ED $\mathbb{Z}[i]$

Lecture 31

Prop 11: Let R be a PID and $a, b \in R$. Then $\gcd(a,b) = ra + sb$ for some $r, s \in R$.

Pf: Consider the ideal (a,b).

Since R is a PID $\therefore (a,b) = (d)$ for some $d \in R$.

Claim d is $\gcd(a,b)$.

$\because a, b \in (d) \Rightarrow d \mid a$ & $d \mid b$.

Let e be any elt s.t. $e \mid a$ & $e \mid b$

WTS $e \mid d$.

Since $e \mid a \Rightarrow a = eq$

and $e \mid b \Rightarrow b = eb_1$.

Since $d \in (a,b) \Rightarrow d = ra + sb$

$\Rightarrow e \mid d$. $\therefore d = \gcd(a,b)$ $= req + seb_1$

$= e(rq + sb_1)$.

Defn A size fn. on an int domain R is any fn. $N : R \setminus \{0\} \to \{0, 1, 2, \ldots\}$ from the set of non-zero elts of R to the set of non-negative integers.

In $\mathbb{Z}$, $N(a) = |a|$

In $k[x]$, $N(f(x)) = \deg f$.

Defn An integral domain R is an Euclidean domain if there is a size fn. N on R s.t for all $a, b \in R$ s.t $a \neq 0$ there are elts $q, r \in R$ s.t $b = aq + r$ and either $r = 0$ or $N(r) < N(a)$. q is called the quotient & r is called the remainder.

Example. $\mathbb{Z}[i]$ is an ED with

$$N(a+ib) = a^2+b^2$$

Let $\alpha = a+ib$ and $\beta = c+id \neq 0$.

Then $\alpha/\beta = \dfrac{a+ib}{c+id} = \dfrac{(a+ib)(c-id)}{c^2+d^2}$

$$= \frac{ac+bd}{c^2+d^2} + i\,\frac{(bc-ad)}{c^2+d^2}$$

$$= r+is \in \mathbb{Q}[i].$$

$\Rightarrow \alpha = \beta(r+is)$

Let p and q be integers closest to r & s.

$\therefore |r-p|$ & $|q-s|$ are atmost $1/2$

Let $\theta = (r-p) + i(s-q)$.

Let $\nu = \beta\theta = \beta\left[(r-p)+i(s-q)\right]$

$$\nu = \beta\theta = \beta(r+is) - \beta(p+iq)$$

$$= \alpha - \beta(p+iq) \in \mathbb{Z}[i]$$

$$\therefore \alpha = \beta(p+iq) + \nu.$$

$$N(\nu) = N(\beta\theta) = N(\beta)N(\theta)$$

$$= N(\beta)\left[|r-p|^2 + |s-q|^2\right]$$

$$\leq N(\beta)\left(\frac{1}{4}+\frac{1}{4}\right)$$

$$= \frac{1}{2}N(\beta).$$

$$\therefore N(\nu) < N(\beta).$$

$\therefore \mathbb{Z}[i]$ is an ED.

Thm. ED are PID.

Pf: Let R be an ED and I be a non-zero ideal of R. Let us consider

set $S = \{N(a) \mid a \in I, a \neq 0\}$.

By well ordering principal S has a minimal elt. say $N(b)$ for some $b \in I$.

WTS $I = (b)$.

Let $a \in I$ then $a = bq + r$ for some $q, r \in R$ & $r = 0$ or $N(r) < N(b)$

Now $r = a - bq \in I$.

$\therefore N(b)$ is minimal in S.

So $r = 0 \Rightarrow I = (b)$.

Thus R is a PID.

field $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ int domain

(1) $\mathbb{Z}$ is an ED but not a field.

(2) $\mathbb{Z}\left[\left(1+\sqrt{-19}\right)/2\right]$ is a PID but not ED. [I will discuss later]

(3) $\mathbb{Z}[x]$ is an UFD but not a PID.

(4) $\mathbb{Z}[\sqrt{-3}]$ is an int domain but not an UFD.

Next we study $\mathbb{Z}[i]$ and investigate which prime number are also prime ideals in $\mathbb{Z}[i]$.

Q Which integers can be written as sum of of two squares i.e which $n = a^2 + b^2$. for some $a, b \in \mathbb{Z}$.

The ring of Gaussian integers $\mathbb{Z}[i]$

If $u \in \mathbb{Z}[i]$ is a unit then $N(u) = 1$. because $uv = 1$.

$$N(u)N(v) = 1.$$

$$\Rightarrow N(u) = 1.$$

Let $u = a + ib$ be an unit in $\mathbb{Z}[i]$

$$N(u) = 1 \Rightarrow a^2 + b^2 = 1.$$

$$\Rightarrow a = \pm 1, b = 0$$

$$\text{or } a = 0, b = \pm 1.$$

$\Rightarrow$ The units are ± 1 & $\pm i$.

Now we determine all prime ideals of $\mathbb{Z}[i]$.

Defn. A prime elt in $\mathbb{Z}[i]$ is called a gaussian prime.

Propn (1) If $N(a+ib) = a^2+b^2 = p$ is a prime no then $a+ib$ is a gaussian prime.

(2) If π is a gaussian prime then $N(\pi) = \pi\bar{\pi}$ is either a prime no or square of a prime number.

Pf: Let $\alpha = a+ib$. WTS α is a prime elt.

Since $\mathbb{Z}[i]$ is an ED so it is an UFD. here prime elt is equivalent to irreducible.

WTS α is irreducible.

Let $\alpha = \beta\nu$ where $\beta, \nu \in \mathbb{Z}[i]$.

Then $N(\alpha) = N(\beta)\,N(\nu) = p$

$\Rightarrow$ either $N(\beta)$ or $N(\nu)$ is 1.

Hence either β or ν is an unit.

Thus α is irreducible.

(2) Let π be a Gaussian prime.

Claim: $(\pi) \cap \mathbb{Z} = (p)$ for some prime no.

WTS $(\pi) \cap \mathbb{Z}$ which an ideal of $\mathbb{Z}$ is in fact a prime ideal.

Observe that $(\pi) \cap \mathbb{Z} \neq (0)$.

since $\pi\bar{\pi}$ is a non-zero integer.

Let $a, b \in \mathbb{Z}$ s.t $ab \in (\pi) \Rightarrow$ eithe

a or $b \in (\pi) \cap \mathbb{Z}$ as (π) is a prime ideal.

$\therefore$ $(\pi) \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and hence $(\pi) \cap \mathbb{Z} = (p)$.

Thus $p \in (\pi) \Rightarrow p = \pi\mu$.

$\therefore$ $N(\pi) N(\mu) = N(p) = p^2$.

$\Rightarrow$ $N(\pi) = p$ or p^2.

Thm. Let p be a prime integer.

TFAE

(1) $p = \pi\overline{\pi}$ where π is a Gaussian prime.

(2) $p = a^2 + b^2$ for some $a, b \in \mathbb{Z}$.

(3) $x^2 \equiv -1 \pmod{p}$ has an int soln

(4) $p = 2$ or $p \equiv 1 \pmod{4}$.

Pf: (1) $\Rightarrow$ (2) $p = \pi\bar{\pi}$ let $\pi = a+ib \in \mathbb{Z}[i]$

Then $\pi\bar{\pi} = (a+ib)(a-ib) = a^2+b^2$

$\therefore \quad p = a^2+b^2.$

(2) $\Rightarrow$ (3) If $p = a^2+b^2$ then $a, b \neq 0$.

Hence $a^2+b^2 \equiv 0 \pmod{p}$

$\Rightarrow a^2 \equiv -b^2 \pmod{p}.$

Since $\mathbb{Z}/p\mathbb{Z}$ is a field.

$\therefore \quad (ab^{-1})^2 \equiv -1 \pmod{p}.$

ab^{-1} is the solution of the eqn.

$x^2 \equiv -1 \pmod{p}.$

(3) $\Rightarrow$ (4). Let p be an odd prime.

Let $a \in \mathbb{Z}/p\mathbb{Z}$ s.t $a^2 \equiv -1 \pmod{p}$

Then $o(a) = 4$ in the multiplicative gp $(\mathbb{Z}/p\mathbb{Z})^\times$.

Hence $4 \mid p-1$.

$\Rightarrow p \equiv 1 \pmod 4$.

(4) $\Rightarrow$ (3). For $p = 2$, 1 is a soln of $x^2 \equiv -1 \pmod p$

Now let $p \neq 2$ and $p \equiv 1 \pmod 4$.

<u>claim</u>. $(\mathbb{Z}/p\mathbb{Z})^\times$ contains a unique elt of order 2.

If $m^2 \equiv 1 \pmod p \Rightarrow p \mid m^2 - 1$.

$\Rightarrow p \mid (m+1)(m-1) \Rightarrow p \mid m-1$ or $p \mid m+1$.

If $p \mid m-1 \Rightarrow m \equiv 1 \pmod{p}$.

If $p \mid m+1 \Rightarrow m \equiv -1 \pmod{p}$

So -1 is the unique residue class of order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Since $4 \mid p-1$. so $\exists$ a subgp of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$ say H.

either H is a Klein 4 gp or a cyclic gp of order 4.

But in Klein 4-gp there are 3 elts of order 2. but $(\mathbb{Z}/p\mathbb{Z})^\times$ has only one elt of order 2.

Hence H is a cyclic gp of order 4.

Hence $\exists$ an n^t a s.t $a^4 \equiv 1 \pmod{p}$.

Thus $a^2 \equiv -1 \pmod{p}$.

(3) $\Rightarrow$ (1). Note that $\mathbb{Z}[i] \cong \frac{\mathbb{Z}[x]}{(x^2+1)}$.

Let a be s.t $a^2 \equiv -1 \pmod{p}$.

$$\frac{\mathbb{Z}[i]}{p} \cong \frac{\mathbb{Z}[x]/(x^2+1)}{(p, x^2+1)/(x^2+1)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)}$$

as a is a soln of $x^2 \equiv -1 \pmod{p}$ $\Rightarrow$ a is a root of the eqn. $x^2+1 \equiv 0 \bmod p$

$$\cong \frac{\mathbb{Z}[x]/p}{(p, x^2+1))/p}$$

$$\cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{x^2+\bar{1}}$$

$$\cong \frac{\mathbb{Z}/p\mathbb{Z}[x]}{(x+a)(x-a)}.$$

Thus p is not irreducible.

Let π be an irreducible factor of p

$p = \pi\delta$ where δ is a non-unit.

$\therefore N(p) = N(\pi)\,N(\delta) = p^2$.

$\Rightarrow N(\pi) = p$. $\quad [\because N(\delta) \neq 1]$.

i.e $\pi\bar{\pi} = p$.

Cor. [Fermat's two square thm]

Let p be a prime no. Then p is a sum of two squares iff $p = 2$ or $p \equiv 1 \pmod 4$.

Cor. The irreducible elts of $\mathbb{Z}[i]$ are

(1) $(1+i^0)$ and its associates which has norm 2.

(2) prime integers p s.t $p \equiv 3 \pmod 4$.

(3) $a+ib$, $a-ib$ the distinct irreducible factors of $p = a^2+b^2$
$= (a+ib)(a-ib)$
for the prime p with $p \equiv 1 \pmod 4$.