HOME EXERCISE 1:

1. $p(x) = x^4 + x^2 + 1$ over $\mathbb{F}_2$

We know that it must be a factor of two irreducible polynomials if it is not irreducible.

We start by looking at the possible roots

$p(0) = 1$ & $p(1) = 1$, thus

$\{x, x+1, x^2+1, x^3+1, x^3+x^2, x^3+x\}$ cannot be factors (if it is irreducible.

Possible factors

$\{x^2+x+1, x^3+x^2+1, x^3+x+1\}$

& since x^2+x+1 is the only factor that can produce a polynomial of deg ≤ 4, we have

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

It is therefore not irreducible.

ANSWER: x^4+x^2+1 over $\mathbb{F}_2$ is reducible.

2. $p(x) = x^3 + x + 1$ over $\mathbb{F}_3$

We look for potential roots

$p(1) = 0$, $p(0) = 1$.

it suggests that $(x+2)$, which is irreducible could be a factor.

Long division gives

$$
\begin{array}{l|l}
\quad x^2 + x + 1 & \\
\hline
x^3 + x + 1 & x+2 \\
-x^3 + x^2 & -x^2(x+2) = -x^3 - 2x^2 = -x^3 + x^2 \\
\quad x^2 + x + 1 & -x(x+2) = -x^2 - 2x = -x^2 + 1 \\
-x^2 + 1 & \\
\quad x + 2 & \\
-x - 2 & \\
\quad 0 &
\end{array}
$$

As we can see, x^3+x+1 is a factor of the irreducible polynomial $x+2$ and is therefor reducable as well.

ANSWER: $\mathbb{F}_3 < x^3 + x + 1 >$ is <u>reducable</u>

3. $x^2 + \alpha^5 x + 1$ over $\mathbb{F}_{2^4}$ where $\alpha^4 + \alpha + 1 = 0$

In order to construct a finite field over $\mathbb{F}_{2^4}$, we use the irreducible polynomial $\pi(y) = y^4 + y + 1$ & that $\pi(\alpha) = \alpha^4 + \alpha + 1 = 0$, so we get that $\alpha^4 = \alpha + 1$ & that $\alpha^5 = \alpha(\alpha^4) = \alpha(\alpha + 1) =$

$= \alpha^2 + \alpha$

HOME EXERCISE 2:

$\pi(x) = x^4 + x + 1$ creates $\mathbb{F}_{2^4}$ & we assume

$\pi(\alpha) = \alpha^4 + \alpha + 1 = 0$ in some extension field.

The order of α is the least positive integer such that $\alpha^t \equiv 1 \pmod{\pi(x)}$

We know that $x^4 + x + 1$ is irreducible & primitive, & thus we must have that the period of $\pi(\alpha)$ is $2^4 - 1 = 15$, i.e $\alpha^{15} \equiv 1 \mod \pi(\alpha)$

& thus we get

1. $(\alpha)^t \equiv 1 \pmod{\pi(\alpha)}$ for $t = 15$

2. $(\alpha^2)^t \equiv 1 \pmod{\pi(\alpha)}$ for $t = 15$

   since 2 doesn't divide 15 but $30 = 2 \cdot 15$ does which $(\alpha^{30}) \equiv 1 \mod \pi(\alpha)$ also holds.

3. $(\alpha^3)^t \equiv 1 \mod (\pi(\alpha))$ for $t = 5$

4. We know $\alpha^4 = \alpha + 1$ & that if we're looking at the multiplication table formed by $\pi(\alpha)$, we have that $\alpha + \alpha^3 = \alpha^9$

   & thus $(\alpha^9)^t \overset{?}{=} \alpha^{15k} \equiv 1 \mod \pi(\alpha)$

   & since $9 \cdot 5 = 45$ & $15 \cdot 3 = 45$ we get that $t = 5$

Summary: 1) $t = 15$, 2) $t = 15$, 3) $t = 5$, 4) $t = 5$

HOME EXERCISE 3:

1. $x^4 + x^2 + 1$ over $\mathbb{F}_2$

As found out in H1, $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ which reduces the problem to find the period of $x^2 + x + 1$

In order to do so. we can look for the least positive integer T such that $(x^2 + x + 1) \mid (1 + x^T)$. We start with $T = 3$

$$
\begin{array}{l|l}
\multicolumn{1}{l}{\quad x + 1} & \\
\hline
\cancel{x^3} + 1 & x^2 + x + 1 \\
\cancel{x^3} + x^2 + x & \\
\hline
x^2 + x + 1 & \\
x^2 + x + 1 & \\
\hline
0 &
\end{array}
$$

thus $T_1 = 3$ & using Theorem 4.5 we have that $T_2 = 2^1 \cdot T_1 = 6$ since

$2^{m-1} < 2 \leq 2^m$ for $m = 1$

we can then form the cycle set

$$1(1) \oplus \frac{(q^{L_1} - 1)}{T_1}(T_1) \oplus \frac{q^{L_1}(q^{L_1} - 1)}{T_2}(T_2) \iff$$

$$1(1) \oplus \frac{4 - 1}{3}(3) \oplus \frac{4(4 - 1)}{6}(6) \iff$$

ANSWER: $1(1) \oplus 1(3) \oplus 2(6)$

2. $x^3 + x + 1$ over $\mathbb{F}_3$

We found out in H1.2 that x^3+x+1 can be factorized as $x^3+x+1 = (x+2)(x^2+x+2)$ which reduces the problem to find out the cycle sets of $x+2$ & x^2+x+2.

First we check if x^2+x+2 is primitive, which we can check by seeing if it divides $x^{q^m} - x = x^{3^2} - x = x^9 - x$, which is the same as checking $x^8 - 1$.

$$
\begin{array}{l|l}
 & x^6 + 2x^5 + 2x^4 + 2x^2 + x + 1 \\
\hline
x^8 - 1 & x^2 + x + 2 \\
-\ x^8 + 2x^7 + x^6 & \\
\hline
2x^7 + x^6 - 1 & \\
-\ 2x^7 + x^6 + 2x^5 & \\
\hline
2x^6 + 2x^5 - 1 & \\
-\ 2x^6 + x^5 + 2x^4 & \\
\hline
2x^4 - 1 & \\
-\ 2x^4 + x^3 + 2x^2 - 1 & \\
\hline
x^3 + 2x^2 - 1 & \\
-\ x^3 - x^2 - 2x & \\
\hline
x^2 + x + 2 & \\
-\ x^2 - x - 2 & \\
\hline
0 &
\end{array}
$$

which means that x^2+x+1 is primitive with period $T_1 = q^L - 1 = 3^2 - 1 = 9 - 1 = 8$ which gives the cycle set:

$$S_1 = 1(1) \oplus 1(8)$$

The next polynomial is $x+2$. We again check if it is primitive by determine if it divides $x^{3^1}-x = x^3 - x$ which we can instead look for x^2-1

$$
\begin{array}{l|l}
\multicolumn{1}{l}{\quad x} & \\
\hline
x^2 - 1 & x+2 \\
\cline{2-2}
-x^2 - 2x & -x(x+2) = -x^2 - 2x \\
\cline{1-1}
\quad x + 2 & \\
\quad \underline{-x - 2} & \\
\qquad 0 &
\end{array}
$$

$x+2$ is also primitive with period $T_2 = 3-1 = 2$

We get the cycle set

$$S_2 = 1(1) \oplus 1(2) =$$

Using theorem 4.6, we get that

$$S_1 \times S_2 = [1(1) \oplus 1(8)] \times [1(1) \oplus 1(2)] =$$

$$= 1(1) \times 1(1) \oplus 1(1) \times 1(2) \oplus 1(8) \times 1(1) \oplus 1(8) \times 1(2) =$$

$$= 1(1) \oplus 1(2) \oplus 1(8) + 1 \cdot 1 \cdot \gcd(8,2)(\mathrm{lcm}(8,2)) =$$

$$= 1(1) \oplus 1(2) \oplus 1(8) + 1 \cdot 1 \cdot 2\ (8) =$$

$$= 1(1) \oplus 1(2) \oplus 3(8)$$

We check that $1 \cdot 1 + 1 \cdot 2 + 3 \cdot 8 = 27$ which we expect for a polynomial of degree 3 over $\mathbb{F}_3$ since $3^3 = 27$ & therefore it is correct

ANSWER: $1(1) \oplus 1(2) \oplus 3(8)$