Math 541
Problem Set 11

9.2.2. It suffices to show that there are q^n polynomials of degree at most $n-1$, since by exercise 9.2.1, the elements of $F[x]/(f)$ are in bijection with such polynomials. A polynomial of degree at most $n-1$ is of the form

$$a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$$

with $a_0, a_1, \ldots, a_{n-1} \in F$. There are $|F| = q$ possibilities for a_0, q possibilities for a_1, and so on, so there are q^n possibilities.

9.2.3. $F[x]/(f)$ is a field if and only if (f) is maximal. If (f) is maximal then it is prime; conversely, if (f) is prime then it is maximal since $F[x]$ is a P.I.D. Now (f) is prime if and only if f is prime, but since $F[x]$ is a U.F.D., primes and irreducibles are the same.

9.3.1. We prove the contrapositive. Suppose that R is a U.F.D. By Gauss' Lemma, there are $r, s \in F$ such that $ra(x), sb(x) \in R[x]$ and $ra(x) \cdot sb(x) = p(x)$. Since $a(x)$ and $b(x)$ are monic, the leading coefficients of $ra(x)$ and $sb(x)$ are r and s, so $r, s \in R$. Comparing the leading coefficients of $p(x)$ and $ra(x) \cdot sb(x)$, we find that $rs = 1$, so $a(x) = s \cdot ra(x)$, so $a(x) \in R[x]$.

Observe that the field of fractions of $\mathbb{Z}[2\sqrt{2}]$ is $\mathbb{Q}[\sqrt{2}]$. Now $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$; everything in sight is monic, but the left-hand side is monic and lies in $\mathbb{Z}[2\sqrt{2}][x]$, while the factors of the left-hand side do not.

9.4.2. We use Eisenstein's Criterion.

(a) The coefficients -4 and 6 are both divisible by 2, but 6 is not divisible by 2^2.

(b) The coefficients 30, -15, 6, and -120 are all divisible by 3, but -120 is not divisible by 3^2.

(c) We take the hint: $(x-1)^4 + 4(x-1)^3 + 6(x-1)^2 + 2(x-1) + 1 = x^4 - 2x + 2$. The coefficients -2 and 2 are divisible by 2, but 2 is not divisible by 2^2.

(d) By the binomial theorem,

$$(x+2)^p = x^p + p \cdot 2x^{p-1} + \binom{p}{2}2^2x^{p-2} + \binom{p}{3}2^3x^{p-3} + \cdots + \binom{p}{p-2}2^{p-2}x^2 + p \cdot 2^{p-1}x + 2^p.$$

Observe that $\binom{p}{n}$ is divisible by p if $1 \leq n \leq p-1$, since

$$\binom{p}{n} = \frac{p(p-1)\cdots(p-n+1)}{n!}$$

and if $n < p$ then p does not divide $n!$, so the p in the numerator cannot be canceled. Thus in

$$\frac{(x+2)^p - 2^p}{x} = x^{p-1} + p \cdot 2x^{p-2} + \binom{p}{2}2^2x^{p-2} + \binom{p}{3}2^3x^{p-3} + \cdots + \binom{p}{p-2}2^{p-2}x + p \cdot 2^{p-1}$$

all the coefficients are divisible by p, but the constant term $p \cdot 2^{p-1}$ is not divisible by p^2.

9.4.3. Let $f(x) = (x-1)(x-2)\cdots(x-n) - 1$, and suppose that $f(x) = a(x)b(x)$, where $\deg a, \deg b < n$. Then $a(1)b(1) = -1$, so $a(1) = \pm 1$ and $b(1) = \mp 1$, so $a(1) + b(1) = 0$. Similarly, $a(2) + b(2) = a(3) + b(3) = \cdots = a(n) + b(n) = 0$. Thus $a(x) + b(x)$ is has degree less than n but has n distinct roots, so $a(x) + b(x) = 0$, so $f(x) = -a(x)^2$. But $f(n+2) > 0$, whereas $-a(n+2)^2 \leq 0$, which is a contradiction.