

ALGEBRAIC CURVES EXERCISE SHEET 2

Exercise 2.1.

- (1) Let V be an algebraic set in $\mathbf{A}^n(k)$ and $P \in \mathbf{A}^n(k)$ a point not in V . Show that there is a polynomial $F \in k[X_1, \dots, X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$.
- (2) Let $P_1, \dots, P_r$ be distinct points in $\mathbf{A}^n(k)$, not in an algebraic set V . Show that there are polynomials $F_1, \dots, F_r \in I(V)$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$.
- (3) With $P_1, \dots, P_r$ and V as in (2), and $a_{ij} \in k$ for $1 \leq i, j \leq r$, show that there are $G_i \in I(V)$ with $G_i(P_j) = a_{ij}$ for all i and j .

Solution 1.

- (1) As $P \notin V$, there exists $f \in I(V)$ such that $f(P) = \lambda \neq 0$. k is a field so there exists $\lambda^{-1} \in k$ such that $\lambda^{-1}f(P) = 1$, so we can choose $F := \lambda^{-1}f \in I(V)$.
- (2) Let $1 \leq i \leq r$. Set the ideal

$$I_i := I \cdot \mathfrak{m}_{P_1} \dots \hat{\mathfrak{m}}_{P_i} \dots \mathfrak{m}_{P_r} \subset I$$

where

- $\hat{}$ means that this term is removed
- $\mathfrak{m}_P$ denotes the maximal ideal defining P .

Then $V(I_i)$ is the algebraic set $V \cup \bigcup_{j \neq i} P_j$. We can apply the previous question to $V(I_i)$ and P_i to find $F_i \in I(V(I_i)) \subset I(V(I))$.

- (3) It suffices to combine the F_i 's of the previous question :

$$G_i := \sum_{j=1}^r a_{ij} F_j$$

Exercise 2.2.

- (1) Determine which of the following sets are algebraic:
 - (a) $\{(x, y) \in \mathbf{A}^2(\mathbf{R}) \mid y = \sin(x)\}$
 - (b) $\{(\cos(t), \sin(t)) \in \mathbf{A}^2(\mathbf{R}) \mid t \in \mathbf{R}\}$
 - (c) $\{(z, w) \in \mathbf{A}^2(\mathbf{C}) \mid |z|^2 + |w|^2 = 1\}$
- (2) Show that any algebraic subset of $\mathbf{A}^n(\mathbf{R})$ can be defined by a single polynomial equation. Is the same true for $\mathbf{A}^n(\mathbf{C})$?

Solution 2.

- (1) (a) $V = \{(x, y) \in \mathbf{A}^2(\mathbf{R}) \mid y = \sin(x)\}$ is not algebraic. If it was, $V \cap \{y = 0\}$ would be an algebraic set in $\mathbf{A}^1(\mathbf{R})$ with an infinite number of (isolated) points (given by $x = k\pi, k \in \mathbf{Z}$).
- (b) $\{(\cos(t), \sin(t)) \in \mathbf{A}^2(\mathbf{R}) \mid t \in \mathbf{R}\} = \{(x, y) \in \mathbf{A}^2(\mathbf{C}) \mid x^2 + y^2 = 1\}$ is clearly algebraic.
- (c) $V = \{(z, w) \in \mathbf{A}^2(\mathbf{C}) \mid |z|^2 + |w|^2 = 1\}$ is not algebraic. Indeed $V \cap \{z = 0\} = \{w \in \mathbf{A}^1(\mathbf{C}) \mid |w|^2 = 1\}$ is a proper subset with infinitely many points, so it cannot be algebraic.
- (2) Let V be an algebraic set in $\mathbf{A}^n(\mathbf{R})$. $\mathbf{R}[X_1, \dots, X_r]$ is Noetherian so $V = V(f_1, \dots, f_r)$. Now it is easy to check that $x \in V(f_1) \cap V(f_2)$ if and only if $f_1(x)^2 + f_2(x)^2 = 0$ using that squares are always non-negative in $\mathbf{R}$. Thus, $f_1^2 + \dots + f_r^2 = 0$ is a single equation defining V .

It does not work for $\mathbf{A}^n(\mathbf{C})$ since squares can be negative and cancel each other. More precisely, you can check that $V = \{0\} \in \mathbf{A}^2(\mathbf{C})$ is an algebraic space (defined by $I(V) = (X, Y)$) but is not cut out by a single polynomial equation. (This is true in fact for any algebraically closed field)

Exercise 2.3.

Let k be a field and I, J two ideals of $k[x_1, \dots, x_n]$. Let $a = (a_1, \dots, a_n) \in k^n$. Recall that $I \cdot J = \{fg, f \in I, g \in J\}$. Show the following assertions:

- (1) If $I \subseteq J$, then $V(J) \subseteq V(I)$.
- (2) $V(I) \cup V(J) = V(I \cdot J)$.
- (3) $V(\{x_1 - a_1, \dots, x_n - a_n\}) = \{a\}$.

Solution 3.

- (1) Suppose $x \in V(J)$ then $f(x) = 0 \forall f \in J$. Using $I \subseteq J$, we get $f(x) = 0 \forall f \in I$ Therefore $x \in V(I)$
- (2) Set $I' = \{f \in k[x_1, \dots, x_n] \mid f(x) = 0 \forall x \in V(I) \cup V(J)\}$. Clearly if $f \in IJ \subseteq I \cap J$, $f \in I'$.
If $x \in V(IJ)$, let $f = f_I f_J \in IJ$ with $f_I \in I$ and $f_J \in J$. $f(x) = 0$ so either $f_I = 0$ or $f_J = 0$. Suppose that $f_I \neq 0$, then $\forall g \in J, f_I(x)g(x) = 0$ so $x \in V(J)$. The argument is symmetric so we get that $x \in V(J)$ or $x \in V(I)$.
- (3) Clearly $a \in V(\{x_1 - a_1, \dots, x_n - a_n\})$. Conversely, $x \in V(\{x_1 - a_1, \dots, x_n - a_n\})$ satisfies $x_1 = a_1, \dots$ so $x = a$.

Exercise 2.4.

Let $V \subseteq \mathbb{A}_k^n$ and $W \subseteq \mathbb{A}_k^m$ be algebraic sets. Show that the following set is an algebraic subset of $\mathbb{A}_k^{m+n}$:

$$V \times W = \{(a_1, \dots, a_n, b_1, \dots, b_m) \in \mathbb{A}_k^{m+n} \mid (a_1, \dots, a_n) \in V, (b_1, \dots, b_m) \in W\}$$

Solution 4.

We label the variables such that $I_V \subset k[X_1, \dots, X_n]$ and $I_W \subset k[X_{n+1}, \dots, X_{n+m}]$. Then the following ideal of $k[X_1, \dots, X_{n+m}]$ defines the algebraic set $V \times W$.

$$I_{V \times W} = I_V \times k[X_{n+1}, \dots, X_{n+m}] + k[X_1, \dots, X_n] \times I_W$$

Exercise 2.5.

A ring is called *local* if it has a unique maximal ideal. Let k be an algebraically closed field.

- (1) Let $I \subseteq R = k[x_1, \dots, x_n]$ be an ideal such that $V(I)$ is a point. Show that R/I is a finite-dimensional local algebra and that the elements of the maximal ideal are nilpotent.
- (2) Let $I \subseteq R = k[x_1, \dots, x_n]$ be a *radical* ideal such that $V(I)$ is a finite set of r points. Show that $R/I \simeq k \times \dots \times k$, with r copies of k in the product. (Hint: consider the intersection of maximal ideals containing I and use the chinese remainder theorem).

Solution 5.

- (1)
 - R/I local : by Nullstellensatz, points in $V(I)$ are in one-to-one correspondence with maximal ideals in R/I .
 - Let $\mathfrak{n}$ be a maximal ideal of R/I . The elements of $\mathfrak{n}$ are nilpotent. Indeed, $\sqrt{I} = \mathfrak{m}$ is a maximal ideal in R . Then, for all $f \in \mathfrak{m}$, there is $n \in \mathbb{N}$, $f^n \in I$. We can conclude using the quotient map $\pi : R \rightarrow R/I$ and $\mathfrak{n} = \pi(\mathfrak{m})$.
 - R/I is a finite dimensional algebra. You can check that there is $N \in \mathbb{N}$ such that $\mathfrak{m}^N \subseteq I$. Now $R/\mathfrak{m}^N \twoheadrightarrow R/I$ and $R/\mathfrak{m}^N$ is finite dimensional as a k -vector space. Indeed, one can always choose r linear generators $f_1, \dots, f_r$ for $\mathfrak{m}$ (of the form $x_i - a_i$). Then a basis is given by

$$\left\{ \prod_{i_1, \dots, i_n} f_{i_1} \dots f_{i_n} \mid n < N \right\}$$

where the empty product is 1.

An example to have in mind is the following : $R = k[x, y]$, $I = (x, y^2)$. $V(I) = (0, 0) \in \mathbb{A}_k^2$.

In this case, $\mathfrak{m} = (x, y)$, $\mathfrak{m}^2 = (x^2, xy, y^2)$ and $\mathfrak{m} \supset I \supset \mathfrak{m}^2$.

As a k -vector space, $R/\mathfrak{m}^2 \simeq k \cdot 1 \oplus k \cdot x \oplus k \cdot y$.

$R/I \simeq k \cdot 1 \oplus k \cdot y$.

- (2) If $V(I)$ is a point $(a_1, \dots, a_n)$ and I radical, then $I = \mathfrak{m}_a = (x_1 - a_1, \dots, x_n - a_n)$ maximal. Using exercise 2.3, (2), we get that if $V(I)$ is a finite set of points $\{y_1, \dots, y_k\}$ with I radical, I is the intersection of the corresponding maximal ideals. They are always pairwise coprime, so we can use the chinese remainder theorem to get the desired isomorphism, knowing that for all $\mathfrak{m}_{y_i}$ there are isomorphism $R/\mathfrak{m}_{y_i} \simeq k$.

Exercise 2.6.

Let k be an algebraically closed field and $V = \{p_1, \dots, p_r\} \subseteq \mathbb{A}_k^n$ a finite algebraic set. We call a_i , $1 \leq i \leq s$ the distinct first coordinates of $p_1, \dots, p_r$. Consider the finite varieties $V_i = \{(x_2, \dots, x_n) \in \mathbb{A}^{n-1} \mid (a_i, x_2, \dots, x_n) \in V\} \subseteq \mathbb{A}^{n-1}$.

- (1) Assume that each V_i is the zero locus of N polynomials $f_{i,1}, \dots, f_{i,N}$ for some $N \geq 1$. Show that there exist polynomials g_k , $1 \leq k \leq N$ such that $g_k(a_i, x_2, \dots, x_n) = f_{i,k}$.
- (2) Show that V is the zero locus of n polynomials in $k[x_1, \dots, x_n]$. (Hint: reason by induction on n)
- (3) Show that $I(V)$ is generated by n polynomials. (Hint: using the previous exercise, $I(V)$ is characterized by $k[x_1, \dots, x_n]/I(V) \simeq k \times \dots \times k$)

Solution 6. Note that i ranges from 1 to $s \leq r$, because we consider only the **distinct** first coordinates of our set of r points.

- (1) It suffices to set

$$g_k(x_1, \dots, x_n) := \sum_{i=1}^s f_{i,k}(x_2, \dots, x_n) \frac{\prod_{j \neq i}(x_1 - a_j)}{\prod_{j \neq i}(a_i - a_j)}.$$

- (2) We use induction. For the base case, $V = \{p_1, \dots, p_r\} \subseteq \mathbb{A}_k^1$ so V is the zero locus of $f_1 = \prod_{i=1}^r (x - p_i)$.

Induction step : suppose each V_i is the zero locus of $n - 1$ polynomials. We can consider the set of $\{g_1, \dots, g_{n-1}\}$ of question (1) together with

$$g_n := \prod_{i=1}^s (x_1 - a_i).$$

We can check that V is the zero set of $\{g_1, \dots, g_n\}$.

- (3) $A = k[x_1, \dots, x_n]$ is of transcendence degree n over k and $A/I(V) \simeq k \times \dots \times k$ has transcendence degree 0 over k . One can verify for any $f \in A$, $A/(f)$ is of transcendence degree at least $n - 1$ (it is an equality if f is non constant). By induction on transcendence degree, we get that we need at least n generators. But we showed in (1) and (2) that we can always find n polynomial such that V is their zero set. Thus, $I(V)$ is generated by exactly n polynomials.