Math 351

Solutions to review problems for Exam #1 **October 8, 2007**

Exam #1 will be given during the normal class period on Monday, October 15. It will cover material through Section 4.4. This set of review problems is about twice as long as the exam.

#1 Find the greatest common divisor of 561 and 1336 and write it in the form $561a+1336b$ where a and b are integers.

Solution: First we note that

$$1336 = 2(561) + 214 \textit{ so } 214 = 1336 - 2(561),$$

$$561 = 2(214) + 133 \textit{ so } 133 = 561 - 2(214),$$

$$214 = 133 + 81 \textit{ so } 81 = 214 - 133,$$

$$133 = 81 + 52 \textit{ so } 52 = 133 - 81,$$

$$81 = 52 + 29 \textit{ so } 29 = 81 - 52,$$

$$52 = 29 + 23 \textit{ so } 23 = 52 - 29,$$

$$29 = 23 + 6 \textit{ so } 6 = 29 - 23,$$

$$23 = 3(6) + 5 \textit{ so } 5 = 23 - 3(6),$$

$$6 = 5 + 1 \textit{ so } 1 = 6 - 5,$$

and

$$1|.5$$

Therefore $(561, 1336) = 1$. Furthermore

$$1 = 6 - 5 = 6 - (23 - 3(6)) = -23 + 4(6) =$$

$$-23 + 4((29 - 23) = 4(29) - 5(23) =$$

$$4(29) - 5(52 - 29) = -5(52) + 9(29) =$$

$$-5(52) + 9(81 - 52) = 9(81) - 14(52) =$$

$$9(81) - 14(133 - 81) = -14(133) + 23(81) =$$

$$-14(133) + 23(214 - 133) = 23(214) - 37(133) =$$

$$23(214) - 37(561 - 2(214) = -37(561) + 97(214) =$$

$$-37(561) + 97(1336 - 2(561)) = 97(1336) - 231(561).$$

#2 Find the greatest common divisor of the polynomials $f(x) = x^5 + 2x^4 + 8x^3 + 16x^2 + 11x + 2$ and $g(x) = x^5 + 11x^3 + 2x^2 + 28x + 8$ and write it in the form $a(x)f(x) + b(x)g(x)$ where $a(x), b(x) \in \mathbf{R}[x]$.

Solution: First we note that

$$f(x) = g(x) + 2x^4 - 3x^3 + 14x^2 - 17x - 6 \textit{ so } 2x^4 - 3x^3 + 14x^2 - 17x - 6 = f(x) - g(x),$$

$$g(x) = (\frac{x}{2} + \frac{3}{4})(2x^4 - 3x^3 + 14x^2 - 17x - 6) + \frac{25}{4}x^3 + \frac{175}{4}x + \frac{25}{2}$$

$$\textit{so } \frac{25}{4}x^3 + \frac{175}{4}x + \frac{25}{2} = g(x) - (\frac{x}{2} + \frac{3}{4})(2x^4 - 3x^3 + 14x^2 - 17x - 6),$$

and

$$(\frac{25}{4}x^3 + \frac{175}{4}x + \frac{25}{2})|(2x^4 - 3x^3 + 14x^2 - 17x - 6).$$

Therefore

$$(f(x), g(x)) = x^3 + 7x + 2 = \frac{4}{25}(g(x) - (\frac{x}{2} + \frac{3}{4})(2x^4 - 3x^3 + 14x^2 - 17x - 6) =$$

$$\frac{4}{25}g(x) - (\frac{2x+3}{25})(2x^4 - 3x^3 + 14x^2 - 17x - 6) =$$

$$\frac{4}{25}g(x) - (\frac{2x+3}{25})(f(x) - g(x)) = -(\frac{2x+3}{25})f(x) + (\frac{2x+7}{25})g(x).$$

#3 Let a, b, and n be integers. State the definition of $a \equiv b(mod\ n)$ and prove that if $a_1 \equiv b_1(mod\ n)$ and $a_2 \equiv b_2(mod\ n)$ then $a_1a_2 \equiv b_1b_2(mod\ n)$.

Solution: The definition is that $a \equiv b(mod\ n)$ if and only if $n|(a-b)$. Now if $a_1 \equiv b_1(mod\ n)$ and $a_2 \equiv b_2(mod\ n)$ then $n|a_1 - b_1$ so $a_1 - b_1 = k_1n$ for some integer k_1 and $n|a_2 - b_2$ so $a_2 - b_2 = k_2n$ for some integer k_2. Then $a_1 = b_1 + k_1n$ and $a_2 = b_2 + k_2n$. Thus

$$a_1a_2 = (b_1 + k_1n)(b_2 + k_2n) = b_1b_2 + (b_1k_2 + k_1b_2 + k_1k_2n)n$$

and so $a_1a_2 - b_1b_2 = (b_1k_2 + k_1b_2 + k_1k_2n)n$ which is a multiple of n, as required.

#4 Let $n > 1$ be an integer. State the definition of $\mathbf{Z}_n$. Using the fact that $\mathbf{Z}$ is a ring, prove that addition in $\mathbf{Z}_n$ is associative.

Solution: $\mathbf{Z}_n$ is defined to be the set of all congruence classes $[a]$ where $a \in \mathbf{Z}$ and

$$[a] = \{b \in \mathbf{Z} | b \equiv a(mod\ n)\}.$$

The ring structure is defined on this set by

$$[x] + [y] = [x + y]$$

and

$$[x][y] = [xy]$$

for all integers x and y. The definition of $[x][y]$ makes sense (i.e., does not depend on the choice of representatives for the congruence classes by the result of the previous problem). A similar (though easier) argument shows that the definition of $[x] + [y]$ also makes sense. Now to show that addition in $\mathbf{Z}_n$ is associative we must show that $([a] + [b]) + [c] = [a] + ([b] + [c])$ for all $a, b, c \in \mathbf{Z}$. We begin with the left hand side and write

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c]$$

where both equalities follow from the definition of addition in $\mathbf{Z}_n$. Now

$$[(a + b) + c] = [a + (b + c)]$$

by associativity of addition in $\mathbf{Z}$ and

$$[a + (b + c)] = [a] + [b + c] = [a] + ([b] + [c])$$

where both equalities follow from the definition of addition in $\mathbf{Z}$. This completes the proof.

\$5 Let R, S, T be rings, let f be a homomorphism from R to S and g be a homomorphism from S to T. Prove that the composition $g \circ f$ is a homomorphism from R to T.

Solution: Let $a, b \in R$. Then $(g \circ f)(a + b) = g(f(a + b)) = g(f(a) + f(b))$ since f is a homomorphism and $g(f(a) + f(b)) = g(f(a)) + g(f(b))$ since g is a homomorphism. Thus $(g \circ f)(a + b) = (g \circ f)(a) + (g \circ f)(b)$. Similarly, $(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b))$ since f is a homomorphism and $g(f(a)f(b)) = g(f(a))g(f(b))$ since g is a homomorphism. Thus $(g \circ f)(ab) = (g \circ f)(a)(g \circ f)(b)$. Thus $g \circ f$ is a homomorphism.

#6 Let R be a ring, with addition $+$ and multiplication $\times_R$. Define a new multiplication $\times_{op}$ on R by $a \times_{op} b = b \times_R a$ for all $a, b \in R$. Then R with addition $+$ and multiplication $\times_{op}$ is a ring. (You don't have to verify this.) Show that $M(\mathbf{R})$ is isomorphic to $M(\mathbf{R})^{op}$. (Hint: Use the transpose map.)

Solution: Define a map $f : M(\mathbf{R}) \to M(\mathbf{R})_{op}$ by $f(A) = A^t$ (the transpose of A) for all $A \in M(\mathbf{R})$. Since $(A^t)^t = A$ we see that f is one-to-one and onto. Thus we only need to show that f is a homomorphism. Let $A, B \in M(\mathbf{R})$. Recall two properties of the transpose (from linear algebra: $(A + B)^t = A^t + B^t$ and $(AB)^t = B^t A^t$. Then

$$f(A + B) = (A + B)^t = A^t + B^t = f(A) + f(B)$$

and (using the symbol $\times_{M(\mathbf{R})}$ to denote multiplication in $M(\mathbf{R})$ and the symbol $\times_{op}$ to denote multiplication in $M(\mathbf{R})_{op}$) we have $f(A \times_{M(\mathbf{R})} B) = (AB)^t = B^t A^t = A^t \times_{op} B^t = f(A) \times_{op} f(B)$. Thus f is an isomorphism.

#7 Let I be an ideal in a ring R and $a \in R$.

(a) State the definition of the coset $a + I$ and of the quotient ring R/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:

(a) The coset $a + I$ is defined to be $\{a + x | x \in I\}$ and the quotient ring R/I is defined to be the set of all cosets of I in R (that is $\{a + I | a \in R\}$.) with addition

$$(a + I) + (b + I) = (a + b) + I$$

and multiplication

$$(a + I)(b + I) = ab + I.$$

(b) This part shows that the definition of addition in R/I given in the previous part actually makes senes, i.e., the result does not depend on the choice of representative for the coset. (There is a corresponding result showing that the definition of multiplication in R/I makes sense.) Let $a_1 + I = b_1 + I$ and $a_2 + I = b_2 + I$. Then $a_1 \in b_1 + I$ and so $a_1 = b_1 + z_1$ for some $z_1 \in I$. Similarly, $a_2 \in b_2 + I$ and so $a_2 = b_2 + z_2$ for some $z_2 \in I$. Now suppose $y \in a_1 + a_2 + I$. Then $y = a_1 + a_2 + x$ for some $x \in I$ and hence $y = (b_1 + z_1) + (b_2 + z_2) + x = b_1 + b_2 + (z_1 + z_2 + x)$. Since $z_1, z_2, x \in I$ and I is closed under addition (since it is an ideal) we have $z_1 + z_2 + x \in I$ and so $y \in (b_1 + b_2) + I$. Thus $(a_1 + a_2) + I \subseteq (b_1 + b_2) + I$. The reversed inclusion follows by symmetry and so the proof is complete.

#8 (a) Is $\{3n | n \in \mathbf{Z}\}$ a subring of $\mathbf{Z}$? Why or why not?

(b) Is $\{3n + 1 | n \in \mathbf{Z}\}$ a subring of $\mathbf{Z}$? Why or why not.

Solution:

(a) $\{3n | n \in \mathbf{Z}\}$ is a subring of $\mathbf{Z}$ since it is nonempty (for example, it contains 0), is closed under subtraction (as $3n_1 + 3n_2 = 3(n_1 + n_2)$) and multiplication (as $(3n_1)(3n_2) = 3(3n_1 n_2)$.

(b) $\{3n + 1 | n \in \mathbf{Z}\}$ is not a subring as it is not closed under addition (for $1 \in \{3n + 1 | n \in \mathbf{Z}\}$ and $1 + 1 = 2$ but $2 \notin \{3n + 1 | n \in \mathbf{Z}\}$. (An even quicker observation is that $0 \notin \{3n + 1 | n \in \mathbf{Z}\}$.

#9 Let U denote the set of upper triangular matrices in $M(\mathbf{R})$, D denote the set of diagonal matrices in $M(\mathbf{R})$, and N denote the set of strictly upper triangular matrices in $M(\mathbf{R})$.

(a) Verify that U and D are subrings of $M(\mathbf{R})$.

(b) Verify that N is an ideal in U.

(c) Show that the map $f : U \to D$ defined by $f(\begin{vmatrix} a & b \\ 0 & d \end{vmatrix}) = \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix}$ is a homomorphism of U onto D.

(d) Show that $D \cong U/N$.

Solution:

(a) Let $a, b, d, a'b'd' \in \mathbf{R}$. Note that both U and D are nonempty. Also

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

and

$$\begin{vmatrix} a & b \\ 0 & d \end{vmatrix}\begin{vmatrix} a' & b' \\ 0 & d' \end{vmatrix} = \begin{vmatrix} aa' & ab' + b'd \\ 0 & dd' \end{vmatrix}$$

These formulas show that U is closed under subtraction and multiplication and so is a subring. The same formulas wit $b = 0$ show that D is closed under subtraction and multiplication and so is a subring.

(b) Note that N is nonempty. Also the first formula in (a) shows that N is closed under addition, the second forumla in (a) with $a = d = 0$ shows that $NU \subseteq N$, and the second formula in (a) with $a' = d' = 0$ shows that $UN \subseteq N$. Thus N is an ideal in U.

(c) Let $A \in D$. Then $A = \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix}$ for some $a, d \in \mathbf{R}$. But then $A \in U$ and $f(A) = A$. Thus f is onto. Using the formulas from (a) we see that

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

$$\begin{vmatrix} a + a' & 0 \\ 0d + d' & \end{vmatrix} = \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix} + \begin{vmatrix} a' & 0 \\ 0 & d' \end{vmatrix} = f(\begin{vmatrix} a & b \\ 0 & d \end{vmatrix}) + f(\begin{vmatrix} a' & b' \\ 0 & d' \end{vmatrix}).$$

Also

$$f(\begin{vmatrix} a & b \\ 0 & d \end{vmatrix}\begin{vmatrix} a' & b' \\ 0 & d' \end{vmatrix}) = f(\begin{vmatrix} aa' & ab' + b'd \\ 0 & dd' \end{vmatrix} =$$

$$\begin{vmatrix} aa' & 0 \\ 0 & dd' \end{vmatrix} = \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix}\begin{vmatrix} a' & 0 \\ 0 & d' \end{vmatrix} = f(\begin{vmatrix} a & b \\ 0 & d \end{vmatrix})f(\begin{vmatrix} a' & b' \\ 0 & d' \end{vmatrix}).$$

Thus f is an isomorphism.

(d) All the work for this has already been done. By the 1st Isomorphism Theorem (applied to the surjective homomorphism f we have $N/(ker(f) \cong D$. Since it is clear that $ker(f) = N$, we are done.

#10 (a) Is the map $A \to\ tr(A)$ (where $tr(A)$ is the trace of the matrix A, i.e., the sum of its diagonal elememts) a homomorphism from $M(\mathbf{R})$ to $\mathbf{R}$? Why or why not?

(b) Is the map $A \to\ det(A)$ a homomorphsim from $M(\mathbf{R})$ to $\mathbf{R}$? Why or why not?

Solution:

(a) Let I denote the (2 by 2) identity matrix. Then $tr(I) = 2$ and so $2 = tr(I) = tr(II) \neq tr(I)tr(I) = 4$. Thus this map is not a homomorphism.

(b) Let e_{ij} denote the matrix with a 1 in the (i, j) position and 0 in all other positions. Then $e_{11} + e_{22} = I$, the identity matrix, so $det(e_{11} + e_{22} = detI = 1$ but $det(e_{11}) = det(e_{22}) = 0$ so $det(e_{11} + e_{22}) \neq det(e_{11}) + det(e_{22})$ and hence the map is not a homomorphsim.

#11 Let S_1 and S_2 be subrings of a ring R.

(a) Is $S_1 + S_2$ (which, by definition, is $\{a + b | a \in S_1, b \in S_2\}$) necessarily a subring of R? Why or why not?

(b) Is S_1S_2 (which, by definition, is $\{ab|a \in S_1, b \in S_2\}$ necessaily a subring of R? Why or why not?

(c) Suppose S_2 is an ideal of R. Is $S_1 + S_2$ necessarily a subring of R? Why or why not?

(d) Show that $S_1 \cap S_2$ is a subring of R.

Solution

(a) No. For example consider $N = \{\begin{vmatrix} 0 & b \\ 0 & 0 \end{vmatrix} |b \in \mathbf{R}\} \subseteq M(\mathbf{R})$ and $L = \{\begin{vmatrix} 0 & 0 \\ c & 0 \end{vmatrix} |b \in \mathbf{R}\} \subseteq M(\mathbf{R})$. Each of these is a subring, but $N + L = \{\begin{vmatrix} 0 & b \\ c & 0 \end{vmatrix} |b, c \in \mathbf{R}\}$ is not a subring since it does not contain the producd $e_{12}e_{21} = e_{11}$.

(b) Again, no. For example let $S_1 = \{\begin{vmatrix} a & 0 \\ b & 0 \end{vmatrix} |a, b \in \mathbf{R}\}$ and $S_2 = \{\begin{vmatrix} c & d \\ 0 & 0 \end{vmatrix} |c, d \in \mathbf{R}\}$. Then any matrix in S_1S_2 has rank one. Now $e_{11} = \begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix}$ is in both S_1 and S_2 so $e_{11} = e_{11}^2 \in S_1S_2$. Also $e_{22} = \begin{vmatrix} 0 & 0 \\ 1 & 0 \end{vmatrix} \begin{vmatrix} 0 & 1 \\ 0 & 0 \end{vmatrix} \in S_1S_2$. However, $e_{11} + e_{22}$, which is the identity matrix, has rank 2 and so is not in S_1S_2.

(c) Yes. Let $x_1, x_2 \in S_1 + S_2$. Then $x_1 = a_1 + b_1, x_2 = a_2 + b_2$ for some $a_1, a_2 \in S_1, b_1, b_2 \in S_2$ and so $x_1 - x_2 = (a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$. Since S_1 and S_2 are subrings, $a_1 - a_2 \in S_1$ and $b_1 - b_2 \in S_2$. Also $x_1x_2 = (a_1 + b_1)(a_2 + b_2) = a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2$. Since S_1 is a subring $a_1a_2 \in S_1$ and since S_2 is an ideal and $b_1, b_2 \in S_2$ we have $a_1b_2, b_1a_2, b_1b_2 \in S_2$. Thus $x_1x_2 \in S_1 + S_2$. Since $S_1 + S_2 \neq \emptyset$ (as, for example, it contains 0) we have that $S_1 + S_2$ is a subring of R.

(d) Since $0 \in S_1$ and $0 \in S_2$ we have $0 \in S_1 \cap S_2$ and so $S_1 \cap S_2 \neq 0$. Now let $x, y \in S_1 \cap S_2$. Then $x, y \in S_1$ and $x, y \in S_2$. Since S_1 and S_2 are subrings, we have $x - y \in S_1, x - y \in S_2, xy \in S_1, xy \in S_2$. Then $x - y \in S_1 \cap S_2$ and $xy \in S_1 \cap S_2$. Hence $S_1 \cap S_2$ is a subring of R.

#12 Prove that if $f(x), g(x), h(x) \in F[x]$ (where F is a field), $(f(x), g(x)) = 1$, and $f(x)$ divides $g(x)h(x)$, then $f(x)$ divides $h(x)$.

Solution: We know $1 = a(x)f(x) + b(x)g(x)$ for some $a(x), b(x) \in F[x]$. Then $h(x) = h(x)(a(x)f(x) + b(x)g(x)) = h(x)a(x)f(x) + b(x)g(x)h(x)$. Since $f(x)$ divides both summands in this expression, it divides $h(x)$.

#13 Prove that if $f(x) \in F[x]$ where F is a field, $a \in F$ and $f(a) = 0$ then $x - a$ divides $f(x)$.

lsolution: Since $x - a$ divides $f(x)$ we have $f(x) = (x - a)f(x)$. Now the evaluation $e_a : F[x] \to F$ defined by $e_a(g(x) = g(a)$ is a homomorphism and so

$$f(a) = e_a(f(x) = e_a((x - a)q(x)) = e_a(x - a)e_a(q(x)) = (a - a)q(a) = 0q(a) = 0.$$

$14 (a) Find all the irreducible polynomials of degree 3 over $\mathbf{Z}_2$.

(b) Find all the irreducible polynomials of degree 3 over $\mathbf{Z}_3$.
(c) Find all the irreducible polynomials of degree 4 over $\mathbf{Z}_2$.

Solution: In each part we will list all the polynomials which are not reducible.

(a) A polynomial of degree 3 over $\mathbf{Z}_2$ has the form $f(x) = x^3 + a_2x^2 + a_1x + a_0$ where each of a_2, a_1, a_0 is either 0 or 1. Note that we are writing 0 instead of [0] and 1 instead of [1]. Now $f(x)$ reducible if and only if it has a root. (Be aware that this statement applies only to polynomials of degree 2 or 3.) Now $f(0) = a_0$ and so $f(x)$ is reducible if $a_0 = 0$. If $a_0 = 1$ then $f(1) = 1 + a_2 + a_1 + 1 = a_2 + a_1$. Thus $f(x)$ is reducible if $a_1 = 1$ and $a_2 = a_1$. Thus the only irrecudible polynomials are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

(b) A polynomial of degree 3 over $\mathbf{Z}_3$ has the form $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ where $a_3 = 1$ or 2 (since $a_3 \neq 0$ as the polynomial has degree 3).

Assume first that $a_3 = 1$. Then $f(0) = a_0, f(1) = 1 + a_2 + a_1 + a_0, f(2) = 2 + a_2 + 2a_1 + a_0$. Thus $f(x)$ is irreducible if and only if $a_0 \neq 0, 1 + a_2 + a_1 + a_0 \neq 0$ and $2 + a_2 + 2a_1 + a_0 \neq 0$. The first inequality says $a_0 = 1$ or 2. Once a_0 is chosen we may take any value for a_1 and then take one of two values for a_2 in order to satisfy the second inequality. Thus there are 12 possible choices of a_0, a_1, a_2 that satisfy the first two inequalities. We check whether or not each of these 12 choices satisfies the third inequality and find that only 8 of them do. The complete list of corresponding polynomials (the monic irreducible polynomials of degree 3 over $\mathbf{Z}_3$ is:

$$x^3 + 2x + 1,$$

$$x^3 + x^2 + 2x + 1,$$

$$x^3 + 2x^2 + 1,$$

$$x^3 + 2x^2 + x + 1,$$

$$x^3 + 2x + 2,$$

$$x^3 + x^2 + 2,$$

$$x^3 + x^2 + x + 2,$$

$$x^3 + 2x^2 + 2x + 2.$$

If $a_3 = 2$, then $2f(x)$ is a monic irreducible polynomial and so is on the above list. Then $f(x) = 2(2f(x)$ is twice one of the polynomials on the above list.

(c) A polynomial of degree 4 is reducible if and only if it has or a root or it is the product of two irreducible polynomials of degree 2. Now a polynomial of degree 2 over $\mathbf{Z}_2$ has the form $x^2 + a_1x + a_0$ and $f(0) = a_0, f(1) = 1 + a_1 + a_0$. Thus this polynomial is irreducible if and only if $a_0 = 1$ and $a_1 = 1$. Hence there is only one irrecucible polynomial, $x^2 + x + 1$, of degree 2 over $\mathbf{Z}_2$. Its square is $x^4 + x^2 + 1$.

A polynomial of degree 4 over $\mathbf{Z}_2$ has the form $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ where each of a_3, a_2, a_1, a_0 is either 0 or 1. Now $f(0) = a_0, f(1) = 1 + a_3 + a_2 + a_1 + a_0$. Thus $f(x)$ has no root if and only if $a_0 = 1$ and $a_3 + a_2 + a_1 = 1$. Since the polynomial

x^4+x^2+1 is reducible (by the result of the previous paragraph) we have that the irreducible polynomials are:

$$x^4+x^3+x^2+x+1$$

$$x^4+x^3+1$$

$$x^4+x+1$$

.