Homework 9

1\. (a) $\mathbb{Z}_3$ is a field, x^3-x+1 has degree 3.

x^3-x+1 is irreducible in $\mathbb{Z}_3[x]$ iff x^3-x+1 has no root in $\mathbb{Z}_3$.

Since
$$0^3-0+1=1 \neq 0$$
$$1^3-1+1=1 \neq 0 \quad \text{in } \mathbb{Z}_3$$
$$2^3-2+1=7 \neq 0$$

$\Rightarrow$ x^3-x+1 has no root in $\mathbb{Z}_3$.

(b) $\mathbb{Z}_3[x]$ is a PID and x^3-x+1 is irreducible in $\mathbb{Z}_3[x]$

$\Rightarrow$ $\langle x^3-x+1\rangle$ is maximal ideal

$\Rightarrow$ $\mathbb{Z}_3/\langle x^3-x+1\rangle$ is a field

(c) We know that $\mathbb{Z}_3[x]/\langle x^3-x+1\rangle$ has $3^3=27$ elements.

Consider the map
$$\phi_a : \mathbb{Z}_3[x] \longrightarrow \mathbb{C}$$
$$g(x) \longmapsto g(a)$$

- $\operatorname{Im}\phi_a = \{c_0+c_1 a+c_2 a^2 \mid c_i \in \mathbb{Z}_3\}$.

  Clearly $c_0+c_1 a+c_2 a^2 \in \operatorname{Im}\phi_a$.

  Now for any $g(x)\in\mathbb{Z}_3[x]$, $g(x)=p(x)(x^3-x+1)+r(x)$, $p(x), r(x)\in\mathbb{Z}_3[x]$, $\deg r(x)\le 2$.

  Then $g(a)=p(a)\cdot 0 + r(a) \in \{c_0+c_1 a+c_2 a^2 \mid c_i\in\mathbb{Z}_3\}$.
- a is a root of x^3-x+1 $\Rightarrow$ $\langle x^3-x+1\rangle \subseteq \ker\phi_a$.

  But $1\notin\ker\phi_a$ $\Rightarrow$ $\ker\phi_a \neq \mathbb{Z}_3[x]$ $\Rightarrow$ $\langle x^3-x+1\rangle = \ker\phi_a$.
- By 1st Isomorphism Theorem, $\mathbb{Z}_3[x]/\langle x^3-x+1\rangle \cong \{c_0+c_1 a+c_2 a^2 \mid c_i\in\mathbb{Z}_3\}$.

$\Rightarrow$ $\{c_0+c_1 a+c_2 a^2 \mid c_i\in\mathbb{Z}_3\}$ is field of 27 elements, with root of x^3-x+1, which is a.

2\. (a). Consider 3, prime number

$3\mid 6$, $3\mid 30$, $3\mid 12$, but $3^2\nmid 12$

$\Rightarrow$ $f(x)$ is irreducible by Eisenstein criteria.

(b). Consider the evaluation map
$$\phi_a : \mathbb{Q}[x] \longrightarrow \mathbb{C}$$
$$g(x) \longmapsto g(a)$$

$f(x)$ has a as root and $f(x)$ is irreducible

$\Rightarrow$ $\ker\phi_a = \langle f(x)\rangle$

By the main theorem of evaluation map, we have since $\deg f(x) = 5$

$\operatorname{Im}\phi = \{ c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + c_4\alpha^4 \mid c_i \in \mathbb{Q} \}$ and the image is a field.

(c). Suppose we have $a_0 + a_1\alpha + \cdots + a_4\alpha^4 = 0$, $a_i \in \mathbb{Q}$.

Consider $g(x) = a_0 + a_1 x + \cdots + a_4 x^4$, $g(\alpha) = 0$ by assumption.

$\Rightarrow g(x) \in \ker\phi_\alpha = \langle f(x) \rangle \Rightarrow g(x) = f(x)\cdot h(x)$

But $\deg g(x) \leq 4 < \deg f(x) = 5$

$\Rightarrow$ the only possibility is that $g(x) = h(x) = 0$

$\Rightarrow a_i = 0$. $i = 0, \cdots, 4$.

3. $f(x)$ is irreducible in $\mathbb{Q}[x]$ iff $f(-x)$ is irreducible iff $f(-(x+1))$ is irreducible.

$f(-(x+1)) = (x+1)^{p-1} + (x+1)^{p-2} + \cdots + (x+1) + 1$

$$= \frac{1-(1+x)^p}{1-(1+x)} = x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1}$$

$p \mid \binom{p}{i}$ but $p^2 \nmid \binom{p}{p-1}$

By Eisenstein's criteria, it's irreducible.

Another way of writting 3:

$f(x)$ is irreducible iff $f(-x)$ is irreducible.

Let $g(x) = f(-x) = x^{p-1} + x^{p-2} + \cdots + x + 1$.

As we did in lecture, $g(x) = \dfrac{x^p - 1}{x - 1}$

$$g(y+1) = \frac{(y+1)^p - 1}{(y+1) - 1} = \frac{y^p + \binom{p}{1} y^{p-1} + \cdots + \binom{p}{p-1} y}{y} = y^{p-1} + \binom{p}{1} y^{p-2} + \cdots + \binom{p}{p-1}.$$

$g(y+1)$ is irreducible by Eisenstein's criterion. ($p \mid \binom{p}{i}$ $1 \leq i \leq p-1$, $p^2 \nmid \binom{p}{p-1}$).

Suppose $g(x)$ is reducible, then

$g(x) = g_1(x) g_2(x)$, with $\deg g_i(x) \geq 1$.

$\Rightarrow g(y+1) = g_1(y+1) g_2(y+1)$ with $\deg g_i(y+1) \geq 1$, contradiction.

$\Rightarrow g(x) = f(-x)$ is irreducible

$\Rightarrow f(x)$ is irreducible.

4. (a) $\alpha^4-2\alpha^2-2 = \left(\sqrt{1+\sqrt{3}}\right)^4 - 2\left(\sqrt{1+\sqrt{3}}\right)^2 - 2$

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

$\Rightarrow$ α is a root of x^4-2x^2-2

By Eisenseein's criteria, we notice that $2 \mid 2$ but $2^2 \nmid 2$.

$\Rightarrow$ x^4-2x^2-2 is irreducible

$\Rightarrow$ x^4-2x^2-2 is minimal polynomial

(b) As usual, consider the evaluation map ϕ_α at α.

x^4-2x^2-2 is irreducible and admits α as a root

$\Rightarrow \ker \phi_\alpha = \langle x^4-2x^2-2 \rangle$

By the main theorem of evaluation map and the fact that $\deg x^4-2x^2-2 = 4$.

We have that $\operatorname{Im}\phi = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{Q}\}$ is a field.

5. x^2+2 is irreducible in $\mathbb{Z}_5[x]$ as it has no root

$\Rightarrow$ $\mathbb{Z}_5[x]/\langle x^2+2 \rangle$ is a field with $5^2 = 25$ elements.