Sam Tay
Professor Aydin
Math 435
Take-Home Midterm 1
02/17/12

Problem 1: Suppose R and S are rings with unities 1_R and 1_S respectively, and $\theta : R \to S$ is a ring isomorphism.

(a) Show that $\theta(1_R) = 1_S$.

Proof. Since θ is an isomorphism, we know that for any $b \in S$ there exists $\theta^{-1}(b) \in R$ where $\theta^{-1}(b) = 1_R \cdot \theta^{-1}(b) = \theta^{-1}(b) \cdot 1_R$. Evaluating each side of this equality under θ, it follows from the homomorphism property that

$$b = \theta(1_R) \cdot b = b \cdot \theta(1_R).$$

This holds for all $b \in S$ and since the multiplicative identity satisfies this property uniquely, we conclude that $\theta(1_R) = 1_S$. $\square$

(b) Show that r is a unit in R if and only if $\theta(r)$ is a unit in S.

Proof. By definition, $r \in R$ is a unit means that there exists $r^{-1} \in R$ so that $r \cdot r^{-1} = r^{-1} \cdot r = 1_R$. Since θ is an isomorphism, we must have

$$\theta(r) \cdot \theta(r^{-1}) = \theta(r^{-1}) \cdot \theta(r) = \theta(1_R) = 1_S,$$

which means $\theta(r)$ has a multiplicative inverse $\theta(r)^{-1} = \theta(r^{-1})$ and is therefore a unit in S.

Conversely, suppose $\theta(r)$ is a unit in S with multiplicative inverse $\theta(r)^{-1}$ so that

$$\theta(r) \cdot \theta(r)^{-1} = \theta(r)^{-1} \cdot \theta(r) = 1_S = \theta(1_R).$$

Again, we evaluate under θ^{-1} to find that for some $a \in R$,

$$r \cdot a = a \cdot r = 1_R$$

which allows us to conclude that r has multiplicative inverse a and is therefore a unit in R. $\square$

(c) For a ring R with unity, let $U(R)$ denote the set of all units in R. Show that $U(R \times S) = U(R) \times U(S)$.

Proof. ($\subseteq$) Suppose $(a, b) \in U(R \times S)$. Then (a, b) has a multiplicative inverse $(c, d) \in R \times S$ so that $(a, b)(c, d) = (ac, bd) = (1_R, 1_S)$. Then $ac = 1_R$ and $bd = 1_S$, so a and b are units in R and S respectively and we have $(a, b) \in U(R) \times U(S)$.

($\supseteq$) On the other hand, suppose $(a, b) \in U(R) \times U(S)$. Then a and b are units in R and S respectively, and have multiplicative inverses $a^{-1} \in R$ and $b^{-1} \in S$. Then we have $(a^{-1}, b^{-1}) \in R \times S$ and obtain

$$(a, b)(a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (1_R, 1_S).$$

Thus (a, b) is a unit in $R \times S$ and $(a, b) \in U(R \times S)$, which completes the proof. □

(d) Using part **(c)** and the Chinese Remainder Theorem (Example 18.15), what can you say about $\phi(mn)$ when m and n are relatively prime positive integers and ϕ is the Euler phi-function.

Proof. Recall that $\phi : \mathbb{Z}^+ \to \mathbb{Z}^+$ is defined such that $\phi(n)$ is the number of positive integers less than n and relatively prime to n. By Theorem 20.12, these are precisely the integers $a \in \mathbb{Z}_n$ such that the equation $ax = 1$ has a unique solution in $\mathbb{Z}_n$. It is now apparent that $\phi(n)$ is the number of units of $\mathbb{Z}_n$, so we write

$$\phi(n) = \big|U(\mathbb{Z}_n)\big|.$$

For relatively prime integers n, m, Example 18.15 states that $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$. Clearly the number of units in isomorphic structures is the same, so that

$$|U(\mathbb{Z}_{nm})| = |U(\mathbb{Z}_n \times \mathbb{Z}_m)| = |U(\mathbb{Z}_n) \times U(\mathbb{Z}_m)| = |U(\mathbb{Z}_n)||U(\mathbb{Z}_m)|,$$

where the penultimate equality follows from part **(c)**. From the reasoning above we can conclude that $\phi(mn) = \phi(m)\phi(n)$ for relatively prime integers n, m. □

(e) Let p be a prime and m be a positive integer. Compute $\phi(p^m)$.

To compute $\phi(p^m)$ we first note that since p is a prime, the only integers $1 \leq n \leq p^m$ that are not relatively prime to p^m are multiples of p. How many multiples are there? We can count

$$p, 2p, 3p, \ldots, p^{m-1}p = p^m,$$

from which it is clear that there are p^{m-1} of them. This is the number of integers $1 \leq n \leq p^m$ that are *not* relatively prime to n, and we conclude that $\phi(p^m) = p^m - p^{m-1}$.

(f) Now find a formula $\phi(n)$ for any integer $n > 1$. Calculate $\phi(2700)$ using your formula.

For any integer $n > 1$ with unique prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, we have

$$
\begin{aligned}
\phi(n) &= \phi(p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}) \\
&= \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) && \text{by part } \textbf{(d)} \\
&= (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_r^{k_r} - p_r^{k_r-1}) && \text{by part } \textbf{(e)} \\
&= p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big) \\
&= n \, \Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big) \cdots \Big(1 - \frac{1}{p_r}\Big).
\end{aligned}
$$

To calculate $\phi(2700)$, we note that $2700 = 3^3 \cdot 2^2 \cdot 5^2$, so

$$\phi(2700) = 2700\Big(1 - \frac{1}{3}\Big)\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{5}\Big) = 720.$$

Problem 2:

Definition An element a of a ring R is nilpotent if $a^n = 0$ for some positive integer n.

(a) Let a be a nilpotent element. Show that a is either 0 or a zero divisor.

Proof. Obviously 0 is nilpotent, as $0^n = 0$ for all positive integers n. For a nonzero nilpotent element $a \in R$, let n be the least positive integer such that $a^n = 0$. Since a is nonzero, $n > 1$. Then we have $a \cdot a^{n-1} = a^n = 0$, and since n is the least such positive integer, the factors a and a^{n-1} are both nonzero. We conclude that a is a zero divisor. □

(b) In a ring R with unity 1, prove that if a is nilpotent, then $1-a$ is invertible.

Proof. Let a be nilpotent so that $a^n = 0$ for some positive integer n. Then

$$1 = 1 - 0 = 1 - a^n = (1-a)(1 + a + a^2 + \cdots + a^{n-1}),$$

which is just the formula for the finite geometric sum. The equation above tells us that $1 - a$ is invertible. □

(c) In a commutative ring R, the product xa of a nilpotent element a by any element x is nilpotent.

Proof. Suppose that a is nilpotent and let n be a positive integer satisfying $a^n = 0$. Then for any $x \in R$,

$$(xa)^n = \overbrace{(xa)(xa)\cdots(xa)}^{n \text{ times}} = x^n a^n$$

since R is commutative. But $a^n = 0$, so $(xa)^n = x^n a^n = x^n \cdot 0 = 0$, and hence the product xa is also nilpotent. $\square$

(d) In a commutative ring R, the sum of two nilpotent elements is nilpotent.

Proof. Suppose that $a, b \in R$ are nilpotent elements with positive integers n, m satisfying $a^n = 0$ and $b^m = 0$. Since R is commutative we can use the binomial theorem to expand $(a+b)^{nm}$ as follows:

$$(a+b)^{nm} = \sum_{k=0}^{nm} \binom{nm}{k} a^k b^{nm-k}.$$

First note that if $n = 1$ then of course $a = 0$ and $a + b = b$ is nilpotent. So suppose that $n > 1$ and let us consider the terms of the sum above. When $k \geq n$, we see that the terms $\binom{nm}{k} a^k b^{nm-k}$ contain a factor of a^n and therefore evaluate to zero. For the terms when $k < n$, we must have $-k > -n$, from which it follows that $nm - k > nm - n > m - 1$, where the last inequality follows from our assumption that $n > 1$. Thus $nm - k \geq m$ and the terms $\binom{nm}{k} a^k b^{nm-k}$ contain a factor of b^m and also evaluate to zero. We have shown that all terms in the binomial expansion above must be zero, so $(a+b)^{nm} = 0$ and we conclude $a + b$ is nilpotent. $\square$

Definition An element a of a ring is unipotent if $1 - a$ is nilpotent.

(e) In a commutative ring R the product of two unipotent elements is unipotent.

Proof. Let $a, b \in R$ be unipotent elements. To show that the product ab is unipotent, we must show that $1 - ab$ is nilpotent. We see that

$$(1 - ab) = (1 - a) + a(1 - b),$$

where $(1 - a)$ and $(1 - b)$ are both nilpotent. By part **(c)**, the product $a(1 - b)$ is also nilpotent, and then by part **(d)** the sum $(1 - a) + a(1 - b)$ is nilpotent. Therefore $(1 - ab)$ is nilpotent and ab is unipotent. $\square$

(f) In a ring R with unity 1, every unipotent element is invertible.

Proof. Let $a \in R$ be unipotent. Then $(1 - a)$ is nilpotent, so by part **(b)** we know $1 - (1 - a)$ is invertible, where $1 - (1 - a) = 1 - 1 - (-a) = a$, which completes the proof. $\square$

Problem 3: Let R be the set of all functions from $\mathbb{R}$ to $\mathbb{R}$. We define addition and multiplication on these functions in the usual way.

(a) Describe the additive and multiplicative identities in the ring R.

The additive identity is the constant zero function $f(x) = 0$. The multiplicative identity is the constant function $f(x) = 1$.

(b) What are the units of R?

The units of R are the functions satisfying $f(x) \neq 0$ for all $x \in \mathbb{R}$. We see that given this constraint, we can construct a well defined function $g : \mathbb{R} \to \mathbb{R}$ defined by $g(x) = \frac{1}{f(x)}$, so that $f(x)g(x) = 1$ for all $x \in \mathbb{R}$. On the other hand, because $\mathbb{R}$ has no zero divisors, if a function h has a root $h(x_0) = 0$ then there is no $r \in \mathbb{R}$ such that $r \cdot h(x_0) = 1$, and therefore no function $g(x)$ such that $h(x_0)g(x_0) = 1$. Therefore the units are precisely the functions satisfying $f(x) \neq 0$ for all $x \in \mathbb{R}$.

(c) Determine all zero divisors in R.

Let $f, g \in R$. Since $\mathbb{R}$ has no zero divisors, the product $(fg)(x) = f(x)g(x)$ is the zero function if and only if for each $x_0 \in \mathbb{R}$, either $f(x_0) = 0$ or $g(x_0) = 0$. Thus $fg = 0$ if $(\ker f) \cup (\ker g) = \mathbb{R}$. However we are interested in the nonzero functions, so consider when $fg = 0$ for nonzero g. Then there exists $x_0 \in \mathbb{R}$ where $g(x_0) \neq 0$, so we must have $f(x_0) = 0$. On the other hand, if $f(y_0) = 0$ for some $y_0 \in \mathbb{R}$, we can construct a nonzero function

$$g(x) = \begin{cases} 0 & \text{if } x \neq y_0 \\ 1 & \text{if } x = y_0 \end{cases}$$

so that $fg = 0$. We conclude that the zero divisors are precisely the nonzero functions f with some root x_0 where $f(x_0) = 0$. In regards to the set notation above, we could equivalently say that f is a zero divisor if and only if $\emptyset \subset \ker f \subset \mathbb{R}$.

(d) Determine all nilpotent elements in R.

Let $f \in R$ be a nilpotent element. Then there exists a positive integer n such that f^n is the zero function, which means $(f(x_0))^n = 0$ for all $x_0 \in \mathbb{R}$. But $f(x_0)$ is just a real number, of which there are no zero divisors. Then it must be the case that $f(x_0) = 0$ for all $x_0 \in \mathbb{R}$, so the only nilpotent function in R is the zero function.

(e) Is the following statement true for R?

"Every nonzero element is either a zero divisor or a unit."

This is true! For any nonzero function $f \in R$, either there exists a root x_0 where $f(x_0) = 0$ or there does not. In the former case f is a zero divisor by part **(c)**, and in the latter case f is a unit by part **(b)**.

(f) Is the statement in part **(e)** true for a general ring with unity?

Of course not: consider the ring of integers $\mathbb{Z}$ with unity 1, which is an integral domain and thus has no divisors of zero. We know that the only units are 1,-1 so there are many elements that are neither units nor divisors of zero. For a concrete counterexample, we'll choose the element $64 \in \mathbb{Z}$ which is nonzero, not a unit, and not a zero divisor.

Problem 4: Let R be a commutative ring and let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in R[x]$. Then $p(x)$ is a zero divisor in $R[x]$ if and only if there is a nonzero $b \in R$ such that $b \cdot p(x) = 0$.

Proof. Let $p(x)$ be defined as above and assume further that $a_n \neq 0$, so that $p(x)$ has degree n. The backward direction is trivial: if $b \cdot p(x) = 0$ for nonzero elements $b, p(x) \in R[x]$ then by definition b and $p(x)$ are zero divisors. In the forward direction, we assume that $p(x)$ is a zero divisor. Then there exists at least one nonzero polynomial $g(x) \in R[x]$ so that $p(x)g(x) = 0$. Let us pick $g(x)$ specifically to have minimal degree among such functions.[1] Without loss of generality, we'll suppose that $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0$, where $b_m \neq 0$ and $\deg(g) = m$. We wish to show that $a_{n-i}g(x) = 0$ for each $0 \leq i \leq n$, from which the claim will follow easily. To this end, we will proceed by strong induction on i. Computing the product $p(x)g(x)$, we find that the leading coefficient is $a_n b_m$, which must be zero since $p(x)g(x)$ is the zero polynomial. Now consider the polynomial

$$\begin{aligned} a_n g(x) &= a_n b_m x^m + a_n b_{m-1} x^{m-1} + \cdots + a_n b_0 \\ &= 0x^m + a_n b_{m-1} x^{m-1} + \cdots + a_n b_0 \\ &= a_n b_{m-1} x^{m-1} + \cdots + a_n b_0. \end{aligned}$$

Then by associativity,

$$(a_n g(x))p(x) = a_n(g(x)p(x)) = a_n \cdot 0 = 0.$$

However this polynomial $a_n g(x)$ has degree less than $g(x)$, which we defined to have minimal degree among the nonzero functions satisfying this equation. The only possibility is that $a_n g(x)$ is the zero polynomial, and our base case is now

[1] Specifically, we are considering the set $T = \{g(x) \in R[x] : p(x)g(x) = 0 \text{ and } g(x) \text{ is nonzero}\}$ and choosing $g \in T$ such that $\deg(g) \leq \deg(h)$ for all $h \in T$.

proven. Next suppose for induction that for some $0 < k \leq n$, $a_{n-i}\, g(x) = 0$ for all $0 \leq i < k$. Again, we consider the product

$$\begin{aligned} 0 = p(x)g(x) &= (a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)\, g(x) \\ &= a_n x^n g(x) + a_{n-1}x^{n-1} g(x) + \cdots + a_0 g(x) \\ &= x^n (a_n g(x)) + x^{n-1}(a_{n-1} g(x)) + \cdots + a_0 g(x) \\ &= a_{n-k}x^{n-k} g(x) + a_{n-k-1}x^{n-k-1} g(x) + \cdots + a_0 g(x), \end{aligned}$$

where the last equality follows from our inductive hypothesis. Let us consider this last expression a bit more carefully. We see that the terms in this sum have degrees (individually of course) as below:

$$0 = p(x)g(x) = \overbrace{a_{n-k}x^{n-k} g(x)}^{\deg \leq m+n-k} + \overbrace{a_{n-k-1}x^{n-k-1} g(x)}^{\deg \leq m+n-k-1} + \cdots + \overbrace{a_0 g(x)}^{\deg \leq m}.$$

In particular, we see that the only occurrence of x^{n+m-k} is within the first term of highest degree; equally clear is that within this term, we find the leading coefficient $a_{n-k}b_m$, which as before must be equal to zero. Just as before, we find that $a_{n-k}g(x)$ has degree less than that of g:

$$\begin{aligned} a_{n-k}g(x) &= a_{n-k}b_m x^m + a_{n-k}b_{m-1}x^{m-1} + \cdots + a_{n-k}b_0 \\ &= 0x^m + a_{n-k}b_{m-1}x^{m-1} + \cdots + a_{n-k}b_0 \\ &= a_{n-k}b_{m-1}x^{m-1} + \cdots + a_{n-k}b_0. \end{aligned}$$

However $(a_{n-k}g(x))p(x) = 0$ where $a_{n-k}g(x)$ is of lesser degree than g, so once again we conclude $a_{n-k}g(x) = 0$. Therefore by induction on i we have shown that $a_{n-i}g(x) = 0$ for all $i = 0, 1, \ldots, n$. Explicitly,

$$\begin{aligned} &a_{n-i}(b_m x^m + b_{m-1}x^{m-1} + \cdots + b_0) = 0 \\ &\quad \Longrightarrow a_{n-i}b_m = 0 \qquad \text{for all } i = 0, 1, \ldots, n. \end{aligned}$$

Finally, recalling that b_m was the *nonzero* leading coefficient of g,

$$\begin{aligned} b_m p(x) &= b_m(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0) \\ &= b_m a_n x^n + b_m a_{n-1}x^{n-1} + \cdots + b_m a_0 \\ &= 0, \end{aligned}$$

and the proof is complete. $\square$

Problem 5: Let F be a field and let $a \in F^*$.

(a) If $af(x)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

Proof. Suppose $f(x)$ is reducible over F. Then there exist $g(x), h(x) \in F[x]$ so that $f(x) = g(x)h(x)$ and the degrees of g, h are both less than that of f. Then $af(x) = ag(x)h(x) = \big(ag(x)\big)h(x)$, and since a has degree 0,

$$\deg(af) = \deg(f) \qquad \text{and} \qquad \deg(ag) = \deg(g).$$

So again the degrees of ag, h are less than that of af, and we conclude that af is reducible over F. $\square$

(b) If $f(ax)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

Proof. Suppose $f(x)$ is reducible over F such that $f(x) = g(x)h(x)$ and

$$\deg f > \deg g, \deg h.$$

Note that for any polynomial $p(x) = \sum_{i=0}^{n} c_i x^i \in F[x]$,

$$p(ax) = \sum_{i=0}^{n} c_i (ax)^i = \sum_{i=0}^{n} c_i a^n x^n$$

and since there are no zero divisors, $\deg(p(ax)) = \deg(p(x))$. Then we have $f(ax) = g(ax)h(ax)$ where

$$\deg(f(ax)) > \deg(g(ax)), \deg(h(ax)),$$

so $f(ax)$ is reducible over F. $\square$

(c) If $f(x+a)$ is irreducible over F, prove that $f(x)$ is irreducible over F.

Proof. Again, let $f(x)$ be reducible over F such that $f = gh$ and the degrees of g, h are less than that of f. Note that for any polynomial $p(x) = \sum_{i=0}^{n} c_i x^i \in F[x]$,

$$p(x+a) = \sum_{i=0}^{n} c_i (x+a)^i = \sum_{i=0}^{n} c_i \left[x^i + \binom{i}{1} x^{i-1} a + \binom{i}{2} x^{i-2} a^2 + \cdots + a^i \right].$$

We see that the leading term of $p(x+a)$ is still $c_n x^n$, so $p(x)$ and $p(x+a)$ have equal degree. Clearly then, $f(x+a) = g(x+a)h(x+a)$ is a product of lesser degree polynomials, so $f(x+a)$ is reducible over F. $\square$

(d) Use part **(c)** to show that $f(x) = 8x^3 - 6x + 1$ is irreducible over $\mathbb{Q}$.

Proof. If we can find a function $f(x+a)$ that we know is irreducible over $\mathbb{Q}$, we can conclude from part **(c)** that $f(x)$ is irreducible over $\mathbb{Q}$ as well. We find that

$$f(x+1) = 8(x+1)^3 - 6(x+1) + 1 = 8x^3 + 24x^2 + 18x + 3.$$

Now we see that $f(x+1)$ satisfies the Eisenstein Criterion for prime $p = 3$. Therefore by Theorem 23.15 $f(x+1)$ is irreducible over $\mathbb{Q}$, and by part **(c)** we conclude that $f(x)$ is also irreducible over $\mathbb{Q}$. $\square$

Problem 6: Let $f(x) \in \mathbb{R}[x]$. If $f(a) = 0$ and $f'(a) = 0$, then $(x-a)^2 \big| f(x)$.

Proof. Since $\mathbb{R}$ is a field, the Factor Theorem states that $f(a) = 0$ implies $f(x) = g(x)(x-a)$ for some $g(x) \in \mathbb{R}[x]$. Therefore to show that $(x-a)^2 \big| f(x)$, it suffices to show $(x-a) \big| g(x)$. Taking the derivative, we know from calculus that

$$f'(x) = g'(x)(x-a) + g(x)(1).$$

Recalling that $f'(a) = 0$, we find

$$\begin{aligned} f'(a) &= g'(a)(a-a) + g(a) \\ \Longrightarrow \qquad 0 &= 0 + g(a). \end{aligned}$$

So a is a zero of $g(x)$ and again by the Factor Theorem $g(x) = h(x)(x-a)$ for some $h(x) \in \mathbb{R}[x]$. As mentioned above, this shows that $(x-a)^2 \big| f(x)$. $\square$