MATH 403 **FINAL** **WINTER 2007**

In this exam we adopt the following conventions, some of which are more restrictive than those in Herstein:

- the letters R and S will always denote rings;
- the letters k, K, and F will always denote fields;
- the letters U, V, and W will always denote vector spaces;
- the letter i always denotes a complex number such that $i^2 = -1$;
- $\mathbb{Z}_n$ always denotes the quotient ring $\mathbb{Z}/n\mathbb{Z}$;
- $\mathbb{F}_q$ always denotes the field with q elements;
- all rings are required to have an identity element 1;
- all ring homomorphisms are required to send 1 to 1;
- all subrings of a ring R are required to contain the identity element of R.

With these conventions, $2\mathbb{Z}$ is not a ring, the map

$$f : \mathbb{R} \to M_2(\mathbb{R}), \qquad f(r) = \begin{pmatrix} r & 0 \\ 0 & 0 \end{pmatrix}$$

is not a ring homomorphism, and $R \times \{0\}$ is not a subring of $R \times S$.

And don't forget the ring with one element! Or the vector space of dimension zero!

1. True/False

You get 2 points for each correct answer and -2 for each incorrect one. Just write T or F as your answer. My advice is to answer the questions you are sure of first, then do the rest of the exam and finally return to look at those you are not so sure about.

(1) The fields $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{31})$ are isomorphic.
(2) The fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ are equal.
(3) The field $\mathbb{Q}(\sqrt[3]{3})$ is isomorphic to $\mathbb{Q}[x]/(x^3-3)$.
(4) $\mathbb{Q}(i)[x]/(x^2-2)$ is a field.
(5) (7) is a maximal ideal in $\mathbb{Z}[\sqrt{3}]$.
(6) 5 is irreducible in $\mathbb{Z}[\sqrt{3}]$.
(7) If $k \subset K$ is a degree 5 extension, then $K = k(\alpha)$ for all $\alpha \in K - k$.
(8) If $k \subset K$ is a degree 7 extension and $\alpha \in K - k$ and $\beta \in K$, then $\beta = f(\alpha)$ for some $f \in k[x]$.
(9) $\mathbb{Q}(\sqrt[7]{3}) = \mathbb{Q}[\sqrt[7]{3}]$.
(10) Let $\xi = e^{\pi i/3}$. Then $[\mathbb{Q}(\xi) : \mathbb{Q}] = 3$.
(11) $\mathbb{F}_5[x]/(x^3+a)$ is not a field for any $a \in \mathbb{F}_5$.
(12) All degree three polynomials in $\mathbb{F}_5[x]$ are reducible.
(13) $\mathbb{F}_7[x]/(x^3+a)$ is a field if and only if $a \neq \pm 1$.
(14) $\mathbb{F}_{11}[x]/(x^3-5)$ is a field.
(15) The ideal $(x^{35}+x^2+1, x^7+x+1)$ in $\mathbb{Q}[x]$ can be generated by one element.
(16) The set of units in a ring R is a group under multiplication.
(17) The set of units in a ring R is a subring.
(18) There is a monic polynomial in $k[x]$ having the same divisors as $3x^4-x^3+x^2+1$.
(19) If f is a polynomial with coefficients in k there is a larger field over which f is a product of degree one polynomials.
(20) If I is an ideal in a commutative ring R, so is $\{a \in R \mid ab = 0 \text{ for all } b \in I\}$.
(21) If R is not a domain, neither is R/I for all ideals $I \neq R$.
(22) $\mathbb{Z}_{121}$ is the field with 121 elements.
(23) There is a commutative domain with 81 elements.
(24) There is a commutative domain with 82 elements.
(25) There is a commutative domain with 83 elements.
(26) There is a field with 81 elements.
(27) There is a field with 82 elements.
(28) There is a field with 83 elements.
(29) If R and S are domains, so is $R \times S$.
(30) The ring $\mathbb{Z}[\sqrt{77}] := \{a + b\sqrt{77} \mid a, b \in \mathbb{Z}\}$ is a domain.
(31) $\mathbb{Z}[\sqrt{77}]$ is a field.
(32) $\mathbb{Q}[\sqrt{77}] := \{a + b\sqrt{77} \mid a, b \in \mathbb{Q}\}$ is a field.
(33) Let $f : R \to S$ be a ring homomorphism. If u is a unit in R, then $f(u)$ is always a unit in S.

(34) Let $f : R \to S$ be a ring homomorphism. If u is not a unit in R, then $f(u)$ is not a unit in S.

(35) If m and n are integers, then there is an isomorphism $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ of rings.

(36) The rings $\mathbb{C}[x]/(x^2 + x - 4)$, $\mathbb{C}[x]/(x^2 - 1)$, and $\mathbb{C} \times \mathbb{C}$ are isomorphic.

(37) There is an isomorphism of rings $\mathbb{C}[x]/(x - 4)^2 \cong \mathbb{C} \times \mathbb{C}$.

(38) There is an isomorphism of rings $\mathbb{C}[x]/(x - 4)^2 \cong \mathbb{C}[t]/(t^2)$.

(39) If d is an integer that is not a square, then $\mathbb{Q}[\sqrt{d}]$ is isomorphic to $\mathbb{Q}[x]/(x^2 - d)$.

(40) There is an integer d such that $\mathbb{Q}[\sqrt{d}]$ is not isomorphic to $\mathbb{Q}[x]/(x^2 - d)$.

(41) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{5})$

(42) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{-2})$

(43) $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(\sqrt{8})$

(44) $\mathbb{Q}(\sqrt{-2}) \cong \mathbb{Q}(i, \sqrt{2})$

(45) $\mathbb{Q}(\sqrt[4]{4}) \cong \mathbb{Q}(i, \sqrt{2})$

(46) There is a vector space over $\mathbb{F}_4$ with 64 elements.

(47) There is a vector space over $\mathbb{F}_{16}$ with 64 elements.

(48) A basis for $k[x]/(x^4)$ is given by the images of $1, x + 1, x^2 + x + 1, x^3 + 1$.

(49) Every ideal in $R = k[x, y]$ is principal.

(50) Every ideal in $\mathbb{Q}[x]$ is principal.

(51) Every ideal in $\mathbb{Q}(i)[x]$ is principal.

(52) If $f : R \to S$ is a ring homomorphism and A is a subring of R, then $f(A)$ a subring of S.

(53) Let $f : R \to S$ be a ring homomorphism and A a subring of S. Define

$$f^{-1}(A) := \{r \in R \mid f(r) \in A\}.$$

Then $f^{-1}(A)$ a subring of R.

(54) Let $f : R \to S$ be a ring homomorphism and I a ideal of S. Define

$$f^{-1}(I) := \{r \in R \mid f(r) \in I\}.$$

Then $f^{-1}(I)$ an ideal of R.

(55) The multiplication map $\mu : R \times R \to R$, $\mu(x, y) = xy$, is a ring homomorphism.

(56) The diagonal map $\delta : R \to R \times R$, $\delta(x) = (x, x)$, is a ring homomorphism.

(57) The composition of the ring homomorphisms

$$k[x] \to k[x, y] \to \frac{k[x, y]}{(x^2 - y)},$$

given by $f(x) \mapsto f(x, 0)$ followed by $g \mapsto g + (x^2 - y)$, is an isomorphism of rings.

(58) The composition of the ring homomorphisms

$$k[y] \to k[x, y] \to \frac{k[x, y]}{(x^2 - y)}$$

given by $f(y) \mapsto f(0, y)$ followed by $g \mapsto g + (x^2 - y)$, is an isomorphism of rings.

(59) There are no surjective linear maps $k^{2006} \to k^{2007}$.

(60) There are no injective linear maps $k^{2007} \to k^{2006}$.

(61) The map $\phi : k^5 \to M_2(k)$ defined by

$$\phi(a,b,c,d,e) = \begin{pmatrix} a & 1 \\ 1 & d \end{pmatrix}$$

is linear.

(62) The map $\phi : k^5 \to M_2(k)$ defined by

$$\phi(a,b,c,d,e) = \begin{pmatrix} 0 & b \\ 2e & e \end{pmatrix}$$

is linear.

(63) The map $\phi : k^5 \to M_2(k)$ defined by

$$\phi(a,b,c,d,e) = \begin{pmatrix} ab & bc \\ cd & de \end{pmatrix}$$

is linear.

(64) The map $\phi : k^5 \to M_2(k)$ defined by

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

is linear.

2. Short Answers and/or complete the sentence

Complete the following sentences. Do NOT waste time by rewriting the part of the sentence that I have already written. Just write the rest of it.

Each question is worth 3 points.

(1) The number of elements in $\mathbb{F}_{97}[x]/(x^{11}-x-1)$ is ....
(2) The number of elements in $\mathbb{F}_3 \times \mathbb{F}_4 \times \mathbb{F}_5$ is ...
(3) The number of solutions in $\mathbb{Z}_{2006}$ to the equation $17x = 0$ is ...
(4) The number of solutions in $\mathbb{Z}_{2007}$ to the equation $17x = 0$ is ...
(5) The number of solutions in $\mathbb{F}_{31}$ to the equation $x^{30} - 1 = 0$ is ...
(6) The number of solutions in $\mathbb{Z}_{12}$ to the equation $x^2 = 1$ is ...
(7) The number of solutions in $\mathbb{Z}_{13}$ to the equation $x^2 = 1$ is ...
(8) The number of homomorphisms $f : \mathbb{Z} \to \mathbb{Z}_8$ is...
(9) Up to isomorphism, the number of vector spaces over $\mathbb{F}_8$ of dimension ≤ 64 is ...
(10) Up to isomorphism, the number of vector spaces over $\mathbb{F}_8$ with ≤ 64 elements is ...
(11) The number of elements in the ring $\mathbb{Z}[x,y]/(5,7)$ is ...
(12) The number of maximal ideals of $\mathbb{F}_2[x]/(x^4-1)$ is ...
(13) The number of maximal ideals of $\mathbb{F}_3[x]/(x^4-1)$ is ...

(14) The number of maximal ideals of $\mathbb{F}_4[x]/(x^4-1)$ is ...

(15) The number of maximal ideals of $\mathbb{F}_5[x]/(x^4-1)$ is ...

(16) The number of maximal ideals of $\mathbb{F}_{13}[x]/(x^4-1)$ is ...

(17) The number of elements in the ideal $(x^5-1)/(x^{15}-1)$ of $\mathbb{F}_3[x]/(x^{15}-1)$ is...

(18) The number of elements in each element of $\mathbb{F}_3[x]/(x^{15}-1)$ is ...

(19) The number of elements in each element of

$$\frac{\mathbb{Z}/24\mathbb{Z}}{8\mathbb{Z}/24\mathbb{Z}}$$

is ...

(20) The number of elements in

$$\frac{\mathbb{Z}/24\mathbb{Z}}{8\mathbb{Z}/24\mathbb{Z}}$$

is ...

(21) Let n be a non-zero integer. The number of elements in the ring $\mathbb{Z}[i]/(n)$ is ...

(22) Let $J \subset I$ be two ideals in a ring R and suppose that R/J is finite. Then the relation between the numbers

$$\left|\frac{R}{J}\right|, \quad \left|\frac{R}{I}\right|, \quad \left|\frac{I}{J}\right|$$

is given by the formula.......

(23) Julia's questions:
- (a) $1+1=0$ in the ring ...
- (b) $1+1=11$ in the fields .... and ...
- (c) $(1+1)^{-1}=11$ in the fields .... and ...
- (d) $(1+1)^{2007}=2007-1$ in the fields .... and ...

(24) Let R be a commutative domain and $a,b \in R-\{0\}$. An element $d \in R$ is a greatest common divisor of a and b if ...

(25) The greatest common divisor of two non-zero integers a and b is ...

(26) The greatest common divisor of two non-zero polynomials $a,b \in k[x]$ is ...

(27) In $\mathbb{F}_5$ the greatest common divisors of 2 and 4 are ...

(28) An element a in a commutative ring R is irreducible if....

(29) An element a in a ring R is a unit if....

(30) If $\phi : \mathbb{Z} \to \mathbb{F}_{81}$ is a ring homomorphism, then $\ker\phi$ is ....

(31) A complex number a is algebraic over $\mathbb{Q}(\sqrt{3}, i)$ if ... .

(32) For example, $\frac{1}{2}(1+\sqrt{-7})$ is algebraic over $\mathbb{Q}$ because ...

(33) The minimal polynomial over $\mathbb{R}$ of $\sqrt{\pi}$ is ...

(34) The minimal polynomial over $\mathbb{R}$ of $i-1$ is ...

(35) Notation: Let K be an extension of k and $a \in K$. Then
- (a) $k[a]$ denotes ...
- (b) $k(a)$ denotes ...
- (c) $k[a]=k(a)$ if and only if ....

(36) Let K be an extension of k An element $a \in K$ is algebraic over k if ....

(37) Let K be an extension of k and suppose that $a \in K$ is algebraic over k. The minimal polynomial of a over k is ....

(38) The degree $[K : k]$ of an extension is ....

(39) Theorem Let K be an extension of k and $a \in K$. The following four conditions are equivalent:

(a) a is algebraic over k;

(b)

(c)

(d)

(40) The non-negative integers are not a subring of $\mathbb{Z}$ because ....

(41) In a non-commutative ring R the elements in the smallest two-sided ideal containing a are ....

(42) The two-sided ideals in the ring $M_3(\mathbb{R})$ of 3×3 matrices with real entries are ...

(43) Let a be the element

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

in the ring $R = M_3(\mathbb{R})$.

(a) The elements in the left ideal Ra are the matrices that have zeroes everywhere except possibly in ...

(b) The elements in the right ideal aR are the matrices that have zeroes everywhere except possibly in ...

(c) Find matrices u, v, w, x, y, z such that $uav + wax + yaz = 1$.

(44) The element $a + n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if ...

(45) In a commutative ring R, the ideal denoted by (a, b, c) is the set $\{\cdots\}$.

(46) A subset S of a ring R is a subring if ....

(47) Let $a = \sqrt[3]{2}$. The ring $\mathbb{Z}[a]$ consists of the elements ....

(48) If I and J are ideals, then IJ denotes the ideal ...

(49) Let $X = \{*, +, x\}$ and $Y = \{1, 2\}$ and $Z = \{a, b, c\}$. Give examples of injective, surjective, and bijective maps between these sets.

(50) A function $f : X \to Y$ is not injective if ...

(51) A function $f : X \to Y$ is not surjective if ...

(52) The subset of $\mathbb{Z}$ consisting of all integers that leave a remainder of 5 when divided by 17 is an element of the ring ...

(53) If I is an ideal in a ring R, there is a homomorphism $\pi : R \to R/I$ given by the formula $\pi(x) = \cdots$.

(54) What is the formula relating the degrees of the extensions $k \subset F \subset K$?

(55) The kernel of the homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Q}$ defined by $\phi(f) = f(-\frac{2}{3})$ is the ideal generated by ...

(56) The image of the homomorphism ϕ in the previous question is ...

(57) The set of all functions from $\mathbb{R}$ to $\mathbb{R}$ with addition defined by $(f+g)(x) = f(x)+g(x)$ and multiplication defined by $(fg)(x) = f(g(x))$ is not a ring because ...

(58) There is a ring isomorphism $\phi : \mathbb{R}[x]/(x^2+x+1) \to \mathbb{C}$ defined by $\phi(f) = ...$

(59) The inverse in $\mathbb{F}_5[x]/(x^2+x+1)$ of the image of $x+1$ is ...

(60) The set of polynomials in $\mathbb{Z}[x]$ whose constant term is a multiple of 6 is an ideal because it is the kernel of the homomorphism $\phi : \mathbb{Z}[x] \to ...$

(61) The ideal in $\mathbb{Z}[x]$ consisting of the polynomials whose constant term is a multiple of 6 is generated by the elements ...

(62) The ideal $(x^2-x-1, 3x+2)$ in $\mathbb{Z}[x]$ is generated by one element, namely...

(63) An ideal I in a commutative ring R is maximal if and only if R/I ....

(64) Let R be a commutative ring and $a \in R$. The ideal generated by a is all of R if and only if...

(65) Let $0 \neq x \in \mathbb{Z}[i]$ and write $\bar{x}$ for its conjugate. There is an isomorphism of rings

$$f : \frac{\mathbb{Z}[i]}{(x)} \to \frac{\mathbb{Z}[i]}{(\bar{x})}$$

given by $f(z+(x)) = ...$

(66) Let $K = \mathbb{F}_2[z]/(z^6+z+1)$. This is the field with 64 elements. The multiplicative group $K - \{0\}$ is generated by α:=the image of z, and $\{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ is a basis for K. For example,

$$\alpha^6 = \alpha+1, \quad \alpha^8 = \alpha^3+\alpha^2, \quad \alpha^9 = \alpha^4+\alpha^3, \quad \text{and}$$
$$\alpha^{27} = \alpha^3+\alpha^2+\alpha, \quad \alpha^{36} = \alpha^4+\alpha^2+\alpha, \quad \alpha^{54} = \alpha^4+\alpha^2+\alpha+1.$$

Write α^{18} and α^{45} in terms of the basis elements.

(67) Compute the minimal polynomial of α^9.

(68) The 25 elements in the field $K = \mathbb{F}_5[x]/(f)$, where $f = x^2+x+1$, are

$$\{0, a^i \mid 1 \leq i \leq 24\} = \{\alpha a + \beta \mid \alpha, \beta \in \mathbb{F}_5\},$$

where a denotes the image of $3x+1$. Fill in at least two of the missing powers of a in the following table:

$$\begin{array}{cccc}
 & a^7 = 2a & a^{13} = 4a & a^{19} = 3a \\
a^2 = 4a+3 & a^8 = 3a+1 & a^{14} = a+2 & a^{20} = 2a+4 \\
a^3 = & a^9 = & a^{15} = & a^{21} = \\
a^4 = 3a+2 & a^{10} = a+4 & a^{16} = 2a+3 & a^{22} = 4a+1 \\
a^5 = 4a+4 & a^{11} = 3a+3 & a^{17} = a+1 & a^{23} = 2a+2 \\
a^6 = 2 & a^{12} = 4 & a^{18} = 3 & a^{24} = 1
\end{array}$$

(69) Write the image of x in K as $\alpha a + \beta$, with $\alpha, \beta \in \mathbb{F}_5$.

(70) Write the image of x^2+x+4 as $\alpha a + \beta$, with $\alpha, \beta \in \mathbb{F}_5$.

(71) Find at least three zeroes in K of $g = t^8 + t^4 + 1 \in K[t]$. (A cryptic hint: try multiplying g by something to get a very nice polynomial and look for zeroes of that.)

(72) Give an example of a field k of positive characteristic, an irreducible $f \in k[x]$, an extension $K \supset k$, and an $\alpha \in K$, such that f is divisible by $(x-\alpha)^2$ in $K[x]$. viewed.

(73) Theorem. Let $f : R \to S$ be a ring homomorphism. Then $R/\ker f \cong \operatorname{im} f$ via the isomorphism $\phi : R/\ker f \to \operatorname{im} f$ given by the formula $\phi(?) =?$.

(74) Proposition: Let K be an extension of k and suppose that $a \in K$ is algebraic over k. The ideal in $k[x]$ generated by the minimal polynomial of a over k is the kernel of ....

(75) Proposition: Let K be an extension of k and suppose that $a \in K$ is algebraic over k. Let f be the minimal polynomial of a over k. Then $k[x]/(f) \cong$ is isomorphic to ....

(76) Proposition: Let K and F be extensions of k and suppose that $a \in K$ and $b \in L$ have the same minimal polynomial over k. Then $k(a) \cong k(b)$ because ...

(77) State the Classification Theorem for finite fields.

(78) What was the best thing about this course? What was the worst thing about this course?