Homework Assigment 12 Solutions

This is a shorter assignment. We will use Sun Tzu's theorem to study the Euler totient function, and we will see an example where the nilradical and Jacobson radical are distinct. First we will need a definition.

Definition 1. *Let $n \in \mathbb{N}$ be a natural number. Then Euler's totient function of n is:*

$$\varphi(n) := \#\{1 \leq a \leq n : \gcd(a, n) = 1.\}$$

This is often also called Euler's φ function.

1. In this problem φ denotes Euler's totient function.

   (a) Let R, S be two unital rings. Show that $(R \times S)^\times \cong R^\times \times S^\times$.

   Proof. We will view both as subsets of $R \times S$, and show they contain eachother. First fix $(r, s) \in (R \times S)^\times$. Then there is some inverse (r', s') such that $(r, s)(r', s') = (1_R, 1_S) = (r', s')(r, s)$. Since multiplication is componentwise, this implies that $rr' = r'r = 1_R$ and $ss' = s's = 1_S$ so that $r \in R^\times$ and $s \in S^\times$. Thus $(R \times S)^\times \subseteq R^\times \times S^\times$. Conversely, fix $(r, s) \in R^\times \times S^\times$. Then r has an inverse r^{-1} and s has an inverse s^{-1} and it is immediate that $(r, s)^{-1} = (r^{-1}, s^{-1})$ so that $(r, s) \in (R \times S)^\times$. □

   (b) Let φ be Euler's totient function, and $n \in \mathbb{N}$. Explain why $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

   Proof. This is immediate, since $(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$, and each element of $\mathbb{Z}/n\mathbb{Z}$ has a unique residue between 1 and n. □

   (c) Let m, n be comprime natural numbers. Use Sun-Tzu's theorem as well as part (a) and (b) to prove that $\varphi(mn) = \varphi(m)\varphi(n)$.

   Proof. Since $\gcd(m, n) = 1$, we know that there is some $u, v \in \mathbb{Z}$ with $um + vn = 1$. Therefore $m\mathbb{Z} + n\mathbb{Z} = 1$ and so m, n are comaximal. Thus by Sun-Tzu's theorem, $(\mathbb{Z}/mn\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ (as rings!). By part (a), $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$. In particular:

   $$\varphi(mn) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times| \cdot |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(m)\varphi(n).$$

   □

   (d) Let p be a prime number and j a positive integer. Give a formula for $\varphi(p^j)$, and fully justify your answer.

   Proof. The numbers $\leq p^j$ which are *not* coprime to p^j are the multiples of p:

   $$\{p, 2p, 3p, ..., (p^{j-1} - 1)p, p^{j-1}p = p^j\}.$$

   There are exactly p^{j-1} of these. $\varphi(p^j)$ counts the numbers $\leq p^j$ which are not in this set, so there are $p^j - p^{j-1}$ of these, so $\varphi(p^j) = \varphi(p^{j-1})$. □

(e) Use parts (c) and (d) to establish the following general formula for φ:

$$\varphi(N) = N \cdot \left(\prod_{\substack{\text{primes } p \\ \text{with } p|N}} \left(1 - \frac{1}{p}\right) \right).$$

Proof. This follows from a formal manipulation. First let $N = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ be the prime factorization of N. Then we have:

$$\begin{aligned}
\varphi(N) &= \varphi\left(\prod_{i=1}^{t} p_i^{\alpha_i}\right) \\
&= \prod_{i=1}^{t} \varphi(p_i^{\alpha_i}) \\
&= \prod_{i=1}^{t} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right) \\
&= \prod_{i=1}^{t} \left(p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)\right) \\
&= p_1^{\alpha_1} \cdots p_t^{\alpha_t} \left(\prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right)\right) \\
&= N \left(\prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right)\right)
\end{aligned}$$

as desired. □

In Takehome 3 we introduced two interesting ideals of a commutative unital ring: the Jacobson radical and the nilradical. These were clearly related, and are often the same, but sometimes they are different. Let's investigate!

2. Prove that $\mathfrak{J}(R) = \mathfrak{N}(R)$ in each of the following cases.

(a) $R = \mathbb{Z}$

Proof. Suppose $n \in \mathfrak{J}(\mathbb{Z})$, so that n is in every maximal ideal of $\mathbb{Z}$. Since the maximal ideals of $\mathbb{Z}$ are the ideals (p) for every prime p, this says that n is a multiple of every prime p, so that $n = 0$. Therefore $\mathfrak{J}(\mathbb{Z}) = 0$. Since $\mathfrak{N}(\mathbb{Z}) \subseteq \mathfrak{J}(\mathbb{Z})$ (by TH3 Problem 4(a)), the nilradical must be zero as well. □

(b) $R = K[x]$ where K is any field.

Proof. As in part (a), we will show that $\mathfrak{J}(K[x]) = 0$. Rather than try to enumerate the maximal ideals of $K[x]$, we will use the characterization of TH3 Problem 4(d). Suppose r is in the Jacobson radical. Then $1 - ry$ is a unit for all $y \in K[x]$. We know the units of $K[x]$ are precisely the constant polynomials. In particular $1 - r = c$ for some

$c \in K^\times$, so that $r = 1 - c \in K$. If $c \neq 1$ then r is a unit, so letting $y = r^{-1}$ we have $1 - rr^{-1} = 1 - 1 = 0$, which is not a unit, contradicting that $r \in \mathfrak{J}(K[x])$. Therefore $c = 1$, and $r = 1 - 1 = 0$. Therefore we have shown that $\mathfrak{J}(K[x]) = 0$, and so by TH3 Problem 4(a), $\mathfrak{N}(K[x]) = 0$ as well. □

(c) $R = \mathbb{Z}/n\mathbb{Z}$.

Proof. We will prove this in two ways, just to give a flavor of the type of techniques at our disposal. For a first proof, we will show that all the prime ideals in $\mathbb{Z}/n\mathbb{Z}$ are maximal, which implies the result. We first take care of the case where n is prime. Then $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field, and the only prime ideal is (0), which is also maximal. For the general case we use the fourth isomorphism theorem to notice that there is a bijection between ideals in $\mathbb{Z}/n\mathbb{Z}$ and ideals in $\mathbb{Z}$ that contain the ideal (n). The ideals in $\mathbb{Z}$ containing (n) are precisely the ideals (d) for $d|n$. These correspond to $d\mathbb{Z}/n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$. Notice that if $d\mathbb{Z}/n\mathbb{Z}$ is prime, so is (d). Indeed, (d) is the preimage of of $d\mathbb{Z}/n\mathbb{Z}$ under the projection, and the preimage of a prime ideal is prime by TH3 Problem 1(a). Therefore the nonzero prime ideals of $\mathbb{Z}/n\mathbb{Z}$ are precisely $p\mathbb{Z}/n\mathbb{Z}$ for prime p dividing n. But these must be maximal by the fourth isomorphism theorem, since and ideal containing $p\mathbb{Z}/n\mathbb{Z}$ corresponds to an ideal containing (p). To finish we must show that when n is not prime, the zero ideal in $\mathbb{Z}/n\mathbb{Z}$ is not prime. Indeed, suppose $ab = n$ for $a, b \neq \pm 1$. Then $\overline{a}, \overline{b} \notin (0) \subseteq \mathbb{Z}/n\mathbb{Z}$, but $ab \in (0)$.
To set up the second proof, we will first prove the following lemma.

Lemma 2. *Let S and T be commutative unital rings. $\mathfrak{J}(S \times T) = \mathfrak{J}(S) \times \mathfrak{J}(T)$, and $\mathfrak{N}(S \times T) = \mathfrak{N}(S) \times \mathfrak{N}(T)$*

Proof. We start with the case for the nilradical. But this is clear, as $(s, t) \in S \times T$ is nilpotent if and only if s and t both are. Next we show the case for the Jacobson radical, using the characterization of TH3 Problem 4(d). Fix a tuples $(s, t) \in S \times T$. Then for any $y = (y_1, y_2)$ we have $1 - y(s, t) = (1 - y_1 s, 1 - y_2 t)$. By 1(a) above, $1 - y(s, t)$ is a unit in $S \times T$ if and only if $1 - y_1 s$ and $1 - y_2 t$ are units in S and T respectively. Therefore, varying y_1 and y_2 over all the elements of S and T and applying TH3 Problem 4(d) we observe that (s, t) is in $\mathfrak{J}(S \times T)$ if and only if $s \in \mathfrak{J}(S)$ and $t \in \mathfrak{J}(T)$. □

Now we prove that $\mathfrak{J}(\mathbb{Z}/n\mathbb{Z}) = \mathfrak{N}(\mathbb{Z}/n\mathbb{Z})$. Let $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ be a prime factorization of n into primes. Then Sun-Tzu's theorem says that

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{\alpha_1}\mathbb{Z} \times \mathbb{Z}/p_2^{\alpha_2}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}.$$

Therefore the Lemma tells us that

$$\mathfrak{J}(\mathbb{Z}/n\mathbb{Z}) \cong \mathfrak{J}(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \mathfrak{J}(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times \mathfrak{J}(\mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}),$$

and

$$\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) \cong \mathfrak{N}(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \mathfrak{N}(\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z}) \times \cdots \times \mathfrak{N}(\mathbb{Z}/p_t^{\alpha_t}\mathbb{Z}).$$

Therefore it suffices to prove the result when $n = p^\alpha$ is a power of a prime. In this case we know by 3(c) below that the only maximal ideal of $\mathbb{Z}/p^\alpha\mathbb{Z}$ is the ideal (p), so that $\mathfrak{J}(\mathbb{Z}/p^\alpha\mathbb{Z}) = (p)$. On the other hand, $p^\alpha = 0$, so that $p \in \mathfrak{N}(\mathbb{Z}/p^\alpha\mathbb{Z})$. Therefore $\mathfrak{J}(\mathbb{Z}/p^\alpha\mathbb{Z}) \subseteq \mathfrak{N}(\mathbb{Z}/p^\alpha\mathbb{Z})$. The reverse containent is TH3 Problem 4(a).

□

To find a ring where they differ, we will use the following definition:

Definition 3. *A commutative unital ring is called a local ring if it has a unique maximal ideal.*

Remark. *This terminology is related to the analogy between points of X and maximal ideals of* $\mathrm{Maps}(X, \mathbb{R})$*, so that only having one maximal ideal is related to having only one point (which is certainly "local").*

3. Let's study some properties of local rings. Throughout, R will denote a commutative unital ring.

   (a) Let R be a local ring. Show that every element not contained in the maximal ideal is a unit.

   Proof. If $r \in R$ is not contained in the unique maximal ideal, it is not contained in *any* maximal ideal, so that by TH3 Problem 4(a), it is a unit. □

   (b) Conversely, show that if the set $\mathfrak{m} = R \setminus R^\times$ of nonunits of R form an ideal, then R is a local ring with maximal ideal $\mathfrak{m}$.

   Proof. We first show that $\mathfrak{m}$ is a maximal ideal. Indeed, suppose $\mathfrak{m} \subseteq J \subseteq R$. If $J \neq \mathfrak{m}$, then J contains a unit (since $R^\times = R \setminus \mathfrak{m}$). Therefore (by HW11 Problem 5(a)), $J = R$. Now let $\mathfrak{n}$ be any maximal ideal of R. Since $\mathfrak{n}$ consists entirely of nonunits, we hae $\mathfrak{n} \subseteq \mathfrak{m}$, so that by maximality of $\mathfrak{n}$ we have $\mathfrak{n} = \mathfrak{m}$. □

   (c) Let p be prime and j a positive integer. Prove that $\mathbb{Z}/p^j\mathbb{Z}$ is a local ring. What is the maximal ideal?

   Proof. The nonunits of $\mathbb{Z}/p^j\mathbb{Z}$ are precisely residue classes a which are not prime to p^j. Arguing as in 1(d), these are precisely the multiples of p. In particular, we see that the set of nonunits of $\mathbb{Z}/p^j\mathbb{Z}$ is precisely the ideal (p). By part (b), we conclude that $\mathbb{Z}/p^j\mathbb{Z}$ is local with maximal ideal (p). □

   (d) Let R be a local ring which is an integral domain and not a field. Prove that $\mathfrak{J}(R) \neq \mathfrak{N}(R)$.

   Proof. We first observe that $\mathfrak{N}(R) = 0$. Indeed, HW10 Problem 3(a) shows that nilpotent elements are either zero divisors or 0, and R has no nonzero zero divisors (being an integral domain), so the only nilpotent element of R is 0. On the other hand, we can see that $\mathfrak{J}(R)$ is nonzero. Indeed, since R is a local ring, $\mathfrak{J}(R) = \mathfrak{m}$, where $\mathfrak{m}$ is the unique maximal ideal. But if $\mathfrak{m}$ is zero, then the only ideals of R would be 0 and R, so that R would have to be a field (applying HW11 Problem 5(d)). Since we are assuming R is not a field, we must conclude that $\mathfrak{m}$ is nonzero. □

Therefore, to construct an example where $\mathfrak{J}(R) \neq \mathfrak{N}(R)$, we must construct a ring satisfying 3(d).

Definition 4. *Let R be a commutative unital ring. The ring of formal power series $R[[x]]$ is the set of power series:*

$$\left\{ \sum_{i=0}^{\infty} a_i x^i \text{ such that } a_i \in R \right\}.$$

The binary operations are:

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) + \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

$$\left(\sum_{i=0}^{\infty} a_i x^i \right) \times \left(\sum_{i=0}^{\infty} b_i x^i \right) = \sum_{i=0}^{\infty} \left(\sum_{k=0}^{i} a_k b_{i-k} \right) x^i.$$

4. Let R be a commutative unital ring.

   (a) Prove that $R[[x]]$ is a commutative unital ring.

   Proof. Rather than check this is a commutative unital ring directly, which is tedious, we will deduce it from the following case for polynomial rings. If $f = \sum_{i=0}^{\infty} a_i x^i \in R[[x]]$ we denote let $f_n = \sum_{i=0}^{n} a_i x^i$ be its truncation of degree n. Then the following observations are immediate from the formulas.

   i. $f = g$ if and only if $f_n = g_n$ for all n.
   ii. $(f+g)_n = f_n + g_n$.
   iii. $(fg)_n = (f_n g_n)_n$ (where we take the polynomial $f_n g_n$ which may have dgree $2n$ and truncate it down to degree n).

   The third is perhaps slightly nontrivial, but follows immediately from the fact that ith coefficient on fg only depends on the 0 through ith coefficients of f and g, which is apparent from the formulas. Now the ring axioms follow easily since we know they hold for polynomial rings, and therefore hold after truncation by n for each n. We do associativity of multiplication as an example. We first observe that for all n $(f_n g_n)h_n = f_n(g_n h_n)$ (since multiplication of polynomials is associative). It therefore follows that $((fg)h)_n = (f(gh))_n$ for all n, so that $(fg)h = f(gh)$. The rest of the checks are identical. That is, given an equation of an axiom in terms of $f \in R[[x]]$, we know the equation holes for f_n for all n because polynomial rings are rings and truncation is compatible with multiplication and addition. Therefore by (1) above, we know it holds for f. □

   (b) If R is an integral domain, prove that $R[[x]]$ is.

   Proof. Let $f, g \in R[[x]]$ be nonzero. Write $f = a_n x^n + a_{n+1} x^{n+1} + \cdots$ and $g = b_m x^m + b_{m+1} x^{m+1} + \cdots$, with $a_n, b_m \neq 0$. Then $fg = (a_n b_m) x^{n+m} + (a_n b_{m+1} + a_{n+1} b_m) x^{n+m+1} + \cdots$. Since R is an integral domain, $a_n b_m \neq 0$, so that $fg \neq 0$, completing the proof. □

   (c) Prove that $1 - x$ is a unit in $R[[x]]$. (Hint: remember the geometric series?).

   Proof. We consider the following formal equation (which you may recognize from studying convergent power series in calculus):

$$\frac{1}{1-x} = \sum_{i=0}^{\infty} x^i.$$

In calculus this power series had a so-called *radius of convergence*, so that $1-x$ was invertible in some neighborhood of 0. In the ring of formal power series, the right side of the equation is a perfectly well defined object of $R[[x]]$. The fact that it is an inverse of $1-x$ is just a formal calculation, indeed on can easily check that:

$$(1-x)(1+x+x^2+x^3+\cdots) = 1-x+(x-x^2)+(x^2-x^3)\cdots = 1.$$

□

(d) Prove that $\sum a_i x^i$ is a unit in $R[[x]]$ if and only if a_0 is.

Proof. If $f = a_0+a_1x+a_2x^2+\cdots$ is a unit, with inverse $g = b_0+b_1x+b_2x^2+\cdots$, then:

$$fg = a_0b_0 + (a_1b_0+a_0b_1)x+\cdots = 1.$$

In particular, $a_0b_0 = 1 \in R$ so that $a_0 \in R^\times$. Conversely, suppose a_0 is a unit. We give 2 proofs that f is invertible. The first is to construct f^{-1} inductively. We want $g = b_0+b_1x+b_2x^2+\cdots$ to be the inverse. Let $fg = c_0+c_1x+c_2x^2+\cdots$ where

$$c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

We want $c_0 = 1$ and $c_k = 0$ for all $k > 0$. So certainly $b_0 = a_0^{-1}$. For c_1 to equal 0 we need $a_0b_1+b_0a_1 = 0$. Solving for b_1 gives $b_1 = \frac{-b_0a_1}{a_0}$. We now proceed by induction. Suppose we've found $b_0,\cdots,b_{k-1}$ so that $c_1 = \cdots = c_{k-1} = 0$. Then we may plug $c_k = 0$ into the equation above and solve for b_k:

$$b_k = \frac{-\sum_{k=1}^{n} a_k b_{i-k}}{a_0}.$$

At each step we may safely divide by a_0, and so we may find each b_k in this fashion.

We present a second proof, that essentially uses a modification of the geometric series trick from part (c). Consider

$$a_0^{-1}f = 1+(a_1/a_0)x+(a_2/a_0)x^2+\cdots = 1-xy,$$

where $y = -(a_1/a_0)-(a_2/a_0)x-\cdots$. Notice that,

$$\frac{1}{1-xy} = \sum_{i=0}^{\infty}(xy)^i,$$

as long as the equation on the right is well defined. Adding up infinitely many elements in a ring need not be well defined. To be well defined, it means it needs to equal $\sum_{i=0}^{\infty} b_i x^i$ for some $b_i \in R$. Let's suppose we wanted to compute b_t. It is clear that b_t is determined by $\sum_{i=0}^{t}(xy)^i$, since all higher powers in the sum on the right start off with an x^{t+1} or a larger power of x, and therefore have no effect on b_t. One can think of this as some sort of algebraic way to say that the sum on the right converges in $R[[x]]$. In some sense this is exactly what we are doing when we solved for the b_k in the inductive proof. □

(e) Let K be a field. Prove that $K[[x]]$ is a local ring with maximal ideal (x). Conclude that $\mathfrak{N}(K[[x]]) \neq \mathfrak{J}(K[[x]])$.

Proof. We use the characterization of local rings from 3(b) above. We saw that a power series $\sum_{i=0}^{\infty} a_i x^i$ is a unit if and only if $a_0 \in K^\times$, which since K is a field is true if and only if $a_0 \neq 0$. In particular, the nonunits of $K[[x]]$ are exactly those with constant term equal to 0. These are precisely the multiples of x, so the nonunits form the ideal (x). Therefore 3(b) says that $K[[x]]$ is a local ring with maximal ideal x. Since $K[[x]]$ is an integral domain (by part (b)), and the not a field (since it has a nontrivial ideal), 3(d) tells us that the nilradical and Jacobson radical don't agree. Indeed, the nilradical is (0) and the Jacobson radical is (x). □