

What is so ideal about the ideal class group?

What is FLT?

$$x^n + y^n = z^n \text{ has no }^{\text{(non-trivial)}} \text{ solutions } (x, y, z) \in \mathbb{Z} \setminus \{0\}$$

$n \geq 3$

Proof? In mid-nineties, by a student of William Taylor - Fermat was a pioneer of the field of Number theory but never really published much.

Kummer

$n=4$, Fermat used "infinite descent"

$n=3$, Euler gave 'proof'

1847 - there was proof for all integers by Gabriel Lamé.

Proved that for $(x, y, z) \in \mathbb{Z} \setminus \{0\}$ $x^p + y^p = z^p$

$$f(x) = x^p + y^p \in \mathbb{Z}[x]$$

where is the solution?

They lie in $\mathbb{Q}(\zeta_p)$ where ζ_p is a primitive p -th root of unity


So $= \gamma, -\zeta_p \gamma, \dots, \zeta_p^{p-1} \gamma$ we can

write factorization for polynomial.

$$f(x) = \prod_{i=0}^{p-1} (x + \zeta_p^i \gamma)$$

Note that $x^p + y^p = z^p$

and $f(x) = \prod_{i=0}^{p-1} (x + \zeta_p^i y)$ in $\mathbb{Z}[\zeta_p]$

Q:  is this an Unique Factorization Domain?

Answer: Rarely

(UFD)

Algebraic Number Theory:

- algebraic # field.

ex: \mathbb{Q}, \mathbb{R}

- K/\mathbb{Q} "over" - finite extension of \mathbb{Q}
means dimension is finite.

- Examples

a) $\mathbb{Q}(\zeta_n)$, ~~how~~ how do we know this is finite?
- cyclotomic field

b) $\mathbb{Q}(\sqrt{d})$, $d \neq 1$
- quadratic field.

c) $\mathbb{Q}(\sqrt[3]{a})$

The collection of algebraic integers.

• $\alpha \in K$ is "alg. integer"

if it satisfies a monic poly. in $\mathbb{Z}[x]$

• Ex: $\sqrt{3}$ satisfies $(x^2 - 3)$, ζ_p , $\sqrt{-1}$

• nonex: $\frac{1}{2}$, $\frac{\sqrt{-1}}{2}$, $\frac{5}{4}$, π

" \mathcal{O}_K " (ring of integers in K)

- its an integral domain with fraction field K .

- free \mathbb{Z} -module of rank $[K:\mathbb{Q}]$

means as an abelian group, $\mathcal{O}_K \cong \mathbb{Z}^{[K:\mathbb{Q}]}$

- every prime ideal of \mathcal{O}_K is maximal

Defn: $P \subseteq \mathcal{O}_K$ $ab \in P$ if $a \in P$ or $b \in P$

ex: $2\mathbb{Z}, 3\mathbb{Z}, 5\mathbb{Z}, \dots, p\mathbb{Z}$ for any rational prime.

- \mathcal{O}_K is Noetherian -

ex: $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & d \equiv 2, 3 \pmod{4} \\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d \equiv 1 \pmod{4} \end{cases}$$

$$\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n] \text{ (hard to prove)}$$

If \mathcal{O}_K a UFD/PID?

NOT ALWAYS

Consider: $\mathbb{Q}(\sqrt{-5}), \mathbb{Z}[\sqrt{-5}]$

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}) \text{ so not unique factorization.}$$

$(2, 1 + \sqrt{-5})$ not principal ideal either.

- Fractional ideal of \mathcal{O}_K is a nonzero f.g.

\mathcal{O}_K - submodule of K

ex: $\mathbb{Z}[\frac{1}{2}]$

- a fractional ideal is called principal if it has one generator.

Suppose I, J are fractional ideals so we can mult. together as:

$$IJ = \left\{ \sum_{i=1}^n x_i y_i \mid x_i \in I, y_i \in J \right\}.$$

It turns out that $I(\mathcal{O}_K)$ is a group w/o inverses(?)

- The identity element is \mathcal{O}_K or the group generated by 1, (monoid)

- Every fractional ideal of \mathcal{O}_K is invertible.

Define the subgroup $\mathcal{P}(\mathcal{O}_K) = \{ \text{principal fractional ideals} \}$
normal.

So we can form the quotient $I(\mathcal{O}_K) / \mathcal{P}(\mathcal{O}_K)$

this is the ideal class group.

Thm: Every ideal of \mathcal{O}_K is uniquely a product of prime ideals.

$$\mathcal{I} = \prod \mathfrak{p}_i^{e_i} \dots \prod \mathfrak{p}_g^{e_g} \quad \text{"ideals" "numbers"}$$

Thm: $\text{Pic}(\mathcal{O}_K)$ is finite
Picard (?)

$$\# \text{Pic}(\mathcal{O}_K) = h_K$$

Thm: The following are equivalent:

- (i) $h_K = 1$
- (ii) \mathcal{O}_K is a PID
- (iii) \mathcal{O}_K is a UFD.

Quadratic imaginary fields: $\mathbb{Q}(\sqrt{-d})$, $d > 1$, \square -free.

$h_K = 1$ exactly 9 times.

(Proved by Kurt Heegner, 60's)

- $\mathbb{Q}(\zeta_p)$ has class #1 iff $p \leq 19$.

So back to Fermat Last Theorem, $x^p + y^p = z^p$

$$p \nmid xyz$$

$$z^p = \prod_{i=0}^{p-1} (x + \zeta_p^i y) \text{ in } \mathbb{Z}[\zeta_p]$$

Not a UFD but is a Dedekind domain

$$\text{So } z^p = (x + \zeta_p y).$$

P is regular if P does not divide the order of the ideal class group
i.e. $P \nmid h(\mathbb{F}_p)$

Let $[I] \in \text{Pic}(\mathcal{O}_K)$

$$[I]^P = 1$$

$$[I] = 1$$

If two principal ideals are equal, then their generators associate
or differ by a unit

So we conclude $\alpha^P = x + \mathfrak{f}_P \gamma$

where $(\alpha)^P = \mathfrak{I}^P = (x + \mathfrak{f}_P \gamma)$