Homework 6

1. (a) By Fermat little theorem, $x^p \equiv x \pmod{p}$ $\forall x \in \mathbb{Z}$.

So in $\mathbb{Z}_p$, $x^p - x + 1 = x - x + 1 = 1 \neq 0$. (since $p \neq 1$)

$\Rightarrow$ The equation $x^p - x + 1$ has no zero in $\mathbb{Z}_p$.

(b). To prove $x^3 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$,

it suffices to prove that $x^3 - x + 1$ has no zero in $\mathbb{Z}_3$ since the degree of $x^3 - x + 1$ is 3,

and $\mathbb{Z}_3$ is a field.

It's true by part (a) if we let $p = 3$.

2. (a). To prove $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, it suffices to prove that $x^3 - 2$ has no rational root since $\mathbb{Q}$ is a field and $\deg(x^3 - 2) = 3$.

Assume by contradiction that $r = \frac{a}{b} \in \mathbb{Q}$ is a root of $x^3 - 2$,

with $a, b \in \mathbb{Z}$, $a \neq 0$ (since 0 is not a root), $b \neq 0$, $\gcd(a, b) = 1$.

Then $(\frac{a}{b})^3 = 2 \Rightarrow a^3 = 2b^3$.

$\gcd(a, b) = 1 \Rightarrow a^3 \mid 2. \Rightarrow a \mid 2 \Rightarrow a = \pm 1$ or ± 2.

$a = \pm 1 \Rightarrow \pm 1 = 2b^3 \Rightarrow b^3 = \pm \frac{1}{2}$ $\lightning$.

$a = \pm 2 \Rightarrow \pm 8 \mid 2$ (since $a^3 \mid 2$). $\lightning$.

$\Rightarrow$ Our assumption is wrong.

(b) (-1). $\phi_{\sqrt[3]{2}}(x^3 - 2) = (\sqrt[3]{3})^3 - 2 = 0 \Rightarrow \langle x^3 - 2 \rangle \subset \operatorname{Ker} \phi_{\sqrt[3]{2}}$.

$x^3 - 2$ is irreducible in $\mathbb{Q}[x]$, and $\mathbb{Q}[x]$ is a principal ideal domain, $\mathbb{Q}[x]$ is not a field (x is not invertible)

$\Rightarrow \langle x^3 - 2 \rangle$ is a maximal ideal.

The inclusion $\langle x^3 - 2 \rangle \subset \operatorname{Ker} \phi_{\sqrt[3]{2}} \Rightarrow \operatorname{Ker} \phi_{\sqrt[3]{2}} = \mathbb{Q}[x]$

or $\ker \phi_{\sqrt[3]{2}} = \langle x^3 - 2 \rangle$.

But $\phi_{\sqrt[3]{2}}(1) = 1 \neq 0 \Rightarrow \ker \phi_{\sqrt[3]{2}} \neq \mathbb{Q}[x]$

$\Rightarrow \operatorname{Ker} \phi_{\sqrt[3]{2}} = \langle x^3 - 2 \rangle$.

(-2) (b-1) implies that $x^3 - 2$ is the minimal polynonimal of $\sqrt[3]{2}$.

By the main theorem of evaluation map : For an algebraic element α, let ϕ_α be the evaluation map, $m_\alpha(x)$ is the minimal polynomial of α s.t. $\operatorname{Ker} \phi_\alpha = \langle m_\alpha(x) \rangle$ and $m_\alpha(x)$ is irreducible. Then

$\mathrm{Im}\,\phi_\alpha = \{c_0 + c_1\alpha + \cdots + c_n\alpha^n \mid c_i \in \mathbb{Q}\}$, where $n = $ degree $m_\alpha(x)$.

Apply this to the case when $\alpha = \sqrt[3]{2}$ and $n = \deg(x^3-2) = 3$,

$\Rightarrow \mathrm{Im}\,\phi_{\sqrt[3]{2}} = \{c_0 + c_1\sqrt[3]{2} + c_1(\sqrt[3]{2})^2 \mid c_i \in \mathbb{Q}\}. = \mathbb{Q}[\sqrt[3]{2}]$

(-3) By 1st isomorphism theorem:

$$\mathbb{Q}[x]/\ker\phi_{\sqrt[3]{2}} \cong \mathrm{Im}\,\phi_{\sqrt[3]{2}}.$$

i.e. $\mathbb{Q}[x]/\langle x^3-2\rangle \cong \mathbb{Q}[\sqrt[3]{2}]$.

(-4). Again by the main theorem of evaluation map, we have $\mathrm{Im}\,\phi_\alpha$ is a field.

(where α, ϕ_α are as above)

$\Rightarrow \mathrm{Im}\,\phi_\alpha = \mathbb{Q}[\sqrt[3]{2}]$ is a field.

Remark: You can also prove (-2) and (-4) without quoting the main theorem.

For (-2), prove the two sides inclusion, you may want to use long division for this.

For (-4), prove $\mathbb{Q}[x]/\langle x^3-2\rangle$ is a field instead, and it's because $\langle x^3-2\rangle$

is maximal ideal.

3. (a). · $\sqrt{-21} \neq 0$

· $\sqrt{-21}$ is not a unit. Otherwise $\exists\ a+b\sqrt{-21} \in \mathbb{Z}[\sqrt{-21}]$ s.t.

$$\sqrt{-21}\cdot(a+b\sqrt{-21}) = 1.$$

$\Rightarrow |\sqrt{-21}\cdot(a+b\sqrt{-21})|^2 = 1^2$ (where $|z|^2 = z\cdot\bar{z}$ for $z \in \mathbb{C}$)

$\Rightarrow |\sqrt{-21}|^2 \cdot |a+b\sqrt{-21}|^2 = 1$.

Note that

$\Rightarrow 21\cdot(a^2+21b^2) = 1$ ↯. $\left(|a+b\sqrt{-21}|^2 = (a+b\sqrt{-21})(a-b\sqrt{-21}) = a^2+21b^2\right)$

· Now suppose $\sqrt{-21} = (a+b\sqrt{-21})(c+d\sqrt{-21})$ with $a,b,c,d \in \mathbb{Z}$.

Then $|\sqrt{-21}|^2 = |a+b\sqrt{-21}|^2\,|c+d\sqrt{-21}|^2$

$\Rightarrow 21 = (a^2+21b^2)(c^2+21d^2)$.

Case 1: $a^2+21b^2 = 3$. $21 > 3 \Rightarrow b=0 \Rightarrow a^2 = 3$ ↯

Case 2: $a^2+21b^2 = 7$. $21 > 7 \Rightarrow b=0 \Rightarrow a^2 = 7$ ↯.

Case 3: $a^2+21b^2 = 1$. $21 > 1 \Rightarrow b=0 \Rightarrow a = \pm1 \Rightarrow a+b\sqrt{-21} = \pm1$ is unit.

Case 4: $a^2+21b^2 = 21 \Rightarrow c^2+21d^2 = 1 \Rightarrow c+d\sqrt{-21} = \pm1$ is unit.

$\Rightarrow \sqrt{-21}$ is irreducible in $\mathbb{Z}[\sqrt{-21}]$

(b). $21 \in \langle \sqrt{-21} \rangle$. $21 = 3 \times 7$. Now we show $3 \notin \langle \sqrt{-21} \rangle$. $7 \notin \langle \sqrt{-21} \rangle$.

Suppose $3 \in \langle \sqrt{-21} \rangle$, then $3 = \sqrt{-21} \cdot (a + b\sqrt{-21})$

$|3|^2 = |\sqrt{-21}|^2 \, |a + b\sqrt{-21}|^2 \Rightarrow 9 = 21(a^2 + 21b^2)$ ↯.

Suppose $7 \in \langle \sqrt{-21} \rangle$, then $7 = \sqrt{-21}(c + d\sqrt{-21})$

$\Rightarrow 49 = 21(a^2 + 21b^2)$. but $21 \nmid 49$. ↯.

$\Rightarrow \langle \sqrt{-21} \rangle$ is not a prime ideal.

(c). Assume by contradiction that $\mathbb{Z}[\sqrt{-21}]$ is PID,

then $\langle \sqrt{-21} \rangle$ is maximal ideal since $\sqrt{-21}$ is irreducible

$\Rightarrow \langle \sqrt{-21} \rangle$ is prime ideal. ↯.

4. (a). First note that $x^2 + x + 1 = 0$ is irreducible in $\mathbb{Q}[x]$ since it's two roots are $\omega, \bar{\omega}$ while $\omega, \bar{\omega} \notin \mathbb{Q}$.

Consider the evaluation map at ω

$$\begin{aligned} \phi_\omega : \mathbb{Q}[x] &\longrightarrow \mathbb{C}. \\ f(x) &\longmapsto f(\omega). \end{aligned}$$

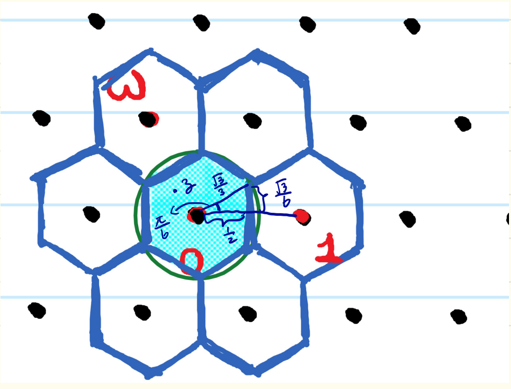
$\langle x^2 + x + 1 \rangle \subset \ker \phi_\omega$ since $x^2 + x + 1$ admits ω as zero.

But $\mathbb{Q}[x]$ is PID & $x^2 + x + 1$ is irreducible $\Rightarrow \langle x^2 + x + 1 \rangle = \ker \phi_\omega$ since $\ker \phi_\omega$ is obviously not $\mathbb{Q}[x]$.

Now apply the main theorem of evaluation map (as stated in 2.(b)(-2)), we have $\operatorname{Im} \phi_\omega = \mathbb{Q}[\omega]$ and $\mathbb{Q}[\omega]$ is a field.

By 1st isomorphism theorem, $\mathbb{Q}[x] / \langle x^2 + x + 1 \rangle \cong \mathbb{Q}[\omega]$.

(b).



The black dots are elements in $\mathbb{Z}[\omega]$. As shown in the figure, the entire complex plane is covered by regular hexagons. $\forall z \in \mathbb{Q}[\omega]$, z must land in one of the hexagons, suppose it's in the blue one. Since the distance of center of hexagon and any other point in hexagon is at most the radius of circle, which is $\frac{\sqrt{3}}{3}$ (as shown in the figure), we are done.

(c). Consider $\frac{a}{b} \in \mathbb{Q}[w]$. By (b), there is $q \in \mathbb{Z}[w]$ s.t. $\left|\frac{a}{b} - q\right| \leq \frac{\sqrt{3}}{3}$

Let $r = b\left(\frac{a}{b} - q\right). = a - bq \in \mathbb{Z}[w]$.

Then $\left|\frac{r}{b}\right| = \left|\frac{a}{b} - q\right| \leq \frac{\sqrt{3}}{3} \Rightarrow |r| \leq \frac{\sqrt{3}}{3}|b|$.

(d) Define Euclidean function on $\mathbb{Z}[w]$

$$\begin{aligned} N:\ \mathbb{Z}[w] \setminus \{0\} &\longrightarrow \mathbb{Z}_{>0} \\ a &\longmapsto |a|^2 \end{aligned}$$

$\forall\ a, b \in \mathbb{Z}[w],\ b \neq 0$.

By (c). $\exists\ q, r \in \mathbb{Z}[w]$ s.t. $a = bq + r$.

Either $r = 0$.

or $N(r) = |r|^2 \leq \frac{1}{3}|b|^2 = \frac{1}{3}N(b) \overset{\text{(since } N(b) \neq 0\text{).}}{<} N(b)$.

$\Rightarrow$ $\mathbb{Z}[w]$ is Euclidean domain.

(e). Euclidean domain implies PID.

Hence $\mathbb{Z}[w]$ is PID.

5. (a). · $a - bw \neq 0$ since otherwise $a = 0 = b$, contradicts that $a^2 + ab + b^2 = p$.

· $a - bw$ is not unit. Otherwise $1 = (a - bw)(c + dw)$.

$\Rightarrow |1|^2 = |a - bw|^2 |c + dw|^2$.

(In general, $|c + dw|^2 = (c + dw)(\overline{c + dw}) = (c + dw)(c + d\bar{w})$

$= c^2 + cd(w + \bar{w}) + d^2 w\bar{w} = c^2 - cd + d^2 \in \mathbb{Z}_{>0}$)

$\Rightarrow 1 = (a^2 + ab + b^2)(c^2 - cd + d^2) = p(c^2 - cd + d^2)$ ↯.

· Suppose $a - bw = (c + dw)(e + fw)$.

Then $|a - bw|^2 = |c + dw|^2 |e + fw|^2$

$\Rightarrow a^2 + ab + b^2 = (c^2 - cd + d^2)(e^2 - ef + f^2) = p$.

$\Rightarrow$ Case 1: $c^2 - cd + d^2 = 1$. $\Rightarrow (c + dw)(c + d\bar{w}) = 1$.

$w + \bar{w} = -1 \Rightarrow \bar{w} \in \mathbb{Z}[w] \Rightarrow c + d\bar{w} \in \mathbb{Z}[w]$

$\Rightarrow c + dw$ is a unit in $\mathbb{Z}[w]$.

Case 2: $c^2 - cd + d^2 = p \Rightarrow (e^2 - ef + f^2) = 1$

$\Rightarrow e + fw$ is unit.

$\Rightarrow a - bw$ is irreducible.

(b). First note that $b \neq 0$ in $\mathbb{Z}_p$.

Otherwise $b \mid p$. $a^2+ab+b^2 = (a+\frac{1}{2}b)^2 + \frac{3}{4}b^2 \geq \frac{3}{4}b^2 \geq \frac{3}{4}p^2 > p$ $\lightning$.

($p > 3 \Rightarrow \frac{3}{4}p > 1 \Rightarrow \frac{3}{4}p^2 > p$).

Conside $\frac{a}{b}$ in $\mathbb{Z}_p$.

$(\frac{a}{b})^2 + \frac{a}{b} + 1 = (\frac{1}{b})^2(a^2+ab+b^2) = 0$ in $\mathbb{Z}_p$ since $a^2+ab+b^2 \equiv 0 \pmod{p}$.

$a - b \cdot \frac{a}{b} = a - a = 0$.

$\Rightarrow \alpha = \frac{a}{b}$ is a solution for (b-1) and (b-2).

(c). · $\phi(a+bw + c+dw) = \phi(a+c+(b+d)w) = (a+c) + (b+d)\alpha$.

$\phi(a+bw) + \phi(c+dw) = a + b\alpha + c + d\alpha = (a+c) + (b+d)\alpha$

· $\phi((a+bw)(c+dw)) = \phi(ac + (ad+bc)w + bdw^2)$

$= \phi(ac + (ad+bc)w + bd(-w-1))$

$= \phi((ac-bd) + (ad+bc-bd)w)$

$= (ac-bd) + (ad+bc-bd)\alpha$.

$\phi(a+bw)\cdot\phi(c+dw) = (a+b\alpha)(c+d\alpha)$

$= ac + (ad+bc)\alpha + bd\alpha^2$

$= ac + (ad+bc)\alpha + bd(-\alpha-1)$

$= (ac-bd) + (ad+bc-bd)\alpha$.

$\Rightarrow$ ϕ is ring homomorphism.

(d) $\phi(a-bw) = a - b\cdot\alpha = 0$ in $\mathbb{Z}_p$ by our choice of α.

$\Rightarrow \langle a-bw \rangle \subset \ker\phi$.

Since $\mathbb{Z}[w]$ is PID (as shown in 4(e)) and $a-bw$ is irreducible.

$\Rightarrow \langle a-bw \rangle$ is maximal

$\Rightarrow \langle a-bw \rangle = \ker\phi$ since apperently $\ker\phi \neq \mathbb{Z}[w]$.

(e). $\forall\, n \in \mathbb{Z}_p$, by abuse of notation, view n as element in $\mathbb{Z}$.

Then $\phi(n) = n$

$\Rightarrow$ ϕ is surjective.

$\Rightarrow$ By 1st Isomorphism Theorem. $\mathbb{Z}[w]/(a-bw) \cong \mathbb{Z}_p$.