1. Introduction

1.1. **From polynomial systems to commutative rings.** Algebraic geometry has many sources, but among them the study of systems of polynomial equations is the most evident one.

Namely, we fix a pair of integers $m, n \geq 1$ and consider m polynomials in n variables

$$P_1(x_1, \dots, x_n), \dots, P_m(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$$

over a commutative unital ring K (such as the field of complex numbers $\mathbb{C}$, the field of rational numbers $\mathbb{Q}$, the ring of rational integers $\mathbb{Z}$, the ring $\mathbb{Z}/N\mathbb{Z}$ of residues modulo N, or any other ring or field you like). Then our objective is to describe "the sets of solutions" of the system of equations (or of congruences modulo N in the case $K = \mathbb{Z}/N\mathbb{Z}$)

$$\text{(P)} \qquad P_1(x_1, \dots, x_n) = \cdots = P_m(x_1, \dots, x_n) = 0,$$

or at least some of their properties.

Example. Consider equation $(x_1^2 + x_2^2)^2 + 4x_1^2 x_2 - x_2^3 = 0$. If you draw the set of solutions on the real plane, you get a trefoil. It should be clear from your picture (or from explicit equations, to be generalized later in Bézout's theorem) that any non-horizontal line passing through and punctured at the origin O has a unique intersection with your curve, with three exceptions being the tangent lines ($x_2 = 0$, $x_2 = \pm 2x_1$) at O to three branches at O. This identifies the solutions (other than O) with the points of the projective line (of lines passing through O) punctured at 3 points (the tangent lines).

Can you solve the following equation of a quadrifoil: $(x_1^2 + x_2^2)^3 - 4x_1^2 x_2^2 = 0$?

Another point of view suggests that the set of *complex* solutions of a polynomial equation in two variables can be visualized as a union of punctured spheres with a finite number of handles. At some point we shall see, how to calculate the number of handles in local terms.

To make precise what "solution" means, we fix an K-algebra L, i.e., a unital ring homomorphism $K \to L$, e.g., $L = K$, and we say that an n-tuple $(b_1, \dots, b_n) \in L^n$ is a *L-solution of the system* (P) if $P_1(b_1, \dots, b_n) = \cdots = P_m(b_1, \dots, b_n) = 0$.

In fact, "the sets of solutions" of the system (P) is a *functor* on the category of K-algebras, cf. Exercise 2.3: any unital homomorphism $L_1 \to L_2$ of K-algebras defines a natural map

$$\{L_1\text{-solutions of the system (P)}\} \to \{L_2\text{-solutions of the system (P)}\}.$$

Exercise 1.1. Define this map.

Even if we are interested in the K-solutions of the system (P), it is often helpful to consider the L-solutions of the system (P) for various K-algebras L.

Examples. 1. We want to know, whether the equation $x^2 + y^2 = n$ for a given integer n has $\mathbb{Z}$-solutions. If $n \equiv -1 \pmod 4$ then the equation does not have $\mathbb{Z}/4\mathbb{Z}$-solutions. If $n < 0$ then the equation does not have $\mathbb{R}$-solutions.

2. When $K = \mathbb{R}$, we can identify the set of $\mathbb{R}$-solutions of the system (P) with the fixed subset of the complex conjugation acting on the set of $\mathbb{C}$-solutions of the system (P).

It is clear that adding to the system (P) an extra equation of type $Q_1 P_1 + \cdots + Q_m P_m = 0$ for some polynomials $Q_1, \dots, Q_m \in K[x_1, \dots, x_n]$ does not affect the set of L-solutions.

Exercise 1.2. Construct a natural bijection

$$\{L\text{-solutions of the system (P)}\} \leftrightarrow \{\text{unital } K\text{-algebra homomorphisms } A \to L\},$$

where the K-algebra A is the quotient of the polynomial algebra $K[x_1, \dots, x_n]$ by the ideal[1] generated by by the polynomials $P_1, \dots, P_m$.

At this point we may forget the initial system (P) and work directly with the K-algebra A.

The following statement, Zorn's lemma, is equivalent to the axiom of choice under the Zermelo–Fraenkel axioms of set theory. We can therefore consider itself as an axiom.

Theorem 1.3 (Zorn's lemma)**.** *Suppose every chain (i.e., totally ordered subset) in a partially ordered set P has an upper bound in P. Then the set P contains at least one maximal element.*

By definition, a set P is *partially ordered* if it is endowed with a binary relation "$\leq$", which is reflexive ($a \leq a$ for any $a \in P$), transitive (for all $a, b, c \in P$ such that $a \leq b$ and $b \leq c$ one has $a \leq c$) and antisymmetric (if $a \leq b$ and $b \leq a$ for some $a, b \in P$ then $a = b$). A subset T of a partially ordered set P is called a *chain* if for any pair of elements $a, b \in T$ either $a \leq b$ or $b \leq a$.

Such a set T *has an upper bound* u in P if $t \leq u$ for all t in T. An element m of P is called a *maximal* element if the set of elements $x \in P$ such that $m \leq x$ consists of the single element m.

Exercise 1.4. Show that (i) any ring $\neq 0$ has a maximal ideal; (ii) a ring $\neq 0$, where the ideal 0 is maximal, is a field.

Exercise 1.5 ("Weak Nullstellensatz")**.** The following conditions on the system (P) are equivalent: (i) for any K-field L (i.e., a homomorphism $K \to L$) the system (P) has no L-solutions; (ii) the ideal generated by $P_1, \dots, P_m$ is $K[x_1, \dots, x_n]$. [Hint. Apply Exercise 1.4 to $K[x_1, \dots, x_n]/(P_1, \dots, P_m)$.]

1.2. **From commutative rings to topological spaces.** Consider the case where the K-algebra L is an *integral domain* (ring in which there are no zero divisors): if $bc = 0$ in L for some $b, c \in L$ then either $b = 0$ or $c = 0$. Then to any unital K-algebra homomorphism $\varphi : A \to L$ we may associate a pair consisting of an ideal $\mathfrak{p} := \ker \varphi$ and an embedding of K-algebras $A/\mathfrak{p} \hookrightarrow L$.

Exercise 1.6. Check that $\mathfrak{p} := \ker \varphi$ is an ideal. Show that this ideal is prime.

Recall, that a *prime* ideal is a proper ideal whose complement is closed under multiplication.

Exercise 1.7. Show that the following conditions on a proper ideal $\mathfrak{p}$ in A are equivalent: (i) $\mathfrak{p}$ is prime, (ii) if $ab \in \mathfrak{p}$ for some $a, b \in A$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, (iii) $A/\mathfrak{p}$ is an integral domain.

Exercise 1.8. Deduce from Exercise 1.7 that the maximal ideals are prime.

Exercise 1.9. A positive integer n is a prime number if and only if the ideal $n\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$.

Exercise 1.10. Show that for any ring homomorphism $f : K \to A$ (sending 1 to 1) the preimage $f^{-1}(\mathfrak{p})$ is prime for any prime ideal $\mathfrak{p} \subset L$.

So far we dealt with algebra, but now we turn slowly to geometry. Namely, we start defining the spectra of commutative rings. By definition, the *spectrum* $\mathrm{Spec}(A)$ of a commutative ring A is a topological space endowed with a *sheaf* of commutative rings.

The underlying set of $\mathrm{Spec}(A)$ is the set of prime ideals of A.

By Exercise 1.10, the topological space of $\mathrm{Spec}(A)$ maps to the underlying topological space of $\mathrm{Spec}(K)$.

We consider the elements of A as *functions* on $\mathrm{Spec}(A)$ taking at a point $\mathfrak{p}$ values in the residue ring $A/\mathfrak{p}$. Namely, a "function" $f \in A$ takes at a point $\mathfrak{p}$ the value $f \pmod{\mathfrak{p}}$. In particular, $f \in A$ "vanishes" at $\mathfrak{p}$ if and only if $f \in \mathfrak{p}$.

[1]Recall, that an *ideal* in a ring A is an additive subgroup in A closed under multiplication by elements of A (i.e., an A-submodule); an *ideal generated by a subset* $S \subset A$ is the minimal ideal containing S.

Exercise 1.11. Show that a "function" $f \in A$ vanishes everywhere on $\mathrm{Spec}(A)$ if and only if it is nilpotent, i.e., $f^r = 0$ for an integer $r \geq 1$. In particular, the nilpotents in A form an ideal.

[Hint. Apply Zorn's lemma to the (partially ordered) set of ideals in A containing no element of type f^r for an integer $r \geq 1$.]

To see the relation of these functions to the functions you are used to, assume that K is a field and consider those points $\mathfrak{p}$ of $\mathrm{Spec}(A)$ that the composition $K \hookrightarrow A \to A/\mathfrak{p}$ is an isomorphism. Then the residue rings of such points are naturally identified with K, so the "functions" $f \in A$ can be considered as usual functions with values in K.

We wish to consider the elements of A as *continuous* functions on $\mathrm{Spec}(A)$. Then the minimal possible choice for the topology on $\mathrm{Spec}(A)$, called the *Zariski topology*, is to postulate that the closed subsets are 'zero loci' of subsets (equivalently, of ideals) $S \subset A$, i.e.,

DEFINITION. A subset in $\mathrm{Spec}(A)$ is closed iff it is of type $\{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq S\}$ for some $S \subset A$.

Exercise 1.12. Show that any ring homomorphism induces a continuous map of spectra.

Exercise 1.13. (1) Describe $\mathrm{Spec}(A)$ for the following rings A: $\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}_{(2)}$ (the ring of 2-integer rational numbers, i.e., with odd denominators), $\mathbb{C}[x]$, $k[x]/(x^2)$ for a field k.

(2) Show that for such rings A any non-zero function on $\mathrm{Spec}(A)$ vanishes at a finite number of points. Is this true for other rings?

Exercise 1.14. Show that the topological spaces of $\mathrm{Spec}(A)$ and of $\mathrm{Spec}(A^{\mathrm{red}})$ coincide. (Here $A^{\mathrm{red}} := A/\{\text{nilpotents}\}$.)

1.3. **Localization.** Let A be a unital commutative ring and $S \subset A \smallsetminus \{0\}$ be a multiplicatively closed subset containing 1, i.e., if $s, s' \in S$ then $ss' \in S$. Let M be an A-*module*, i.e., M is an abelian group endowed with an associative distributive multiplication of A: $A \times M \to M$, $(a, m) \mapsto am$, such that $1m = m$, $a(a'm) = (aa')m$, $(a + a')m = am + a'm$, $a(m + m') = am + am'$.

Exercise 1.15.
(1) Consider the following category $\mathcal{C}_{M,S}$: its objects are morphisms of A-modules $M \to N$ such that the multiplication by elements of S on N is invertible; the morphisms are morphisms of A-modules. Show that this category admits an initial object, denoted by $S^{-1}M$. Namely, $S^{-1}M$ can be described as equivalence classes of "fractions" m/s for all $m \in M$ and $s \in S$, where $m/s \sim m'/s'$ if $(ms' - m's)s'' = 0$ for some $s'' \in S$. Show that $\ker[M \to S^{-1}M] = \bigcup_{s \in S} \ker(s|_M)$.
(2) Consider the following category: its objects are morphisms of A-algebras $A \to B$ such that the images of elements S are invertible in B; the morphisms are morphisms of A-algebras. Show that (i) this category admits a forgetful functor to the category $\mathcal{C}_{A,S}$, (ii) this category admits an initial object ($\neq 0$), (iii) the forgetful functor to $\mathcal{C}_{A,S}$ respects the initial objects.

Exercise 1.16. Let A be a commutative ring.
(1) Describe the closed points of $\mathrm{Spec}(A)$.
(2) Show that for any element $f \in A$ the localization homomorphism $A \to A[1/f] := S^{-1}A$ identifies $\mathrm{Spec}(A[1/f])$ with an open subset of $\mathrm{Spec}(A)$, where $S = \{1, f, f^2, f^3 \ldots\}$.
(3) Let $\{f_i\}_{i \in I}$ be a collection of elements of the ring A. Show that the open sets $\mathrm{Spec}(A[1/f_i])$ cover $\mathrm{Spec}(A)$ if and only if the elements f_i generate the unit ideal. Deduce that the topological space of $\mathrm{Spec}(A)$ is quasicompact.
(4) Show that the following conditions are equivalent: (i) A^{red} is an integral domain, (ii) $\mathrm{Spec}(A)$ is (topological) closure of a (unique) point, (iii) any non-empty open subset is dense in $\mathrm{Spec}(A)$, i.e., intersection of any pair of non-empty open subsets is non-empty.

1.4. **Presheaves and sheaves.** Definition. 1. A *presheaf* (of sets) on a topological space X is a contravariant functor $\mathcal{F}$ on the category of open subsets of X, cf. footnote 2 in §2, (to the category of sets). The elements of $\mathcal{F}(U)$ are called *sections* of $\mathcal{F}$ over U.

2. A presheaf $\mathcal{F}$ is called a *sheaf* if its sections are determined locally, i.e., for any open U, any covering $U = \bigcup_i U_i$ and any compatible system of sections $s_i \in \mathcal{F}(U_i)$: $s_i|_{U_i \cap U_j} = s_j|_{U_i \cap U_j}$ for all i there exists a unique section $s \in \mathcal{F}(U)$ such that $s|_{U_i} = s_i$.

2. Categories

By definition, a *category* $\mathcal{C}$ consists of *objects* and *morphisms* (or arrows) between objects. The objects form a class, denoted by $\mathrm{Ob}(\mathcal{C})$. For each pair $A, B \in \mathrm{Ob}(\mathcal{C})$ the morphisms from A to B form a set, denoted by $\mathrm{Hom}_{\mathcal{C}}(A, B)$ (and sometimes by $\mathcal{C}(A, B)$). For each object $A \in \mathrm{Ob}(\mathcal{C})$ a morphism, calles the identity, $id_A \in \mathcal{C}(A, A)$ is fixed. (In particular, the set of endomorphisms $\mathcal{C}(A, A)$ is not empty.) For each triple $A, B, C \in \mathrm{Ob}(\mathcal{C})$ the map of sets, called the *composition*, $\mathrm{Hom}_{\mathcal{C}}(B, C) \times \mathrm{Hom}_{\mathcal{C}}(A, B) \stackrel{\circ}{\longrightarrow} \mathrm{Hom}_{\mathcal{C}}(A, C)$ is fixed. The composition should be associative and compatible with the identity morphisms, i.e., the diagram

$$\begin{array}{ccc} \mathcal{C}(C,D) \times \mathcal{C}(B,C) \times \mathcal{C}(A,B) & \stackrel{id \times \circ}{\longrightarrow} & \mathcal{C}(C,D) \times \mathcal{C}(A,C) \\ \downarrow \circ \times id & & \downarrow \circ \\ \mathcal{C}(B,D) \times \mathcal{C}(A,B) & \stackrel{\circ}{\longrightarrow} & \mathcal{C}(A,D) \end{array}$$

is commutative for any quadruple $A, B, C, D \in \mathrm{Ob}(\mathcal{C})$ and $\varphi \circ id_A = id_B \circ \varphi = \varphi \in \mathcal{C}(A, B)$ for any $\varphi \in \mathcal{C}(A, B)$. A morphism $\varphi \in \mathcal{C}(A, B)$ is called *isomorphism* if there exists $\psi \in \mathcal{C}(B, A)$ such that $\psi \circ \varphi = id_A$ and $\varphi \circ \psi = id_B$.

You have already met (or heard about) many categories: of sets, of topological spaces, of groups, of rings (satisfying some extra conditions, like associativity and/or commutativity, etc.), of modules over a ring (e.g., abelian groups are $\mathbb{Z}$-modules; vector spaces over a field k are k-modules), of certain subsets of a given set (e.g., of open subsets of a topological space; such categories correspond to partially ordered sets).[2]

Also, given a category $\mathcal{C}$ one can construct new categories, e.g., the *opposite* category $\mathcal{C}^{\mathrm{op}}$: $\mathrm{Ob}(\mathcal{C}^{\mathrm{op}}) := \mathrm{Ob}(\mathcal{C})$, $\mathcal{C}^{\mathrm{op}}(X, X') := \mathcal{C}^{\mathrm{op}}(X', X)$ and the composition is defined in an evident way.

Each object X of $\mathcal{C}$ gives rise to the category $\mathcal{C}_X$ of objects over X: its objects are morphisms $Y \stackrel{\varphi}{\longrightarrow} X$ in $\mathcal{C}$ and $\mathcal{C}_X(Y \stackrel{\varphi}{\longrightarrow} X, Y' \stackrel{\varphi'}{\longrightarrow} X)$ consists of morphisms $\psi \in \mathcal{C}_X(Y, Y')$ such that $\varphi = \varphi' \circ \psi$.

An object A is called *initial* (resp., *final*) if any object admits a unique morphism from (resp., to) A.

Exercise 2.1. For each of the above categories find initial and final objects, whenever possible.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be categories. A (covariant) *functor* $\mathcal{F} : \mathcal{C}_1 \to \mathcal{C}_2$ associates an object $\mathcal{F}(X)$ of $\mathcal{C}_2$ to each object X of $\mathcal{C}_1$ and a morphism $\mathcal{F}(\varphi) : \mathcal{F}(X) \to \mathcal{F}(X')$ in $\mathcal{C}_2$ to each morphism $\varphi : X \to X'$ in $\mathcal{C}_1$. We require that $\mathcal{F}$ respects the identity morphisms and the compositions: $\mathcal{F}(id_X) = id_{\mathcal{F}(X)}$ and $\mathcal{F}(\varphi') \circ \mathcal{F}(\varphi) = \mathcal{F}(\varphi' \circ \varphi)$ for any pair of composable morphisms φ, φ' in $\mathcal{C}_1$. A *contravariant functor* from $\mathcal{C}_1$ to $\mathcal{C}_2$ is a covariant functor from the opposite category $\mathcal{C}_1^{\mathrm{op}}$ to $\mathcal{C}_2$.

Exercise 2.2. Show that any functor preserves isomorphisms.

[2] This is an example of a partially ordered set. Conversely, to any partially ordered set $(P, \leq)$ one associates the following set, indexed by the elements $\alpha \in P$, of the subsets of P: $S_\alpha := \{x \in P \mid x \leq \alpha\}$, so $\alpha \leq \alpha'$ iff $S_\alpha \subseteq S_{\alpha'}$. The *category of a partially ordered set* is described as follows: its objects are elements of P and $\mathrm{Hom}(\alpha, \beta)$ consists of a single element if $\alpha \leq \beta$ and it is empty otherwise.

Exercise 2.3 (Representable functors)**.** Let $\mathcal{C}$ be a category and X be an object of $\mathcal{C}$. Show that correspondence $Y \mapsto \mathcal{C}(X, Y)$ gives rise to a functor from $\mathcal{C}$ to the category of sets.

Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be categories and $\mathcal{F}_1, \mathcal{F}_2 : \mathcal{C}_1 \to \mathcal{C}_2$ be a pair of functors. A *natural transformation* between the functors $\mathcal{F}_1$ and $\mathcal{F}_2$ is the collections of morphisms $\psi_X \in \mathcal{C}_2(\mathcal{F}_1(X), \mathcal{F}_2(X))$, one for each object $X \in \mathcal{C}_1$, commuting with the morphisms in $\mathcal{C}_1$, i.e., the following diagram commutes

$$\begin{array}{ccc} \mathcal{F}_1(X) & \xrightarrow{\psi_X} & \mathcal{F}_2(X) \\ \downarrow \mathcal{F}_1(\varphi) & & \downarrow \mathcal{F}_2(\varphi) \\ \mathcal{F}_1(X') & \xrightarrow{\psi_{X'}} & \mathcal{F}_2(X') \end{array} \quad \text{for any morphism } \varphi : X \to X'.$$

Exercise 2.4. Let $\mathcal{C}$ be a *small* category, i.e., its objects form a set. Let $\mathcal{C}'$ be another category. Check that the functors from $\mathcal{C}$ to $\mathcal{C}'$, with the natural transformations as morphisms, form a category.