# Math 538, Lecture 2, 12/1/2024

Last time: $\mathbb{Z}$, $\mathbb{Z}[i]$ both Euclidean domains; every $p \in \mathbb{Z}_{>0}$ (prime) factors in $\mathbb{Z}[i]$ as:

(1) $p = \pi\bar{\pi}$ if $p \equiv 1\ (4)$ split

(2) $p$ if $p \equiv 3\ (4)$ inert

(3) $2 = -i(1+i)^2$ if $p = 2$ ramified

Today: continue introduction

[Please send me an email so I have a mailing list for announcements: lior@math.ubc.ca]

HW: similar theory for $\mathbb{Z}[\omega]$, $\omega^2+\omega+1=0$

Let's examine $x^p + y^p = z^p \Leftrightarrow x^p - y^p = z^p$
p odd prime.

Let $\zeta = \zeta_p$ be a root of $\frac{x^p - 1}{x - 1} = 0$
So that

$$x^p - y^p = (x-y)(x-\zeta y)\cdots(x-\zeta^{p-1}y)$$

Study integral solutions $x, y, z$, but natural to calculate in $\mathcal{O} = \mathbb{Z}[\zeta]$. Eg. gcd:

$$(x - \zeta^j y, \ x - \zeta^k y)$$

If $\mathfrak{p}$ divides both, $\mathfrak{p}$ divides $\zeta^k y - \zeta^j y = \zeta^j(\zeta^{k-j} - 1)y$

similarly $\mathfrak{p}$ divides $\zeta^{j-k} x - x = \zeta^{j-k}(\zeta^{k-j} - 1)x$

Now may assume wlog that $(x, y) = 1$.

So $\mathfrak{p} \mid (\zeta^{k-j} - 1) = \dfrac{\zeta^{k-j} - 1}{\zeta - 1} \cdot (\zeta - 1)$

Observe $\dfrac{\zeta^{k-j} - 1}{\zeta - 1} \in \mathbb{Z}[\zeta]$

Also, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ acts transitively on $\{\zeta^j\}_{j=1}^{p-1}$.

$\Rightarrow$ For any $a, b \in (\mathbb{Z}/p\mathbb{Z})^\times$ $\quad \dfrac{\zeta^a - 1}{\zeta^b - 1}$ $\quad$ if $\sigma(\zeta^b) = \zeta$

$$\sigma\left(\frac{\zeta^a - 1}{\zeta^b - 1}\right) = \frac{\zeta^{a\bar{b}} - 1}{\zeta - 1} \in \mathbb{Z}[\zeta] \qquad b\bar{b} \equiv 1 \ (p)$$

So $\frac{\zeta^a - 1}{\zeta^k - 1}$ is a unit in $\mathbb{Z}[\zeta]$

(in fact $\mathbb{Z}[\zeta]^\times = \langle \{ \frac{\zeta^a - 1}{\zeta^k - 1} \mid a, k \not\equiv 0\ (p) \} \cup \{ \zeta^i \} \rangle$.

$\Rightarrow \quad \rho \mid \pi = 1 - \zeta$

Observe: $\quad \prod_{\sigma \in Gal} \sigma(1-\zeta) = \prod_{\sigma \in Gal} (1 - \sigma(\zeta)) = \prod_{j=1}^{p-1} (1 - \zeta^j)$

$$= \frac{x^p - 1}{x - 1} \Big|_{x=1} = \underbrace{1 + 1 + \dots + 1}_{p} = p$$

but $1 - \zeta^j,\ 1 - \zeta^k$ associate $\Rightarrow$ in $\mathbb{Z}[\zeta]$,
have

$$p = \pi^{p-1} \times (\text{unit})$$

and $\quad N^{\mathbb{Q}(\zeta)}_{\mathbb{Q}}\, \pi = p$

$\Rightarrow \pi$ irred: if $\rho \mid \pi$ then $N\rho \mid N\pi = p$
if $N\rho = \pm 1$ $\rho$ is a unit $\rho^{-1} = \pm \prod_{\sigma \neq id} \sigma(\rho)$.

if $N\rho = \pm p$ then $N(\frac{\pi}{\rho}) = \pm 1$, $\rho$ assoc. to $\pi$.

Check $\pi$ is prime: mod $\pi$ $\quad \zeta \equiv 1\ (\pi)$

Look at $(\pi) \subset \mathcal{O}$, $\mathbb{Z}$ surjects on $\mathcal{O}/(\pi)$
since image of $\zeta$ is in image of $\mathbb{Z}$

So $\mathcal{O}/(\pi) = \mathbb{Z}/\mathbb{Z}\cap(\pi)$ the ideal $\mathbb{Z}\cap(\pi)$
contains $p$ = multiple of $\pi$. It's not $(1)$ since
$\pi$ isn't a unit: $N\pi = p$.

$$\Rightarrow \mathcal{O}/(\pi) \cong \mathbb{Z}/p\mathbb{Z}$$

Back to our solution $x^p - y^p = z^p$

<u>Case 1:</u> $p \nmid x~~y~~z$

<u>Case 2:</u> $p \mid z$ (wlog)

<u>Case 1:</u> All the $x - \zeta^j y$ are relatively prime

From unique factorization have $\varepsilon \in \mathcal{O}^\times$, $t \in \mathcal{O}$
s.t.

$$x - \zeta y = \varepsilon t^p$$

But $\mathbb{Z}[\zeta]$ <u>not</u> a PID/UFD

If $\tau \in Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$ is complex conjugation

$\Rightarrow$

$$x - \zeta^{-1} y = \tau(\varepsilon)\,\tau(t)^p.$$

If $\sigma \in Gal$ then $\sigma\left(\frac{\tau(\varepsilon)}{\varepsilon}\right) = \frac{\sigma\tau(\varepsilon)}{\sigma(\varepsilon)} = \frac{\tau\sigma(\varepsilon)}{\sigma(\varepsilon)}$

because gp is commutative.

So $\left|\frac{\tau(\varepsilon)}{\varepsilon}\right| = 1$, similarly $\left|\sigma\left(\frac{\tau(\varepsilon)}{\varepsilon}\right)\right| = \underbrace{\left|\frac{\tau(\sigma(\varepsilon))}{\sigma(\varepsilon)}\right|}_{=1}$

$\Rightarrow \frac{\tau(\varepsilon)}{\varepsilon} \in \mathcal{O}$ has all conjugates of modulus 1

__Ex:__ $\Rightarrow \frac{\tau(\varepsilon)}{\varepsilon}$ is a root of unity

$\Rightarrow \frac{\tau(\varepsilon)}{\varepsilon} = \zeta^{-r}$ for some $r$.

Also (said above) $\exists a \in \mathbb{Z}$ st $t \equiv a \; (\pi)$

so $t^p - a^p \equiv (t-a)^p \quad (p)$

but $p \sim \pi^{p-1} \,/\, \pi^p \mid (t-a)^p$ so $t^p \equiv a^p \; (p)$

so $\tau(t^p) \equiv a^p \; (p)$

so $$x - \zeta^{-1} y = \zeta^{-r} \varepsilon\, \tau(t)^p \equiv \zeta^{-r} \varepsilon\, t^p \; (p)$$
$$\equiv \zeta^{-r}(x - \zeta y)$$

so if $\zeta^r = 1$ then $(\zeta - \zeta^{-1}) y \equiv 0 \; (p)$

$\Rightarrow \quad \pi^{p-1} \mid \zeta^{-1}(\zeta+1)\, \pi\, y$

$\Rightarrow \quad \pi^{p-2} \mid y \quad \Rightarrow \quad p \mid y$ not true by assumption

rearranging get $(1 \leq r \leq p-1)$:

$$\zeta^{r-1}(\zeta x - y) \equiv x - \zeta y \quad (p)$$

i.e. $(1-\pi)^{r-1}(x-y-\pi x) - (x-y+\pi y) \equiv 0 \quad (p)$

write as poly in $\pi$ ($\mathbb{Z}[\zeta] = \mathbb{Z}[\pi]$)

highest-order term is $\pi^r x$, not a multiple of $p$ (if $r \geq 2$) if $r=1$ get a contradiction

Case 2: $p \mid z$ so factors $(x-\zeta^j y)$ each divisible by $\pi$ so

$\dfrac{x-\zeta^j y}{\pi}$ relatively prime

$\vdots$

get smaller solution $(x')^p + (y')^p = (z')^p$

Proof fails: $\mathbb{Z}[\zeta]$ not UFD

motivates study of such rings.

Kummer noticed this issue, found solution:
bijection

$$\{a \in \mathbb{Z}\}/\mathbb{Z}^\times \leftrightarrow \left\{\begin{array}{c}\text{divisibility}\\ \text{conditions}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{subsets of } \mathbb{Z}\\ \text{closed}\\ \text{under } +,\\ \cdot \text{ by } \mathbb{Z}\end{array}\right\}$$

$\{n \in \mathbb{Z} : a \mid n\}$ : $a \mid n$ $a \mid m$
then $a \mid (xn+m)$
for all $x \in \mathbb{Z}$

but in ring $\mathcal{O} = \mathbb{Z}[\zeta]$ (and others) there are "divisibility conditions" not of this form

Kummer called them "ideal numbers"

<u>Thm:</u> Unique factorization holds for ideal numbers.

---

Different example: if $E: y^2 = x^3 + ax + b$, $a,b \in \mathbb{Z}$

is a nonsingular cubic, typically $\mathrm{End}(E) \cong \mathbb{Z}$

sometimes, $\mathrm{End}(E) \cong \mathbb{Z}[\alpha]$, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$,
$\alpha \notin \mathbb{R}$

---

On $\mathbb{Z}/p\mathbb{Z} \cong \mathcal{O}/(\pi)$

mod $\pi$, $\zeta \equiv 1$ $\quad (\pi = \zeta - 1)$

so image of $a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-2}\zeta^{p-2}$
mod $\pi$ is same as that of
$a_0 + a_1 + a_2 + \cdots + a_{p-2} \in \mathbb{Z}$

$\Downarrow$

map $\mathbb{Z} \hookrightarrow \mathcal{O} \twoheadrightarrow \mathcal{O}/(\pi)$ is surjective.

Kernel is an ideal of $\mathbb{Z}$; contains $p$ $(\pi \mid p)$
so $\mathbb{Z} \neq \mathrm{Ker} \supseteq (p)$ : $1 \notin (\pi)$

so $\mathrm{Ker} = (p)$ so get isom $\mathbb{Z}/p\mathbb{Z} \xrightarrow{\sim} \mathcal{O}/(\pi)$

# Chapter 1: Rings of integers

**Def:** A number field is a finite extension of $\mathbb{Q}$.

Fix a # field $K$, let $n = [K:\mathbb{Q}]$, its degree.

**Def:** An element $\alpha \in K$ is an algebraic integer if $p(\alpha)=0$ for some non-zero monic polynomial $p \in \mathbb{Z}[x]$ ("monic" = top coeff is 1)

**Def:** The maximal order / ring of integers of $K$ is the set $\mathcal{O}_K$ of algebraic integers in $K$

**Lemma:** $\alpha \in K$ is an algebraic integer iff its minimal polynomial is in $\mathbb{Z}[x]$

always assumed monic

**Pf:** Let $m \in \mathbb{Q}[x]$ be the min. poly. of $\alpha$.
If $m \in \mathbb{Z}[x]$, $\alpha$ is integral
If $\alpha$ is integral, evinced by $p \in \mathbb{Z}[x]$, $m | p$ in $\mathbb{Q}[x]$ by minimality of $m$, then $m \in \mathbb{Z}[x]$ by Gauss's lemma.

Example: $K = \mathbb{Q}$. The min poly of $\alpha \in \mathbb{Q}$ is $x - \alpha$

so $\alpha$ is an alg. integer iff $\alpha \in \mathbb{Z}$

("rational root thm")

$\boxed{\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}}$

Examples $K = \mathbb{Q}(i)$ min poly of $a+bi$ $(b \neq 0)$

is

$$(x-a+bi)(x-a-bi) = (x-a)^2 + b^2$$
$$= x^2 - (2a)x + (a^2+b^2)$$

so $\alpha = a+bi \in \mathcal{O}_K$ iff $2a,\ a^2+b^2 \in \mathbb{Z}$

$\Rightarrow a \in \frac{1}{2}\mathbb{Z} \Rightarrow 4b^2 \in \mathbb{Z} \Rightarrow 2b \in \mathbb{Z} \Rightarrow b \in \frac{1}{2}\mathbb{Z}$

If $a \in \mathbb{Z} \Rightarrow b \in \mathbb{Z}$ $\alpha = a+bi \in \mathbb{Z}[i]$

If $a \notin \mathbb{Z}$: $(2a)^2 + (2b)^2 \in 4\mathbb{Z}$

$2a$ odd $\Rightarrow (2a)^2 \equiv 1\ (4)$ $\qquad 1+0,\ 1+1 \not\equiv 0\ (4)$

$2b \in \mathbb{Z} \Rightarrow (2b)^2 \equiv 0, 1\ (4)$

$\Rightarrow \Leftarrow$.

$\Rightarrow \mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i]$

order in $\mathbb{Q}(\sqrt{-3})$

Example: $\mathbb{Z}[\sqrt{-3}] \subset \mathcal{O}_{\mathbb{Q}(\sqrt{-3})}$

Pf: $(x - a - b\sqrt{-3})(x - a + b\sqrt{-3})$

$= (x-a)^2 + 3b^2 \in \mathbb{Z}[x]$ if $a, b \in \mathbb{Z}$

But $\left(x - \frac{-1+\sqrt{-3}}{2}\right)\left(x - \frac{-1-\sqrt{-3}}{2}\right)$

$= x^2 + x + 1 \in \mathbb{Z}[x]$