Math 137 Problem Set 2

Lev Kruglyak

March 29, 2022

I collaborated with AJ LaMotta and Eliot Hodges for this problem set.

Problem 1. Let A be an algebraic subset of K^n and let B be an algebraic subset of K^m. Show that the cartesian product $A \times B$ is an algebraic subset of $K^n \times K^m = K^{n+m}$.

Suppose A satisfies $f_1(x) = \cdots = f_n(x) = 0$ for $x = x_1, x_2, \ldots, x_n$ and B satisfies $g_1(y) = \cdots = g_m(y) = 0$ for $y = y_1, y_2, \ldots, y_m$. Define $\overline{f_i}(x, y) = f_i(x)$ and $\overline{g_i}(x, y) = g_i(y)$. Then clearly,

$$A \times B = \{(x, y) \in K^{n+m} \mid \overline{f_1}(x, y) = \cdots = \overline{f_n}(x, y) = \overline{g_1}(x, y) = \cdots = \overline{g_m}(x, y) = 0\}.$$

Thus $A \times B$ is an algebraic subset of K^{n+m}.

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

Suppose for the sake of contradiction that X were an algebraic set. Then there must be some finite set of nonzero polynomials $f_i \in \mathbb{R}[x, y]$ such that $X = \mathcal{V}(f_1, f_2, \ldots, f_n)$, i.e. $f_i(t, e^t) = 0$ for all $t \in \mathbb{R}$. Pick any of the f_i, say $f_i = f$ and consider the function $f(t, e^t)$ as a polynomial in the formal symbol e^t with coefficients in $\mathbb{R}[t]$, so

$$f(t, e^t) = \sum_{k=0}^{N} g_k(t)(e^t)^k, \quad g_k(t) \in \mathbb{R}[t].$$

We'll now induct on the degree N to show that such a polynomial cannot exist. For the base case of $N = 0$, this means that $f(t, e^t) = g_0(t) = 0$ for all $t \in \mathbb{R}$, a contradiction since a nonzero real valued polynomial cannot vanish on all of $\mathbb{R}$.

Now suppose there cannot exist such a polynomial for all degrees less than N, and that $f(t, e^t)$ is of degree N. If $g_0(t) = 0$, since $e^t \neq 0$, we can factor out e^t from f and be left with a degree $N - 1$ polynomial which still vanishes everywhere, completing the induction step. Otherwise, let $M = \deg g_0(t)$ be the degree of the nonzero constant term of f. Then

$$\begin{aligned} f^{(M+1)}(t, e^t) &= \sum_{k=1}^{N} \left(g_k(t)(e^t)^k \right)^{(M+1)} + g_0^{(M+1)}(t) \\ &= \sum_{k=1}^{N} \sum_{j=0}^{M+1} \binom{M+1}{j} g_k^{(M+1-j)}(t) k^j (e^t)^k \\ &= \sum_{k=1}^{N} h_k(t)(e^t)^k \end{aligned}$$

where $f^{(n)}$ denotes the n-th derivative with respect to t. Observe that $h_k(t)$ are nonzero if $g_k(t)$ was nonzero, and $f^{(M+1)}(t, e^t)$ has no constant term, so we can again factor out e^t to get a polynomial of degree $N-1$ which vanishes on $\mathbb{R}$. This completes the induction.

Problem 3. For each of the following ideals I of $\mathbb{C}[X, Y]$, is $1 \in I$? If so, show how to write 1 as a linear combination of the given generators.

a) $I = (X - Y, X^2 + XY - 2Y^2, X + Y - 2)$

b) $I = (X^2 + Y^2 - 1, X + Y - 1, X - Y)$

(a) Note that $(1, 1)$ is a root of every element of I, so $\mathcal{V}(I) \neq \varnothing$. However if $1 \in I$, then $I = \mathbb{C}[X, Y]$. This is a contradiction since the weak Nullstellensatz implies $\mathcal{V}(\mathbb{C}[X, Y]) = \varnothing$, so $1 \notin I$.

First we'll show that $I = (X - 1, Y - 1)$. Clearly $(X - 1, Y - 1) \subset I$ because $X - 1 = \frac{1}{2}(X - Y) + \frac{1}{2}(X + Y - 2)$. Similarly, $Y - 1 = (X + Y - 2) - (X - 1)$. To prove the converse, note that

$$\begin{aligned} X - Y &= (X - 1) - (Y - 1) \\ X^2 + XY - 2Y^2 &= (X + Y + 1)(X - 1) - (2Y + 1)(Y - 1) \\ X + Y - 2 &= (X - 1) + (Y - 1). \end{aligned}$$

So $I = (X - 1, Y - 1)$. Next we claim that $1 \notin I$. Suppose $a(X, Y)(X - 1) + b(X, Y)(Y - 1) = 1$ for some $a, b \in \mathbb{C}[X, Y]$. Then substituting $X = Y$, we get $(a(X, Y) + b(X, Y))(X - 1) = 1$, however this is impossible because the only way $(a(X, Y) + b(X, Y))(X - 1)$ can have no non constant terms is if $a(X, Y) + b(X, Y) = 0$, which would also violate the equation. So $1 \notin I$.

(b) We claim that $I = \mathbb{C}[X, Y]$. This is very easy to show; consider the linear combination:

$$-2 \cdot (X^2 + Y^2 - 1) + (1 + 2X) \cdot (X + Y - 1) + (1 - 2Y) \cdot (X - Y) = 1.$$

Since $1 \in I$, it follows that $I = \mathbb{C}[X, Y]$.

Problem 4. Let I be an ideal of a polynomial ring $K[X_1, \ldots, X_n]$ over a field K. Let $J = \sqrt{I}$ be its radical. Show that $J^n \subseteq I$ for some $n \geq 1$.

Let I be an ideal in $K[X_1, \ldots, X_n]$. Then $\sqrt{I}$ is an ideal in $K[X_1, \ldots, X_n]$ so it is finitely generated by Hilbert's basis theorem, say $\sqrt{I} = (f_1, \ldots, f_m)$. For each of these generators

$f_i^{e_i} \in I$ for some e_i. So write $\sqrt{I} = (f_1) + \cdots + (f_m)$. Then letting $e = e_1 + \cdots + e_m$,

$$\left(\sqrt{I}\right)^e = ((f_1) + \cdots + (f_m))^e = \sum_{b_1 + \cdots + b_m = e} (f_1^{b_1}) \cdots (f_m^{b_m}).$$

Since for every choice of partition b_i, there will always be a term in the product such that $b_i \geq e_i$, it follows that $(\sqrt{I})^e \subset I$.

Problem 5. Let K be any field and let A and B be algebraic subsets of K^n. Show that there exists an integer $m \geq n$ and an algebraic subset C of K^m such that the image of C under the projection $K^m \to K^n$ sending $(x_1, \ldots, x_m)$ to $(x_1, \ldots, x_n)$ is the set difference $A - B$.

Suppose $A = \mathcal{V}(f_1, \ldots, f_a)$ and $B = \mathcal{V}(g_1, \ldots, g_b)$. We claim that the space K^{n+b} suffices. Construct polynomials

$$\overline{g_i}(x_1, \ldots, x_n, t_1, \ldots, t_b) = g_i(x_1, \ldots, x_n)t_i - 1,$$
$$\overline{f_i}(x_1, \ldots, x_n, t_1, \ldots, t_b) = f_i(x_1, \ldots, x_n).$$

Let $\pi : K^{n+b} \to K^n$ be the projection map. Then $\pi(\mathcal{V}(\overline{g_i})) = K^n - \mathcal{V}(g_i)$, since the only way $\overline{g_i}$ could be zero for a given point $x_1, \ldots, x_n$ was if there exists some t_i such that $t_i = 1/g_i(x_1, \ldots, x_n)$, so $\pi(\mathcal{V}(\overline{g_i}))$ is precisely the set of points for which g_i is nonzero. Clearly $\pi(\mathcal{V}(\overline{f_i})) = \mathcal{V}(f_i)$, so if $C = \mathcal{V}(\overline{f_1}, \ldots, \overline{f_a}, \overline{g_1 g_2} \cdots \overline{g_b})$,

$$\pi(C) = \bigcup_i (K^n - \mathcal{V}(g_i)) \cap \bigcap_i \mathcal{V}(f_i) = (K^n - B) \cap A = A - B.$$

This concludes the proof.

Problem 6. Give an example of an algebraic field extension L of a field K that is not module-finite (i.e. not a finite-dimensional vector space)

Let $K = \mathbb{F}_p$ and $L = \overline{\mathbb{F}_p}$ be its algebraic closure. This is an algebraic extension by definition, however it isn't a finite extension because

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n}.$$

Problem 7. Let K be an infinite field and let $P_1, \ldots, P_m$ be m distinct nonzero points in K^n. Show that there is an invertible linear map $f : K^n \to K^n$ such that the $n \cdot m$ coordinates of the m points $f(P_1), \ldots, f(P_m)$ are distinct.

Consider the linear map f as a point in K^{n^2}. Then $\det(f)$ is a polynomial in $K[x_1, \ldots, x_{n^2}]$, so the set of invertible matrices is the complement of an algebraic set, namely $\det(f) = 0$. Now suppose we have a set of nonzero distinct points $P_1, \ldots, P_m$. Consider the polynomial $g \in K[x_1, \ldots, x_{n^2}]$ defined by

$$g(f) = \prod_{i<j} \prod_{a<b} (f(P_a)_i - f(P_b)_j).$$

Since each P_i has at least one nonzero coordinate, each $f(P_a)_i - f(P_b)_j$ is nonzero for some $f \in K^{n^2}$. So to find a linear map satisfying the conditions of the problem, it suffices to find some $f \in K^{n^2}$ such that $g(f) \neq 0$ and $\det(f) \neq 0$. If no such f exists, then $g \cdot \det$ vanishes on all of K^{n^2}, which is impossible by the Nichtnullstellensatz since K is infinite.