9. *Motivation from algebraic geometry*

Let K be a field and $n \in \mathbb{N}$. We are interested in subsets of the n-dimensional K-vectorspace that are characterized by a system of polynomial equations in n variables with coefficients on K.

To every subset S of the polynomial ring $K[x_1, \ldots, x_n]$ we associate the set of its zeros

$$Z(S) = \{(a_1, \ldots, a_n) \in K^n \mid \forall f \in S \; f(a_1, \ldots, a_n) = 0\}$$

and to every subset A of the n-dimensional K-space the set of polynomials that are zero on A

$$I(A) = \{f \in K[x_1, \ldots, x_n] \mid \forall (a_1, \ldots, a_n) \in A \; f(a_1, \ldots, a_n) = 0\}.$$

We can consider Z as a function whose arguments are subsets of $K[x_1, \ldots, x_n]$ and whose values are subsets of K^n (and vice versa for I), or, without losing any information, we can restrict the arguments of Z and the values of I to ideals of $K[x_1, \ldots, x_n]$. This is so because $I(A)$ is an ideal of $K[x_1, \ldots, x_n]$ for every $A \subseteq K^n$, and $Z(S) = Z((S))$, where (S) is the ideal of $K[x_1, \ldots, x_n]$ generated by S, for every set of polynomials $S \subseteq K[x_1, \ldots, x_n]$. (Exercise: check this.)

Subsets of K^n of the form $A = Z(J)$ for some ideal $J \trianglelefteq K[x_1, \ldots, x_n]$ are called **algebraic** sets.

9.1 Remark. The more obvious properties of I and Z: For all $A, B \subseteq K[x_1, \ldots, x_n]$, and all $C, D \subseteq K^n$

(i) $A \subseteq B \implies Z(A) \supseteq Z(B)$ and $C \subseteq D \implies I(C) \supseteq I(D)$

(ii) $A \subseteq I(Z(A))$ and $C \subseteq Z(I(C))$

(iii) $Z(A) = Z(I(Z(A)))$ and $I(C) = I(Z(I(C)))$

(iv) There is a bijective correspondence between ideals of $K[x_1, \ldots, x_n]$ of the form $J = I(S)$ (for some $S \subseteq K^n$) and subsets of K^n of the form $A = Z(L)$ (for some ideal L of $K[x_1, \ldots, x_n]$) given by the restrictions of I and Z to arguments of this form.

(*i*) and (*ii*) are easy to see. By (*i*) and (*ii*), I and Z constitute a Galois correspondence between subsets of K^n and ideals of $K[x_1, \ldots, x_n]$ (each ordered by set-theoretic inclusion). (*iii*) and (*iv*) then follow from the Galois correspondence.

9.2 Definition. A **Galois Correspondence** between two partially ordered sets $(\mathcal{X}, \leq)$ and $(\mathcal{Y}, \leq)$ consists of functions $f\colon \mathcal{X} \to \mathcal{Y}$ and $g\colon \mathcal{Y} \to \mathcal{X}$ satisfying the following conditions for all $A, B \in \mathcal{X}$ and all $C, D \in \mathcal{Y}$:

(i) $A \leq B \implies f(A) \geq f(B)$ and $C \leq D \implies g(C) \geq g(D)$

(ii) $A \leq f(g(A))$ and $C \leq g(f(C))$

9.3 Remark. The conditions defining a Galois correspondence are symmetric in f and g. To reflect this symmetry and to allow us to express two statements in one, we can write both f and g in prime notation: for $A \in \mathcal{X}$, $A' := f(A)$ and for $A \in \mathcal{Y}$, $A' := g(A)$. Conditions (i) and (ii) become

(i) $A \leq B \implies A' \geq B'$

(ii) $A \leq A''$

Given a Galois correspondence, we call an element A of $\mathcal{X}$ or $\mathcal{Y}$ **closed** with respect to the Galois correspondence, if it satisfies $A'' = A$.

It is easy to see that conditions (i) and (ii) above imply

(iii) $A' = A'''$,

which in turn implies

(iv) The subset of elements A in $\mathcal{X}$ (or $\mathcal{Y}$) satisfying $A = A''$ is exactly the subset of elements of the form B' for some $B \in \mathcal{Y}$ (or $\mathcal{X}$, respectively).

(v) There is a bijective correspondence, given by $A \mapsto A'$ (in either direction) between the set of closed elements in $\mathcal{X}$ and the set of closed elements in $\mathcal{Y}$.

* * * * * * * * *

Like in other situations in mathematics, the nontrivial facts connected with a Galois correspondence between two sets consist of characterizations of the closed elements in either set from a different point of view, independent of the Galois structure.

The following Lemma shows that there is a topology on K^n whose closed sets are exactly the subsets of K^n of the form $Z(J)$ (for some ideal J of $K[x_1, \ldots, x_n]$).

9.4 Lemma.

1) If A, $B \subseteq K^n$ are algebraic sets then so is $A \cup B$. Indeed, for all sets $S, T \subseteq K[x_1, \ldots, x_n]$,

$$Z(S) \cup Z(T) = Z(ST),$$

where $ST = \{st \mid s \in S, t \in T\}$.

2) If A_λ is an algebraic set for all $\lambda \in \Lambda$ (an arbitrary index set) then $\bigcap_{\lambda\in\Lambda} A_\lambda$ is an algebraic set. Indeed,

$$\bigcap_{\lambda\in\Lambda} Z(S_\lambda) = Z(\bigcup_{\lambda\in\Lambda} S_\lambda).$$

3) $\emptyset$ and K^n are algebraic sets: $\emptyset = Z(1) = Z(K[x_1,\ldots,x_n])$ and $K^n = Z(0)$.

Proof. Ad 1) Clearly, $Z(S) \cup Z(T) \subseteq Z(ST)$. For the reverse inclusion, we consider a point $a \in Z(ST)$ that is not in $Z(S)$ and show that it is in $Z(T)$. Fix $s_0 \in S$ with $s_0(a) \neq 0$. For all $t \in T$, $0 = (s_0 \cdot t)(a) = s_0(a)t(a)$, therefore for all $t \in T$ $t(a) = 0$, i.e., $a \in Z(T)$.

Ad 2) $\bigcap_{\lambda\in\Lambda} Z(S_\lambda) = \{a \in K^n \mid \forall\lambda \in \Lambda\, \forall f \in S_\lambda f(a) = 0\} = Z(\bigcup_{\lambda\in\Lambda} S_\lambda)$. $\square$

9.5 Remark.

1) If I and J are ideals of a ring R then IJ is defined as

$$IJ = \{i_1 j_1 + \ldots + i_k j_m \mid m \in \mathbb{N}, i_k \in I, j_k \in J\},$$

which is the ideal generated by $\{ij \mid i \in I, j \in J\}$.

With this definition of IJ, we have, for ideals I, J of $K[x_1,\ldots,x_n]$:

$$Z(I \cap J) = Z(IJ) = Z(I) \cup Z(J).$$

Proof: $\{ij \mid i \in I, j \in J\} \subseteq IJ \subseteq I \cap J$ implies $Z(I\cap J) \subseteq Z(IJ) \subseteq Z(\{ij \mid i \in I, j \in J\})$; $Z(\{ij \mid i \in I, j \in J\}) = Z(I) \cup Z(J)$ holds by lemma 9.4, and $Z(I) \cup Z(J) \subseteq Z(I \cap J)$ for purely logical reasons.

2) If S_λ is a subset of K^n for all $\lambda \in \Lambda$ then

$$I(\bigcup_{\lambda\in\Lambda} S_\lambda) = \bigcap_{\lambda\in\Lambda} I(S_\lambda).$$

In particular, for any set $A \subseteq K^n$,

$$I(A) = \bigcap_{a\in A} I(a).$$

9.6 Definition. Let R be a commutative ring and I an ideal of R. The **radical of** I is defined by

$$\sqrt{I} = \{r \in R \mid \exists n \in \mathbb{N}\ r^n \in I\}.$$

Note that $I \subseteq \sqrt{I}$ for every ideal I and that $\sqrt{I} = R$ if and only if $I = R$. It is easy to see that $\sqrt{Q} = Q$ whenever Q is a prime ideal or, more generally, an intersection of prime ideals. (We shall see in chapter 4 that $\sqrt{I}$ is the intersection of all prime ideals containing I.)

9.7 Theorem (Hilbert's Nullstellensatz). Let K be an algebraically closed field and $f_1, \dots, f_m, g \in K[x_1, \dots, x_n]$ such that $g(a) = 0$ for all $a \in Z(f_1, \dots, f_m)$ then $g \in \sqrt{(f_1, \dots, f_m)}$.

Proof. Will be proved in chapter 3. □

The importance of Hilbert's Nullstellensatz lies in the following corollary.

9.8 Corollary. Let J be an ideal of $K[x_1, \dots, x_n]$, where K is an algebraically closed field. Then

$$I(Z(J)) = \sqrt{J}.$$

Proof. The Nullstellensatz says $I(Z(J)) \subseteq \sqrt{J}$ for finitely generated J, and from Hilbert's basis theorem we know that every ideal of $K[x_1, \dots, x_n]$ is finitely generated. The reverse inclusion is easy; it holds even if K is not algebraically closed: if $g \in \sqrt{J}$ then for some $m \in \mathbb{N}$ $g^m \in J$ and therefore $g^m(a) = g(a) \dots g(a) = 0$ for every $a \in Z(J)$. Since K is an integral domain, $g(a) = 0$ follows. □

9.9 Lemma (maximal ideals). Let K be a field, $a = (a_1, \dots, a_n) \in K^n$, and define $M_{\bar{a}}$ to be the ideal of $K[x_1, \dots, x_n]$ generated by $x_1 - a_1, \dots, x_n - a_n$. Then $M_{\bar{a}} = I(\{a\})$ and $M_{\bar{a}}$ is a maximal ideal of $K[x_1, \dots, x_n]$.

Proof. The substitution homomorphism $\varphi: K[x_1, \dots, x_n] \to K[x_1, \dots, x_n]$ with $\varphi(x_i) = x_i - a_i$ and $\varphi(k) = k$ for $k \in K$ is an automorphism of $K[x_1, \dots, x_n]$. Therefore the residue class ring of $M_{\bar{a}}$ is isomorphic to the residue class ring of $(x_1, \dots, x_n)$, which is K. As K is a field, $M_{\bar{a}}$ is a maximal ideal. Therefore $M_{\bar{a}} \subseteq I(\{a\}) \subset K[x_1, \dots, x_n]$ implies $M_{\bar{a}} = I(\{a\})$. □

With this in mind, $\sqrt{J} = I(Z(J))$ becomes

$$\sqrt{J} = \bigcap_{a \in Z(J)} I(a) = \bigcap_{J \subseteq I(a)} I(a) = \bigcap_{J \subseteq M_{\bar{a}}} M_{\bar{a}},$$

the statement that the radical of every ideal of $K[x_1, \dots, x_n]$ (K algebraically closed) is an intersection of ideals of the form $M_{\bar{a}}$. (Since this also holds for maximal ideals, every maximal ideal is of the form $M_{\bar{a}}$.) Therefore, one way to see the Nullstellensatz is:

9.10 Theorem (Variant of Hilbert's Nullstellensatz). Let K be an algebraically closed field.

(1) ("$K[x_1, \dots, x_n]$ is a Hilbert ring.") In $K[x_1, \dots, x_n]$, the radical of every ideal is an intersection of maximal ideals.

(2) ("Weak Nullstellensatz") Every maximal ideal of $K[x_1, \dots, x_n]$ is of the form $M_{\bar{a}}$, $a \in K^n$.

* * * * * * * * *

9.11 Definition. A subset A of K^n is called **irreducible** if $A \subseteq B \cup C$, where $B, \subseteq K^n C$ are algebraic sets, implies $A \subseteq B$ or $A \subseteq C$.

For an algebraic set A, the above definition is equivalent to: $A = B \cup C$ with B, C algebraic implies $A = B$ or $A = C$.

9.12 Proposition. Let $A \subseteq K^n$. Then A is irreducible iff $I(A)$ is a prime ideal.

Proof. ($\Rightarrow$) Suppose A is irreducible and $JL \subseteq I(A)$ for some $J, L \trianglelefteq K[x_1, \ldots, x_n]$; to show $J \subseteq I(A)$ or $L \subseteq I(A)$.

$$Z(J) \cup Z(L) = Z(JL) \supseteq Z(I(A)) \supseteq A$$

By irreducibility of A we get $A \subseteq Z(J)$ or $A \subseteq Z(L)$, say the former, which implies $I(A) \supseteq I(Z(J)) \supseteq J$.

($\Leftarrow$) Suppose $I(A)$ is prime and $A \subseteq Z(J) \cup Z(L)$; to show $A \subseteq Z(J)$ or $A \subseteq Z(L)$.

$$I(A) \supseteq I(Z(J) \cup Z(L)) = I(Z(J)) \cap I(Z(L)) \supseteq I(Z(J))I(Z(L))$$

$I(A)$ being prime we have $I(Z(J)) \subseteq I(A)$ or $I(Z(L)) \subseteq I(A)$, say the former. Then $A \subseteq Z(I(A)) \subseteq Z(I(Z(J))) = Z(J)$. $\square$

9.13 Corollary. For $I \trianglelefteq K[x_1, \ldots, x_n]$, $Z(I)$ is irreducible iff $\sqrt{I}$ is prime.

The weak Nullstellensatz establishes a bijection between the points of K^n and the maximal ideals of $K[x_1, \ldots, x_n]$ (when K is algebraically closed). Thus the topology on K^n (whose closed sets are the algebraic sets) translates to a topology on $\mathrm{MaxSpec}(K[x_1, \ldots, x_n])$ (the set of maximal ideals of $K[x_1, \ldots, x_n]$). A set S of maximal ideals is closed if and only if there exists an ideal I of $K[x_1, \ldots, x_n]$ such that S is exactly the set of maximal ideals containing I.

This topology can be generalized to the spectrum of an arbitrary commutative ring R.

9.14 Definition. Let R be a commutative ring and $\mathrm{Spec}(R)$ the set of prime ideals of R. For every ideal I of R we define a set of prime ideals $V(I) = \{P \in \mathrm{Spec}(R) \mid I \subseteq P\}$.

Zariski topology on $\mathrm{Spec}(R)$ is defined by the convention: a set S of prime ideals of R is closed if and only if there exists an ideal I of R such that $S = V(I)$.

To show that this is a valid definition of a topology, we have to check:

9.15 Lemma.

1) Finite unions of closed sets are closed. Indeed, $V(I) \cup V(J) = V(IJ)$.
2) Arbitrary intersections of closed sets are closed. Indeed,

$$\bigcap_{\lambda \in \Lambda} V(I_\lambda) = V((\bigcup_{\lambda \in \Lambda} I_\lambda)).$$

3) $\emptyset$ and $\mathrm{Spec}(R)$ are closed: $\emptyset = V(R)$ and $\mathrm{Spec}(R) = V((0))$.

We have a Galois connection between ideals of R on one hand and sets of prime ideals of R on the other hand given by $I \mapsto V(I)$ for $I \trianglelefteq R$ and $S \mapsto \bigcap_{P \in S} P$ for $S \subseteq \mathrm{Spec}(R)$, which gives a bijection between radical ideals of R and Zariski-closed sets of prime ideals.

It is clear that the Zariski-closure of a set S of prime ideals consists of all prime ideals containing $\bigcap_{P \in S} P$.

9.16 Definition. A topological space X is called Noetherian, if it satisfies the descending chain condition on closed sets, i.e., whenever $A_1 \supseteq A_2 \supseteq \dots A_m \supseteq A_{m+1} \supseteq \dots$ with A_i closed for all i, then there exists $N \in \mathbb{N}$ such that for all $i > N$ $A_i = A_N$.

If R is a Noetherian ring then $\mathrm{Spec}(R)$ with Zariski topology is easily seen to be a Noetherian topological space.