

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

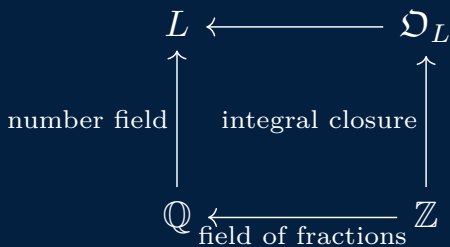
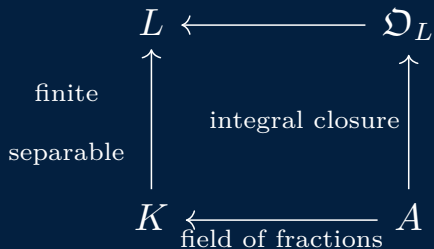
$$x^n + y^n = z^n$$

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 ($ABC \implies FLT$, 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

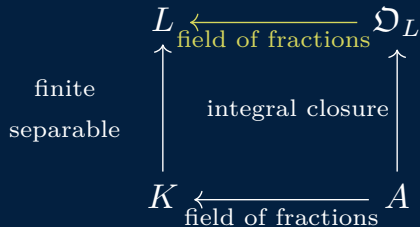
当前进展

Current Progress



当前进展

Current Progress



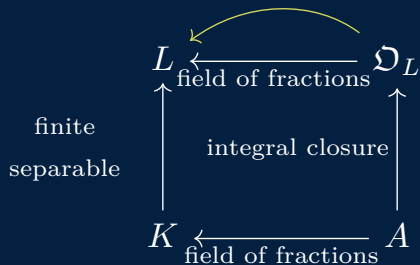
\mathcal{O}_L :

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 ←

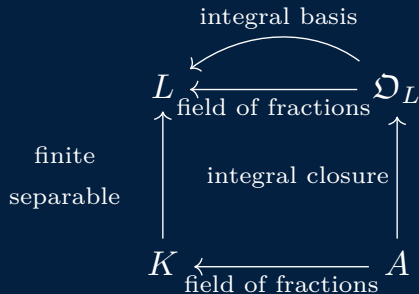


\mathfrak{O}_L :

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

当前进展

Current Progress

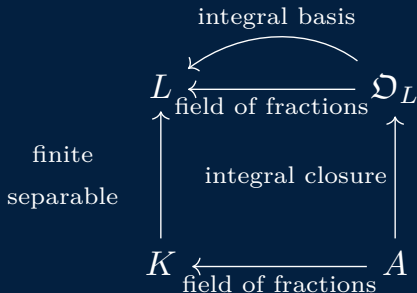


\mathfrak{O}_L :

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



\mathcal{O}_L :

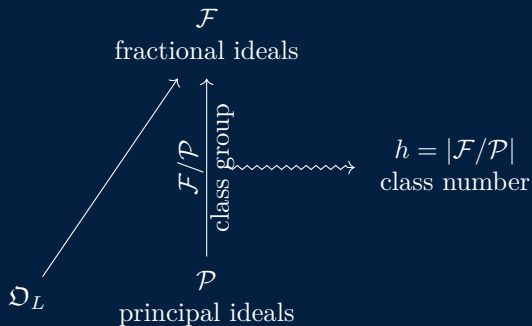
1. forms a ring
2. (when A is PID) finitely generated A -module
3. Noetherian (\Rightarrow factorization of ideal into irreducibles)
4. **Dedekind**
(\Rightarrow fractional ideal, inverse of ideal)
(\Rightarrow unique prime factorization of ideal)

当前进展

Current Progress

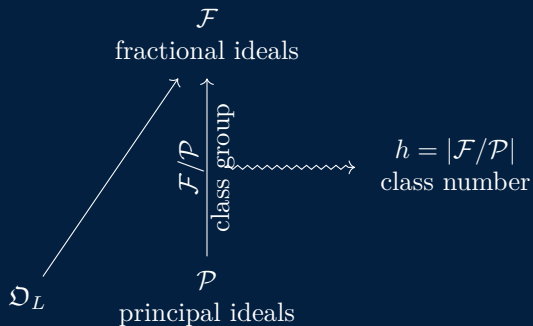
\mathfrak{D}_L :

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 , α^q principal,
then α principal

当前进展

Current Progress

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

units of $\mathbb{Z}[\zeta]$ (unit theorem)

if a unit in $\mathbb{Q}(\zeta)$ is congruent modulo p
to a rational integer, then it is a p th
power of another unit in $\mathbb{Q}(\zeta)$

↑
...

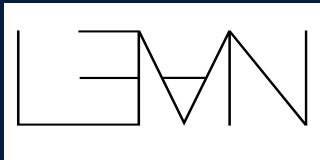
Kummer's Theorem
(n divides none of x, y, z)

Kummer's Theorem
(n divides only 1 of x, y, z)

→ Kummer's Theorem

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

```
135 section nontrivial
593 namespace Z, -- Case 1: 'd ≡ 2 or 3 (mod 4)', i.e., '¬(d ≡ 1 [ZMOD 4])'
660
661 /-- The second element of the power basis 'zbase' is the generator 'δ
= √d'. -/
662 private theorem base_equiv_one : adj (base_dim sqf one) = δ := by
663   have : (finCongr (base_dim sqf one) 1) =
664     (1, by rw [← base_dim sqf one]; omega) := rfl -- Index 1 is valid
665   rw [adj, this, basis_eq_pow zbase _] -- Def of adj and basis element
666   simp only [adjoin.powerBasis_gen, pow_one] -- 'gen ^ 1 = gen'
667   exact Algebra.adjoin.powerBasis'_gen integralz -- Generator of
        basis is the element itself
668
669 /-- Any element 'a' in 'Z[√d]' can be written as 'r + s * √d' with
        'r, s ∈ Z'. -/
670 private theorem int_linear_comb (a : Algebra.adjoin Z {√d}) :
671   ∃ r s : Z, a = r + s * (√d) := by
672     have := quadratic.repr (base_dim sqf one) a -- Apply general
        quadratic representation over Z
673     rw [base_equiv_one sqf one] at this -- Substitute the generator
674     simp only [algebraMap_int_eq, eq_intCast, SetLike.mk_smul_mk,
```

Lean-Example

Lean Infoview

▼ QuadraticExtension.lean:671:39

▼ Tactic state

1 goal

├ ∃ r s, a = r + s * δ

a : i(Algebra.adjoin Z {√d} (1 / 2))

one : δ ≠ 1

sqf : Squarefree δ

d : Z

▼ Messages (1)

▼ QuadraticExtension.lean:670:8

Goals accomplished!

► All Messages (0)

Restart File

main Launchpad 0 0

You, 上周 Suzuki Yu (1 周前) 行 671, 列 40 空格: 2 UTF-8 LF {} lean4 Background

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 discriminant of a quadratic extension $\mathbb{Q}(\sqrt{d})$, where d is a square free integer is

$$\begin{cases} d, & d \equiv 1 \pmod{4} \\ 4d, & d \not\equiv 1 \pmod{4} \end{cases}$$

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 ($ABC \implies FLT$, 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

