HOMEWORK 7

JASON MEDCOFF

93. We can use the isomorphism theorem by showing that there is a homomorphism $f : R[x]/ \to R$, demonstrating the kernel of f to be (x), and showing that the image of f is R itself. So first, choose f such that $r(x) = r_0 + \ldots + r_n x^n \mapsto r_0$; in other words, f is the evaluation function that sends polynomials $r(x)$ to $r(0)$.

This map is well defined since equality of polynomials is defined by equality of coefficients. The map is a homomorphism since

$$f(r(x) + s(x)) = r_0 + s_0 = f(r(x)) + f(s(x))$$

and

$$f(r(x)s(x)) = r_0 s_0 = f(r_0)f(s_0),$$

and furthermore, the zero polynomial obviously maps to zero in R. Thus f is a homomorphism.

The kernel of f is given by

$$\begin{aligned}\ker f &= \{r(x) \in R[x] : f(r(x)) = 0\}\\ &= \{r_1 x + \ldots + r_n x^n\}\\ &= (x)\end{aligned}$$

since polynomials without constant terms are divisible by x without remainder. Finally, the image of f is clearly the entirety of R since one can choose any constant polynomial $r(x) = r_0$ with $r_0 \in R$. Thus by the first isomorphism theorem, there exists an isomorphism between $R[x]/(x)$ and R.

97.

Lemma. In a finite field of prime order n, $(a + b)^n = a^n + b^n$. By binomial coefficients,

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

but for $n > k$, n divides $n!$ but not $k!$. Then the coefficients of all terms but the first and the last are divisible by the characteristic. All that is left is $a^n + b^n$.

i) F obeys the additive homomorphism rule since

$$F(a + b) = a^p + b^p = (a + b)^p = F(a) + F(b)$$

since by binomial coefficients,

$$(a + b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$$

where

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

but since

100. i) By the lemma in 97, we can write $x^4 + 1 = x^4 + 1^4 = (x+1)^4$.
ii) We can write

$$\begin{aligned}(x^2+ax+b)(x^2+cx+d) &= x^4+cx^3+dx^2+ax^3+acx^2+adx+bx^2+bcx+bd \\ &= x^4+(c+a)x^3+(d+ac+b)x^2+(ad+bc)x+(bd) \\ &= x^4+1\end{aligned}$$

and by equating coefficients, clearly $bd = 1$, $c + a = 0$ or $c = -a$, $d + ac + b = 0$, and $ad + bc = 0$. The latter two can be written as $d + b - a^2 = 0$ and $ad - ab = 0$ or $a(d - b) = 0$.