可換環論のMizarによる形式化

TTP@北見工大　2021 .11.21

渡瀬泰成

内容

- 可換代数の形式化動向
- Mizarライブラリの既存アーティクル
- Affine Space
- 代数的集合：イデアルが定める数空間の部分集合
- 空間の点集合が定める多項式環のイデアル
- 今後の展開

可換代数の形式化動向

- 体論の諸定理の形式化（Mizar）
  - Christoph Schwarzweller, Agnieszka Rowińska-Schwarzweller, Algebraic Extensions, 2021Formalized Mathematics 29(1):39-47, 2021
  - Christoph Schwarzweller, Ring and Field Adjunctions, Algebraic Elements and Minimal Polynomials, Formalized Mathematics 28(3):251-261, 2020
- Dedekind domains and class groups of global fields(LEAN)
  - Anne Baanen, Sander R. Dahmen, Ashvni Narayanan, Filippo A. E. Nuccio A formalization of Dedekind domains and class groups of global fields.PrePrint arXiv:2102.02600[v1] Feb 2021
- Witt ベクトルの形式化 (LEAN)
  - Johan Commelin　Robert Y. Lewis Formalizing the Ring of Witt Vectors (arXiv:2010.02595　2020-10-6.)
- Grothendieck's Schemes in Algebraic Geometry (ISABEL)
  - Anthony Bordg, Lawrence Paulson and Wenda Li 2021-03-29

Mizarライブラリの既存アーティクル
(Update from last year TPP 2020 Nov.)

Mizar Library

- 環上の左、右、両側加群
- 可換・整域の定義と性質
- 整数環の商体
- 付値環
- 多項式環（一変数、多変数）
  - Little Bezout(因数定理)
  - 代数学の基本定理
  - 1変数実多項式の形式的微分
  - ヒルベルトの基底定理
- Buchbergerアルゴリズムの形式化

Scope of my research

(mainly from Atiyah/MacDonald’s Text)

- 代数的数
- Zariski位相
- 局所環
- 環の微分（2021 Issued in FM)
- 準素イデアル(2021 Issued in FM)

将来的には、

以下の定義諸定理の形式化

- 準素イデアル分解(to be continued)
- ~~DVR/Dedekind Domain等~~
- ~~べき級数環/体の微分~~
- Affine Algebraic Geometry(on- going)

  Based on W. Fulton: Algebraic Curve
- A-Moduleの形式化の整備(A:Comm. Ring)

Affine Space

- kは体、任意標数、濃度は∞
- n変数の多項式の零点を扱うので代数幾何ではkの要素の n 個の対が空間の点。
- n次元ベクトル空間自体はアファイン空間
- $\mathrm{G}+\vec{v}$ $(\mathrm{G} \in GL_n, \vec{v} \in k^n)$ がアファイン変換
- Mizarの状況
  - 実・複素アファイン空間の形式化が多くを占めている
  - n 個の対の集合n-tuples_on k が n 次ベクトル空間であることが形式化されている。
  - ベクトルは長さnの有限列として形式化され$\{1,2,\ldots,n\} \to k$
- 今回の形式化をすすめるうえでk^nは$Funcs(n,k)$として形式化をしている。

代数的集合：イデアルが定める数空間の部分集合

- $k[x_1, x_2, \dots, x_n]$の多項式の零点とk^nの点を対応付ける。
- 通常$Varity$のVでを用い$V(f)$で多項式fの零点集合を表す。
  - 目下暫定的に形式化ではRoots(f)を利用している。
- 多項式$f, g \in k[x_1, x_2, \dots, x_n]$について
  - $V(fg) = V(f) \cup V(g)$
  - $V(f + g) = V(f) \cap V(g)$
- イデアル$I, J \subset k[x_1, x_2, \dots, x_n]$ について同様の公式が成り立つ
- 体kではなく可換環で成り立つ定理は環Rとして証明している。
  - このときは空間k^nは単なる環Rの要素の対の集合でしかない。

代数的集合：イデアルが定める数空間の部分集合

- $k[x_1, x_2, \ldots, x_n]$の多項式の零点とk^nの点を対応付ける。
- 通常$Varity$のVでを用い$V(f)$で多項式fの零点集合を表す。
  - 目下暫定的に形式化ではRoots(f)を利用している。

```
definition ::Zero set of f
  let R,n;
  let f be Polynomial of n,R;
  func Roots(f) -> Subset of Funcs(n,[#]R) equals
  {x where x is Function of n,R : eval(f,x) = 0.R};
```

代数的集合：イデアルが定める数空間の部分集合

- $S \subset k[x_1, x_2, \dots, x_n\ ]$の部分集合Sの各要素の定める零点の共通部分$k^n$の点集合を対応付ける。
  - 目下暫定的に形式化ではZero_(S)を利用している。

```
::reserve S,T for non empty Subset of Polynom-Ring(n,R);
definition
  let R,n,S;
  func Zero_(S) -> Subset of Funcs(n,[#]R) equals
:Def17:
  meet {Roots(f) where f is Polynomial of n,R : f in S};
```

代数的集合：イデアルが定める数空間の部分集合

```
definition
  let R,n;
  let IT be Subset of Funcs(n,[#]R);
  attr IT is Algebraic_Set means :Def18:
  ex S be non empty Subset of Polynom-Ring(n,R) st IT =
Zero_(S);
end;
theorem Th52:
    for Z be Subset of Funcs(n,[#]R) st Z is Algebraic_Set holds
    ex I be Ideal of Polynom-Ring(n,R) st Z = Zero_(I)
```

代数的集合：イデアルが定める数空間の部分集合

- 多変数多項式の取り扱い

新たに$wpoly(a,i) = x_i - a_i$なる一次の多項式を導入した。

```
definition
  let n,R;
  let a be Function of n,R, i be Element of n;
  func wpoly(a,i) -> Element of Polynom-Ring(n,R) equals
  1_1(i,R) - (a.i)*1_(n,R);
```

$x_i - a_i$

```
theorem Th56:
    for a be Function of n,R holds Zero_(polyset(a)) = {a}
```

$\{x_i - a_i | 0 \leq i \ \leq n-1\}$

点と多項式の対応付けができる。

空間の点集合が定める多項式環のイデアル

- 空間の部分集合 $X(\subset k^n)$上 ゼロとなる多項式の全体はイデアルとなることの形式化, 通常テキストでは $I(X)$と書かれるものである。

```
definition ::Ideal of set of points X;
  let R, n, X;
  func Ideal_X -> non empty Subset of Polynom-Ring(n,R) equals
  :Def24:
  {f where f is Polynomial of n,R : X c= Roots(f)};
theorem Th61: ::(6)
    X c= Y implies Ideal_Y c= Ideal_X
theorem Th62:  ::(7)
      X c= Zero_(Ideal_X)
theorem Th63:  ::(7)
    X = {} implies Ideal_X = [#]Polynom-Ring(n,R)
theorem Th64:  ::(7)
   X = Funcs(n,[#]R) implies {0.Polynom-Ring(n,R)} c= Ideal_(X)
```

反対の包含関係はRが無限体を仮定すれば成り立つ。

- $V(I(V(S))) = V(S), I(V(I(X))) = I(X)$, $I(X)$が根基イデアル($I = \sqrt{I}$)となることを形式化する。
- Hilbert's Nullstellensatz :　$I(V(I)) = \sqrt{I}$ (k:閉体)

今後の展開

- Mizarの形式化能力でどの程度のことができるのだろうか？
  - 可換環の理論の整備(特に環A上の加群)
  - 体論・超越拡大体の整備
  - Affine平面上の曲線論　2次曲線の分類等よく知られた内容の形式化によりノウハウを蓄積
  - 標準的な多項式を出力するルーチンを開発してComputer Algebraに曲線を出力させる。
    - 上記を通してCAとのInterfaceを考察する

Backup

- Mizar概要、及び代数系の形式化の簡潔な説明は以下の論文を参照されたい。

  Christoph Schwarzweller, Representation Matters: An Unexpected Property of Polynomial Rings and its Consequences for Formalizing Abstract Field Theory (Proceedings of the Federated Conference on Computer Science and Information Systems pp. 67–72, 2018)