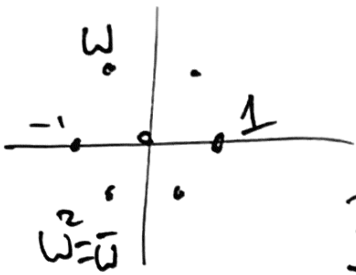
Recall: Eisenstein Integers $R = \mathbb{Z}[\omega]$, $\omega^2+\omega+1=0$. $(\omega^3=1)$.



Def: A ring R is a Euclidean domain if

$\exists\, \mathcal{N} : R \setminus \{0\} \to \mathbb{N}$, $\cancel{\mathcal{N}(0)=0}$, $\cancel{\mathcal{N}(n)=0 \Rightarrow n=0}$ s.t.

$\forall\, n, m \in R$, $m \neq 0$, $\exists\, q, r \in R$ s.t. $n = mq + r$ &

either $\mathcal{N}(r) < \mathcal{N}(m)$. or $r = 0$

polynomials in x, coeff in k.

Another example to keep in mind: $R = k[x]$ $(R = \mathbb{Q}[x]$ or

$R = \mathbb{R}[x]$ or $R = \mathbb{C}[x])$

field

$\boxed{\text{Exercise 1:}}$ $R = k[x]$ is a ring.

Q: Is $R = \mathbb{R}[x]$ $(\ni \sqrt{2} + \pi x + e x^2)$ a Euclidean domain?

i.e. is there a "norm function"? $\mathcal{N}(a_0 + a_1 x + \dots + a_n x^n) = n$, $a_n \neq 0$

i.e. $\mathcal{N}(\text{poly of degree } d) = d$.

Q: Is there a division algorithm?

Ex: $n = x^5 + 4x^4 + 1$, $m = \underbrace{2x^3 + x^2}$.

$$\frac{n}{m}$$

$\frac{1}{2}, \frac{7}{4}, -\frac{7}{8} \leftarrow q$

$m \rightarrow 2, 1, 0, 0 \;|\; 1, 4, 0, 0, 0, 1 \leftarrow x^5 + 4x^4 + 1.$

$-1, -\frac{1}{2},$

$0, 3\frac{1}{2}, 0$

$\frac{7}{2}$

$-\frac{7}{2}, -\frac{7}{4}$

$0, -\frac{7}{4}, 0$

$+\frac{7}{4}, +\frac{7}{8}$

$r \rightarrow \underbrace{\frac{7}{8}, 0, 1}$

$\boxed{\text{Exercise 2}}$: Check that

$$\Big[\underbrace{(2x^3 + x^2)}_{m} \cdot \underbrace{\left(\tfrac{1}{2}x^2 + \tfrac{7}{4}x - \tfrac{7}{8}\right)}_{q} + \underbrace{\tfrac{7}{8}x^2 + 1}_{r}\Big] = n$$

$$= x^5 + 4x^4 + 1$$

$\boxed{\text{Exercise 3:}}$ Do same,

$n = 3x^4 + 2x^2 - 1$

$m = x^2 + 2x - 7.$

Find q & r.

Thm: $k[x]$ is a Euclidean Domain. $\left(\text{degree}(0) = -\infty\right).$

pf: Polynomial Division.

Thm: R a Euclidean Domain $\Rightarrow$ R is a PID.

(Examples: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\omega]$, $\mathbb{R}[x]$).

(all $I \subset R$ ideals are principal, $I = (a)$.).

$((n,m) = \{nx + my \mid x, y \in \mathbb{Z}\})$

{ideal generated by $n_1, \dots, n_k$ is $\{n_1 r_1 + \dots + n_k r_k,\ r_i \in R\}$

Pf: Either $I = (0)$ ✓ or $I \ni a \neq 0$.

Let $S = \{N(i) : i \in I \setminus \{0\}\} \subseteq \mathbb{N}$

Let $s \in S$ be least element. & let $d \in I$ have $N(d) = s$. $\Rightarrow$ $(d) \subseteq I$.

Want: $(d) = I$ ($\Rightarrow I$ is principal). If $\exists\ m \in I \setminus (d)$, then By Division algorithm, $\exists\ q, r \in R$ s.t. $m = d \cdot q + r$, $r \in I$.

& since $m \notin (d) \Rightarrow r \neq 0$. $\Rightarrow$ $N(r) < N(d)$. $\times$.

$\boxed{\text{Exercise 4:}}$ Let $I = (x^3 + x + 1, x^2 + 1) \subseteq R = \mathbb{Q}[x]$.

Find d s.t. $I = (d)$. (Ans: $I = R$).

$\boxed{\text{Exercise 5:}}$ Let $I = (x^3+x^2+x+1,\ x^4+x^3+x+1) \subset R = \mathbb{Q}[x]$. Find $d \in R$ s.t. $I = (d)$.

$\Leftrightarrow \boxed{R^\times = \mathbb{Q}^\times}$.

<u>Def:</u> $u \in R^\times$ = units of $R \Leftrightarrow \exists v \in R$ s.t. $u \cdot v = 1$

<u>Def:</u> $a, b \in R$ are <u>associate</u> $\Leftrightarrow \exists u \in R^\times$ s.t. $a = b \cdot u$. $\Leftrightarrow a \sim b$.

<u>Def:</u> $a \in R$ is <u>irreducible</u> $\Leftrightarrow d \mid a \Rightarrow d \in R^\times$ or $d \sim a$.

<u>Def:</u> $p \in R$ is <u>prime</u> $\Leftrightarrow (p \mid ab \Rightarrow p \mid a$ or $p \mid b)$.

<u>Def:</u> $a \mid b \Leftrightarrow (b) \subseteq (a)$. <u>Def:</u> $u \in R^\times \Leftrightarrow (u) = R$.

<u>Def:</u> $a \sim b \Leftrightarrow (a) = (b)$. <u>Def:</u> $p \in R$ is prime $\Leftrightarrow a \cdot b \in (p) \Rightarrow \begin{cases} a \in (p) \text{ or} \\ b \in (p) \end{cases}$.

<u>~~Def.~~Q:</u> $a, b \in R$ are coprime & R is PID $\Leftrightarrow (a, b) = R$.

Def: d is a gcd of $a \& b \in R$ iff: ① $d|a \& d|b$ &

② if $d'|a \& d'|b \Rightarrow d'|d$.

$\boxed{\text{Exercise 6:}}$ Restate this in language of ideals.

Prop: If R is a PID, & $a, b \in R \Rightarrow \exists$ gcd d of $a \& b$ s.t. $(a,b) = (d)$.

pf: Already know that $(a,b) = (d)$, for some d. Need: d is a gcd.

Well, $b \in (a,b) \subseteq (d)$. $\Rightarrow b = d \cdot k \Rightarrow d|b$. & $d|a$. (same). ① ✓

If $d'|a \& d'|b \Rightarrow a = d' \cdot l$, $b = d' \cdot k$. so $a \in (d')$, $b \in (d')$.

$(d) = (a,b) \subset (d')$. $\Rightarrow d \in (d')$. $\Rightarrow d = d' \cdot r$. $\Rightarrow d'|d$. ② ✓

Def: A ring R is Noetherian. (Emmy Noether) if

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ is a chain of ideals, then

chain stops in finite time, ⑤ i.e. $\exists N$ s.t. $\forall n > N$, $I_N = I_n$

Is $\mathbb{Z}$ Noetherian? Know: $\mathbb{Z}$ is a PID.

$$(60) \subseteq (12) \subseteq (6) \subseteq (2) \begin{cases} \subseteq (2) \subseteq (2) \subseteq (2) \cdots \\ \subseteq (1) = R \subseteq (1) \subseteq (1) \ldots \end{cases}$$

("No infinite descent").

<u>Thm:</u> R is a PID $\Rightarrow$ R is Noetherian.

<u>pf:</u> let $\underset{(a_1)}{\underset{\shortparallel}{I_1}} \subseteq \underset{(a_2)}{\underset{\shortparallel}{I_2}} \subseteq \cdots$ be an increasing chain.

let $I = \bigcup_{k=1}^{\infty} I_k$ $\boxed{\text{Exercise 7:}}$ I is an ideal

~~Unions of ideals are ideals.~~

Then I is an ideal $\Rightarrow$ $I = (a)$. for some a.

So $\exists N$ s.t. $a \in I_N$. so $I = (a) \subseteq I_N \Rightarrow R$ is Noetherian.