MATH 850 Midterm Exam 3/8/17 10:10–11:00 a.m.

Show complete work—that is, all the steps needed to completely justify your answer. Simplify your answers as much as possible. You may refer to theorems in the book and class notes.

1. Prove that $x^4 + 1 \in \mathbb{Z}[x]$ is irreducible.

   Proof. One way to show this is through the factorization of $x^4 + 1$ in $\mathbb{C}[x]$. Here's a proof using Eisenstein's criterion: $f(x) = x^4 + 1$ is irreducible in $\mathbb{Z}[x]$ if and only if $f(x+1)$ is. However,

   $$f(x+1) \;=\; x^4 + 4x^3 + 6x^2 + 4x + 2$$

   is irreducible by Eisenstein's criterion applied with the prime 2. □

2. Let R be an integral domain.

   (a) Define what it means for $\preceq$ to be a term order on $\mathbb{Z}^n_{\geq 0}$.

   (b) Define the initial term $\mathrm{in}_{\preceq}(f)$ for a polynomial $f \in R[x_1, \ldots, x_n]$.

   (c) Prove that, if $f, g \in R[x_1, \ldots, x_n]$, then

   $$\mathrm{in}_{\preceq}(fg) \;=\; \mathrm{in}_{\preceq}(f)\,\mathrm{in}_{\preceq}(g)\,.$$

   Proof of (c). Suppose $\mathrm{in}_{\preceq}(f) = a\,\mathbf{x}^{\mathbf{v}}$ and $\mathrm{in}_{\preceq}(f) = b\,\mathbf{x}^{\mathbf{w}}$. Then $ab\,\mathbf{x}^{\mathbf{v}+\mathbf{w}}$ is a term in fg, and any other term in fg is of the form $c\,\mathbf{x}^{\mathbf{y}+\mathbf{z}}$ for some $\mathbf{y} \preceq \mathbf{v}$ and $\mathbf{z} \preceq \mathbf{w}$. However, because $\preceq$ is a term order,

   $$\mathbf{y} + \mathbf{z} \;\preceq\; \mathbf{v} + \mathbf{z} \;\preceq\; \mathbf{v} + \mathbf{w}$$

   and so $ab\,\mathbf{x}^{\mathbf{v}+\mathbf{w}}$ is the initial term of fg. □

3. Let I be an ideal in $F[x_1, \ldots, x_n]$, for some field F, and let $\preceq$ be a term order on $\mathbb{Z}^n_{\geq 0}$.

   (a) Define what it means for $G \subseteq F[x_1, \ldots, x_n]$ to be a Gröbner basis for I with respect to $\preceq$.

   (b) Given a Gröbner basis G for I, prove that $f \in I$ if and only if the remainder when dividing G into f is 0.

   Proof of (b). Suppose $G = \{g_1, g_2, \ldots, g_m\}$ is a Gröbner basis for I with respect to $\preceq$. Let $f \in I$. The division algorithm gives

   $$f \;=\; q_1\,g_1 + q_2\,g_2 + \cdots + q_m\,g_m + r$$

   for some polynomials $q_1, q_2, \ldots, q_m, r$ such that $r = 0$ or none of the initial terms of g_j divides $\mathrm{in}_{\preceq}(r)$. But since $f, g_1, g_2, \ldots, g_m \in I$, we know that $r \in I$, and since G is a Gröbner basis for I, there exists g_j whose initial term divides $\mathrm{in}_{\preceq}(r)$. The only way out of this conundrum is $r = 0$. □

MATH 850 Take Home Midterm Exam 6–8–10 March 2017

Show complete work—that is, all the steps needed to completely justify your answer. Simplify your answers as much as possible. You may refer to theorems in the text book. You are welcome to use books and internet sources, but you are not allowed to discuss this exam with anyone (including your class mates).

1. (a) Show that x^2+1, x^2+x+2, and x^2+2x+2 are the only monic irreducible polynomials of degree 2 in $\mathbb{Z}_3[x]$.

   (b) Show that, if the polynomial $f(x)$ has degree 4 or 5, has no roots, and is reducible, then there is a monic irreducible polynomial of degree 2 dividing $f(x)$.

   (c) Prove that x^5+2x+1 is irreducible in $\mathbb{Z}_3[x]$ and deduce that

   $$F \;:=\; \mathbb{Z}_3[x] \,/\, \langle x^5+2x+1 \rangle$$

   is a field with 243 elements.

   (d) Compute the multiplicative inverse of $x+\langle x^5+2x+1\rangle$ in F.

   Proof.

   (a) follows from checking the nine monic quadratic polynomials in $\mathbb{Z}_3[x]$ for roots.

   (b) Because $\mathbb{Z}_3$ is a field, we can make any factor of $f(x)$ monic, and the degrees add up. Since $f(x)$ has no linear factor (which would correspond to a root), it needs to have a quadratic factor because otherwise the degrees of the factors of $f(x)$ would add up to more than 5.

   (c) One can quickly check that none of the polynomials in (a) divide x^5+2x+1. Thus x^5+2x+1 is irreducible and F is a field. Its elements are of the form $a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+\langle x^5+2x+1\rangle$ for some $a_0,a_1,\ldots,a_4\in\mathbb{Z}_3$ and the division algorithm shows that they are unique. Hence there are $3^5=243$ elements in F.

   (d) Multiplying $x\,(x^4+2)+\langle x^5+2x+1\rangle \;=\; 2+\langle x^5+2x+1\rangle$ by $2+\langle x^5+2x+1\rangle$ gives

   $$x\left(2x^4+1\right)+\left\langle x^5+2x+1\right\rangle \;=\; 1+\left\langle x^5+2x+1\right\rangle,$$

   and so the inverse of $x+\langle x^5+2x+1\rangle$ is $2x^4+1+\langle x^5+2x+1\rangle$. □

2. (a) Show that the relation $\preceq$ defined on $\mathbb{Z}^2_{\geq 0}$ through

   $$\mathbf{v}\preceq\mathbf{w} \qquad\Longleftrightarrow\qquad v_1+v_2\leq w_1+w_2$$

   is not a term order.

   (b) Show that the relation $\preceq$ defined on $\mathbb{Z}^2_{\geq 0}$ through

   $$\mathbf{v}\preceq\mathbf{w} \qquad\Longleftrightarrow\qquad v_1+v_2\sqrt{2}\leq w_1+w_2\sqrt{2}$$

   is a term order.

(c) Compute the reduced Gröbner basis for the ideal

$$I \;:=\; \left\langle x^2+y,\; x^2y+1\right\rangle \;\subseteq\; \mathbb{R}[x,y]\,.$$

with respect to the term order defined in (b).

Proof.

(a) This is not a total order, as $(1,2) \preceq (2,1) \preceq (1,2)$.

(b) Reflexivity and transitivity follow from $\leq$ on $\mathbb{R}$, and antisymmetry follows because

$$a+b\sqrt{2} \;\leq\; c+d\sqrt{2} \;\leq\; a+b\sqrt{2}$$

implies $a+b\sqrt{2} = c+d\sqrt{2}$ and hence (since $a,b,c,d \in \mathbb{Z}$) $a=c$ and $b=d$. This shows that $\preceq$ is a total order. It is a term order because $a+b\sqrt{2} \geq 0$ for $a,b \geq 0$, and because the dot product with $(1,\sqrt{2})$ is additive.

(c) Using S-polynomials and Buchberger's algorithm gives the reduced Gröbner basis

$$\left\{x^2+y,\; y^2-1\right\}.$$ □

3. Decide whether

$$f(x,y) \;:=\; x^3y+x^3+x^2y^3-x^2y+xy+x$$

is in the ideal I defined in 2(c). (Note that you are not required to use the term order from 2(b).) If it is, find $a(x,y)$ and $b(x,y)$ such that

$$f(x,y) \;=\; a(x,y)\left(x^2+y\right)+b(x,y)\left(x^2y+1\right).$$

Proof. We could use the term order and reduced Gröbner basis from 2. Just for fun, let's use the usual lex order. Let $g_1(x,y) := x^2+y$ and $g_2(x,y) := x^2y+1$. We compute

$$S(g_1,g_2) \;=\; y\,g_1(x,y)-g_2(x,y) \;=\; y^2-1 \;=:\; g_3(x,y)$$

and after two more iterations of Buchberger's algorithm deduce that $\{g_1,g_2,g_3\}$ is the reduced Gröbner basis for I. The division algorithm gives

$$f(x,y) \;=\; \left(xy+x+y^3-y\right)g_2(x,y)+\left(-x-y^2\right)g_3(x,y)$$

and so $f \in I$. Retracing our steps (i.e., replacing $g_3(x,y)$ in the above expression in terms of $g_1(x,y)$ and $g_2(x,y)$) gives

$$f(x,y) \;=\; \left(-xy-y^3\right)g_1(x,y)+\left(xy+2x+y^3+y^2-y\right)g_2(x,y)\,.$$ □