**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.
F

(2) The fields $\mathbb{Q}(\sqrt{2},\sqrt{3})$ and $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ are equal.
T

(3) The field $\mathbb{Q}(\sqrt[3]{3})$ is isomorphic to $\mathbb{Q}[x]/(x^3-3)$.
T

(4) $\mathbb{Q}(i)[x]/(x^2-2)$ is a field.
T

(5) (7) is a maximal ideal in $\mathbb{Z}[\sqrt{3}]$.
T

(6) 5 is irreducible in $\mathbb{Z}[\sqrt{3}]$.
F

(7) If $k \subset K$ is a degree 5 extension, then $K = k(\alpha)$ for all $\alpha \in K - k$.
T

(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 $f \in k[x]$.
T

(9) $\mathbb{Q}(\sqrt[7]{3}) = \mathbb{Q}[\sqrt[7]{3}]$.
T

(10) Let $\xi = e^{\pi i/3}$. Then $[\mathbb{Q}(\xi) : \mathbb{Q}] = 3$.
F

(11) $\mathbb{F}_5[x]/(x^3+a)$ is not a field for any $a \in \mathbb{F}_5$.
T

(12) All degree three polynomials in $\mathbb{F}_5[x]$ are reducible.
F

(13) $\mathbb{F}_7[x]/(x^3+a)$ is a field if and only if $a \notin \{0, 1, -1\}$.
T

(14) $\mathbb{F}_{11}[x]/(x^3-5)$ is a field.
F

(15) The ideal $(x^{35}+x^2+1, x^7+x+1)$ in $\mathbb{Q}[x]$ can be generated by one element.
T

(16) The set of units in a ring $R$ is a group under multiplication.
T

(17) The set of units in a ring $R$ is a subring.
F

(18) There is a monic polynomial in $k[x]$ having the same divisors as $3x^4 - x^3 + x^2 + 1$.
T

(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.
T

(20) If $I$ is an ideal in a commutative ring $R$, so is $\{a \in R \mid ab = 0 \text{ for all } b \in I\}$.
T

(21) If $R$ is not a domain, neither is $R/I$ for all ideals $I \neq R$.
F

(22) $\mathbb{Z}_{121}$ is the field with 121 elements.
F

(23) There is a commutative domain with 81 elements.
T

(24) There is a commutative domain with 82 elements.
F

(25) There is a commutative domain with 83 elements.
T

(26) There is a field with 81 elements.
T

(27) There is a field with 82 elements.
F

(28) There is a field with 83 elements.
T

(29) If $R$ and $S$ are domains, so is $R \times S$.
F

(30) The ring $\mathbb{Z}[\sqrt{77}] := \{a + b\sqrt{77} \mid a, b \in \mathbb{Z}\}$ is a domain.
T

(31) $\mathbb{Z}[\sqrt{77}]$ is a field.
F

(32) $\mathbb{Q}[\sqrt{77}] := \{a + b\sqrt{77} \mid a, b \in \mathbb{Q}\}$ is a field.
T

(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 $S$.
T

(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 $S$.
F

(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.
F

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(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 $R$.
T

(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 $R$.
T

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

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

(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.
T

(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.
F

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

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

(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.
F

(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.
T

(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.
F

(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.
T

## 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 ....
$97^{11}$

(2) The number of elements in $\mathbb{F}_3 \times \mathbb{F}_4 \times \mathbb{F}_5$ is ...
60

(3) The number of solutions in $\mathbb{Z}_{2006}$ to the equation $17x = 0$ is ...
17

(4) The number of solutions in $\mathbb{Z}_{2007}$ to the equation $17x = 0$ is ...
1

(5) The number of solutions in $\mathbb{F}_{31}$ to the equation $x^{30} - 1 = 0$ is ...
30

(6) The number of solutions in $\mathbb{Z}_{12}$ to the equation $x^2 = 1$ is ...
4

(7) The number of solutions in $\mathbb{Z}_{13}$ to the equation $x^2 = 1$ is ...
2

(8) The number of homomorphisms $f : \mathbb{Z} \to \mathbb{Z}_8$ is...
1

(9) Up to isomorphism, the number of vector spaces over $\mathbb{F}_8$ of dimension $\leq 64$ is ...
65

(10) Up to isomorphism, the number of vector spaces over $\mathbb{F}_8$ with $\leq 64$ elements is ...
3

(11) The number of elements in the ring $\mathbb{Z}[x, y]/(5, 7)$ is ...
1

(12) The number of maximal ideals of $\mathbb{F}_2[x]/(x^4 - 1)$ is ...
1

(13) The number of maximal ideals of $\mathbb{F}_3[x]/(x^4 - 1)$ is ...
3

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

(15) The number of maximal ideals of $\mathbb{F}_5[x]/(x^4 - 1)$ is ...
2

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

(17) The number of elements in the ideal $(x^5 - 1)/(x^{15} - 1)$ of $\mathbb{F}_3[x]/(x^{15} - 1)$ is...
$3^{10}$

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

(19) The number of elements in each element of

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

is ...
3

(20) The number of elements in

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

is ...
8

(21) Let $n$ be a non-zero integer. The number of elements in the ring $\mathbb{Z}[i]/(n)$ is ...
$n^2$

(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.....

$$\left|\frac{R}{J}\right| = \left|\frac{R}{I}\right| \times \left|\frac{I}{J}\right|$$

(23) Julia's questions:
(a) $1 + 1 = 0$ in the ring ...
$\mathbb{Z}_2$ OR $\mathbb{F}_2$ OR $\mathbb{F}_4$ OR $\mathbb{F}_{16}[x]$ OR $\mathbb{F}_{32}[x]/I$ OR ...
(b) $1 + 1 = 11$ in the fields .... and ...
$\mathbb{F}_3$ and $\mathbb{F}_9$
(c) $(1 + 1)^{-1} = 11$ in the fields .... and ...
$\mathbb{F}_3$ AND $\mathbb{F}_7$
(d) $(1 + 1)^{2007} = 2007 - 1$ in the fields .... and ...
$\mathbb{F}_2$ AND $\mathbb{F}_3$

(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 ...
IT DIVIDES BOTH $a$ AND $b$ AND WHENEVER $e$ DIVIDES BOTH $a$ AND $b$ IT ALSO DIVIDES $d$.

(25) The greatest common divisor of two non-zero integers $a$ and $b$ is ...
THE LARGEST POSITIVE INTEGER THAT DIVIDES BOTH $a$ AND $b$

(26) The greatest common divisor of two non-zero polynomials $a, b \in k[x]$ is ...
THE MONIC POLYNOMIAL OF LARGEST DEGREE THAT DIVIDES BOTH $a$ AND $b$

(27) In $\mathbb{F}_5$ the greatest common divisors of 2 and 4 are ...
1, 2, 3, 4

(28) An element $a$ in a commutative ring $R$ is irreducible if....
IN EVERY FACTORIZATION $a = bc$ EITHER $b$ OR $c$ IS A UNIT

(29) An element $a$ in a ring $R$ is a unit if....
IT HAS A TWO-SIDED INVERSE, I.E., $ab = ba = 1$ FOR SOME $b$ IN $R$

(30) If $\phi : \mathbb{Z} \to \mathbb{F}_{81}$ is a ring homomorphism, then $\ker \phi$ is ....
$3\mathbb{Z}$

(31) A complex number $a$ is algebraic over $\mathbb{Q}$ if ... .
IF THERE IS A NON-ZERO POLYNOMIAL $f \in \mathbb{Q}[x]$ SUCH THAT $f(a) = 0$

(32) For example, $\frac{1}{2}(1 + \sqrt{-7})$ is algebraic over $\mathbb{Q}$ because ...
IT IS A ZERO OF THE POLYNOMIAL $x^2 - x + 2$

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

(34) The minimal polynomial over $\mathbb{R}$ of $i - 1$ is ...
$(a + 1)^2 + 1$ OR $a^2 + 2a + 2$

(35) Notation: Let $K$ be an extension of $k$ and $a \in K$. Then
(a) $k[a]$ denotes ...
THE SMALLEST SUBRING OF $K$ THAT CONTAINS BOTH $k$ AND $a$
(b) $k(a)$ denotes ...
THE SMALLEST SUBFIELD OF $K$ THAT CONTAINS BOTH $k$ AND $a$
(c) $k[a] = k(a)$ if and only if ....
$a$ IS ALGEBRAIC OVER $k$

(36) Let $K$ be an extension of $k$ An element $a \in K$ is algebraic over $k$ if ....
IT IS THE ZERO OF A NON-ZERO POLYNOMIAL $f \in k[x]$

(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 ....
THE SMALLEST DEGREE MONIC POLYNOMIAL $f \in k[x]$
SUCH THAT $f(a) = 0$

(38) The degree $[K : k]$ of an extension is ....
THE DIMENSION OF $K$ AS A VECTOR SPACE OVER $k$

(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) $\dim_k k(a) < \infty$
(c) $\dim_k k[a] < \infty$
(d) $k(a) = k[a]$

(40) The non-negative integers are not a subring of $\mathbb{Z}$ because ....
THEY DON'T CONTAIN 1

(41) In a non-commutative ring $R$ the elements in the smallest two-sided ideal containing $a$ are ....
ALL SUMS OF ALL ELEMENTS OF THE FORM $xay$ WHERE
$x$ AND $y$ ARE ARBITRARY ELEMENTS OF $R$.

(42) The two-sided ideals in the ring $M_3(\mathbb{R})$ of $3 \times 3$ matrices with real entries are ...
$\{0\}$ AND $M_3(\mathbb{R})$

(43) Let $a$ be the element

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

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 ...
THE FIRST COLUMN

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

(c) Find matrices $u, v, w, x, y, z$ such that $uav + wax + yaz = 1$.
$1 = 1a1 + e_{21}ae_{12} + e_{31}ae_{13}$

($43\frac{1}{2}$) An element $u$ is a unit in a ring $R$ if it has an inverse. The element $a + n\mathbb{Z}$ is a unit in $\mathbb{Z}/n\mathbb{Z}$ if and only if ...
$(a, n) = 1$

(44) In a commutative ring $R$, the notation $(a, b, c)$ denotes the set $\{\cdots\}$....
$\{ax + by + cz \mid x, y, z \in R\}$

(45) A subset $S$ of a ring $R$ is a subring if ....
IT IS A SUBGROUP UNDER + AND CLOSED UNDER MULTIPLICATION AND CONTAINS 1

(46) Let $a = \sqrt[3]{2}$. The ring $\mathbb{Z}[a]$ consists of the elements ....
$x + y\sqrt[3]{2} + z\sqrt[3]{4}$ AS $x, y, z$ RANGE OVER ALL INTEGERS

(47) If $I$ and $J$ are ideals, then $IJ$ denotes the ideal ...
$\{\sum_{i=1}^{n} a_i, b_i \mid$ where $a_i \in I$ and $b_i \in J\}$

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

(49) A function $f : X \to Y$ is not injective if ... .
THERE ARE DIFFERENT ELEMENTS $x_1, x_2 \in X$ SUCH THAT $f(x_1) = f(x_2)$

(50) A function $f : X \to Y$ is not surjective if ...
THERE IS $y \in Y$ SUCH THAT $y \neq f(x)$ FOR ANY $x \in X$

(51) 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 ...
$\mathbb{Z}/17\mathbb{Z}$

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

(53) What is the formula relating the degrees of the extensions $k \subset F \subset K$?
$[K : k] = [K : F] \times [F : k]$

(54) 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 ...
$3x + 2$

(55) The image of the homomorphism $\phi$ in the previous question is ...
$\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ AND } b = 3^n \text{ FOR SOME } n \in \mathbb{Z} \right\}$

(56) 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 ..
THE DISTRIBUTIVE LAW FAILS: e.g., IF $f(x) = x^3$ AND $g(x) = x^2$, THEN $\big(f(g+g)\big)(x) = f(x^2+x^2) = (2x^2)^3 = 8x^6$ BUT
$(fg+fg)(x) = (fg)(x) + (fg)(x) = x^6 + x^6 = 2x^6$.

(57) There is a ring isomorphism $\phi : \mathbb{R}[x]/(x^2+x+1) \to \mathbb{C}$ defined by $\phi(f) = ...$
$\phi(f) := f\left(\frac{-1+\sqrt{-3}}{2}\right)$ OR $\phi(f) := f\left(\frac{-1-\sqrt{-3}}{2}\right)$

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

(59) 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 $\phi : \mathbb{Z}[x] \to ...$
$\phi : \mathbb{Z}[x] \to \mathbb{Z}_6$ DEFINED BY $\phi(\sum_{i=0}^n a_i x^i = \bar{a}_0$ WHERE $\bar{a}_0$ IS THE IMAGE IN $\mathbb{Z}_6$ OF THE INTEGER $a_0$; NAMELY $a_0 + 6\mathbb{Z}$.

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

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

(62) An ideal $I$ in a commutative ring $R$ is maximal if and only if $R/I$ ....
IS A FIELD

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

(64) 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 $f(z) = ...$
IF $z \in \mathbb{Z}[i]$, THEN $f(z+(x)) = \bar{z}+(\bar{x})$, WHERE $\bar{z}$ IS THE USUAL COMPLEX CONJUGATE OF THE COMPLEX NUMBER $z$

(65) 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 $\alpha$:=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 $\alpha^{18}$ and $\alpha^{45}$ in terms of the basis elements.
$\alpha^{18} = (\alpha^6)^3 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1$
$\alpha^{45} = \alpha^9\alpha^{36} = \alpha^8 + \alpha^7 + \alpha^6 + \alpha^4 = \alpha^4 + \alpha^3 + 1$

(66) Compute the minimal polynomial of $\alpha^9$.

WE JUST SHOWED $(\alpha^9)^5 = \alpha^9 + 1$, SO THE MINIMAL POLYNOMIAL IS $x^5 + x + 1$ PROVIDED THIS IS IRREDUCIBLE. IF IT WERE NOT IRREDUCIBLE IT WOULD EITHER HAVE A ROOT IN $\mathbb{F}_2$ OR WOULD BE DIVISIBLE BY AN IRREDUCIBLE POLYNOMIAL OF DEGREE 2. OBVIOUSLY IT HAS NO ROOT, AND IF WE DIVIDE IT BY THE ONLY IRREDUCIBLE POLYNOMIAL OF DEGREE TWO IN $\mathbb{F}_2[x]$ WE FIND THAT $x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$. BUT $x^3 + x + 1$ IS IRREDUCIBLE AND VANISHES AT $\alpha^9$, SO $x^3 + x + 1$ IS THE MINIMAL POLYNOMIAL OF $\alpha^9$

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

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

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

| | | | |
|---|---|---|---|
| | $a^7 = 2a$ | $a^{13} = 4a$ | $a^{19} = 3a$ |
| $a^2 = 4a + 3$ | $a^8 = 3a + 1$ | $a^{14} = a + 2$ | $a^{20} = 2a + 4$ |
| $a^3 =$ | $a^9 =$ | $a^{15} =$ | $a^{21} =$ |
| $a^4 = 3a + 2$ | $a^{10} = a + 4$ | $a^{16} = 2a + 3$ | $a^{22} = a + 3$ |
| $a^5 = 4a + 4$ | $a^{11} = 3a + 3$ | $a^{17} = a + 1$ | $a^{23} = 2a + 2$ |
| $a^6 = 2$ | $a^{12} = 4$ | $a^{18} = 3$ | $a^{24} = 1$ |

$$a^3 = 4a + 1, \quad a^9 = 3a + 2, \quad a^{15} = a + 4, \quad a^{21} = 2a + 3$$

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

$x = 2a + 3$

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

3

(70) 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.)

SINCE $(t^4 - 1)g = t^{12} - 1$ ANY $b \in K$ SUCH THAT $b^{12} = 1$ BUT $b^4 \neq 1$ IS A ZERO OF $g$. FROM THE TABLE ABOVE WE SEE THAT $(a^2)^{12} = 1$ but $(a^2)^4 \neq 1$, SO $a^2, a^4, a^8, a^{10}, a^{14}, a^{16}, a^{20}, a^{22}$ ARE ZEROES OF $g$. THESE ARE ALL OF THEM.

(71) 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 $K[x]$.

LET $K = \mathbb{F}_2(t)$, $k = \mathbb{F}_2(t^2)$ AND $f = x^2 - t^2$.

(72) 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 $\phi(?) = ?$.

$\phi(x + \ker f) := f(x)$

(73) 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 ....

THE EVALUATION HOMOMORPHISM $\phi : k[x] \to K$ GIVEN BY $\phi(f) = f(a)$.

(74) 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 ....

$k(a)$

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

BOTH ARE ISOMORPHIC TO $k[x]/(f)$ where $f$ IS THE MINIMAL POLYNOMIAL OF $a$ AND/OR $b$

(76) State the Classification Theorem for finite fields.

FOR EVERY PRIME $p$ AND INTEGER $n \geq 1$ THERE IS, UP TO ISOMORPHISM, A UNIQUE FIELD WITH $p^n$ ELEMENTS. THERE ARE NO OTHER FINITE FIELDS.

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

This is an easy question—the professor, of course! Don't forget to rate me on rateyourprofessor.com and give me a terrific hotness rating :) It has been fun teaching you. Say "hi" if you see me on campus. Stop by my office if you would like to, especially if you have chocolate.