Notes

November 3, 2014

Section 4.1: 3, 5(d), 6, 19.

3

$f(x) = x^3 + x^2 - 2x + 1 \to f(x) = q(x)(x-1) + f(1)$

5d

$x^3 + 2x + 3; c = 2; F = \mathbb{Z}_5$

$$\begin{aligned} x^3 + 2x + 3 &= q(x)(x-c) + f(c) \\ &= q(x)(x-2) + f(2) \\ &= q(x)(x-2) + 8 + 4 + 3 \\ &= q(x)(x-2) \end{aligned}$$

$$\begin{array}{c|cccc} 2 & 1 & 0 & 2 & 3 \\ & \vdots & 2 & 4 & 2 \\ \hline & 1 & 2 & 1 & 0 \end{array}$$

6

everything but zero is a root from 1.4.11

$$a^{\varphi(n)} \equiv 1 \mod n$$

for $(a, n) = 1$ if n is print and $(a, p) = 1$ then $a^{p-1} \equiv 1 \mod p$ that is $a^{p-1} = 1$ in $\mathbb{Z}_p$. and $x(x^{p-1} - 1) = x^p - x$ has a zero for all elements in $\mathbb{Z}_p$

corollary p is prime means that $a^p \equiv a \mod p$ (1.4.12)

4.2

theorem 4.2.1 $f(x) = q(x)g(x) + r(x)$ where $\deg r < \deg g$ or $\deg r = 0$ proof, if $\deg f < \deg g$ then $q = 0, r = f$

now assume $\deg f \geq \deg g$. easily see that if $\deg f = 0$ is true

now assume that $\deg f = m$ and $\deg g =$.

4.2.2

I is an **ideal** of $F[x]$ notation $I = d(x)K[x] = (d(x))$ where the last one is ideal notation