Homework 2

MAT1100
Due: November 6, 2014

Ling-Sang Tse

Solution to Problem 1
We first prove Part 2.

Claim 1: $(a)(0) = 0$.
Proof of claim 1:
Since 0 is the additive identity,

$$(a)(0) = (a)(0 + 0),$$

and by the distributive property,

$$(a)(0) = (a)(0 + 0) = (a)(0) + (a)(0).$$

Subtracting both sides by (a)(0), (a)(0) = 0.

Claim 2: $-(a^2) = (-a)(a)$.
Proof of claim 2:
To show that $-(a^2) = (-a)(a)$, we show that (-a)(a) is the additive inverse of a^2.

$$\begin{aligned} a^2 + (-a)(a) &= (a)(a) + (-a)(a) \\ &= (a)[a + (-a)] \text{ by the distributive property} \\ &= (a)(0) \ \text{ since (-a) is the additive inverse of a} \\ &= 0 \text{ by Claim 1} \end{aligned}$$

Therefore, $-(a^2) = (-a)(a)$.
Then

$$\begin{aligned} -(a^2) + (-a)^2 &= (-a)(a) + (-a)(-a) \\ &= (-a)(a + (-a)) \text{ by the distributive property} \\ &= (-a)(0) \text{ since (-a) is the additive inverse of a} \\ &= 0 \text{ by Claim 1} \end{aligned}$$

Therefore, $(-a)^2$ is also an additive inverse of $-(a^2)$. But a^2 is also an additive inverse of a^2 by definition, and additive inverses are unique, so $(-a)^2 = a^2$.

To prove Part 1, letting a = 1, we have $(-1)^2 = 1$.

Solution to Problem 2

1. Let R be a finite integral domain with n elements, and let $r_1, r_2, ..., r_n$ enumerate the elements in R. To show that R is a field, we must show that if x $\in R$ and $x \neq 0$, then x has an inverse.

Consider the set $\{xr_1, .., xr_n\}$.

Claim: $xr_i \neq xr_j$ for any $i \neq j$.
Proof of claim:
Suppose $xr_i = xr_j$. Then

$$xr_i - xr_j = 0 \Leftrightarrow x(r_i - r_j) = 0$$

Then $x = 0$ or $(r_i - r_j) = 0$ because R is an integral domain. Since $x \neq 0$, $r_i = r_j$, so the claim is proven.

Then $xr_1, .., xr_n$ are n distinct elements in R, so $xr_i = 1$ for some r_i. i.e., x has an inverse. Since x was arbitrary, so R is a field.

2. Suppose R is a finite commutative ring, and let P be a prime ideal. Then R/P is an integral domain (this is a theorem from the lecture notes, that if I is an ideal, R/I is an integral domain if and only if I is a prime ideal). But since R is finite, R/P is also finite, so R/P is a finite integral domain. From part a), R/P is then a field, so P is maximal (this is also a theorem from the lecture notes, that if I is an ideal, R/I is a field if and only if I is a maximal ideal).

Solution to Problem 3

1. Suppose R is a Boolean ring, and suppose $x, y \in R$.
Then

$$x^2 + y^2 = (x + y) = (x + y)^2 = x^2 + y^2 + xy + yx$$

Subtracting x^2, y^2, and xy on both sides,

$$-xy = yx$$

.
Then using the last problem, $(-xy)^2 = (xy)^2$, so

$$yx = -xy = (-xy)^2 = (xy)^2 = xy.$$

Since x, y was arbitrary, so R is a commutative ring.

2. Suppose R is a Boolean ring and an integral domain, and suppose $x \in R$.

Since R is a Boolean ring, $x^2 = x$, so $x^2 - x = x(x - 1) = 0$. R is an integral domain, so x=0 or x-1= 0. i.e, x= 0 or x =1. Also, $0 \neq 1$, since R is an integral domain, so 0 or 1 are the only two possible elements in R. Therefore $R = \mathbb{Z}/2$.

Solution to Problem 4
Let R be a commutative ring, and let N(R) be the set of all nilpotent elements of R.

To show that N(R) is a subring:

Let x,y = N(R), so $x^n = y^m = 0$ for some n, m $\in \mathbb{Z}$. Then since R is commutative,

$$\begin{aligned}(x-y)^{n+m} &= \sum_{i}^{n+m} x^i(-y)^{n+m-i} \\ &= \sum_{i=1}^{n-1}(-1)^{n+m-i}x^i y^{n+m-i} + \sum_{i=n}^{n+m}(-1)^{n+m-i}x^i y^{n+m-i} \\ &= 0\end{aligned}$$

To show that the last equality holds:

In the left summation, $n+m-i \geq m$ for all $1 \leq i \leq n-1$, so $y^{n+m-i} = 0$ for all $1 \leq i \leq n-1$, so $\sum_{i=1}^{n-1}(-1)^{n+m-i}x^i y^{n+m-i} = 0$.

In the right summation, $i \geq n$ for all $n \leq i \leq n+m$, so $x^i = 0$ for all $n \leq i \leq n+m$, so $\sum_{i=n}^{n+m}(-1)^{n+m-i}x^i y^{n+m-i} = 0$.

Therefore, x-y is nilpotent, and so N(R) is a subring.

To show that N(R) is an ideal:
Let $r \in R, x \in N(R)$, so $x^n = 0$ for some $n \in \mathbb{Z}$.
Then $(rx)^n = r^n x^n = r^n(0) = 0$, since R is commutative, so $rx \in N(R)$.

Therefore, N(R) is an ideal.

2. Consider the non-commutative ring $M_2(/Z)$, the 2x2 matrices.
Let

$$x = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and

$$y = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Then $x^2 = y^2 = 0$, but

$$x + y = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

so

$$(x+y)^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

is the identity matrix, so x+y is not nilpotent.

Solution to Problem 5
($\Longrightarrow$)
We prove this by induction on the degree of f. Suppose f(x) is invertible, and let g(x) = $b_0 + b_1x + b_2x^2 + ... + b_nx^n$ be its inverse.

Base case: Suppose f = a_0 and $f \in A[x]$ is invertible. If $a_0(b_0 + b_1x + b_2x^2 + ... + b_nx^n) = 1$, then $a_0b_0 = 1$, so a_0 is a unit, and trivially, all other coefficients of f is nilpotent.

Now, assume that for any $p(x) \in A[x]$ such that p(x) has degree n-1 and p(x) is invertible, then p_0 is a unit and all other coefficients are nilpotent. We prove for $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, that a_0 is a unit and all other a_i's are nilpotent:

$$\begin{aligned} f \in A[x] \text{ is invertible } &\Leftrightarrow (a_0 + a_1x + a_2x^2 + ... + a_nx^n)(b_0 + b_1x + b_2x^2 + ... + b_nx^n) = 1 \\ &\text{for some } b_0 + b_1x + b_2x^2 + ... + b_mx^m \in A[x] \\ &\Leftrightarrow \sum_{i=0}^{n}\sum_{j=0}^{m} a_ib_jx^{i+j} = 1 \end{aligned}$$

Matching the coefficients of the constant terms on both sides of the equation, $a_0b_0 = 1$, so a_0 is invertible.

To show that a_n is nilpotent:

Claim: $a_n^{r+1}b_{m-r} = 0$ for all $0 \leq r \leq m$.

Proof of claim by induction:
Base case: Take r = 0. Since the coefficients of x_{n+m} on both sides is 0, so $a_nb_m = 0$.

Now, assume that $a_n^{r+1}b_{m-r} = 0$ for $0 \leq r \leq k-1$, and we show that $a_n^kb_{m-k} = 0$.

$$\begin{aligned} \sum_{j=0}^{k} a_jb_{k-j} = 0 &\Longrightarrow \sum_{j=0}^{k} a_n^k a_jb_{k-j} = 0 \\ &\Longrightarrow a_n^{k+1}b_k = 0 \text{ since } a_n^{r+1}b_{m-r} = 0 \text{ for } 0 \leq r-1 \leq k. \end{aligned}$$

So the claim holds.

Since the claim holds for r = m, $a_n^{m+1}b_0 = 0$. But $a_0b_0 = 1$, so since R is a commutative ring,

$$a_n^{m+1} = a_n^{m+1}a_0b_0 = a_0a_n^{m+1}b_0 = a_0(0) = 0$$

.
Therefore, a_n is nilpotent.

To show that $a_1, .., a_n - 1$ are nilpotent:

Consider h(x) = f(x) - $a_n x^n$.

Claim: h(x) is invertible.

Proof of claim:

Consider g(x)h(x) = g(x)f(x) - g(x)$a_n x^n$ = 1 - g(x)$a_n x^n$.

Note that g(x)$a_n x^n$ is nilpotent, since N(R) is a an ideal and a_n is nilpotent. Then $(g(x)a_n x^n)^m$ = 0 for some integer m.

Then

$$\begin{aligned}
&(g(x)h(x))(1 - g(x)a_n x^n + (g(x)a_n x^n)^2 - ... + (-1)^{m-1}(g(x)a_n x^n)^{m-1}) \\
&= (1 - g(x)a_n x^n)(1 + g(x)a_n x^n - (g(x)a_n x^n)^2 - ... + (-1)^{m-2}(g(x)a_n x^n)^{m-1}) \\
&= 1 + g(x)a_n x^n - (g(x)a_n x^n)^2 - ... + (-1)^{m-2}(g(x)a_n x^n)^{m-1} \\
&- g(x)a_n x^n(1 - g(x)a_n x^n + (g(x)a_n x^n)^2 - ... + (-1)^{m-1}(g(x)a_n x^n)^{m-1}) \\
&= 1 + (-1)^{m-2}(g(x)a_n x^n)^m \\
&= 1
\end{aligned}$$

Therefore, $(g(x))(1 - g(x)a_n x^n + (g(x)a_n x^n)^2 - ... + (-1)^{m-1}(g(x)a_n x^n)^{m-1})$ is an inverse for h(x), so h(x) is invertible, and so the claim holds.

Then h(x) = $a_0 + ... + a_{n-1}x^{n-1}$ is a polynomial of degree n-1, so by assumption in the induction on the degree of f, $a_1, ..., a_{n-1}$ are all nilpotent.

($\Longleftarrow$)
Suppose $f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n \in A[x]$, with a_0 a unit and the rest of the coefficients nilpotent. Then let b_0 be such that $a_0 b_0 = 1$ and $a_i^m = 0$ for the rest of the coefficients $a_i's$. i.e., $(f(x) - a_0)^m = 0$.

$$\begin{aligned}
&b_0 f(x)(1 + b_0[(f(x) - a_0) - (f(x) - a_0)^2 - ... + (-1)^{m-2}(f(x) - a_0)^{m-1})]) \\
&= (1 - (b_0)(f(x) - a_0))(1 + b_0[(f(x) - a_0) - (f(x) - a_0)^2 - ... + (-1)^{m-2}(f(x) - a_0)^{m-1})]) \\
&= (1 - b_0[(f(x) - a_0) + (f(x) - a_0)^2 - ... + (-1)^{m-2}(f(x) - a_0)^{m-1})]) - \\
&[b_0(f(x) - a_0)](1 - b_0[(f(x) - a_0) + (f(x) - a_0)^2 - ... + (-1)^{m-2}(f(x) - a_0)^{m-1})]) \\
&= 1 + (-1)^{m-2}[b_0(f(x) - a_0)]^m \\
&= 1
\end{aligned}$$

Therefore, $b_0(1 + b_0[(f(x) - a_0) - (f(x) - a_0)^2 - ... + (-1)^{m-2}(f(x) - a_0)^{m-1})])$ is an inverse for f(x), so f is invertible in $A[x]$.