Ring Theory

Lecture 24

Propn: 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

$\therefore (a,b) = (d)$

claim: $d = \gcd(a,b)$.

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

Let e be any elt s.t $e \mid a$ and $e \mid b$. **WTS** $e \mid d$.

$\because d \in (a,b)$

$\therefore d = ra + sb$ for some $r, s \in R$.

$$d = ra + sb$$
$$= rea_1 + seb_1 \quad \text{for some } a_1, b_1 \in R$$
$$= e(ra_1 + sb_1)$$

$\Rightarrow e \mid d$.

$\therefore d = \gcd(a, b)$.

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

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

Q what are the units in $\mathbb{Z}[i]$?

Let $u \in \mathbb{Z}[i]$ be a unit elt

$\exists\, v \in \mathbb{Z}[i]$ s.t $uv = 1$.

$$N(uv) = N(1) = 1.$$

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

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

If $u = a+ib$, $N(u) = a^2+b^2$.

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

Then $N(u) = a^2+b^2$.

$a^2+b^2 = 1 \Rightarrow$ either $\begin{cases} a = \pm 1 \\ b = 0 \end{cases}$ or $\begin{cases} b = \pm 1 \\ a = 0 \end{cases}$

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

Next 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 number then $a+ib$ is a gaussian prime.

(2) If π is a gaussian prime then $N(\pi) = \pi\bar{\pi}$ is either a prime number or square of a prime number.

Pf: (1) Let $\alpha = a+ib$ s.t

$N(\alpha) = a^2+b^2 = p$ a prime no.

WTS α is a prime elt in $\mathbb{Z}[i]$.

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

WTS α is irreducible elt.

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

Then $N(\alpha) = N(\beta)\,N(\gamma) = p$.

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

Hence either β or γ is an unit

$\therefore$ α is irreducible.

(2) Let π be a Gaussian prime

claim: $(\pi) \cap \mathbb{Z} = (p)$ where p is a prime no.

Since $\pi\bar{\pi}$ is a non-zero int

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

Note that $(\pi) \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ and hence

$$(\pi) \cap \mathbb{Z} = (p).$$

Thus $p \in (\pi) \Rightarrow p = \pi\mu$ where $\mu \in \mathbb{Z}[i]$.

p^2

$\Rightarrow N(p) = N(\pi)\, N(\mu)$

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

Thm Let p be a prime int. TFAE

(1) $p = \pi\bar{\pi}$ 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 $\pi\bar{\pi} = a^2+b^2 = p$.

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

Hence $4 \mid p-1$.

$\Rightarrow \quad p \equiv 1 \pmod{4}$.

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

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

claim $(\mathbb{Z}/p\mathbb{Z})^\times$ 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 $p \equiv 1 \pmod 4 \Rightarrow 4 \mid p-1$.

$$\left|(\mathbb{Z}/p\mathbb{Z})^\times\right| = p-1.$$

So $\exists$ a subgp of order 4 in $(\mathbb{Z}/p\mathbb{Z})^\times$ Say H.

either H is $\mathbb{Z}_2 \times \mathbb{Z}_2$ or H is cyclic gp of order 4.

But H can not be $\mathbb{Z}_2 \times \mathbb{Z}_2$ as there are 3 elts of order 2 in $\mathbb{Z}_2 \times \mathbb{Z}_2$ whereas H has one elt of order 2.

Hence H is a cyclic gp of order 4. Hence $\exists$ an elt a s.t

$$a^4 \equiv 1 \pmod{p}$$

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