不定方程相关理论及其应用

郑欢誉

2025 年 4 月 15 日

中期报告目录

Contents of Interim Report

研究内容和目标 Research Contents & Object
当前进展 Current Progress
未来计划 Future Plan

中期报告目录

Contents of Interim Report

研究内容和目标 Research Contents & Object
当前进展 Current Progress
未来计划 Future Plan

中期报告目录

Contents of Interim Report

研究内容和目标 Research Contents & Object
当前进展 Current Progress
未来计划 Future Plan

研究内容和目标

Research Contents & Object

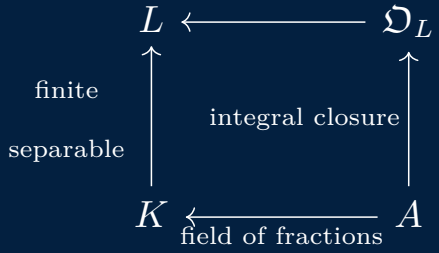
$$x^n + y^n = z^n$$

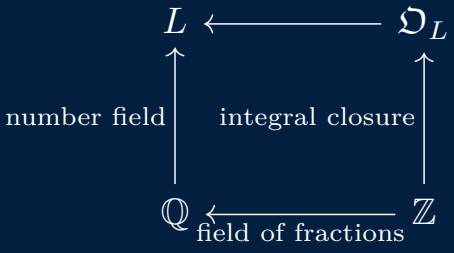
当 $n \geq 3$ 为正规素数 时，方程没有非零整数解 (x, y, z)

1. FLT & ABC 猜想（ABC $\Longrightarrow$ FLT，ABC 猜想次指数界改良）
2. 渐进费马大定理（Asymptotic Fermat's Last Theorem）
3. 正规素数情况的形式化

当前进展

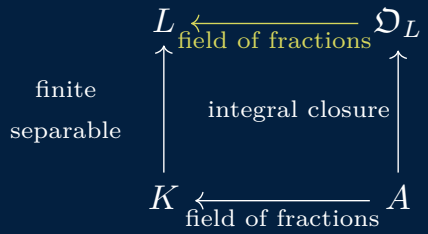
Current Progress





当前进展

Current Progress



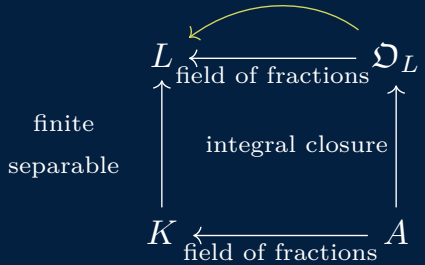
$\mathfrak{O}_L$:

1. forms a ring
2. (when A is PID) finitely generated A-module

当前进展

Current Progress

integral basis is a K-basis for L

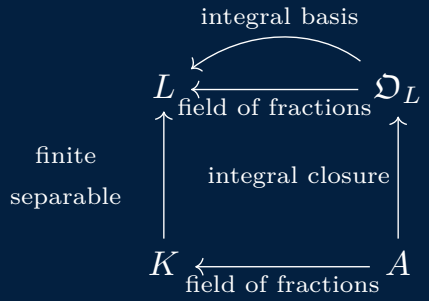


$\mathfrak{O}_L$:

1. forms a ring
2. (when A is PID)
   finitely generated A-module

当前进展

Current Progress

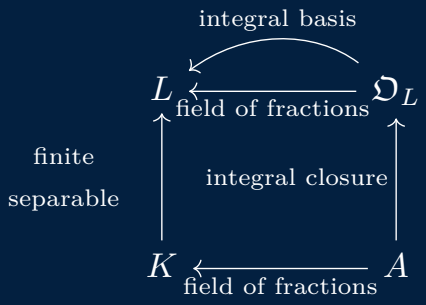


$\mathfrak{O}_L$:

1. forms a ring
2. (when A is PID) finitely generated A-module
3. Noetherian ($\Rightarrow$ factorization of ideal into irreducibles)

当前进展

Current Progress



$\mathfrak{O}_L$:

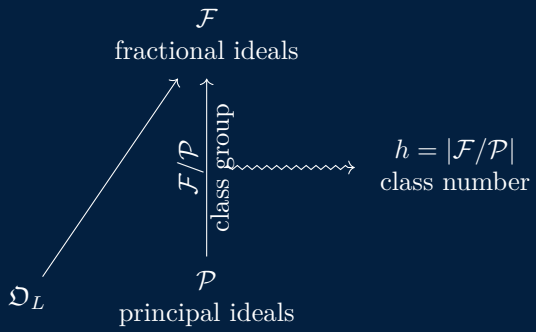
1. forms a ring
2. (when A is PID) finitely generated A-module
3. Noetherian ($\Rightarrow$ factorization of ideal into irreducibles)
4. Dedekind
   ($\Rightarrow$ fractional ideal, inverse of ideal)
   ($\Rightarrow$ unique prime factorization of ideal)

当前进展

Current Progress

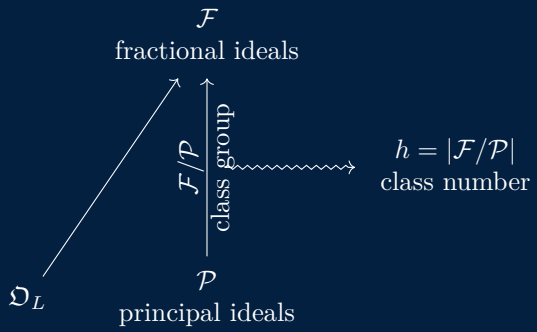
$\mathfrak{O}_L$:

1. forms a ring
2. (when A is PID) finitely generated A-module
3. Noetherian ($\Rightarrow$ factorization of ideal into irreducibles)
4. Dedekind
   ($\Rightarrow$ fractional ideal, inverse of ideal)
   ($\Rightarrow$ unique prime factorization of ideal)



当前进展

Current Progress



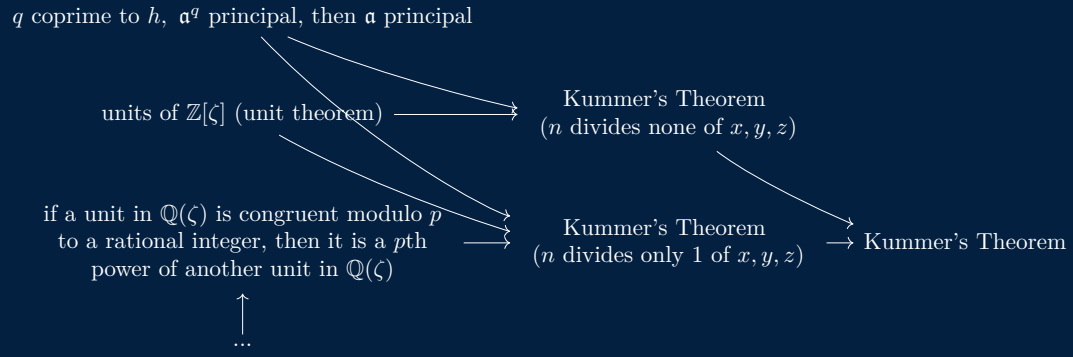
Minkowski's Theorem

$\Rightarrow$class number finite

$\Rightarrow q$ coprime to h, $\mathfrak{a}^q$ principal, then $\mathfrak{a}$ principal

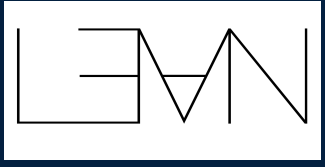
当前进展

Current Progress



当前进展

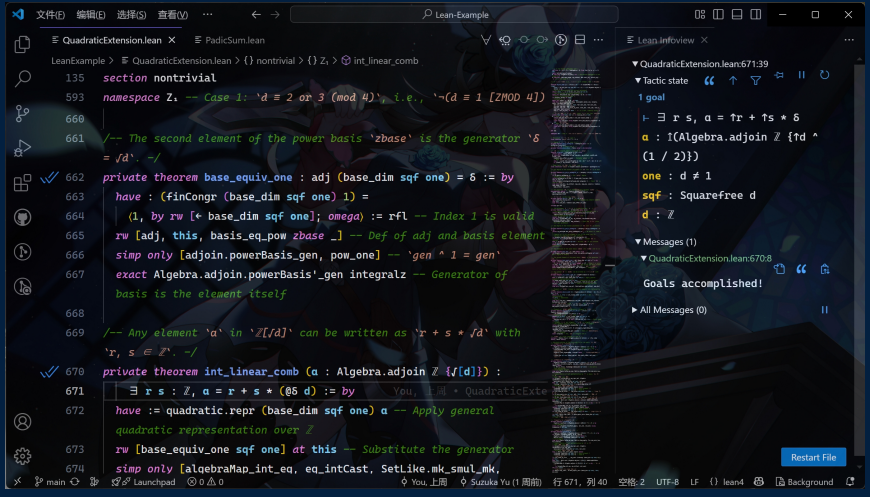
Current Progress



Lean is an interactive theorem prover based on dependent type theory, designed for use both in cutting-edge mathematics and in software verification.

当前进展

Current Progress



当前进展

Current Progress

```
1  def hello : IO Unit := IO.println "Hello, world!"
2
3  theorem bogus : False := by sorry
```

当前进展

Current Progress

相关实验：

1. (1300 行) The discriminate of a quadratic extension $\mathbb{Q}(\sqrt{d})$, where d is a square free integer is
$$\begin{cases} d, & d \equiv 1 \ (mod\ 4) \\ 4d, & d \not\equiv 1 \ (mod\ 4) \end{cases}$$
2. (100 行) Every epimorphism of Grps is the coequalizer of two homomorphisms.
3. (200 行) Every monomorphism of Grps is the equalizer of two homomorphisms.
4. (200 行) Let $0 \neq x \in \mathbb{Q}$. $|x|(\prod_{p \text{ prime}} |x|_p) = 1$

未来计划

Future Plan

1. FLT & ABC 猜想（ABC $\Longrightarrow$ FLT，ABC 猜想次指数界改良）
2. 渐进费马大定理（Asymptotic Fermat's Last Theorem）
3. 正规素数情况的形式化


1896
XI'AN JIAOTONG UNIVERSITY