Lecture 2

Convention: All rings are commutative and have a 1.

Integral Domain: A ring R w/o zero divisors
i.e. $a \cdot b = 0 \Rightarrow$ one of $a, b = 0$.

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

Non Ex: $\mathbb{Z} \times \mathbb{Z}$ (w/ componentwise mult.)

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

[As per last time, will focus on factoring, etc. of integral domains. One type that possesses all these props is.]

Euclidean Domain: An int domain R with a norm $N: R \to \mathbb{Z}_{\geq 0}$ sat

① $N(0) = 0$

② For a, b in R w/ $b \neq 0$, $a = qb + r$ (quotient, remainder)
where $r = 0$ or $N(r) < N(b)$.

Ex: $\mathbb{Z}$, with $N(a) = |a|$; $F[x]$ for F a field with $N(f(x)) = \deg f$.
F any field with $N = 0$

$\mathbb{Z}[i]$ with $N(a+bi) = |a+bi|^2 = a^2 + b^2$

[Will justify this later.]

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

For $a, b \in R$, write $a \mid b$ if $b = ga$ for $g \in R$.

Def: A gcd for $a, b \in R$ is an elt g s.t. if $d \mid a$ and $d \mid b$ then $d \mid g$. [When it exists, its unique up to units.]

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

Thm In a Euclidean domain, any $a, b \in R$ have a gcd.

Proof: If $a = qb + r$, then the common divisors of (a,b) are the same as those of (b,r). [Hence one has a gcd iff the other one does.]

Lem. if $b = q'r + r'$, then (a,b) has the same common divisors as (r,r'). Repeating, this stops at some pt with $r_n = q_{n+1} r_{n+1} + 0$ since $N(b) > N(r) > N(r') > \cdots \geq 0$. As a gcd of $(r_{n+1}, 0)$ is r_{n+1}, we have r_{n+1} is a gcd of (a,b)

Recall an ideal $I \subseteq R$ is an additive subgroup with $r \cdot i \in I$ for all $r \in R$ and $i \in I$.

[Note: needed background, see Chapter 7.]

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

[Motivate: kernels of ring homom; ideal numbers (below).]

Thm: If R is Euclidean, then every ideal is principle.

Pf: Choose $a \neq 0$ in I with minimal norm among all nonzero elements. If $b \in I$, then $b = qa + r$ with $r = 0$ or $N(r) < N(a)$. As $r = b - qa \in I$, must have $b = qa$. So $I = (a)$. ▨

Note: For R Euclidean, if $I = (a, b)$

$$= \{r_1 a + r_2 b \mid r_1, r_2 \in R\}$$

then $I = (g)$ where g is a gcd of (a, b).

Reason: Clearly $I \subseteq (g)$ since

$$r_1 a + r_2 b = r_1 a' g + r_2 b' g = (r_1 a + r_2 b) g$$

The Euclidean algorithm shows that $g = ra + sb$ and so $I \supseteq (g)$.

[Details: cf $a = qb + r$ and $g = r_1 b + r_2 r$ is a gcd of (b, r) then $g = r_2 a + (r_1 - q r_2) b$.]

Next time: cf every ideal is principle, then R has unique factorization

A non-principle ideal: $(2, 1+\sqrt{5})$ in $\mathbb{Z}[\sqrt{-5}]$

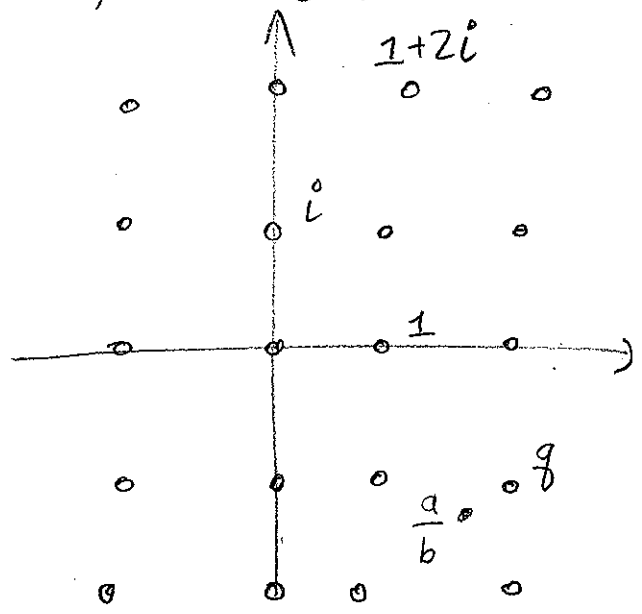
Proof that $\mathbb{Z}[i]$ is Euclidean: $a, b \in \mathbb{Z}[i] \subseteq \mathbb{C}$

$N(a) = |a|^2$ ← usual complex abs. value.

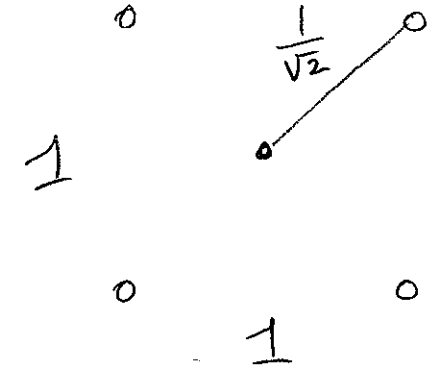
Let q be the elt'n $\mathbb{Z}[i]$ closest to $\frac{a}{b} \in \mathbb{C}$. Then

$a = q \cdot b + r$ where

$r = a - qb$



Now $N(r) = |r|^2 = \left|\frac{a}{b} - q\right|^2 |b|^2 \leq \frac{1}{4}|b|^2 < N(b)$.



Problem with $\mathbb{Z}[\sqrt{-5}]$: grid is too big...