

Math 351 (Section 03)  
Exam #1 Answer Key  
October 2006

1. (10 points) This is a “gimmie”

(a) Write out the definition of a ring – give me all of the gory details please!

**Answer:** See the basic definitions handout.

(b) Give the definition of the greatest common divisor of two polynomials  $f(x)$  and  $g(x)$  in  $\mathbb{F}[x]$  where  $\mathbb{F}$  is a field (and either  $f(x) \neq 0$  or  $g(x) \neq 0$ ).

A **monic** polynomial  $d(x) \in \mathbb{F}[x]$  is called the **greatest common divisor** of  $f(x)$  and  $g(x)$  if  $d(x)$  divides  $f(x)$ ,  $d(x)$  divides  $g(x)$ , and  $d(x)$  has the largest possible degree among all common divisors of  $f(x)$  and  $g(x)$ .

2. (25 points) Circle “True” if the statement is always true, “Possible” if the statement is true for some examples but false for others, or “False” if the statement is never true. **Then justify your choice!**

(a) Let  $a, b, u,$  and  $v$  be integers such that  $au + bv = 2$ .

**TRUE** / **POSSIBLE** / **FALSE**: The greatest common divisor of  $a$  and  $b$  is 2.

If  $au + bv = 2$ , then we know that 2 is a multiple of the g.c.d. of  $a$  and  $b$ . So  $a$  and  $b$  could be relatively prime, or they could have the g.c.d. 2.

Example:  $2(-1) + 4(1) = 2$  the g.c.d. of:  $a = 2$  and  $b = 4$  is 2 OR  $a = -1$  and  $b = 1$  is 1.

(b) Let  $y \in \mathbb{Z}$ .

**TRUE** / **POSSIBLE** / **FALSE**: The equation  $2x \equiv y \pmod{999}$  has a solution  $x \in \mathbb{Z}$ .

Since 2 is relatively prime to 999, we know 2 is a unit in  $\mathbb{Z}_{999}$ . Thus  $x = 2^{-1}y$  is a solution no matter what  $y$  happens to be.

Alternatively, since 2 is relatively prime to 999 we can find  $u, v \in \mathbb{Z}$  such that  $2u + 999v = 1$ . Therefore,  $2(uy) + 999(vy) = y$  which means  $2(uy) \equiv y \pmod{999}$  ( $x = uy$  is a solution).

(c) Let  $n$  be a positive integer.

**TRUE** / **POSSIBLE** / **FALSE**: Both cancellation laws hold in  $\mathbb{Z}_n$ .

Cancellation laws hold in an integral domain and fail if there are zero divisors. We know  $\mathbb{Z}_3$  is an integral domain (because 3 is prime), so the cancellation laws hold in  $\mathbb{Z}_3$ . However,  $\mathbb{Z}_6$  is not an integral domain because it has zero divisors, so the cancellation laws do not hold in  $\mathbb{Z}_6$ .

(d) Let  $\mathbb{F}$  be a field.

**TRUE** / **POSSIBLE** / **FALSE**:  $\mathbb{F} \cong M(\mathbb{F})$ .

We know that  $\mathbb{F}$  is commutative (since it's a field). But  $M(\mathbb{F})$  is not commutative for any field  $\mathbb{F}$ . Thus they can never be isomorphic.

Example of non-commuting matrices:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

(e) Let  $\mathbb{F}$  be a field, and let  $f(x) \in \mathbb{F}[x]$  be a polynomial of degree 5 such that  $f(x)$  has no irreducible factors of degree 3 or 4.

**TRUE** / **POSSIBLE** / **FALSE**:  $f(x)$  is irreducible.

Almost by the definition of irreducible, if  $f(x)$  is irreducible of degree 5, it cannot have factors of degree 3 or 4. So for example  $f(x) = x^5 + 2$  is irreducible (by Eisenstein's criterion) in  $\mathbb{Q}[x]$  (thus has no factors of degree 3 or 4).

On the other hand,  $f(x) = x^5$  is not irreducible in  $\mathbb{Q}[x]$  (or in fact over any field). Notice that the irreducible factors of  $f(x)$  are  $x, x, x, x,$  and  $x$  (thus by the uniqueness of factorizations,  $f(x)$  has no irreducible factors of degree 3 or 4).

### 3. (10 points) Basics

(a) Let  $R$  be a ring with 1. Prove that  $1 = 0$  if and only if  $R = \{0\}$  (the trivial ring).

Suppose that  $1 = 0$ . Let  $a \in R$ . Then  $a = a1 = a0 = 0$ . Thus all elements of  $R$  are 0. So  $R = \{0\}$ .

Suppose that  $R = \{0\}$ . We have  $0a = a = a0$  for all  $a \in R$  (since  $00 = 0$ ). Thus 0 is the multiplicative identity. Therefore  $1 = 0$ .

(b) Let  $R$  be a ring with 1 and  $r \in R$ . Show that  $r$  cannot be both a zero divisor and a unit.

Suppose that  $r$  is both a zero divisor and a unit. This implies that there exists  $r^{-1} \in R$  such that  $rr^{-1} = r^{-1}r = 1$ . Also, there exists some  $s \in R, s \neq 0$  such that  $rs = 0$  or  $sr = 0$ .

If  $rs = 0$ , then  $r^{-1}rs = r^{-1}0$ . Thus  $s = 1s = 0$  (contradiction).

If  $sr = 0$ , then  $srr^{-1} = 0r^{-1}$ . Thus  $s = s1 = 0$  (contradiction).

Thus  $r$  cannot be both a zero divisor and a unit!

### 4. (10 points) Choices! Prove ONE of the following:

I. Let  $R$  be a ring where  $a^2 = a$  for each  $a \in R$ . Show that  $R$  is commutative. *Hint*: For all  $a, b \in R$ ,  $(a+b)^2 = (a+b)$  and  $(a+a)^2 = (a+a)$ .

Let  $a, b \in R$ . Consider  $a+a = (a+a)^2 = (a+a)(a+a) = a^2+a^2+a^2+a^2 = a+a+a+a$ . Thus  $0 = a+a$ . So  $a = -a$ . Also,  $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$ . Therefore,  $0 = ab+ba$ . Thus  $ab = -ba = ba$ . So  $R$  is commutative.

II. Let  $R$  be a ring with 1. Prove that the characteristic of  $R$  and the characteristic of  $M(R)$  are the same.

Let  $n \in \mathbb{Z}_{>0}$ . Suppose that  $n1 = 0$ . Then  $n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} n1 & 0 \\ 0 & n1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . Conversely if  $n \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . Then  $\begin{pmatrix} n1 & 0 \\ 0 & n1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ . Thus  $n1 = 0$ .  
So  $n1 = 0$  if and only if  $nI_2 = 0$ . Therefore,  $R$  and  $M(R)$  have the same characteristic.

**5. (10 points)** Let  $\phi : R \rightarrow S$  be a homomorphism from a ring  $R$  to a ring  $S$ . Also, let  $T$  be a subring of  $R$ . Prove that  $\phi(T) = \{\phi(x) \in S \mid x \in T\}$  is a subring of  $S$ .

Obviously  $\phi(T)$  is a subset of  $S$  (since  $\phi$  is a mapping into  $S$ ).

First notice that  $0 \in T$  (since  $T$  is a subring). Therefore,  $0 = \phi(0) \in \phi(T)$ . Next, suppose that  $a, b \in \phi(T)$ . This implies that there exists  $x, y \in T$  such that  $\phi(x) = a$  and  $\phi(y) = b$ . Now we know that  $T$  is a subring, so  $x - y \in T$ . Thus  $a - b = \phi(x) - \phi(y) = \phi(x - y) \in \phi(T)$ . Also,  $xy \in T$  (since  $T$  is a subring). Thus  $ab = \phi(x)\phi(y) = \phi(xy) \in \phi(T)$ .

Therefore, by the (short) subring test  $\phi(T)$  is a subring of  $S$ .

**6. (12 points)** Workin' in  $\mathbb{Z}_9$ .

(a) Write the multiplication table for  $\mathbb{Z}_9$ .

$\mathbb{Z}_9, \times$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

(b) List all of the members of  $U(\mathbb{Z}_9)$ .

From the table we see that:  $1^{-1} = 1$ ,  $2^{-1} = 5$ ,  $4^{-1} = 7$ ,  $5^{-1} = 2$ ,  $7^{-1} = 4$ , and  $8^{-1} = 8$ .  
 $U(\mathbb{Z}_9) = \{1, 2, 4, 5, 7, 8\}$  (i.e. all numbers relatively prime to 9).

(c) List all of the zero divisors in  $\mathbb{Z}_9$ .

Again from our table we see that  $3 \cdot 3 = 0$  and  $6 \cdot 3 = 0$ . Thus 3 and 6 are the zero divisors of  $\mathbb{Z}_9$ .

- (d) Is  $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$  a unit of  $M(\mathbb{Z}_9)$ ? If so, find its inverse. If not, explain why.

Recall that the formula for the inverse of a 2 by 2 matrix is:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = (ad - bc)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

So the inverse exists if  $(ad - bc)$  is a unit. So for our matrix  $(ad - bc) = (1(4) - 2(3)) = -2 \equiv 7 \pmod{9}$ . We know from part (b) that 7 is a unit and  $7^{-1} = 4$ . Thus the inverse exists.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = 7^{-1} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} = 4 \begin{pmatrix} 4 & 7 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 7 & 1 \\ 6 & 4 \end{pmatrix}$$

### 7. (12 points) Isomorphisms.

- (a) Is  $\mathbb{Q}$  isomorphic to  $\mathbb{Z}$ ? Why or why not?

No.  $\mathbb{Q}$  is not isomorphic to  $\mathbb{Z}$  for many reasons. For example,  $\mathbb{Z}$  is not a field, but  $\mathbb{Q}$  is. Related to this is the fact that  $\mathbb{Z}$  has exactly two units ( $\pm 1$ ) whereas  $\mathbb{Q}$  has infinitely many units (every nonzero rational is a unit).

- (b) Is  $\mathbb{R} \times \mathbb{R}$  isomorphic to the subring of 2x2 real diagonal matrices  $D = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$ ?

Why or why not?

Yes. These rings are isomorphic. Consider the map  $\phi : \mathbb{R} \times \mathbb{R} \rightarrow D$  defined by  $\phi(a, b) = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ . First, notice that  $\phi$  does in fact map  $\mathbb{R} \times \mathbb{R}$  into  $D$ .

Next, if  $\phi(a, b) = \phi(c, d)$  then  $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix}$ . Thus  $a = c$  and  $b = d$ , so  $(a, b) = (c, d)$ . Therefore  $\phi$  is injective.

Also, let  $A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \in D$ . Then  $\phi(a, b) = A$ . Thus  $\phi$  is surjective.

Finally, notice that

$$\phi((a, b) + (c, d)) = \phi(a + c, b + d) = \begin{pmatrix} a + c & 0 \\ 0 & b + d \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} + \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \phi(a, b) + \phi(c, d)$$

and

$$\phi((a, b)(c, d)) = \phi(ac, bd) = \begin{pmatrix} ac & 0 \\ 0 & bd \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \begin{pmatrix} c & 0 \\ 0 & d \end{pmatrix} = \phi(a, b)\phi(c, d)$$

for all  $a, b, c, d \in \mathbb{R}$ . Thus  $\phi$  is a homomorphism.

Hence,  $\phi$  is an isomorphism from  $\mathbb{R} \times \mathbb{R}$  to  $D$  which proves that these rings are isomorphic.

- (c) Is  $M(\mathbb{Z}_2)$  isomorphic to  $\mathbb{Z}_{16}$ ? Why or why not?

No. These rings are not isomorphic. Notice that  $M(\mathbb{Z}_2)$  is not a commutative ring whereas  $\mathbb{Z}_{16}$  is. Another way to see that they are not isomorphic is to notice that the characteristic of  $M(\mathbb{Z}_2)$  is 2, and the characteristic of  $\mathbb{Z}_{16}$  is 16.



$$\begin{array}{r}
 x^3 \quad +1 \\
 \hline
 x^2 + x + 2 \left) \begin{array}{r}
 x^5 + x^4 + 2x^3 + x^2 + x + 1 \\
 -x^5 - x^4 - 2x^3 \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} + x^2 + x + 1 \\
 \phantom{x^5 + x^4 + 2x^3} -x^2 - x - 2 \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} \phantom{+ x^2 + x + 1} \phantom{-x^2 - x - 2} \\
 \text{a nonzero remainder} \rightarrow 2
 \end{array}
 \end{array}$$

$$\begin{array}{r}
 x^3 + 2x^2 + 2x + 2 \\
 \hline
 x^2 + 2x + 2 \left) \begin{array}{r}
 x^5 + x^4 + 2x^3 + x^2 + x + 1 \\
 -x^5 - 2x^4 - 2x^3 \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} 2x^4 \phantom{+ x^2 + x + 1} \\
 \phantom{x^5 + x^4 + 2x^3} -2x^4 - x^3 - x^2 \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} \phantom{-2x^4 - x^3 - x^2} 2x^3 + x + 1 \\
 \phantom{x^5 + x^4 + 2x^3} \phantom{-2x^4 - x^3 - x^2} -2x^3 - x^2 - x \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} \phantom{-2x^4 - x^3 - x^2} \phantom{-2x^3 - x^2 - x} 2x^2 + 1 \\
 \phantom{x^5 + x^4 + 2x^3} \phantom{-2x^4 - x^3 - x^2} \phantom{-2x^3 - x^2 - x} -2x^2 - x - 1 \\
 \hline
 \phantom{x^5 + x^4 + 2x^3} \phantom{-2x^4 - x^3 - x^2} \phantom{-2x^3 - x^2 - x} \phantom{2x^2 + 1} \\
 \text{a nonzero remainder} \rightarrow 2x
 \end{array}
 \end{array}$$

So we see that the three irreducible monics of degree 2 do not divide  $x^5 + x^4 + 2x^3 + x^2 + x + 1$ . Therefore, we conclude that it must be irreducible.