

<i>Problem</i>	1	2	3	4	5	<b>Bonus:</b>	<b>Total:</b>
<i>Scores</i>							

MAT 534 – ALGEBRA I – FALL 2005

Name: \_\_\_\_\_

**Test 1** (December 1 / 80 minutes)

1. Denote by  $\mathbb{F}$  the subset of  $\mathbb{R}$  consisting of all elements of the form  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ , where  $a$ ,  $b$  and  $c$  are rational numbers.

(a) Verify that that  $\mathbb{F}$  is closed under addition, subtraction and multiplication, i.e.  $\mathbb{F}$  is a subring of  $\mathbb{R}$ . Show that  $\mathbb{F}$  is isomorphic to the quotient ring  $\mathbb{Q}[x]/(x^3 - 2)$ .

(b) Show that  $\mathbb{F}$  is a field.

(a) First,  $F$  is closed under addition and subtraction:

$$(a + b\sqrt[3]{2} + c\sqrt[3]{4}) \pm (a' + b'\sqrt[3]{2} + c'\sqrt[3]{4}) = (a \pm a') + (b \pm b')\sqrt[3]{2} + (c \pm c')\sqrt[3]{4}.$$

Then  $F$  is also closed under multiplication by rational numbers:

$$a'(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = (a'a + a'b\sqrt[3]{2} + a'c\sqrt[3]{4}).$$

Since multiplication is distributive, it is enough to check that all pairwise products of  $\sqrt[3]{2}$  and  $\sqrt[3]{4}$  belong to  $\mathbb{F}$ :

$$\sqrt[3]{2}^2 = \sqrt[3]{4}, \quad \sqrt[3]{2} \cdot \sqrt[3]{4} = 2, \quad \sqrt[3]{4}^2 = 2\sqrt[3]{2}.$$

The map  $a + b\sqrt[3]{2} + c\sqrt[3]{4} \mapsto a + bx + cx^2 \pmod{(x^3 - 2)}$  is an isomorphism between  $\mathbb{F}$  and  $\mathbb{Q}[x]/(x^3 - 2)$ . It respects addition by definition and respects multiplication since  $x \cdot x^2 = 2 \pmod{(x^3 - 2)}$  and  $x^2 \cdot x^2 = 2x \pmod{(x^3 - 2)}$ .

(b) We use the isomorphism  $\mathbb{F} \simeq \mathbb{Q}[x]/(x^3 - 2)$  to show that each element in  $\mathbb{F}$  has the inverse. Since the polynomial  $f(x) = x^3 - 2$  does not have rational roots, the only divisors of  $f$  are scalar multiples of 1 and  $f$ . Hence, if  $g(x) = ax^2 + bx + c$  is a polynomial of degree less than 3 then the greatest common divisor of  $f$  and  $g$  is 1. Since  $\mathbb{Q}[x]$  is a P.I.D., we have that  $h_1f + h_2g = 1$  for some polynomials  $h_1$  and  $h_2$ . Then  $h_2 \pmod{(x^3 - 2)}$  is the inverse of  $g \pmod{(x^3 - 2)}$  in  $\mathbb{F}$ .

Another proof uses Problem 2. Multiplication by any element  $a \in \mathbb{F}$  is a linear operator  $M_a$  on  $\mathbb{F}$ , and  $\mathbb{F}$  does not have zero divisors. Hence,  $M_a$  is onto. Indeed, since  $ab \neq 0$  for all  $b \in \mathbb{F} \setminus \{0\}$ , the kernel of  $M_a$  is trivial, and the image is the whole  $\mathbb{F}$ . Then the preimage of 1 is the inverse of  $a$ , since  $a \cdot M_a^{-1}(1) = 1$ .

2. Let  $\mathbb{F}$  be as in Problem 1.

(a) Verify that  $\mathbb{F}$  is a vector space over the field of rational numbers  $\mathbb{Q}$ , and find its dimension. Find a basis in  $\mathbb{F}$ .

(b) Verify that for any  $a \in \mathbb{F}$ , the map

$$M_a : \mathbb{F} \rightarrow \mathbb{F}; \quad M_a : x \mapsto ax$$

is a  $\mathbb{Q}$ -linear operator. For  $a = \sqrt[3]{2}$ , find the matrix of  $M_a$  with respect to the basis you found in part (a).

(c) Let  $a = \sqrt[3]{2}$ . Find the characteristic polynomial of  $M_a$ . Does  $M_a$  have any nonzero eigenvectors in the vector space  $\mathbb{F}$ ?

(a) We already checked in Problem 1 that  $\mathbb{F}$  is closed under addition and multiplication by rational numbers. A natural basis is  $1, \sqrt[3]{2}$  and  $\sqrt[3]{4}$ , since these three vectors span  $\mathbb{F}$  over  $\mathbb{Q}$  and are linearly independent. Indeed, if  $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$ , then  $\sqrt[3]{2}$  is the root of the polynomial  $a + bx + cx^2$ . So the greatest common divisor of  $a + bx + cx^2$  and  $x^3 - 2$  is not a constant polynomial. Hence, it is  $x^3 - 2$ , and  $a = b = c = 0$ .

(b) The  $\mathbb{Q}$ -linearity of  $M_a$  follows from the fact that  $\mathbb{F}$  is a commutative ring containing  $\mathbb{Q}$ . Hence,  $M_a$  respects addition because of distributivity, and commutes with multiplication by any  $r \in \mathbb{Q}$  because  $ar = ra$ . Actually, operators  $M_a$  for all  $a \in \mathbb{F}$  commute with each other. The matrix of  $M_a$  in the basis  $1, \sqrt[3]{2}, \sqrt[3]{4}$  for  $a = \sqrt[3]{2}$  is

$$\begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

(c) By definition of  $M_a$ , the operator  $M_a^3$  is the operator of multiplication by  $a^3$ . If  $a = \sqrt[3]{2}$ , then  $M_a^3 = 2I$ . So the characteristic polynomial of  $M_a$  is  $x^3 - 2$  because it is irreducible of degree 3 and annihilates  $M$ .

Since none of the eigenvalues of  $M_a$  lies in  $\mathbb{Q}$ , this operator does not have any nonzero eigenvectors in the vector space  $\mathbb{F}$  (regarded as a vector space over  $\mathbb{Q}$ ).

**Remark:** Note that if we regard  $\mathbb{F}$  as a vector space over  $\mathbb{F}$  (not over  $\mathbb{Q}$ ), and  $M_a$  as an  $\mathbb{F}$ -linear operator, then the answers for all questions change significantly (although from the set theoretic point of view the set  $\mathbb{F}$  and the map  $M_a$  are the same in both cases). The dimension of  $\mathbb{F}$  will be 1, a possible basis is  $\{1\}$ . The matrix of  $M_a$  for  $a = \sqrt[3]{2}$  will be the  $1 \times 1$  matrix  $\sqrt[3]{2}$ . The characteristic polynomial will be the linear polynomial  $x - \sqrt[3]{2}$ , and  $1 \in \mathbb{F}$  will be an eigenvector with the eigenvalue  $\sqrt[3]{2}$ .

3. Consider the sequence  $a_0, a_1, a_2, \dots$  given by the formula

$$a_{n+1} = 2(a_n - a_{n-1}),$$

$$a_0 = a_1 = 1.$$

Find  $a_{50}$ .

Consider the collection of vectors  $v_n = (a_n, a_{n+1})$  in the coordinate plane. Then the vector  $v_n$  is the image of the vector  $v_{n-1}$  under the action of the operator

$$A = \begin{pmatrix} 0 & 1 \\ -2 & 2 \end{pmatrix}.$$

Hence,  $v_{50} = A^{50}(v_0)$ . The eigenvalues of  $A$  are  $1 + i$  and  $1 - i$ , and the corresponding eigenvectors are  $u_1 = (1, 1 + i)$  and  $u_2 = (1, 1 - i)$ . Since  $v_0 = \frac{1}{2}(u_1 + u_2)$ , we have that  $A^{50}(v_0) = \frac{1}{2}(A^{50}(u_1) + A^{50}(u_2)) = \frac{1}{2}((1 + i)^{50}u_1 + (1 - i)^{50}u_2)$ . Hence  $a_{100} = [(1 + i)^{50} + (1 - i)^{50}]/2 = 0$ , because  $(1 + i)^{50} = (2i)^{25} = (1 - i)^{50}$ .

4. Let  $R$  be a commutative ring with 1. Show that the principal ideal generated by  $x$  in the polynomial ring  $R[x]$  is a prime ideal if and only if  $R$  is an integral domain. Prove that  $(x)$  is a maximal ideal if and only if  $R$  is a field.

First, note that a polynomial  $f \in R[x]$  belongs to the ideal  $(x)$  if and only if  $f(0) = 0$ .

Let  $f$  and  $g$  be two polynomials in  $R[x]$  such that  $fg \in (x)$ . Then  $f(0)g(0) = fg(0) = 0$ . If  $R$  is an integral domain, then either  $f(0)$  or  $g(0)$  is zero, hence either  $f$  or  $g$  belongs to  $(x)$ . So  $(x)$  is a prime ideal.

Suppose now that the ideal  $(x)$  is prime. Then for any two constant polynomials  $a$  and  $b$  in  $R \subset R[x]$  we have that if  $ab = 0 \in (x)$ , then either  $a \in (x)$  or  $b \in (x)$  and hence either  $a = 0$  or  $b = 0$ . So  $R$  is an integral domain.

If  $(x)$  is maximal, then the ideal  $(a, x)$  coincides with  $R[x]$  for any  $a \in R \setminus \{0\}$ . Hence,  $1 = af + xg$  for some polynomials  $f$  and  $g$ . Comparing the constant terms in both sides we get that  $1 = af(0)$ , so  $a$  is invertible.

If  $R$  is a field, then for any polynomial  $f \notin (x)$  we have that  $f(0)^{-1}(f - (f - f(0))) = 1$  so the ideal  $(f, x)$  coincides with  $R[x]$ . Hence,  $(x)$  is maximal.

5. Determine the Jordan canonical form for the  $n \times n$  matrix over  $\mathbb{F}_p$  whose entries are all equal to 1 (the answer depends on whether or not  $p$  divides  $n$ ).

Let  $A : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$  be the operator, whose matrix has all entries 1. Then the image of  $A$  has dimension one, since it is spanned by the vector  $(1, \dots, 1) \in \mathbb{F}_p^n$ . Thus the kernel has dimension  $n - 1$ . Hence,  $A$  has exactly  $n - 1$  linearly independent eigenvectors with the eigenvalue 0 (in fact, any vector in  $\mathbb{F}_p^n$  with the zero sum of coordinates is an eigenvector for  $A$  with the zero eigenvalue).

The vector  $v = (1, \dots, 1)$  is an eigenvector of  $A$  with the eigenvalue  $n$ . If  $n \not\equiv 0 \pmod{p}$ , then the Jordan form of  $A$  is diagonal with the entries  $(n, 0, \dots, 0)$  on the diagonal. If  $n \equiv 0 \pmod{p}$ , then  $v$  lies in the kernel, and hence  $A^2 = 0$ . In this case, the Jordan form of  $A$  has zeroes on the diagonal and one nonzero entry 1 above the diagonal.

**Bonus Problem.** Let  $\mathbb{Z}[x]$  be the ring of polynomials with integer coefficients, and  $f(x) = x^3 + 2x + 1$  and  $g(x) = 2x^2 + 1$  two polynomials in  $\mathbb{Z}[x]$ . Find the smallest positive integer number contained in the ideal  $(f, g)$ .