LECTURE 32 Dec. 5/2003

Gaussian integers

$R := \mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$

$\delta(a+bi) = a^2+b^2 = (a+bi)(a-bi)$

makes $R=\mathbb{Z}[i]$ into a Euclidean domain:

$\beta = q\alpha + r$ w/ $\delta(r) < \delta(\alpha)$ or $r=0$.

① Every ideal $I \subset \mathbb{Z}[i]$ is principal
($I=(\alpha)$ w/ $\delta(\alpha)$ minimal)

Also if $I \neq (0)$, then $\mathbb{Z}[i]/I$ is a finite ring: so I has finite index in R.

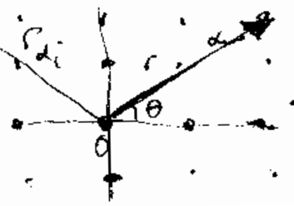
Pf) (of last assertion)
Assume $\alpha \neq 0$ in I; then $\alpha\bar{\alpha} = a^2+b^2 = n > 0$ is in I. $\underbrace{R \supset I \supset (n)}_{\boxed{\text{finite index } n^2}}$ $\therefore [R:I] < \infty$ too $\boxtimes$

[$\boxed{\text{Rmk}}$: this is true because
$(n) = \{na + nbi : a,b \in \mathbb{Z}\}$
$R/(n) = \{\overline{a+bi} : 0 \le a \le n,\ 0 \le b \le n\}$
$\uparrow$ n^2 elements (cosets).]

In fact: if $I=(\alpha)$ then $\#(R/I) = \delta(\alpha) = a^2+b^2$.

(Note: we've already shown this works when $\alpha = n \in \mathbb{Z}$.)

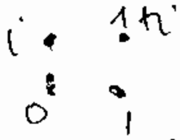
Pf) Write $\alpha = re^{i\theta}$ $r \in \mathbb{R}$, $\theta \in [0,2\pi)$.
Note: $\delta(\alpha) = r^2$. $\mathbb{Z}[i]$ looks like square lattice



what is αR?

$\leftarrow$ Look at example: $\alpha = 2+2i$, to get intuition.

So a fundamental domain for the quotient looks like basic box



scaled by r & rotated by θ. This new box has area r^2: i.e. r^2 elements of lattice fit into it $\boxtimes$.

② R has unique factorization into primes $\alpha = \underset{\uparrow \text{ unit}}{u} \cdot \underbrace{p_1 p_2 \cdots p_r}_{\text{primes}}$

p_i = prime in R, $R/\underset{\uparrow \text{ maximal ideal}}{(p)}$ = finite field

$\mathbb{Z}$: units $\mathbb{Z}^\times = \{\pm 1\}$
primes $2, 3, 5, 7, \ldots$

$R = F[X]$ (F field) units $R^\times = F^\times$ = nonzero polys of deg 0
primes: irreducible polynomials.

$F = \mathbb{C}$: $p(X) = X - \alpha \quad \alpha \in \mathbb{C}$
$F = \mathbb{R}$: $p(X) = \begin{cases} X - r & \text{or} \\ X^2 - rX + s \end{cases}$

$\delta : R \longrightarrow \mathbb{Z}_{\geq 0}$
$\alpha \longmapsto \alpha\bar{\alpha} = a^2 + b^2.$

Nice property: $\delta(\alpha\beta) = \delta(\alpha)\,\delta(\beta)$
(Check this in $\mathbb{C}$: $|\alpha\beta|^2 = |\alpha|^2 |\beta|^2$).

Claim: α is a unit $\iff \delta(\alpha) = 1$.

Pf) ($\Leftarrow$) $\delta(\alpha)=1$, then $\bar{\alpha}$ is a mult. inverse in R.

($\Rightarrow$) $\alpha \cdot \beta = 1$ for some β in R

$\delta(\alpha)\delta(\beta) = \delta(1) = 1$

$\Rightarrow \delta(\alpha) = 1$ ($\delta(\alpha)$ $\delta(\beta)$ are positive integers) $\boxtimes$.

What elements have $\delta(\alpha) = 1$?

$\alpha = a + bi$ has $\delta(\alpha) = 1 \iff$

$a = 0$, $b = \pm 1$ OR $a = \pm 1$, $b = 0$.

So: $R^\times = \{\pm 1, \pm i\}$.

Next question: What are the primes π of R?

$R/(\pi)$ is a finite field, so

$\#(R/(\pi)) = p^n$ for some $p \in \mathbb{Z}$, $n \geq 1$.

In fact: $R/(\pi)$ has order p or p^2, since $\mathbb{Z}/(p) \hookrightarrow R/(\pi) \Rightarrow$

$p \in (\pi) \Rightarrow \underbrace{(p) \subset (\pi) \subset R}_{\text{index } p^2}$

2 cases:

① $R/(\pi)$ has order p^2

Then $(\pi) = (p)$ by

So $\pi = u \cdot p$ & p is itself a prime in $\mathbb{Z}$ and R. (so $R/(p)$ is a field of order p^2)

② $R/(p)$ is not a field, so there are nontrivial ideals (π) between (p) and R.

These are generated by primes with $R/(\pi) \cong \mathbb{Z}/(p)$

Consequence

To each prime $\pi \in \mathbb{Z}[i]$ we can associate a rational prime p, and every rational prime occurs. p is already prime in $\mathbb{Z}[i]$ $\Leftrightarrow$ $\mathbb{Z}[i]/(p)$ is a field.

Study the ring $R/(p)$ for a prime p of $\mathbb{Z}$. Now

$$R/(p) = \mathbb{Z}[i]/(p) = \left(\mathbb{Z}[X]/(X^2+1)\right)/(p)$$

$$= \mathbb{Z}[X]/(X^2+1, p) = (\mathbb{Z}/(p))[X]/(X^2+1)$$

So this is a field $\Leftrightarrow$ X^2+1 is irreducible in $\mathbb{Z}/(p)[X]$.

$\Leftrightarrow$ X^2+1 has no roots in $\mathbb{Z}/p\mathbb{Z}$

$\Leftrightarrow$ we can't solve $X^2 \equiv -1 \pmod p$.

If $p=2$: $X^2+1 \equiv (X+1)^2$.

In this case, there is a unique prime $(1+i)$;

$R \underset{2}{\supsetneq} (\pi) \supset (2)$; $\delta(\pi) = a^2+b^2 = 2$

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

If $p \equiv 3 \pmod 4$: $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1 = 2\cdot\text{odd}$.

Then X^2+1 is irreduc. $\pmod p$ and $R/(p)$ is field (since $(\mathbb{Z}/p\mathbb{Z})^\times$ contains no elements of order 4!)

If $p \equiv 1 \pmod 4$:

Then X^2+1 factors as $(X-a)(X-b)$ $\pmod p$ where $a^2 \equiv -1 \pmod p$.

Why? $\#(\mathbb{Z}/p\mathbb{Z})^\times = p-1 = 2^k \cdot \text{odd}$
$k \geq 2$.

Thus Sylow 2-subgp has order 2^k, but the only elements of order 2 are ± 1. So there must be element(s) a of order 4 (mod p).

π s.t. $(\pi) = (p, i-a)$ &
π' s.t. $(\pi') = (p, i+a)$ are (up to units) the only primes s.t.
$\mathbb{Z}[i]/(\pi) \simeq \mathbb{Z}/(p)$.