Math 100B: Homework 4

Merrick Qiu

Problem 1

We can reproduce Euclids proof that $\mathbb{Z}$ has infinitely many primes to show that $F[x]$ has infinitely many monic irreducible polynomials. Suppose that there were only a finite number of monic irreducible polynomials in $F[x]$, say $p_1, p_2, \ldots, p_n$. Then consider the polynomial $p_{n+1} = p_1 p_2 \cdots p_n + 1$ which is also a monic polynomial. Since p_{n+1} is not divisible by any of the p_i, it must be irreducible.

Therefore the monic irreducible polynomials are not given by $p_1, p_2, \ldots, p_n$ which is a contradiction. Therefore there must be a infinite number of monic irreducible polynomials. Since the maximal ideals of $F[x]$ are the principal ideals generated by the monic irreducible polynomials, there are also an infinite number of maximal ideals.

Problem 2

(a) This is simply proving Fermats Little theorem, which we can do by looking at the multiplicative group $\mathbb{F}_p^\times$. For any element $a \in \mathbb{F}_p^\times$, the order give by k must divide $p-1$ by Lagrange's theorem. If $p-1 = kn$ for some n then $a^{p-1} - 1 = a^{kn} - 1 = (a^k)^n - 1 = 1 - 1 = 0$. Therefore all elements in $\mathbb{F}_p^\times$ are roots of $f(x)$.

(b) Since every nonzero element of $\mathbb{F}_p$ is a root of $f(x)$, we can write $f(x) = (x-1)(x-2)\ldots(x-(p-1))g(x)$ for some polynomial $g(x)$. However in order for the leading coefficients and degrees of the left and right hand side to match, $g(x) = 1$ so we can simply write $f(x) = (x-1)(x-2)\ldots(x-(p-1))$.

(c) The constant term of $f(x)$ is -1 and the constant term of the right hand side is the product $(p-1)!$ modulo p so it must be that $(p-1)! \equiv -1 \mod p$.

Problem 3

1. Let $f(x) \in R$ with leading coefficient a and $g(x)$ has leading coefficient b. If we set $f(x) - \frac{a}{b}g(x) = r(x)$ then $\deg r < \deg g$ and $f(x) = r(x) + \frac{a}{b}g(x)$. This representation is unique since if $f(x) = r(x) + \frac{a}{b}g(x) = s(x) + cg(x)$ with $\deg s < \deg g$ and $c \neq \frac{a}{b}$, then that would imply that $r(x) - s(x) = (c - \frac{a}{b})g(x)$, but this is a contradiction since the degrees of the left and right hand side do not match.

2. Each element of R corresponds to a coset $r(x) + (g(x))$ where $r(x)$ has degree $n-1$. Since $r(x)$ has n different coefficients and each of these coefficients can take on p different values, there are in total p^n different cosets in $\mathbb{F}_p[x]/(g(x))$.

Problem 4

1. By the previous problem we have that E has a total of $3^2 = 9$ elements. It is a field because it is the quotient of a polynomial ring by an irreducible polynomial.
2. $E^\times$ is cyclic since $x+1$ generates it.$(x+1)^2 = 2x$, $(x+1)^4 = 2$, and $(x+1)^8 = 1$.
3. $\mathbb{F}_3[x]/(x^3+1)$ is a field with 27 elements.

Problem 5

1. The units of R are the constants $a_0 \in F$ with degree 0. If x^2 are reducible then it can be written as the product of two degree 1 polynomials, but since R contains no degree 1 polynomials x^2 must be irreducible. Likewise x^3 must be written as the product of a degree 1 polynomial and a degree 2 polynomial, but R contains no degree 1 polynomials.

2. We can factor $x^6 = x^2 \cdot x^2 \cdot x^2 = x^3 \cdot x^3$ in two ways into irreducible elements, so R is not a unique factorization domain.

Problem 6

1. RS^{-1} is closed under subtraction since for $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in RS^{-1}$
$$\frac{r_1}{s_1} - \frac{r_2}{s_2} = \frac{r_1 s_2 - r_2 s_1}{s_1 s_2} \in RS^{-1}$$
since $r_1 s_2 - r_2 s_1 \in R$ and $s_1 s_2 = S^{-1}$.
RS^{-1} is closed under subtraction since for $\frac{r_1}{s_1}, \frac{r_2}{s_2} \in RS^{-1}$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2} \in RS^{-1}$$
since $r_1 r_2 \in R$ and $s_1 s_2 = S^{-1}$. Since $\frac{1}{1} \in RS^{-1}$ as well, RS^{-1} is a subring of F.

2. Define $\hat{\phi}\left(\frac{r}{s}\right) = \phi(r)\phi(s)^{-1}$. This is well defined since $\phi(s)$ is a unit and it sends two equivalent fractions to the same element. If $\frac{r}{s} = \frac{a}{b}$ then $rb = as$ which can be written as $rs^{-1} = ab^{-1}$ and
$$\hat{\phi}\left(\frac{r}{s}\right) = \phi(r)\phi(s)^{-1} = \phi(rs^{-1}) = \phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \hat{\phi}\left(\frac{a}{b}\right).$$
It is a homomorphism since
$$\hat{\phi}\left(\frac{1}{1}\right) = 1$$
$$\begin{aligned}\hat{\phi}\left(\frac{r}{s} + \frac{a}{b}\right) &= \hat{\phi}\left(\frac{rb + as}{sb}\right)\\ &= \phi(rb + as)\phi(sb)^{-1}\\ &= \phi((rb + as)(sb)^{-1})\\ &= \phi(rs^{-1} + ab^{-1})\\ &= \phi(r)\phi(s)^{-1} + \phi(a)\phi(b)^{-1}\\ &= \hat{\phi}\left(\frac{r}{s}\right) + \hat{\phi}\left(\frac{a}{b}\right)\end{aligned}$$
$$\begin{aligned}\hat{\phi}\left(\frac{r}{s} \cdot \frac{a}{b}\right) &= \hat{\phi}\left(\frac{ra}{sb}\right)\\ &= \phi(ra)\phi(sb)^{-1}\\ &= \phi(r)\phi(s)^{-1}\phi(a)\phi(b)^{-1}\\ &= \hat{\phi}\left(\frac{r}{s}\right)\hat{\phi}\left(\frac{a}{b}\right)\end{aligned}$$
It is unique since another homomorphism with these properties φ would have
$$\begin{aligned}\varphi(\frac{r}{s})\varphi(s) &= \varphi(\frac{r}{s}\frac{s}{1})\\ &= \varphi(\frac{r}{1})\\ &= \phi(r)\end{aligned}$$
Also $\varphi(s) = \phi(s)$ so
$$\varphi(\frac{r}{s}) = \phi(r)\phi(s)^{-1} = \hat{\phi}(\frac{r}{s})$$

Problem 7

Since $\phi(\frac{a}{p^k}) = \phi(a)\phi(p)^{-k}$ for $\frac{a}{p^k} \in RS^{-1}$, each homomorphism is uniquely determined by where it sends a and p. Since a is an integer and $\phi(1) = 1$, $\phi(a) = \phi(1 + \ldots + 1) = \phi(1) + \ldots + \phi(1) = a$. Since p must be sent to a unit of $\mathbb{Z}/n\mathbb{Z}$, and there are $\varphi(n)$ units in $\mathbb{Z}/n\mathbb{Z}$, there are $\varphi(n)$ different homomorphisms, where $\varphi(n)$ is eulers totient function.