Math 137 Problem Set 5

Lev Kruglyak

April 21, 2022

Throughout, K is assumed to be an algebraically closed field. I collaborated with AJ LaMotta.

Problem 1. Let $f \in K[X_1, \ldots, X_n]$. Show that i

$$\mathcal{V}\left(f, \frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) = \varnothing,$$

then the polynomial f is squarefree.

Suppose $f = g^2 h$ for $g, h \in K[X_1, \ldots, X_n]$. Then

$$\frac{\partial f}{\partial x_i} = \frac{\partial g^2}{\partial x_i} h + g^2 \frac{\partial h}{\partial x_i} = 2g \frac{\partial g}{\partial x_i} h + g^2 \frac{\partial h}{\partial x_i} = g\left(2\frac{\partial g}{x_i} h + g^2 \frac{\partial h}{\partial x_i}\right) = gh_i.$$

for some $h_i \in K[X_1, \ldots, X_n]$. We can assume that $\frac{\partial f}{\partial x_i} \neq 0$ without loss of generality, so we know that $\mathcal{V}(g^2 h, gh_1, \ldots, gh_n) = \varnothing$. However this means that g has no roots, yet since K is algebraically closed, g must be a constant polynomial. This proves that f is squarefree.

Problem 2. Show that every monomial order $\leq$ on $\mathcal{S}(X_1, \ldots, X_n)$ is a well-order.

Let $\leq$ is a monomial order, suppose for the sake of contradiction that $\leq$ isn't a well order. By definition this means that there is an infinitely descending chain of monomials, i.e. monomials $M_1, M_2, \ldots$ with $M_1 > M_2 > \cdots$. Now letting $I_n = (M_1, \ldots, M_n)$ be the ideal generated by the first n ideals, we know that $M_{n+1} \notin I_n$ because otherwise $M_{n+1} = c_1 M_1 + \cdots + c_n M_n$ so M_{n+1} would be divisible by a greater monomial in the order M_i. Then $M_{n+1} = RM_i$ for some monomial R, which implies that $M_{n+1} < RM_i = M_{n+1}$ which is clearly contradictory. However this contradiction gives rise to an infinite increasing chain of ideals $I_1 \subset I_2 \subset \cdots$, which is impossible since $K[X_1, \ldots, X_n]$ is a Noetherian ring.

Problem 3. Let G be a Gröbner basis of $I \subseteq K[X_1, \ldots, X_n]$. Show that the set $\mathcal{V}(I)$ is finite if and only if for all $1 \leq i \leq n$, there is an element $g \in G$ such that $\operatorname{lm}(g) = X_i^t$ for some $t \geq 0$.

To prove the forward direction, suppose $\mathcal{V}(I)$ is finite. Then we have

$$\sqrt{I} \ni (X_i - a_1) \cdots (X_i - a_m)$$

where $a_1, \ldots, a_m$ are the i-th coordinates of points in $\mathcal{V}(I)$. Then the leading monomial of this polynomial is X_i^m. Recall that there is some t such that $I \supset (\sqrt{I})^t$ so there is a polynomial in I with leading monomial X_i^{tm}. Since G is a Gröbner basis, there must be a g with $\operatorname{lm}(g) = X_i^{tm}$. We can do this for every X_i, so we are done.

To prove the backward direction, suppose that $\mathrm{lm}(g_i) = X_i^{a_i}$ for a collection of Gröbner bases $g_1, \ldots, g_n$. Then the standard monomials of I are of the form $X_i^{b_i}$ with $b_i < a_i$. This is a finite collection, so by Corollary 8.3 the vanishing locus of I must be finite as well.

Problem 4.

a) Let $a, b > 0$ and consider the set

$$V = \{(x, y) \in \mathbb{Z}^2 : x, y \geq 0 \text{ and } ax + by \leq 1\}.$$

Fix any monomial ordering. Show that $X^r Y^s$ is a standard monomial for $\mathcal{I}(V)$ if and only if $(r, s) \in V$.

b) What is the smallest (total) degree d of a nonzero polynomial $f \in \mathcal{I}(V)$?

(a) First, let $(r, s) \in V$. Let $A = \{0, 1, \ldots, r\}$, and $B = \{0, 1, \ldots, s\}$. Applying the combinatorial Nullstellensatz to $A \times B$, we conclude that $X^r Y^s$ is a standard monomial for $\mathcal{I}(A \times B)$. However note that $\mathcal{I}(V) \subset \mathcal{I}(A \times B)$ since $A \times B \subset V$, so a standard monomial for $\mathcal{I}(A \times B)$ is also a standard monomial for $\mathcal{I}(V)$. Since V is finite of size $(1 + \lfloor 1/a \rfloor)(1 + \lfloor 1/b \rfloor)$ so there are $|V|$ standard monomials in $\mathcal{I}(V)$, and they are all exactly of the form $X^r Y^s$.

(b) We claim that $d = \min(\lfloor 1/a \rfloor, \lfloor 1/b \rfloor) + 1$. We've seen in A that the leading monomial of any nonzero $f \in \mathcal{I}(V)$ must be of the form $X^r Y^s$ with $(r, s) \notin V$, this means that $ar + bs > 1$. The smallest degree (with respect to lexicographic ordering) is $d = \min\{x + y \mid ax + by > 1\}$. However this quantity is straightforwardwardly proven to be $\min(\lfloor 1/a \rfloor, \lfloor 1/b \rfloor) + 1$, as desired.

Problem 5. Let $\leq$ be any monomial order on $K[X_1, \ldots, X_n]$ and let $0 \neq f, g \in K[X_1, \ldots, X_n]$. Show that if $\gcd(\mathrm{lm}(f), \mathrm{lm}(g)) = 1$, then 0 is a reduction of

$$S(f, g) = \frac{M}{\mathrm{lt}(f)} \cdot f - \frac{M}{\mathrm{lt}(g)} \cdot g$$

with respect to $\{f, g\}$, where $M = \mathrm{lcm}(\mathrm{lm}(f), \mathrm{lm}(g)) = \mathrm{lm}(fg)$.

Let's express the polynomials f and g as $f = \sum_{i=1}^{k} a_i M_i$ and $\sum_{i=1}^{\ell} b_i N_i$ for some nonzero coefficients. Let's further assume without loss of generality that $M_1 < M_2 < \cdots < M_k$ and $N_1 < N_2 < \cdots < N_\ell$, so that $\mathrm{lm}(f) = M_k$ and $\mathrm{lm}(g) = N_\ell$. Then we have

$$S(f, g) = \left(\sum_{i=1}^{k} \frac{a_i}{a_k} N_\ell M_i \right) - \left(\sum_{i=1}^{\ell} \frac{b_i}{b_\ell} M_k N_i \right).$$

Now note that if $N_\ell M_i = M_k N_j$ for some $j < \ell$ then we have $N_\ell | M_k N_j$, and since N_ℓ is coprime to M_k we have $N_\ell | N_j$. This is a contradiction since $j < \ell$. We get the same thing if we consider the M side, so the terms coming from M all cancel. Next, consider the identity

$$S(f, g) = \left(\frac{\mathrm{lt}(g) - g}{\mathrm{lc}(f)\mathrm{lc}(g)} \right) f + \left(\frac{f - \mathrm{lt}(f)}{\mathrm{lc}(f)\mathrm{lc}(g)} \right) g.$$

Notice then that if the first summand is nonzero, we have

$$\mathrm{lm}\left(\left(\frac{\mathrm{lt}(g) - g}{\mathrm{lc}(f)\mathrm{lc}(g)} \right) f \right) = \mathrm{lm}(\mathrm{lt}(g) - g)\mathrm{lm}(f) \leq \mathrm{lm}(S(f, g)).$$

However $S(f, g) = 0$, so repeating the same argument for the second summand, we have that 0 is a reduction of $S(f, g)$ with respect to $\{f, g\}$.