HW # 12 Solutions

#1 a) Since $\overset{f(x)}{x^3+2x+1}$ is a cubic, showing it has no zeros is sufficient to see it is irred.

$f(0) = 1 \neq 0$

$f(1) = 1+2+1 = 1 \neq 0$

$f(2) = 8+4+1 = 1 \neq 0$, so x^3+2x+1 is irred over $\mathbb{Z}_3$.

#1b) Say α is a root of x^3+2x+1 in an extension field of $\mathbb{Z}_3$. Let's factor x^3+2x+1 over $\mathbb{Z}_3(\alpha)$.

$$
\begin{array}{r}
x^2 + \alpha x + (2+\alpha^2) \\
x-\alpha \;\overline{)\; x^3 + 0x^2 + 2x + 1} \\
\underline{-x^3 + \alpha x^2} \\
\alpha x^2 + 2x \\
\underline{-\alpha x^2 + \alpha^2 x} \\
(2+\alpha^2)x + 1 \\
\underline{-(2+\alpha^2)x + \alpha(2+\alpha^2)} \\
\alpha^3 + 2\alpha + 1 = 0 \quad \text{since } f(\alpha) = 0.
\end{array}
$$

Now we need to find the remaining 2 zeros of the quadratic that's left.

Unfortunately we have 27 candidates (since $\mathbb{Z}_3(\alpha)$ has $3^3 = 27$ elements). At least you know you don't need to recheck the constants: 0, 1, 2.

Note Just as with quadratics over $\mathbb{Z}$, with $x^2 + \alpha x + (2+\alpha^2)$, the two roots should add to $(-\alpha)$ and multiply to $(2+\alpha^2)$.

This is quite tricky because of the strange multiplication, but it should lead to some hope for ~~linear~~ elements that are linear in α, since $-\alpha = 2\alpha$, ~~or~~ in $\mathbb{Z}_3(\alpha)$. (and $\alpha^2+2 = \alpha^2-1$)

If you try $\alpha+1$ and $\alpha+2 = \alpha-1$, these will both work. Note you can avoid a second round of polynomial division by realizing this fact about the sum and product of roots of a quadratic.

Thus $x^3 + 2x + 1 = (x-\alpha)(x-(\alpha+1))(x-(\alpha+2))$

$= (x+2\alpha)(x+2\alpha+2)(x+2\alpha+1)$

(Any legitimate version of this is ok.)

#2) We can easily check that $x^3+x^2+1 = f(x)$ is an irreducible cubic over $\mathbb{Z}_2$, since $f(0)=1$ and $f(1)=1$.

(this is from problem 25 in Section 29, but another option is x^3+x+1.)

Since $\mathbb{Z}_2$ is a field, this irreducible poly generates a principal ideal which is maximal in $\mathbb{Z}_2[x]$. (This is one of our Section 29 thms.) Next, since $\langle f(x) \rangle$ is a maximal ideal of the commutative ring $\mathbb{Z}_2[x]$, we know the quotient $\mathbb{Z}_2[x]/\langle f(x)\rangle = \mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$ is a field (using Thm: R/M = field iff M = maxl)

Finally, we know there is exactly one coset for each remainder allowed by the division algorithm. The possible remainders are for

$x^3 + x^2 + 1$ (or whichever cubic you used)

are $a_2 x^2 + a_1 x + a_0$, where $a_i \in \mathbb{Z}_2$.

There are 8 such remainders, so our field $\mathbb{Z}_2[x] / \langle x^3 + x^2 + 1 \rangle$ has 8 elements.

Let's compute our inverses. Let $I = \langle x^3 + x^2 + 1 \rangle$.

Then $0 + I$ has no multiplicative inverse.

Then $(1 + I)^{-1} = 1 + I$

and ~~$(1 + I)^{-1} = 1 + I$~~

ie ~~$(2 + I)^{-1} = 2 + I$~~

(Note in any field, 1 and -1 are their own inverses.) irrelevant here, as $1 = -1$.

The rest requires experimentation with multiplying. You need not put all your scratch work in, just the parts that worked. A quick way to get them all is as follows: Note

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

So $(x+I)(x^2+x+I) = x^3+x^2+I$

$= -1+I$

$= 1+I.$

So $(x+I)$ and (x^2+x+I) are an inverse pair.

Similarly $(x^2+I)(x+1+I) = x^3+x^2+I$

$= 1+I$

so (x^2+I) and $(x+1+I)$ are an inverse pair.

Note only 2 of our 8 elements remain:

$(x^2+x+1)+I$ and $(x^2+1)+I$. Due to counting, they must either be an inverse pair, or both be self-inverses. Let's see if $(x^2+1)+I$ is it's own inverse:

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

$= x^4+1$

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

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

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

This means $\left((x^2+1)+I\right)^2 \neq 1+I$

(it's x^2+I),

so $(x^2+1)+I$ is not its own inverse,

and thus $(x^2+1)+I$ and $(x^2+x+1)+I$

are an inverse pair.

(Note at the bottom of the previous page, I was essentially doing long division. You should convince yourself that I could also have substituted $x^4 \to x(x^3) \to (x)(x^2+1)$.
if I had the $+I$ ideal part in there
Note it's not true for the plain polynomials, but it's fine with the cosets.

Note the inverses will be different if you used x^3+x+1

#3a) Since F is a finite field, we know

$\langle F, + \rangle$ is a finite abelian group, so

by the FTFGAG, it is isomorphic

to a product of the form

$$\mathbb{Z}_{p_1^{R_1}} \times \mathbb{Z}_{p_2^{R_2}} \times \cdots \times \mathbb{Z}_{p_k^{R_k}} \quad \text{with } p_i \text{ all prime, } R_i \in \mathbb{Z}^+$$

We know $\text{char}(\mathbb{Z}_n) = n$ and the characteristic

of a product of rings satisfies $\text{char}(R \times S) =$

$\text{lcm}(\text{char } R, \text{char } S)$, and similar for products

of more rings.

thus $\text{lcm}\left(p_1^{k_1}, p_2^{k_2}, \ldots, p_k^{R_k}\right) = p = \text{char } F.$

But the only way this can happen is if

$$p_i = p \ \forall i \quad \text{and} \quad R_i = 1 \ \forall i.$$

thus $\langle F, + \rangle \cong \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{k \text{ copies}}$, so

$|F| = p^k$.

#36) Let F^* denote the multiplicative group of units of F. Since all elements except 0 are units, $|F^*| = p^k - 1$.

Thus, using the theorem (from ages ago) that $g^{|G|} = e_G$ for any group G with $g \in G$, identity element e_G,

We see that $\forall\ a \in F$, we have $a^{(p^k-1)} = 1$. Thus a is a root of the polynomial $x^{(p^k-1)} - 1 \in P[x]$.