Name: Huize Shi - A92122910
Discussion: A04
Homework: 6

---

1. (a) Suppose p is a prime number. Prove that $x^p - x + 1$ has no zero in $\mathbb{Z}_p$.
   By Fermat's Little Theorem, $x^p \overset{p}{\equiv} x$. Hence the following is true:
   $$x^p - x + 1 \overset{p}{\equiv} 0$$
   $$1 \overset{p}{\not\equiv} 0$$
   Ergo, $x^p - x + 1$ has no zero in $\mathbb{Z}_p$.

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

2. (a) Prove that $f(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$.
   Since $2 \leq deg\ f \leq 3$, it is sufficient to show that f does not have a zero in $\mathbb{Q}[x]$. Suppose towards contrary $\exists b, c \in \mathbb{Z}, c > 0, gcd(b, c) = 1, f(\frac{b}{c}) = 0$.
   $$\begin{aligned} f\left(\frac{b}{c}\right) = 0 &= \left(\frac{b}{c}\right)^3 - 2 \\ b^3 &= 2c^3 \\ c \mid b^3,\ gcd(c,b) = 1 &\Rightarrow c \mid 1 \\ &\Rightarrow c = 1 \\ b \mid 2c^3,\ gcd(c,b) = 1 &\Rightarrow b \mid 2 \\ &\Rightarrow b = \pm 1,\ b = \pm 2 \end{aligned}$$
   This limits the possibility of zeros to $x = \pm 1$ and $x = \pm 2$.
   $$\begin{aligned} f(1) &= -1 \neq 0 \\ f(-1) &= -3 \neq 0 \\ f(2) &= 6 \neq 0 \\ f(-2) &= -10 \neq 0 \end{aligned}$$
   Hence shown $f(x) = x^3 - 2$ is irreducible in $\mathbb{Q}[x]$.

   (b) Let $\phi_{\sqrt[3]{2}} : \mathbb{Q}[x] \mapsto \mathbb{R}$ be the evaluation map $\phi_{\sqrt[3]{2}}(f(x)) = f(\sqrt[3]{2})$. We know that $\phi_{\sqrt[3]{2}}$ is a ring homomorphism.

   (b-1) Prove that $ker\ \phi_{\sqrt[3]{2}} = \langle x^3 - 2 \rangle$
   $$\begin{aligned} \phi_{\sqrt[3]{2}}(x^3 - 2) &= (\sqrt[3]{2})^3 - 2 \\ &= 2 - 2 = 0 \end{aligned}$$
   Hence shown $\langle x^3 - 2 \rangle \subseteq ker\ \phi_{\sqrt[3]{2}}$. By part **a**, we know $x^3 - 2$ is irreducible. This implies that $\langle x^3 - 2 \rangle$ is maximal. Since $ker\ \phi_{\sqrt[3]{2}} \neq \mathbb{Q}[x]$, $\langle x^3 - 2 \rangle \subseteq ker\ \phi_{\sqrt[3]{2}} \Rightarrow \langle x^3 - 2 \rangle = ker\ \phi_{\sqrt[3]{2}}$.

(b-2) Prove that $Im\ \phi_{\sqrt[3]{2}} = \{a_0 + \sqrt[3]{2}a_1 + (\sqrt[3]{2})^2 a_2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$

$$\begin{aligned} \forall f \in \mathbb{Q}[x],\ f(x) &= q(x)(x^3 - 2) + r(x) \\ r(x) &= a_0 + x a_1 + x^2 a_2 \\ \phi(f) &= q(\sqrt[3]{2})((\sqrt[3]{2})^3 - 2) + r(\sqrt[3]{2}) \\ &= 0 + r(\sqrt[3]{2}) \\ &= a_0 + \sqrt[3]{2}a_1 + (\sqrt[3]{2})^2 a_2 \end{aligned}$$

(b-3) Let $\mathbb{Q}[\sqrt[3]{2}] := \{a_0 + \sqrt[3]{2}a_1 + (\sqrt[3]{2})^2 a_2 \mid a_0, a_1, a_2 \in \mathbb{Q}\}$**. Prove that** $\mathbb{Q}[x] / \langle x^3 - 2 \rangle \simeq \mathbb{Q}[\sqrt[3]{2}]$

In (b-2), we showed that ϕ is surjective. In (b-1) we showed that $ker\ \phi_{\sqrt[3]{2}} = \langle x^3 - 2 \rangle$. The 1^{st} isomorphism theorem gives that $\mathbb{Q}[x] / \langle x^3 - 2 \rangle \simeq \mathbb{Q}[\sqrt[3]{2}]$.

(b-4) Prove that $\mathbb{Q}[\sqrt[3]{2}]$ **is a field.**

Since we know that $x^3 - 2$ is irreducible, $\langle x^3 - 2 \rangle$ is therefore a maximal ideal. This means that $\mathbb{Q}[x] / \langle x^3 - 2 \rangle$ is a field. By isomorphic relationship shown in (b-3) $\mathbb{Q}[\sqrt[3]{2}]$ is a field.

3. (a) Prove that $\sqrt{-21}$ is irreducible in $\mathbb{Z}[\sqrt{-21}]$
$\sqrt{-21} \neq 0$, $\sqrt{-21}$ is not a zero divisor since $\mathbb{Z}[\sqrt{-21}]$ is a subring of $\mathbb{C}$.

$$\begin{aligned} \sqrt{-21}(a + b\sqrt{-21}) &= 1 \\ \sqrt{-21}a - 21b &= 1 \\ a &= 0 \\ b &= \frac{1}{-21} \end{aligned}$$

This is impossible since $\frac{1}{-21} \notin \mathbb{Z}$. Hence $\sqrt{-21} \notin \mathcal{U}(\mathbb{Z}[\sqrt{-21}])$.

$$\begin{aligned} \sqrt{-21} &= (a + b\sqrt{-21})(c + d\sqrt{-21}) \\ 21 &= (a^2 + 21b^2)(c^2 + 21d^2) \\ a^2 + 21b^2 &= 3 \Rightarrow b = 0 \Rightarrow a^2 = 3 \\ a^2 + 21b^2 &= 7 \Rightarrow b = 0 \Rightarrow a^2 = 7 \end{aligned}$$

Since $a \in \mathbb{Z}$, this is impossible since $3, 7$ are not perfect sqaures. This means either $(a^2 + 21b^2) = 1$ or $(c^2 + 21d^2) = 1$. This means Either $(a^2 + 21b^2)$ or $(c^2 + 21d^2)$ must be a unit hence become 1 under absolute norm (multiplied by conjugate). Hence shown $\sqrt{-21}$ is irreducible in $\mathbb{Z}[\sqrt{-21}]$.

(b) Prove that $\langle\sqrt{-21}\rangle$ is not a prime ideal of $\mathbb{Z}[\sqrt{-21}]$

$$3\cdot(-7) = -21 = \sqrt{-21}\sqrt{-21} \in \langle\sqrt{-21}\rangle$$

Claim $3, -7 \notin \langle\sqrt{-21}\rangle$. Assume to the contrary that $3 \in \langle\sqrt{-21}\rangle$:

$$\begin{aligned} 3 &= \sqrt{-21}(a + b\sqrt{-21}) \\ 3 &= \sqrt{-21}a - 21b \\ a &= 0 \\ b &= \frac{-3}{21} = \frac{-1}{7} \end{aligned}$$

This is impossible since $b \in \mathbb{Z}$.

$$\begin{aligned} -7 &= \sqrt{-21}(a + b\sqrt{-21}) \\ -7 &= \sqrt{-21}a - 21b \\ a &= 0 \\ b &= \frac{7}{21} = \frac{1}{3} \end{aligned}$$

This is impossible since $b \in \mathbb{Z}$. Hence we have shown $3, -7 \notin \langle\sqrt{-21}\rangle$, $3\cdot(-7) = -21 \in \langle\sqrt{-21}\rangle$. Ergo, $\langle\sqrt{-21}\rangle$ is not a prime ideal of $\mathbb{Z}[\sqrt{-21}]$.

(c) Prove that $\mathbb{Z}[\sqrt{-21}$ is not a PID.
Assume towards contrary that $\mathbb{Z}[\sqrt{-21}$ is a PID. Since $\sqrt{-21}$ is irreducible in $\mathbb{Z}[\sqrt{-21}$, $\langle\sqrt{-21}\rangle$ is a maximal ideal of $\mathbb{Z}[\sqrt{-21}$. This means that $\langle\sqrt{-21}\rangle$ is also a prime ideal. This is a contradiction by the result of part **b**. Hence $\mathbb{Z}[\sqrt{-21}$ is not a PID.

4. let $\omega := \frac{-1+\sqrt{3}}{2}$. $\omega^2 + \omega + 1 = 0$; $\omega + \bar{\omega} = -1$ and $\omega\bar{\omega} = 1$ where $\bar{\omega}$ is the complex conjugate of ω. Let $\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$. We know that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$. Let $\mathbb{Q}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Q}\}$.

   (a) Prove that $\mathbb{Q}[x]/\langle x^2 + x + 1\rangle \simeq \mathbb{Q}[\omega]$ and $\mathbb{Q}[\omega]$ is a field.
   The evaluation map $\phi_\omega : \mathbb{Q}[x] \mapsto \mathbb{Q}[\omega]$ by $\phi_\omega(f(x)) = f(\omega)$ is a ring homomorphism. $Im\ \mathbb{Q}[\omega] = \mathbb{Q}[\omega]$ by definition of evaluation map.

$$\phi(x^2 + x + 1) = \omega^2 + \omega + 1 = 0$$

   This shows that $\langle x^2 + x + 1\rangle \subseteq ker\ \phi$.
   Show that $x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$:
   Since we know that $\mathbb{Q}[x]$ is a integral domain, $x^2 + x + 1$ is not a zero divisor.

$x^2 + x + 1 \neq 0$. Assume $x^2 + x + 1$ has a zero in $\mathbb{Q}[x]$, $\frac{a}{b}$, $gcd(a, b) = 1$, $b > 0$.

$$\left(\frac{a}{b}\right)^2 + \frac{a}{b} + 1 = 0$$
$$a^2 + ab + b^2 = 0$$
$$a^2 = b(-a - b)$$
$$b \mid a^2,\ gcd(a, b) = 1 \Rightarrow b \mid 1 \Rightarrow b = 1$$
$$b^2 = a(-a - b)$$
$$a \mid b^2,\ gcd(a, b) = 1 \Rightarrow a \mid 1 \Rightarrow a = \pm 1$$
$$1^2 + 1 + 1 = 3 \neq 0$$
$$(-1)^2 - 1 + 1 = 1 \neq 0$$

Since the degree is between 2 and 3, this means $x^2 + x + 1$ is irreducible. Hence $\langle x^2 + x + 1\rangle$ is maximal, $\langle x^2 + x + 1\rangle \subseteq ker\ \phi \Rightarrow \langle x^2 + x + 1\rangle = ker\ \phi$.
By 1^{st} isomorphism theorem, we have $\mathbb{Q}[x] / \langle x^2 + x + 1\rangle \simeq \mathbb{Q}[\omega]$. Since $\langle x^2+x+1\rangle$ is maximal, we know $\mathbb{Q}[x] / \langle x^2 + x + 1\rangle$ is a field, and by isomorphism $\mathbb{Q}[\omega]$ is also a field.

(b) Prove that for any $z \in \mathbb{Q}[\omega]$ there is $u \in \mathbb{Z}[\omega]$ such that $\mid z - u \mid \leq \frac{\sqrt{3}}{3}$.
As the image suggests, any z chosen on the plain of $\mathbb{Q}[\omega]$ plain, there exist a $u \in \mathbb{Z}[w]$ such that z fall within the regular hexagon centered around u. Hence the maximum distance would be the distance between a vertex and the center of the hexagon.

$$|z - u| \leq \frac{1}{2} \cdot cos\left(\frac{\pi}{6}\right)^{-1}$$
$$|z - u| \leq \frac{1}{2} \cdot \frac{2}{\sqrt{3}}$$
$$|z - u| \leq \frac{\sqrt{3}}{3}$$

(c) Prove that for any $a \in \mathbb{Z}[\omega]$ and $b \in \mathbb{Z}[\omega] \setminus \{0\}$, there are $q, r \in \mathbb{Z}[\omega]$ such that

$$a = bq + r$$
$$r = a - bq$$
$$r = b(\frac{a}{b} - q)$$
$$|r| \leq \frac{\sqrt{3}}{3}|b|$$

Consider $\frac{a}{b} \in \mathbb{Q}[\omega]$, by part **b** we know $\exists q \in \mathbb{Z}[\omega]$ such that $|\frac{a}{b} - q| \leq \frac{\sqrt{3}}{3}$.

$$\begin{aligned}
\left|\frac{a}{b} - q\right| &\leq \frac{\sqrt{3}}{3} \\
\left|b\left(\frac{a}{b} - q\right)\right| &\leq \frac{\sqrt{3}}{3}|b| \\
|r| &\leq \frac{\sqrt{3}}{3}|b|
\end{aligned}$$

(d) Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain

$$\begin{aligned}
\mathcal{N}(a) &= |a|^2 \\
|a|^2 &= 0 \Rightarrow a = 0 \\
|r| \leq \frac{\sqrt{3}}{3}|b| \Rightarrow |r|^2 &\leq \left|\frac{\sqrt{3}}{3}b\right|^2 \\
&\Rightarrow \mathcal{N}(r) \leq \mathcal{N}\left(\frac{\sqrt{3}}{3}b\right) \\
\left|\frac{\sqrt{3}}{3}\right|^2 &> 1 \Rightarrow \mathcal{N}(r) < \mathcal{N}(b)
\end{aligned}$$

Hence shown $\mathbb{Z}[\omega]$ is a Euclidean domain.

(e) Show that $\mathbb{Z}[\omega]$ is a PID.
By theorem, a Euclidean domain is a PID. Hence shown that $\mathbb{Z}[\omega]$ is a PID by part **d**.

5. Suppose $a, b \in \mathbb{Z}$ and $a^2 + ab + b^2 = p$ is a prime number > 3.

(a) Prove that $a - b\omega$ is irreducible in $\mathbb{Z}[\omega]$.
$a - b\omega \neq 0$, since $\mathbb{Z}[\omega]$ is a integral domain, $a - b\omega$ is not a zero divisor.
Assume $a - b\omega$ is a unit:

$$\begin{aligned}
(a - b\omega)(c + d\omega) &= 1 \\
|(a - b\omega)(c + d\omega)|^2 &= |1|^2 \\
(a - b\omega)(a - b\bar{\omega})(c + d\omega)(c + d\bar{\omega}) &= 1 \\
(a^2 - ab\bar{\omega} - ab\bar{\omega} + b^2\omega\bar{\omega})(c^2 + cd\bar{\omega} + cd\bar{\omega} + d^2\omega\bar{\omega}) &= 1 \\
(a^2 - ab(\bar{\omega} + \bar{\omega}) + b^2\omega\bar{\omega})(c^2 + cd(\bar{\omega} + \bar{\omega}) + d^2\omega\bar{\omega}) &= 1 \\
(a^2 + ab + b^2)(c^2 - cd + d^2) &= 1 \\
p(c^2 - cd + d^2) &= 1 \\
c^2 - cd + d^2 &= \frac{1}{p}
\end{aligned}$$

This is impossible since $c^2 - cd + d^2 \in \mathbb{Z}$. Hence $a - b\omega$ is not a unit.

$$\begin{aligned} a - b\omega &= (c + d\omega)(e + f\omega) \\ |a - b\omega|^2 &= |(c + d\omega)(e + f\omega)|^2 \\ a^2 + ab + b^2 &= (c^2 - cd + d^2)(e^2 - ef + f^2) = p \end{aligned}$$

Since this is set to equal a prime, $c^2 - cd + d^2$ or $e^2 - ef + f^2$ must be 1. Since absolute norm is just multplication by conjugate, we know that either $c + d\omega$ or $e + f\omega$ is in $\mathcal{U}(\mathbb{Z}[\omega])$.
Ergo $a - b\omega$ is irreducible in $\mathbb{Z}[\omega]$.

(b) Prove that $\exists \alpha \in \mathbb{Z}_p$ such that

(b-1) $\alpha^2 + \alpha + 1 = 0$ **in** $\mathbb{Z}_p$

$$a^2 + ab + b^2 = p$$
$$a^2 + ab + b^2 \overset{p}{\equiv} 0$$

Wants to show $b \neq 0$. Assume $b = 0$:

$$\begin{gathered} p \mid b \Rightarrow p \mid ab \Rightarrow p \mid a^2 \\ p^2 \mid b^2 \Rightarrow p^2 \mid ab \Rightarrow p^2 \mid a^2 \\ p^2 \mid a^2 + ab + b^2 \end{gathered}$$

This is a contradiction. Hence $b \neq 0$.

$$\begin{aligned} a^2 + ab + b^2 &\overset{p}{\equiv} 0 \\ \left(\frac{a}{b}\right)^2 + \frac{a}{b} + 1 &\overset{p}{\equiv} 0 \end{aligned}$$

Since $\mathbb{Z}_p$ is a field, $b \neq 0$, $\frac{a}{b} \in \mathbb{Z}_p$. Let $\alpha := \frac{a}{b}$. We have $\alpha^2 + \alpha + 1 \overset{p}{\equiv} 0$ as specified.

(b-2) $a - b\alpha = 0$ **in** $\mathbb{Z}_p$

$$\begin{aligned} \alpha &:= \frac{a}{b} \\ a - b\alpha &= a - b\frac{a}{b} \\ &= a - a = 0 \end{aligned}$$

$\alpha := \frac{a}{b}$ satisfies both conditions.

(c) Let $\phi : \mathbb{Z}[\omega] \mapsto \mathbb{Z}_p$, $\phi_\alpha(c + d\omega) := c + d\alpha$ where α is given in part **b**. Prove that ϕ is a ring homomorphism.

Closed under addition:

$$(c + d\alpha) + (e + f\alpha) = (c + e) + (d + f)(\alpha)$$

Closed under multiplication:

$$\begin{aligned}(c + d\alpha) \cdot (e + f\alpha) &= ce + (de + cf)\alpha + df\alpha^2 \\ &= ce + (de + cf + df\frac{a}{b})\alpha\end{aligned}$$

Hence shown ϕ is a ring homomorphism.

(d) Prove that $ker\ \phi = \langle a - b\omega \rangle$

$$\begin{gathered}\phi_\alpha(a - b\omega) = a - b\alpha = 0 \\ a - b\alpha \in ke\ \phi \Rightarrow \langle a - b\omega \rangle \subseteq ke\ \phi\end{gathered}$$

By part **5 a**, we know that $a - b\omega$ is irreducible in $\mathbb{Z}[\omega]$, since $\mathbb{Z}[\omega]$ is a PID, we know that $\langle a - b\omega \rangle$ is a maximal ideal, $\langle a - b\omega \rangle \subseteq ke\ \phi$ means that $ker\ \phi = \langle a - b\omega \rangle$.

(e) Prove that $\mathbb{Z}[\omega]/\langle a - b\omega \rangle \simeq \mathbb{Z}_p$
Show that ϕ is surjective: $\forall z \in \mathbb{Z}_p, \phi(z) = z$.
By part **5 d**, we know $ker\ \phi = \langle a - b\omega \rangle$. By part **5 c**, we know that ϕ is a ring homomorphism. By the 1^{st} isomorphism theorem, $\mathbb{Z}[\omega]/\langle a - b\omega \rangle \simeq \mathbb{Z}_p$.