5 Affine algebraic varietes. Hilbert Nullstellensatz.

5.1 Affine algebraic varietes.

Definition 5.1. *A nonempty affine algebraic set $V \subseteq k^n$ will be called an **affine algebraic variety** if the ideal $\mathcal{I}(V)$ of the ring $k[x_1, ..., x_n]$ is prime.*

Definition 5.2. *A nonempty affine algebraic set $V \subseteq k^n$ will be called **irreducible**, if for affine algebraic sets $A, B \subseteq k^n$:*

$$V = A \cup B \Rightarrow V = A \vee V = B.$$

Theorem 5.3. *A nonempty affine algebraic set $V \subseteq k^n$ is irreducible if and only if it is an affine algebraic variety.*

Proof. Assume that an affine algebraic set $V \subseteq k^n$ is not irreducible. Then $V = A \cup B$, for some affine algebraic sets $A, B \subseteq k^n$, with $V \neq A$ and $V \neq B$. Since $V \supseteq A$, we see that $\mathcal{I}(V) \subseteq \mathcal{I}(A)$. Also, since $V \neq A$, by Remark 4.6.5 $\mathcal{I}(V) \neq \mathcal{I}(A)$. Thus there exists $f \in \mathcal{I}(A)$ with $f \notin \mathcal{I}(V)$. Likewise, there exists $g \in \mathcal{I}(B)$ with $g \notin \mathcal{I}(V)$. But $fg \in \mathcal{I}(V)$, as for $\underline{a} \in V$ either $\underline{a} \in A$ and then $f(\underline{a}) = 0$, or $\underline{a} \in B$ and then $g(\underline{a}) = 0$ – consequently, $fg(\underline{a}) = 0$. Therefore the ideal $\mathcal{I}(V)$ is not prime.

Conversely, suppose that V is irreducible and the ideal $\mathcal{I}(V)$ is not prime. Let $f, g \in k[x_1, ..., x_n]$ be such that $fg \in \mathcal{I}(V)$ and $f \notin \mathcal{I}(V)$, $g \notin \mathcal{I}(V)$. Then

$$A = \mathcal{Z}(f) \cap V \quad \text{and} \quad B = \mathcal{Z}(g) \cap V$$

are both algebraic sets. We shall show that

$$V = A \cup B \quad \text{and} \quad V \neq A, V \neq B.$$

Indeed, if $\underline{a} \in V$ then, as $fg \in \mathcal{I}(V)$, $fg(\underline{a}) = f(\underline{a})g(\underline{a}) = 0$, so that either $f(\underline{a}) = 0$ or $g(\underline{a}) = 0$, and, consequently, $\underline{a} \in A$ or $\underline{a} \in B$. Hence $V \subseteq A \cup B$, and as $V \supseteq A$ and $V \supseteq B$, this yields $V = A \cup B$.

Moreover, suppose that $V = A$. Then $\mathcal{I}(V) = \mathcal{I}(A)$, but $f \in \mathcal{I}(A)$ with $f \notin \mathcal{I}(V)$. Thus $V \neq A$ and similarly $V \neq B$. □

Theorem 5.4. *Every affine algebraic set V is a finite sum of affine algebraic varieties:*

$$V = V_1 \cup ... \cup V_r, \quad r \geq 1.$$

If in the above decomposition the varieties V_i are incomparable (that is $V_i \not\subset V_j$ for $i \neq j$), then they are uniquely defined.

Proof. We shall prove the existence of such a decomposition first. Let

$$\mathcal{R} = \{V \subseteq k^n | \, V \text{ is algebraic and not a sum of affine algebraic varieties}\}.$$

Suppose $\mathcal{R} \neq \emptyset$. By Remark 4.15 there is a minimal element in $\mathcal{R}$, say Z, which is thus not a sum of affine algebraic varieties. It is not a variety itself then, and hence is not irreducible. Hence

$$Z = A \cup B \quad \text{and} \quad Z \neq A, Z \neq B,$$

for some affine algebraic sets $A, B \subseteq k^n$. By the minimality of Z, $A, B \notin \mathcal{R}$, so that both A and B are sums of affine algebraic varieties. But then so is Z – a contradiction.

For the proof of uniqueness, suppose that

$$V = V_1 \cup ... \cup V_r = W_1 \cup ... \cup W_s,$$

where $V_1, ..., V_r, W_1, ..., W_s \subseteq k^n$ are incomparable affine algebraic varieties. For a fixed $i \in \{1, ..., r\}$:

$$V_i = V \cap V_i = (W_1 \cup ... \cup W_s) \cap V_i = (W_1 \cap V_i) \cup ... \cup (W_s \cap V_i),$$

and since V_i is a variety, hence an irreducible set, $V_i = W_{k_i} \cap V_i$, for some $k_i \in \{1, ..., s\}$ and, in particular, $V_i \subseteq W_{k_i}$. Likewise, for every $j \in \{1, ..., s\}$ there exists $l_j \in \{1, ..., r\}$ such that $W_j \subseteq V_{l_j}$. Consequently, as V_i's and W_j's are incomparable, $V_i \subseteq W_{k_i} \subseteq V_{l_{k_i}}$ leads to $i = l_{k_i}$ and $V_i = W_{k_i}$. Therefore every V_i is equal to some of the W_j's and $r \leqslant s$. Likewise, every W_j is equal to some of the V_i's and $s \leqslant r$. This together means that $r = s$ and $V_1, ..., V_r$ differ from $W_1, ..., W_s$ at most by the order of appearance. □

Remark 5.5. Let $V \subseteq k^n$ be an affine algebraic variety endowed with the Zariski topology inherited from k^n. Then every nonempty open subset $U \subseteq V$ is dense.

Proof. Let $U \subseteq V$ be a nonempty open subset of V, and denote by $\bar{U}$ the closure of U in V. Then $V = \bar{U} \cup (V \setminus \bar{U})$ is a decomposition of V into two affine algebraic sets. But as V is a variety and hence irreducible, it follows that $V = \bar{U}$ or $V = V \setminus \bar{U}$, the latter case being impossible as U is nonempty. □

Remark 5.6. Let $V \subseteq k^n$ be an affine algebraic variety endowed with the Zariski topology inherited from k^n. Then in V every two nonempty open sets have a nonempty intersection.

Proof. Let $U_1, U_2 \subseteq V$ be two open sets. Thus $U_1 = V \setminus V_1$ and $U_2 = V \setminus V_2$, for some affine algebraic sets $V_1, V_2 \subseteq k^n$. But then

$$V = V_1 \cup V_2 \cup [(V \setminus V_1) \cap (V \setminus V_2)] = V_1 \cup V_2 \cup (U_1 \cap U_2).$$

If $U_1 \cap U_2 = \emptyset$, then $V = V_1$ or $V = V_2$, as V is a variety and hence an irreducible set. But since U_1, $U_2 \neq \emptyset$, this is impossible. □

Remark 5.7. Let $\operatorname{Spec} k[x_1, ..., x_n]$ denote the **prime spectrum** of the ring $k[x_1, ..., x_n]$, that is the set of all prime ideals. Let $\operatorname{Var} k^n$ denote the set of all affine algebraic varieties in k^n. The map

$$\mathcal{I} \colon \operatorname{Var} k^n \to \operatorname{Spec} k[x_1, ..., x_n], \quad V \mapsto \mathcal{I}(V)$$

is

1. injective,
2. surjective if and only if for every prime ideal $\mathfrak{p}$ of the ring $k[x_1, ..., x_n]$

$$\mathfrak{p} = \mathcal{I}(\mathcal{Z}(\mathfrak{p})).$$

Proof. The map $\mathcal{I}$ is injective by Remark 4.6.5. Assume that the map $\mathcal{I}$ is surjective, that is for every $\mathfrak{p} \in \operatorname{Spec} k[x_1, ..., x_n]$, $\mathfrak{p} = \mathcal{I}(V)$, for some affine algebraic variety $V \subseteq k^n$. But then $\mathcal{Z}(\mathfrak{p}) = \mathcal{Z}(\mathcal{I}(V)) = V$, so that $\mathfrak{p} = \mathcal{I}(\mathcal{Z}(\mathfrak{p}))$.

Conversely, assume that $\mathfrak{p} = \mathcal{I}(\mathcal{Z}(\mathfrak{p}))$ for all $\mathfrak{p} \in \operatorname{Spec} k[x_1, ..., x_n]$. But then $\mathcal{Z}(\mathfrak{p})$ is a variety, and the ideal $\mathfrak{p}$ is its image via the map $\mathcal{I}$. □

5.2 Hilbert Nullstellensatz.

Remark 5.8. Let $\mathfrak{a} \lhd k[x_1, ..., x_n]$. Then

$$\mathfrak{a} \subseteq \operatorname{rad}(\mathfrak{a}) \subseteq \mathcal{I}(\mathcal{Z}(\mathfrak{a})).$$

Proof. Fix $f \in \operatorname{rad}(\mathfrak{a})$. Then $f^m \in \mathfrak{a}$, for some $m \in \mathbb{N}$. In particular, $f^m(\underline{a}) = 0$, for all $\underline{a} \in \mathcal{Z}(\mathfrak{a})$, but then also $f(\underline{a}) = 0$, for all $\underline{a} \in \mathcal{Z}(\mathfrak{a})$. Thus $f \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. □

Theorem 5.9. (Hilbert Nullstellensatz) *Let k be algebraically closed, let $\mathfrak{a} \lhd k[x_1, ..., x_n]$. Then* $\operatorname{rad}(\mathfrak{a}) = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$.

The proof follows from a series of lemmas which we shall prove now. We will also need some basic definitions and facts from the theory of extensions of rings.

Definition 5.10. *Let B be a domain and let A be a subring of B. An element $x \in B$ is* ***integral*** *over A if there exist $a_1, ..., a_n \in A$ such that*

$$a_1 + a_2 x + ... + a_n x^{n-1} + x^n = 0;$$

The set of all elements of B integral over A will be denoted by $C_B(A)$ and called the ***integral closure*** *of A in B.*

Proposition 5.11. *Let B be a domain and let A be a subring of B. Then the integral closure $C_B(A)$ of A in B forms a ring.*

We shall give a somewhat old-fashioned proof here that utilizes the notions of symmetric polynomials[5.1], elementary symmetric polynomials[5.2], and the fundamental theorem on symmetric polynomials.[5.3]

Proof. Let $f = a_1 + a_2 x + ... + a_n x^{n-1} + x^n \in A[x]$ and let $\alpha_1, ..., \alpha_n$ be the roots of f in some larger ring. By the Viete's formulas

$$a_n = -S_1(\alpha_1, ..., \alpha_n), a_{n-1} = S_2(\alpha_1, ..., \alpha_n), ..., a_1 = \pm S_n(\alpha_1, ..., \alpha_n),$$

5.1. A polynomial $P(x_1, ..., x_n) \in A[x_1, ..., x_n]$ is **symmetric** if for every permutation $\sigma \in S(n)$:

$$P(x_1, ..., x_n) = P(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

5.2. The **elementary symmetric polynomials** are defined as follows:

$$\begin{aligned}
S_1(x_1, ..., x_n) &= x_1 + ... + x_n, \\
S_2(x_1, ..., x_n) &= x_1x_2 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n, \\
&\vdots \\
S_k(x_1, ..., x_n) &= \sum_{i_1 < i_2 < ... < i_k} x_{i_1} \cdot ... \cdot x_{i_k}, \\
&\vdots \\
S_n(x_1, ..., x_n) &= x_1 \cdot ... \cdot x_n.
\end{aligned}$$

5.3. **Theorem (Fundamental Theorem on Symmetric Polynomials):** Every symmetric polynomial $P(x_1, ..., x_n) \in A[x_1, ..., x_n]$ is equal to a polynomial in the elementary symmetric polynomials with coefficients in A, i.e. $P \in A[S_1, ..., S_n]$.

that is the elementary symmetric polynomials in roots of f lie in A. Consequently, by the fundamental theorem on symmetric polynomials, every symetric polynomial with coefficients from A in the roots of f lies in A. Moreover, every polynomial $g(\alpha_1, ..., \alpha_n)$ with coefficients from A in the roots of f is a root of a monic polynomial in $A[x]$: indeed, the polynomial

$$h(x) = \prod_{\sigma \in S(n)} (x - g(\alpha_{\sigma(1)}, ..., \alpha_{\sigma(n)}))$$

is a monic polynomial whose coefficients are symmetric polynomials in the α_i's, and therefore lie in A. But $g(\alpha_1, ..., \alpha_n)$ is one of the roots of h.

Now if α_1 and α_2 are two elements of B integral over A, then there exists a monic polynomial with coefficients in A having both α_1 and α_2 as roots. Take $g(\alpha_1, \alpha_2, ...) = \alpha_1 \pm \alpha_2$ and then $g(\alpha_1, \alpha_2, ...) = \alpha_1 \cdot \alpha_2$ to deduce that these elements are also integral over A. □

Definition 5.12. *Let A be a domain and B a subring of A. We say that A is **integrally closed in** B if $C_B(A) = A$. We say that A is **integrally closed**, if it is integrally closed in its own field of fractions.*

Remark 5.13. Let A be an UFD. Then A is integrally closed.

Proof. Let k be the field of fractions of A. If $x \in C_k(A)$, then x is a root of a monic polynomial f with coefficients from A. If $x = \frac{a}{b}$ with $\gcd(a, b) = 1$, $a, b \in A$, then a is a divisor of the least, and b of the highest coefficient of f, so that, in particular, $b = \pm 1$ and $x = \pm a \in A$. □

Lemma 5.14. *Let k be a subfield of a commutative ring with identity A and let $L = k[x_1, ..., x_n]$ be a subring of A generated by the elements $x_1, ..., x_n \in A$ over k. If L is a field, then L is a finite extension of k.*

Proof. We shall proceed by induction on n. For $n = 1$, assume that $K = k[x_1]$ is a field. We may also assume that $x_1 \neq 0$, and thus $\frac{1}{x_1} \in L$. By the definition of L, there exists a polynomial $g \in k[x]$ such that $g(x_1) = \frac{1}{x_1}$. Therefore $x_1 g(x_1) - 1 = 0$ which means that the element x_1 is algebraic over k. Thus $L = k[x_1]$ is a finite extension of k.

For $n > 1$ assume that $L = k[x_1, ..., x_n]$ is a field. Thus L contains the subfield $k(x_1)$ and hence

$$L = k(x_1)[x_2, ..., x_n].$$

By the inductive hypothesis the elements $x_2, ..., x_n$ are algebraic over $k(x_1)$ and it suffices to show that x_1 is algebraic over k.

Suppose then that x_1 is transcendental over k. The field $k(x_1)$ is the field of fractions of the ring $k[x_1]$. Since $x_2, ..., x_n$ are algebraic over $k(x_1)$, there exist polynomials $a_2(x_1), ..., a_n(x_1) \in k[x_1]$ such that the elements $a_2(x_1)x_2$, ..., $a_n(x_1)x_n$ are integral over $k[x_1]$. This follows from the following elementary claim: if x_i is a zero of a nonzero polynomial

$$f = c_0 + c_1 x + ... + c_{m-1} x^{m-1} + a_i x^m$$

with coefficients from the ring $k[x_1]$, then $a_i x_i$ is a zero of the polynomial

$$c_0 a_i^{m-1} + c_1 a_i^{m-2} x + ... + c_{m-1} x^{m-1} + x^m.$$

Clearly all elements of $k[x_1]$ are integral over $k[x_1]$, so, by Proposition 5.11 the elements $a_2(x_1)a_3(x_1)\cdot\ldots\cdot a_n(x_1)x_i$, $i\in\{2,\ldots,n\}$, are integral over $k[x_1]$. Let $a(x_1)=a_2(x_1)a_3(x_1)\cdot\ldots\cdot a_n(x_1)$. Thus for every $f(x_1,\ldots,x_n)\in k[x_1,\ldots,x_n]$ there exists a sufficiently large $s\in\mathbb{N}$ such that

$$a(x_1)^s f(x_1,\ldots,x_n)=g(x_1,a(x_1)x_2,\ldots,a(x_1)x_n),$$

for some polynomial $g\in k[x_1,\ldots,x_n]$. In particular, for every element $\alpha\in k(x_1)$, there exists $s\in\mathbb{N}$ such that $a(x_1)^s\alpha$ is integral over $k[x_1]$. But $k[x_1]$ is a PID, hence an UFD, and thus is integrally closed. Therefore $a(x_1)^s\alpha\in k[x_1]$. This is obviously false, as it means that every rational function $\alpha\in k(x_1)$ is of the form

$$\alpha=\frac{h(x_1)}{a(x_1)^s},$$

for some $s\in\mathbb{N}$ and $h(x_1)\in k[x_1]$ ($\frac{1}{1+a(x_1)}$ is clearly not of that form). This contradiction show that x_1 is, in fact, algebraic. □

Lemma 5.15. *Let k be algebraically closed, let $\mathfrak{a}\lhd k[x_1,\ldots,x_n]$ be a proper ideal. Then $\mathcal{Z}(\mathfrak{a})\neq\emptyset$.*

Proof. Let $(1)\neq\mathfrak{a}\lhd k[x_1,\ldots,x_n]$. Let $\mathfrak{m}$ be a maximal ideal that contains $\mathfrak{a}$. Since $\mathfrak{a}\subseteq\mathfrak{m}$, it follows that $\mathcal{Z}(\mathfrak{a})\supseteq\mathcal{Z}(\mathfrak{m})$, so that it suffices to show that $\mathcal{Z}(\mathfrak{m})\neq\emptyset$ for every maximal ideal $\mathfrak{m}$ of $k[x_1,\ldots,x_n]$.

Let $\mathfrak{m}\lhd k[x_1,\ldots,x_n]$ be any maximal ideal. Then $L=k[x_1,\ldots,x_n]/\mathfrak{m}$ is a field. Moreover, L is a homomorphic image of the ring $k[x_1,\ldots,x_n]$ via the canonical epimorphism $\kappa\colon k[x_1,\ldots,x_n]\to k[x_1,\ldots,x_n]/\mathfrak{m}=L$. In particular, $\kappa(k)$ is a subfield of L isomorphic to k – we shall thus identify elements $a\in k$ with their images $a+\mathfrak{m}\in L$.

The generators $x_1,\ldots,x_n$ of the ring $k[x_1,\ldots,x_n]$ are mapped by κ onto the generators $x_1+\mathfrak{m},\ldots,x_n+\mathfrak{m}$ of L. Since L is a field, by Lemma 5.14 L is a finite extension of k. But k is algebraically closed, so that it does not have any proper finite extensions, and thus $k=L$. In particular $x_1+\mathfrak{m},\ldots,x_n+\mathfrak{m}\in k$ and it suffices to show that every $f\in\mathfrak{m}$ vanishes at $(x_1+\mathfrak{m},\ldots,x_n+\mathfrak{m})$. Indeed:

$$f(x_1+\mathfrak{m},\ldots,x_n+\mathfrak{m})=f(\kappa(x_1),\ldots,\kappa(x_n))=\kappa(f(x_1,\ldots,x_n))=f+\mathfrak{m}=\mathfrak{m}.$$ □

Lemma 5.16. *Let k be algebraically closed, let $\mathfrak{a}=\langle f_1,\ldots,f_r\rangle\lhd k[x_1,\ldots,x_n]$. Then $\mathcal{Z}(\mathfrak{a})=\emptyset$ if and only if there exist polynomials $h_1,\ldots,h_r\in k[x_1,\ldots,x_n]$ such that*

$$f_1h_1+\ldots+f_rh_r=1.$$

Proof. If the condition of Lemma 5.16 is satisfied, then $\mathfrak{a}=(1)$ and thus $\mathcal{Z}(\mathfrak{a})=\emptyset$. If it is not satisfied, then $\mathfrak{a}\neq(1)$ and by Lemma 5.15 $\mathcal{Z}(\mathfrak{a})\neq\emptyset$. □

Lemma 5.17. *Let k be algebraically closed, let $\mathfrak{a}\lhd k[x_1,\ldots,x_n]$ and let $f\in\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. Then $f\in\operatorname{rad}(\mathfrak{a})$.*

Proof. The theorem is trivially satisfied when $f=0$. Assume then $f\neq0$ and let $\mathfrak{a}=(f_1,\ldots,f_r)$. Consider the ring of polynomials in $n+1$ variables $k[x_1,\ldots,x_n,z]$ and its elements

$$f_1,\ldots,f_r,1-z\cdot f.$$

Let $g=1-z\cdot f$. The polynomials $f_1,\ldots,f_r,g$ have no common zero in k^{n+1}, as every common zero of $f_1,\ldots,f_r$ in k^{n+1} is also a zero of f and thus g takes there the value 1. By Lemma 5.16 there exist polynomials $g_1,\ldots,g_r,h\in k[x_1,\ldots,x_n,z]$ such that

$$f_1g_1+\ldots+f_rg_r+(1-z\cdot f)h=1.$$

We might as well consider this equality holds in the function field $k(x_1, ..., x_n, z)$ and then substitute $\frac{1}{f}$ for z. This yields

$$f_1\hat{g_1} + ... + f_r\hat{g_r} = 1,$$

where the $\hat{g_i}$'s have denominators equal to powers of f. Multiplying both sides by a sufficiently large power of f we get

$$f_1h_1 + ... + f_rh_r = f^m,$$

for some $h_1, ..., h_r \in k[x_1, ..., x_n]$. □

The Nullstellensatz now follows from Lemma 5.17 and Remark 5.8.