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 $F \in k[X_1, ..., X_n]$ such that $F(Q) = 0$ for all $Q \in V$, but $F(P) = 1$.
(2) Let $P_1, ..., P_r$ be distinct points in $\mathbf{A}^n(k)$, not in an algebraic set V. Show that there are polynomials $F_1, ..., F_r \in I(V)$ such that $F_i(P_j) = 0$ if $i \neq j$, and $F_i(P_i) = 1$.
(3) With $P_1, ..., P_r$ 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) For every $1 \leq i \leq r$, let V_i be the algebraic set

$$V_i = V \cup \{P_1, \ldots, P_{i-1}, P_{i+1}, \ldots, P_r\}$$

(recall that finite sets and finite unions of algebraic sets are algebraic, see Exercise 2.3). By point (1), there exists $F_i \in I(V_i)$ such that $F_i(P_i) = 1$. In particular, we have $F_i \in I(V)$ and $F_i(P_j) = 0$ for all $j \neq i$.
(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) $\{(cos(t), sin(t)) \in \mathbf{A}^2(\mathbf{R}) \mid t \in \mathbf{R}\} = \{(x,y) \in \mathbf{A}^2(\mathbf{R}) \mid x^2 + y^2 = 1\}$ 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 $\mathbf{A}^n(\mathbf{R})$. $\mathbf{R}[X_1, \ldots X_r]$ is Noetherian so $V = V(f_1, \ldots, f_r)$ ofr some $f_1, \ldots, f_r \in \mathbf{R}[X_1, \ldots X_r]$. 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, $f_1^2 + \cdots + f_r^2 = 0$ 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 $k[x_1, \ldots, x_n]$. Let $a = (a_1, \ldots, a_n) \in k^n$. 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) $V(\{x_1 - a_1, \ldots, x_n - a_n\}) = \{a\}$.

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 $I' = \{f \in k[x_1, \ldots, x_n] \mid f(x) = 0\ \forall x \in V(I) \cup V(J)\}$. Clearly if $f \in IJ \subseteq I \cap J$, it follows that $f \in I'$.

Conversely, 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 $a \in V(\{x_1 - a_1, \ldots, x_n - a_n\})$. Conversely, $x \in V(\{x_1 - a_1, \ldots, x_n - a_n\})$ satisfies $x_i = a_i$ for all i, so $x = a$.

Exercise 2.4.

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

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

Solution 4.

We label the variables such that $I_V \subset k[X_1, \ldots, X_n]$ and $I_W \subset k[X_{n+1}, \ldots, X_{n+m}]$. We can view $k[X_1, \ldots, X_n]$ and $k[X_{n+1}, \ldots, X_{n+m}]$ as subrings of $k[X_1, \ldots, X_{n+m}]$, and so we can also consider I_V and I_W as subsets of $k[X_1, \ldots, X_{n+m}]$. Then the following ideal of $k[X_1, \ldots, X_{n+m}]$ defines the algebraic set $V \times W$.

$$I_{V\times W} = I_V \cdot k[X_1, \ldots, X_{n+m}] + I_W \cdot k[X_1, \ldots, X_{n+m}].$$

That is, the ideal generated by (the images of) I_V and I_W inside $k[X_1, \ldots, X_{n+m}]$. Indeed, if $(a, b) \in V \times W$, then for any $f \in I_V$ and $g \in I_W$, viewed as elements of $k[X_1, \ldots, X_{n+m}]$, we have $f(a, b) = 0$ and $g(a, b) = 0$. Therefore, (a, b) is in the vanishing locus of (the ideal generated by) I_V and I_W viewed as subsets of $k[X_1, \ldots, X_{n+m}]$, i.e. $(a, b) \in V(I_{V\times W})$, and thus $V \times W \subseteq V(I_{V\times W})$

On the other hand, suppose that $(a, b) \in V(I_{V\times W})$. Then if $f \in I_V$ and $g \in I_W$ are arbitrary, we have

$$0 = \underset{\substack{\uparrow \\ \boxed{\text{viewed as element of } k[X_1,\ldots,X_{n+m}]}}}{f(a, b)} = \underset{\substack{\uparrow \\ \boxed{\text{viewed as element of } k[X_1,\ldots,X_n]}}}{f(a)}$$

and

$$0 = \underset{\substack{\uparrow \\ \boxed{\text{viewed as element of } k[X_1,\ldots,X_{n+m}]}}}{g(a, b)} = \underset{\substack{\uparrow \\ \boxed{\text{viewed as element of } k[X_{n+1},\ldots,X_{n+m}]}}}{g(b)}.$$

As $f \in I_V$ and $g \in I_W$ were arbitrary, we obtain $a \in V$ and $b \in W$, so that $(a, b) \in V \times W$. Hence we conclude also $V(I_{V\times W}) \subseteq V \times W$, so that in fact $V(I_{V\times W}) = V \times W$.

Exercise 2.5.

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

(1) Let $I \subseteq R = k[x_1, \ldots, x_n]$ 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 $I \subseteq R = k[x_1, \ldots, x_n]$ be a *radical* ideal such that $V(I)$ is a finite set of r points. Show that $R/I \simeq k \times \ldots \times k$, 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 the 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 $n \in \mathbf{N}$, $f^n \in I$. We can conclude using the quotient map $\pi : R \longrightarrow R/I$ and $\mathfrak{n} = \pi(\mathfrak{m})$.
- R/I is a finite dimensional algebra. You can check that there is $N \in \mathbf{N}$ such that $\mathfrak{m}^N \subseteq I$ (using the fact that $\mathfrak{m}$ is finitely generated and the pigeonhole principle). 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 $f_1, \ldots, f_r$ for $\mathfrak{m}$ (of the form $x_i - a_i$). Then a basis is given by

$$\{ \prod_{i_1,\ldots,i_n} f_{i_1} \ldots f_{i_n} \mid n < N\}$$

where the empty product is 1.

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

$$R/\mathfrak{m}^2 \simeq k \cdot 1 \oplus k \cdot x \oplus k \cdot y$$

whereas

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

(2) If $V(I)$ is a point $(a_1, \ldots, a_n)$ and I radical, then $I = \mathfrak{m}_a = (x_1-a_1, \ldots, x_n-a_n)$ maximal. Using Exercise 2.3, part (2), we get that if $V(I)$ is a finite set of points $\{y_1, \ldots, y_k\}$ with I radical, I is the product 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 is an isomorphism $R/\mathfrak{m}_{y_i} \simeq k$.

Exercise 2.6.

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

(1) Assume that each V_i is the zero locus of N polynomials $f_{i,1}, \ldots, f_{i,N}$ for some $N \geq 1$. Show that there exist polynomials g_k, $1 \leq k \leq N$ such that $g_k(a_i, x_2, \ldots, x_n) = f_{i,k}$.

(2) Show that V is the zero locus of n polynomials in $k[x_1, \ldots, x_n]$. (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 $k[x_1, \ldots, x_n]/I(V) \simeq k \times \ldots \times k$)

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

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

(2) We use induction. For the base case, $V = \{p_1, \ldots, p_r\} \subseteq \mathbb{A}^1_k$ 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 $f_{i,n-1}, \ldots, f_{i,n-1}$. We can consider the set of $\{g_1, \ldots, g_{n-1}\}$ 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 $\{g_1, \ldots, g_n\}$.

(3) Let us refine the proof of point (2) to obtain this stronger statement. So as in (2), we proceed by induction on n: if $n = 1$, then $V = \{p_1, \ldots, p_r\} \subseteq \mathbb{A}^1_k$, so $I(V) = (\prod_{i=1}^{r}(x - p_i))$ (the generator has only simple roots, so this is indeed a radical ideal). For the induction step, suppose that for all i we have $I(V_i) = (f_{i,1}, \ldots, f_{i,n-1})$ for some $f_{i,1}, \ldots, f_{i,n-1} \in k[x_2, \ldots, x_n]$. As in (2), we use (1) to produce polynomials $g_1, \ldots, g_{n-1} \in k[x_1, \ldots, x_n]$ with the property that $g_k(a_i, x_2, \ldots, x_n) = f_{i,k}$ for all i, k, and we also pose $g_n = \prod_{i=1}^{s}(x_1 - a_i)$. We now aim to show that $I(V) = (g_1, \ldots, g_n)$. Note that $g_1, \ldots, g_n \in I(V)$, so it remains to prove that $I(V) \subseteq (g_1, \ldots, g_n)$. To do so, let $f \in I(V)$ be arbitrary. Then for any i, we have $f(a_i, x_2, \ldots, x_n) \in I(V_i)$, and thus by induction hypothesis, there exist $r_{i,1}, \ldots, r_{i,n-1} \in k[x_2, \ldots, x_n]$ such that

$$f(a_i, x_2, \ldots, x_n) = \sum_{k=1}^{n-1} r_{i,k} f_{i,k}$$

as polynomials in $k[x_2, \ldots, x_n]$. By point (1), there exist polynomials $s_1, \ldots, s_{n-1} \in k[x_1, \ldots, x_n]$ such that for all i, k we have $s_k(a_i, x_2, \ldots, x_n) = r_{i,k}$. Let us consider the polynomial $h = \sum_{k=1}^{n-1} s_k g_k$. By construction, we have

$$\begin{aligned}h(a_i, x_2, \ldots, x_n) &= \sum_{k=1}^{n-1} s_k(a_i, x_2, \ldots, x_n) g_k(a_i, x_2, \ldots, x_n) \\ &= \sum_{k=1}^{n} r_{k,i} f_{k,i} = f(a_i, x_2, \ldots, x_n).\end{aligned}$$

for all i. Therefore, if we write

$$f = \sum_{I=(i_2,\ldots,i_n)\in\mathbb{Z}_{\geq 0}^{n-1}} F_I \cdot x_2^{i_2} \cdots x_n^{i_n} \qquad \text{and} \qquad h = \sum_{I=(i_2,\ldots,i_n)\in\mathbb{Z}_{\geq 0}^{n-1}} H_I \cdot x_2^{i_2} \cdots x_n^{i_n}$$

for some $F_I, H_I \in k[x_1]$, we obtain that $F_I(a_i) = H_I(a_i)$ for all I and i. Note that the ideal of $\{a_1, \ldots, a_s\} \subseteq \mathbb{A}_k^1$ is given by $I(\{a_1, \ldots, a_s\}) = (g_n) \subseteq k[x_1]$ by the proof for the case $n = 1$. As $F_I - H_I \in I(\{a_1, \ldots, a_s\})$, we obtain that there exists $q_I \in k[x_1]$ such that

$$F_I - H_I = q_I \cdot g_n$$

for all $I \in \mathbb{Z}_{\geq 0}^{n-1}$. Thus, we obtain

$$\begin{aligned}f &= \sum_{I=(i_2,\ldots,i_n)\in\mathbb{Z}_{\geq 0}^{n-1}} F_I \cdot x_2^{i_2} \cdots x_n^{i_n} = \sum_{I=(i_2,\ldots,i_n)\in\mathbb{Z}_{\geq 0}^{n-1}} (H_I + q_I \cdot g_n) \cdot x_2^{i_2} \cdots x_n^{i_n} \\ &= h + \left(\sum_{I=(i_2,\ldots,i_n)\in\mathbb{Z}_{\geq 0}^{n-1}} q_I \cdot x_2^{i_2} \cdots x_n^{i_n} \right) \cdot g_n.\end{aligned}$$

As $h = \sum_{k=1}^{n-1} s_k g_k$ by definition, we obtain $f \in (g_1, \ldots, g_n)$. As $f \in I(V)$ was arbitrary, we conclude that $f \in I(V)$, so the proof is complete.