putting them together gives a decomposition for $(*)$, so $X \notin \Sigma$. This contradiction proves $\Sigma = \emptyset$. This proves the existence part of (b). The uniqueness is an easy exercise, see Ex. 3.8. Q.E.D.

The proof of (b) is a typical algebraist's proof: it's logically very neat, but almost completely hides the content: the real point is that if X is not irreducible, then it breaks up as $X = X_1 \cup X_2$, and then you ask the same thing about X_1 and X_2, and so on; eventually, you must get to irreducible algebraic sets, since otherwise you'd get an infinite descending chain.

3.8 Preparation for the Nullstellensatz

I now want to state and prove the Nullstellensatz. There is an intrinsic difficulty in any proof of the Nullstellensatz, and I choose to break it up into two segments. Firstly I state without proof an assertion in commutative algebra, which will be proved in (3.15) below (in fact parts of the proof will have strong geometric content).

Hard Fact *Let k be a (infinite) field, and $A = k[a_1, \dots, a_n]$ a finitely generated k-algebra. Then*

$$A \text{ is a field} \implies A \text{ is algebraic over } k.$$

Just to give a rough idea why this is true, notice that if $t \in A$ is transcendental over k, then $k[t]$ is a polynomial ring, so *has infinitely many primes* (by Euclid's argument). Hence the extension $k \subset k(t)$ is not finitely generated as k-algebra: finitely many elements $p_i/q_i \in k(t)$ can have only finitely many primes among their denominators.

3.9 Definition: radical ideal

Definition If I is an ideal of A, the *radical* of I is

$$\operatorname{rad} I = \sqrt{I} = \left\{ f \in A \;\middle|\; f^n \in I \text{ for some } n \right\}.$$

$\operatorname{rad} I$ is an ideal, since $f, g \in \operatorname{rad} I \implies f^n, g^m \in I$ for suitable n, m, and therefore

$$(f+g)^r = \sum \binom{r}{a} f^a g^{r-a} \in I \quad \text{if } r \geq n+m-1.$$

An ideal I is *radical* if $I = \operatorname{rad} I$.

Note that a prime ideal is radical. It's not hard to see that in a UFD like $k[X_1, \dots, X_n]$, a principal ideal $I = (f)$ where $f = \prod f_i^{n_i}$ (factorisation into distinct prime factors), has $\operatorname{rad} I = (f_{\text{red}})$, where $f_{\text{red}} = \prod f_i$.

Nullstellensatz 3.10 (Hilbert's zeros theorem) *Let k be an algebraically closed field.*

(a) Every maximal ideal of the polynomial ring $A = k[X_1, \dots, X_n]$ is of the form $m_P = (X_1 - a_1, \dots, X_n - a_n)$ for some point $P = (a_1, \dots, a_n) \in \mathbb{A}^n_k$; that is, it's the ideal $I(P)$ of all functions vanishing at P.

(b) Let $J \subset A$ be an ideal, $J \neq (1)$; then $V(J) \neq \emptyset$.

(c) For any $J \subset A$,

$$I(V(J)) = \operatorname{rad} J.$$

The essential content of the theorem is (b), which says that if an ideal J is not the whole of $k[X_1, \dots, X_n]$, then it will have zeros in $\mathbb{A}_k^n$. Note that (b) is completely false if k is not algebraically closed, since if $f \in k[X]$ is a nonconstant polynomial then it will not generate the whole of $k[X]$ as an ideal, but $V(f) = \emptyset \subset \mathbb{A}_k^1$ is perfectly possible. The name of the theorem (*Nullstelle* = zero of a polynomial+*Satz* = theorem) should help to remind you of the content (but stick to the German if you don't want to be considered an ignorant peasant).

Corollary *The correspondences* V *and* I

$$\begin{array}{lccc} & \{\textit{ideals } I \subset A\} & \xleftrightarrow{V,I} & \{\textit{subsets } X \subset \mathbb{A}_k^n\} \\ \textit{induce bijections} & \bigcup & & \bigcup \\ & \{\textit{radical ideals}\} & \longleftrightarrow & \{\textit{algebraic subsets}\} \\ \textit{and} & \bigcup & & \bigcup \\ & \{\textit{prime ideals}\} & \longleftrightarrow & \{\textit{irreducible alg. subsets}\}. \end{array}$$

This holds because $V(I(X)) = X$ for any algebraic set X by (3.6, b), and $I(V(J)) = J$ for any radical ideal J by (c) above.

Proof of NSS (assuming (3.8)) (a) Let $m \subset k[X_1, \dots, X_n]$ be a maximal ideal; write $K = k[X_1, \dots, X_n]/m$, and φ for the composite of natural maps $\varphi\colon k \to k[X_1, \dots, X_n] \to K$. Then K is a field (since m is maximal), and it is finitely generated as k-algebra (since it is generated by the images of the X_i). So by (3.8), $\varphi\colon k \to K$ is an algebraic field extension. But k is algebraically closed, hence φ is an isomorphism.

Now for each i, $X_i \in k[X_1, \dots, X_n]$ maps to some element $b_i \in K$; so taking $a_i = \varphi^{-1}(b_i)$ gives $X_i - a_i \in \ker\{k[X_1, \dots, X_n] \to K\} = m$. Hence there exist $a_1, \dots, a_n \in k$ such that $(X_1 - a_1, \dots, X_n - a_n) \subset m$. On the other hand, it's clear that the left-hand side is a maximal ideal, so $(X_1 - a_1, \dots, X_n - a_n) = m$. This proves (a).

(a) $\implies$ (b) This is easy. If $J \neq A = k[X_1, \dots, X_n]$ then there exists a maximal ideal m of A such that $J \subset m$ (the existence of m is easy to check, using the a.c.c.). By (a), m is of the form

$$m = (X_1 - a_1, \dots, X_n - a_n);$$

then $J \subset m$ just means that $f(P) = 0$ for all $f \in J$, where $P = (a_1, \dots, a_n)$. Therefore $P \in V(J)$.

(b) $\implies$ (c) This requires a cunning trick. Let $J \subset k[X_1, \dots, X_n]$ be any ideal, and $f \in k[X_1, \dots, X_n]$. Introduce another variable Y, and consider the new ideal

$$J_1 = (J, fY - 1) \subset k[X_1, \dots, X_n, Y]$$

generated by J and $fY - 1$. Roughly speaking, $V(J_1)$ is the variety consisting of $P \in V(J)$ such that $f(P) \neq 0$. More precisely, a point $Q \in V(J_1) \subset \mathbb{A}_k^{n+1}$ is an $(n+1)$-tuple $Q = (a_1, \dots, a_n, b)$ such that

$$g(a_1, \dots, a_n) = 0 \text{ for all } g \in J, \quad \text{that is,} \quad P = (a_1, \dots, a_n) \in V(J),$$

and

$$f(P) \cdot b = 1, \quad \text{that is,} \quad f(P) \neq 0 \text{ and } b = f(P)^{-1}.$$

Now suppose that $f(P) = 0$ for all $P \in V(J)$; then clearly, from what I've just said, $V(J_1) = \emptyset$. So I can use (b) to deduce that $1 \in J_1$, that is, there exists an expression

$$1 = \sum g_i f_i + g_0(fY - 1) \in k[X_1, \dots, X_n, Y] \tag{$**$}$$

with $f_i \in J$, and $g_0, g_i \in k[X_1, \dots, X_n, Y]$.

Consider the way in which Y appears in the right-hand side of $(**)$: apart from its explicit appearance in the second term, it can appear in each of the g_i; suppose that Y^N is the highest power of Y appearing in any of g_0, g_i. If I then multiply through both sides of $(**)$ by f^N, I get a relation of the form

$$f^N = \sum G_i(X_1, \dots, X_n, fY) f_i + G_0(X_1, \dots, X_n, fY)(fY - 1); \tag{$***$}$$

here G_i is just $f^N g_i$ written out as a polynomial in $X_1, \dots, X_n$ and fY.

$(***)$ is just an equality of polynomials in $k[X_1, \dots, X_n, Y]$, so I can reduce it modulo $(fY - 1)$ to get

$$f^N = \sum h_i(X_1, \dots, X_n) f_i \in k[X_1, \dots, X_n, Y]/(fY - 1);$$

both sides of the equation are elements of $k[X_1, \dots, X_n]$. Since the natural homomorphism $k[X_1, \dots, X_n] \hookrightarrow k[X_1, \dots, X_n, Y]/(fY-1)$ is injective (it is just the inclusion of $k[X_1, \dots, X_n]$ into $k[X_1, \dots, X_n][f^{-1}]$, as a subring of its field of fractions), it follows that

$$f^N = \sum h_i(X_1, \dots, X_n) f_i \in k[X_1, \dots, X_n];$$

that is, $f^N \in J$ for some N. Q.E.D.

Remark Several of the textbooks cut the argument short by just saying that $(**)$ is an identity, so it remains true if we set $Y = f^{-1}$. This is of course perfectly valid, but I have preferred to spell it out in detail.

3.11 Worked examples

(a) Hypersurfaces. The simplest example of a variety is the hypersurface $V(f) : (f = 0) \subset \mathbb{A}^n_k$. If k is algebraically closed, there is just the obvious correspondence between irreducible elements $f \in k[X_1, \dots, X_n]$ and irreducible hypersurfaces: it follows from the Nullstellensatz that two distinct irreducible polynomials f_1, f_2 (not multiples of one another) define different hypersurfaces $V(f_1)$ and $V(f_2)$. This is not at all obvious (for example, it's false over $\mathbb{R}$), although it can be proved without using the Nullstellensatz by *elimination theory*, a much more explicit method with a nice 19th century flavour; see Ex. 3.13.

(b) Once past the hypersurfaces, most varieties are given by "lots" of equations; contrary to intuition, it is usually the case that the ideal $I(X)$ needs many generators, that is, many more than the codimension of X. I give an example of a curve $C \subset \mathbb{A}^3_k$ for which $I(C)$ needs 3 generators; assume that k is an infinite field.