Lecture 18: Euclidean domains; PIDs

§25-26 of [R2] §8.1-8.2 of [DF]

Working towards factoring non-units in rings such as $\mathbb{Z}[i]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{-D})}$, $\mathbb{Q}[x]$, $\mathbb{F}_p[x,y,z]$, etc.

<u>Euclidean domain</u>: An integral domain R with a <u>norm</u> $N: R\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ where for all $a, b \in R$ with $b \neq 0$, have $a = qb + r$ with $r = 0$ <u>or</u> $N(r) < N(b)$.

quotient (q), remainder (r)

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

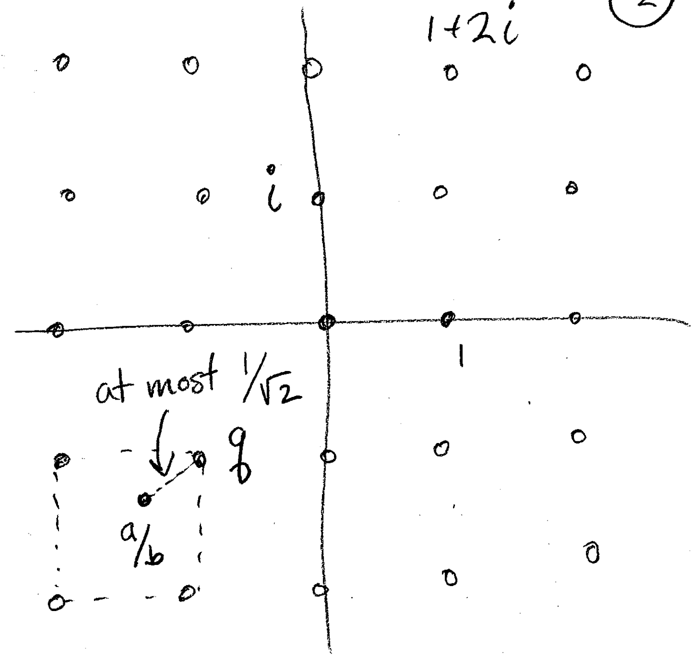
<u>Ex</u>: $\mathbb{F}[x]$, $N(f) = \deg f$ ($\mathbb{F}$ a field)

<u>Ex</u>: Any field with $N = 0$.

<u>Ex</u>: $\mathbb{Z}[i]$ with $N(u+vi) = |u+vi|^2 = u^2+v^2$

<u>Proof</u>: Suppose $a, b \in \mathbb{Z}[i]$. Let q be an elt of $\mathbb{Z}[i]$ closest to $\frac{a}{b} \in \mathbb{C}$. Setting $r = a - qb$, have $a = qb + r$. Now

$$N(r) = |r|^2 = \left|\frac{a}{b} - q\right|^2 |b|^2$$
$$\leq \frac{1}{2}|b|^2 < N(b).$$



Non-Ex: $\mathbb{Z}[\sqrt{-5}]$

[since doesn't have unique factorization. Proof fails because of "grid size"]

Principal ideal domain (PID): An integral domain where every ideal is principal.

Thm: Euclidean domains are PIDs.

Pf: Let $I \neq \{0\}$ be an ideal of R. Let $b \in I$ be a nonzero element of minimal norm. Will show $I = (b)$. Given $a \in I$, have $a = qb + r$ with $r = 0$ or $N(r) < N(b)$. If $r = 0$, have $a \in (b)$ as needed. Otherwise, $r = a - qb \in I$ contradicts minimality of $N(b)$. ∎

Note: There are PIDs that are not Euclidean, e.g. $\mathcal{O}_{\mathbb{Q}(\sqrt{-19})} = \mathbb{Z}\left[\frac{1+\sqrt{19}\,i}{2}\right]$.

R an integral domain. Write $a \mid b$ if $b = qa$ for some $q \in R$. A $g \in R$ is a <u>gcd</u> of $a, b \in R$ if $g \mid a$ and $g \mid b$ and whenever $d \mid a$ and $d \mid b$ then $d \mid g$. [g is unique up to units.]

<u>Non-Ex</u>: 6 and $2 + 2\sqrt{-5}$ have no gcd in $\mathbb{Z}[\sqrt{-5}]$.

[Will show later.]

<u>Thm</u>. If R is a PID, any $a, b \in R$ have a gcd.

<u>Pf</u>. Set $I = (a, b)$ and find g with $(g) = I$. Thus $g \mid a$ and $g \mid b$ as $a, b \in I$. As $g \in I$, have $g = ua + vb$ and so any common divisor of a and b also divides g. So $g = \gcd(a, b)$. $\blacksquare$

<u>Note</u>: When R is Euclidean, can use Euclid's algorithm to compute gcds, using that if $a = qb + r$ then $\gcd(a, b) = \gcd(b, r)$.

<u>Thm</u>: R a PID. Any nonzero prime ideal I of R is maximal.

Pf: Have $I = (p) \subsetneq R$. Suppose $(p) \subseteq (a) \subseteq R$.
Need to show $(p) = (a)$ or $(a) = R$. Now $p = ab$ for some $b \in R$. As (p) is prime either $a \in (p)$ or $b \in (p)$. If the former, have $(p) = (a)$.
Otherwise, $b = cp$, so $p = (ac)p \implies ac = 1$ $\overset{R \text{ domain}}{\implies}$ a unit $\implies (a) = R$. So (p) is maximal ▨

[Expect to end here.]

For $R = \mathbb{Z}[\sqrt{-5}]$, consider $N(a+b\sqrt{-5}) = |a+b\sqrt{-5}|^2 = a^2 + b^2 5$. Set $\alpha = 6$ and $\beta = 2+2\sqrt{-5}$, which have norms $36 = 2^2 \cdot 3^2$ and $24 = 2^3 \cdot 3$. If $\gcd(a,b) = \gamma$, then $\gamma | \alpha$ and $\gamma | \beta \Rightarrow N(\gamma)$ divides $N(\alpha)$ and $N(\beta) \Rightarrow N(\gamma) \mid 12$. If η is a comm. div. of α, β then $\eta | \gamma \Rightarrow N(\eta) \mid N(\gamma)$.

As 2 and $1+\sqrt{-5}$ are common divisors of α, β (as $6 = (1+\sqrt{-5})(1-\sqrt{-5})$) with norms 4 and 6, learn $N(\gamma) = 12$. Now $2 | \gamma$ so $\gamma = 2\varepsilon$. Taking norms gives $N(\varepsilon) = 3$. But R has no elts of norm 12, a contradiction. So α and β have no gcd $\Rightarrow R$ is not a PID $\Rightarrow R$ is not Euclidean.