

1. (a) Prove that  $\sqrt{-10}$  is irreducible in  $\mathbb{Z}[\sqrt{-10}] = \{a + \sqrt{-10}b \mid a, b \in \mathbb{Z}\}$

$$\begin{aligned}
 \sqrt{-10} &= (a + \sqrt{-10}b)(c + \sqrt{-10}d) \\
 10 &= (a^2 + 10b^2)(c^2 + 10d^2) \\
 a^2 + 10b^2 &\in \{1, 2, 5, 10\}
 \end{aligned}$$

If  $b \neq 0$ ,  $a^2 + 10b^2 \geq 10$ . This means that  $(c^2 + 10d^2) = 1$ , which implies  $(c + \sqrt{-10}d)(c - \sqrt{-10}d) = 1$ , and this shows that  $(c + \sqrt{-10}d) \in \mathbb{U}(\mathbb{Z}[\sqrt{-10}])$ . If  $b = 0$ ,  $a^2 + 10b^2 \in \{1, 2, 5, 10\} \Rightarrow a^2 = a = 1$  since 1 is the only perfect square option. This implies the following:

$$\begin{aligned}
 a^2 + 10b^2 &= 1 \\
 (a + \sqrt{-10}b)(a - \sqrt{-10}b) &= 1 \\
 a + \sqrt{-10}b &\in \mathbb{U}(\mathbb{Z}[\sqrt{-10}])
 \end{aligned}$$

Hence shown  $\sqrt{-10}$  is irreducible in  $\mathbb{Z}[\sqrt{-10}]$ .

- (b) Show that  $2 \times 5 \in \langle \sqrt{-10} \rangle$  and  $2 \notin \langle \sqrt{-10} \rangle$  and  $5 \notin \langle \sqrt{-10} \rangle$ .

$$2 \times 5 = 10 = -\sqrt{-10} \times \sqrt{-10} \in \langle \sqrt{-10} \rangle$$

Assume towards contradiction that  $2 \in \langle \sqrt{-10} \rangle$ .

$$\begin{aligned}
 2 &= \sqrt{-10} \cdot (a + b\sqrt{-10}) \\
 &= \sqrt{-10}a - 10b \\
 \Rightarrow a &= 0, \quad b = -\frac{1}{5}
 \end{aligned}$$

$b = -\frac{1}{5} \notin \mathbb{Z}$ , Contradiction!!

Assume towards contradiction that  $5 \in \langle \sqrt{-10} \rangle$ .

$$\begin{aligned}
 5 &= \sqrt{-10} \cdot (a + b\sqrt{-10}) \\
 &= \sqrt{-10}a - 10b \\
 \Rightarrow a &= 0, \quad b = -\frac{1}{2}
 \end{aligned}$$

$b = -\frac{1}{2} \notin \mathbb{Z}$ , Contradiction!!

Hence shown  $2 \times 5 \in \langle \sqrt{-10} \rangle$  and  $2 \notin \langle \sqrt{-10} \rangle$  and  $5 \notin \langle \sqrt{-10} \rangle$ .

- (c) Prove that  $\mathbb{Z}[-10]$  is not a PID.

*Proof.* Assume towards contrary that  $\mathbb{Z}[-10]$  is a PID. By part a, we have shown that  $\sqrt{-10}$  is irriducible. This means that  $\langle \sqrt{-10} \rangle$  is maximal therefore prime. By part b, we have shown that it is not prime. This means that the assumption is false,  $\mathbb{Z}[-10]$  is not a PID.  $\square$

2. We are told that  $p(x) = x^4 - 2x^3 + 2x^2 - 2x + 2$  is irreducible in  $\mathbb{Q}[x]$  and  $\alpha \in \mathbb{C}$  is a zero of  $p(x)$ . Let

$$\begin{aligned}\phi_\alpha : \mathbb{Q}[x] &\mapsto \mathbb{C} \\ \phi_\alpha(f(x)) &:= f(\alpha)\end{aligned}$$

We know that  $\phi_\alpha$  is a ring homomorphism.

- (a) Prove that  $\ker \phi_\alpha = \langle p(x) \rangle$   
 $\langle p(x) \rangle \subseteq \ker \phi_\alpha$  since  $\phi_\alpha(p(x)) = 0$ .  
 Since we know  $p(x)$  is irreducible in  $\mathbb{Q}[x]$ ,  $\langle p(x) \rangle$  is therefore a maximal ideal.  
 Since we have shown  $\langle p(x) \rangle \subseteq \ker \phi_\alpha \subsetneq \mathbb{Q}[x]$ , by definition of maimal idea,  $\ker \phi_\alpha = \langle p(x) \rangle$ .
- (b) Prove that  $\text{Im } \phi_\alpha = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$   
 First show that  $\{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\} \subseteq \text{Im } \phi_\alpha$ :

$$\phi_\alpha(c_0 + c_1x + c_2x^2 + c_3x^3) = c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3$$

Then show that  $\text{Im } \phi_\alpha \subseteq \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$ :

$$\begin{aligned}\forall f(x) \in \mathbb{Q}[x], \exists q(x), r(x) \in \mathbb{Q}[x] \\ f(x) &= q(x)p(x) + r(x) \\ \phi_\alpha(f) &= q(\alpha)p(\alpha) + r(\alpha) \\ \phi_\alpha(f) &= 0 + r(\alpha) \\ \phi_\alpha(f) &= c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3\end{aligned}$$

Hence shown  $\text{Im } \phi_\alpha = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$ .

- (c) Prove that  $\mathbb{Q}[x]/\langle p(x) \rangle \simeq \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$

By 1<sup>st</sup> isomorphism theorem,  $\mathbb{Q}[x]/\ker \phi_\alpha \simeq \text{Im } \phi_\alpha$ . By part a, we have shown that  $\ker \phi_\alpha = \langle p(x) \rangle$ . By part b, we have shown that  $\text{Im } \phi_\alpha = \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$ . By subsituting the corresponding parts we obtain the following:

$$\mathbb{Q}[x]/\langle p(x) \rangle \simeq \{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$$

- (d) Prove that  $\{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$  is a field. We know that  $p(x)$  is irreducible, therefore  $\langle p(x) \rangle$  is a maximal ideal. This means that  $\mathbb{Q}[x]/\langle p(x) \rangle$  is a field. By isomorphism established in part c, we have  $\{c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 \mid c_0, c_1, c_2, c_3 \in \mathbb{Q}\}$  is a field.

3. We are told that  $R = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$  is a unital commutative ring. Let  $\phi : R \mapsto$

$$\mathbb{Z}, \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) = a - b$$

(a) Prove that  $\phi$  is a ring homomorphism.

**Addition:**

$$\begin{aligned} \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} + \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) &= \phi \left( \begin{bmatrix} a+c & b+d \\ b+d & a+c \end{bmatrix} \right) \\ &= (a+c) - (b+d) \\ &= (a-b) + (c-d) \\ &= \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) + \phi \left( \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) \end{aligned}$$

**Multiplication:**

$$\begin{aligned} \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) &= \phi \left( \begin{bmatrix} ac+bd & ad+bc \\ bc+ad & bd+ac \end{bmatrix} \right) \\ &= \phi \left( \begin{bmatrix} ac+bd & ad+bc \\ ad+bc & ac+bd \end{bmatrix} \right) \\ &= (ac+bd) - (ad+bc) \\ &= ac - ad - bc + bd \\ &= (a-b)(c-d) \\ &= \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) \phi \left( \begin{bmatrix} c & d \\ d & c \end{bmatrix} \right) \end{aligned}$$

Hence shown  $\phi$  is a ring homomorphism.

(b) Find  $\ker \phi$ .

$$\begin{aligned} \phi \left( \begin{bmatrix} a & b \\ b & a \end{bmatrix} \right) &= a - b = 0 \\ a &= b \\ \ker \phi &= \left\{ \begin{bmatrix} a & a \\ a & a \end{bmatrix} \mid a \in \mathbb{Z} \right\} \end{aligned}$$

(c) Prove that  $R/\ker \phi \simeq \mathbb{Z}$

By 1<sup>st</sup> isomorphism theorem, showing that  $\phi : R \mapsto \mathbb{Z}$  is surjective completes the isomorphism proof.

$$\forall z \in \mathbb{Z}, \phi \left( \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} \right) = z - 0 = z$$

By 1<sup>st</sup> isomorphism theorem,  $R/\ker \phi \simeq \mathbb{Z}$ .

(d) Is  $\ker \phi$  a prime ideal?  
Yes, since  $\mathbb{Z}$  is a integral domain.

(e) Is  $\ker \phi$  a maximal ideal?  
No, since  $\mathbb{Z}$  is not a field.

4. (a) Show that  $x^2 - 5 = 0$  has no zero in  $\mathbb{Q}[\sqrt{2}]$ .  
Suppose towards contrary that  $\exists \alpha \in \mathbb{Q}[\sqrt{2}]$  such that  $m_\alpha(x) = x^2 - 5 \in \mathbb{Q}[x]$ .

$$\begin{aligned}\alpha &= a + b\sqrt{2} \\ \phi_\alpha(m_\alpha) &= (a + b\sqrt{2})^2 - 5 = 0 \\ 0 &= a^2 + 2ab\sqrt{2} + 2b^2 - 5 \\ ab &= 0 \\ a^2 + 2b^2 &= 5\end{aligned}$$

Since  $\mathbb{Q}[\sqrt{2}]$  is a subring of  $\mathbb{C}$ , it is an integral domain hence contain no zero divisors. This means either  $a$  or  $b$  must be 0.

**Case  $a = 0$ :**

$$\begin{aligned}2b^2 &= 5 \\ b &= \sqrt{\frac{5}{2}}\end{aligned}$$

Since  $b \in \mathbb{Q}$ , this is impossible.

**Case  $b = 0$ :**

$$\begin{aligned}a^2 &= 5 \\ a &= \sqrt{5}\end{aligned}$$

Since  $a \in \mathbb{Q}$ , this is impossible.

Hence shown  $x^2 - 5 = 0$  has no zero in  $\mathbb{Q}[\sqrt{2}]$ .

- (b) Prove that  $\mathbb{Q}[\sqrt{2}] \not\simeq \mathbb{Q}[\sqrt{5}]$ .  
Suppose that  $\phi : \mathbb{Q}[\sqrt{2}] \mapsto \mathbb{Q}[\sqrt{5}]$  is an isomorphism.

$$\begin{aligned}\phi(1) &= 1 \\ \phi(a) &= a, \forall a \in \mathbb{Q} \\ \phi(2) &= \phi(\sqrt{2}^2) \\ 2 &= \phi(\sqrt{2})^2 \\ 2 &= (a + b\sqrt{5})^2 \\ 2 &= a^2 + 2ab\sqrt{5} + 5b^2 \\ ab &= 0 \\ a^2 + 5b^2 &= 2\end{aligned}$$

Since  $\mathbb{Q}[\sqrt{5}]$  is a subring of  $\mathbb{C}$ , it is an integral domain hence contain no zero divisors. Either  $a$  or  $b$  must be 0. If  $a = 0$ :

$$5b^2 = 2$$

$$b = \sqrt{\frac{2}{5}}$$

This is a contradiction since  $b \in \mathbb{Q}$ . If  $b = 0$ :

$$a^2 = 2$$

$$a = \sqrt{2}$$

This is a contradiction since  $a \in \mathbb{Q}$ .

Hence shown such an isomorphic mapping does not exist,  $\mathbb{Q}[\sqrt{2}] \not\cong \mathbb{Q}[\sqrt{5}]$ .

5. (a) Suppose  $p$  is an odd prime, and there is  $a \in \mathbb{Z}_p$  such that  $a^2 = -1$  in  $\mathbb{Z}_p$ . Prove that the multiplicative order of  $a$  is 4.

$$a^2 \stackrel{p}{\equiv} -1$$

$$a^2 \stackrel{p}{\equiv} p - 1$$

$$(a^2)^2 \stackrel{p}{\equiv} (p - 1)^2$$

$$a^4 \stackrel{p}{\equiv} p^2 - 2p + 1$$

$$a^4 \stackrel{p}{\equiv} 1$$

We know  $a \neq 1$  since  $a^2 = -1$  which also tells us  $a^2 \neq 1$ .  $a^3 \neq 1$  because as shown above,  $a^4 = 1$ ,  $a^3 = 1$  implies that  $a = 1$  which is a contradiction.

Hence shown the multiplicative order of  $a$  is 4.

- (b) Use Lagrange's theorem to deduce: if  $p$  is a prime and  $p \stackrel{4}{\equiv} 3$ , then there is no  $a \in \mathbb{Z}_p$  such that  $a^2 = -1$ .

First we examine the unit of  $\mathbb{Z}_p$ ,  $\mathcal{U}(\mathbb{Z}_p) = \mathbb{Z}_p \setminus \{0\}$ . The order of  $\mathcal{U}(\mathbb{Z}_p)$  is  $p - 1$ . A subgroup of this unit would be one generated by  $a$  with multiplication,  $\langle a \rangle = \{a^n \mid n \in [0, 3]\}$ . Order of  $\langle a \rangle$  is 4. By Lagrange's theorem, 4 divides  $p-1$ :

$$4 \mid p - 1$$

$$p - 1 \stackrel{4}{\equiv} 0$$

$$p \stackrel{4}{\equiv} 1$$

Hence shown if  $p \stackrel{4}{\equiv} 3$ , then there is no  $a \in \mathbb{Z}_p$  such that  $a^2 = -1$

- (c) Suppose  $p$  is a prime and  $p \stackrel{4}{\equiv} 3$ . Prove that  $p$  is irreducible in  $\mathbb{Z}[i]$ .  $p \neq 0$  and  $p$  has no multiplicative inverse in  $\mathbb{Z}[i]$ , hence not a unit.

$$p = (a + bi)(c + di)$$

$$|p|^2 = |a + bi|^2 |c + di|^2$$

$$p^2 = (a^2 + b^2)(c^2 + d^2)$$

This means  $(a^2 + b^2)$  must be either 1,  $p$ ,  $p^2$ .

**Case**  $(a^2 + b^2) = 1$ :

$$\begin{aligned}(a^2 + b^2) &= 1 \\ (a + bi)(a - bi) &= 1\end{aligned}$$

Hence shown  $(a + bi)$  is a unit.

**Case**  $(a^2 + b^2) = p^2 \Rightarrow (c^2 + d^2) = 1$ :

$$\begin{aligned}(c^2 + d^2) &= 1 \\ (c + di)(c - di) &= 1\end{aligned}$$

This means that  $(c + di)$  is a unit.

**Case**  $(a^2 + b^2) = p$ :

$$(a^2 + b^2) \equiv 0$$

We know that  $b \neq 0$  since that would imply  $a^2 = p$  which is impossible since  $p$  is prime.

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

Since  $\mathbb{Z}_p$  is a field therefore  $b \neq 0 \Rightarrow b^{-1} \in \mathbb{Z}_p \Rightarrow \frac{a}{b} \in \mathbb{Z}_p$ . Hence by part b, we know that this is impossible. By contradiction, we have shown that  $p$  is irreducible in  $\mathbb{Z}[i]$ .

- (d) Use part (c) to show  $\mathbb{Z}[i]/\langle p \rangle$  is a field if  $p$  is a prime if  $p$  is a prime and  $p \not\equiv 3 \pmod{4}$ .

Since we know if  $p$  is a prime and  $p \not\equiv 3 \pmod{4}$ ,  $p$  is irreducible in  $\mathbb{Z}[i]$ . This means  $\langle p \rangle$  is a maximal ideal of  $\mathbb{Z}[i]$ . The factor ring of  $\mathbb{Z}[i]$  over its maximal ideal,  $\mathbb{Z}[i]/\langle p \rangle$  is therefore a field by lemma proven in class.