HW 2

① (a). $f = \sum_{n=0}^{\infty} a_n X^n \in R[\![X]\!]$ invertible

$\Leftrightarrow$ $a_0 \in R^\times$ for any commutative ring $R^\times$

if $d(f) < d(g)$ then $f = 0 \cdot g + f$.

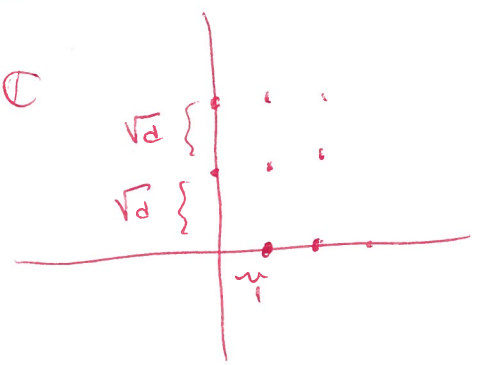
else if $d(f) \geq d(g)$ then $f = X^{d(f)} \cdot f_1$

$g = X^{d(g)} g_1$

$d(f_1) = d(g_1) = 0$ so $f_1, g_1 \in K[\![X]\!]^\times$

and so $f = X^{d(f)-d(g)} \underbrace{f_1 g_1^{-1}}_{\in K[\![X]\!]^\times} + 0.$

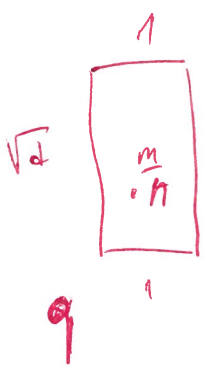
(b) $\mathbb{Z}[\sqrt{d}] \subset \mathbb{C}$ looks like



$m, n \in \mathbb{Z}[\sqrt{d}]$

$\frac{m}{n} \in \mathbb{Q}(\sqrt{d})$

let $q \in \mathbb{Z}[\sqrt{d}]$ closest to $\frac{m}{n}$



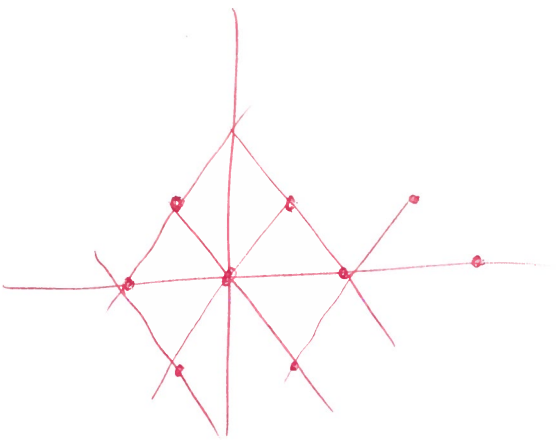
$\left|\frac{m}{n} - q\right| \leq \frac{\text{diagonal}}{2} = \frac{\sqrt{d+1}}{2} \leq \frac{\sqrt{3}}{2} < 1$

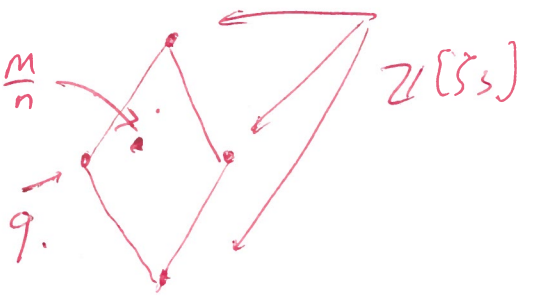
so $\frac{|m - nq|}{|n|} < 1$ so $|m - nq| < |n|$

$r = m - nq$ then has $d(r) = |r|^2 < |n|^2 = d(n)$

□.

(c) Same as (b) $\mathbb{Z}[\zeta_5] \subset \mathbb{C}$





$\left|\frac{m}{n} - q\right| < 1$ and again $d(r) = |r|^2$

$= |m - nq|^2 < |n|^2 = d(n)$

□.

(2) (a) by UF $p_i^n \neq p_i^{n+1}$ $\forall n$

choose $\alpha_i \in p_i^{e_i} - p_i^{e_i+1}$

by CRT $\exists$ $x \in R$ $x \equiv \alpha_i \pmod{p_i^{e_i}}$

$\Rightarrow$ $x \in p_i^{e_i} - p_i^{e_i+1}$ $\Rightarrow$ $v_{p_i}(x) = e_i$

(b) $I \subset R$ ideal $I = \prod p_i^{e_i}$

let x st $v_{p_i}(x) = e_i$ $\Rightarrow$ $(x) \in p_i^{e_i}$ $\forall i$

$\Rightarrow$ $p_i^{e_i} \mid (x)$ $\Rightarrow$ $I \mid (x)$

but $v_{p_i}\left(I^{-1}\cdot(x)\right) = 0$ $\forall i$

$\Rightarrow$ $I^{-1}(x) = R$ $\Rightarrow$ $I = (x)$

(c) suppose m, n coprime.

CRT $\Rightarrow \exists$ $r \in R$ $r \equiv m \pmod{n}$

$r \equiv 1 \pmod{p_i}$

$\forall\ p_i \nmid n$

so $m = nq + r$ for some $q \in R$

and $v_{p_i}(r) = 0 \quad \forall\ p_i \nmid n$

and if $p_j \mid n \Rightarrow p_j \nmid m$ so $p_j \nmid r$

so $v_{p_j}(r) = 0 \quad \forall\ p_j \nmid n$

so $d(r) = 0$ as $r \in R^\times$

If $d(n) = 0 \Rightarrow n \in R^\times$ (all $v_p(n) = 0\ \forall p$)

so $m = \frac{m}{n}\, n + 0$

If $d(n) > 0$ $\quad m = nq + r$ $\quad d(r) < d(n)$ or 0

If m, n not coprime, by R = PID

$m = d\,m'$ $\quad m', n'$ coprime

$n = d\,n'$

so $m' = qn' + r'$

$m = nq + r'd$

either $r' = 0 \Rightarrow r'd = 0$
OR $d(r') < d(n')$

and $d(r'd) = \underbrace{d(r')}_{< d(n')} + d(d) = d(n'd) = d(n)$.

□.

(3) (a) I ideal $\quad \{d(x) \mid x \in I\} \subset \mathbb{Z}_{\geq 0}$

so $\exists\ n \in I$ with $d(n)$ minimal.

if $m \in I$ either $n \mid m$ so $m \in (n)$

or $m = nq + r$ $\quad d(r) < d(n)$

$r \neq 0$ is also in I

Contradicting minimality of $d(n)$.

So $I = (n)$.

(b) say $P, Q \in R = PID$ P, Q coprime

$\frac{P}{Q} \in \text{Frac } R$ integral $/\mathbb{Z}$

so $\frac{P^n}{Q^n} + a_{n-1}\frac{P^{n-1}}{Q^{n-1}} + \cdots + a_0 = 0$ $a_i \in \mathbb{Z}$

so $P^n + \left(a_{n-1}P^{n-1} + a_{n-2}P^{n-2}Q + \cdots + a_1 Q^{n-1}\right)Q = 0$

so $Q \mid P^n$

but $(Q, P) = 1$ so any prime ideal $\mathfrak{p} \mid Q$ (x)

$\Rightarrow (x) \mid P^n$ must also divide P contradicting our assumption.

But $\frac{1+\sqrt{-3}}{2} \in \mathbb{Q}(\sqrt{-3})$ is integral $/\mathbb{Z}$

$\notin \mathbb{Z}[\sqrt{-3}]$ so $\mathbb{Z}[\sqrt{-3}]$

cannot be Euclidean or else $PID \Rightarrow$ integrally closed

(4) (a) if $p \mid x$ or $y \Rightarrow p \mid x$ & y

assume $p \nmid x, y$ so $a = \frac{x}{y}$

$\Rightarrow a^2 + a + 1 \equiv 0 \pmod{p}$

$p \equiv 2 (3)$ so $a^3 \equiv 1 \ (p)$

$a \not\equiv 1 \ (p)$

but $a^{p-1} \equiv 1$

$\| $

$a^{\frac{p-2}{3}\cdot 3+1} \equiv (a^3)^{\frac{p-2}{3}} \cdot a \equiv 1$

$\| $

1

so $a \equiv 1$ false.

(b) $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ $\quad p \equiv 1 \ (3)$

$\Rightarrow$ if $\langle g \rangle = \mathbb{F}_p^\times$ then $a = g^{\frac{p-1}{3}} \not\equiv 1 \ (p)$

but $a^3 \equiv 1 \ (p)$

so $a^2 + a + 1 \equiv 0 \ (p)$.

(c) if $p \equiv 1 \ (3)$ $\quad p \mid a^2+a+1$ for some $a \in \mathbb{Z}$

if p prime in $\mathbb{Z}[\zeta_3]$ $\Rightarrow$ $p \mid (a-\zeta)(a-\zeta^2)$

$\Rightarrow$ $p \mid a-\zeta$ or $p \mid a-\zeta^2$

but $p \cdot (m+n\zeta) \neq a-\zeta$

as $pn \neq -1$

So p splits in $\mathbb{Z}[\zeta_3]$ as $(x-y\zeta_3)(x-y\zeta_3^2)$

(take $x-y\zeta_3 \mid p \Rightarrow \overline{x-y\zeta_3} = x-y\zeta_3^2 \mid p$

not unit

and $N_{K/\mathbb{Q}}\left(\frac{p}{(x-y\zeta)(x-y\zeta^2)}\right) = \frac{p^2}{N(x-y\zeta)^2} \in \mathbb{Z}$

so $N(x-y\zeta) = p$ so $p^2 = N(x-y\zeta) = x^2+xy+y^2$

$\#$

1

(d) $n = 3^k \prod_{\equiv 1} p^{n_p} \prod_{\equiv 2} q^{n_q}$

if $x^2 + xy + y^2 = n$

$\| $

$(x - \zeta y)(x - \zeta^2 y)$

so $x - \zeta y \mid n$ in $\mathbb{Z}[\zeta_3] = PID.$

but up to a unit $n = (1-\zeta)^{2k} \prod_{p \equiv 1} (a_p - b_p\zeta)^{n_p} (a_p - b_p\zeta^2)^{n_p} \prod_{q \equiv 2} q^{n_q}$

$p = a_p^2 + a_p b_p + b_p^2$

so $x - \zeta y$ is of the form

$$(\text{unit}) \times (1-\zeta)^k \prod_{p \equiv 1} (a_p - b_p\zeta)^{u_p} (a_p - b_p\zeta^2)^{n_p - u_p} \prod_{q \equiv 2} q^{\frac{n_q}{2}}$$

as $(x - \zeta y) \cdot (\overline{x - \zeta y}) = n$

and n_q MUST be even!

How many choices?

6 units

$0 \le u_p \le n_p$ so

$$\#\{x^2 + xy + y^2 = n\} = 6 \prod_{\substack{p \equiv 1 (3) \\ p \mid n}} (n_p + 1)$$

Now $d \mid n$ is of the form $3^a \prod p^{a_p} \prod q^{b_q}$

$a \le k \qquad a_p \le n_p \quad b_q \le n_q.$

and $d \equiv \begin{cases} 0 \mod 3 & a > 0 \\ (-1)^{\sum b_q} & a = 0 \end{cases}$

So $d_{+/-}(n) = \#\left\{ \begin{matrix} 0 \le a_p \le n_p \\ 0 \le b_q \le n_q \end{matrix} \;\middle|\; \sum b_q \text{ even/odd} \right\}$

$$d_+(n) - d_-(n) = \sum_{\substack{a_p \\ b_q}} (-1)^{\sum b_q}$$

$$= \sum_{a_p} \sum_{b_q} (-1)^{\sum b_q} = \sum_{a_p} \prod_q \left(\sum_{b_q=0}^{n_q} (-1)^{b_q} \right)$$

n_q even no $\displaystyle\sum_{b_q=0}^{n_q} (-1)^{b_q} = 1 - 1 + 1 - 1 + \cdots + 1 = 1$

$$\Rightarrow \quad d_+ - d_- = \sum_{a_p} 1 = \prod_{\substack{p \equiv 1 (3) \\ p \mid n}} (n_p + 1)$$

□.

(5) $2, 7, 1 \pm \sqrt{-13}$ irreducible

because else a divisor α would have norm 2 or 7 and $x^2 + 13y^2 \neq 2, 7$

$$2 = (2, 1+\sqrt{-13})(2, 1-\sqrt{-13})$$
$$7 = (7, 1+\sqrt{-13})(7, 1-\sqrt{-13})$$
$$1 \pm \sqrt{-13} = (2, 1 \pm \sqrt{-13})(7, 1 \pm \sqrt{-13})$$

Why? say $2 = \prod p_i^{e_i}$

$\Rightarrow \prod \|p_i\|^{e_i} \mid \|2\| = 4$

so $\sum e_i \leq 2$ and cannot be [redacted]

the case that $\sum e_i = 1$ because $(2) \neq$ prime ideal

or else $(2) \mid 1 \pm \sqrt{-13}$ untrue.

so $2 = \mathfrak{p} \cdot \bar{\mathfrak{p}}$ and $\mathfrak{p} \mid 1 \pm \sqrt{-13}$ by

UFD into prime ideals.

So $\mathfrak{p} \mid 2$ $\mathfrak{p} \mid$ say $1 + \sqrt{-13}$

$\Rightarrow \mathfrak{p} \mid (2, 1 + \sqrt{-13})$ which is prime $\square$.