Math 351

Solutions to review problems for Exam #1 **October 4, 2010**

#1 (a) Find the greatest common divisor of 357 and 756 and write it in the form $a(357) + b(756)$ where a and b are integers.

Solution: $(756, 357) = 21$ and $21 = -8(756) + 17(357)$.

(b) Find the greatest common divisor of $x^3 - 5x^2 + 7x - 2$ and $x^4 - 2x^3 + x^2 + x - 6$ in $\mathbf{Q}[x]$.

Solution: $(x^3 - 5x^2 + 7x - 2, x^4 - 2x^3 + x^2 + x - 6) = x - 2$ and

$$x - 2 = (\frac{x^2}{9})(x^3 - 5x^2 + 7x - 2) - (\frac{1}{9})(x - 3)(x^4 - 2x^3 + x^2 + x - 6).$$

(c) Find the greatest common divisof of $x^4 + x^2 + 1$ and $x^4 + x^3 + x^2 + x + 1$ in $\mathbf{Z}_2[x]$.

Solution: $(x^4 + x^2 + 1, x^4 + x^3 + x^2 + x + 1) = 1$ and

$$1 = (x + 1)(x^4 + x^2 + 1) + x(x^4 + x^3 + x^2 + x + 1).$$

#2 Let $n \in \mathbf{Z}, n \geq 1$. Prove that $\mathbf{Z}_n$ is a field if and only if n is a prime. You may use (without proving them) results about the greatest common divisor of two integers.

Solution: Assume n is a prime and that x is a nonzero element in $\mathbf{Z}_n$. Then $x = [a]$ for some integer a such that a is not a multiple of n. Then $(n, a) = 1$ and so there exist integers u and v such that $1 = au + nv$. Then $[1] = [a][u] + [n][v] = [a][u]$. Thus $x = [a]$ is a unit in $\mathbf{Z}$. Since every nonzero element in $\mathbf{Z}_n$ is a unit, $\mathbf{Z}_n$ is a field.

Now assume that $\mathbf{Z}_n$ is a field and that a, b are two integers with $n|(ab)$. Then $[a][b] = [0]$ in $\mathbf{Z}_n$ and so $[a] = [0]$ or $b = [0]$. Thus $n|a$ or $n|b$. This shows that n is prime.

#3 Let R be a ring and I be an ideal in R. Recall that the coset $a + I$ is defined to be $\{a + x | x \in I\}$.

(a) Prove that if $(a + I) \cap (b + I) \neq \emptyset$ then $a + I = b + I$.

Solution: Since $(a + I) \cap (b + I) \neq \emptyset$ there is some element $c \in (a + I) \cap (b + I)$. Then $c \in a + I$ so $c - a \in I$. Also $c \in b + I$ so $c - b \in I$. Then $a - b = ((c - b) - (c - a) \in I$. Now an element $r \in R$ belongs to $a + I$ if and only if $r - a \in I$. Since $a - b \in I$ we see that $r - b \in I$ if and only if $r - a = (r - b) - (a - b) \in I$. Thus $r \in a + I$ if and only if $r \in b + I$ so $a + I = b + I$.

(b) Prove that if $a_1 + I = b_1 + I$ and $a_2 + I = b_2 + I$, then $a_1 a_2 + I = b_1 b_2 + I$.

Solution: Since $a_1 + I = b_1 + I$ we have $a_1 - b_1 \in I$. Then since I is an ideal we have $(a_1 - b_1)a_2 \in I$. Also, since $a_2 + I = b_2 + I$ we have $a_2 - b_2 \in I$ and, since I is an ideal, $b_1(a_2 - b_2) \in I$. Then

$$a_1 a_2 - b_1 b_2 = (a_1 - b_1)a_2 + b_1(a_2 - b_2) \in I$$

giving the result.

#4 Let F be a field and let $f(x), g(x) \in F[x]$. Assume $f(x)$ and $g(x)$ are not both 0.

(a) State (but don't prove) the division algorithm for $F[x]$.

Solution: Assume $g(x) \neq 0$. Then there exist $q(x), r(x) \in F[x]$ with $r(x) = 0$ or $deg\ r(x) < deg\ g(x)$ such that

$$f(x) = g(x)q(x) + r(x).$$

(b) State the definition of the greatest common divisor of $f(x)$ and $g(x)$.

Solution: $h(x)$ is a common divisor of $f(x)$ and $g(x)$ if $h(x)|f(x)$ and $h(x)|g(x)$. The monic polynomial $d(x)$ of greatest degree which is a common divisor of $f(x)$ and $g(x)$ is the greatest common divisor.

(c) Prove that $f(x)$ and $g(x)$ have a greatest common divisor and that it may be written in the form $a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in F[x]$.

Solution: Let $S = \{u(x)f(x) + v(x)g(x) | u(x), v(x) \in F[x]\}$. Let $S^* = \{k(x) \in S | k(x) \neq 0\}$. Let $d(x)$ be a monic polynomial of smallest degree in S^*. We claim that $d(x)$ is the greatest common divisor of $f(x)$ and $g(x)$. Since $d(x) \in S$ we see that any common divisor of $f(x)$ and $g(x)$ divides $d(x)$ and so the degree of $d(x)$ is greater than or equal to the degree of any common divisor. It remains to show that $d(x)$ is a common divisor of $f(x)$ and $g(x)$. By the division algorithm, we may find $q(x), r(x) \in F[x]$ such that $r(x) = 0$ or $deg\ r(x) < deg\ d(x)$ and

$$f(x) = q(x)d(x) + r(x).$$

Since $d(x) = u(x)f(x) + v(x)g(x)$ we have

$$r(x) = f(x) - q(x)d(x) = f(x) - q(x)(u(x)f(x) + v(x)g(x)) =$$

$$(1 - q(x)u(x))f(x) - q(x)v(x)g(x) \in S.$$

Since the degree of $d(x)$ is minimal among nonzero elements of S^* we must have $r(x) = 0$ and so $d(x)|f(x)$. Similarly, $d(x)|g(x)$ and so $d(x)$ is a common divisor of $f(x)$ and $g(x)$. Hence it is the greatest common divisor.

#5 Let R and S be commutative rings with identity. Recall that $R \times S$ denotes $\{(r, s) | r \in R, s \in S\}$ with operations $(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$ and $(r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2)$. Recall also that $R \times S$ is a ring.

(a) Let I be an ideal in $R \times S$. Define $J_1 = \{r \in R | (r, 0) \in I\}$ and $J_2 = \{s \in S | (0, s) \in I\}$. Prove that J_1 is an ideal in R and that J_2 is an ideal in S. Then prove that $I = \{(a, b) \in R \times S | a \in J_1, b \in J_2\}$.

Solution: Since $(0_R, 0_S) \in I$ we have $0_R \in J_1$ and $0_S \in J_2$. Thus J_1 and J_2 are nonempty. Now suppose $a_1, a_2 \in J_1$. Then $(a_1, 0_S) \in I$ and $(a_2, 0_S) \in I$ so $(a_1 - a_2, 0_S) \in I$, giving $a_1 - a_2 \in J_1$. Also, if $r \in R$, $(a_1 r, 0) = (a_1, 0)(r, 0) \in I$ and so $a_1 r \in J_1$. Thus J_1 is an ideal in R. Similarly, J_2 is an ideal in S. Now if $a \in J_1$ and $b \in J_2$ we have $(a,0) \in I$ and $(0,b) \in I$ so $(a,b) = (a,0)+(0,b) \in I$. Conversely, if $(a,b) \in I$ then $(a,0) = (a,b)(1_R,0) \in I$ and $(0,b) = (a,b)(0,1_S) \in I$. Thus $a \in J_1, b \in J_2$.

(b) Suppose the hypothesis that R and S have identity elements is omitted. Does the result of (a) remain true? Why or why not?

Solution: The result does not remain true. For example, let $R = S = 2\mathbf{Z}$. Then

$$I = \{(a,b) \in 2\mathbf{Z} \times 2\mathbf{Z} | a \equiv b (mod\ 4)\}$$

is an ideal in $2\mathbf{Z} \times 2\mathbf{Z}$ and $J_1 = J_2 = 4\mathbf{Z}$. However, $(2,2) \in I$.

#6 Let W denote $\{\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix} | a,b \in \mathbf{R}\} \subseteq M(\mathbf{R})$, Y denote $\{\begin{vmatrix} a & 0 \\ 0 & 0 \end{vmatrix} | a \in \mathbf{R}\} \subseteq M(\mathbf{R})$, and N denote $\{\begin{vmatrix} 0 & b \\ 0 & 0 \end{vmatrix} | b \in \mathbf{R}\} \subseteq M(\mathbf{R})$

(a) Show that W and Y are subrings of $M(\mathbf{R})$.

Solution: W and Y are both nonempty. Since

$$\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix} - \begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix} = \begin{vmatrix} a-c & b-d \\ 0 & 0 \end{vmatrix}$$

and

$$\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix} \begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix} = \begin{vmatrix} ac & ad \\ 0 & 0 \end{vmatrix}$$

we see that W and Y are subrings. (Note that if we take $a = c = 0$ the elements in the above equations are elements of Y.)

(b) Define a map g from W to Y by $g(\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix}) = \begin{vmatrix} a & 0 \\ 0 & 0 \end{vmatrix}$. Show that g is a homomorphism.

Solution:

$$g(\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix} + \begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix}) = g(\begin{vmatrix} a+c & b+d \\ 0 & 0 \end{vmatrix}) =$$

$$\begin{vmatrix} a+c & 0 \\ 0 & 0 \end{vmatrix} = \begin{vmatrix} a & 0 \\ 0 & 0 \end{vmatrix} + \begin{vmatrix} c & 0 \\ 0 & 0 \end{vmatrix} =$$

$$g(\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix}) + g(\begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix})$$

and

$$g(\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix} \begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix}) = g(\begin{vmatrix} ac & ad \\ 0 & 0 \end{vmatrix}) =$$

$$\begin{vmatrix} ac & 0 \\ 0 & 0 \end{vmatrix} = \begin{vmatrix} a & 0 \\ 0 & 0 \end{vmatrix} \begin{vmatrix} c & 0 \\ 0 & 0 \end{vmatrix} =$$

$$g(\begin{vmatrix} a & b \\ 0 & 0 \end{vmatrix})g(\begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix}).$$

(c) Show that N is an ideal in W and that W/N is isomorphic to Y.

Solution: Since g is surjective and N is the kernel of g, the result follows from the First Isomorphism Theorem

#7 Prove that a finite integral domain is a field.

Solution: Let R be a finite integral domain and let R^* denote $\{r \in R | r \neq 0\}$. We must show that any element $r \in R^*$ is a unit. For $r \in R^*$ let

$$f_r : R \to R$$

be the map defined by

$$f_r(s) = rs.$$

If $f_r(s_1) = f_r(s_2)$ then $rs_1 = rs_2$ and so $r(s_1 - s_2) = 0$. Since R is an integral domain and $r \neq 0$ this implies $s_1 - s_2 = 0$ and so $s_1 = s_2$. Thus f_r is injective. Since R is finite, f_r must be surjective and so there is some $u \in R$ such that $f_r(u) = 1_R$. But then $ru = f_r(u) = 1_R$, so r is a unit.

#8 Let R be a ring and $a, b \in R$. Prove, directly from the definition of a ring, that $0_R a = a 0_R = 0_R$ and that $-(ab) = (-a)b = a(-b)$.

Solution: Note that if $x, y \in R$ and $x + y = x$, then

$$y = 0_R + y = ((-x) + x) + y = (-x) + (x + y) = (-x) + x = 0_R.$$

Now

$$0_R a + 0_R a = (0_R + 0_R)a = 0_R a$$

and so $0_R a = 0_R$. Similarly,

$$a0_R + a0_R = a(0_R + 0_R) = a0_R$$

and so $a0_R = 0_R$. Finally,

$$ab + (-a)b = (a + (-a))b = 0_R b = 0,$$

so $(-a)b = -(ab)$ and

$$ab + a(-b) = a(b + (-b)) = a0_R = 0_R,$$

so $a(-b) = -(ab)$.