MATH 392 – Seminar in Computational Commutative Algebra
Solutions for Midterm Exam
March 22, 2019

I.

A) (20) Prove that every ideal I in the polynomial ring $k[x]$ (one variable) is principal (that is, $I = \langle g(x) \rangle$ for some single polynomial).

Solution: Let I be an ideal in $k[x]$. If $I = \{0\}$, then we can take g to be the zero polynomial. If I contains nonzero polynomials, let $g(x)$ be any nonzero element of I of minimal degree. We must show that every $f(x) \in I$ is a multiple of $g(x)$. So using the division algorithm in $k[x]$, write $f(x) = q(x)g(x) + r(x)$, where either $r(x)$ is identically zero, or else $\deg(r(x)) < \deg(g(x))$. We have $r(x) = f(x) - q(x)g(x)$. $f(x) \in I$ by assumption. $g(x)$ is also in I by construction. I is an ideal, hence closed under products by arbitrary polynomials, so $q(x)g(x) \in I$. Similarly I is closed under sums, so $r(x) = f(x) - q(x)g(x) \in I$. But $g(x)$ was a nonzero element of I of minimal degree and $r(x)$ is either identically zero, or else $\deg(r(x)) < \deg(g(x))$. Since the second alternative is not possible, $r(x) = 0$, which shows $f(x) = q(x)g(x)$. This shows $I \subseteq \langle g(x) \rangle$. The opposite inclusion is also true because $g(x) \in I$, so $\langle g(x) \rangle \subseteq I$ since I is closed under multiplication by arbitrary polynomials.

B) (10) Find $g(x)$ as in part A for the ideal $I = \langle x^2 + 7x + 10, x^3 + 2x^2 + 4 \rangle$ in $\mathbf{Q}[x]$.

Solution 1: The polynomial $g(x)$ must be the gcd of the two generators for I. We see by factoring that $x^2 + 7x + 10 = (x+2)(x+5)$ and $x^3 + x^2 + 4 = (x+2)(x^2 - x + 2)$ and $x^2 - x + 2$ does not factor farther in $\mathbf{Q}[x]$ because this polynomial has no rational (or even real) roots. Hence the gcd is $x + 2$.

Solution 2: We can also find the gcd using the Euclidean Algorithm in $\mathbf{Q}[x]$. Dividing:

$$x^3 + 2x^2 + 4 = (x-6)(x^2 + 7x + 10) + 32x + 64$$
$$x^2 + 7x + 10 = \left(\frac{x}{32} + \frac{5}{32}\right)(32x + 64) + 0$$

The last nonzero remainder is the gcd, up to a constant multiple. Note $32x + 64 = 32(x+2)$ so the monic gcd is $x + 2$ as in the first solution.

II.

A) (15) Define: G is a Gröbner basis for an ideal $I \subset k[x_1, \ldots, x_n]$ with respect to a monomial order $>$.

Solution: A Gröbner basis for I with respect to $>$ is a finite collection of polynomials $G = \{g_1, \ldots, g_t\} \subset I$ such that the monomial ideal $\langle LT_>(I) \rangle$ is generated by $LT_>(g_1), \ldots, LT_>(g_t)$. (Equivalently you could also say it is a finite collection of polynomials G as above such that for every nonzero $f \in I$, $LT_>(f)$ is divisible by $LT_>(g_i)$ for some i.)

B) (10) Assuming the statement of Dickson's Lemma, prove that Gröbner bases exist for every ideal I in $k[x_1, \ldots, x_n]$ and with respect to every monomial order.

Solution: We may assume that $I \neq \{0\}$, since in that case we can take $G = \emptyset$. Dickson's Lemma is the statement that every monomial ideal in $k[x_1, \ldots, x_n]$ is generated by a *finite set* of monomials. We apply that result to the monomial ideal $\langle LT_>(I)\rangle = \langle LT_>(f) \mid f \in I\rangle$. This says $\langle LT_>(I)\rangle$ is generated by some finite collection of monomials $x^{\alpha(1)}, \ldots, x^{\alpha(t)}$. Moreover, by definition each of those is equal to the leading term of some element in I:

$$x^{\alpha(i)} = LT_>(g_i),$$

for some $g_i \in I$. By the definition (part A), this says $\{g_1, \ldots, g_t\}$ is a Gröbner basis for I.

C) (5) What else do you need to know in order for the result from part B to give a proof of the Hilbert Basis Theorem? (You don't need to give the proof, just say what else must be proved.)

Solution: The other fact that must be proved to get a proof of the Hilbert Basis Theorem (the statement that every ideal in $k[x_1, \ldots, x_n]$ has a finite basis) is that a Gröbner basis for I is also an ideal basis for I, or equivalently that if G is a Gröbner basis for I and $f \in I$, then the remainder on division of f by G is zero: $\overline{f}^G = 0$. This follows from the definition of a Gröbner basis and the properties of the Division Algorithm.

III.

A) (20) State and prove the Elimination Theorem.

Solution: Let I be an ideal in $k[x_1, \ldots, x_n]$ and let $I_\ell = I \cap k[x_{\ell+1}, \ldots, x_n]$ be the elimination ideals for $\ell = 1, \ldots, n-1$. The Elimination Theorem states that if G is a Gröbner basis for I with respect to the lexicographic order with $x_1 > x_2 > \ldots > x_n$, then $G_\ell = G \cap k[x_{\ell+1}, \ldots, x_n]$ is a Gröbner basis of I_ℓ, for all $\ell = 1, \ldots, n-1$. Proof: We must show that if f is any element of I_ℓ, then $LT_{lex}(f)$ is divisible by one of the leading terms of the elements of G_ℓ. But if $f \in I_\ell$, then f depends only on the variables $x_{\ell+1}, \ldots, x_n$, and the same is true for $LT_{lex}(f)$. Since G is a Gröbner basis for I, $LT_{lex}(f)$ is divisible by $LT_{lex}(g)$ for some $g \in G$. But this means that $LT_{lex}(g)$ can only depend on the variables $x_{\ell+1}, \ldots, x_n$. By the properties of the lex order with

$$x_1 > x_2 > \cdots > x_\ell > x_{\ell+1} > \cdots x_n,$$

any monomial containing any of the variables $x_1, \ldots, x_\ell$ is *greater than* all monomials containing only the variables $x_{\ell+1}, \ldots, x_n$. This means that no term in g can contain any of the variables $x_1, \ldots, x_\ell$. Hence by definition $g \in G_\ell$. We have shown that for every nonzero $f \in I_\ell$, $LT_{lex}(f)$ is divisible by $LT_{lex}(g)$ for some $g \in G_\ell$. This shows that G_ℓ is a Gröbner basis for I_ℓ by the definition.

B) (10) A certain ideal $J \subset \mathbf{Q}[x, y, z]$ has a Gröbner basis

$$B = \{x^3 - 3x^2 + 2x, x^2y - xy, y^2 - y, z - xy\}$$

with respect to the lexicographic order with $z > y > x$. What are bases for the elimination ideals

$$J_1 = J \cap \mathbf{Q}[y, x] \quad \text{and} \quad J_2 = J \cap \mathbf{Q}[x]?$$

Solution: $J_1 = \langle x^3 - 3x^2 + 2x, x^2y - xy, y^2 - y\rangle$ and $J_2 = \langle x^3 - 3x^2 + 2x\rangle$.

C) (10) Use the information in part B to determine all of the points in $V(J)$.

Solution: We begin by setting the generator of J_2 equal to zero and by factoring we find $x(x-1)(x-2) = 0$, so $x = 0$, $x = 1$, or $x = 2$. If we substitute $x = 0$ in the rest of the Gröbner basis, we find:

$$B|_{x=0} = \{0, 0, y^2 - y, z\}$$

From this we see $y(y-1) = 0$ so $y = 0$ or $y = 1$. And then with either of those y-values, $z = 0$. So we have two points with $x = 0$, namely $(0, 0, 0)$ and $(0, 1, 0)$. If we substitute $x = 1$ in the rest of the Gröbner basis, we find:

$$B|_{x=1} = \{0, 0, y^2 - y, z - y\}$$

Hence we find two more points $(1, 0, 0)$ and $(1, 1, 1)$. Finally, if we substitute $x = 2$ into the rest of the Gröbner basis, we find

$$B|_{x=2} = \{0, 2y, y^2 - y, z - 2y\}$$

The only solution is $(2, 0, 0)$. This means that $V(J)$ consists of five points in all:

$$V(J) = \{(0, 0, 0), (0, 1, 0), (1, 0, 0), (1, 1, 1), (2, 0, 0)\}.$$