, x)$ was constructed, and the fact that $G(y, z, x) = 0$, we see that the first term vanishes, and hence

$$G(Y, Z, X) = \sum (Z_i + F_i^*/X_q^{d_i})^{\mu_i} H_{\mu_i}(Y, Z, X).$$

Clearing denominators of $X_q$, for some integer $s$ we get

$$X_q^s G(Y, Z, X) \equiv 0 \bmod (F_i, \ldots, F_r),$$

or in other words, $(*)_q$ is satisfied. This concludes the proof of the theorem.

**Remark.** Of course the same statement and proof as in Theorem 3.4 holds with $\mathbf{Z}$ replaced by a field $k$. In that case, we denote by $\mathfrak{a}_k$ the ideal in $k[W, X]$ generated by the generic forms, and similarly by $\mathfrak{p}_k$ the associated prime

ideal. Then

$$\mathfrak{a}_{k,1} = \mathfrak{a}_k \cap k[W] \quad \text{and} \quad \mathfrak{p}_{k,1} = \mathfrak{p}_k \cap k[W].$$

The ideal $\mathfrak{p}$ in Theorem 3.4 will be called the **prime associated with the ideal of generic forms**. The intersection $\mathfrak{p}_1 = \mathfrak{p} \cap \mathbf{Z}[W]$ will be called the prime **elimination ideal** of these forms. If $\mathfrak{A}$ denotes as before the zeros of $\mathfrak{p}$ (or of $\mathfrak{a}$), and $\mathfrak{A}_1$ is its projection on the first factor, then $\mathfrak{p}_1$ is the prime associated with $\mathfrak{A}_1$. The same terminology will be used if instead of $\mathbf{Z}$ we work over a field $k$. (*Note*: homogeneous elements of $\mathfrak{p}_1$ have been called **inertia forms** in the classical literature, following Hurwitz. I am avoiding this terminology because the word "inertia" is now used in a standard way for inertia groups as in Chapter VII, §2.) The variety of zeros of $\mathfrak{p}_1$ will be called the **resultant variety**. It is determined by the given degrees $d_1, \ldots, d_n$, so we could denote it by $\mathfrak{A}_1(d_1, \ldots, d_n)$.

**Exercise.** Show that if $\mathfrak{p}$ is the prime associated with the ideal of generic forms, then $\mathfrak{p} \cap \mathbf{Z} = (0)$ is the zero ideal.

**Theorem 3.5.** *Assume $r = n$, so we deal with $n$ forms in $n$ variables. Then $\mathfrak{p}_1$ is principal, generated by a single polynomial, so $\mathfrak{A}_1$ is what one calls a hypersurface. If $(w)$ is a generic point of $\mathfrak{A}_1$ over a field $k$, then the transcendence degree of $k(w)$ over $k$ is $m - 1$.*

*Proof.* We prove the second statement first, and use the same notation as in the proof of Theorem 3.4. Let $u_j = x_j/x_n$. Then $u_n = 1$ and $(y)$, $(u_1, \ldots, u_{n-1})$ are algebraically independent. By (3), we have $z_i = -F_i^*(y, u)$, so

$$k(w) = k(y, z) \subset k(y, u),$$

and so the transcendence degree of $k(w)$ over $k$ is $\leqq m - 1$. We claim that this transcendence degree is $m - 1$. It will suffice to prove that $u_1, \ldots, u_{n-1}$ are algebraic over $k(w) = k(y, z)$. Suppose this is not the case. Then there exists a place $\varphi$ of $k(w, u)$, which is the identity on $k(w)$ and maps some $u_j$ on $\infty$. Select an index $q$ such that $\varphi(u_i/u_q)$ is finite for all $i = 1, \ldots, n - 1$. Let $v_i = u_i/u_q$ and $v_i' = \varphi(u_i/u_q)$. Denote by $Y_{iq}$ the coefficient of $X_q^{d_i}$ in $F_i$ and let $Y^*$ denote the variables $(Y)$ from which $Y_{1q}, \ldots, Y_{nq}$ are deleted. By (3) we have for $i = 1, \ldots, n$:

$$\begin{aligned} 0 &= y_{iq} u_q^{d_i} + z_i + F_i^{**}(y^*, u) \\ &= y_{iq} + z_i/u_q^{d_i} + F_i^{**}(y^*, u/u_q). \end{aligned}$$

Applying the place yields

$$0 = y_{iq} + F_i^{**}(y^*, v').$$

In particular, $y_{iq} \in k(y^*, v')$ for each $i = 1, \ldots, n$. But the transcendence degree of $k(v')$ over $k$ is at most $n - 1$, while the elements $(y_{1q}, \ldots, y_{nq}, y^*)$ are algebraically independent over $k$, which gives a contradiction proving the theorem.

**Remark.** There is a result (I learned it from [Jo 80]) which is more precise than Theorem 3.5. Indeed, let $\mathfrak{A}$ as in Theorem 3.5 be the variety of zeros of $\mathfrak{p}$, and $\mathfrak{A}_1$ its projection. Then this projection is birational in the following sense. Using the notation of the proof of Theorem 3.5, the result is not only that $k(w)$ has transcendence degree $m - 1$ over $k$, but actually we have

$$\mathbf{Q}(y, z) = \mathbf{Q}(w) = \mathbf{Q}(y, u).$$

*Proof.* Let $\mathfrak{p}_1 = (R)$, so $R$ is the resultant, generating the principal ideal $\mathfrak{p}_1$. We shall need the following lemma.

**Lemma 3.6.** *There is a positive integer $s$ with the following properties. Fix an index $i$ with $1 \leqq i \leqq n - 1$. For each pair of $n$-tuples of integers $\geqq 0$*

$$(\alpha) = (\alpha_1, \ldots, \alpha_n) \quad \textit{and} \quad (\beta) = (\beta_1, \ldots, \beta_n)$$

*with $|\alpha| = |\beta| = d_i$, we have*

$$X_n^s\left(M_{(\alpha)}(X)\frac{\partial R}{\partial W_{i,(\beta)}} - M_{(\beta)}(X)\frac{\partial R}{\partial W_{i,(\alpha)}}\right) \equiv 0 \bmod (F_1, \ldots, F_n).$$

To see this, we use the fact from Theorem 3.4 that for some $s$,

$$X_n^s R(W) = Q_1F_1 + \cdots + Q_nF_n \text{ with } Q_j \in \mathbf{Z}[W, X].$$

Differentiating with respect to $W_{i,(\beta)}$ we get

$$X_n^s \frac{\partial R}{\partial W_{i,(\beta)}} \equiv Q_i M_{(\beta)}(X) \bmod (F_1, \ldots, F_n),$$

and similarly

$$X_n^s \frac{\partial R}{\partial W_{i,(\alpha)}} \equiv Q_i M_{(\alpha)}(X) \bmod (F_1, \ldots, F_n).$$

We multiply the first congruence by $M_{(\alpha)}(X)$ and the second by $M_{(\beta)}(X)$, and we subtract to get our lemma.

From the above we conclude that

$$M_{(\alpha)}(X)\frac{\partial R}{\partial W_{i,(\beta)}} - M_{(\beta)}(X)\frac{\partial R}{\partial W_{i,(\alpha)}}$$

vanishes on $\mathfrak{A}$, i.e. on the point $(w, u)$, after we put $X_n = 1$. Then we select

$$M_{(\alpha)}(X) = X_i^{d_i} \quad \text{and} \quad M_{(\beta)}(X) = X_i^{d_i - 1}X_n \text{ for } i = 1, \ldots, n - 1,$$

and we see that we have the rational expression

$$u_i = \frac{\partial R/\partial W_{i,(\beta)}}{\partial R/\partial W_{i,(\alpha)}}\bigg|_{(W)=(w)}, \text{ for } i = 1, \ldots, n - 1,$$

thus showing that $\mathbf{Q}(u) \subset \mathbf{Q}(w)$, as asserted.

We note that the argument also works over the prime field of characteristic $p$. The only additional remark to be made is that there is some partial derivative $\partial R/\partial W_{i,(\alpha)}$ which does not vanish on $(w)$. This is a minor technical matter, which we leave to the reader.

The above argument is taken from [Jo 80], Proposition 3.3.1. Jouanolou links old-time results as in Macaulay [Ma 16] with more recent techniques of commutative algebra, including the Koszul complex (which will be discussed in Chapter XXI). See also his monographs [Jo 90], [Jo 91].

Still following van der Waerden, we shall now give a fairly explicit determination of the polynomial generating the ideal in Theorem 3.5. We deal with the generic forms $F_i(W, X)$ $(i = 1, \ldots, n)$. According to Theorem 3.5, the ideal $\mathfrak{p}_1$ is generated by a single element. Because the units in $\mathbf{Z}[W]$ consist only of $\pm 1$, it follows that this element is well defined up to a sign. Let

$$R(W) = R(F_1, \ldots, F_n)$$

be one choice of this element. Later we shall see how to pick in a canonical way one of these two possible choices. We shall prove various properties of this element, which will be called the **resultant** of $F_1, \ldots, F_n$.

For each $i = 1, \ldots, n$ we let $D_i$ be the product of the degrees with $d_i$ omitted; that is,

$$D_i = d_1 \cdots \overset{\wedge}{d_i} \cdots d_n.$$

We let $d$ be the positive integer such that $d - 1 = \sum (d_i - 1)$.

**Lemma 3.7.** *Given one of the indices, say n, there is an element $R_n(W)$ lying in $\mathfrak{p}_1$, satisfying the following properties.*

(a) *For each i, $R_n(W)X_i^d \equiv 0 \bmod (F_1, \ldots, F_n)$ in $\mathbf{Z}[W, X]$.*
(b) *For each i, $R_n(W)$ is homogeneous in the set of variables $(W_{i,(\nu)})$, and is of degree $D_n$ in $(W_{n,(\nu)})$,* i.e. *in the coefficient of $F_n$.*
(c) *As a polynomial in $\mathbf{Z}[W]$, $R_n(W)$ has content* 1, i.e. *is primitive.*

*Proof.* The polynomial $R_n(W)$ will actually be explicitly constructed. Let $M_\sigma(X)$ denote the monomials of degree $|\sigma| = d$. We partition the indexing set $S = \{\sigma\}$ into disjoint subsets as follows.

Let $S_1 = \{\sigma_1\}$ be the set of indices such that $M_{\sigma_1}(X)$ is divisible by $X_1^{d_1}$.

Let $S_2 = \{\sigma_2\}$ be the set of indices such that $M_{\sigma_2}(X)$ is divisible by $X_2^{d_2}$ but not by $X_1^{d_1}$.

...

Let $S_n = \{\sigma_n\}$ be the set of indices such that $M_{\sigma_n}(X)$ is divisible by $X_n^{d_n}$ but not by $X_1^{d_1}, \ldots, X_{n-1}^{d_{n-1}}$.

Then $S$ is the disjoint union of $S_1, \ldots, S_n$. Write each monomial as follows:

$$\begin{aligned} M_{\sigma_1}(X) &= H_{\sigma_1}(X)X_1^{d_1} \quad \text{so} \quad \deg H_{\sigma_1} = d - d_1 \\ &\vdots \qquad\quad \vdots \\ M_{\sigma_1}(X) &= H_{\sigma_n}(X)X_n^{d_n} \quad \text{so} \quad \deg H_{\sigma_n} = d - d_n. \end{aligned}$$

Then the number of polynomials

$$H_{\sigma_1}F_1, \ldots, H_{\sigma_n}F_n \text{ (with } \sigma_1 \in S_1, \ldots, \sigma_n \in S_n)$$

is precisely equal to the number of monomials of degree $d$. We let $R_n$ be the determinant of the coefficients of these polynomials, viewed as forms in $(X)$ with coefficients in $\mathbf{Z}[W]$. Then $R_n = R_n(W) \in \mathbf{Z}[W]$. We claim that $R_n(W)$ satisfies the properties of the lemma.

First we note that if $\sigma_n \in S_n$, then $H_{\sigma_n}(X)$ is divisible by a power of $X_i$ at most $d_i - 1$, for $i = 1, \ldots, n-1$. On the other hand, the degree of $H_{\sigma_n}(X)$ in $X_n$ is determined by the condition that the total degree is $d - d_n$. Hence $S_n$ has exactly $D_n$ elements. It follows at once that $R_n(W)$ is homogeneous of degree $D_n$ in the coefficients of $F_n$, i.e. in $(W_{n,(\nu)})$. From the construction it also follows that $R_n$ is homogeneous in each set of variables $(W_{i,(\nu)})$ for each $i = 1, \ldots, n-1$.

If we specialize the forms $F_i$ $(i = 1, \ldots, n)$ to $X_i^{d_i}$, then $R_n$ specializes to 1, and hence $R_n \neq 0$ and $R_n$ is primitive. For each $\sigma_i$ we can write

$$H_{\sigma_i}F_i = \sum_{\sigma \in S} C_{\sigma,\sigma_i}(W)M_\sigma(X),$$

where $M_\sigma(X)$ $(\sigma \in S)$ ranges over all monomials of degree $d$ in $(X)$, and $C_{\sigma,\sigma_i}(W)$ is one of the variables $(W)$. Then by definition

$$R_n(W) = \det(C_{\sigma,\sigma_1}(W)_{(\sigma_1 \in S_1)}, \ldots, C_{\sigma,\sigma_n}(W)_{(\sigma_n \in S_n)}) = \det(C).$$

where $\sigma_1 \in S_1, \ldots, \sigma_n \in S_n$ indexes the columns, and $\sigma$ indexes the rows. Let $B = \tilde{C}$ be the matrix with components in $\mathbf{Z}[W, X]$ such that

$$BC = \det(C)I = R_n I.$$

(See Chapter XIII, Corollary 4.17.) Then for each $\sigma$, we have

$$R_n(W)M_\sigma(X) = \sum_i \sum_{\sigma_i \in S_i} B_{i,\sigma_i}F_i.$$

Given $i$, we take for $\sigma$ the index such that $M_\sigma(X) = X_i^d$ in order to obtain the first relation in Lemma 3.7. By Theorem 3.4, we conclude that $R_n(W) \in \mathfrak{p}_1$. This concludes the proof of the lemma.

Of course, we picked an index $n$ to fix ideas. For each $i$ one has a polynomial $R_i$ satisfying the analogous properties, and in particular homogeneous of degree $D_i$ in the variables $(W_{i,(\nu)})$ which are the coefficients of the form $F_i$.

**Theorem 3.8.** *Let $R$ be the resultant of the $n$ generic forms $F_i$ over $\mathbf{Z}$, in $n$ variables. Then $R$ satisfies the following properties.*

(a) *$R$ is the greatest common divisor in $\mathbf{Z}[W]$ of the polynomials $R_1, \ldots, R_n$.*
(b) *$R$ is homogeneous of degree $D_i$ in the coefficients of $F_i$.*
(c) *Let $F_i = \ldots + W_{i,(d_i)}X_i^{d_i}$, so $W_{i,(d_i)}$ is the coefficient of $X_i^{d_i}$. Then $R$ contains the monomial*

$$\pm \prod_{i=1}^{n} W_{i,(d_i)}^{D_i}.$$

*Proof.* The idea will be to specialize the forms $F_1, \ldots, F_n$ to products of generic linear forms, where we can tell what is going on. For that we need a lemma of a more general property eventually to be proved. We shall use the following notation. If $f_1, \ldots, f_n$ are forms with coefficients $(w)$, then we write

$$R(f_1, \ldots, f_n) = R(w).$$

**Lemma 3.9.** *Let $G$, $H$ be generic independent forms with $\deg(GH) = d_1$. Then $R(GH, F_2, \ldots, F_n)$ is divisible by $R(G, F_2, \ldots, F_n)R(H, F_2, \ldots, F_n)$.*

*Proof.* By Theorem 3.5, there is an expression

$$X_n^s R(F_1, \ldots, F_n) = Q_1F_1 + \cdots + Q_nF_n \text{ with } Q_i \in \mathbf{Z}[W, X].$$

Let $W_G, W_H, W_{F_2}, \ldots, W_{F_n}$ be the coefficients of $G, H, F_2, \ldots, F_n$ respectively, and let $(w)$ be the coefficients of $GH, F_2, \ldots, F_n$. Then

$$R(w) = R(GH, F_2, \ldots, F_n),$$

and we obtain

$$X_n^s R(w) = Q_1(w, X)GH + Q_2(w, X)F_2 + Q_n(w, X)F_n.$$

Hence $R(GH, F_2, \ldots, F_n)$ belongs to the elimination ideal of $G, F_2, \ldots, F_n$ in the ring $\mathbf{Z}[W_G, W_H, W_{F_2}, \ldots, W_{F_n}]$, and similarly with $H$ instead of $G$. Since $W_H$ is a family of independent variables over $\mathbf{Z}[W_G, W_{F_2}, \ldots, W_{F_n}]$, it follows that $R(G, F_2, \ldots, F_n)$ divides $R(GH, F_2, \ldots, F_n)$ in that ring, and similarly for $R(H, F_2, \ldots, F_n)$. But $(W_G)$ and $(W_H)$ are independent sets of variables, and so $R(G, F_2, \ldots, F_n)$, $R(H, F_2, \ldots, F_n)$ are distinct prime elements in that ring, so their product divides $R(GH, F_2, \ldots, F_n)$ as stated, thus proving the lemma.

Lemma 3.9 applies to any specialized family of polynomials $g, h, f_1, \ldots, f_n$ with coefficients in a field $k$. Observe that for a system of $n$ linear forms in $n$ variables, the resultant is simply the determinant of the coefficients. Thus if $L_1, \ldots, L_n$ are generically independent linear forms in the variables $X_1, \ldots, X_n$, then their resultant $R(L_1, \ldots, L_n)$ is homogeneous of degree 1 in the coefficients of $L_i$ for each $i$. We apply Lemma 3.9 to the case of forms $f_1, \ldots, f_{n-1}$, which are products of generically independent linear forms. By Lemma 3.9 we conclude that for this specialized family of form, their resultant has degree at least $D_n$ in

the coefficients of $F_n$, so for the generic forms $F_1, \ldots, F_n$ their resultant has degree at least $D_n$ in the coefficients of $F_n$. Similarly $R(F_1, \ldots, F_n)$ has degree at least $D_i$ in the coefficients of $F_i$ for each $i$. But $R$ divides the $n$ elements $R_1(W), \ldots, R_n(W)$ constructed in Lemma 3.7. Therefore we conclude that $R$ has degree exactly $D_i$ in the coefficients of $F_i$. By Theorem 3.5, we know that $R$ divides each $R_i$. Let $G$ be the greatest common divisor of $R_1, \ldots, R_n$ in $\mathbf{Z}[W]$. Then $R$ divides $G$ and has the same degree in each set of variables $(W_{i,(\nu)})$ for $i = 1, \ldots, n$. Hence there exists $c \in \mathbf{Z}$ such that $G = cR$. We must have $c = \pm 1$, because, say, $R_n$ is primitive in $\mathbf{Z}[W]$. This proves (a) and (b) of the theorem.

As to the third part, we specialize the forms to $f_i = X_i^{d_i}$, $i = 1, \ldots, n$. Then $R_n$ specializes to 1, and since $R$ divides $R_n$ it follows that $R$ itself specializes to $\pm 1$. Since all coefficients of the forms specialize to 0 except those which we denoted by $W_{i,(d_i)}$, it follows that $R(W)$ contains the monomial which is the product of these variables to the power $D_i$, up to the sign $\pm 1$. This proves (c), and concludes the proof of Theorem 3.8.

We can now normalize the resultant by choosing the sign such that $R$ contains the monomial

$$M = \prod_{i=1}^{n} W_{i,(d_i)}^{D_i},$$

with coefficient $+1$. This condition determines $R$ uniquely, and we then denote $R$ also by

$$R = \operatorname{Res}(F_1, \ldots, F_n).$$

Given forms $f_1, \ldots, f_n$ with coefficients $(w)$ in a field $K$ (actually any commutative ring), we can then define their **resultant**

$$\operatorname{Res}(f_1, \ldots, f_n) = R(w)$$

with the normalized polynomial $R$. With this normalization, we then have a stronger result than Lemma 3.9.

**Theorem 3.10.** *Let $f_1 = gh$ be a product of forms such that* $\deg(gh) = d_1$. *Let $f_2, \ldots, f_n$ be arbitrary forms of degrees $d_2, \ldots, d_n$. Then*

$$\operatorname{Res}(gh, f_2, \ldots, f_n) = \operatorname{Res}(g, f_2, \ldots, f_n)\operatorname{Res}(h, f_2, \ldots, f_n).$$

*Proof.* From the fact that the degrees have to add in a product of polynomials, together with Theorem 3.8(a) and (b), we now see in Lemma 3.9 that we must have the precise equality in what was only a divisibility before we knew the precise degree of $R$ in each set of variables.

Theorem 3.10 is very useful in proving further properties of the determinant, because it allows a reduction to simple cases under factorization of polynomials.

For instance one has:

**Theorem 3.11.** *Let $F_1, \ldots, F_n$ be the generic forms in n variables, and let $\overline{F}_1, \ldots, \overline{F}_n$ be the forms obtained by substituting $X_n = 0$, so that $\overline{F}_1, \ldots, \overline{F}_{n-1}$ are the generic forms in $n-1$ variables. Let $n \geqq 2$. Then*

$$\mathrm{Res}(F_1, \ldots, F_{n-1}, X_n^{d_n}) = \mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})^{d_n}.$$

*Proof.* By Theorem 3.10 it suffices to prove the assertion when $d_n = 1$. By Theorem 3.4, for each $i = 1, \ldots, n-1$ we have an expression

$$(*) \qquad X_i^s \mathrm{Res}(F_1, \ldots, F_{n-1}, X_n) = Q_1 F_1 + \cdots + Q_{n-1} F_{n-1} + Q_n X_n$$

with $Q_j \in \mathbf{Z}[W, X]$ (depending on the choice of $i$). The left-hand side can be written as a polynomial in the coefficients of $F_1, \ldots, F_{n-1}$ with the notation

$$X_i^s R(W_{F_1}, \ldots, W_{F_{n-1}}, 1_{X_n}) = X_i^s P(W_{F_1}, \ldots, W_{F_{n-1}}) = X_i^s P(W^{(n-1)}), \text{ say;}$$

thus in the generic linear form in $X_1, \ldots, X_n$ we have specialized all the coefficients to 0 except the coefficient of $X_n$, which we have specialized to 1. Substitute $X_n = 0$ in the right side of (*). By Theorem 3.4, we conclude that $P(W^{(n-1)})$ lies in the resultant ideal of $\overline{F}_1, \ldots, \overline{F}_{n-1}$, and therefore $\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})$ divides $P(W^{(n-1)})$. By Theorem 3.8 we know that $P(W^{(n-1)})$ has the same homogeneity degree in $W_{\overline{F}_i}$ $(i = 1, \ldots, n-1)$ as $\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1})$. Hence there is $c \in \mathbf{Z}$ such that

$$c\mathrm{Res}(\overline{F}_1, \ldots, \overline{F}_{n-1}) = \mathrm{Res}(F_1, \ldots, F_{n-1}, X_n).$$

One finds $c = 1$ by specializing $\overline{F}_1, \ldots, \overline{F}_{n-1}$ to $X_1^{d_1}, \ldots, X_{n-1}^{d_{n-1}}$ respectively, thus concluding the proof.

The next basic lemma is stated for the generic case, for instance in Macaulay [Ma 16], and is taken up again in [Jo 90], Lemma 5.6.

**Lemma 3.12.** *Let $A$ be a commutative ring. Let $f_1, \ldots, f_n$, $g_1, \ldots, g_n$ be homogeneous polynomials in $A[X_1, \ldots, X_n]$. Assume that*

$$(g_1, \ldots, g_n) \subset (f_1, \ldots, f_n)$$

*as ideals in $A[X]$. Then*

$$\mathrm{Res}(f_1, \ldots, f_n) \text{ divides } \mathrm{Res}(g_1, \ldots, g_n) \text{ in } A.$$

*Proof.* Express each $g_i = \sum h_{ij} f_j$ with $h_{ij}$ homogeneous in $A[X]$. By specialization, we may then assume that $g_i = \sum H_{ij} F_j$ where $H_{ij}$ and $F_j$ have algebraically independent coefficients over $\mathbf{Z}$. By Theorem 3.4, for each $i$ we have a relation

$$X_i^s \mathrm{Res}(g_1, \ldots, g_n) = Q_1 g_1 + \cdots + Q_n g_n \text{ with some } Q_i \in \mathbf{Z}[W_H, W_F],$$

where $W_H$, $W_F$ denote the independent variable coefficients of the polynomials $H_{ij}$ and $F_j$ respectively. In particular,

$$(*) \qquad X_i^s \operatorname{Res}(g_1, \ldots, g_n) \equiv 0 \bmod (F_1, \ldots, F_n)\mathbf{Z}[W_H, W_F, X].$$

Note that $\operatorname{Res}(g_1, \ldots, g_n) = P(W_H, W_F) \in \mathbf{Z}[W_H, W_F]$ is a polynomial with integer coefficients. If $(w_F)$ is a generic point of the resultant variety $\mathfrak{A}_1$ over $\mathbf{Z}$, then $P(W_H, w_F) = 0$ by (*). Hence $\operatorname{Res}(F_1, \ldots, F_n)$ divides $P(W_H, W_F)$, thus proving the lemma.

**Theorem 3.13.** *Let $A$ be a commutative ring and let $d_1, \ldots, d_n$ be integers $\geqq 1$ as usual. Let $f_i$ be homogeneous of degree $d_i$ in $A[X] = A[X_1, \ldots, X_n]$. Let $d$ be an integer $\geqq 1$, and let $g_i, \ldots, g_n$ be homogeneous of degree $d$ in $A[X]$. Then*

$$f_i \circ g = f_i(g_1, \ldots, g_n)$$

*is homogeneous of degree $dd_i$, and*

$$\operatorname{Res}(f_1 \circ g, \ldots, f_n \circ g) = \operatorname{Res}(g_1, \ldots, g_n)^{d_1 \cdots d_n} \operatorname{Res}(f_1, \ldots, f_n)^{d^{n-1}} \text{ in } A.$$

*Proof.* We start with the standard relation of Theorem 3.4:

$$(*) \qquad X_i^s \operatorname{Res}(F_1, \ldots, F_n) \equiv 0 \bmod (F_1, \ldots, F_n)\mathbf{Z}[W_F, X].$$

We let $G_1, \ldots, G_n$ be independent generic polynomials of degree $d$, and let $W_G$ denote their independent variable coefficients. Substituting $G_i$ for $X_i$ in (*), we find

$$G_i^s \operatorname{Res}(F_1, \ldots, F_n) \equiv 0 \bmod (F_1 \circ G, \ldots, F_n \circ G)\mathbf{Z}[W_F, W_G, X].$$

Abbreviate $\operatorname{Res}(F_1, \ldots, F_n)$ by $R(F)$, and let $g_i = G_i^s R(F)$. By Lemma 3.12, it follows that

$$\operatorname{Res}(f_1 \circ G, \ldots, F_n \circ G) \text{ divides } \operatorname{Res}(G_1^s R(F), \ldots, G_n^s R(F)) \text{ in } \mathbf{Z}[W_F, W_G].$$

By Theorem 3.10 and the homogeneity of Theorem 3.8(b) we find that

$$\operatorname{Res}(G_1^s R(F), \ldots, G_n^s R(F)) = \operatorname{Res}(G_1, \ldots, G_n)^M \operatorname{Res}(F_1, \ldots, F_n)^N$$

with integers $M, N \geqq 0$. Since $\operatorname{Res}(G_1, \ldots, G_n)$ and $\operatorname{Res}(F_1, \ldots, F_n)$ are distinct prime elements in $\mathbf{Z}[W_G, W_F]$ (distinct because they involve independent variables), it follows that

$$(**) \qquad \operatorname{Res}(F_1 \circ G, \ldots, F_n \circ G) = \varepsilon \operatorname{Res}(G_1, \ldots, G_n)^a \operatorname{Res}(F_1, \ldots, F_n)^b$$

with integers $a, b \geqq 0$ and $\varepsilon = 1$ or $-1$. Finally, we specialize $F_i$ to $W_i X_i^{d_i}$ and we specialize $G_i$ to $U_i X_i^d$, with independent variables $(W_1, \ldots, W_n, U_1, \ldots, U_n)$.

Substituting in (**), we obtain

$$\operatorname{Res}(W_1U_1^{d_1}X_1^{dd_1}, \ldots, W_nU_n^{d_n}X_n^{dd_n}) = \varepsilon \operatorname{Res}(U_1X_1^d, \ldots, U_nX_n^d)^a \operatorname{Res}(W_1X_1^{d_1}, \ldots, W_nX_n^{d_n})^b.$$

By the homogeneity of Theorem 3.8(b) we get

$$\prod_i (W_iU^{d_i})^{d_1 \ldots \hat{d}_i \ldots d_n d^{n-1}} = \varepsilon \prod_i U_i^{d^{n-1}a} \prod_i W_i^{d_1 \ldots \hat{d}_i \ldots d_n b}.$$

From this we get at once $\varepsilon = 1$ and $a$, $b$ are what they are stated to be in the theorem.

**Corollary 3.14.** *Let $C = (c_{ij})$ be a square matrix with coefficients in $A$. Let $f_i(X) = F_i(CX)$ (where $CX$ is multiplication of matrices, viewing $X$ as a column vector). Then*

$$\operatorname{Res}(f_1, \ldots, f_n) = \det(C)^{d_1 \ldots d_n} \operatorname{Res}(F_1, \ldots, F_n).$$

*Proof.* This is the case when $d = 1$ and $g_i$ is a linear form for each $i$.

**Theorem 3.15.** *Let $f_1, \ldots, f_n$ be homogeneous in $A[X]$, and suppose $d_n \geqq d_i$ for all $i$. Let $h_i$ be homogeneous of degree $d_n - d_i$ in $A[X]$. Then*

$$\operatorname{Res}(f_1, \ldots, f_{n-1}, f_n + \sum_{j=1}^{n-1} h_j f_j) = \operatorname{Res}(f_1, \ldots, f_n) \text{ in } A.$$

*Proof.* We may assume $f_i = F_i$ are the generic forms, $H_i$ are forms generic independent from $F_1, \ldots, F_n$, and $A = \mathbf{Z}[W_F, W_H]$, where $(W_F)$ and $(W_H)$ are the coefficients of the respective polynomials. We note that the ideals $(F_1, \ldots, F_n)$ and $(F_1, \ldots, F_n + \sum_{j \neq n} H_jF_j)$ are equal. From Lemma 3.12 we conclude that the two resultants in the statement of the theorem differ by a factor of 1 or $-1$. We may now specialize $H_{ij}$ to 0 to determine that the factor is $+1$, thus concluding the proof.

**Theorem 3.16.** *Let $\pi$ be a permutation of $\{1, \ldots, n\}$, and let $\varepsilon(\pi)$ be its sign. Then*

$$\operatorname{Res}(F_{\pi(1)}, \ldots, F_{\pi(n)}) = \varepsilon(\pi)^{d_1 \ldots d_n} \operatorname{Res}(F_1, \ldots, F_n).$$

*Proof.* Again using Lemma 3.12 with the ideals $(F_1, \ldots, F_n)$ and $(F_{\pi(1)}, \ldots, F_{\pi(n)})$, which are equal, we conclude the desired equality up to a factor $\pm 1$, in $\mathbf{Z}[W_F]$. We determine this sign by specializing $F_i$ to $X_i^{d_i}$, and using the multiplicativity of Theorem 3.10. We are then reduced to the case when $F_i = X_i$, so a linear form; and we can apply Corollary 3.14 to conclude the proof.

The next theorem was an exercise in van der Waerden's *Moderne Algebra*.

**Theorem 3.17.** *Let $L_1, \ldots, L_{n-1}$, $F$ be generic forms in $n$ variables, such that $L_1, \ldots, L_{n-1}$ are of degree 1, and $F$ has degree $d = d_n$. Let*

$$\Delta_j (j = 1, \ldots, n)$$

*be $(-1)^{n-j}$ times the $j$-th minor determinant of the coefficient matrix of the forms $(L_1, \ldots, L_{n-1})$. Then*

$$\operatorname{Res}(L_1, \ldots, L_{n-1}, F) = F(\Delta_1, \ldots, \Delta_n).$$

*Proof.* We first claim that for all $j = 1, \ldots, n$ we have the congruence

$$(*) \qquad X_n \Delta_j - X_j \Delta_n \equiv 0 \bmod (L_1, \ldots, L_{n-1})\mathbf{Z}[W, X],$$

where as usual, $(W)$ are the coefficients of the forms $L_1, \ldots, L_{n-1}, F$. To see this, we consider the system of linear equations

$$\begin{aligned} W_{11}X_1 + \cdots + W_{1,n-1}X_{n-1} &= L_1(W, X) - W_{1,n}X_n \\ &\cdots\cdots \\ W_{n-1,1}X_1 + \cdots + W_{n-1,n-1}X_{n-1} &= L_{n-1}(W, X) - W_{n-1,n}X_n . \end{aligned}$$

If $C = (C^1, \ldots, C^{n-1})$ is a square matrix with columns $C^j$, then a solution of a system of linear equations $CX = C^n$ satisfies Cramer's rule

$$X_j \det(C^1, \ldots, C^{n-1}) = \det(C^1, \ldots, C^n, \ldots, C^{n-1}).$$

Using the fact that the determinant is linear in each column, (*) falls out.

Then from the congruence (*) it follows that

$$X_n^d F(\Delta_1, \ldots, \Delta_n) \equiv \Delta_n^d F(X_1, \ldots, X_n) \bmod (L_1, \ldots, L_{n-1})\mathbf{Z}[W, X],$$

whence

$$X_n^d F(\Delta_1, \ldots, \Delta_n) \equiv 0 \bmod (L_1, \ldots, L_{n-1}, F).$$

Hence by Theorem 3.4 and the fact that $\operatorname{Res}(L_1, \ldots, L_{n-1}, F) = R(W)$ generates the elimination ideal, it follows that there exists $c \in \mathbf{Z}[W]$ such that

$$F(\Delta_1, \ldots, \Delta_n) = c\operatorname{Res}(L_1, \ldots, L_{n-1}, F).$$

Since the left side is homogeneous of degree 1 in the coefficients $W_F$ and homogeneous of degree $d$ in the coefficients $W_{L_i}$ for each $i = 1, \ldots, n-1$, it follows from Theorem 3.8 that $c \in \mathbf{Z}$. Specializing $L_i$ to $X_i$ and $F$ to $X_n^d$ makes $\Delta_j$ specialize to 0 if $j \neq n$ and $\Delta_n$ specializes to 1. Hence the left side specializes to 1, and so does the right side, whence $c = 1$. This concludes the proof.

### Bibliography

[Jo 80] J. P. JOUANOLOU, Idéaux résultants, *Advances in Mathematics* **37** No. 3 (1980), pp. 212–238

[Jo 90] J. P. JOUANOLOU, Le formalisme du résultant, *Advances in Mathematics* **90** No. 2 (1991) pp. 117–263

[Jo 91] J. P. JOUANOLOU, *Aspects invariants de l'élimination*, Départment de Mathématiques, Université Louis Pasteur, Strasbourg, France (1991)

[Ma 16] F. MACAULAY, *The algebraic theory of modular systems*, Cambridge University Press, 1916

## §4. RESULTANT SYSTEMS

The projection argument used to prove Theorem 3.4 has the advantage of constructing a generic point in a very explicit way. On the other hand, no explicit, or even effective, formula was given to construct a system of forms defining $\mathfrak{A}_1$. We shall now reformulate a version of Theorem 3.4 over $\mathbf{Z}$ and we shall prove it using a completely different technique which constructs effectively a system of generators for an ideal of definition of the arithmetic variety $\mathfrak{A}_1$ in Theorem 3.2.

**Theorem 4.1.** *Given degrees $d_1, \ldots, d_r \geqq 1$, and positive integers $m$, $n$. Let $(W) = (W_{i,(\nu)})$ be the variables as in* §3, (2) *viewed as algebraically independent elements over the integers $\mathbf{Z}$. There exists an effectively determinable finite number of polynomials $R_\rho(W) \in \mathbf{Z}[W]$ having the following property. Let $(f)$ be as in* (1), *a system of forms of the given degrees with coefficients $(w)$ in some field $k$. Then $(f)$ has a non-trivial common zero if and only if $R_\rho(w) = 0$ for all $\rho$.*

A finite family $\{R_\rho\}$ having the property stated in Theorem 4.1 will be called a **resultant system** for the given degrees. According to van der Waerden (*Moderne Algebra*, first and second edition, §80), the following technique of proof using resultants goes back to Kronecker elimination, and to a paper of Kapferer (Über Resultanten und Resultantensysteme, *Sitzungsber. Bayer. Akad. München* 1929, pp. 179–200). The family of polynomials $\{R_\rho(W)\}$ is called a **resultant system**, because of the way they are constructed. They form a set of generators for an ideal $\mathfrak{b}_1$ such that the arithmetic variety $\mathfrak{A}_1$ is the set of zeros of $\mathfrak{b}_1$. I don't know how close the system constructed below is to being a set of generators for the prime ideal $\mathfrak{p}_1$ in $\mathbf{Z}[W]$ associated with $\mathfrak{A}_1$. Actually we shall not need the whole theory of Chapter IV, §10; we need only one of the characterizing properties of resultants.

Let $p$, $q$ be positive integers. Let

$$f_v = v_0X_1^p + v_1X_1^{p-1}X_2 + \cdots + v_pX_2^p$$
$$g_w = w_0X_1^q + w_1X_1^{q-1}X_2 + \cdots + w_qX_2^q$$

be two generic homogeneous polynomials in $\mathbf{Z}[v, w, X_1, X_2] = \mathbf{Z}[v, \mathrm{w}][X]$. In Chapter IV, §10 we defined their resultant $\mathrm{Res}(f_v, g_w)$ in case $X_2 = 1$, but we find it now more appropriate to work with homogeneous polynomials. For our purposes here, we need only the fact that the resultant $R(v, w)$ is characterized by the following property. If we have a specialization $(a, b)$ of $(v, w)$ in a field $K$, and if $f_a, f_b$ have a factorization

$$f_a = a_0 \prod_{i=1}^{p} (X_1 - \alpha_i X_2)$$

$$g_b = b_0 \prod_{j=1}^{q} (X_1 - \beta_j X_2)$$

then we have the symmetric expressions in terms of the roots:

$$R(a, b) = \mathrm{Res}(f_a, f_b) = a_0^q b_0^p \prod_{i,j} (\alpha_i - \beta_j)$$
$$= a_0^q \prod_i g_b(\alpha_i, 1) = (-1)^{pq} b_0^p \prod_j f_a(\beta_j, 1).$$

From the general theory of symmetric polynomials, it is *a priori* clear that $R(v, w)$ lies in $\mathbf{Z}[v, w]$, and Chapter IV, §10 gives an explicit representation

$$\varphi_{v,w} f_v + \psi_{v,w} g_w = X_2^{p+q-1} R(v, w)$$

where $\varphi_{v,w}$ and $\psi_{v,w} \in \mathbf{Z}[v, w, X]$. This representation will not be needed. The next property will provide the basic inductive step for elimination.

**Proposition 4.2.** *Let $f_a$, $g_b$ be homogeneous polynomials with coefficients in a field $K$. Then $R(a, b) = 0$ if and only if the system of equations*

$$f_a(X) = 0, \quad g_b(X) = 0$$

*has a non-trivial zero in some extension of $K$ (which can be taken to be finite).*

If $a_0 = 0$ then a zero of $g_b$ is also a zero of $f_a$; and if $b_0 = 0$ then a zero of $f_a$ is also a zero of $g_b$. If $a_0 b_0 \neq 0$ then from the expression of the resultant as a product of the difference of roots $(\alpha_i - \beta_j)$ the proposition follows at once.

We shall now prove Theorem 4.1 by using resultants. We do this by induction on $n$.

If $n = 1$, the theorem is obvious.

If $n = 2$, $r = 1$, the theorem is again obvious, taking the empty set for $(R_\rho)$.

If $n = 2$, $r = 2$, then the theorem amounts to Proposition 4.2.

Assume now $n = 2$ and $r > 2$, so we have a system of homogeneous equations

$$0 = f_1(X) = f_2(X) = \ldots = f_r(X)$$

with $(X) = (X_1, X_2)$. Let $d_i$ be the degree of $f_i$ and let $d = \max d_i$. We replace the family $\{f_j(X)\}$ by the family of all polynomials

$$f_i(X)X_1^{d-d_i} \quad \text{and} \quad f_i(X)X_2^{d-d_i}, \; i = 1, \ldots, r.$$

These two families have the same sets of non-trivial zeros, so to prove Theorem 4.1 we may assume without loss of generality that all the polynomials $f_1, \ldots, f_r$ have the same degree $d$.

With $n = 2$, consider the generic system of forms of degree $d$ in $(X)$:

(4) $\quad F_i(W, X) = 0$ with $i = 1, \ldots, r$, in two variables $(X) = (X_1, X_2)$,

where the coefficients of $F_i$ are $W_{i,0}, \ldots, W_{i,d}$ so that

$$(W) = (W_{1,0}, \ldots, W_{1,d}, \ldots, W_{r,0}, \ldots, W_{r,d}).$$

The next proposition is a special case of Theorem 4.1, but gives the first step of an induction showing how to get the analogue of Proposition 4.2 for such a larger system. Let $T_1, \ldots, T_r$ and $U_1, \ldots, U_r$ be independent variables over $\mathbf{Z}[W, X]$. Let $F_1, \ldots, F_r$ be the generic forms of §3, (2). Let

$$f = F_1(W, X)T_1 + \cdots + F_r(W, X)T_r$$
$$g = F_1(W, X)U_1 + \cdots + F_r(W, X)U_r$$

so $f, g \in \mathbf{Z}[W, T, U][X]$. Then $f, g$ are polynomials in $(X)$ with coefficients in $\mathbf{Z}[W, T, U]$. We may form their resultant

$$\mathrm{Res}(f, g) \in \mathbf{Z}[W, T, U].$$

Thus $\mathrm{Res}(f, g)$ is a polynomial in the variables $(T, U)$ with coefficients in $\mathbf{Z}[W]$. We let $(Q_\mu(W))$ be the family of coefficients of this polynomial.

**Proposition 4.3.** *The system $\{Q_\mu(W)\}$ just constructed satisfies the property of Theorem 4.1,* i.e. *it is a resultant system for r forms of the same degree d.*

*Proof.* Suppose that there is a non-trivial solution of a special system $F_j(W, X) = 0$ with $(w)$ in some field $k$. Then $(w, T, U)$ is a common non-trivial zero of $f, g$, so $\mathrm{Res}(f, g) = 0$ and therefore $Q_\mu(w) = 0$ for all $\mu$. Conversely, suppose that $Q_\mu(w) = 0$ for all $\mu$. Let $f_i(X) = F_i(w, X)$. We want to show that $f_i(X)$ for $i = 1, \ldots, r$ have a common non-trivial zero in some extension of

$k$. If all $f_i$ are 0 in $k[X_1, X_2]$ then they have a common non-trivial zero. If, say, $f_1 \neq 0$ in $k[X]$, then specializing $T_2, \ldots, T_r$ to 0 and $T_1$ to 1 in the resultant $\mathrm{Res}(f, g)$, we see that

$$\mathrm{Res}(f_1, f_2U_2 + \cdots + f_rU_r) = 0$$

as a polynomial in $k[U_2, \ldots, U_r]$. After making a finite extension of $k$ if necessary, we may assume that $f_1(X)$ splits into linear factors. Let $\{\alpha_i\}$ be the roots of $f_1(X_1, 1)$. Then some $(\alpha_i, 1)$ must also be a zero of $f_2U_2 + \cdots + f_rU_r$, which implies that $(\alpha_i, 1)$ is a common zero of $f_1, \ldots, f_r$ since $U_2, \ldots, U_r$ are algebraically independent over $k$. This proves Proposition 4.3.

We are now ready to do the inductive step with $n > 2$. Again, let

$$f_i(X) = F_i(w, X) \text{ for } j = 1, \ldots, r$$

be polynomials with coefficients $(w)$ in some fields $k$.

**Remark 4.4.** *There exists a non-trivial zero of the system*

$$f_i = 0 \ (i = 1, \ldots, r)$$

*in some extension of $k$ if and only if there exist*

$$(x_1, \ldots, x_{n-1}) \neq (0, \ldots, 0) \text{ and } (x_n, t) \neq (0, 0)$$

*in some extension of $k$ such that*

$$f_i(tx_1, \ldots, tx_{n-1}, x_n) = 0 \text{ for } i = 1, \ldots, r.$$

So we may now construct the system $(R_\rho)$ inductively as follows.

Let $T$ be a new variable, and let $X^{(n-1)} = (X_1, \ldots, X_{n-1})$. Let

$$g_i(W, X^{(n-1)}, S_n, T) = F_i(W, TX_1, \ldots, TX_{n-1}, X_n) \in \mathbf{Z}[W, X^{(n-1)}][X_n, T].$$

Then $g_i$ is homogeneous in the two variables $(X_n, T)$. By the theorem for two variables, there is a system of polynomials $(Q_\mu)$ in $\mathbf{Z}[W, X^{(n-1)}]$ having the property: *if $(w, x^{(n-1)})$ is a point in a field $K$, then*

$$g_i(w, x^{(n-1)}, X_n, T) \text{ *have a non-trivial common zero for* } i = 1, \ldots, r.$$
$$\Leftrightarrow Q_\mu(w, x^{(n-1)}) = 0 \text{ *for all* } \mu.$$

Viewing each $Q_\mu$ as a polynomial in the variables $(X^{(n-1)})$, we decompose each $Q_\mu$ as a sum of its homogeneous terms, and we let $(H_\lambda(W, X^{(n-1)}))$ be the family of these polynomials, homogeneous in $(X^{(n-1)})$. From the homogeneity property of the forms $F_j$ in $(X)$, it follows that if $t$ is transcendental over $K$ and $g_i(w, x^{(n-1)}, X_n, T)$ have a non-trivial common zero for $j = 1, \ldots, r$ then $g_i(w, tx^{(n-1)}, X_n, T)$ also have a non-trivial common zero. Therefore

$Q_\mu(w, tx^{(n-1)}) = 0$ for all $\mu$, and so $H_\lambda(w, x^{(n-1)}) = 0$. Therefore we may use the family of polynomials $(H_\lambda)$ instead of the family $(Q_\mu)$, and we obtain the property: *if* $(w, x^{(n-1)})$ *is a point in a field* $K$, *then*

$$g_i(w, x^{(n-1)}, X_n, T) \text{ have a non-trivial common zero for } i = 1, \ldots, r$$
$$\Leftrightarrow H_\lambda(w, x^{(n-1)}) = 0 \text{ for all } \lambda.$$

By induction on $n$, there exists a family $(R_\rho(W))$ of polynomials in $\mathbf{Z}[W]$ (actually homogeneous), having the property: *if* $(w)$ *is a point in a field* $K$, *then*

$$H_\lambda(w, X^{(n-1)}) \text{ have a non-trivial common zero for all } \lambda$$
$$\Leftrightarrow R_\rho(w) = 0 \text{ for all } \rho.$$

In light of Remark 4.4, this concludes the proof of Theorem 4.1 by the resultant method.

## §5. SPEC OF A RING

We shall extend the notions of §2 to arbitrary commutative rings.

Let $A$ be a commutative ring. By spec$(A)$ we mean the set of all prime ideals of $A$. An element of spec$(A)$ is also called a **point** of spec$(A)$.

If $f \in A$, we view the set of prime ideals $\mathfrak{p}$ of spec$(A)$ containing $f$ as the set of **zeros** of $f$. Indeed, it is the set of $\mathfrak{p}$ such that the image of $f$ in the canonical homomorphism

$$A \to A/\mathfrak{p}$$

is 0. Let $\mathfrak{a}$ be an ideal, and let $\mathfrak{Z}(\mathfrak{a})$ (the set of **zeros** of $\mathfrak{a}$) be the set of all primes of $A$ containing $\mathfrak{a}$. Let $\mathfrak{a}, \mathfrak{b}$ be ideals. Then we have:

**Proposition 5.1.**

(i) $\mathfrak{Z}(\mathfrak{ab}) = \mathfrak{Z}(\mathfrak{a}) \cup \mathfrak{Z}(\mathfrak{b})$.

(ii) *If* $\{\mathfrak{a}_i\}$ *is a family of ideals, then* $\mathfrak{Z}(\sum \mathfrak{a}_i) = \bigcap \mathfrak{Z}(\mathfrak{a}_i)$.

(iii) *We have* $\mathfrak{Z}(\mathfrak{a}) \subset \mathfrak{Z}(\mathfrak{b})$ *if and only if* $\mathrm{rad}(\mathfrak{a}) \supset \mathrm{rad}(\mathfrak{b})$, *where* $\mathrm{rad}(\mathfrak{a})$, *the radical of* $\mathfrak{a}$, *is the set of all elements* $x \in A$ *such that* $x^n \in \mathfrak{a}$ *for some positive integer* $n$.

*Proof.* Exercise. See Corollary 2.3 of Chapter X.

A subset $C$ of spec$(A)$ is said to be **closed** if there exists an ideal $\mathfrak{a}$ of $A$ such that $C$ consists of those prime ideals $\mathfrak{p}$ such that $\mathfrak{a} \subset \mathfrak{p}$. The complement of a closed subset of spec$(A)$ is called an **open subset** of spec$(A)$. The following statements are then very easy to verify, and will be left to the reader.

**Proposition 5.2.** *The union of a finite number of closed sets is closed. The intersection of an arbitrary family of closed sets is closed.*

*The intersection of a finite number of open sets is open. The union of an arbitrary family of open sets is open.*

*The empty set and* spec($A$) *itself are both open and closed.*

If $S$ is a subset of $A$, then the set of prime ideals $\mathfrak{p} \in \operatorname{spec}(A)$ such that $S \subset \mathfrak{p}$ coincides with the set of prime ideals $\mathfrak{p}$ containing the ideal generated by $S$.

The collection of open sets as in Proposition 5.2 is said to be a **topology** on spec($A$), called the **Zariski topology**.

**Remark.** In analysis, one considers a compact Hausdorff space $S$. "Hausdorff" means that given two points $P$, $Q$ there exists disjoint open sets $U_P$, $U_Q$ containing $P$ and $Q$ respectively. In the present algebraic context, the topology is not Hausdorff. In the analytic context, let $R$ be the ring of complex valued continuous functions on $S$. Then the maximal ideals of $R$ are in bijection with the points of $S$ (Gelfand-Naimark theorem). To each point $P \in S$, we associate the ideal $M_P$ of functions $f$ such that $f(P) = 0$. The association $P \mapsto M_P$ gives the bijection. There are analogous results in the complex analytic case. For a non-trivial example, see Exercise 19 of Chapter XII.

Let $A$, $B$ be commutative rings and $\varphi: A \to B$ a homomorphism. Then $\varphi$ induces a map

$$\varphi^* = \operatorname{spec}(\varphi) = \varphi^{-1} : \operatorname{spec}(B) \to \operatorname{spec}(A)$$

by

$$\mathfrak{p} \mapsto \varphi^{-1}(\mathfrak{p}).$$

Indeed, it is immediately verified that $\varphi^{-1}(\mathfrak{p})$ is a prime ideal of $A$. Note however that the inverse image of a maximal ideal of $B$ is not necessarily a maximal ideal of $A$. Example? The reader will verify at once that spec($\varphi$) is continuous, in the sense that if $U$ is open in spec($B$), then $\varphi^{-1}(U)$ is open in spec($A$).

We can then view spec as a contravariant functor from the category of commutative rings to the category of topological spaces.

By a **point** of spec($A$) **in a field** $L$ one means a mapping

$$\operatorname{spec}(\varphi) : \operatorname{spec}(L) \to \operatorname{spec}(A)$$

induced by a homomorphism $\varphi : A \to L$ of $A$ into $L$.

For example, for each prime number $p$, we get a point of spec($\mathbf{Z}$), namely the point arising from the reduction map

$$\mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}.$$

The corresponding point is given by the reversed arrow,

$$\operatorname{spec}(\mathbf{Z}) \leftarrow \operatorname{spec}(\mathbf{Z}/p\mathbf{Z}).$$

As another example, consider the polynomial ring $k[X_1, \ldots, X_n]$ over a field $k$. For each $n$-tuple $(c_1, \ldots, c_n)$ in $k^{a(n)}$ we get a homomorphism

$$\varphi : k[X_1, \ldots, X_n] \to k^a$$

such that $\varphi$ is the identity on $k$, and $\varphi(X_i) = c_i$ for all $i$. The corresponding point is given by the reversed arrow

$$\operatorname{spec} k[X] \leftarrow \operatorname{spec}(k^a).$$

Thus we may identify the points in $n$-space $k^{a(n)}$ with the points of spec $k[X]$ (over $k$) in $k^a$.

However, one does not want to take points only in the algebraic closure of $k$, and of course one may deal with the case of an arbitrary variety $V$ over $k$ rather than all of affine $n$-space. Thus let $k[x_1, \ldots, x_n]$ be a finitely generated entire ring over $k$ with a chosen family of generators. Let $V = \operatorname{spec} k[x]$. Let $A$ be a commutative $k$-algebra, corresponding to a homomorphism $k \to A$. Then a point of $V$ in $A$ may be described either as a homomorphism

$$\varphi\colon k[x_1, \ldots, x_n] \to A,$$

or as the reversed arrow

$$\operatorname{spec}(A) \to \operatorname{spec}(k[x])$$

corresponding to this homomorphism. If we put $c_i = \varphi(x_i)$, then one may call $(c) = (c_1, \ldots, c_n)$ the **coordinates of the point in** $A$. By a **generic point** of $V$ in a field $K$ we mean a point such that the map $\varphi\colon k[x] \to K$ is injective, i.e. an isomorphism of $k[x]$ with some subring of $K$.

Let $A$ be a commutative Noetherian ring. We leave it as an exercise to verify the following assertions, which translate the Noetherian condition into properties of closed sets in the Zariski topology.

Closed subsets of spec($A$) satisfy the **descending chain condition**, i.e., if

$$C_1 \supset C_2 \supset C_3 \supset \cdots$$

is a descending chain of closed sets, then we have $C_n = C_{n+1}$ for all sufficiently large $n$. Equivalently, let $\{C_i\}_{i \in I}$ be a family of closed sets. Then there exists a relatively minimal element of this family, that is a closed set $C_{i_0}$ in the family such that for all $i$, if $C_i \subset C_{i_0}$ then $C_i = C_{i_0}$. The proof follows at once from the corresponding properties of ideals, and the simple formalism relating unions and intersections of closed sets with products and sums of ideals.

A closed set $C$ is said to be **irreducible** if it cannot be expressed as the union of two closed sets

$$C \neq C_1 \cup C_2$$

with $C_1 \neq C$ and $C_2 \neq C$.

**Theorem 5.3.** *Let $A$ be a Noetherian commutative ring. Then every closed set $C$ can be expressed as a finite union of irreducible closed sets, and this expression is unique if in the union*

$$C = C_1 \cup \cdots \cup C_r$$

*of irreducible closed sets, we have $C_i \not\subset C_j$ if $i \neq j$.*

*Proof.* We give the proof as an example to show how the version of Theorem 2.2 has an immediate translation in the more general context of spec($A$). Suppose the family of closed sets which cannot be represented as a finite union of irreducible ones is not empty. Translating the Noetherian hypothesis in this case shows that there exists a minimal such set $C$. Then $C$ cannot be irreducible, and we can write $C$ as a union of closed sets

$$C = C' \cup C'',$$

with $C' \neq C$ and $C'' \neq C$. Since $C'$ and $C''$ are strictly smaller than $C$, then we can express $C'$ and $C''$ as finite unions of irreducible closed sets, thus getting a similar expression for $C$, and a contradiction which proves existence.

As to uniqueness, let

$$C = C_1 \cup \cdots \cup C_r = Z_1 \cup \cdots \cup Z_s$$

be an expression of $C$ as union of irreducible closed sets, without inclusion relations. For each $Z_j$ we can write

$$Z_j = (Z_j \cap C_1) \cup \cdots \cup (Z_j \cap C_r).$$

Since each $Z_j \cap C_i$ is a closed set, we must have $Z_j = Z_j \cap C_i$ for some $i$. Hence $Z_j = C_i$ for some $i$. Similarly, $C_i$ is contained in some $Z_k$. Since there is no inclusion relation among the $Z_j$'s, we must have $Z_j = C_i = Z_k$. This argument can be carried out for each $Z_j$ and each $C_i$. This proves that each $Z_j$ appears among the $C_i$'s and each $C_i$ appears among the $Z_j$'s, and proves the uniqueness of our representation. This proves the theorem.

**Proposition 5.4.** *Let $C$ be a closed subset of* spec($A$). *Then $C$ is irreducible if and only if $C = \mathfrak{Z}(\mathfrak{p})$ for some prime ideal $\mathfrak{p}$.*

*Proof.* Exercise.

More properties at the same basic level will be given in Exercises 14–19.

# EXERCISES

## Integrality

1. (Hilbert-Zariski) Let $k$ be a field and let $V$ be a homogeneous variety with generic point $(x)$ over $k$. Let $\mathfrak{Z}$ be the algebraic set of zeros in $k^a$ of a homogeneous ideal in $k[X]$ generated by forms $f_1, \ldots, f_r$ in $k[X]$. Prove that $V \cap \mathfrak{Z}$ has only the trivial zero if and only if each $x_i$ is integral over the ring $k[f(x)] = k[f_1(x), \ldots, f_r(x)]$. (Compare with Theorem 3.7 of Chapter VII.)
2. Let $f_1, \ldots, f_r$ be forms in $n$ variables and suppose $n > r$. Prove that these forms have a non-trivial common zero.
3. Let $R$ be an entire ring. Prove that $R$ is integrally closed if and only if the local ring $R_\mathfrak{p}$ is integrally closed for each prime ideal $\mathfrak{p}$.
4. Let $R$ be an entire ring with quotient field $K$. Let $t$ be transcendental over $K$. Let $f(t) = \sum a_i t^i \in K[t]$. Prove:
   (a) If $f(t)$ is integral over $R[t]$, then all $a_i$ are integral over $R$.
   (b) If $R$ is integrally closed, then $R[t]$ is integrally closed.

For the next exercises, we let $R = k[x] = k[X]/\mathfrak{p}$, where $\mathfrak{p}$ is a homogeneous prime ideal. Then $(x)$ is a homogeneous generic point for a $k$-variety $V$. We let $I$ be the integral closure of $R$ in $k(x)$. We assume for simplicity that $k(x)$ is a regular extension of $k$.

5. Let $z = \sum c_i x_i$ with $c_i \in k$, and $z \neq 0$. If $k[x]$ is integrally closed, prove that $k[x/z]$ is integrally closed.
6. Define an element $f \in k(x)$ to be **homogeneous** if $f(tx) = t^d f(x)$ for $t$ transcendental over $k(x)$ and some integer $d$. Let $f \in I$. Show that $f$ can be written in the form $f = \sum f_i$ where each $f_i$ is homogeneous of degree $i \geqq 0$, and where also $f_i \in I$. (Some $f_i$ may be 0, of course.)

We let $R_m$ denote the set of elements of $R$ which are homogeneous of degree $m$. Similarly for $I_m$. We note that $R_m$ and $I_m$ are vector spaces over $k$, and that $R$ (resp. $I$) is the direct sum of all spaces $R_m$ (resp. $I_m$) for $m = 0, 1, \ldots$ This is obvious for $R$, and it is true for $I$ because of Exercise 6.

7. Prove that $I$ can be written as a sum $I = Rz_1 + \cdots + Rz_s$, where each $z_i$ is homogeneous of some degree $d_i$.
8. Define an integer $m \geqq 1$ to be **well behaved** if $I_m^q = I_{qm}$ for all integers $q \geqq 1$. If $R = I$, then all $m$ are well behaved. In Exercise 7, suppose $m \geqq \max d_i$. Show that $m$ is well behaved.
9. (a) Prove that $I_m$ is a finite dimensional vector space over $k$. Let $w_0, \ldots, w_M$ be a basis for $I_m$ over $k$. Then $k[I_m] = k[w]$.
   (b) If $m$ is well behaved, show that $k[I_m]$ is integrally closed.
   (c) Denote by $k((x))$ the field generated over $k$ by all quotients $x_i/x_j$ with $x_j \neq 0$, and similarly for $k((w))$. Show that $k((x)) = k((w))$.

(If you want to see Exercises 4–9 worked out, see my *Introduction to Algebraic Geometry*, Interscience 1958, Chapter V.)

## Resultants

10. Prove that the resultant defined for $n$ forms in $n$ variables in §3 actually coincides with the resultant of Chapter IV, or §4 when $n = 2$.

11. Let $\mathfrak{a} = (f_1, \ldots, f_r)$ be a homogeneous ideal in $k[X_1, \ldots, X_n)$ (with $k$ algebraically closed). Assume that the only zeros of $\mathfrak{a}$ consist of a finite number of points $(x^{(1)}), \ldots, (x^{(d)})$ in projective space $\mathbf{P}^{n-1}$, so the coordinates of each $x^{(j)}$ can be taken in $k$. Let $u_1, \ldots, u_n$ be independent variables and let

$$L_u(X) = u_1X_1 + \cdots + u_nX_n.$$

Let $R_1(u), \ldots, R_s(u) \in k[u]$ be a resultant system for $f_1, \ldots, f_r, L_u$.

(a) Show that the common non-trivial zeros of the system $R_i(u)$ $(i = 1, \ldots, s)$ in $k$ are the zeros of the polynomial

$$\prod_j L_u(x^{(j)}) \in k[u].$$

(b) Let $D(u)$ be the greatest common divisor of $R_1(u), \ldots, R_s(u)$ in $k[u]$. Show that there exist integers $m_j \geqq 1$ such that (up to a factor in $k$)

$$D(u) = \prod_{j=1}^{d} L_u(x^{(j)})^{m_j}.$$

[See van der Waerden, *Moderne Algebra*, Second Edition, Volume II, §79.]

12. For forms in 2 variables, prove directly from the definition used in §4 that one has

$$\operatorname{Res}(fg, h) = \operatorname{Res}(f, h) \operatorname{Res}(g, h)$$

$$\operatorname{Res}(f, g) = (-1)^{(\deg f)(\deg g)} \operatorname{Res}(g, f).$$

13. Let $k$ be a field and let $\mathbf{Z} \to k$ be the canonical homomorphism. If $F \in \mathbf{Z}[W, X]$, we denote by $\overline{F}$ the image of $F$ in $k[W, X]$ under this homomorphism. Thus we get $\overline{R}$, the image of the resultant $R$.

(a) Show that $\overline{R}$ is a generator of the prime ideal $\mathfrak{p}_{k,1}$ of Theorem 3.5 over the field $k$. Thus we may denote $\overline{R}$ by $R_k$.

(b) Show that $R$ is absolutely irreducible, and so is $R_k$. In other words, $R_k$ is irreducible over the algebraic closure of $k$.

## Spec of a ring

14. Let $A$ be a commutative ring. Define spec$(A)$ to be **connected** if spec$(A)$ is not the union of two disjoint non-empty closed sets (or equivalently, spec$(A)$ is not the union of two disjoint, non-empty open sets).

(a) Suppose that there are idempotents $e_1, e_2$ in $A$ (that is $e_1^2 = e_1$ and $e_2^2 = e_2$), $\neq 0, 1$, such that $e_1e_2 = 0$ and $e_1 + e_2 = 1$. Show that spec$(A)$ is not connected.

(b) Conversely, if spec$(A)$ is not connected, show that there exist idempotents as in part (a).

In either case, the existence of the idempotents is equivalent with the fact that the ring $A$ is a product of two non-zero rings, $A = A_1 \times A_2$.

15. Prove that the Zariski topology is **compact**, in other words: let $\{U_i\}_{i \in I}$ be a family of open sets such that

$$\bigcup_i U_i = \text{spec}(A).$$

Show that there is a finite number of open sets $U_{i_1}, \ldots, U_{i_n}$ whose union is spec($A$). [*Hint*: Use closed sets, and use the fact that if a sum of ideals is the unit ideal, then 1 can be written as a finite sum of elements.]

16. Let $f$ be an element of $A$. Let $S$ be the multiplicative subset $\{1, f, f^2, f^3, \ldots\}$ consisting of the powers of $f$. We denote by $A_f$ the ring $S^{-1}A$ as in Chapter II, §3. From the natural homomorphism $A \to A_f$ one gets the corresponding map $\text{spec}(A_f) \to \text{spec}(A)$.
    (a) Show that $\text{spec}(A_f)$ maps on the open set of points in spec($A$) which are not zeros of $f$.
    (b) Given a point $\mathfrak{p} \in \text{spec}(A)$, and an open set $U$ containing $\mathfrak{p}$, show that there exists $f$ such that $\mathfrak{p} \in \text{spec}(A_f) \subset U$.

17. Let $U_i = \text{spec}(A_{f_i})$ be a finite family of open subsets of spec($A$) covering spec($A$). For each $i$, let $a_i/f_i \in A_{f_i}$. Assume that as functions on $U_i \cap U_j$ we have $a_i/f_i = a_j/f_j$ for all pairs $i, j$. Show that there exists a unique element $a \in A$ such that $a = a_i/f_i$ in $A_{f_i}$ for all $i$.

18. Let $k$ be a field and let $k[x_1, \ldots, x_n] = A \subset K$ be a finitely generated subring of some extension field $K$. Assume that $k(x_1, \ldots, x_n)$ has transcendence degree $r$. Show that every maximal chain of prime ideals

$$A \supset P_1 \supset P_2 \supset \ldots \supset P_m \supset \{0\},$$

with $P_1 \neq A$, $P_i \neq P_{i+1}$, $P_m \neq \{0\}$, must have $m = r$.

19. Let $A = \mathbf{Z}[x_1, \ldots, x_n]$ be a finitely generated entire ring over $\mathbf{Z}$. Show that every maximal chain of prime ideals as in Exercise 18 must have $m = r + 1$. Here, $r$ = transcendence degree of $\mathbf{Q}(x_1, \ldots, x_n)$ over $\mathbf{Q}$.