MAT 1100 Homework 3

Michael Yu

1. Note that I let multiplication have precedence over taking additive inverse, *i.e.* $-ab = -(ab)$.

2.
Lemma. $(-a)b = -ab = a(-b)$

Proof.

$$\begin{aligned} & (-a)b \\ &= (-a)b + ab + (-ab) \\ &= ((-a) + a)b + (-ab) \\ &= 0b + (-ab) \\ &= -ab \\ &= (-ab) + a0 \\ &= (-ab) + a(b + (-b)) \\ &= (-ab) + ab + a(-b) \\ &= a(-b) \end{aligned}$$

□

The equation in the problem follow from applying 2. twice. $(-a)(-a) = -a(-a) = -(-aa) = aa$

1. Use (2.) by taking $a = 1$.

2. Another note: I *despise* the $f(x)$ function application notation and will instead write fx in place, where an invisible "application" operator connects f and x. This function application operator shall be the highest precedence operator I will use so there is no ambiguity in parsing.

1. Let R be an integral domain and consider any $a \in R$ where $a \neq 0$. By the cancellation property of multiplication in R, we have for any $b, b' \in R$ that $ab = ab' \implies b = b'$. In other words, the multiplication-by-a function $\mu_a : R \to R,\ b \mapsto ab$ is injective. By the pigeonhole principle, this implies $|\operatorname{im} \mu_a| \geq |R|$, and since $\operatorname{im} \mu_a \subseteq R$, this means $\operatorname{im} \mu_a = R$. Hence μ_a is a bijection $R \to R$ and has an inverse μ_a^{-1}, whence we have an element $\mu_a^{-1} 1 \in R$ satisfying $a(\mu_a^{-1} 1) = \mu_a(\mu_a^{-1} 1) = 1$ and then also $(\mu_a^{-1} 1)a = 1$ by commutativity. Therefore $(R \setminus \{0\})^{\times}$ satisfies all the conditions for being a field and hence R is a field.

2. Let R be a finite commutative ring and let P be a prime ideal of R. Then R/P, being a set of equivalence classes of the finite set R, must itself be finite. Since P is prime, we know R/P is an integral domain. But by (1.), every finite integral domain is a field. Finally, R/P being a field implies P is a maximal ideal.

3. Let R be a boolean ring, with or without unit for more generality.

1.

Lemma. *Every $a \in R$ satisfies $a + a = 0$. In other words $a = -a$.*

Proof.

$$\begin{aligned}0 &= (a+a) - (a+a)\\ &= (a+a)^2 - (a+a)\\ &= a(a+a) + a(a+a) - (a+a)\\ &= a^2 + a^2 + a^2 + a^2 - (a+a)\\ &= (a+a) + (a+a) - (a+a)\\ &= a + a\end{aligned}$$

$\square$

Back to the problem. Let $a, b \in R$.

$$\begin{aligned}0 &= (a+b)^2 - (a+b)\\ &= a(a+b) + b(a+b) - (a+b)\\ &= a^2 + ab + ba + b^2 - (a+b)\\ &= (ab+ba) + (a+b) - (a+b)\\ &= ab + ba\end{aligned}$$

Therefore $ab = -ba = ba$.

2. Assume furthermore that R is a domain, and if R is a ring without unit, also assume that R is nontrivial.

   Let $a \in R$ with $a \neq 0$. Suppose for contradiction there is another $b \in R$ where $0 \neq b \neq a$. Then $a - b \neq 0$ so it follows from R being a domain that

   $$0 \neq (a-b)b = ab - b^2 = ab - b$$

   but then

   $$0 \neq a(ab-b) = a^2b - ab = ab - ab = 0$$

   leading to a contradiction, showing b cannot exist. Therefore $R = \{0, a\}$ where $a + a = 0$ and $a^2 = a$, showing the map $R \to \mathbb{Z}/2\mathbb{Z}$ that takes $0 \mapsto 0$ and $a \mapsto 1$ is an isomorphism.

4. 1. Let $x, y \in \eta R$ where $x^m = 0 = y^n$ with $m, n > 0$ and let $a \in R$ be arbitrary.

   * $0^1 = 0 \implies 0 \in \eta R$
   * Note that if $n \in \mathbb{N}$ then nx just means $\underbrace{x + \cdots + x}_{n \text{ repetitions of } x}$

$$\begin{aligned}(x+y)^{m+n} &= \sum_{k=0}^{m+n} \binom{m+n}{k} x^k y^{m+n-k}\\ &= \sum_{k=0}^{m-1} \binom{m+n}{k} x^k y^n y^{m-k} + \binom{m+n}{m} x^m y^n + \sum_{k=m+1}^{m+n} \binom{m+n}{k} x^m x^{k-m} y^{m+n-k}\\ &= \sum_{k=0}^{m-1} \binom{m+n}{k} x^k 0 y^{m-k} + \binom{m+n}{m} 00 + \sum_{k=m+1}^{m+n} \binom{m+n}{k} 0 x^{k-m} y^{m+n-k}\\ &= 0 \quad \implies \quad x + y \in \eta R\end{aligned}$$

- $*$ $(-x)^m$ equals either $-(x^m) = -0 = 0$ or $x^m = 0$ by problem (**1.**), showing $-x \in \eta R$.
- $*$ $(ax)^m = a^m x^m = a^m 0 = 0 \implies ax \in \eta R$

2. Consider the ring of 2×2 $\mathbb{R}$-valued matrices. Let

$$x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

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

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

So $x + y$ is not nilpotent and hence ηR is not an ideal.

5. Write $f = \sum_{i=0}^m a_i x^i$ where $a_m \neq 0$. We will use these variables throughout this problem.

$\Longleftarrow$ We prove the required using a few intermediate results.
Lemma. *If $t \in A$ is nilpotent with $t^n = 0$, then $1 - t$ is a unit.*

Proof. $(1-t)\left(\sum_{k=0}^{n-1} t^k\right) = \left(1 + \sum_{k=1}^{n-1} t^k\right) - \left(\sum_{k=1}^{n-1} t^k + t^n\right) = 1 - t^k = 1$ □

Corollary. *If u is a unit and p is nilpotent with $t^n = 0$, then $u + t$ is a unit.*

Proof. The nilpotent elements form an ideal, so $-u^{-1}p$ is nilpotent. So $u + p = u(1 - u^{-1}p)$ is then a product of units and hence a unit itself. □

Lemma. *Any polynomial $h = \sum_{k=0}^n c_k x^k$ with $c_n \neq 0$ in $A[x]$ where all its coefficients are nilpotent in A is itself nilpotent in $A[x]$.*

Proof. $h = (\dots(c_n x + c_{n-1})x + c_{n-2})\dots)x + c_0$. But to be precise we will use induction on n.

If $n = 0$ then $g = a_0$ which is then nilpotent. Now assume for some $n > 0$ any polynomial with nilpotent coefficients with degree less than n is nilpotent. We have $h = a_0 + x(h/x)$, where h/x is a polynomial with degree less than n and with all coefficients nilpotent, so it is nilpotent. Because nilpotent polynomials form an ideal, h is also nilpotent. □

Now to tackle the problem. We have $f = a_0 + \sum_{i=1}^m a_i x^i$ where a_0 is a unit and each other a_i is nilpotent. By the second lemma, the polynomial $\sum_{i=1}^m a_i x^i$ is nilpotent. By the corollary to the first lemma, f is a unit in $A[x]$.

$\Longrightarrow$ First I show that the nonconstant term coefficients are nilpotent. Consider any $k \in \{1, \dots, m\}$ and define the set $S_k := \left\{a_k^j : j \in \mathbb{N}\right\}$ (note $\mathbb{N} \ni 0$). Clearly S_k is multiplicatively closed, so we can consider the localization at S_k, the ring $S_k^{-1}A$. Suppose for contradiction that $S_k \not\ni 0$, *i.e.* that $S_k^{-1}A$ is a nontrivial ring. Then $S_k^{-1}A$ has a proper maximal ideal J (since the collection of proper ideals contain at least $\{0\}$ and so must have a maximal element by Zorn's lemma). Define

$$\phi_k : A \to S_k^{-1}A, \qquad \psi_k : S_k^{-1}A \to S_k^{-1}A/J$$

to be the canonical homomorphisms. We then have the induced homomorphisms

$$\Phi_k : A[x] \to S_k^{-1}A[x], \qquad \Psi_k : S_k^{-1}A[x] \to S_k^{-1}A/J[x]$$

Now

$$((\Psi_k \circ \Phi_k)f)((\Psi_k \circ \Phi_k)f^{-1}) = (\Psi_k \circ \Phi_k)(ff^{-1}) = (\Psi_k \circ \Phi_k)1 = 1$$

where that final 1 is $1_{S_k^{-1}A/J[x]}$, the multiplicative unit in the polynomial ring $S_k^{-1}A/J[x]$. We know that

$$(\Psi_k \circ \Phi_k)f = \sum_{i=0}^{m}((\psi_k \circ \phi_k)a_i)x^i$$

Since J is a maximal ideal, $S_k^{-1}A/J$ is a field. But we know that in the ring of polynomials of a field, a polynomial is invertible if and only if the polynomial has inverible constant term and no other terms, because the degree of the polynomial does not decrease when multiplied by any polynomial except 0. Hence for each $i > 0$, the coefficient $(\psi_k \circ \phi_k)a_i$ equals 0. In particular, $\psi_k(\phi_k a_k) = 0$, but $\phi_k a_k$ is a unit in $S_k^{-1}A$ that is not in J, showing $\phi_k a_k = 0 \in S_k^{-1}A$, implying $S_k^{-1}A$ is the trivial ring, a contradiction.

(*Explanation.* Note that this is only a proof by contradiction because the "trivial field" with 1 element cannot exist by definition and a maximal ideal is not allowed to equal the whole ring; if the trivial field is considered a field and J can equal $S_k^{-1}A$ then this proof would just prove that $S_k^{-1}A/J$ is the trivial field, implying $S_k^{-1}A$ is the trivial ring.)

(*More explanation.* This is another side of the coin of the following approach. Each a_k $(k > 0)$ is in every prime ideal, or equivalently $a_k = 0$ in the quotient ring, because taking the quotient by a prime ideal yields an integral domain and an invertible polynomial in an integral domain cannot have positive degree because degree does not decrease when multiplied by something nonzero in a polynomial ring of an integral domain. But the nilradical just equals the intersection of all prime ideals, so each a_k is in the nilradical, *i.e.* each a_k is nilpotent.)

From the above we conclude that $0 \in S_k$, *i.e.* a_k is nilpotent.

Next, to show the constant term is invertible, we can use the first part. If f is a unit, then $a_0 = f - (f - a_0)$ is the sum of a unit and a polynomial with nilpotent coefficients, which must be nilpotent, so a_0 is a unit in $A[x]$. Multiplying by a unit constant term in $A[x]$ does not decrease degree, so the inverse of a_0 also has degree 0, whence a_0 is a unit in A.