CS203: Abstract Algebra
Assignment 4 Solutions

Ayush Bansal
Roll No. 160177

September 11, 2017

I   Problem 1 Solution

1.1   Part 1

We are given a commutative ring R. This ring contains nilpotent elements i.e. $x^n = 0, x \in R$ for a certain positive integer n.

I have to prove that set of all nilpotent elements of a ring R forms an ideal which is known as **nilradical** of R.

Proof. Consider 2 nilpotent elements x and y such that $x^m = 0$ and $y^n = 0$, let these elements belong to an ideal I, Now we consider the 2 properties of ideals.

1. If $a \in I, b \in I \Rightarrow a + b \in I$:

Let $x + y = k$, raising power on both sides to $m + n$ which gives us the following equations when expanded by binomial expansion.

$$k^{m+n} = x^{m+n} + {}^{m+n}C_1 x^{m+n-1} y + \cdots + y^{m+n}$$

The above equation shows that $k^{m+n} = 0$ and thus k is nilpotent which means $k \in I$.

2. If $a \in I, b \in R \Rightarrow ab \in I$:

Let a be an element of ring R, multiplying x and a and raising the power to m we get $x^m a^m = 0$ since $x^m = 0$, which means that $xa \in I$ as xa is nilpotent.

By above 2 properties, the proof is complete. $\square$

1.2   Part 2

A set S is defined such that it is the intersection of all the prime ideals of the ring R.

I have to prove that set S contains **nilradical** of R.

Proof. Let x be an element from the nilradical of R, such that $x^n = 0$.

Consider a prime ideal P, I will show that $x \in P$ which will in turn prove our claim that each nilpotent element of R will lie in each and every prime ideal.

We know that $x^n = 0$, $\because P$ is a prime ideal, $0 \in P$ which means $x^n \in P$ or we can say $x \cdot x^{n-1} \in P$ and by **definition of prime ideal**, $x \cdot x^{n-1} \in P$ means either $x \in P$ or $x^{n-1} \in P$, if first is true then we are done otherwise we do same thing with $x^{n-1} \in P$ as follows until $x \in P$:

$$x^n \in P \Rightarrow x \in P \parallel x^{n-1} \in P$$
$$x^{n-1} \in P \Rightarrow x \in P \parallel x^{n-2} \in P$$
$$\vdots$$
$$x^2 \in P \Rightarrow x \in P.$$

Thus by above equations it is clear that every nilpotent element will be there in each and every prime ideal. $\square$

1.3 Part 3

Assume x is not a nilpotent element and consider the following relation:

$$\mathscr{Y} = \{I \mid I \text{ is an ideal of } R \text{ and } \forall n \in \mathbb{Z}_{>0}, x^n \notin I\}$$

I have to prove that $\mathscr{Y}$ forms a partially ordered set w.r.t. set inclusion operation.

Proof. Firstly this set will be non-empty as there will be atleast zero ideal (0) in the set.
The elements of the set $\mathscr{Y}$ are ideals of R, we will see the relation of set inclusion operation in this set, consider the following 3 properties:
Reflexivity: Each element is comparable to itself.
    Consider an ideal $I \in \mathscr{Y}$, since $I \subseteq I$, the property is satisfied.
Anti-symmetry: No two different elements precede each other.
    Consider ideals $I_1, I_2 \in \mathscr{Y}$, $I_1 \subseteq I_2$ and $I_2 \subseteq I_1$ which implies $I_1 = I_2$, thus this property is also satisfied.
Transitivity: The start of a chain of precedence relations must precede the end of the chain.
    Consider ideals $I_1, I_2, I_3 \in \mathscr{Y}$, $I_1 \subseteq I_2$ and $I_2 \subseteq I_3$ which implies $I_1 \subseteq I_3$, thus the final property is satisfied.
By above three properties, we can say by **definition of Poset**, that the set $\mathscr{Y}$ is a **Partially Ordered Set**. $\qquad\square$

1.4 Part 4

We have to work on the same set $\mathscr{Y}$ given in the last part.
I have to prove that $\mathscr{Y}$ has a maximal element.

Proof. I will first start by proving 2 properties of the set $\mathscr{Y}$.

Claim 1.4.1. *Set $\mathscr{Y}$ is non-empty.*

Proof. Firstly, since x is not nilpotent, $x^n \neq 0$ for any n, so $x^n \notin (0)$ for any n, thus there is atleast one element in the set which is the **zero ideal** (0), so the set is non-empty. $\qquad\square$

Claim 1.4.2. *Any **chain of ideals** in $\mathscr{Y}$ has an upper bound in $\mathscr{Y}$.*

Proof. Let C be a chain of ideals in $\mathscr{Y}$, now take the union of all the ideals in the this chain which will give us an ideal of R, also since the powers of the elements in this ideal will remain the same they were before in the chain because we are just taking the union and not manipulating the elements.
By above arguments we can see that the union of all the ideals in a chain C will be an ideal in $\mathscr{Y}$ and this **union** will be our **upper bound** of chain C. $\qquad\square$

    Hence, by using the proven claims we can apply the following **Zorn's Lemma**:

Lemma 1.1 (Zorn's Lemma). *Suppose a partially ordered set P has the property that every chain in P has an upper bound in P. Then the set P contains at least one maximal element.*

    Thus, by above lemma, it is clear that set $\mathscr{Y}$ will have a **maximal element**. $\qquad\square$

1.5   Part 5

Continuing from where I left off in the last part.
I have to prove that every maximal element in $\mathscr{Y}$ is a prime ideal.

Proof. Since we have proven in the last part that $\mathscr{Y}$ has atleast one maximal element, let the **maximal element** of $\mathscr{Y}$ be P.

Claim 1.5.1. *Let $a, b \in R$ such that $a, b \notin P$, this implies that $ab \notin P$*

Proof. Since $a \notin P$, the ideal generated by P and a i.e. (P, a) must be strictly greater than P i.e. $P \subset (P, a)$, but P is maximal in the poset $\mathscr{Y}$, so (P, a) cannot be in the set $\mathscr{Y}$.
Now by definition of the set $\mathscr{Y}$ we can have a positive integer m such that $x^m \in (P, a)$, also $x^n \in (P, b)$ for some positive integer n, so it can easily be seen that $x^{m+n} \in (P, ab)$ (here x is not a nilpotent element), which is an ideal generated by P and ab.
Thus, $(P, ab) \notin S$ and so $P \subset (P, ab)$ or (P, ab) is strictly greater than P, which implies that $ab \notin P$ which proves my claim. $\qquad\square$

By above claim we can see that P is a prime ideal. $\qquad\square$

1.6   Part 6

I have to finally prove the following final claim:

Claim 1.6.1. *All elements of set S which is the intersection of all the prime ideals of the ring R are* ***nilpotent*** *elements.*

Proof. Now, we will put everything what we have proved together, Since the set P which is the maximal element of $\mathscr{Y}$ is a prime ideal and $x \notin P$ where x is not a nilpotent element, we can conclude that $x \notin \bigcap P$, the intersection of all prime ideals of R which is set S.
Thus, finally only elements which will remain in S will be the **nilpotent** elements. $\qquad\square$

II Problem 2 Solution

We are given a commutative ring R, one ideal I of the ring R, a set $\mathscr{Y}$ of ideals of R such that $\mathscr{Y} = \{U \mid U \text{ is an ideal of } R \text{ and } I \subseteq U\}$, a set $\mathscr{Y}'$ be a set of all ideals of R/I.

Claim 2.0.1. *There exists a bijection $f : \mathscr{Y} \rightleftarrows \mathscr{Y}'$.*

Proof. Firstly, we are given a subring R/I of the ring R such that elements of this subring are of the form $x + I \mid x \in R$.
Consider a function f which takes each and every element of ideal $U \in \mathscr{Y}$, adds an element of ideal I to it i.e. converts each element to a set of elements $U' = \{a + I \mid a \in U\}$, i.e. $f(U) = U'$.
I am going to prove the claim via 3 lemmas.

Lemma 2.1. *Set $U' = \{a + I \mid a \in U\}$, where $U \in \mathscr{Y}$ is an **ideal** of the subring R/I.*

Proof. Looking at both properties of ideals:
1. If $a + I \in U', b + I \in U' \Rightarrow a + b + I \in U'$:
    Consider $a, b \in U, U \in \mathscr{Y}$, since U is an ideal $a + b \in U$, thus $a + I, b + I \in U' = f(U) \Rightarrow a + b + I \in U' = f(U)$, where $a + b + I = a + I + b + I$.
2. If $a + I \in U', x + I \in R/I \Rightarrow ax + I \in U'$:
    Consider $a \in U, U \in \mathscr{Y}$ and $x \in R$, since U is an ideal $ax \in U$, thus $a + I \in U' = f(U) \Rightarrow ax + I \in U' = f(U)$, where $ax + I = (a + I) * (x + I), x + I \in R/I$.
Thus, the set U' satisfies both properties for being an ideal of R/I. □

By above lemma, all the images of U under the function f are ideals in ring R/I.

Lemma 2.2. *The function $f : \mathscr{Y} \to \mathscr{Y}'$ is **one-one**, i.e. there is an **injection** from set $\mathscr{Y}$ to $\mathscr{Y}'$.*

Proof. Let us consider 2 different ideals $U, V \in \mathscr{Y}$ such that $U \neq V$, which means that there is some element $a \in U$ and $a \notin V$.
Assume that $f(U) = f(V) = U'$, thus $a + I \in U'$ but $a \notin V$ which means $\exists b \in V$ such that $a \neq b, b + I = a + I \Rightarrow a - b \in I$, but $I \subseteq V \Rightarrow a - b \in V$, since $b \in V \Rightarrow a \in V$ which is a **contradiction** to our assumption.
Thus, we cannot assume $U \neq V, f(U) = f(V)$ and the result which holds is $U \neq V \Rightarrow f(U) \neq f(V)$. □

The above lemma proves that function f is **injective**, the last lemma which remains is:

Lemma 2.3. *The function $f : \mathcal{Y} \rightarrowtail \mathcal{Y}'$ is **onto**, i.e. there is a **surjection** from set $\mathcal{Y}$ to $\mathcal{Y}'$.*

Proof. Since we have already proven that the function f is injective by **Lemma 2.2**, we can have a **partial** function $f^{-1} = g$, if we show g is complete, we will have a pre-image for every element in $\mathcal{Y}'$ and thus the function will be surjective.

Proving $g(U') = U \supseteq I$:

Consider $a, b \in U$ such that $a + I, b + I \in U'$ and $a + I = b + I$, thus $a - b \in I$, also we know that U' is an ideal, thus $a - b + I \in U'$ then $a - b \in U$.

Now when we fix one of a or b and vary the other, by above arguments we can see that whenever $a - b \in I \Rightarrow a - b \in U$ which means $I \subseteq U$.

Proving g **is complete**:

Consider 2 elements $a + I, b + I \in U'$, since we know U' is an ideal of ring R/I, $a + b + I \in U'$, now we define $f^{-1}(U') = g(U') = \{a \mid a + I \in U', a \in R\}$.

Since U' is an ideal of ring R/I, $a + I \in U', a \in R$ and $g(U') \subseteq R$, since $a + I, b + I, a + b + I \in U' \Rightarrow a, b, a + b \in U$.

Consider $a + I \in U'$ and $x + I \in R/I, x \in R$, then $(a + I) * (x + I) = ax + I \in U' \Rightarrow ax \in U$, so by these arguments the function g is complete.

$\square$

By the results of above three lemmas, it is clear that the function we defined is **injective** as well as **surjective** which proves that it is **bijective**. $\square$

III Problem 3 Solution

3.1 Part 1

We are given R which is a **Noetherian** ring.

Claim 3.1.1. *Every non-unit element of ring R is contained in a maximal ideal.*

Proof. Consider an ideal (a), since we know that element a is not a unit, this ideal will not contain 1 as element i.e. it does not form the whole ring.
Now we have to check whether if we can make a bigger ideal I_2 which contains the whole (a) or not such that, that ideal is not the complete ring.
If we cannot do it, we are done as (a) is the required maximal ideal, if we can make it bigger then we will get some ideal I_2 such that I_2 does not form the complete ring but contains all elements of the ideal (a).
We will keep doing this until we get a maximal ideal:

$$(a) \subset I_2 \subset I_3 \subset I_4 \subset \ldots$$

Let $(a) = I_1$ and suppose the above sequence is infinite, we define $I = \bigcap_{i \geq 1} I_i$. Set I is also an ideal of R as if $a, b \in I$ then $a, b \in I_j$ for some j, then $a + b \in I_j \subseteq I$ and if $a \in I$ then $a \in I_j$, then $ab \in I_j \subseteq I, b \in R$.
Since R is **Noetherian**, I is finitely generated. Let it's generators be $a_1, a_2, \ldots, a_k$, then $\exists j$ such that $a_1, a_2, \ldots, a_k \in I_j$, then $I = (a_1) + (a_2) + \cdots + (a_k) \subseteq I_j$. Hence $I = I_j$, a **contradiction**.
Thus, the sequence above is finite and thus $\exists I_j$ which is a maximal ideal and contains element a. □

3.2 Part 2

Proof. **Firstly,**
We consider that $x \in S$, where S is the intersection of all maximal ideals of ring R, now assume $1 - x$ is not a unit in the ring R, thus by proof of **3.1 Part 1**, $1 - x$ is contained in a maximal ideal m of R. But we know that $x \in S \subseteq m$, we have $1 - x \in m \Rightarrow 1 \in m$ which is **false**.
Thus, our assumption is wrong and $1 - x$ will be a unit.
Conversely, it is **false**, I am going to give a counter example to prove this
Consider the ring of integers $\mathbb{Z}$, I first make the following claim.

Claim 3.2.1. *Ring of integers $\mathbb{Z}$ is **Noetherian**.*

Proof. We first see that $\mathbb{Z}$ is **Principal ideal domain** as all the ideals in the ring $\mathbb{Z}$ are principal ideals. We can show ring $\mathbb{Z}$ to be **PID** by using **Euclid's GCD Algorithm**, consider $a, b \in I$, where I is an ideal, thus using $gcd(a, b) = as + bt \in I$, we will keep doing this to get a simplest number which will produce all the elements of the ideal.
By this we can see that each and every ideal is principal ideal and it is finitely generated, 2 elements with $gcd(a, b) = 1$ will generate the entire ring. □

We can say that (3) is a maximal ideal of the ring $\mathbb{Z}$ as any other number which is not in this ideal is of the form $3n + 1, 3n + 2$ and taking any 1 of them we get $3n + 1 - 3n = 1, 3n + 3 - 3n - 2 = 1$ which gives (1) in the ideal which will form the whole ring.
Now consider $x = 2$ which gives $1 - 2 = -1$ and -1 is a unit in the ring $\mathbb{Z}$ but consider maximal ideal (3) of the ring $\mathbb{Z}$, x does not lie in this ideal and thus $x \notin S$ which proves that statement is **false**.
Thus, the above statement should be - **"Prove that $x \in S$ if $1 - x$ is a unit in R".** □