初等整数論の形式化

−代数学の形式化の充実に向け−

渡瀬　泰成

内容

- 代数学の形式化の現状
  - 形式化の整備の必要性
- 初等整数論への期待
  - 形式化のよき練習問題
    - 帰納法
    - 背理法
    - 部屋割り論法
  - 形式化固有の概念の理解
    - 素因数分解に現れるMany Sorted Set
  - Mizar 普及への貢献

形式化の現状(多項式環の例)

基本事項	キーワード	形式化の有無
1. 多項式の定義	整式、単項式、冪級数	有
2. 環構造	環の演算、	環構造のみ
	同型定理、	有
3. 一変数多項式の素元分解	剰余定理、組立除法、既約、アイゼンシュタイン判定	無
	因数定理	有
4. 方程式	対称式、根の置換、根の対称式、判別式、終結式、消去法	無
	円分多項式	有
5. 多項式のイデアル論	素イデアル、零点定理、整元、正規化定理、局所化	無
	素イデアルの列、アルチン環、根基、零化イデアル	無
	ヒルベルトの基底定理、グレーブナ基底、S-多項式	有

課題の設定

代数学の基本定理は形式化されている。POLYNOM5

$f \in \mathbb{C}[X]$ が定数でなければ少なくとも $\mathbb{C}$ 中 1 つの零点をもつ。

だが、その一般化であるHilbertの零点定理は形式化されていない！

$f_1, f_2, \cdots, f_r \in \mathbb{C}[X_1, X_2, \cdots, X_n]$ が $< f_1, f_2, \cdots, f_r > \neq 1$ ならば $\mathbb{C}^n$ 中少なくとも 1 組の共通零点をもつ。

零点定理の証明は色々ある。

- Zariski 1947
- Kaplansky 1974
- Arrondo 2006

“Another Elementary Proof of the Nullstellensatz”, THE MATHEMATICAL ASSOCIATION OF AMERICA Monthly 113, pages 169-171,2006

- **閉体のモデル完全性によるモデル論的証明**

形式化の準備が最短なものを探求せよ！形式化の工夫

The Hundred Greatest Theorems の例

1	The Irrationality of the Square Root of 2	Pythagoras and his school	500 B.C.
2	Fundamental Theorem of Algebra	Karl Frederich Gauss	1799
3	The Denumerability of the Rational Numbers	Georg Cantor	1867
4	Pythagorean Theorem	Pythagoras and his school	500 B.C.
5	Prime Number Theorem	Jacques Hadamard and Charles-Jean de la Vallee Poussin (separately)	1896
6	Godel's Incompleteness Theorem	Kurt Godel	1931
7	Law of Quadratic Reciprocity	Karl Frederich Gauss	1801
8	The Impossibility of Trisecting the Angle and Doubling the Cube	Pierre Wantzel	1837
9	The Area of a Circle	Archimedes	225 B.C.
10	Euler's Generalization of Fermat's Little Theorem (Fermat's Little Theorem)	Leonhard Euler (Pierre de Fermat)	1760 (1640)
11	The Infinitude of Primes	Euclid	300 B.C.
12	The Independence of the Parallel Postulate	Karl Frederich Gauss, Janos Bolyai, Nikolai Lobachevsky, G.F. Bernhard Riemann collectively	1870-1880
13	Polyhedron Formula	Leonhard Euler	1751
14	Euler's Summation of 1 + (1/2)^2 + (1/3)^2 + ….	Leonhard Euler	1734
15	Fundamental Theorem of Integral Calculus	Gottfried Wilhelm von Leibniz	1686
16	Insolvability of General Higher Degree Equations	Niels Henrik Abel	1824
17	DeMoivre's Theorem	Abraham DeMoivre	1730
18	Liouville's Theorem and the Construction of Trancendental Numbers	Joseph Liouville	1844
19	Four Squares Theorem	Joseph-Louis Lagrange	1770
20	All Primes Equal the Sum of Two Squares	?	?
21	Green's Theorem	George Green	1828
22	The Non-Denumerability of the Continuum	Georg Cantor	1874
23	Formula for Pythagorean Triples	Euclid	300 B.C.
24	The Undecidability of the Coninuum Hypothesis	Paul Cohen	1963
25	Schroeder-Bernstein Theorem	?	?

Freek Wiedijk氏のリストによるProverの比較

http://www.cs.ru.nl/~freek/100/index.html

Mizar, Takashi Mitsuishi & Noboru Endou & Keiji Ohkubo: statement
Isabelle, Jacques D. Fleuriot: statements
Coq, contrib, Frédérique Guilhot: statement
ProofPower, Rob Arthan: statement

18. **Liouville's Theorem and the Construction of Transcendental Numbers**
    HOL Light, John Harrison: statements
    Coq, C-CoRN, Valentin Blot: statement

19. **Four Squares Theorem**
    HOL Light, John Harrison: statement
    Isabelle, Roelof Oosterhuis: statement

20. **All Primes (1 mod 4) Equal the Sum of Two Squares**
    HOL Light, John Harrison: statement
    Mizar, Marco Riccardi: statement
    Isabelle, Roelof Oosterhuis: statement
    Coq, contrib, Laurent Théry: statement
    ProofPower, Rob Arthan: statement

21. *Green's Theorem*

22. **The Non-Denumerability of the Continuum**

Lagrangeの4平方数の定理

任意の自然数 n に対して、

整数 $x_1,\ x_2\ , x_3, x_4$が存在して

$$n = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2$$ ■

証明の例

- 初等的証明
  - Hardy, Wright『数論入門』,
  - 和田秀男 『数の世界』,
  - 河田　敬義 『数論　I』.
  - 板井昌典 『幾何的モデル理論入門』(2章整数論との交流)

- ４元数体の理論による証明
  - Samuel “Algebraic theory of Numbers”.

証明の流れ

- 恒等式

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$
$$= (x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4)^2 +$$
$$(x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3)^2 +$$
$$(x_1 y_3 - x_3 y_1 + x_4 y_2 - x_2 y_4)^2 +$$
$$(x_1 y_4 - x_4 y_1 + x_2 y_3 - x_3 y_2)^2$$

- 任意の素数 p に対してx_1, x_2, x_3, x_4 が存在して

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

- 上記を任意の自然数の素因数分解に適応すると定理が示される。

Pigeon Hole Principle

$mp = {x_1}^2 + {x_2}^2 + 1 \quad (0 < m < p)$ の解の存在を
$0 \leq \quad x_1, x_2 \quad \leq (p-1)/2$ の範囲で示す.

x_1, x_2が 0 から $(p-1)/2$ を走る時
${x_1}^2$ と $-1-{x_2}^2$ の $mod\ p$ での像を考えるとp + 1個の像.
${x_1}^2 = -1-{x_2}^2\ mod\ p$ となる x_1, x_2が取れる.

```
::$N Dirichlet Principle
::$N Pigeon Hole Principle
theorem :: FINSEQ_4:65
 card B in card A & B <> {} implies ex x,y st x in A & y in A &
x <> y  & f.x = f.y ;
```

素因数分解の定理の活用

- 素因数分解の形式化
  - 関数で与える
  - 自然数→多種集合

```
definition
  let n be non zero Nat;
  func prime_factorization n -> ManySortedSet of SetPrimes means
:: NAT_3:def 9
support it = support pfexp n & for p being Nat st p in support pfexp
  n holds it.p = p |^ (p |-count n);
end;
notation
  let n be non zero Nat;
  synonym ppf n for prime_factorization n;
end;
```

形式化すると

::$N Fundamental Theorem of Arithmetic
theorem :: NAT_3:61
  Product ppf n = n;

素因数分解のイメージ

n に対して、素数上の関数ppf n, pfexp nが決まってnの素因数とその指数が与えられる。

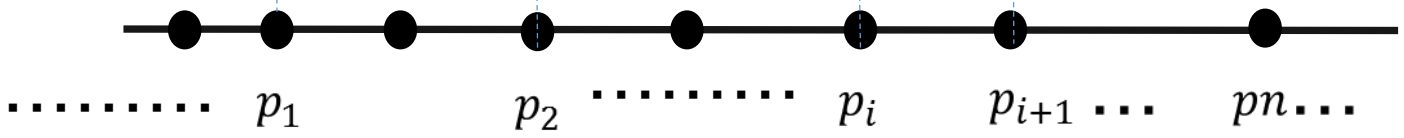
$$n = p_1^{e1} \cdot p_2^{e2} \cdot p_i^{ei} \cdot p_{i+1}^{ei+1}$$

ppf n = p_1^{e1} p_2^{e2} p_i^{ei} p_{i+1}^{ei+1}

pfexp n = e_1 e_2 e_i e_{i+1}

素数全体

m-Spec Z



support pfexp n = { p_1 p_2 p_i p_{i+1}

Mizar普及の課題

形式化(Mizar)でわかりにくい概念が障壁

- そこで整数論に題材をもとめる。
  - 形式化の題材としてはわかりやすい。
  - 形式化(Mizar)でわかりにくい概念の習得
  - 形式化されていない題材が多い
    - ペル方程式
    - 二次体の整数論
    - 無理数、超越数　e, πの超越性