1. Prove the irreducible elements in $\mathbb{Z}[i]$ has and only has the following 3 forms:

(1). $1+i$ (2) $a+bi$, $a^2+b^2=p\equiv 1 \mod 4$ (3) $p\equiv 3 \mod 4$

$\mathbb{Z}[i]$ is a ED, so PID

sps prime ideal in $\mathbb{Z}[i]$ is (α)

Step 1°. show $(\alpha)\cap\mathbb{Z}$ is ideal in $\mathbb{Z}$

$\forall r\in\mathbb{Z}$, then

(i) $\forall x\in(\alpha)\cap\mathbb{Z}$, $rx\in\mathbb{Z}$

(ii) view $x\in(\alpha)\triangleleft\mathbb{Z}[i]$, $r\in\mathbb{Z}[i]$ then $rx\in(\alpha)$

from (i), (ii), $rx\in(\alpha)\cap\mathbb{Z}$

Addition is closed since we can view (α) and $\mathbb{Z}$ as subring of $\mathbb{Z}[i]$, so $(\alpha)\cap\mathbb{Z}$ also subring.

and all elements in $(\alpha)\cap\mathbb{Z}$ are integers

so $(\alpha)\cap\mathbb{Z}$ is a subring in $\mathbb{Z}$

Step 2°. show $(\alpha)\cap\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$

sps for some $a.b\in\mathbb{Z}$. $ab\in(\alpha)\cap\mathbb{Z}$

then view $a.b$ as elements in $\mathbb{Z}[i]$.

we have $a\in(\alpha)$ or $b\in(\alpha)$. WLOG, $a\in(\alpha)$

and don't forget we pick a from $\mathbb{Z}$

so $a \in (\alpha) \cap \mathbb{Z}$. done.

Step 3: Now we denote $(\alpha) \cap \mathbb{Z}$ as (p) in $\mathbb{Z}$

since $p \in (\alpha)$ we have $\alpha \mid p$

and $\bar{\alpha} \mid \bar{p}$ shows $\bar{\alpha} \mid p$

we disscuss p by mod 4

there are 3 conditions: $p=2$, $p \equiv 1 \bmod 4$ $p \equiv 3 \bmod 4$

Condition 1 $p=2$

$2=(1+i)(1-i)$

$1+i$ is irreducible since if we take norm as

$N(a+bi)=a^2+b^2$, $\forall r,s \in \mathbb{Z}[i]$ $N(rs)=N(r)N(s)$

and if $N(r)=1$ then we already know $r \in \{\pm 1, \pm i\}$ which is unit.

i.e. if $1+i=rs$ then one of r and s is unit

so $1+i$ is irreducible.

and $1-i=-i(1+i)$ shows they are associate.

Condition 2 $p \equiv 1 \bmod 4$

By last homework we know $\exists\, a,b \in \mathbb{Z}$ s.t. $a^2+b^2=p$

i.e $p=(a+bi)(a-bi)$ under such a,b

Now we claim $a+bi$ is irreducible in $\mathbb{Z}[i]$

sps $a+bi$ is reducible, i.e $\exists\ c_1, d_1, c_2, d_2 \in \mathbb{Z}$ s.t

$$a+bi = (c_1+d_1 i)(c_2+d_2 i)$$

then $p = (a+bi)(a-bi) = (a+bi)\overline{(a+bi)} = (c_1+d_1 i)(c_2+d_2 i)\overline{(c_1+d_1 i)(c_2+d_2 i)}$

$$= (c_1+d_1 i)(c_1-d_1 i)(c_2+d_2 i)(c_2-d_2 i) = (c_1^2+d_1^2)(c_2^2+d_2^2)$$

Contradiction to p is prime.

<u>Condition 3</u> if $p \equiv 3 \mod 4$. claim p is irreducible in $\mathbb{Z}[i]$

Sps p is reducible

then $\exists\ a+bi \mid p$ where $b \neq 0$ since p is prime integer.

By we discussed before. $a-bi \mid p$

$$\Rightarrow \quad (a+bi)(a-bi) = a^2+b^2 \mid p \Rightarrow a^2+b^2 = p.$$

take mod 4, for a square number of integer

only has residue 0 and 1

i.e $a^2+b^2 = p \equiv 3 \mod 4$ is impossible

So $p \equiv 3 \mod 4$ is irreducible in $\mathbb{Z}[i]$.

2. Let R be UFD, $K = \text{frac}(R)$. $f(x) \in R[x]$, monic

if $g(x) \in K[x]$ s.t $g(x)$ monic and $g \mid f$. prove $g \in R[x]$

Since R UFD, we have $R[x]$ UFD

So we can decomposite $f(x)$ into

$f(x) = u\,p_1(x)\cdots p_t(x)$ where $p_1 \cdots p_t$ are irreducible over $R[x]$

Since $f(x)$ monic, it shows we can set $p_1 \cdots p_t$ monic and $u=1$

$\forall p_i$, p_i irred. monic over $R[x]$

By Gauss Lemma, p_i irred. monic over $k[x]$. Since $g(x)$ monic

if $g(x) \mid f(x)$ over k, it show $g(x)$ is a product of several $p_i(x)$

So $g(x) \in R[x]$

3. Pro Eisenstein Criterion:

Suppose f reducible in $R[x]$

Let $f = (b_t x^t + \cdots + b_0)(C_s x^s + \cdots + C_0)$ $b_i, C_j \in R$. $s, t > 0$
$s+t = \deg f$

So $a_r = \sum_{i+j=r} b_i C_j$ ($\forall r = 0, \ldots n$)

$\because p \mid a_0$, $p^2 \nmid a_0$. WLOG. let $p \nmid b_0$. $p \mid C_0$

since $p \nmid a_n$, we have $p \nmid C_s$

Now find $p \nmid C_k$ but $p \mid C_0, C_1 \ldots C_{k-1}$ for some k.

Consider $a_k = C_k b_0 + C_{k-1} b_1 + \cdots + C_0 b_k$

then $p \mid a_k$ but $p \mid C_{k-1} b_1, \ldots, C_0 b_k$. $p \nmid C_k b_0$ Contradiction!

So $f(x)$ is irreducible in $R[x]$

By Gauss Lemma, $f(x)$ is irreducible in $F[x]$

(2) (i). $x^{p-1}+\cdots+1$.

Step 1. We prove $f(x)$ irreducible $\Leftrightarrow$ $f(x+r)$ irreducible.

$\forall r\in R$, this is trivial since.

$$f(x)=g(x)h(x) \Leftrightarrow f(x+r)=g(x+r)h(x+r)$$

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

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

pt 1, $p\mid a_{p-2}$. $p^2\nmid p$

1°. If $p=2$, $x+1$ irre in $\mathbb{Q}(i)[x]$

2°. if $p\equiv 3 \mod 4$. p is irreducible in $\mathbb{Z}[i]$

Notice that $\mathbb{Q}(i)=\mathrm{frac}(\mathbb{Z}[i])$

By Eissenstein criterion. $f(x)$ is irreducible.

3°. if $p\equiv 1 \mod 4$. Sps $p=(a+bi)(a-bi)$

then $a+bi$ irre. in $\mathbb{Z}[i]$

use $a+bi$ check $f(x)$ by Eisenstein Criterion.

Also, $f(x)$ is irre in $\mathbb{Z}[i][x]$, irre in $\mathbb{Q}(i)[x]$.

(ii) $x^4+(8+i)x^3+(3-4i)x+5$

Notice that $1+2i$ irre in $\mathbb{Z}[i]$

$1+2i \nmid 1 \quad 1+2i \mid 8+i \quad 1+2i \mid 3-4i$

$1+2i \mid 5$ and $(1+2i)^2 \nmid 5 \Rightarrow$ irr.

4. $E \cup F$ is field iff $E \subseteq F$ or $F \subseteq E$

($\Leftarrow$). $E \subseteq F$ then $E \cup F = F$

($\Rightarrow$) if $E \nsubseteq F$ and $F \nsubseteq E$, take $a \in E - F$ and $b \in F - E$

then $a+b \notin E$ and $a+b \notin F \Rightarrow a+b \notin E \cup F$

contradict to $E \cup F$ is a field.

5. (1), Prove $Aut(\mathbb{Q}) = \{id\}$.

Let $\sigma \in Aut(\mathbb{Q})$, then $\sigma(1) = 1$

so $\sigma(n) = n, \ \forall n \in \mathbb{Z}$

So $\sigma(\frac{1}{m}) = \frac{1}{m}, \ \forall m \in \mathbb{Z}$

So $\sigma(\frac{m}{n}) = \frac{m}{n}, \ \forall, m, n \in \mathbb{Z}$, i.e $\forall r \in \mathbb{Q}, \sigma(r) = r$

i.e $\sigma = id$.

(2). Give all field embedding: $\sigma: \mathbb{Q}(i) \longrightarrow \mathbb{C}$

$\sigma(1) = 1$

Since $\sigma(\mathbb{Q})$ is a copy of $\mathbb{Q}$ in $\mathbb{C}$

and $\forall a+bi \in \mathbb{Q}(i)$ $\quad \sigma(a+bi) = \sigma(a) + \sigma(b)\sigma(i)$

$= a + b\sigma(i)$

So only need to identify $\sigma(i)$

$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1 \Rightarrow \sigma(i) = \pm i$

Thus. there a two embedding

① $\mathbb{Q}(i) \longrightarrow \mathbb{C}$ ② $\mathbb{Q}(i) \longrightarrow \mathbb{C}$

$i \longmapsto i$ $i \longmapsto -i$

(3). prove no embedding from $\mathbb{Q}(i)$ to $\mathbb{Q}(\sqrt{2})$

if $\exists\, \sigma$ s.t $\sigma: \mathbb{Q}(i) \to \mathbb{Q}(\sqrt{2})$ field embedding.

$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -\sigma(1) = -1$

but in $\mathbb{Q}(\sqrt{2})$, the square root of -1 does not exist.

6. prove $i: k(\alpha) \to k(\alpha)$ Infinitely many.

take $\sigma_n: k(\alpha) \longmapsto k(\alpha)$

$\alpha \longmapsto \alpha^n$ $n = 1, 2, \cdots$

7. (1). $x^2 - 2ax + a^2 + b^2 = 0$

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

8. $[k:F] = p$. $\alpha \in k - F$ the $k = F(\alpha)$

Consider $k \supseteq F(\alpha) \supseteq F$

$[k:F] = [k:F(\alpha)][F(\alpha):F]$

9. (1). 1, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{6}$

(2). 1, i, $\sqrt{3}$, $\sqrt{3}i$

(3). 1. $e^{\frac{2\pi i}{p}}$, $e^{\frac{4\pi i}{p}}$, $\cdots$, $e^{\frac{(2p-4)\pi i}{p}}$

P. Let σ be a F-endo. of K

then $\sigma(F) = F \Rightarrow \sigma \neq 0$

and all field homo. are mono. so $\ker \sigma = 0$

K/F is finite $\Rightarrow K$ is finite dimensional vector space over F.

σ is also a linear endo. of K as F-vector space.

Since $\dim_F K < \infty$, σ mono $\Rightarrow \sigma$ epi

$\Rightarrow \sigma$ is iso.