Math 305, Fall 2007
Final Exam Review Solutions

(1) For each of the following sets, determine if it is a ring. If so, decide if it is an integral domain. Supply a proof only for a *negative* answer.
   (a) The set of diagonal $n \times n$ matrices for a fixed $n \in \mathbb{Z}_{\geq 1}$. Note: we say that a square matrix $A = (a_{ij})$ is *diagonal* if $a_{ij} = 0$ whenever $i \neq j$.
   (b) The set of all $f \in M(\mathbb{R})$ such that $f(q) = 0$ for all $q \in \mathbb{Q}$.
   (c) The set of all $f \in \text{Cont}([0,1], \mathbb{R})$ for which $\int_0^1 f(x)\,dx = 0$. Here $\text{Cont}([0,1], \mathbb{R})$ means the set of continuous functions $f\colon [0,1] \to \mathbb{R}$.
   (d) The set of rational numbers $\frac{m}{n}$ such that 3 does not divide n when $\frac{m}{n}$ is written in lowest terms. Note: obviously $m \in \mathbb{Z}$ and $n \in \mathbb{Z}_{\geq 1}$.

Solution:
   (a) This set is a ring but not an integral domain. Consider the $n \times n$ matrix A which is zero everywhere expect which is 1 in the $(1,1)$ entry. Consider the $n \times n$ matrix B which is zero everywhere except which is 1 in the $(2,2)$ entry. Then A and B are nonzero but $AB = 0$.
   (b) This set is a ring but not an integral domain. Consider f and g defined by

$$f(x) = \begin{cases} 0 & \text{if } x \neq e, \\ 1 & \text{if } x = e, \end{cases} \quad \text{and } g(x) = \begin{cases} 0 & \text{if } x \neq \pi, \\ 1 & \text{if } x = \pi. \end{cases}$$

   Then f and g are nonzero but $fg = 0$.
   (c) This set is not a ring. Consider f given by $f(x) = x - 1/2$ for all $x \in [0,1]$. Then $\int_0^1 f(x)\,dx = 0$ but $\int_0^1 f(x)^2\,dx \neq 0$. Hence the set is not closed under multiplication.
   (d) This set is a ring and is an integral domain.

(2) (a) Prove that a ring R is commutative iff $a^2 - b^2 = (a+b)(a-b)$ for all $a, b \in R$.
   (b) Let R be a ring such that $x^2 = x$ for all $x \in R$. Prove that R is commutative. Such a ring is called a *Boolean ring*. (Hint: Consider both the quantities $(a+b)^2$ and $(ab)^2$.)

Solution:
   (a) We have $a^2 - b^2 = (a+b)(a-b)$ for all $a, b \in R$ iff $a^2 - b^2 = a^2 - ab + ba - b^2$ for all $a, b \in R$ iff $0 = -ab + ba$ for all $a, b \in R$ iff $ab = ba$ for all $a, b \in R$ iff R is commutative.
   (b) Let $a, b \in R$. Then $(a+b)^2 = a + b$, so $a^2 + ab + ba + b^2 = a^2 + b^2$. So $ab = -ba$. But $ab = (ab)^2 = (-ba)^2 = (ba)^2 = ba$. So R is commutative.

(3) (a) Prove that, if $\phi\colon R \to S$ is a ring isomorphism, then $\phi^{-1}\colon S \to R$ is also a ring isomorphism.
   (b) Let C be the collection of all rings. For all R and S in C, we say that $R \sim S$ if there is a ring isomorphism $\phi\colon R \to S$. Prove that $\sim$ is an equivalence relation on C.

Solution:
   (a) Certainly ϕ^{-1} is bijective since ϕ is bijective. Let $a, b \in S$. Let $x = \phi^{-1}(a)$ and $y = \phi^{-1}(b)$, so $\phi(x) = a$ and $\phi(y) = b$. Then $\phi^{-1}(a+b) = \phi^{-1}(\phi(x)+\phi(y)) = \phi^{-1}\phi(x+y) = x + y = \phi^{-1}(a) + \phi^{-1}(b)$ and $\phi^{-1}(ab) = \phi^{-1}(\phi(x)\phi(y)) = \phi^{-1}\phi(xy) = xy = \phi^{-1}(a)\phi^{-1}(b)$. Hence ϕ^{-1} is a ring isomorphism.
   (b) Clearly if R is a ring then the identity map $\phi\colon R \to R$ is a ring isomorphism, so $R \sim R$. Let $R \sim S$. Then there is a ring isomorphism $\phi\colon R \to S$. Then $\phi^{-1}\colon S \to R$ is a ring bijective ring homomorphism from (a), so ϕ^{-1} is an isomorphism. Thus $S \sim R$. Suppose now that $R \sim S$ and $S \sim T$. Then there are ring isomorphisms $\phi\colon R \to S$ and $\psi\colon S \to T$. We claim that $\psi \circ \phi\colon R \to T$ is a ring isomorphism. Certainly it is a bijection. Let $a, b \in R$. Then

$$(\psi \circ \phi)(a+b) = \psi(\phi(a+b)) = \psi(\phi(a) + \phi(b)) = \psi(\phi(a)) + \psi(\phi(b)) = (\psi \circ \phi)(a) + (\psi \circ \phi)(b).$$

Also we have

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi)(a)(\psi \circ \phi)(b).$$

Therefore $\psi \circ \phi$ is a bijective ring homomorphism and thus a ring isomorphism. So $R \sim T$ and $\sim$ is an equivalence relation.

(4) The following are subrings of the ring $\mathbb{Z}[x]$. Decide whether or not each is an ideal, giving a proof only if it is *not* an ideal.
   (a) The subring I of all polynomials whose constant term is a multiple of 3.
   (b) The subring $\mathbb{Z}[x^2]$ of all polynomials with even power terms.
   (c) The subring I of polynomials p such that $p'(0) = 1$. Here $p'(0)$ is the first derivative of p evaluated at 0.
   (d) The subring I of polynomials p such that $p(0) = p'(0) = 0$.
   (e) The subring I of polynomials whose coefficients sum to zero. (Hint: write this condition in a different way.)

Solution:
   (a) This I is an ideal.
   (b) This I is not an ideal. Let $a = x^2$ and let $r = x$. Then $ra = x^3$ which does not belong to $\mathbb{Z}[x^2]$.
   (c) This I is not an ideal. Consider $a = x$ and $b = x^2$. Then $a \in I$ and $ba = x^3$ which does not belong to I.
   (d) This I is an ideal.
   (e) This I is an ideal.

(5) Let $\phi\colon R \to S$ be a ring homomorphism. Prove that, if ϕ is surjective and I is an ideal of R, then $\phi(I)$ is an ideal of S. Give an example where this statement fails if ϕ is not surjective.

Solution: Certainly $0 = \phi(0) \in \phi(I)$, so $\phi(I)$ is nonempty. Suppose that $r, s \in \phi(I)$. Then there are $a, b \in I$ such that $\phi(a) = r$ and $\phi(b) = s$. Then $r - s = \phi(a) - \phi(b) = \phi(a - b)$. Since $a - b \in I$, it follows that $r - s \in \phi(I)$. Let $a \in \phi(I)$ and $b \in S$. Then there are $r \in I$ and $s \in R$ such that $a = \phi(r)$ and $b = \phi(s)$, since ϕ is surjective. Then $ab = \phi(r)\phi(s) = \phi(rs) \in \phi(I)$ since $rs \in I$. Similarly $ba \in \phi(I)$, so $\phi(I)$ is an ideal.

Consider the map $\phi\colon \mathbb{Z} \to \mathbb{Q}$ given by $\phi(n) = n$ for all $n \in \mathbb{Z}$. Then $\phi(\mathbb{Z}) = \mathbb{Z}$ which is not an ideal in $\mathbb{Q}$.

(6) Prove that the following rings are not isomorphic.
   (a) $\mathbb{Z}_5$ and $\mathbb{Z}_8$
   (b) $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$
   (c) $\mathbb{Z}_3[x]$ and $\mathbb{Z}_5[x]$
   (d) $\mathbb{Z}$ and $\mathbb{Q}$
   (e) $\mathbb{R}$ and $\mathbb{C}$ (hint: assume that there is an isomorphism $\phi\colon \mathbb{C} \to \mathbb{R}$ and show that $\phi(i)$ cannot be defined)
   (f) $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$

Solution:
   (a) The two rings have different orders, so there cannot be a bijection between them.
   (b) The ring $\mathbb{Z}$ is an integral domain and $\mathbb{Z} \times \mathbb{Z}$ is not.
   (c) The rings have different characteristics.
   (d) The ring $\mathbb{Q}$ is a field and $\mathbb{Z}$ is not.
   (e) Let $\phi\colon \mathbb{C} \to \mathbb{R}$ be an isomorphism. Then $\phi(i)^2 = \phi(i^2) = \phi(-1) = -\phi(1) = -1$. Since there is no $a \in \mathbb{R}$ such that $a^2 = -1$, there is no way to define $\phi(i)$, a contradiction.
   (f) Let $\phi\colon \mathbb{Q}[x] \to \mathbb{Z}[x]$ be an isomorphism. Then $1 = \phi(1) = 2\phi(1/2)$. Since there is no $a \in \mathbb{Z}[x]$ such that $2a = 1$, there is no way to define $\phi(1/2)$, a contradiction.

(7) Let R be a commutative ring and let I be an ideal of R. Let $\operatorname{rad} I$ be the subset of R defined by $\operatorname{rad} I = \{\, r \in R\colon\ r^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 1} \,\}$.
   (a) Prove that $\operatorname{rad} I$ is an ideal of R.
   (b) Prove that $(\operatorname{rad} I)/I = N(R/I)$, where $N(R/I)$ is the ideal of nilpotent elements of R/I. (Hint: prove that each set is a subset of the other. This problem looks scary but is not.)

Solution:
   (a) Since $0^1 \in I$, we have $0 \in \operatorname{rad} I$, so $\operatorname{rad} I$ is nonempty. Let $a \in \operatorname{rad} I$ and $r \in R$. Choose $n \in \mathbb{Z}_{\geq 1}$ such that $a^n \in I$. Then $(ra)^n = r^n a^n \in I$ since I is an ideal. Hence $ra \in \operatorname{rad} I$. Similarly $ar \in \operatorname{rad} I$. Suppose that $a, b \in \operatorname{rad} I$. Choose $n, m \in \mathbb{Z}_{\geq 1}$ such that $a^n \in I$ and $b^m \in I$. Then
$$(a-b)^{m+n} = a^{m+n} - \binom{m+n}{1} a^{m+n-1} b + \cdots + (-1)^{m+n} b^{m+n}.$$
   For every term $(-1)^k \binom{m+n}{k} a^{m+n-k} b^k$, either $a^{m+n-k} \in I$ or $b^k \in I$. Hence every term belongs to I, so $(a-b)^{m+n} \in I$. So $a - b \in \operatorname{rad} I$. Therefore $\operatorname{rad} I$ is an ideal.
   (b) We note that $a + I \in (\operatorname{rad} I)/I$ iff $a^n \in I$ for some $n \in \mathbb{Z}_{\geq 1}$ iff $a^n + I = I$ for some $n \in \mathbb{Z}_{\geq 1}$ iff $(a+I)^n = I$ for some $n \in \mathbb{Z}_{\geq 1}$ iff $a + I \in N(R/I)$. Hence $(\operatorname{rad} I)/I = N(R/I)$.

(8) Let x be a nilpotent element of a commutative unital ring R. Recall that a *unit* is an element of a unital ring R with a multiplicative inverse.
   (a) Prove that x is either zero or a zero divisor.
   (b) Prove that rx is nilpotent for all $r \in R$.
   (c) Prove that $1 + x$ is a unit in R.
   (d) Prove that the sum of a nilpotent element and a unit is a unit.

Solution:
   (a) Let x be nonzero nilpotent element. Let $n \in \mathbb{Z}_{\geq 2}$ be the smallest positive integer such that $x^n = 0$. Then $xx^{n-1} = 0$. Since $x^{n-1} \neq 0$, we conclude that x is a zero divisor.
   (b) Choose $n \in \mathbb{Z}_{\geq 1}$ such that $x^n = 0$. Then for all $r \in R$ we have $(rx)^n = r^n x^n = 0$, so rx is nilpotent.
   (c) Choose $n \in \mathbb{Z}_{\geq 1}$ such that $x^n = 0$. Then $(1+x)(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1}) = 1+(-1)^{n-1}x^n = 1$. Similarly $(1 - x + x^2 - \cdots + (-1)^{n-1}x^{n-1})(1+x) = 1$, so $1 + x$ is a unit.
   (d) Let x be a nilpotent element and let u be a unit. Then $u + x = u(1 + u^{-1}x)$. Certainly $u^{-1}x$ is nilpotent by (b) so $1 + u^{-1}x$ is a unit by (c). Therefore $u + x$ is the product of two units, so is itself a unit.

(9) Find q and r guaranteed by the Division Algorithm for the given a and b in the given polynomial ring $F[x]$.
   (a) $a = x^4 + 3x + 2$ and $b = 2x + 1$ in $\mathbb{Q}[x]$
   (b) $a = x^2 + ix$ and $b = ix + 2$ in $\mathbb{C}[x]$
   (c) $a = 3x^3 + 2x + 1$ and $b = 2x + 1$ in $\mathbb{Z}_5[x]$

Solution:
   (a) $q = \frac{1}{2}\,x^3 - \frac{1}{4}\,x^2 + \frac{1}{8}\,x + \frac{23}{16}$ and $r = \frac{9}{16}$
   (b) $q = -ix + 3$ and $r = -6$
   (c) $q = 4x^2 + 3x + 2$ and $r = 4$

(10) Decide if each of the following polynomials is reducible in the given polynomial rings. If so, write down its factorization into irreducible elements. No explanation required. (Hint: A reducible quadratic or cubic must have a root. A reducible quartic will either have a root or will factor into two irreducible quadratics. If it factors into two quadratics, then it can be expressed as $(x^2+ax+b)(x^2+cx+d)$ for some $a, b, c, d \in F$. Multiply this expression out, collect terms and you should be able to solve for a, b, c, d.)
   (a) $p = x^2 + x + 1$ in $\mathbb{Z}_2[x]$
   (b) $p = x^2 + 1$ in $\mathbb{Z}_3[x]$
   (c) $p = x^3 + 1$ in $\mathbb{Z}_2[x]$

(d) $p = x^4 + 1$ in $\mathbb{Z}_5[x]$
(e) $p = x^4 + 4$ in $\mathbb{Z}[x]$
(f) $p = x^2 + 2x + 2$ in $\mathbb{R}[x]$

Solution:
(a) irreducible
(b) irreducible
(c) $(x + 1)(x^2 + x + 1)$
(d) $(x^2 + 2)(x^2 + 3)$
(e) $(x^2 - 2x + 2)(x^2 + 2x + 2)$
(f) irreducible

(11) In each of the following examples is a homomorphism $\theta\colon F[x] \to E$ for various fields F and E. The function θ is given by $\theta(f) = f(c)$ for some fixed $c \in E$. In each case, identify the kernel and image of θ explicitly and write down the isomorphism guaranteed by the First Isomorphism Theorem for rings.
(a) $\theta : \mathbb{Q}[x] \to \mathbb{Q}$ given by $\theta(f) = f(3)$
(b) $\theta : \mathbb{Q}[x] \to \mathbb{R}$ given by $\theta(f) = f(1 + \sqrt{2})$
(c) $\theta : \mathbb{R}[x] \to \mathbb{C}$ given by $\theta(f) = f(2 - i)$

Solution:
(a) $\mathbb{Q}[x]/(x - 3) \cong \mathbb{Q}$
(b) $\mathbb{Q}[x]/(x^2 - 2x - 1) \cong \mathbb{Q}(\sqrt{2})$
(c) $\mathbb{R}[x]/(x^2 - 4x + 5) \cong \mathbb{C}$