Elliptic Curve 第1回セミナー

平成 28 年 9 月 29 日

1 Introduction

楕円曲線のセミナーの忘備録

1.1 概要

- 環とイデアル．素イデアル
- 体とガロア群の
- アフィン代数多様体の定義

初めてということもあり，本の 1 章の前提となる.『環とイデアル』,『体とガロア理論』の知識についても説明をした．本論としてはアフィン代数多様体を定義し．アフィン代数多様体の次元を定義するところまで話した．だが, 次元についてうまく説明できず, 次元の幾何的イメージや理論については次回までの宿題となった.

2 内容

2.1 環とイデアル

Definition 2.1. 以下が成り立つとき，R を *(*単位元 *1* を持つ可換*)* 環という.

1. $+ : R \times R \to R, \cdot : R \times R \to R$ が定義されている.
2. 任意の $a, b, c \in R$ に対し，$(a + b) + c = a + (b + c)$ となる.
3. 任意の $a, b \in R$ に対し，$a + b = b + a$ となる.
4. 任意の $a \in R$ に対し，$a + 0 = 0 + a = a$ を満たす元 $0 \in R$ が存在する.
5. 任意の $a \in R$ に対し，$a + b = b + a = 0$ を満たす元 $b \in R$ が存在する.
6. 任意の a, b に対し，$a \cdot b = b \cdot a$ となる.
7. 任意の $a \in R$ に対し，$a \cdot 1 = 1 \cdot a = a$ を満たす元 $1 \in R$ が存在する.
8. 任意の $a, b, c \in R$ に対し，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ となる.

誤解を恐れずにいうと，足し算と引き算と掛け算が定義できるものである．定義を与えたので，例をみる．

Example 2.2. 整数全体の集合 $\mathbb{Z}$ は通常の加法と乗法により，環になる．

Example 2.3. 有理数係数の多項式全体のなす集合 $\mathbb{Q}[X]$ は通常の加法と乗法により，環になる．

環のもっとも重要な例が上記２つである．イデアルについて定義する．

Definition 2.4. I が環 R のイデアルとは，$I \subset R$ であって，以下が成り立つことである．

1. 任意の $a, b \in I$ に対し，$a + b \in I$
2. 任意の $a, b \in I$ に対し，$a \cdot b \in I$

環に対して，イデアルで割るという操作ができる．イデアルで割った世界は，代数幾何的 (多項式環) にいうと，イデアルの零点集合が作る図形上に関数を制限することになる．

2.1.1 体とガロア理論

体を定義する．

Definition 2.5. K が体とは以下を満たす時である．

1. $+ : K \times K \to K, \cdot : K \times K \to K$ が定義されている．
2. 任意の $a, b, c \in K$ に対し，$(a + b) + c = a + (b + c)$ となる．
3. 任意の $a, b \in K$ に対し，$a + b = b + a$ となる．
4. 任意の $a \in K$ に対し，$a + 0 = 0 + a = a$ を満たす元 $0 \in K$ が存在する．
5. 任意の $a \in K$ に対し，$a + b = b + a = 0$ を満たす元 $b \in K$ が存在する．
6. 任意の a, b に対し，$a \cdot b = b \cdot a$ となる．
7. 任意の $a \in K$ に対し，$a \cdot 1 = 1 \cdot a = a$ を満たす元 $1 \in K$ が存在する．
8. 任意の $a \in K - \{0\}$ に対し，$a \cdot b = b \cdot a = 1$ となる $b \in K$ が存在する．
9. 任意の $a, b, c \in K$ に対し，$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ となる．

ざっくりというなら，足し算，引き算，掛け算，割り算が定義できるもののことである．

Example 2.6. 実数全体のなす集合 $\mathbb{R}$ は体をなす．

体の準同型を定義する．体 K, L に対し，$\mathrm{Hon}(K, L)$ の元を $f : K \to L$ であって，以下を満たすものとする．

1. $f(x + y) = f(x) + f(y)$

2. $f(xy) = f(x)f(y)$

3. $f(1) = 1$

Remark. $f(1) = 1$ を課さないという定義もあってもよい．ちなみに $f(1) = 1$ を満たさず，残りの 2 つを満たす射は任意の元を 0 に映す写像のみである．そのような写像に興味がないため，今回は $f(1) = 1$ を課した．

体同士の準同型には以下の面白い性質がある．

Propostion 2.7. 体の準同型 $f : K \to L$ は単射である．

Proof. $a \in K$ に対し，$f(a) = 0$ となったとする.a が 0 がでないとすると，乗法について逆元 a^{-1} を持つ．この時，$f(a \cdot a^{-1}) = 1$ となるが，これは $0 \cdot f(a^{-1}) = 1$ となり，矛盾する. よって $a = 0$ となり，単射が示された． □

体同士の射は単射であるため, この射を通して，体 K を体 L の部分集合とみなすことが多い．この時，体 K を体 L の部分体といい，L を K の拡大体という. また体 L が体 K の拡大となってい時，拡大 L/K と書く．

体の拡大を性質でいくつかに分類する．例えば，体の拡大には以下のような種類がある．

2.2 アフィン代数多様体

アフィン代数多様体を説明する前に最も基本的なアフィン空間を定義する．以降では, K を完全体とし, K の代数閉包を一つ固定し, $\bar{K}$ で表す．また,$\bar{K}/K$ のガロア群を $\mathrm{G}_{\bar{K}/K}$ で表す．

Definition 2.8. $\mathbb{A}^n(\bar{K}) := \{(x_1, \ldots, x_n) \in \bar{K}^n\}$ を n 次アフィン空間といい，その K-有理点 $\mathbb{A}^n(K)$ を $\{(x_1, \ldots, x_n) \in K^n\}$ と定義する．

$\mathrm{G}_{\bar{K}/K}$ を $\mathbb{A}^n(\bar{K})$ は自然に作用する．具体的に書くと，$\sigma \in \mathrm{G}_{\bar{K}/K}$ に対し，$\sigma \cdot (x_1, \ldots, x_n) = (\sigma(x_1), \ldots, \sigma(x_n))$ である．この時，$\mathbb{A}^n(\bar{K})^{\mathrm{G}_{\bar{K}/K}} = \mathbb{A}^n(K)$ となる．

アフィン空間を用いて，代数的集合を定義する．

Definition 2.9. あるイデアル $I \subset \bar{K}[X_1, \ldots, X_n]$ に対し，V_I を以下で定める．

$$\{(x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{K}) | \forall f(X_1, \ldots, X_n) \in \bar{K}[X_1, \ldots, X_n] \text{ に対し}, f(x_1, \ldots, x_n) = 0\}$$

$V \subset \mathbb{A}^n(\bar{K})$ がある $I \subset \bar{K}[X_1, \ldots, X_n]$ を用いて，V_I と表せるとき V を代数的集合という．

$V \subset \mathbb{A}^n(\bar{K})$ に対し，イデアル $I(V) \subset \bar{K}[X_1, \ldots, X_n]$ を以下で定める．

$$\{f(X_1, \ldots, X_n) \in \bar{K}[X_1, \ldots, X_n] | \forall (x_1, \ldots, x_n) \in \mathbb{A}^n(\bar{K}) \text{ に対し}, f(x_1, \ldots, x_n) = 0\}$$

上の定義より，V に対し，I を対応させ，I に対し，V を対応させることができた．では2つの関係を考えたい．例えば, 2つを合成すると．元に戻るのか.

実は，代数的集合 V に対しては，$V_{I(V)} = V$ になる．任意の $V \subset \mathbb{A}^n(\bar{K})$ の場合，つまり，V が代数的集合と限らない時は $V_{I(V)} \supset V$ にはなるが，等号が成り立つとは限らない．例えば代数的集合 V が無限集合だとして，そこから 1 点 x を除いた集合 $V' := V - \{x\}$ に対し，$V_{I(V')} = V$ となる．逆に I について考えてみよう．$I(V_I)$ は I になるとは限らない.$I(V_I) = \sqrt{I}$ となることがわかっている．これはヒルベルトの零点定理として，知られている．記号を説明しておくと，$\sqrt{I}$ は I の Radical と言われるイデアルで，$\{x \in \bar{K}[X_1, \ldots, X_n] |$ ある m が存在し $x^m \in I$ となる $\}$　で定める．では，$I(V_I)$ と I はいつ一致するだろう． 例えば，I が素イデアルの場合，$I = \sqrt{I}$ となる．

Excersize 2.10. I が素イデアルの場合，$I = \sqrt{I}$ を示せ.

準備ができたので，アフィン代数多様体を定義する．アフィン代数多様体は I と V が逆の対応を定めるような場合を考えている．

Definition 2.11. 代数的集合 V がアフィン代数多様体であるとはとは，$I(V)$ が素イデアルであること．

この時 $\bar{K}[X_1, \ldots, X_n]/I(V)$ をアフィン座標環という．アフィン座標環は整域となるので，その商体が定義できる．

$\mathrm{Frac}(\bar{K}[X_1, \ldots, X_n]/I(V))/\bar{K}$ という拡大に対し，その超越次数 $\mathrm{tr.deg}_{\bar{K}}\mathrm{Frac}\bar{K}[X_1, \ldots, X_n]/I(V)$ を V の次元という．