Review: A ring R: closed under $+$ & $\times$.

i.e. if $r, s \in R$, $r+s \in R$, $r-s \in R$, $0 \in R$, $r \cdot s \in R$, $1 \in R$. (s^{-1} need not exist)

Ex: $R = \mathbb{Z}$, $\mathbb{Z}[i]$ Gaussian integers,

$\mathbb{Z}[\omega]$ Eisenstein integers, $\omega = e^{2\pi i/3}$, $\bar{\omega} = \omega^2$ | $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.,

$R = \mathbb{Z}[\sqrt{5}]$,

$R = \mathbb{Z}[x] = \{ a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in \mathbb{Z} \}$.

$R = \mathbb{Q}[x] = \{ \cdots \mid a_i \in \mathbb{Q} \}$.

(or for any field k, $R = k[x]$)

An ideal $I \subset R$ s.t. closed under $+$ in I & $\times$ in R. I.e. $\forall n, m \in I$, $n+m \in I$, $n-m \in I$, $\forall n \in I$, $r \in R$, $n \cdot r \in I$.

Ex: $R = \mathbb{Z}$, $I = (6) = \{\ldots, -6, 0, 6, 12, \ldots\} = 6\mathbb{Z}$.

$R = \mathbb{Q}[x]$, $I = (x^2+2) = \{x^3+2x, 0, x^2+2, 2x^2+4\}$

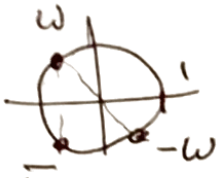
$\cap$

A ring R is a <u>Euclidean Domain</u>: If it has a division algorithm. I.e. $\exists N: R\setminus\{0\} \to \mathbb{N}$.

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

$$n = qm + r \quad \& \quad \begin{cases} N(r) < N(m) \\ \text{or } r = 0 \end{cases}.$$

<u>Ex:</u> $R = \mathbb{Z}$, $N(n) = |n|$.



$R = \mathbb{Z}[i]$, $N(x+iy) = x^2+y^2 = |z|^2 = z\cdot\bar{z}$. ($x+iy = z$)

$R = \mathbb{Z}[\omega]$, $N(x+\omega y) = (x+\omega y)(x+\bar{\omega} y)$

$= x^2 - xy + y^2$.

$R = k[x]$, $N(a_0 + a_1 x + \dots + a_n x^n) = n$. = degree

$R = \mathbb{Z}[\sqrt{-5}]$, $N(x+\sqrt{-5}y) = (x+\sqrt{-5}y)(x-\sqrt{-5}y)$

$= x^2 + 5y^2$.

$6 = 2\cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$.

<u>No division algorithm!</u>

(We will prove: Euclidean Domain $\Rightarrow$ PID $\Rightarrow$ Noetherian $\Rightarrow$ UFD.)

Note: In general, no bijection between rings, even if both are Euclidean Domains.
Reason: both $\mathbb{Z}$ & $R = \mathbb{R}[x]$ are Euclidean.

Why do $\mathbb{Z}[i]$ & $\mathbb{Z}[\omega]$ have division algorithms?

$n = mq + r$, $\frac{n}{m} \in \mathbb{Q}[i]$.

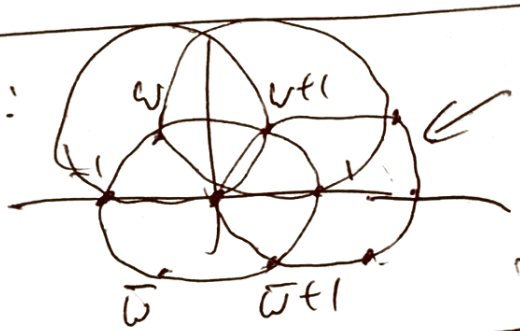
$q = [\frac{n}{m}]$ nearest Gaussian integer.

Then $|r|^2 = |n - mq|^2 = \underbrace{\left(\frac{n}{m} - q\right)}_{< 1} \cdot \underbrace{|m|^2}_{N(m)}$

$N(r)$

< 1 because $< \frac{\sqrt{2}}{2} < 1$.

In $\mathbb{Z}[\omega]$:



← circles of radius 1 around lattice points fill all of $\mathbb{R}^2$.

In $R = K[x]$, $\frac{n}{m}$ polynomial ~~long~~ division.

$\Rightarrow \exists\ q \in R$ & $r \in R$ s.t. $n = mq + r$,

& either $r = 0$, or $\deg(r) < \deg(m)$

Why can't we take larger circles in $\mathbb{Z}[\sqrt{-5}]$?
Like radius $\sqrt{5}$ circles? These circles will fill all of $\mathbb{R}^2$.

$\left[\frac{n}{m}\right] = q$, $n = mq + r$.

$N(r) = |r|^2 = |n - mq|^2 = \left|\frac{n}{m} - q\right|^2 |m|^2$

$\frac{3}{2} \cdot N(m) > 1$.

$\left(\frac{1}{2}\right)^2 + \left(\frac{\sqrt{5}}{2}\right)^2 = \left(\quad\right)^2$

$= \frac{1}{4} + \frac{5}{4} = \frac{6}{4} = \left(\sqrt{\frac{3}{2}}\right)^2 = \frac{3}{2}$.

Maybe we're not clever enough to find a "good" norm function? (Need not be $N(m) = |m|^2$.) If we could, would get that $\mathbb{Z}[\sqrt{-5}]$ is a UFD but we know it isn't. ["Class Number One Problem".]

Review: Thm: Euclidean Domain $\Rightarrow$ PID.

Pf: (Claim: If $\mathcal{I} = (n, m)$, $n, m \in R$, then $\mathcal{I} = (d)$ & d is a gcd of n & m.)

Terminology: A unit $u \in R$ has $v \in R$ s.t. $uv = 1$.

Recall: $R^\times = \{u \in R \mid \text{unit}\}$ is a group.

Def: $a \& b \in R$ are **associates** if $a = bu$, $u \in R^\times$, $\Leftrightarrow (a) = (b)$.

Def: $r \in R$ is **irreducible** if: $r = s \cdot t$, $s, t \in R$
$\Rightarrow s \in R^\times$ or $(s) = (r)$.

Def: $p \in R$ is **prime** if: $p \mid a \cdot b \Rightarrow p \mid a$ or $p \mid b$.
$\Leftrightarrow$ ~~[illegible]~~ $a \cdot b \in (p) \Rightarrow a$ or $b \in (p)$. (or both).

E.g.: Recall: $2 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime.
$2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$
& $2 \nmid (1 \pm \sqrt{-5})$.

Exercise 1: p prime $\Rightarrow p$ is irreducible.

Exercise 2: If R is a PID $\Rightarrow$ (irreducible $\Leftrightarrow$ prime)

Ex: In $R = \mathbb{R}[x]$, $R^\times = \mathbb{R} \setminus \{0\}$.

Ex: Is x^2+1 irreducible? In $\mathbb{R}[x]$, yes!
In $\mathbb{C}[x]$, not irreducible, $x^2+1 = (x+i)(x-i)$.

Exercise 3: Is x^2+1 irreducible in $(\mathbb{Z}/5)[x]$? ($\mathbb{Z}/5$ is a field.) In $(\mathbb{Z}/6)[x]$?

Exercise 4: Is x^2+1 irreducible in $(\mathbb{Z}/7)[x]$?