1. (1). Integral closure of $\mathbb{Z}$ in $\mathbb{C}$

(2). If R is a UFD

$\forall a,b \in R$, sps. $a = u p_1^{e_1} \cdots p_t^{e_t}$ $b = v p_1^{f_1} \cdots p_t^{f_t}$

where $e_i, f_i \geq 0$, $u, v \in U(R)$, p_i are primes

claim. $d = \prod_{i=1}^{t} p_i^{\min\{e_i, f_i\}}$ is the gcd of a, b

1°. $d \mid a$ and $d \mid b$

2°. if for some $g \in R$ s.t $g \mid a$ and $g \mid b$

then we can write g into $g = w \cdot p_1^{h_1} \cdots p_t^{h_t}$

where $w \in U(R)$ and $h_i \leq \min\{e_i, f_i\}$

i.e $g \mid d$

from 1°, 2°, d is the GCD of a and b.

If $\forall a, b \in R$, $\gcd(a,b)$ exists. Since R satisfies chain condition. only need to prove R satisfies prime condition.

i.e. if p is irreducible element in R. then p is a prime.

Now take $p \in R$ s.t p is irreducible.

we need to prove. $\forall a, b \in R$. if $p \mid ab$ then $p \mid a$ or $p \mid b$

Now given $p \mid ab$

1°. if $(p, a) = p$, then $p \mid a$

2°. if $(p, a) \neq p$, then $(p, a) = 1$. since p is irreducible.

Sps $(pb, ab) = d$. then $b \mid d$

Let $d = ub$ since $d \mid pb$, $\exists\, g \in R$ s.t

$pb = gd$ i.e $pb = gub \Rightarrow p = gu$

Similarly, $\exists\, f \in R$ s.t $fd = ab \Rightarrow a = fu$

$(a, p) = 1$, $u \mid a$ and $u \mid p \Rightarrow u$ is a unit

$\Rightarrow (pb, ab) = b$ since $p \mid pb$, $p \mid ab \Rightarrow p \mid b$ □

2. (1). To prove $S^{-1}R$ is a UFD. we need to prove $S^{-1}R$

satisfies: it is a ID and

1° Chain condition 2° prime condition.

The refrence anwers is too omited. To solve this question

we need some claim:

Construction: Let S be the multiplicatively closed set

and since R is a UFD, $\forall\, a \in S$. $a = up_1^{e_1} \cdots p_t^{e_t}$

Let T be the set of all such p_i, i.e

Let T be the set of all irreducibles that divide an element in S.

and let M be the set of all irreducibles that not in T

claim 1: $p \in T$ iff $(p,1)$ in $S^{-1}R$ is a unit.

proof: $p \in T \Rightarrow \exists\, s \in S$ s.t $p \mid s$

$\Rightarrow \exists\, x \in R$ s.t $px = s \cdot 1$

$$\Rightarrow \quad \frac{p}{1} \cdot \frac{x}{s} = \frac{px}{s} = \frac{px}{px} = 1 \in S^{-1}R$$

So $(p,1)$ is a unit in $S^{-1}R$

If $(p,1)$ is a unit in $S^{-1}R$

then $\exists\, t \in S$ and $y \in R$ s.t $\frac{p}{1} \cdot \frac{y}{t} = 1 \in S^{-1}R$

i.e: $py = t$ in R it shows $p \mid t$ where $t \in S$

So $p \in T$.

claim 2: $p \in M$ then $(p,1)$ is irreducible in $S^{-1}R$

We proof by contradiction.

Sps. $\frac{p}{1} = \frac{xy}{ss'} = \frac{x}{s} \cdot \frac{y}{s'}$ in $S^{-1}R$

then $pss' = xy$ in R, i.e $p \mid xy$.

since R is UFD, p irreducible. $\Rightarrow$ p prime

$\Rightarrow$ $p \mid x$ or $p \mid y$

Since $p \notin T$, $p \nmid ss'$

it shows p appears once in the irre. decomp. in xy

i.e. $p \mid x$ or $p \mid y$ but $p \nmid (x, y)$

i.e. x or y in S

i.e. $\frac{x}{s}$ or $\frac{y}{s'}$ is a unit in $S^{-1}R$

$\Rightarrow$ $(p, 1)$ is irreducible.

claim 3.

if (p, s) irre in $S^{-1}R$

then p irre in R

proof: if ~~not~~

suppose $p = p_1 p_2$, $p_1, p_2 \notin U(R)$

then $\frac{p}{s} = \frac{p_1}{s} \frac{p_2 s}{s}$

Since $\frac{p}{s}$ irre, not unit

$\Rightarrow$ $p \in M$ by claim 1

$\Rightarrow$ $p_1, p_2 \neq S$

$\Rightarrow$ $\frac{p_1}{s}$, $\frac{p_2 s}{s}$ not unit in $S^{-1}R$ $\lightning$.

Step 1: Since $\forall$ (x, s) and (y, s')

$$\frac{x}{s} \cdot \frac{y}{s'} = \frac{xy}{ss'} = \frac{yx}{s's} = \frac{y}{s'} \cdot \frac{x}{s}$$

and $\frac{x}{s} \frac{y}{s'} = 0$ iff either x or $y = 0$

so $S^{-1}R$ is a ID

Step 2: $\forall$ $(x, s) \in S^{-1}R$, $x = u p_1^{e_1} \cdots p_t^{e_t}$

then $$\frac{x}{s} = \frac{u}{s} \cdot \underbrace{\left(\frac{p_1}{1}\right)^{e_1} \cdots \cdots \left(\frac{p_t}{1}\right)^{e_t}}_{}$$

some are units, some are irreducibles

it shows $S^{-1}R$ satisfies factor chain condition.

Step 3. $\forall$ irreducible element (p, s) in $S^{-1}R$

by claim 3. p irre. in R and $p \in M$

so if $(p, s) \mid (x, s_1)(y, s_2)$

it shows $\exists\ \frac{r}{t}$ s.t $\frac{p}{s} \cdot \frac{r}{t} = \frac{x}{s_1} \cdot \frac{y}{s_2}$

i.e $p r s_1 s_2 = s t x y$ $p \in M$, $s, t \in S$

then $p \mid xy \Rightarrow p \mid x$ or $p \mid y$

WLOG. Let $p \mid x$, $\exists\ x' \in R$ s.t $x' p = x$

$$\Rightarrow \frac{x}{s_1} = \frac{x' p}{s_1} = \frac{x' p s}{s_1 s} = \frac{p}{s} \cdot \frac{x' s}{s_1}$$

i.e $(p, s) \mid (x, s_1)$

i.e if $p \mid x$, $(p, s) \mid (x, s_1)$; if $p \mid y$, $(p, s) \mid (y, s_2)$ $\Rightarrow (p, s)$ is prime in $S^{-1}R$.

Therefore. $S^{-1}R$ also satisfies prime condition.

I must say, this is not "hard", just a bit tedious.

Remember, "check by definition" is trivial work.

(2). $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, regard it as subring of $\mathbb{C}$

where $\mathbb{C}$ is a field, $\mathbb{C}$ is a UFD.

(3). take $\mathbb{Z}[x]$ as a UFD and (x^2+5) is its prime ideal.

$\mathbb{Z}[x]/(x^2+5) \cong \mathbb{Z}[\sqrt{-5}]$ shows $\mathbb{Z}[x]/(x^2+5)$ is not UFD.

3. (1). Let $n \in \mathbb{Z}$, $f \in \mathbb{Z}[x]$, $\deg f \geq 1$

$\mathbb{Z}[x]/(n) = \mathbb{Z}_n[x]$, not field $\Rightarrow$ (n) not maximal.

if constant of f is 0, $(f) \subset (x) \subset (2, x)$, not maximal.

if constant of f is not 0, $(f) \subset (p, f)$ for some prime p.

not maximal.

(2). Let p be prime in R. R is PID

Sps $(p) \subseteq (m) \subseteq R$

$\Rightarrow p \in (m) \Rightarrow \exists r \in R \quad p = mr$

Since p prime, $p \mid m$ or $p \mid r$

if $p \mid m$, $(p) = (m)$

if $p \mid r$, m is a unit $\Rightarrow (m) = R$

$\Rightarrow (p)$ is maximal.

$\Leftarrow$

4. (1). if $a_0 = 0$, $\forall g \in k[[x]]$

$\deg fg \geq 1 \Rightarrow f$ is not invertible.

$\Leftarrow$ if $a_0 \neq 0$

set $f^{-1} = a_0^{-1}\left(1 + \sum_{j=1}^{\infty}\left(-\sum_{i=1}^{\infty} \frac{a_i}{a_0} x^i\right)^j\right) \in k[[x]]$

then you can check $f f^{-1} = 1 \Rightarrow f$ invertible.

(2). If $I \trianglelefteq k[[x]]$

1° if $\exists f \in I$ s.t $a_0 \neq 0$, then $I = (1)$

2° if $\forall f \in I$ s.t $a_0 = 0$

then take $N = \min\{\deg f \mid f \in I\}$

$I = (x^N)$

5. if $(a.b) = (d)$ then $(a) \subseteq (d)$, $(b) \subseteq (d)$

i.e. $d \mid a$ and $d \mid b$

sps $\exists f$ s.t $f \mid a$ and $f \mid b$

then $(d) = (a, b) \subseteq (f)$

it shows $f \mid d$. so d is the greatest common divisor.

if d is the greatest common divisor.

since R is PID, $\exists r \in R$

s.t $(a, b) = (r) \subseteq (d)$ i.e $d \mid r$, but d is the

greatest common divisor it forces.

$r \mid d$, i.e $(r)=(d)$

6. Why we can use Bezout's Thm?

Lemma: Let R be a PID.

$d = \gcd(a,b) \iff \exists\, x, y \in R$ s.t $ax+by=d$.

$\Leftarrow$ trivial.

$\Rightarrow$ check by youself !

Now, in R $d = \gcd(a,b)$

$\Rightarrow \exists\, x, y \in R$, $ax+by=d$. and $R \subseteq D$

regard a, b, x, y, d as elements in D

i.e $\exists\, x, y \in D$. $ax+by=d$

by our lemma, $d=\gcd(a,b)$ in D.

7. Since $[K:\mathbb{Q}]=2$.

$\forall\, \alpha \in K$, $Irr(\alpha) \in \mathbb{Q}[x]$ s.t $\deg(Irr(\alpha))=2$.

i.e. take any $\beta \in \mathcal{O}_K$. $\deg(Irr(\beta))=2$ and

$Irr(\beta)$ is monic, integer coefficients poly.

Construct

$(x-a-b\sqrt{d})(x-a+b\sqrt{d})$

$= x^2-2ax+a^2-b^2d \in \mathbb{Z}[x]$

i.e. $\{a+b\sqrt{d} \mid a,b\in\mathbb{Z}\} \subseteq \mathcal{O}_K$

similarly if $d\equiv 1 \mod 4$ also you have

$\{a+b\frac{1+\sqrt{d}}{2} \mid a,b\in\mathbb{Z}\} \subseteq \mathcal{O}_K$.

Now for the other direction:

take $\alpha = a+b\sqrt{d}$ with $a,b\in\mathbb{Q}$ and sps α is a algebraic integer.

1° if $b=0$ $\alpha = a\in\mathbb{Q}$

and α is a root of monic integer coefficient ploynomial.

it shows $a\in\mathbb{Z}$.

2°. If $b\neq 0$, α is root of $x^2-2ax+(a^2-b^2d)$

$\Rightarrow$ $2a$ and $a^2-b^2d\in\mathbb{Z}$.

$\Rightarrow$ $4a^2-4b^2d\in\mathbb{Z}$

$\Rightarrow$ $4b^2d\in\mathbb{Z}$

$\Rightarrow$ $2b\in\mathbb{Z}$

$\Rightarrow$ $(2a)^2-(2b)^2d\equiv 0 \mod 4$

since $(2a)^2, (2b)^2 \mod 4$ only 0 and 1.

(i). $d \equiv 2, 3 \mod 4$, $\Rightarrow (2a)^2, (2b)^2 \equiv 0 \mod 4$

$\Rightarrow a, b \in \mathbb{Z}$

(2). $d \equiv 1 \mod 4$

$(2a)^2, (2b)^2 \equiv 0 \mod 4$, $a, b \in \mathbb{Z}$

or. $(2a)^2, (2b)^2 \equiv 1 \mod 4$

i.e. α is of the form. $a + b\frac{1+\sqrt{d}}{2}$ where $a, b \in \mathbb{Z}$.

8. (1). take norm. $a^2 + 3b^2$

(2). take norm. $|a^2 - 2b^2|$

(3). take $w = \frac{1+\sqrt{5}}{2}$, $v = \frac{1-\sqrt{5}}{2}$

take norm $|(a+bw)(a+bv)|$

9. take norm. a^2+b^2

if $r \in R$ invertible.

$\|r\| \leq 1$ only $\{\pm 1, \pm i\}$.

10. this is number theory problem.