Math 395

Homework 4

Due: 2/27/2024

Name: Avinash Iyer

Collaborators: Ling Chen, Timothy Rainone

Problem 1

Let F be a field, with $F[x]$ denoting the ring of polynomials with coefficients in F. Let $f(x) \in F[x]$ be a monic polynomial. Let $g(x) \in F[x]$ be a nonzero polynomial. We will show that there exist unique $q(x)$ and $r(x)$ in $F[x]$ such that $f(x) = g(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg g(x)$.

For existence, we examine the set $\{f(x) - g(x)q(x) \mid q(x) \in F[x]\}$, and take the element of the set with smallest degree to be $r(x)$. Such an $r(x)$ must exist by the well-ordering principle, since the given set is non-empty and the degrees of elements of such sets are natural numbers.

If $\deg g > \deg f$, then it must be the case that $r(x) = f(x)$. If there exists $q(x)$ such that $g(x)q(x) = f(x)$, then $r(x) = 0$. Additionally, if $f(x) = 0$, then both $q(x)$ and $r(x)$ are equal to 0.

We claim that $r(x)$ must have degree less than $g(x)$ if $r(x)$ is nonzero. If it were the case that $r(x)$ had degree greater than $g(x)$, then we can extract $r^*(x)$ by the same process from $\{r(x) - g(x)q^*(x) \mid q^*(x) \in F[x]\}$, finding a polynomial with necessarily smaller degree. Then, $g(x)q(x) + r(x) = g(x)(q(x) + q^*(x)) + r^*(x)$ with $r^*(x)$ of degree smaller than $g(x)$.

To show uniqueness, suppose there exist $q_1(x) \neq q_2(x)$ and $r_1(x) \neq r_2(x)$ such that $f(x) = g(x)q_1(x) + r_1(x)$ and $f(x) = g(x)q_2(x) + r_2(x)$. Then,

$$r_1(x) - r_2(x) = g(x)\left(q_1(x) - q_2(x)\right).$$

Since $r_1(x) - r_2(x)$ has degree at most $\deg g(x) - 1$, while $g(x)\left(q_1(x) - q_2(x)\right)$ has degree at least $\deg g(x)$, this cannot hold. Thus, $r_1(x)$ must be equal to $r_2(x)$ and $q_1(x)$ must be equal to $q_2(x)$.

Problem 4

Let $p \in \mathbb{Z}$ be a prime. Let $\mathfrak{m} = \{(pa, b) \mid a, b \in \mathbb{Z}\}$. We will prove that $\mathfrak{m}$ is a maximal ideal in $\mathbb{Z} \times \mathbb{Z}$.

We will do so by showing that $(\mathbb{Z} \times \mathbb{Z})/\mathfrak{m}$ is isomorphic to the field $\mathbb{Z}/p\mathbb{Z}$. Let $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be defined by $\varphi((i,j)) = [i]_p$. We will show that φ is a surjective homomorphism with kernel $\mathfrak{m}$.
Let $(i,j),(k,\ell) \in \mathbb{Z} \times \mathbb{Z}$. Then,

$$\begin{aligned}\varphi((i,j) + (k,\ell)) &= \varphi((i+k, j+\ell)) \\ &= [i+k]_p \\ &= [i]_p + [k]_p \\ &= \varphi((i,j)) + \varphi((k,\ell)),\end{aligned}$$

and

$$\begin{aligned}\varphi((i,j)(k,\ell)) &= \varphi((ik, j\ell)) \\ &= [ik]_p \\ &= [i]_p[k]_p \\ &= \varphi((i,j))\varphi((k,\ell)).\end{aligned}$$

Finally, for any $[a]_p \in \mathbb{Z}/p\mathbb{Z}$, we set $(a,1) \in \mathbb{Z} \times \mathbb{Z}$ such that $\varphi((a,1)) = [a]_p$, meaning φ is surjective.

For $\varphi((x,y)) = [0]_p$, it must be the case that $[x]_p = [0]_p$, meaning $x = pa$ for some $a \in \mathbb{Z}$. Thus, $\ker \varphi = \{(pa, b) \mid a, b \in \mathbb{Z}\} = \mathfrak{m}$. By the first isomorphism theorem, it is the case that $(\mathbb{Z} \times \mathbb{Z})/\mathfrak{m} = \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, $\mathfrak{m}$ must be maximal.

Problem 5

Let p be a prime, and let J be the collection of polynomials in $\mathbb{Z}[x]$ whose constant term is divisible by p. We will show that J is a maximal ideal in $\mathbb{Z}[x]$.

Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ be defined by

$$a_0 + a_1x + \cdots + a_nx^n \mapsto [a_0]_p.$$

For any $[a]_p \in \mathbb{Z}/p\mathbb{Z}$, we select an element of $\mathbb{Z}[x]$ with constant term equal to a, meaning that φ is a surjective map. We will show that φ is a homomorphism. Let $a = a_0 + a_1x + \cdots + a_nx^n$ and $b = b_0 + b_1x + \cdots + b_mx^m$ be elements of $\mathbb{Z}[x]$. Without loss of generality, $n \geq m$. Then,

$$\begin{aligned}
\varphi(a+b) &= \varphi\left((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_m + b_m)x^m + \cdots + a_nx^n\right) \\
&= [a_0 + b_0]_p \\
&= [a_0]_p + [b_0]_p \\
&= \varphi(a_0 + a_1x + \cdots + a_nx^n) + \varphi(b_0 + b_1x + \cdots + b_mx^m),
\end{aligned}$$

and

$$\begin{aligned}
\varphi(ab) &= \varphi\left((a_0 + a_1x + \cdots + a_nx^n)(b_0 + b_1x + \cdots + b_mx^m)\right) \\
&= \varphi\left((a_0b_0) + \cdots + (a_nb_m)x^{n+m}\right) \\
&= [a_0b_0]_p \\
&= [a_0]_p[b_0]_p \\
&= \varphi(a_0 + a_1x + \cdots + a_nx^n)\varphi(b_0 + b_1x + \cdots + b_mx^m) \\
&= \varphi(a)\varphi(b).
\end{aligned}$$

Therefore, φ is a homomorphism with

$$\ker\varphi = \left\{a_0 + a_1x + \cdots + a_nx^n \mid a_i \in \mathbb{Z}, [a_0]_p = [0]_p\right\},$$

which is precisely the set of all polynomials in $\mathbb{Z}[x]$ with with $a_0|p$, or J. By the first isomorphism theorem, it is thus the case that $\mathbb{Z}[x]/J \cong \mathbb{Z}/p\mathbb{Z}$. Since $\mathbb{Z}/p\mathbb{Z}$ is a field, it must be the case that J is a maximal ideal.

Problem 7

Let R be a commutative ring with identity. Let $I \subset R$ be an ideal. The radical of I is defined as

$$\text{rad } I = \{r \in R \mid r^n \in I \text{ for some } n \in \mathbb{Z}_{>0}\}$$

We say I is a radical ideal if rad $I = I$. We will show that every prime ideal of R is a radical ideal.

Let I be a prime ideal. Let $r \in \text{rad } I$. Then, $\exists n \in \mathbb{Z}_{>0}$ such that $r^n \in I$. We will show that $r \in I$ by induction.

In the base case, we let $n = 1$. Then, since $r^1 = (1)(r) \in I$. Since I is prime, it must be the case that either 1 or r is an element of I; however, since $I \neq R$, it must be the case that $1 \notin I$ (as 1 is a unit in R), so $r \in I$.

Suppose that for $2, \ldots, n-1$, it is the case that if $r^{n-1} \in I$, then $r \in I$. Then, if $r^n \in I$, we have $r^n = (r^{n-1})(r) \in I$. Since I is prime, either $r \in I$ or $r^{n-1} \in I$. If the first is the case, then we are done; otherwise, if $r^{n-1} \in I$, the inductive hypothesis holds that $r \in I$. Thus, rad $I \subseteq I$.

Let $a \in I$. Then, since $a \in R$, we have that $a^1 \in I$, meaning $n = 1$, so $a \in \text{rad } I$. Thus, $I \subseteq \text{rad } I$. Therefore, for I a prime ideal, rad $I = I$.