3.7 Irreducible algebraic set

An algebraic set $X \subset \mathbb{A}^n_k$ is *irreducible* if there does not exist a decomposition

$$X = X_1 \cup X_2 \quad \text{with} \quad X_1, X_2 \subsetneq X$$

of X as a union of two strict algebraic subsets. For example, the algebraic subset $V(xy) \subset \mathbb{A}^2_k$ is the locus consisting of the two coordinate axes, and is obviously the union of $V(x)$ and $V(y)$, hence reducible.

Proposition *(a) Let $X \subset \mathbb{A}^n_k$ be an algebraic set and $I(X)$ the corresponding ideal; then*

$$X \text{ is irreducible} \iff I(X) \text{ is prime.}$$

(b) Any algebraic set X has a (unique) expression

$$X = X_1 \cup \cdots \cup X_r \tag{$*$}$$

with X_i irreducible and $X_i \not\subset X_j$ for $i \neq j$.
The X_i in $(*)$ are the irreducible components *of X.*

Proof (a) In fact I prove that X is reducible $\iff$ $I(X)$ is not prime.

($\Longrightarrow$) Suppose $X = X_1 \cup X_2$ with $X_1, X_2 \subsetneq X$ algebraic subsets. Then $X_1 \subsetneq X$ means that there exists $f_1 \in I(X_1) \setminus I(X)$, and similarly $X_2 \subsetneq X$ gives $f_2 \in I(X_2) \setminus I(X)$. Now the product $f_1 f_2$ vanishes at all points of X, and so $f_1 f_2 \in I(X)$. Therefore $I(X)$ is not prime.

($\Longleftarrow$) Suppose that $I(X)$ is not prime; then there exist $f_1, f_2 \notin I(X)$ such that $f_1 f_2 \in I(X)$. Let $I_1 = (I(X), f_1)$ and $V(I_1) = X_1$; then $X_1 \subsetneq X$ is an algebraic subset; similarly, setting $I_2 = (I(X), f_2)$ and $V(I_2) = X_2$ gives $X_2 \subsetneq X$. But $X \subset X_1 \cup X_2$, since for all $P \in X$, $f_1 f_2(P) = 0$ implies that either $f_1(P) = 0$ or $f_2(P) = 0$.

(b) First of all, I establish the following proposition: the algebraic subsets of $\mathbb{A}^n_k$ satisfy the descending chain condition, that is, every chain

$$X_1 \supset X_2 \supset \cdots \supset X_n \supset \cdots$$

eventually stops with $X_N = X_{N+1} = \cdots$. This is because

$$I(X_1) \subset I(X_2) \subset \cdots \subset I(X_n) \subset \cdots$$

is an ascending chain of ideals of A, and this stops, giving $X_N = X_{N+1} = \cdots$. Thus just as in (3.1),

$$\text{any nonempty set } \Sigma \text{ of algebraic subsets of } \mathbb{A}^n_k \text{ has a minimal element.} \tag{!}$$

Now to prove (b), let Σ be the set of algebraic subsets of $\mathbb{A}^n_k$ which do not have a decomposition $(*)$. If $\Sigma = \emptyset$ then (b) is proved. On the other hand, if $\Sigma \neq \emptyset$ then by (!), there must be a minimal element $X \in \Sigma$, and this leads speedily to one of two contradictions: if X is irreducible, then $X \notin \Sigma$, a contradiction; if X is reducible, then $X = X_1 \cup X_2$, with $X_1, X_2 \subsetneq X$, so that by minimality of $X \in \Sigma$, I get $X_1, X_2 \notin \Sigma$. So each of X_1, X_2 has a decomposition $(*)$ as a union of irreducibles, and 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*

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

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 $\operatorname{rad} I = (f_{\mathrm{red}})$, where $f_{\mathrm{red}} = \prod f_i$.

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 $V(J) \neq \emptyset$.