Lecture 2: Euclidean Domains

All rings are commutative and have a 1.

<u>Integral Domain</u>: A ring without zero divisors, i.e. $a \cdot b = 0 \Rightarrow a = 0$ or $b = 0$.

<u>Ex</u>: $\mathbb{Z}$, any field (or subset thereof)

<u>Non Ex</u>: $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$ [with componentwise mult]

$2 \cdot 3 = 0$. $(1,0)\cdot(0,1) = (0,0)$

[Initial focus is factoring, etc, in integral domains. One kind that has all the props we're familiar with from $\mathbb{Z}$ is.]

<u>Euclidean Domain</u>: An integral domain R with a <u>norm</u> $N : R \to \mathbb{Z}_{\geq 0}$ where

1. $N(0) = 0$.
2. For $a, b \in R$ with $b \neq 0$, then $a = qb + r$ (quotient q, remainder r) where $r = 0$ <u>or</u> $N(r) < N(b)$.

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

$F[x]$ for F a field with $N(p(x)) = \deg p$

F a field with $N = 0$.

Ex: $\mathbb{Z}[i]$ with $N(a+bi) = |a+bi|^2 = a^2+b^2$
[Will show at end of hour]

Non Ex: $\mathbb{Z}[\sqrt{-5}]$ [since this doesn't have unique fac.]

[Origin of name: These are the rings where the Euclidean Algorithm for finding gcd's works.]

For $a, b \in R$, write $a|b$ if $b = qa$ for some $q \in R$.

Def: A $g \in R$ is a gcd for $a, b \in R$ if $g|a$ and $g|b$ and whenever $d|a$ and $d|b$ then $d|g$. [Unique up to units.]

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

Thm: In a Euclidean domain, any $a, b \in R$ with $b \neq 0$ have a gcd.

Pf: If $a = qb + r$, then the common divisors of (a, b) are the same as those of (b, r). [Hence one pair has a gcd iff the other does.] Similarly, if $b = q'r + r'$, then (b, r) has the same common divisors as (r, r'). Since R is Euclidean can arrange that $N(b) > \underset{r_0}{N(r)} > \underset{r_1}{N(r')} > \cdots \geq 0$

as we repeat with $r_n = q_{n+1} r_{n+1} + r_{n+2}$. So eventually

get $r_n = q_{n+1} r_{n+1} + 0$. As the gcd of $(r_{n+1}, 0)$ is r_{n+1},

we have r_{n+1} is the gcd of (a,b). ▨

An ideal $I \subseteq R$ is an additive subgp where $r \cdot i \in I$ for all $r \in R$ and $i \in I$. [For needed background, see Ch 7.]

<u>Ex</u>: For $a \in R$, have the principle ideal $(a) = \{ra \mid r \in R\}$

<u>Principle</u>: $3\mathbb{Z} \subseteq \mathbb{Z}$ <u>Not</u>: $(2, x) \subseteq \mathbb{Z}[x]$

[Motivation: Kernels of ring hom; ideal numbers.]

<u>Thm</u>: If R is Euclidean, then every ideal is principle.

<u>Pf</u>: Choose $a \neq 0$ in I of minimal norm. If $b \in I$, then $b = qa + r$ with $r = 0$ or $N(r) < N(a)$. Since $r = b - qr \in I$ must have $r = 0$ and $b = qa$. So $I = (a)$. ▨

Note: For R Euclidean, if $I = (a,b) = \{r_1 a + r_2 b \mid r_i \in R\}$ then $I = (g)$ where $g = \gcd(a,b)$.

Reason: Clearly $I \subseteq (g)$ since $g \mid a$ and $g \mid b$.
As for $\mathbb{Z}$, the Euclidean algorithm gives that $g = ra + sb$ for some $r, s \in R$ and hence $(g) \subseteq I$.

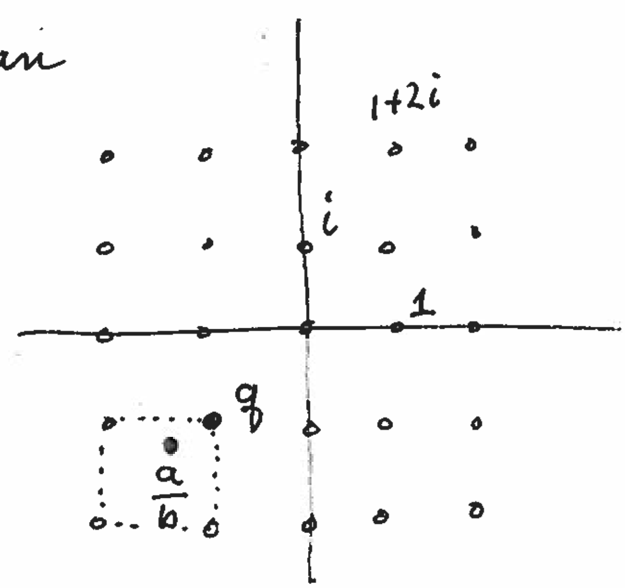
[Can have gcd's without this prop, e.g. $\mathbb{Q}[x,y]$ where x and y have gcd $= 1$.]

[Next time: If every ideal is principle, then R has unique factorization.]

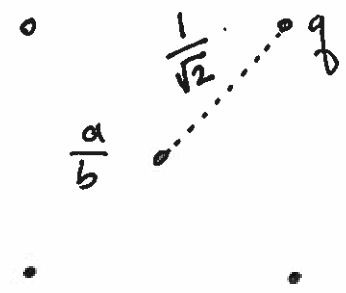
Proof that $\mathbb{Z}[i]$ with $N = |\,|^2$ is Euclidean:

$a, b \in \mathbb{Z}[i] \subseteq \mathbb{C}$. Let q be an elt of $\mathbb{Z}[i]$ closest to $\frac{a}{b} \in \mathbb{C}$

Then $a = qb + r$ where $r = a - qb$. Now



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



The problem with $\mathbb{Z}[\sqrt{-5}]$ is that the grid is too big...