Math 530: Algebraic Number Theory

Urbana, Spring 2009

→ Handout syllabus. ← 19 currently enrolled

This course is about: Number fields: finite extensions K of $\mathbb{Q}$. e.g. $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\zeta_n)$

and their

alg #, sat a poly with rat'l coeff.

Rings of integers: $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}\Big[\underbrace{\tfrac{1+\sqrt{5}}{2}}_{=\varphi \text{ where } \varphi^2-\varphi-1=0}\Big]$

like $\mathbb{Z}$ for $\mathbb{Q}$, though some things are different, e.g. unique factorization may fail.

Beyond their intrinsic interest, also provide a nat'l context to study elementary questions about $\mathbb{Z}$ (e.g. F.L.T.) $x^n+y^n=z^n$

Personal interest: Applications to topology/geometry.

Today: Gaussian integers $\mathbb{Z}[i] = \{a+bi \mid a,b\in\mathbb{Z}\}$, $i^2=-1$

Thm An odd prime in $\mathbb{Z}$ is of the form $p=a^2+b^2$ for $a,b\in\mathbb{Z}$ iff $p\equiv 1 \bmod 4$

E.g. $5=1^2+2^2$, $13=3^2+2^2$, $17=1^2+4^2$

($\Rightarrow$) is clear as $a^2\equiv 0,1 \bmod 4$.

Connection: $p = a^2 + b^2 = (a+bi)(a-bi) \Rightarrow p$ factors in $\mathbb{Z}[i]$ (is not irreducible)

no zero divisors

[Recall: in an integral domain R, two key notions:
irreducible — not a product of non-units.
prime — $p \mid ab \Rightarrow p \mid a$ or $p \mid b$

cf. $(2+\sqrt{-5})(2-\sqrt{-5}) = 9$
$\Rightarrow 3$ is irred but not prime in $\mathbb{Z}[\sqrt{-5}]$]

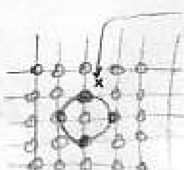
Lemma: $\mathbb{Z}[i]$ is a unique factorization domain.

norm is mult.
$N(\alpha\beta) = N(\alpha)N(\beta)$

Pf: $\mathbb{Z}[i]$ is Euclidean w.r.t. $\alpha = a+bi \longrightarrow N(\alpha) = |\alpha|^2 = a^2+b^2$.

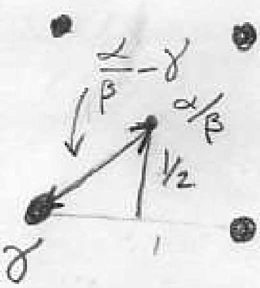
That is, given $\beta \neq 0$ in $\mathbb{Z}[i]$ there are γ, ρ in $\mathbb{Z}[i]$ where

$$\alpha = \gamma\beta + \rho \text{ with } N(\rho) < N(\beta)$$

Reason: 

$\frac{\alpha}{\beta}$ Take γ in $\mathbb{Z}[i]$ closest to $\frac{\alpha}{\beta}$, and set $\rho = \alpha - \gamma\beta$. Then

$$N(\rho) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) \leq N(\beta)\frac{1}{2} < N(\beta)$$



Pf of Thm. $p \equiv 1 \bmod 4 \Rightarrow p = a^2+b^2$

Claim: Suffices to show p factors in $\mathbb{Z}[i]$

Reason: If $p = \alpha\beta$ for non-units α, β then

$$p^2 = N(p) = N(\alpha)N(\beta) \text{ where } N(\alpha), N(\beta) \neq 1 \Rightarrow$$

$p = N(\alpha) = a^2+b^2$.

Pf of Claim: Over $\mathbb{Z}$, the equation $-1 \equiv x^2 \bmod p$ has a solution, namely $x = \left(\frac{p-1}{2}\right)!$ (*) Thus $p \mid x^2+1$.

If p is irreducible it is prime as $\mathbb{Z}[i]$ is a U.F.D.

Then $p \mid \left(x^2+1 = (x+i)(x-i)\right) \Rightarrow p \mid (x+i)$ or $p \mid (x-i)$ which is a contradiction. So p factors proving the claim. $\blacksquare$

(*) Details: $p = 4n+1$, $x = 2n$. Recall that Wilson's Theorem says $-1 \equiv (p-1)! \bmod p$

$$= (1 \cdot 2 \cdots 2n)\left[(p-2n) \cdots (p-2)(p-1)\right] \bmod p$$

$$= ((2n)!)^2 (-1)^{2n} \bmod p = (2n)! \bmod p.$$

Properties of $\mathbb{Z}[i]$:

Units = elts of norm 1 = $\{\pm 1, \pm i\}$

Primes: (up to units)

① $\pi = 1+i$

② $\pi = a+bi$ with $a > |b| > 0$ and $N(\pi) = p \equiv 1 \bmod 4$ (rat'l prime)

③ $\pi = p$ with $p \equiv 3 \bmod 4$

Pf: That (1)–(3) are prime is easy: (1–2) prime norm is prime
(3) not prime $\Rightarrow p = a^2 + b^2 \Rightarrow$ ✗.

Conversely, suppose π is prime. Then

$$N(\pi) = \pi \cdot \bar{\pi} = p_1 \cdot \cdots \cdot p_r \quad \text{for } p_i \in \mathbb{Z} \text{ prime.}$$

$\Rightarrow \pi \mid p_i$ for some i $\Rightarrow N(\pi) \mid N(p_i) = p_i^2 \Rightarrow$

$N(\pi) = p \Longrightarrow$ case (1) or (2)

or

$N(\pi) = p^2 \Longrightarrow$ case (3) as $\pi\bar{\pi} = p^2 \overset{\text{as } \pi \text{ is prime}}{\Longrightarrow} \pi \mid p \Rightarrow \underbrace{\frac{p}{\pi}}_{\substack{\text{norm } 1 \\ \text{so a unit}}} \in \mathbb{Z}[i]$

$\Rightarrow \pi = (\text{unit})\, p.$ ▨

What happens to primes in $\mathbb{Z}$ in $\mathbb{Z}[i]$:

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

(2) $p \equiv 1 \bmod 4$ then $p = \pi\bar{\pi}$ where $\pi, \bar{\pi}$ are the two
"split." kinds of primes of norm p.

(3) $p \equiv 3 \bmod 4$ then p is prime in $\mathbb{Z}[i]$
"inert."

Analogy: $\mathbb{Z}$ is to $\mathbb{Q}$ as $\mathbb{Z}[i]$ is to $\mathbb{Q}[i]$ as...

<u>Prop</u>: $\mathbb{Z}[i]$ = those elts of $\mathbb{Q}[i]$ sat. <u>monic</u> poly. equations $x^2 + ax + b = 0$ for $a, b \in \mathbb{Z}$.

<u>Pf</u>: If $\alpha = c + di$ is a root of ↶ then $a = -2c$ and $b = c^2 + d^2$.
If $a, b \in \mathbb{Z}$, then $2c$ and $2d \in \mathbb{Z}$. Then $(2c)^2 + (2d)^2 = 4b \equiv 0 \bmod (4)$
$\Rightarrow (2c)^2 \equiv (2d)^2 \equiv 0 \bmod 4 \Rightarrow c, d \in \mathbb{Z}$.