Math 228 (R1) Final Exam

April 20, 2009

Instructor: Matilde N. Lalín

NAME:

SID:

1. This exam consists of 8 pages, including this one.
2. No books, notes, or electronic devices are allowed.
3. Ensure that **your *full* name and student number** appear on this page.
4. Read the questions carefully before starting to work.
5. **Justify your answers. Show all your work**
6. Continue on the back of the page if you run out of space.
7. The total mark will be multiplied by $\frac{4}{3}$ and rounded to the closest integer in order to give the final mark.

Question:	1	2	3	4	5	6	7	Total
Points:	14	6	10	8	6	10	21	75
Score:								

1. (a) (6 points) Factor the polynomial $3x^4+2x^3+2x^2+2x-1$ into irreducible polynomials in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$.

   (b) (2 points) For what values of k is $x+1$ a factor of $x^4+2x^3-3x^2+kx+1$ in $\mathbb{Z}_5[x]$? Justify.

   (c) (6 points) Show that the following polynomials are irreducible in $\mathbb{Q}[x]$:
   (i) $4x^5+3x^4-12x^2+3$
   (ii) $x^4+7x^3+14x^2+3$

Solution: (a) First we look for rational roots for $f(x)=3x^4+2x^3+2x^2+2x-1$. By the rational root theorem, a rational root $\frac{r}{s}$ (in lowest terms) must verify that $r|1$ and $s|3$. We try with -1.

$$f(-1)=3-2+2-2-1=0$$

Therefore, we can divide the polynomial by $(x+1)$.

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

Now we look at the polynomial $g(x)=3x^3-x^2+3x-1$. We try with $\frac{1}{3}$.

$$g\left(\frac{1}{3}\right)=3\left(\frac{1}{3}\right)^3-\left(\frac{1}{3}\right)^2+3\left(\frac{1}{3}\right)-1=0.$$

Then

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

The roots of x^2+1 are $x=\pm i$, which are complex and not real. Since it is a degree 2 polynomial, it is irreducible in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$. Therefore:

Factorization in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$:

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

Factorization in $\mathbb{C}[x]$:

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

(b) $x+1$ is a factor of $f(x)=x^4+2x^3-3x^2+kx+1$ in $\mathbb{Z}_5[x]$ iff -1 is a root.

We check:

$$f(-1)=1-2-3-k+1=2-k.$$

In order to get zero we need $k=2$. Therefore, that is the answer.

(c)(i) We notice that 3 divides all the coefficients of $4x^5+3x^4-12x^2+3$ except for the leading coefficient. Furthermore, $3^2 \not| 3$ (the independent coefficient). Therefore, the polynomial is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion.

(ii) We reduce modulo 2: $x^4+7x^3+14x^2+3 = x^4+x^3+1$ in $\mathbb{Z}_2[x]$. The polynomial x^4+x^3+1 does not have roots in $\mathbb{Z}_2$, since it equals 1 when $x=0$ or $x=1$. Now we look for degree 2 irreducible factors. The degree 2 polynomials in $\mathbb{Z}_2[x]$ are x^2, x^2+x, x^2+1 and x^2+x+1. The first two are reducible with $x=0$ root. The third one is reducible, with $x=1$ root. The last one is irreducible, with no roots in $\mathbb{Z}_2$. Therefore, that is the only possible factor. But $(x^2+x+1)^2 = x^4+x^2+1 \neq x^4+x^3+1$. Then the polynomial x^4+x^3+1 is irreducible in $\mathbb{Z}_2[x]$ and therefore, $x^4+7x^3+14x^2+3$ is irreducible in $\mathbb{Q}[x]$.

2. (a) (2 points) There is exactly one element $n \in \mathbb{Z}_8$ such that $n \neq [0]$ but $n^2 = [0]$. Find this n.

   (b) (1 point) In the polynomial ring $\mathbb{Z}_8[x]$ with the same n as in part (a), prove that

$$([1] + nx)([1] - nx) = [1]$$

   (c) (3 points) In the polynomial ring $\mathbb{Z}_8[x]$ with the same n as in part (a), prove that $u = [1] + nf(x)$ is a unit of $\mathbb{Z}_8[x]$, for any polynomial $f(x) \in \mathbb{Z}_8[x]$.

Solution: (a) $n = [4]$, since $[4]^2 = [16] = [0]$.

(b)

$$([1] + [4]x)([1] - [4]x) = [1] + [4]x - [4]x + [4]^2x^2 = [1]$$

(c)

$$([1] + [4]f(x))([1] - [4]f(x)) = [1] + [4]f(x) - [4]f(x) + [4]^2f(x)^2 = [1]$$

since the ring is commutative, we also have $([1] - [4]f(x))([1] + [4]f(x)) = [1]$. Therefore, $[1] + [4]f(x)$ is a unit.

3. Consider $f(x) = x^3 + x^2 + 1 \in \mathbb{Z}_2[x]$.

   (a) (3 points) Prove that $\mathbb{Z}_2[x]/(f(x))$ is a field.

   (b) (2 points) How many elements does this field have?

   (c) (2 points) Find an integer n such that $\mathbb{Z}_n$ has as many elements as $\mathbb{Z}_2[x]/(f(x))$ does. Decide whether the ring $\mathbb{Z}_2[x]/(f(x))$ and the ring $\mathbb{Z}_n$ for the integer n that you found are isomorphic. If so, give an isomorphism between them, if not, explain why not.

   (d) (3 points) Let $\alpha = [x] \in \mathbb{Z}_2[x]/(f(x))$. Then α is a root of $f(x)$ (you do not have to prove this). Prove that α^2 is also a root of $f(x)$.

Solution: (a) We see that $f(0) = f(1) = 1$, therefore, f has no roots in $\mathbb{Z}_2$. Since it has degree 3, it is irreducible. Then $\mathbb{Z}_2[x]/(f(x))$ is a field.

(b) The elements in this field may be described as $[ax^2 + bx + c]$ with $a, b, c \in \mathbb{Z}_2$. Therefore, it has $2^3 = 8$ elements.

(c) We take $n = 8$, so $\mathbb{Z}_8$ has eight elements. However, it is not isomorphic to $\mathbb{Z}_2[x]/(f(x))$ since the former is not a field.

(d) We need to evaluate $f(\alpha^2)$.

$$\alpha^3 + \alpha^2 + 1 = 0$$

$$(\alpha^3 + \alpha^2 + 1)^2 = 0 = \alpha^6 + \alpha^4 + 1 = (\alpha^2)^3 + (\alpha^2)^2 + 1.$$

Therefore, α^2 is a root as well.

4. (a) (4 points) Is 313 a unit in $\mathbb{Z}_{343}$? If yes, find its inverse; otherwise show that it is a zero divisor.

   (b) (4 points) Let r, s be integers. Prove that r is a zero-divisor in $\mathbb{Z}_s$ if and only if s is a zero-divisor in $\mathbb{Z}_r$.

Solution: (a) We compute the greatest common divisor of 313 and 343 using the Euclidean algorithm

$$343 = 313 \cdot 1 + 30$$

$$313 = 30 \cdot 10 + 13$$

$$30 = 13 \cdot 2 + 4$$

$$13 = 4 \cdot 3 + 1$$

$$4 = 1 \cdot 4$$

Therefore, $(343, 313) = 1$ which implies that 313 is a unit in $\mathbb{Z}_{343}$. In order to find the inverse, we use the linear combination: $1 = 13 - 4 \cdot 3 = 13 - (30 - 13 \cdot 2)3 = 13 \cdot 7 - 30 \cdot 3 = (313 - 30 \cdot 10)7 - 30 \cdot 3 = 313 \cdot 7 - 30 \cdot 73 = 313 \cdot 7 - (343 - 313)73 = 313 \cdot 80 - 343 \cdot 73$.

Therefore, the inverse of 313 in $\mathbb{Z}_{343}$ is 80.

(b) r is a zero-divisor in $\mathbb{Z}_s$ if and only if there is a $t \neq 0$ such that $rt = 0$ in $\mathbb{Z}_s$. This implies that $s|rt$, and $s \not| t$. Therefore, $(s, r) = d > 1$, since $(s, r) = 1$ would imply that $s|t$. Now take $h = \frac{r}{d}$. Then $h \neq 0$ in $\mathbb{Z}_r$, but $r|hs$, which implies $hs = 0$ in $\mathbb{Z}_r$, and s is a zero-divisor.

5. All the ideals in this question are ideals of the ring $\mathbb{Z}[x]$. Let I be the ideal of polynomials whose constant coefficient is even.

   (a) (2 points) Give an element in I that is not contained in (2) and an element in I that is not contained in (x). (No justification necessary).

   (b) (4 points) Show that the ideal generated by x and 2 in the ring $\mathbb{Z}[x]$ is equal to I.

Solution:

(a) $2, x \in I$ while $2 \notin (x)$ and $x \notin (2)$.

(b) 2 and x belong to I, which implies $(x, 2) \subset I$. Now let $f(x) \in I$. Then $f(x) = a_n x^n + \ldots + a_1 x + a_0$ with a_0 even, so we can write $a_0 = 2b$. Then $f(x) = (a_n x^{n-1} + \ldots + a_1)x + b2 \in (x, 2)$. Therefore, $I \subset (x, 2)$.

6. (10 points) Answer TRUE of FALSE. No justification is necessary.

   Let $a, b, c \in \mathbb{Z} \neq 0$.

   (a) If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$

   (b) If $a|bc$, then $a|b$ or $a|c$

   (c) Let $u, v, d \in \mathbb{Z}$ such that $au + bv = d$, then $(a, b) = d$.

   (d) If $e, f, g \in R$ where R is a ring and $ef = eg$, then $f = g$.

   (e) Let n be a positive integer such that whenever $ef = 0$ in $\mathbb{Z}_n$ we have $e = 0$ or $f = 0$ in $\mathbb{Z}_n$. Then n is prime.

   (f) Let F be a field and let $f(x) \in F[x]$. If $f(x)$ is reducible in $F[x]$, then $f(x)$ has a root in F.

   (g) Let R be a commutative ring and let $f(x), g(x) \in R[x]$ and nonzero. Then $\deg(f(x)g(x)) \leq \deg(f(x)) + \deg(g(x))$.

   (h) Let F be a field and let $f(x) \in F[x]$ be a polynomial of degree n. Then $f(x)$ has n roots in F.

   (i) The rings $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are isomorphic.

   (j) The polynomial $x^5 - 2x + 1$ is irreducible over $\mathbb{Z}_7[x]$.

Solution: (a) True (b) False (c) False (d) False (e) True (f) False (g) True (h) False (i) False (j) False

7. Let $T = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \middle| \, a \in \mathbb{R}, b \in \mathbb{R} \right\} \subset M_2(\mathbb{R})$.

(a) (5 points) Prove that T is a subring of $M_2(\mathbb{R})$ with multiplicative identity.

(b) (2 points) What are the units in T? (no justification, just the answer)

(c) (2 points) What are the zero divisors in T? (no justification, just the answer)

(d) (4 points) Consider $f : T \to \mathbb{R}$ defined by $f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) = a$. Prove that f is a homomorphism. Is it surjective? Is it injective? Justify.

(e) (3 points) Is $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| \, b \in \mathbb{R} \right\}$ an ideal of T? Justify.

(f) (3 points) Is I an ideal of $M_2(\mathbb{R})$? Justify.

(g) (2 points) Are I and $\mathbb{R}$ isomorphic? Justify.

Solution: (a) Let $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} \in T$. Then

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix} \in T$$

so T is closed under addition.

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix} \in T$$

so T is closed under multiplication. Also, taking $a = b = 0$, we have that $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in T$. Finally, the additive inverse of $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ is $\begin{pmatrix} -a & -b \\ 0 & -a \end{pmatrix}$, which is also an element of T.

Therefore, T is a subring of $M_2(\mathbb{R})$.

The multiplicative identity is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in T$.

(b) The multiplicative units are the elements of the form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ with $a \neq 0$.

(c) The zero divisors are the elements of the form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ with $b \neq 0$.

(d)

$$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} + \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = f\left(\begin{pmatrix} a+c & b+d \\ 0 & a+c \end{pmatrix}\right) = a + c$$

$$= f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) + f\left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right)$$

$$f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right) = f\left(\begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}\right) = ac$$

$$= f\left(\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\right) \cdot f\left(\begin{pmatrix} c & d \\ 0 & c \end{pmatrix}\right)$$

Therefore, it is a homomorphism.

It is surjective, since for any $a \in \mathbb{R}$, we have $a = f\left(\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}\right)$.

It is not injective, since $f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1 = f\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right)$.

(e) I is an ideal of T. Let $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} \in I$. Then the difference

$$\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & b-c \\ 0 & 0 \end{pmatrix} \in I.$$

For multiplication, we have

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix} \in I$$

$$\begin{pmatrix} 0 & c \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & ac \\ 0 & 0 \end{pmatrix} \in I$$

therefore, I is an ideal of T.

(f) I is not an ideal of $M_2(\mathbb{R})$.

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin I$$

(g) I and $\mathbb{R}$ are not isomorphic since all the elements in I are zero divisors, but $\mathbb{R}$ is a field, with no zero divisors.