Lec 11/8

Thursday, November 8, 2018 11:31

$D \in \mathbb{Z}_{\leq -1}$ (square-free)

$D =$	-1	-2	-3	-5	. . .	-19
$\omega =$	$\sqrt{-1}$	$\sqrt{-2}$	$\frac{1+\sqrt{-3}}{2}$	$\sqrt{-5}$		$\omega = \frac{1+\sqrt{-19}}{2}$
$\mathcal{O}(\sqrt{D}) = \mathbb{Z}[\omega]$	Euclidean $\Longrightarrow$ P.I.D. $D = -7, -11$			Not P.I.D. $\Longrightarrow$ Not euclidean		P.I.D. but <u>not</u> euclidean

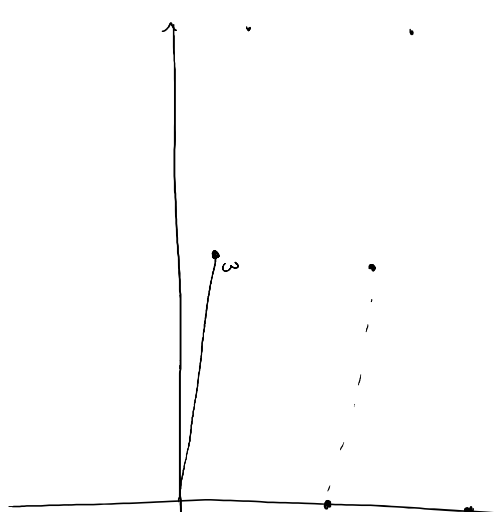
$R = \mathbb{Z}[\omega]$; $\omega = \frac{1+\sqrt{-19}}{2}$ is not euclidean.

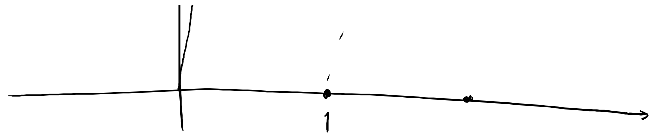
Assume R is euclidean. then $\exists\ N : R \longrightarrow \mathbb{Z}_{\geq 0}$ $(N(0) = 0)$ s.t.

$\forall a, b \in R$ w/ $b \neq 0$, $\exists\ q, r$ s.t. $a = qb + r$ w/ $N(r) < N(b)$ or $r = 0$.

$\Longrightarrow$ $\exists\ u \in R \setminus \{0, R^\times\}$ s.t. $\forall x \in R$, $x = qu + r$ w/ $r \in R^\times$ or $r = 0$.

<u>Pf</u>. take $u \in R \setminus \{0, R^\times\}$ of smallest $N(\cdot)$.





take $x=2$. only units in R are ± 1.

- u divides 2, 1, or 3. not 1 since $u \notin R^\times$.

$u \mid 2 \Rightarrow 2 = u \cdot v \Rightarrow |2|^2 = |u|^2 \cdot |v|^2. \Rightarrow |u|^2 = 1, 2, \text{ or } 4.$

$|u|^2 \neq 1$ since $u \neq \pm 1$

$|u|^2 \neq 2$ since $|a + b\omega| = (a + \frac{b}{2})^2 + \frac{19}{4}b^2 \geq \frac{19}{4} > 2$ if $b \neq 0$.

$|u|^2 = 4 \Rightarrow |v|^2 = 1 \Rightarrow v = \pm 1 \Rightarrow u = \pm 2$.

Check 2 cannot divide $\omega, \omega+1, \omega-1$

$u \mid 3 \xRightarrow{3=u\cdot v} 9 = |u|^2 \cdot |v|^2 \Rightarrow |u|^2 = 1, 3, \text{ or } 9.$ can't be 1 or 3 again

So $u = \pm 3$. check 3 cannot divide $\omega, \omega+1, \omega-1$.

$|\omega|^2 = 5 = |\omega - 1|^2, \quad |\omega + 1|^2 = 7$ so no integer divides $\omega, \omega+1, \omega-1$.

Noetherian Domains

Hilbert's Basis Theorem

- Being Noetherian is preserved under our operations: $(R_1 \times R_2,\ R/I,\ S^{-1}R,\ R[x])$

- $I = Q_1 \cap Q_2 \cap \cdots \cap Q_\ell$ more or less uniquely.

↳ for P.I.D.'s: uniqueness, $\cap \to \cdot$, $Q_1 = (p^k) = (p)^k$

So $\underbrace{n = u p_1^{k_1} \cdots p_\ell^{k_\ell} \text{ uniquely}}$ (up to choice of unit).

$\left.\begin{array}{l} I = P_1^{k_1} \cdots P_\ell^{k_\ell} \\ \text{uniquely} \end{array}\right\}$ → [Dedekind Domains $\supset$ P.I.D. $\subset$ Unique factorization domains

Dedekind Domains $\cup$ $\mathcal{O}(\sqrt{D})$ or any nice "ring of integers"

P.I.D. $\cup$ euclidean domains $\cup$ fields

Unique factorization domains.

Unique factorization domain:

- R is an integral domain. $a \in R$, $a \notin R^\times$, $a \neq 0$.
  a is called irreducible element if $a = xy \Rightarrow$ one of x, y is a unit.

- R is a UFD if $\forall n \in R$; $n \notin R^\times$; $n \neq 0$, there exist
  $p_1, \dots, p_\ell \in R$ s.t. $n = p_1 \cdot \dots \cdot p_\ell$ and for any $q_1, \dots, q_m \in R$
  s.t. $n = q_1 \cdot \dots \cdot q_m$, $m = \ell$ and $\exists \sigma \in S_\ell$, $u_1, \dots, u_\ell \in R$ s.t.
  $u_i q_i = p_{\sigma(i)} \quad \forall i = 1, \dots, \ell$.

eg every P.I.D. is a U.F.D.

$\mathbb{Z}[\sqrt{-5}]$ is not a U.F.D.

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

(2) $\exists$ irreducible elements which don't generate a prime ideal.

$3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible. $3 = u \cdot v \Rightarrow 9 = |u|^2 \cdot |v|^2$, $u = a + b\sqrt{-5}$, $|u|^2 = a^2 + 5b^2$

$|u|^2 \neq 3$ since $|u|^2 \geq 5$ if $b \neq 0$ So either $u = \pm 1$ or $v = \pm 1$

$2 \in \mathbb{Z}[\sqrt{-5}]$ is also irreducible.

$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3 \in (3)$ but $(1 \pm \sqrt{-5}) \notin (3)$ since $1 \pm \sqrt{-5} \neq 3 \cdot (a + b\sqrt{-5})$.

So (3) is not a prime ideal.

Prop. Let R be a U.F.D., $a \in R$, $a \neq 0$, $a \notin R^\times$, a irreducible element then (a) is a prime ideal.

Conversely, if $P = (a) \subsetneq R$ is a prime ideal then a is irreducible.

Pf of converse: $P = (a) \subsetneq R$ is prime. Suppose $a = x \cdot y$. then one of x or $y \in P$.
Say $x \in P$; $x = ar$. then $a = yra \Rightarrow yr = 1$ so y & r are

unit so y is unit. (only use fact that R is a domain).

<u>Pf of propn</u>: Assume a is an irreducible **element**. (T.S.: $P = (a)$ is prime).

Let $xy \in P = (a)$. $xy = ar$ for some $r \in R$. suppose $r = p_1 \cdots p_\ell$, $xy = q_1 \cdots q_m$

p_i, q_i irreducible. one p_i must be ua for some unit, meaning $ua \mid x$ or $ua \mid y$.

So either x or $y \in (a)$.

Read P.I.D. $\Rightarrow$ U.F.D. in §8.3