MATH 403 RINGS AND VECTOR SPACES WINTER 2006

(1) Define a ring.
(2) Define a subring.
(3) If R and S are rings we can impose a ring structure on the Cartesian product

$$R \times S := \{(r, s) \mid r \in R, s \in S\}.$$

What are the addition and multiplication?
(4) Suppose we are given rings R, S, T and homomorphisms $f : T \to R$ and $g : T \to S$. Is the map $\alpha : T \to R \times S$ defined by $\alpha(t) := (f(t), g(t))$ a ring homomorphism? Prove it.
(5) Suppose we are given rings R, S, T and homomorphisms $f : R \to T$ and $g : S \to T$. Is the map $\alpha : R \times S \to T$ defined by $\alpha(r, s) := f(r) + g(s)$ a ring homomorphism? Prove it.
(6) Let R be the ring $\mathbb{Z}_2 \times \mathbb{Z}_3$. Is the set $\mathbb{Z}_2 \times \{0\}$ a subring? Explain.
(7) What are all the rings with 4 elements (up to isomorphism)? Explain why the different rings on your list are not isomorphic to one another.
(8) Define a homomorphism $f : R \to S$ between the rings R and S.
(9) What adjective do we use to describe a ring in which $ab = ba$ for all a, b?
(10) Give an example of a ring and elements a and b such that $ab \neq ba$.
(11) Give an example of a *commutative* ring and non-zero elements a and b such that $ab = 0$.
(12) Define a field.
(13) Define a domain.
(14) Is a field a domain? Explain.
(15) Define an ideal.
(16) If $f : R \to S$ is a ring homomorphism prove that $\ker f$ is an ideal.
(17) If I is an ideal in a ring R how is the set R/I defined? i.e., what are its elements? How do we make R/I a ring? i.e., how do we define addition and multiplication on it?
(18) There is an obvious ring homomorphism $\pi : R \to R/I$. What is it? Prove it is a hmomorphism. What is its kernel?
(19) Let R be any ring. Show there is a unique homomorphism $f : \mathbb{Z} \to R$. What is it?
(20) Show that $\mathbb{Z}/n\mathbb{Z}$ is a domain if and only if n is zero or prime.
(21) Show that a finite domain is a field. (Hint: fix a non-zero element, say a, in the domain and look at the function $f(b) = ab$.)
(22) Define a vector space.
(23) Define a subspace

(24) Define a homomorphism, or linear map, between two vector spaces over the same field k.
(25) Can one define a linear map between vector spaces over different fields?
(26) Fix a field k. Up to isomorphism how many n-dimensional vector spaces are there over k?
(27) Define a basis of a vector space.
(28) If R is a ring containing a field k as a subring, prove that R is a vector space over k.
(29) If R is a ring containing a field k as a subring, prove that every ideal in R is a vector space over k.
(30) Let k be a finite field. Show there is a prime number p such that for every element $x \in k$ the p-fold sum $x + \cdots + x$ is zero. (Hint: you might want to consider the image and/or kernel of a homomorphism $f : \mathbb{Z} \to k$.
(31) Using the previous exercise, explain why a finite field k must contain a subring that is isomorphic to $\mathbb{F}_p$ for some prime p.
(32) If R is a finite ring containing a copy of $\mathbb{F}_p$ (i.e., a subring isomorphic to $\mathbb{F}_p$, p prime) show that R has p^n elements for some n.
(33) Give an example of a subset $S \subset \mathbb{R}^4$ containing three different elements such that S is not linearly independent but every proper subset of it is.
(34) If I take a linearly independent subset $S \subset \mathbb{R}^4$ that has 4 elements, must it be a basis for $\mathbb{R}^4$? Explain.
(35) If I take a linearly independent subset $S \subset \mathbb{R}^4$ that has spans $\mathbb{R}^4$, must it be a basis for $\mathbb{R}^4$? Explain.
(36) If I take a subset $S \subset \mathbb{R}^4$ that has 4 elements and spans $\mathbb{R}^4$, must it be a basis for $\mathbb{R}^4$? Explain.
(37) Let A and B be ideals in a ring R. Define their sum

$$A + B := \{x + y \mid x \in A,\, y \in B\}$$

and product

$$AB := \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; x_i \in A,\, y_i \in B, n \text{ arbitrary} \right\}.$$

Show both $A + B$ is an ideal and that AB is an ideal when R is commutative.
(38) Show that every (possibly infinite) intersection of ideals is an ideal.
(39) What is a principal ideal.
(40) Define a principal ideal domain.
(41) Give three examples of a PID and one example of a ring that is not a PID.
(42) Give an example of a group of order 63 that is not a quotient of the integers.
(43) Give an example of a group of order 63 that is a quotient of the integers.
(44) State the theorem about the classification of finite fields.
(45) Give an example of a ring with 125 elements that has only two ideals, $\{0\}$ and itself.
(46) Give an example of a ring with 125 elements that has more than two ideals.

(47) Let k be a field and R any (non-zero!) ring. Show that every ring homomorphism $f : k \to R$ is injective.
(48) Give an example of a homomorphism $f : \mathbb{Z} \to \mathbb{F}_4$. You *might* need some sort of description of $\mathbb{F}_4$ for this.
(49) Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is the only ring with 6 elements (up to isomorphism).
(50) Describe all ring homomorphisms $f : \mathbb{F}_{25} \to \mathbb{Z}$.
(51) Describe all ring homomorphisms $f : \mathbb{Z} \to \mathbb{F}_{25}$.
(52) Describe all ring homomorphisms $f : \mathbb{Q}[x] \to \mathbb{Z}$.
(53) Describe three different ring homomorphisms $f : \mathbb{Q}[x] \to \mathbb{Q}$.
(54) Prove that there is a unique ring homomorphism $f : \mathbb{Q} \to \mathbb{Q}[x]$? What is it?
(55) Write down a formula for $\dim(V/U)$ when U is a subspace of V.
(56) For the following questions, let $V = \mathbb{R}^3$, and let $L = x$-axis, $M = xy$-plane, and $N =$the line $x = y = z$.
  (a) Does the notation M/N make sense? If so, what is it? If not, explain why not.
  (b) Does the notation M/L make sense? If so, what is it? If not, explain why not.
  (c) Is the line $\{(0, 5, 0) + t(1, 0, 0) \mid t \in \mathbb{R}\}$ a subspace of V? Is it an element of V/N? Is it an element of V/L?
  (d) Are $(1, 2, 0) + L$ and $(1, 1, 0) + L$ equal as elements of V/L? Explain
  (e) Are $(3, 3, 0) + L$ and $(4, 3, 0) + L$ equal as elements of V/L? Explain
(57) Up to isomorphism, there are four rings with 4 elements, namely $\mathbb{Z}_4 = \mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_4$, $\mathbb{F}_2[x]/(x^2)$, and $\mathbb{F}_2 \times \mathbb{F}_2$.
  (a) $\mathbb{Z}_4$ is not isomorphic to $\mathbb{F}_4$ because ...
  (b) $\mathbb{F}_4$ is not isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ because ....
  (c) $\mathbb{Z}_4$ is not isomorphic to $\mathbb{F}_2 \times \mathbb{F}_2$ because ...
  (d) $\mathbb{F}_2[x]/(x^2)$ is not isomorphic to $\mathbb{F}_4$ because ...
  (e) $\mathbb{F}_2[x]/(x^2)$ is not isomorphic to $\mathbb{Z}_4$ because ...
  (f) $\mathbb{F}_2[x]/(x^2)$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ because ...
  (g) There are two groups of order four, so some of those four rings are isomorphic as groups. Which ones? Give reasons.
  (h) Let R be the following subring of the ring of 2×2 matrices $M_2(\mathbb{Z}_2)$:

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in \mathbb{Z}_2 \right\}.$$

  Which of the rings of order four is R isomorphic to? Give reasons.
  (i) Let $R = \mathbb{Z}_2[x]/(x^2 + 1)$. Which of the rings of order four is R isomorphic to? Give reasons.
  (j) Let $R = \mathbb{Z}_2[x]/(x^2)$. Which of the rings of order four is R isomorphic to? Give reasons.
  (k) Let $R = \mathbb{Z}_2[x]/(x^2 + x + 1)$. Which of the rings of order four is R isomorphic to? Give reasons.
(58) Let $f : A \to B$ be a homomorphism.
  (a) If A and B are groups what is the definition of the kernel of f?

(b) If A and B are vector spaces what is the definition of the kernel of f?
(c) If A and B are rings what is the definition of the kernel of f?
(d) If A and B are groups, then $\ker f$ is ...
(e) If A and B are vector spaces, then $\ker f$ is ...
(f) If A and B are rings, then $\ker f$ is ...

(59) Let $f : A \to B$ be a homomorphism of vector spaces. State the First Isomorphism Theorem for vector spaces.

(60) Let $f : A \to B$ be a ring homomorphism. State the First Isomorphism Theorem for rings.

(61) Prove that every ideal in $k[x]$ is principal.

(62) Let R be a ring and A a subgroup, so the quotient group R/A is well-defined. Define a multiplication on R/A by

$$(x + A).(y + A) := xy + A.$$

Show this product is well-defined if and only if A is an ideal.

(63) Define an irreducible polynomial.

(64) Find all monic degree two irreducible polynomials in $\mathbb{F}_3[x]$. Explain.

(65) Find a degree five irreducible polynomial in $\mathbb{F}_2[x]$. Explain.

(66) State and prove a theorem that begins $\mathbb{Z}/n\mathbb{Z}$ *is a field if and only if ....*

(67) Let U be a subspace of a vector space V. Show that there is a bijection between the subspaces of V/U and the subspaces of V that contain U. Begin by saying explicitly what this bijection is.

(68) Let V be a vector space over $\mathbb{C}$ with basis $\{a, b, c\}$. Write down two different bases for V as a vector space over $\mathbb{R}$. Keep it simple!

(69) What is the classification of finite dimensional vector spaces over a field?

(70) Let U be a subspace of V. Give a formula for $\dim(V/U)$ in terms of $\dim V$ and $\dim U$.

(71) If U and V are subspaces of a vector space W, prove that

$$\frac{U + V}{U} \cong \frac{V}{U \cap V}$$

and as a corollary deduce that

$$\dim(U + V) = \dim U + \dim V - \dim(U \cap V).$$

(72) Let V be a vector space and $\mathcal{S}$ a possibly infinite subset of V. Complete the following sentence: $\mathcal{S}$ *is linearly independent if ...*

(73) Let V be a vector space and $\mathcal{S}$ a possibly infinite subset of V. Complete the following sentence: $\mathcal{S}$ *is linearly dependent if there are elements ...*

(74) Let V be a vector space and $\mathcal{S}$ a possibly infinite subset of V. Complete the following sentence: $\mathcal{S}$ *is a basis for* V *if ...*

(75) Let V be a vector space and $\mathcal{S}$ a possibly infinite subset of V. Complete the following sentence: *An element* $w \in V$ *belongs to the linear span of* $\mathcal{S}$ *if...*

(76) Let W be a subspace of a vector space V and $\mathcal{S}$ a subset of V. Complete the following sentence: *The linear span of* $\mathcal{S}$ *is contained in* W *if and only if ...*

(77) Let $\mathcal{S} \subset \mathcal{T}$ be subsets of a vector space V. What is the relation between the linear spans of $\mathcal{S}$ and $\mathcal{T}$?
(78) Let $\mathcal{S}$ and $\mathcal{T}$ be subsets of a vector space V. Suppose that every element in $\mathcal{S}$ is a difference of two elements in $\mathcal{T}$ What is the relation between the linear spans of $\mathcal{S}$ and $\mathcal{T}$? Why?
(79) True or False with reasons. The subset of $k[x]$ consisting of zero and all polynomials of even degree is a subspace.
(80) True or False with reasons. The subset of $k[x]$ consisting of zero and all polynomials of odd degree is a subspace.
(81) True or False with reasons. The subset of $\mathbb{R}[x]$ consisting of all polynomials that take the value zero at 1, 2, and 3 is a subspace. u
(82) True or False with reasons. The subset of $\mathbb{R}[x]$ consisting of all polynomials that take the value 1 at 1, 2, and 3 is a subspace.
(83) True or False with reasons. If $\{v_1, v_2, v_3, v_4, v_5\}$ spans V, then $\dim V = 5$.
(84) True or False with reasons. If $\{v_1, v_2, v_3, v_4, v_5\}$ spans V, then $\dim V \leq 5$.
(85) True or False with reasons. If $\{v_1, v_2, v_3, v_4, v_5\}$ spans V, then $\dim V \geq 5$.
(86) List 4 linearly independent vectors in the ring $M_2(\mathbb{R})$ of 2×2 matrices with entries in $\mathbb{R}$.
(87) Is the subset of $M_n(\mathbb{R})$ consisting of all symmetric matrices, i.e., those A such that $A = A^T$, a subspace? Explain.
(88) Is the subset of $M_n(\mathbb{C})$ consisting of all invertible matrices a subspace? Explain.
(89) Is the subset of $M_n(\mathbb{C})$ consisting of all non-invertible matrices a subspace? Explain.
(90) The subset of $M_n(\mathbb{R})$ consisting of all anti-symmetric matrices, i.e, those A such that $A^T = -A$, is a subspace. What is its dimension? Write down a basis for it.
(91) Define what is meant by "*the ideal generated by the elements* $x, y, z \in R$".
(92) Give an example of two fields k and K such that neither is isomorphic to a subfield of the other.
(93) Give an example of a field k such that no subfield of it is isomorphic to a subfield of the complex numbers.
(94) Give an example of two fields k and K with the following property: If F is any field containing K, then there are no homomorphisms $\phi : k \to F$.
(95) Is there a field that contains both $\mathbb{F}_5$ and $\mathbb{F}_7$? Give the reason for your answer.
(96) Define the characteristic of a field.
(97) If $f : \mathbb{Z} \to \mathbb{F}_{125}$ is a ring homomorphism, then $\ker f = ??$
(98) If $f : \mathbb{Z} \to \mathbb{F}_{27}$, then $f(33) = ??$
(99) If $f : \mathbb{Z} \to \mathbb{F}_{27}$, then $f(34) = ??$
(100) The fields $\mathbb{Q}(\sqrt{7})$ and $\mathbb{Q}(\sqrt{11})$ are not isomorphic because ...
(101) The fields $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $\mathbb{Q}(\sqrt{2} + \sqrt{3})$ are equal because ...
(102) Let k be any field. Prove that if $\phi : \mathbb{Q}[x] \to k$ is a ring homomorphism, then there is an element $a \in k$ such that $\phi(f) = f(a)$ for all $f \in \mathbb{Q}[x]$.
(103) Is there an injective ring homomorphism $f : \mathbb{Q}[x] \to \mathbb{C}$? Explain.
(104) Show that a ring homomorphism $f : R \to S$ is injective if and only if $\ker f = 0$.

(105) Is there an injective homomorphism $\phi : \mathbb{Z}_2 \to \mathbb{R}$? Explain.
(106) Is there a surjective homomorphism $\phi : \mathbb{R}[x] \to \mathbb{Z}_2$? Explain.
(107) Is there an injective homomorphism $\phi : \mathbb{Z}_3 \to \mathbb{F}_9$? Explain.
(108) Is there an injective homomorphism $\phi : \mathbb{F}_9 \to \mathbb{F}_{27}$? Explain.
(109) Suppose there is a ring isomorphism $f : A \to B$. Is there a ring isomorphism $g : B \to A$? Explain.
(110) Suppose there are ring isomorphisms $f : A \to B$ and $g : B \to C$. Is there a ring isomorphism $\phi : A \to C$? Explain.
(111) Suppose there are ring isomorphisms $f : A \to B$ and $g : B \to C$. Is there a ring isomorphism $\phi : C \to A$? Explain.
(112) Let A and B be subrings of a ring R. Is $A \cap B$ a subring? Explain.
(113) Let A and B be subrings of a ring R. Is $A \cup B$ a subring? Explain.
(114) Let A and B be subrings of a ring R. Is $A + B$ a subring? Explain.
(115) Let A and B be ideals of a ring R. Is $A \cup B$ an ideal? Explain.
(116) Let R be a ring that is not necessarily commutative. The center of R is $\{x \in R \mid xy = yx \text{ for all } y \in R\}$. We usually denote it by Z or $Z(R)$ (from the German word *zentrum*). Show that the center of R is a subring of R.
(117) Let $R \times S$ denote the Cartesian product of two rings. Show there is a surjective ring homomorphism $f : R \times S \to S$. What is its kernel?
(118) Write down a ring isomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$.
(119) If a and b are positive integers whose greatest common divisor is 1 show that $\mathbb{Z}_{ab}$ is isomorphic to $\mathbb{Z}_a \times \mathbb{Z}_b$.
(120) Prove that if two elements of a commutative ring R generate the same ideal then each is a unit multiple of the other.
(121) Let I and J be ideals in a commutative ring R such that $I \cap J = 0$ and $I + J = R$. Prove there are elements e and f such that $I = eR$, $J = fR$, and $e^2 = e$, $f^2 = f$, and $ef = fe = 0$.
(122) In the previous exercise show that the I becomes a ring with identity element e, and likewise J becomes a ring with identity element f. Then prove that as rings, $R \cong I \times J$.
(123) Suppose R is subring of a ring S and $xy \in R$. Is it true that $x \in R$ and $y \in R$? If so give a proof. If not give a counter-example.
(124) Suppose I is an ideal of a ring S and $xy \in I$. Is it true that $x \in I$ and $y \in I$? If so give a proof. If not give a counter-example
(125) Let $f : R \to S$ be a ring homomorphism and $u \in R$ and $v = f(u)$. Prove or give a counterexample to the following statements:
  (a) If u is a unit so is v.
  (b) If v is a unit, so is u.
(126) Let k be a finite field. Prove there is a prime number p such that
  (a) $\mathbb{F}_p$ is a subring of k;
  (b) $|k| = p^n$ for some integer n.
(127) Prove there is no ring homomorphism $\mathbb{F}_{p^n} \to \mathbb{F}_{q^m}$ if p and q are different positive primes.

(128) Show that a composition of linear maps is a linear map.
(129) Show that a composition of ring homomorphisms is a ring homomorphism.
(130) Define a ring homomorphism.
(131) Is there a ring with an ideal in it that does not contain zero?
(132) Is $\{0, 1, 2, 3, 4, ...\}$ a subring of $\mathbb{Z}$?
(133) Is $\{0, 1, 2, 3, 4, ...\}$ an ideal of $\mathbb{Z}$?
(134) Give an example of a domain that is not a PID.
(135) Give another example of a domain that is not a PID.
(136) A complex number a is algebraic over $\mathbb{Q}(\sqrt{3}, i)$ if ...
(137) Is $\mathrm{GL}_n(k)$ a subring of $M_n(k)$?
(138) Is $\mathbb{Z}[x]$ a PID? If so, prove it. If not, give an example, with proof, of a non-principal ideal.
(139) What is the ring $\mathbb{Z}[x]/I$ when $I = (3, 1 + 2x)$?
(140) What is the ring $\mathbb{Z}[x]/I$ when $I = (3, 1 + 6x)$?
(141) What is the ring $\mathbb{Z}[x]/I$ when $I = (12, 1 + 2x)$?
(142) What is the ring $\mathbb{Z}[x]/I$ when $I = (3, 1 + 2x^2)$?
(143) What is the ring $\mathbb{Z}[x]/I$ when $I = (5, 1 + 2x^2)$?
(144) What is the ring

$$\frac{\mathbb{Z}/12\mathbb{Z}}{6\mathbb{Z}/12\mathbb{Z}}?$$

(145) In $\mathbb{F}_7$ the greatest common divisors of 2 and 5 are ...
(146) Give an example of a ring with infinitely many elements that is not a domain.
(147) The kernel of the ring homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}_{75}$ defined by $\phi(f) = f(\overline{8})$ is principal.
(148) Give an example of a ring that is an infinite-dimensional vector space over $\mathbb{C}$ that is not a domain.
(149) If α is the image of z in $K = \mathbb{F}_2[z]/(z^6 + z + 1)$, then $1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$ is a basis for K as a vector space over $\mathbb{F}_2$ because ...
(150) Fix a prime $p \in \mathbb{Z}$. Let $R \subset \mathbb{Q}$ be the subring consisting of all a/b where b is not divisible by p. Show that R has a unique maximal ideal. What is it?
(151) Let R be the ring in the previous question. Show that the only ideals in R are 0, R, and the powers of the unique maximal ideal.
(152) Let R be as in the previous question. Find all units in R.
(153) Let R be as in the previous question. Show R is a PID.
(154) Prove that $(u) = R$ if and only if u is a unit.
(155) Let λ, ν be distinct elements of k. Prove there is a ring isomorphism

$$\frac{k[x]}{(x - \lambda)(x - \nu)} \cong k \times k.$$

Hint: use the first isomorphism theorem and dimensions of vector spaces.
(156) If U is a subspace of a vector space V having the same finite dimension as V show that $U = V$.

(157) Let R be a ring containing a field k as a subring. Let $\phi : R \to S$ be a non-zero homomorphism. Explain how you can use this to give R and S the structure of vector spaces over k. Is ϕ a k-linear map?
(158) Let V be a vector space over $\mathbb{R}$. Suppose that $a_1, a_2, \ldots, a_{2n}$ is a basis for V as a vector space over $\mathbb{R}$. Is $a_1, \ldots, a_n$ a basis for V as a vector space over $\mathbb{C}$? Explain.
(159) Let V be a vector space over $\mathbb{C}$. Suppose that $a_1, a_2, \ldots, a_n$ is a basis for V as a vector space over $\mathbb{C}$. Write down a basis for V as a vector space over $\mathbb{R}$. Prove that you actually do have a basis.
(160) Let $f, g \in k[x]$. If $k[x]/(f)$ and $k[x]/(g)$ are isomorphic rings does it follow that $(f) = (g)$? Explain.
(161) Let R be a ring containing a copy of the field k in its center, i.e., R need not be commutative but $k \subset R$ is a subring and elements of k commute with all elements in R. Define the minimal polynomial of $r \in R$.
(162) Define a homomorphism $\phi : k[x] \to R$ such that $\ker \phi$ is generated by the minimal polynomial of r.
(163) What is the minimal polynomial in $\mathbb{Q}[x]$ of $\sqrt{3} - 1$?
(164) What is the minimal polynomial in $\mathbb{R}[x]$ of $\sqrt{3} - 1$?
(165) What is the minimal polynomial in $\mathbb{Q}[x]$ of $\sqrt[3]{5} - 1$?
(166) What is the minimal polynomial in $\mathbb{R}[x]$ of $\sqrt[3]{5} - 1$?
(167) What is the minimal polynomial of

$$\begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}?$$

(168) Find a 2×2 matrix with entries in $\mathbb{R}$ whose minimal polynomial is $x^2 + 1$.
(169) Give an example of a subring of $M_2(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $\mathbb{R}$.
(170) Give an example of a subring of $M_2(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $\mathbb{R}[x]/(x^2)$.
(171) Give an example of a subring of $M_2(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $\mathbb{R} \times \mathbb{R}$.
(172) Give an example of a subring of $M_2(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $\mathbb{C}$.
(173) Give an example of a subring of $M_2(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $\mathbb{R}[x]/(x^2 - 1)$.
(174) Give an example of a subring of $M_3(\mathbb{R})$, the ring of 2×2 matrices with entries in $\mathbb{R}$, that is isomorphic to $M_2(\mathbb{R})$.
(175) Give an example of a subring of $\mathbb{R}$ that is isomorphic to $\mathbb{Q}[x]/(x^3 - 6)$.
(176) There is not a subring of $\mathbb{R}$ that is isomorphic to $\mathbb{Q}[x]/(x^3 - 1)$ because .....
(177) There is not a subring of $\mathbb{R}$ that is isomorphic to $\mathbb{Q}[x]/(x^2 + 2x + 2)$ because .....
(178) Is $\mathbb{Q}[x]/(x^2 + 2x + 2)$ isomorphic to $\mathbb{Q}[x]/(x^2 + 1)$? Explain.
(179) What is the relation between the condition that a polynomial $f \in k[x]$ is divisible by $x - a$, $a \in k$, and the value of $f(a)$?
(180) Is there a product of (perhaps several) fields having 20062007 elements? Explain.

(181) When two fields are isomorphic? i.e., when is there a bijective linear map between them?
(182) Write down a basis for $k[x]/(f)$ when f is a polynomial of degree $n \geq 0$.
(183) If $f : U \to V$ is a homomorphism between two vector spaces what is the relation between the dimensions of the $\operatorname{im} f$ and $\ker f$?
(184) Let f and g be non-zero polynomials in $k[x]$ such that g divides f. Use the previous question and the third isomorphism theorem to compute $\dim(g)/(f)$. We need such information when constructing a BCH code.
(185) Is there a field having 25, 26, 27, 28, 29 elements?
(186) What are the basic results about finite fields?
  (a) The number of elements in a finite field K is ...
  (b) There is exactly one field with ... elements up to isomorphism.
  (c) If K is a finite field then the group $K^\times = (K - \{0\}, .)$ is ...
  (d) If K is a finite field with ... elements then every element in K is a zero of the polynomial ...
(187) Does the notation $\mathbb{Z}[\sqrt{2}]$ make sense? If so, explain what it means. If not, explain why.
(188) Does the notation $\mathbb{Q}[\sqrt{2}]$ make sense? If so, explain what it means. If not, explain why.
(189) Does the notation $\mathbb{F}_2[\sqrt{2}]$ make sense? If so, explain what it means. If not, explain why.
(190) Does the notation $\mathbb{F}_3[\sqrt{2}]$ make sense? If so, explain what it means. If not, explain why.
(191) Does the notation $\mathbb{F}_4[\sqrt{2}]$ make sense? If so, explain what it means. If not, explain why.
(192) $1 + 1 = 0$ in the ring ...
(193) $1 + 1 = 11$ in the fields .... and ...
(194) $(1 + 1)^{-1} = 11$ in the fields .... and ...
(195) $(1 + 1)^{2007} = 2007 - 1$ in the fields .... and ...
(196) $\{x \in \mathbb{Z}_{84} \mid 7x = 0\} = ...$
(197) If $f \in \mathbb{F}_p[x]$ is the minimal polynomial of $\alpha \in \mathbb{F}_{p^n}$, what is the minimal polynomial of α^p?
(198) Let f be a monic polynomial in $\mathbb{F}_q[x]$ and $\alpha \in \mathbb{F}_{q^n}$. What are the two reasons why f may not be the minimal polynomial of α?
(199) Define a new addition and multiplication on $\mathbb{Z}$ as follows:

$$a \oplus b = a + b - 3 \qquad a \odot b = 3a + 3b - ab - 6,$$

where the operations on the right-hand sides of these equations are the usual operations in $\mathbb{Z}$. To avoid confusion write R for $\mathbb{Z}$ with this new ring structure. The operations $\oplus$ and $\odot$ make R a commutative ring with identity. The zero element for this new addition is ...
(200) The identity element for this new multiplication is ...
(201) The negative of an element a with respect to this new addition is ...

(202) The n-fold sum $a \oplus a \oplus \cdots \oplus a =$....

(203) There is an isomorphism $f : \mathbb{Z} \to R$, from the integers with its usual ring structure, given by $f(n) = ...$

(204) And the inverse isomorphism $f^{-1} : R \to \mathbb{Z}$ is $f^{-1}(n) =$...

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

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = (a + 2b, 3b + 4c, 5c + 6d, 7d + 8a, 0)$$

is linear. True or false?

(206) The map $\phi : M_2(k) \to M_2(k)$ defined by

$$\phi \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c & a \\ d & b \end{pmatrix}$$

is linear. True or false?

(207) What is wrong with the following argument: The polynomial $x^2 - 10$ is irreducible in $\mathbb{F}_{13}[x]$ because its zeroes, namely $\pm\sqrt{10}$, are in $\mathbb{C}$, not $\mathbb{F}_{13}$.

(208) What is inadequate about the following sentence? If K is an extension of k and $a \in K$ is algebraic over k,then the ideal in $k[x]$ generated by the minimal polynomial of a is the kernel of the homomorphism $\phi : k[x] \to K$.

(209) True or false: If K and L are extension fields of k and $\dim_k K = \dim_k L$, then $K \cong L$. Discuss.

(210) True or false: If $f : K \to L$ is a bijective function between two fields, then $K \cong L$. Discuss.

(211) [1] 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 ...

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

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

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

(215) An element a in a commutative domain R is irreducible if ...

(216) Let K be an extension field of k. Define the minimal polynomial of an element a in K and explain why it must be irreducible.

(217) Complete the sentence and explain your answer: The ideal generated by an element a in a commutative ring R is all of R if and only if ...

---

[1] Questions 211–214 were on a recent exam I gave. Most answers were inadequate. For example, many students did not realize that the word "greatest" does not make sense in an arbitrary commutative domain, only the complete phrase "greatest common divisor" makes sense. Many people gave the same answers for questions 212 and 213 as they gave for question 211, but the point of questions 212 and 213 is that they have shorter sharper answers than does 211. In question 214 many people failed to give a plural answer despite the clear wording of the question. It was surprising to me that although perhaps twenty people gave a correct definition in answer to question 211 only one of those was able to use that definition to give a correct answer to question 214.

(218) What is wrong with the answer $\phi(f) = f(i)$ to the following question: Define a ring isomorphism

$$\phi : \frac{\mathbb{R}[x]}{(x^2 + 3x + 3)} \to \mathbb{C}.$$

What is the correct answer?

(219) What is the minimal polynomial of $\sqrt{e} + \sqrt{\pi}$ over $\mathbb{R}$?

(220) What is the minimal polynomial of $2 + i$ over $\mathbb{R}$.

(221) Write down all the irreducible polynomials of degree ≤ 5 in $\mathbb{F}_2[x]$.

(222) Write $x^{11} - 1$ as a product of irreducible polynomials in $\mathbb{F}_2[x]$.

(223) An (n, k) binary linear code is ...

(224) Give an example of a binary linear $(5, 3)$ code.

(225) Define the Hamming distance and Hamming weight.

(226) What are the two decoding rules that underlie nearest neighbor decoding?

(227) A linear code corrects t errors if ...

(228) A linear code detects $2t$ errors if ...

(229) Give an example of a $(3, 2)$ code that detects one error. Explain.

(230) Give an example of a $(3, 1)$ code that corrects one error. Explain.

(231) Does your code in the previous example detect two errors? Explain.

(232) Given an example of a $(4, 2)$ code that detects one error. Explain.

(233) Does your code in the previous example detect two errors? Explain.

(234) Does your code in the previous example correct one error? Explain.

(235) Give an example of a $(5, 2)$ code that corrects one error. Explain.

(236) Let $v \in \mathbb{F}_2^n$. What is the definition of the ball $B_t(v)$?

(237) How many elements are in the ball $B_t(v)$?

(238) A code $C \subset \mathbb{F}_2^n$ corrects t errors if and only if the minimal weight of elements in C is ...

(239) A code $C \subset \mathbb{F}_2^n$ corrects t errors if and only if for all pairs u and v of distinct elements in C, $d(u, v) \geq ...$

(240) A code $C \subset \mathbb{F}_2^n$ detects $2t$ errors if and only if the minimal weight of elements in C is ...

(241) A code $C \subset \mathbb{F}_2^n$ detects $2t$ errors if and only if for all pairs u and v of distinct elements in C, $d(u, v) \geq ...$

(242) We say that an (n, k) linear code $C \subset \mathbb{F}_2^n$ is an (n, k, d) code if ....

(243) How many errors does an (n, k, d) code correct?

(244) How many errors does an (n, k, d) code detect?

(245) An (n, k, d) code $C \subset \mathbb{F}_2^n$ is perfect if ....

(246) Tell me the essential facts about the Hamming $(7, 4)$ code. Label the facts (1), (2), ... Keep your statements short and clear. Pay attention to the basic rules of writing a clear sentence.

(247) State the result that says that an (n, k, d) code is perfect if and only if

$$2^{n-k} = \cdots$$

(248) Give the recipe for constructing a BCH code.

(249) Give an example of a $(5, 2)$ code that corrects one error and detects 2 errors.
(250) The Hamming distance between 01010101 and 10101010 is ...
(251) 0-521-22909-X is a valid ISBN number. True or false?