Homework 7.

1. $x+2$ is a factor of $x^6 - x^4 + x^3 - x + 1$ in $\mathbb{Z}_p[x]$

$\iff$ -2 is a root of $x^6 - x^4 + x^3 - x + 1$ in $\mathbb{Z}_p$

$\iff$ $p \mid (-2)^6 - (-2)^4 + (-2)^3 - (-2) + 1$

$\iff$ $p \mid 43$

$\iff$ $p = 43$

2. Since $1^3 - 2\times 1 + 1 = 0$ in $\mathbb{Z}_5$. $\Rightarrow$ 1 is a zero of $x^3 - 2x + 1$ in $\mathbb{Z}_5$.

$\Rightarrow$ $x^3 - 2x + 1$ has $x-1$ as a factor

Compute

$$
\begin{array}{r|l}
 & x^2 + x - 1 \\
\hline
x - 1 & x^3 - 2x + 1 \\
 & x^3 - x^2 \\
\hline
 & \quad x^2 - 2x + 1 \\
 & \quad x^2 - x \\
\hline
 & \qquad -x + 1
\end{array}
$$

$\Rightarrow$ $x^3 - 2x + 1 = (x-1)(x^2 + x - 1)$.

Remark : In fact $x^3 - 2x + 1 = (x-1)(x-2)^2$

2 is also a zero of $x^3 - 2x + 1$.

You may write $x^3 - 2x + 1 = (x-2)(x^2 - 3x + 2)$ in this case.

3. · Consider arbitrary degree 2 polynomial $ax^2 + bx + c$ in $\mathbb{Z}_2[x]$.

$a = 1$ to be degree 2, so there are $2 \times 2 = 4$ polynomials in total.

x^2	×	0 is zero
$x^2 + x$	×	0 is zero
$x^2 + 1$	×	1 is zero
$x^2 + x + 1$	✓	

$\Rightarrow$ there is 1 degree 2 polynomial in $\mathbb{Z}_2[x]$ without zero

· Similarly, there are $2\times 2\times 2 = 8$ degree 3 polynomials in $\mathbb{Z}_2[x]$.

x^3	×	0 is zero
$x^3 + x^2$	×	0 ···
$x^2 + x$	×	0 ···
$x^3 + 1$	×	1 is zero

$x^3 + x^2 + x$	✓	
$x^3 + x^2 + 1$	✓	
$x^3 + x + 1$	✓	
$x^3 + x^2 + x + 1$	×	1 is zero

$\Rightarrow$ there are 3 degree 3 polynomials in $\mathbb{Z}_2[x]$ without zero

4. (a). $f(x) := x^4 - 2x^2 - 2.$

$f(\alpha) = (1+\sqrt{3})^2 - 2(1+\sqrt{3}) - 2 = (1+2\sqrt{3}+3) - (2+2\sqrt{3}) - 2 = 0.$

Consider the evaluation map $\phi_\alpha : \mathbb{Q}[x] \longrightarrow \mathbb{C}$

$$g(x) \longmapsto g(\alpha).$$

Clearly $\langle f(x) \rangle \subseteq \ker \phi_\alpha.$

$f(x)$ is irreducible and $\mathbb{Q}[x]$ is PID $\Rightarrow \langle f(x) \rangle$ is maximal ideal

$\Rightarrow$ either $\langle f(x) \rangle = \ker \phi_\alpha$ or $\ker \phi_\alpha = \mathbb{Q}[x].$

$1 \notin \ker \phi_\alpha \Rightarrow$ We have $\langle f(x) \rangle = \ker \phi_\alpha.$

$\Rightarrow$ $f(x)$ is the minimal polynomial of α.

$\Rightarrow$ By the main theorem of evaluation map and $\deg f(x) = 4$

We have $\operatorname{Im} \phi_\alpha = \{ c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_i \in \mathbb{Q} \}.$

By 1st Isomorphism theorem,

$$\mathbb{Q}[x] / \langle x^4 - 2x^2 - 2 \rangle \cong \{ c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_i \in \mathbb{Q} \}.$$

(b). $f(\alpha) = \alpha^4 - 2\alpha^2 - 2 = 0.$

$\Rightarrow \quad \alpha^4 - 2\alpha^2 = 2$

$\Rightarrow \quad \dfrac{\alpha^4 - 2\alpha^2}{2} = 1$

$\Rightarrow \quad \alpha \left(\dfrac{\alpha^3 - 2\alpha}{2} \right) = 1.$

$\Rightarrow \quad \alpha^{-1} = \dfrac{\alpha^3 - 2\alpha}{2} = -\alpha + \frac{1}{2}\alpha^3$