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

$$\operatorname{rad} I = \sqrt{I} = \bigl\{ f \in A \bigm| f^n \in I \text{ for some } n \bigr\}.$$

$\operatorname{rad} I$ 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 $V(J) \neq \emptyset$.*