Math 137 Problem Set 1

Lev Kruglyak

February 1, 2022

Problem 1. Let K be a field and let X be a set of m points in K^n.

(a) Show that there is a set $S \subseteq K[X_1, \ldots, X_n]$ of size at most n^m such that $X = \mathcal{V}(S)$.

(b) Assuming that $K = \mathbb{R}$, show that there is a polynomial $f \in K[X_1, \ldots, X_n]$ such that $X = \mathcal{V}(f)$.

(c) *(bonus)* Assuming that the field K is finite, show that there is a polynomial $f \in K[X_1, \ldots, X_n]$ such that $X = \mathcal{V}(f)$. (Hint: Use Fermat's little theorem / Lagrange's theorem.)

(d) *(bonus)* Assuming that the field K is infinite, show that there is a set $S \subseteq K[X_1, \ldots, X_n]$ of size at most $n + 1$ such that $X = \mathcal{V}(S)$.

Let $X = \{x_1, x_2, \ldots, x_m\}$ be the set of points, with coordinates $x_i = (x_{i1}, x_{i2}, \ldots, x_{in})$.

(a) Recall that $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cdot J)$. Given any point $x_i \in X$, consider the set $S_i = \{X_1 - x_{i1}, X_2 - x_{i2}, \ldots, X_n - x_{in}\}$. Then clearly $\mathcal{V}(S_i) = \{x_i\}$, so letting $S = S_1 \cdot S_2 \cdots S_m$ we have $\mathcal{V}(S) = X$. Since S consists of all products of m elements chosen from sets of n elements, we have $|S| = n^m$.

(b) More generally, let K be any ordered field. We can construct f as

$$f(X_1, \ldots, X_n) = \prod_{i=1}^{m} \left((X_1 - x_{i1})^2 + \cdots + (X_n - x_{in})^2 \right).$$

Because K is an ordered field, each of these factors $(X_1 - x_{i1})^2 + \cdots + (X_n - x_{in})^2$ only vanishes at x_i. Hence when we multiply them all together, we get a polynomial which vanishes at X only.

(c) Let K be a field of order p^k. Then Lagrange's theorem tells us that

$$a^{p^k - 1} = \begin{cases} 0 & \text{if } a = 0 \\ 1 & \text{if } a \neq 0 \end{cases}, \quad a \in K$$

This means that for any point x_j, the term $1 - (X_i - x_{ji})^{p^k - 1}$ will only equal zero if $X_i \neq x_{ji}$, and 1 otherwise. Then the product $\prod_i (1 - (X_i - x_{ji})^{p^k - 1})$ will only be equal to 1 if $X_i = x_{ji}$ for all i. Thus, subtracting this function from 1 gives us the desired function:

$$f_i(X_1, \ldots, X_n) = 1 - \prod_i (1 - (X_i - x_{ji})^{p^k - 1}).$$

Since this vanishes exactly on x_j, we can just take $f = f_1 f_2 \cdots f_m$ and we are done.

(d) To start, add the n polynomials $f_i(X_1, \ldots, X_n) = (X_i - x_{1i})(X_i - x_{2i}) \cdots (X_i - x_{mi})$. This gives us a grid of points consisting of all $X_1, X_2, \ldots, X_n$ combinations between the points. Next, we'll use the property that in any field, $A_1 + A_2 + \cdots + A_m = A_j$ if all the other terms are zero. Constructing this polynomial is becoming quite difficult to describe at this hour of the night, so I will do an example and hope this suffices to convince the reader on the correctness of my construction.

Suppose we had points $(1,1), (1,2), (2,3)$. Then the first n polynomials vanish on the points $(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)$. The last polynomial eliminates the extraneous points, taking the form

$$f(x,y) = (x-1)\left((y-3)(y-1) + (y-3)(y-2)\right) + (x-2)\left((y-1)(y-2)\right).$$

In this manner, by isolating each line and weaving through the points, we can hit every required point on the grid.

Problem 2. Show that $A = \{(t, \sin(t)) \mid t \in \mathbb{R}\}$ is not an algebraic subset of $\mathbb{R}^2$.

Suppose for the sake of contradiction that A is algebraic set. Consider $\mathbb{R}$ as a subspace of $\mathbb{R}^2$, embedded along the line $y = 0$. Then $A \cap \mathbb{R} = \frac{\pi}{2}\mathbb{Z}$ is an algebraic set in $\mathbb{R}$, since the Zariski topology agrees with subspaces. However the only algebraic sets in $\mathbb{R}$ are finite sets of points and $\mathbb{R}$ itself, so we have a contradiction. Hence A is not algebraic.

Problem 3. Consider the *one-sheet hyperboloid*

$$V = \{(x,y,z) \in \mathbb{R}^3 \mid x^2 + y^2 = z^2 + 1\} \subseteq \mathbb{R}^3.$$

Prove that every point $P \in V$ lies on exactly two (straight) lines $l_1, l_2 \subseteq V$.

To prove that there are exactly two lines in V going through a point (x,y,z), suppose

$$\begin{bmatrix} x' \\ y' \\ z' \end{bmatrix} = \begin{bmatrix} x + at \\ y + bt \\ z + ct \end{bmatrix}$$

is some line in V parametrized by t, determined by the slopes $a, b, c \in \mathbb{R}$. Then for every t, we would have

$$\begin{aligned} (x+at)^2 + (y+bt)^2 - (z+ct)^2 - 1 &= 0 \\ (x^2 + y^2 - z^2 - 1) + 2t(ax + by - cz) + t^2(a^2 + b^2 - c^2) &= 0 \\ 2(ax + by - cz) + t(a^2 + b^2 - c^2) &= 0. \quad (t \neq 0) \end{aligned}$$

Since this is true for all nonzero t, we set $t = 1$ and $t = -1$ and add the two equations together to get

$$\begin{cases} a^2 + b^2 = c^2 \\ ax + by = cz. \end{cases}$$

To show that there are two lines on the hyperboloid, it suffices to show that the solution set to this equation consists of two intersecting lines. Note that the transformation $(a,b,c) \to$

$(\lambda a, \lambda b, \lambda c)$ doesn't affect the equation (i.e. it is homogenous), so we can reduce a dimension by performing the variable change $A = \frac{a}{c}$ and $B = \frac{b}{c}$ to get the system

$$\begin{cases} A^2 + B^2 = 1 \\ Ax + By = z. \end{cases}$$

Now to show that there are two lines on the hyperboloid it suffices to show that there are two solutions to this system for all x, y, z satisfying $x^2 + y^2 = z^2 + 1$. Solving for B in the second equation we get

$$B = \frac{z}{y} - \left(\frac{x}{y}\right) A.$$

We can assume without loss of generality that $y \neq 0$, since both x and y can't be zero. Then note that,

$$\left(\frac{z}{y}\right)^2 + \left(\frac{1}{y}\right)^2 = \left(\frac{x}{y}\right)^2 + 1.$$

This justifies the variable transformation $X = \frac{z}{y}$, $Y = \frac{1}{y}$, and $Z = \frac{x}{y}$, so in these coordinates $B = X - ZA$. Substituting this into the first equation, we get

$$(1 - Z^2)A^2 + (-2XZ)A + (X^2 - 1) = 0$$

Using the above identities, the discriminant of this quadratic simplifies to $\Delta = 4Y^2$, which is clearly nonzero, so we have exactly two solutions. So we are done.

Problem 4. For every $n \geq 1$, show that the ideal $I = (X, Y)^n$ of $K[X, Y]$ is not generated by n of its elements.

It is clear that $(X, Y)^n = (X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n)$. Suppose for the sake of contradiction that there were generators $g_1, g_2, \ldots, g_n$. We can assume without loss of generality that all of these generators have smallest degree term greater than or equal to n. Consider the K-vector space spanned by formal symbols $X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n$. Let v be any vector in this space. Then $v \in (X, Y)^n$ so there are some constants $c_1, c_2, \ldots, c_n \in K$ such that $v = c_1 g_1 + \cdots + c_n g_n$. Since v has degree less than or equal to n, we can assume that c_i all must be constant. So $g_1, g_2, \ldots, g_n$ span the vector space, a contradiction because it is $n + 1$ dimensional.

Problem 5. Let K be any field and let A be any subset of K^n. Show that $\mathcal{V}(\mathcal{I}(A))$ is the closure of A with respect to the Zariski topology. (This is called the Zariski closure of A.)

Clearly $A \subset \mathcal{V}(\mathcal{I}(A))$ so $\overline{A} \subset \overline{\mathcal{V}(\mathcal{I}(A))}$, however since $\mathcal{V}(\mathcal{I}(A))$ is closed, it follows that $\overline{A} \subset \mathcal{V}(\mathcal{I}(A))$. To show that this inclusion is an equality, it suffices to show that any closed set $\mathcal{V}(C)$ containing A must also contain $\mathcal{V}(\mathcal{I}(A))$. Since $\mathcal{V}(C)$ contains A, every polynomial $f \in C$ must vanish on all of A, so $f \in \mathcal{I}(A)$ and so $C \subset \mathcal{I}(A)$. Since $\mathcal{V}$ reverses inclusions, $\mathcal{V}(C) \supset \mathcal{V}(\mathcal{I}(A))$ and so we are done.