Assignment #6 Due 3-8-05

P149 9.5, 9.7 (32 only, multiplication only)

9.5 Show all polynomials of degree 1 are irreducible

Pf If $\deg f = 1$ then $f \neq 0$ and if $f = gh$ then $1 = \deg f = \deg g + \deg h \Rightarrow (\deg g = 0, g \neq 0)$ or $(\deg h = 0, h \neq 0)$. If $\deg g = 0, g \neq 0$ then $g = 1$ and $f = h$. Otherwise $\deg h = 0$, $h \neq 0$ so $h = 1$ and $g = f$. In either case the only factors of f are 1 and f.

Thus $\underline{I(1) = 2}$ since X, $X+1$ are irreducible.

<u>Degree</u> 2: $X^2 = X \cdot X$, $X^2 + 1 = (X+1)\cdot(X+1)$, $X^2 + X = X \cdot (X+1)$ are reducible. If $X^2 + X + 1$ ~~were~~ were reducible, it would have a factor of degree 1, either X or $X+1$. But

$$X^2 + X + 1 = (X+1)X + 1 \text{ and}$$
$$X^2 + X + 1 = X(X+1) + 1$$

so neither X nor $X+1$ is a factor and $X^2 + X + 1$ is irreducible.

Thus $\underline{I(2) = 1}$

<u>Degree 3</u> $X^3 = X \cdot X^2$, $X^3 + 1 = (X+1)(X^2 + X + 1)$

$X^3 + X = X(X^2+1)$, $X^3 + X^2 = X(X^2+X)$,

$X^3 + X^2 + X + 1 = (X+1)(X^2+1)$. If $X^3 + X^2 + 1$ or $X^3 + X + 1$ were reducible, they would have a factor of degree 1. Neither has X as a factor, and

$$X^3 + X^2 + 1 = X^2(X+1) + 1$$
$$X^3 + X + 1 = (X^2 + X)(X + 1) + 1$$

So both are irreducible and

$\underline{I(3) = 2}$

<u>Degree 4</u>

$x^4 = x\cdot x^3$, $x^4+1 = (x^2+1)(x^2+1)$, $x^4+x = x(x^3+1)$,
$x^4+x^2 = x(x^3+x)$, $x^4+x^2+1 = (x^2+x+1)(x^2+x+1)$
$x^4+x^2+x+1 = (x+1)(x^3+x^2+1)$, $x^4+x^3 = x(x^3+x^2)$
$x^4+x^3+x = x(x^3+x^2+1)$
$x^4+x^3+x+1 = (x^3+1)(x+1)$,
$x^4+x^3+x^2 = x(x^3+x^2+x)$, $x^4+x^3+x^2+1 = (x+1)(x^3+x+1)$
$x^4+x^3+x^2+x = x(x^3+x^2+x+1)$. This leaves
x^4+x+1, x^4+x^3+1, and $x^4+x^3+x^2+x+1$.

$$x^4+x+1 = (x+1)(x^3+x^2+x)+1$$
$$x^4+x^3+1 = x^3(x+1)+1$$
$$x^4+x^3+x^2+x+1 = (x^3+x)(x+1)+1$$

So none have $(x+1)$ as a factor, and x is not a factor. If they are reducible, they have an irreducible factor of degree 2, namely x^2+x+1.

$$x^4+x+1 = (x^2+x)(x^2+x+1)+1$$
$$x^4+x^3+1 = (x^2+1)(x^2+x+1)+x$$
$$x^4+x^3+x^2+x+1 = x^2(x^2+x+1)+(x+1).$$

So x^2+x+1 not a factor of any, all irreducible

Thus $\underline{I(4)=3}$

$$\sum_{d|2} d\cdot I(d) = 1\,I(1)+2\,I(2) = 2+2 = 4 = 2^2$$

$$\sum_{d|3} d\cdot I(d) = 1\,I(1)+3\,I(3) = 2+3\cdot 2 = 8 = 2^3$$

$$\sum_{d|4} d\,I(d) = 1\,I(1)+2\,I(2)+4\,I(4)$$
$$= 2+2+4\cdot 3 = 16 = 2^4$$

9.7 Answer depends on choice of f used to make $\mathbb{Z}_2(x)/f$

Choose $f = x^5 + x^2 + 1$

To check f irreducible: if not, f has factor of degree 1 or 2 which is irreducible, but

$$x^5+x^2+1 = (x^4+x)x+1$$
$$x^5+x^2+1 = (x^4+x^3+x^2)(x+1)+1$$
$$x^5+x^2+1 = (x^3+x^2)(x^2+x+1)+1$$

so neither x, nor $x+1$, nor x^2+x+1 is a factor of f.

Let $a_4 a_3 a_2 a_1 a_0 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, so the elements of $\mathbb{Z}_2(x)/(x^5+x^2+1)$ are binary 5 tuples.

In $\mathbb{Z}_2(x)/(x^5+x^2+1)$ we have the following: let $\alpha = x$. Then

00001	$= \alpha^0 = \alpha^{31}$	01110	$= \alpha^{12}$	11011	$= \alpha^{16}$
00010	$= \alpha$	01111	$= \alpha^{23}$	11100	$= \alpha^{13}$
00011	$= \alpha^{18}$	10000	$= \alpha^{4}$	11101	$= \alpha^{14}$
00100	$= \alpha^{2}$	10001	$= \alpha^{10}$	11110	$= \alpha^{24}$
00101	$= \alpha^{5}$	10010	$= \alpha^{30}$	11111	$= \alpha^{15}$
00110	$= \alpha^{19}$	10011	$= \alpha^{17}$		
00111	$= \alpha^{11}$	10100	$= \alpha^{7}$		
01000	$= \alpha^{3}$	10101	$= \alpha^{22}$		
01001	$= \alpha^{29}$	10110	$= \alpha^{28}$		
01010	$= \alpha^{6}$	10111	$= \alpha^{26}$		
01011	$= \alpha^{27}$	11000	$= \alpha^{21}$		
01100	$= \alpha^{20}$	11001	$= \alpha^{25}$		
01101	$= \alpha^{8}$	11010	$= \alpha^{9}$		

To construct the multiplication table, use

$$\alpha^i \alpha^j = \alpha^{i+j} \quad \text{and} \quad \alpha^{31} = 1$$

For example, $(0\,0\,1\,1\,0) \otimes (1\,0\,0\,1\,1) = \alpha^{19}\alpha^{17} = \alpha^{36} = \alpha^{31+5}$
$= \alpha^5$
$= (0\,0\,1\,0\,1)$