CIMPA school on Arithmetic, coding and cryptography
National Higher School of Mathematics Sidi Abdellah (Algiers), Algeria, April 5-16, 2026
Problem set on basic algebraic geometry (Elliptic curves' course)

In this set of exercise we use the following notations:

- If $X \subset \mathbb{A}_K^n$ then $I_X = \{f \in K[x_1, \ldots, x_n]$ such that $f(P) = 0$ for all $P \in X\}$.
- If $S \subset K[x_1, \ldots, x_n]$ then $V_S(K) = \{P \in A_K^n$ such that $f(P) = 0$ for all $f \in S\}$.
- If $f \in K[x_1, \ldots, x_n]$ we set $V_f = V_{(f)}$.

Exercise 1. Let I and J be ideals in $K[x_1, \ldots, x_n]$ and $X \subset \mathbb{A}_K^n$. Prove the following:

a) If I_S is the ideal generated by S in $K[x_1, \ldots, x_n]$, then $V_S(K) = V_{I_S}(K)$.
b) Let $\{I_\alpha\}_{\alpha \in A}$ be any collection of ideals. Set $\overline{I} = \cup_{\alpha \in A} I_\alpha$ Then $V_{\overline{I}}(K) = \cap_{\alpha \in A} V_{I_\alpha}(K)$
c) If $I \subseteq J$, then $V_I(K) \supseteq V_J(K)$.
d) $V_I(K) \cup V_J(K) = V_{IJ}(K)$. In particular $V_{fg}(K) = V_f(K) \cup V_g(K)$, for all $f, g \in K[x_1, \ldots, x_n]$
e) $V_{(0)}(K) = \mathbb{A}^n(K)$ and $V_{(1)}(K) = \emptyset$
f) Given $P = (a_1, \ldots, a_n) \in \mathbb{A}^n K$, let $\mathfrak{m}_P = (x_1 - a_1, \ldots, x_n - a_n) \subset K[x_1, \ldots, x_n]$.
Then $V_{\mathfrak{m}_P}(K) = (a_1, \ldots, a_n)$

Exercise 2. Let $X, Y \subset \mathbb{A}_K^n$ and $S \subset K[x_1, \ldots, x_n]$. Prove the following:

a) If $X \subseteq Y$, then $I_X \supseteq I_Y$.
b) $I_{V_S(K)} \supseteq S$, provide an example of a S for which the inclusion is strict.
c) $V_{I_X}(K) \supseteq X$, provide an example of a X for which the inclusion is strict.
d) If $X = V_T(K)$, for some $T \subset K[x_1, \ldots, x_n]$, then $V_{I_X}(K) = X$.

Exercise 3. Prove the following:

a) If $X = \{(a_1, \ldots a_n)\}$, then $I_X = (x - a_1, \ldots, x - a_n)$
b) If K is infinite, then $I_{A^n(K)} = (0)$.
c) If K is a finite field then $I_{A^n(K)} \neq (0)$.
d) If K is a finite field, then every subset of $\mathbb{A}^n(K)$ is the set of k-rational points of an affine set defined over K.
e) The only affine set of $\mathbb{A}^1(K)$ are finite sets.
f) If $X \subseteq \mathbb{A}_{\overline{K}}^n$ is an affine subset then I_X is a radical ideal of I.

Exercise 4. (Irreducible components of a topological space) Let X be a non empty a topological space. We say that X is *irreducible* if it is not the union of two proper closed subset, and reducible otherwise. A subspace of X is irreducible if it is irreducible with respect to the induced (or subspace) topology.

a) Prove that if X is a non empty topological space, then the set of irreducible subspaces of X admits maximal elements for the inclusion relation and X is the union of this maximal elements. (Hint: use Zorn's Lemma: *Let $\mathcal{P}$ be, a non empty, partially ordered set such that every chain in $\mathcal{P}$ has an upper bound in $\mathcal{P}$, Then $\mathcal{P}$ has at least one maximal element.*) The maximal elements of the set of irreducible subspaces of X are called the irreducible components of X.
b) Prove that if X is irreducible then any open, non empty, subset of X is dense
c) Let U be an open subset of X, then the irreducible components of U are $X_i \cap U$ where the X_i are the irreducible components of X that intersect U. (Hint: prove first the an irreducible component of U has to be contained in an irreducible component of X then use b) to conclude.
d) Prove that If X is the union of finitely many irreducible subspace $Z_1, \ldots, Z_m$, then every irreducible components of X coincide with one of the Z_j. If, in addition, the $Z_j \not\subset Z_i$ for all $i \neq j$, then $Z_1, \ldots, Z_m$ are the irreducible components of X.

Exercise 5. Let K be a field.

a) Prove that if K is finite, then the only irreducible affine subset of $\mathbb{A}_K^n$ are the those consisting of one point.
b) Prove that if K is infinite, then $\mathbb{A}_K^n$ is irreducible.
c) Consider the polynomial $f = x^2 y - y^3 + y^2 - x^2 + x + y$ belonging to $\mathbb{R}[x, y]$. Find the irreducible components of $V_f(\mathbb{R})$.

Exercise 6. Let R be a Noetherian ring. Let $\mathcal{S}$ be a non empty collection of ideals in R. Prove that $\mathcal{S}$ admits a maximal element.

Exercise 7. Let $\{V_\alpha\}$ be a collection of affine varieties. Prove that $\{V_\alpha\}$ admits a minimal element. (Hint: $K[x_1, \dots x_n]$ is a Noetherian ring.

Exercise 8. Let X be affine subset of $\mathbb{A}^n(K)$. Prove that there exist $X_1, \dots, X_m$ irreducible affine set such that:

$$X = X_1 \cup X_2 \cup \dots \cup X_m \qquad \text{and} \qquad X_i \not\subset X_j \text{ for all } i \neq j.$$

Moreover the X_i's are uniquely determined up to permutations.

Exercise 9. Irreducible affine varieties of $\mathbb{A}^2_K$, where K is a infinite field.

a) Let f and g be polynomials in $K[x, y]$ and assume that f and g have no common factor. Prove that there exist $d \in K[x]$, and $a, b \in K[x, y]$, such thath $af + bg = d$. (Hint: use the fact that $K[x, y] = K[x][y]$ and Gauss' lemma.)

b) Prove that if f and g are polynomials in $K[x, y]$ with no common factor, then $V_{(f,g)}(K) = V_f(K) \cap V_g(K)$ consist of finitely many points. (Hint: use a))

c) Prove that the only irreducible affine varieties in $\mathbb{A}^2_K$ are: $\mathbb{A}^2_K$, the empty set, points and irreducible affine curves (i.e. $V_f(K)$, with f an irreducible polynomial in $K[x, y]$.