数学入門公開講座

平成１２年７月３１日（月）から平成１２年８月４日（金）

京都大学数理解析研究所

講師及び内容

1．球面の対称性（6時間15分）

京都大学数理解析研究所・助手　永田　雅嗣

「対称性」というのは、実生活にもなじみの深い概念です。「球面という図形にどんな対称性があるか」と問われれば、誰でも点対称、回転対称、面対称などのアイデアを思い起こすでしょう。では、点対称や面対称が必ず周期２の対称性であるのは、なぜでしょうか。「周期３の点対称」のようなものがありえないことの理由をつきつめて考えていくと、図形のグローバルな性質をつかさどる、美しい数学が見えてきます。図形の定性的な性質と、定量的な群論とを結ぶ、変換群論と呼ばれる幾何理論を紹介したいと思います。

2．有理点の問題と符号暗号への応用について（6時間15分）

京都大学数理解析研究所・教授　伊原　康隆

代数曲線の有理点が符号、暗号(主に符号)の問題にどのように使われるかについて、入門的な話をしたいと思います。

体、とくに有限体とは何か(？)といったあたりから話をはじめ、代数曲線とその有理点、楕円曲線の場合、等についての基礎的な話をし、それらが符号、暗号に関する如何なる問題にどう応用されるかについて、その一端を紹介したいと思います。

3．離散と連続 － 微分方程式の数値解析（6時間15分）

京都大学数理解析研究所・助手　降簱　大介

「数えられるもの＝離散量」と「数えられないもの＝連続量」という素朴な感覚にたがわず、数学では離散量と連続量は異なった扱いを受けます。

しかし、離散と連続の間には、連続は離散の極限であるという直感を越えて微妙で意義深い関係があるらしいことが各分野の様々な結果によって強く示唆されていて、非常に興味深いものがあります。

本講座では、そうした離散と連続の関係の一端を紹介するべく、離散量を対象としアルゴリズムの構築と計算量の解析を柱とする計算機科学と、連続量を対象とし関数空間の解析を柱とする関数解析学とが合流する分野－微分方程式の数値解析－を中心に講演を行います。

時　間　割

日 / 時　間	7月31日（月）	8月1日（火）	2日（水）	3日（木）	4日（金）
10：30～11：45	永田	永田	永田	永田	永田
11：45～13：00	休　憩				
13：00～14：15	伊原	伊原	伊原	伊原	伊原
14：15～14：45	休　憩				
14：45～16：00	降簱	降簱	降簱	降簱	降簱

平成12年度(第22回)数学入門公開講座テキスト(京都大学数理解析研究所, 平成12年7月31日～8月4日開催)

有理点の問題と符号暗号への応用について

京都大学数理解析研究所・教　授　　伊　原　康　隆

2000, JULY 31, AUGUST 1,2,3,4,　13:00～14:15

[有理点の問題と符号暗号への応用について]

伊原康隆

[目次]

この予稿集では, 特に基礎的なところにスペースを多く使いました. 具体的な符号の説明や暗号については この予稿では触れませんでしたが, §1, 2, 3, 4+5 をそれぞれ一回づつの講義で無理なく出来れば、五回目の講義で触れたいと思います. その意味で この予稿は 全体の8割の予稿で, 残りは模様替がめになります. 聴講者の皆様には, とくに有限体に親しんでいただく事が 第一の目標です.

1 有限体

方程式論、そして早熟な天才として有名なガロア (Evariste Galois; 1811-1832) の発見した最も重要な概念は「ガロア群」かと思いますが、「有限体」もガロアがその重要性をはじめて理解し指摘したもので、今日整数論, 群論, 代数幾何学, トポロジー など基礎数学分野では勿論, 符号, 暗号理論等, 応用部門でも盛んに使われています。

今日はまずそれについて慣れていただきたいと思います.

$$\mathbb{Z} = \{\cdots, -1, 0, 1, \cdots\}$$

で整数全体の集合を表わします. 素数とは, 1より大きな整数 p で, $\mathbb{Z}$ 内では ± 1 と $\pm p$ 以外では割れないものの事です。(素数は英語で prime number というので, しばしば素数を表わす記号として p を用いる.) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... 等が素数を下から並べたもので, 100以下では25個, N が十分大きいとき, N 以下の素数は大体 $\frac{N}{\log N}$ 個あることが知られています. ($\log$ は自然対数.) とにかく, 素数は無限に多く存在します.

p を素数とするとき, p^n 型の数 (例えば p, p^2 など) を素数巾(べき)といいます. 素数巾を表わす記号として, しばしば q を用います。例えば $q = 27, 31, 1024$. 素数巾 q を一つとると, 有限体 F_q と呼ばれる新しい「数の集まり」が定義されます. F_q は q 個の「数」から成っていて, その間に和と積が定義されています。まず q が素数 p のとき F_p を定義します。

F_p は集合としては p 個の数 $\{0, 1, \cdots, p-1\}$ の集合で, そこに「普通の和, 積をとってそれを p で割った余りを F_p での (それぞれ) 和, 積と定める」という規則で 和と積を導入したものです. 例えば

$$F_5 = \{0, 1, 2, 3, 4\}; \qquad 2+3=0, \quad 2\times 3 = 1, \text{ など.}$$

最も簡単な $F_2 = \{0, 1\}$ では

$$\begin{cases} 0+0=0, \quad 1+0=0+1=1, \quad 1+1=0, \\ 0\times 0 = 1\times 0 = 0\times 1 = 0, \quad 1\times 1 = 1. \end{cases}$$

この中で 通常と異るのは $1+1=0$ だけです。 0と1の数列が工学で重要なのは御存知と思いますが, この演算がなぜ重要かというと, F_2 の数を係数とするベクトル空間, 多項式, 代数方程式などを実数や複素数係数のものと同様に考え同様に扱うことで, 様々な新しい構造が見通しよく研究でき, それが応用上も

役に立つからです。これら F_p や，実数全体，複素数全体，有理数（整数の比として表わせる実数）全体などでの和 $a+b$ と積 ab の満す共通の性質を列挙すると，

(i) $(a+b)+c=a+(b+c)$，(ii) $a+b=b+a$，(iii) $a+0=a$，(iv) 各 a に対して，$a+a'=0$ となる a' が唯一つ存在，(v) $(ab)c=a(bc)$，(vi) $ab=ba$，(vii) $a\cdot 1=a$，(viii) 各 $a\neq 0$ に対して，$aa^*=1$ となる a^* が唯一つ存在，(ix) $(a+b)c=ac+bc$．

一般に，和，積が定義され 0，1 という相異る特別な元を有する集合 K であって，K の任意の元 a,b,c に対して条件 (i)～(ix) を満すものを体（たい）と呼びます。そして (iv) に於る a' を $-a$，(viii) に於る a^* を a^{-1} と書きます。又 a の整数倍 na や整数巾 a^n を，$3a=a+a+a$，$-2a=-(2a)(=2(-a))$，$a^2=a\times a$，$a^{-5}=(a^5)^{-1}(=(a^{-1})^5)$ のように定義します。又 (i)～(ix) より容易に，$a\cdot 0=0$ がすべての $a\in K$ に対して成立つこと（主に (ix) を用いよ），又 $a\neq 0, b\neq 0$ なら $ab\neq 0$ であること（主に (viii)）などがわかります。

定理1　F_p は体である.

証明は, (viii) 以外は容易. (viii) でのみ p が素数であることが必要になる.

(viii) を示す為, まず次の基本的な補題を証明します。

補題1　$a, b \in \mathbb{Z}$ が公約数をもたないなら,

$$ma + nb = 1$$

を満す $m, n \in \mathbb{Z}$ が存在する.

(例えば $a=23, b=15$ なら　$2\times 23 + (-3)\times 15 = 1$)

(証明)　今 $ma+nb$ $(m, n \in \mathbb{Z})$ の形で書ける整数を

すべて 考え, その集合を I とする. 例えば $0, a, b, a-b, 5a+7b, \cdots$

など すべて I の元. I の元の和や, I の元の整数倍はすべて I に属する.

$a=b=0$ は題意に反するし, $\pm a, \pm b \in I$ ゆえ, I は ある正の整数

を 含む. I に含まれる 正整数で最小のものを d とおくとき,

d の倍数はすべて I に属するが, 逆に I の勝手な元 c をとると, それを

d で割った 余りも I に属するから, d の最小性から, その余り $=0$, 即ち,

c は d の倍数. よって I は d の倍数全体の集合と一致する. とくに

a, b は d で割れることになり, 仮定より, $d=1$. よって $ma+nb=1$

となる $m, n \in \mathbb{Z}$ が存在. (補題1の証明終)

F_p が (viii) を満たすことの証明.

$a \in \{0, 1, \cdots, p-1\}$, $a \neq 0$ とすると, a と p は公約数をもたないから, 補題 1 より

$$ma + np = 1$$

となる $m, n \in \mathbb{Z}$ が存在する. m を p で割った余りを a^* とすれば a^*a を p で割った余りが 1 となるので F_p においては $a^*a = 1$.

(証明終)

有限個の元からなる体を有限体といいます. F_p はその基本的な例です. 次の目標は,

定理 2　有限体の元の個数は素数のべき $q = p^n$ である. 逆に q を素数べきとすると, 丁度 q 個の元をもつ有限体が(表示法の相異は別として)唯一つ存在する.

この詳しい証明は難しいので, 代わりに, 感じを掴んでいただくための説明を試みます.

まず 第一の点ですが, F を 有限体 とすると, $1,\ 1+1,\ 1+1+1,\ \cdots$, のうち 等しいものが なくては ならないので, $N\cdot 1=0$ となる 自然数 $N>1$ が ある. そういう N のうちで 最小なものを とる. もし N が 素数 でないとすると, $N=dd'$ と 分解し, $(d\cdot 1)\cdot(d'\cdot 1)=0$, $d\cdot 1\neq 0$, $d'\cdot 1\neq 0$ となるが, これは F が 体 だから, あり得ない. 従って $N=p$ (素数). この場合 F は $F_p=\{0,1,\cdots,p-1\}$ を 含む 体 になるので, F_p 上のベクトル空間と見なせ, その次元は 有限. それを n とすると F の 元の個数は p^n.

逆に $q=p^n$ のとき q 個の元をもつ体が 唯一つ 有在することを 示さなくては なりません.

$n=1$ のときの有在は 定理 1 で 示しましたが, 一意性も 上で 実質的に 示されています.

$n=2$ のときを 考えてみます. まず

補題 2　F_p 係数の 2次式 x^2+ax+b $(a,b\in F_p)$ であって, 既約, つまり F_p 上の 1次式の積には 分解しないものが 有在する.

(証明)　上の形の 2次式 全体の個数は a,b の 選び方の個数で p^2 個. その中で 1次式の積に 分解するものの 個数は, $(x+c)(x+c')=(x+c')(x+c)$ に 注意して, 丁度 $\frac{1}{2}p(p+1)$ 個。 よって 既約なものが 丁度 $\frac{1}{2}p(p-1)$ 個 ある

(証明終)

これを用いて, p^2 個の元をもつ有限体の存在と一意性を示します。

$f(x) = x^2 + ax + b$ を F_p 上の既約な2次式とします。 F_{p^2} を、集合としては

$$F_{p^2} = \{ cx + d \mid c, d \in F_p \} \qquad (F_p\text{-係数1次式全体})$$

と定義し, F_{p^2} に於る和と積を「通常の和積を $f(x)$ で割った余りの1次式」と定義します。(和の方は1次式にとどまるから実際には割って余りをとらなくてもそのままで同じ。)

皆さんは, この定義が, $\mathbb{Z}$ と p から F_p を定義したのと全く同様の定義であることに気付かれたでしょう。 $\mathbb{Z}$ のかわりに F_p 係数の x の多項式全体をとり, 素数 p のかわりに既約な2次式 $f(x)$ をとったわけです。従って, これが体であることを示すには,

補題1' K を体とし, K 係数の2つの多項式 $a(x), b(x)$ が共通の因子(1次以上の多項式で両方を割切るもの)を持たないとすると, ある K 係数多項式 $m(x), n(x)$ が存在して

$$m(x)a(x) + n(x)b(x) = 1 \qquad \text{となる}$$

が示されればよい事がおわかりでしょう。この補題1'も補題1と全く同じ方法で示せるので(やってみて下さい!) これで F_{p^2} も体であることが示せました。しかも, より一般に次の定理も示せたことになります。

定理3　K を体とし，$f(x)=x^n+a_1x^{n-1}+\cdots+a_n$ を K 係数の既約(即ち、次数の低い(1次以上の)多項式では割れない)多項式とし，K 上の $n-1$ 次以下の多項式全体の集合に，和は多項式の和，積は多項式としての積を $f(x)$ で割った余り，によって 和と積を定義したものは 体 になる．

これは K を(0次式全体として)含んでいて，K 上 n 次元ベクトル空間とみなせる体で，これを

$f(x)$ によって定まる K の拡大体

と呼びます．

(例1)　$p=2$, $n=2$.　このとき既約な2次式は $f(x)=x^2+x+1$ だけで，

$F_4=\{0,1,x,x+1\}$　　積は $x^2+x+1=0$, $2=0$, と考えて計算する．例えば $x(x+1)=1$

(例1)　$p=3$, $n=2$　　このとき既約な $f(x)=x^2+\cdots$ は3つ

$f_1(x)=x^2+1$,　$f_2(x)=x^2+x-1$,　$f_3(x)=x^2-x-1$

しかし　$f_1(x+1)=f_3(x)$,　$f_1(x-1)=f_2(x)$ だから，実際は同じ体。

一般の p では $f(x)$ は $\frac{1}{2}p(p-1)$ 個あるが，$x\to\alpha x+\beta$

$\alpha=1,2,\cdots,\frac{1}{2}(p-1)$; $\beta=0,1,\cdots,p-1$ で一つの $f(x)$ から他のに移るので，体としては1つしか出て来ない．

n を一般とするときは:

補題 2′　　各素数 p と $n \in \mathbb{Z}$, $n \geq 1$ に対して, $\mathbb{F}_p$ 上の n 次既約多項式 $f(x) = x^n + \cdots$ が存在する

が成立ち, この $f(x)$ によって定まる $\mathbb{F}_p$ の拡大体として $\mathbb{F}_{p^n}$ が得られます.

補題 2′ は証明しませんが, $\mathbb{F}_p$ 係数の多項式

$$x^{p^n} - x$$

は 重根を持たず, これを既約分解すると, n 次の既約多項式 (最高次係数 1) がおべて 1回づつ 出て来て (残りは ある $d \mid n$, $d < n$ に対して $x^{p^d} - x$ の因子となるもの)

そのどれを 使っても 同じ 拡大体 が 生じます. 例えば

$n = 3$　　$\dfrac{x^{p^3} - x}{x^p - x}$ は $\dfrac{p^3 - p}{3}$ 个の既約3次式の積

$n = 4$　　$\dfrac{x^{p^4} - x}{x^{p^2} - x}$ は $\dfrac{p^4 - p^2}{4}$ 〃 4 〃

$n = 5$　　$\dfrac{x^{p^5} - x}{x^p - x}$ は $\dfrac{p^5 - p}{5}$ 〃 5 〃

$n = 6$　　$\dfrac{(x^{p^6} - x)(x^p - x)}{(x^{p^3} - x)(x^{p^2} - x)}$ は $p^6 - p^3 - p^2 + p$ 〃 6 〃

一般に, 最高次係数1の F_p 上の n 次既約多項式の個数は

$$\frac{1}{n}\sum_{d|n}\mu(d)p^{\frac{n}{d}}$$

で与えられます. ここで d は n の正の約数 ($1, n$ を含む) 全体を動き, $\mu(d)$ はメービウスの関数, 即ち

$$\mu(1)=1, \quad \mu(p_1\cdots p_r)=(-1)^r \quad \cdots\ p_1,\cdots,p_r \text{ 相異る素数のとき},$$
$$\mu(d)=0 \quad \cdots\ d \text{ が平方数で割りきるとき}.$$

となります. この個数は n 次多項式全体の個数 p^n の大体 $\frac{1}{n}$ で, $n=\log_p(p^n)$ ですから, はじめに述べた N 以下の素数の個数のおおよその個数を与える式と似ています。(証明は多項式の場合の方がはるかにやさしい.)

又 F_{p^n} の元は, すべて方程式 $\alpha^{p^n}=\alpha$ を満し, $d|n$ とすると, F_{p^d} は F_{p^n} の中で $\alpha^{p^d}=\alpha$ を満すものの全体として F_{p^n} に含まれています. 又 F_{p^n} の元 α に α^p を対応させる写像

$$F_{p^n}\ni\alpha\longrightarrow\alpha^p\in F_{p^n}$$

は和と積を保ち, 1対1になっています. ($p=0$ だから $(\alpha+\beta)^p=\alpha^p+\beta^p$)

F_p 上の n 次既約多項式はすべて F_{p^n} で1次因子の積に分解します.

2 線型符号

有限体 F_q をとり, F_q の元を横に n 個並べたもの全体を

$$(F_q)^n = \{x = (x_1, \cdots, x_n) \mid x_i \in F_q\}$$

とします. これは F_q 上の n 次元ベクトル空間になっています.

$$C \subset (F_q)^n$$

を $(F_q)^n$ の一つの部分空間とします (これを線型符号ともよぶ).

$(F_q)^n$ の2元 $x = (x_i)$, $x' = (x_i')$ の間の距離 $d(x, x')$ を

$$d(x, x') = \boxed{x_i \neq x_i' \text{ となる } i \ (1 \leq i \leq n) \text{ の個数}}$$

と定義します. 例えば $(F_2)^3$ において $x = (0,1,0)$, $x' = (1,1,1)$ なら $d(x,x') = 2$. 次に

$$d(C) = \operatorname{Min}\{d(x,x') \mid x, x' \in C, \ x \neq x'\}$$
$$= \operatorname{Min}\{d(x,0) \mid x \in C, \ x \neq 0\}$$

(Min は最小値を表わす) とおきます. 例えば

$$C = \{(x_1, x_2, x_3) \in (F_2)^3 \mid x_1 + x_2 + x_3 = 0\}$$

とすると, $C = \{(0,0,0), (1,1,0), (1,0,1), (0,1,1)\}$ ですから, $d(C) = 2$.

F_q の元を「アルファベット」、$(F_q)^n$ の元を「長さ n の単語」、C の元を「名前として許される長さ n の単語」と考えて見ましょう。そうすると、$d(C)$ は、「2つの異る名前は、最低何ケ所で文字が異るか」を表わす量ということになります。どのように C を選ぶとよいか？ C が小さいと"同姓同名"を許さざるを得なくなるし、$d(C)$ が小さくても混同しやすい名前があって不都合です。そこで、n に比べて $\dim(C)$ (C の次元)、$d(C)$ が共になるべく大きい C を採したいという事になります。例えば $q=2$, $n=3$, $\dim C=2$ なる C は、先程の例の他に6個ありますが、そのうち $C_{(i)}=\{(x_1,x_2,x_3)\mid x_i=0\}$ タイプ ($i=1,2,3$) では $d(C_{(i)})=1$, $C_{(ij)}=\{(x_1,x_2,x_3)\mid x_i+x_j=0\}$ タイプ(三個)でも $d(C_{(ij)})=1$ ですから、上の意味で都合のよいのは先の例 C だけです。この例では、2つの異る名前は、どこか2ケ所(以上)で、(それらを構成する)文字が異るから、まぎらわしくない、というわけです。

(注意：上の「名前」による説明は、実用上の符号の使われ方に基いたものではありません。実用上は、より信頼度の高い通信手段を求める為、等で使われます。)

一般に q と n を与えたとき, $\dim C$ も $d(C)$ もなるべく大きい C を見つけるのが問題です.

そこで

$$\delta(C)=\frac{d(C)}{n}\ (C\text{の相対距離}),\qquad R(C)=\frac{\dim(C)}{n}\ (C\text{の情報率})$$

と置き, q は固定して n, C を動かし, $(\delta(C), R(C))$ を座標にもつ点を δR 平面上の正方形 $S=\{(\delta, R)\mid 0\le\delta, R\le 1\}$ 内にマークして行きます. なるべく"右上"の点がほしいわけです. マークされた点の無限列の集積点の集合を

$$U_q=\left\{(\delta,R)\in S \;\middle|\; \begin{array}{l}\text{無限列 } C_i\subset(\mathbb{F}_q)^{n_i}\ (i=1,2,\cdots)\text{で}\\ n_i\to\infty\text{ となるものが存在して}\\ (\delta,R)=\lim_{\to}(\delta(C_i),R(C_i))\end{array}\right\}$$

で定義します. どういう符号がつくれるかを理論的に調べるには, まず U_q が S の中でどういう図形になるかを知ることが大切です.

これについて以前から研究され, 次の事が知られていました.

定理4

1) ある連続写像 $\alpha_q : [0,1] \to [0,1]$ が存在して,

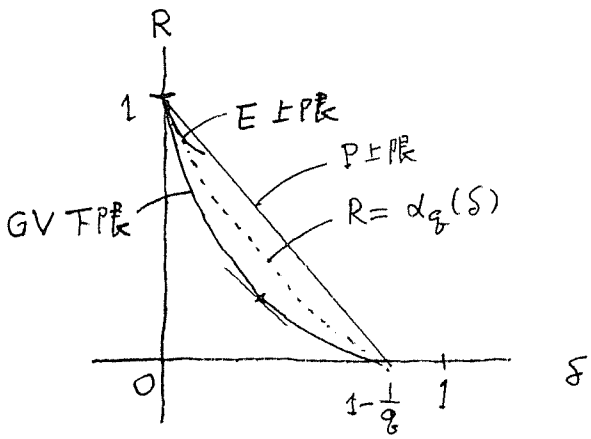
$$U_q = \{(\delta, R) \in S \mid 0 \le R \le \alpha_q(\delta)\} \quad \text{となる.}$$

2) $\alpha_q(\delta) \le \mathrm{Max}\{1 - \frac{q}{q-1}\delta,\ 0\}$ (Plotkin 上限)

2)' Elias 上限 (δ の小さいところで 2) より よい) (略)

3) $\alpha_q(\delta) \ge 1 - \delta \log_q(q-1) + \delta \log_q \delta + (1-\delta)\log_q(1-\delta)$

(Gilbert-Varshamov 下限)



[注意 GV] 後の参考の為,

G-V 曲線の勾配 $2-1$ の接点は,

$$\delta + R = 1 - \log_q\left(\frac{2q-1}{q}\right)$$

で, 接点の δ 座標は $\delta = \frac{q-1}{2q-1}$.

さて G-V 下限の上には U_q の点は 約25年前 発見されなかった為, GV を与える曲線が α_q のグラフと一致するのではないかとの予想もあったようです. しかし Goppa 符号によって 有理点を沢山もつ $\mathbb{F}_q$ 上の代数曲線の理論と結びつき, 昔の結果 (Ihara, Tsfasman-Vladut-Zink) によって この記録は破られました. これについて, 順次 説明したいと思います.

§3 代数曲線

K を任意の体 (例えば F_8 など) とするとき, K 上の代数曲線とは, 基本的には, K 上の2変数多項式 $f(x,y)$ に対して方程式

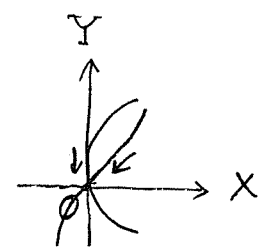
(1) $$f(x,y)=0$$

の解 (x,y) 全体のつくる集合 (K が実数体のときのイメージで曲線と考える) の事です. この際, 解 x,y の範囲を K に制限すると, K が有限体のように小さいときは多項式 $f(x,y)$ のすべての性質を解全体の集合が十分反映できないので, K を含む大きな体 (例えば $K=F_8$ なら, $F_8 \subset F_{8^2} \subset F_{8^6} \subset F_{8^{24}} \subset \cdots \subset F_{8^{(n!)}} \subset \cdots$ の合成体 $\overline{F_8}$ などを考える) で考えます. そして $x,y \in K$ のときの (1) の解は (1) の K-有理点 と呼びます. 例えば $K=\mathbb{R}$ (実数体) のとき, $x^2+y^2-1=0$ の K-有理点全体は単位円の円周, 又 $K=F_3$ なら, それは4つの有理点 $(1,0),(2,0),(0,1),(0,2)$ から成る. 次に, $f(x,y)$ は K 係数多項式なら何でもよいわけではなく, 勿論定数ではなく, 又それは既約, つまり定数以外の多項式の積 $f(x,y)=g(x,y)h(x,y)$ には分解しないとします. この g,h の係数の範囲は K だけでなく, K を含むどんなる体をとっても そこでも分解しない (絶対既約) とする必要があるのですが,

実際には $f(x,y)=0$ が少なくも一つ K-有理点をもつときは、既約なら絶対既約になります。こういう $f(x,y)$ から出発しても「よい曲線」をつくる為には、まだ二種類の修正が必要です。まず (a,b) を(1)を満す点とし、$X=x-a$, $Y=y-b$, $f(x,y)=F(X,Y)$ とおくと、$F(X,Y)=cX+dY+$(2次以上)となりますが、$(c,d)\neq(0,0)$ のとき (a,b) は曲線(1)の滑らかな点といいます。滑かでない点は、$f(a,b)=\frac{\partial f}{\partial x}(a,b)=\frac{\partial f}{\partial y}(a,b)=0$ を満す点で、タカダカ有限個です。さて (a,b) が滑らかでないとき、$F(X,Y)$ は2次以上になるので、最低次(d次とする, $d\geq 2$)の項をまとめたものを $F_d(X,Y)$ とかく。又 K を十分大きくとって、

$$F_d(X,Y)=c_0X^{r_0}\prod_{i=1}^{s}(Y-\alpha_iX)^{r_i} \qquad (c_0,\alpha_1,\cdots,\alpha_s\in K,\ \alpha_1,\cdots,\alpha_s \text{は互いに相異る})$$

と分解する。このとき、点 $(x,y)=(a,b)$ (つまり $(X,Y)=(0,0)$) は1つの点と考えずに、上の分解に出てくる1次因子(X, $Y-\alpha_iX$ など)毎に1つづつ新しい点があると考えます。例えば $F(X,Y)=X^3-X^2Y+$(4次以上) なら $F_3(X,Y)=X^2(X-Y)$ ゆえ $K=\mathbb{R}$ での図は



となり、$(X,Y)=(0,0)$ は近づき方の異る2つの成分(新しい"点")から成ると考えます。一方、$X=x^{-1}$, $Y=y^{-1}$ について書直したときの原点も、(滑らかでないときはこの方法で有限個の点にわけて)それを「無限遠点」としてつけ加えます。このようにして $f(x,y)=0$ の附全体を修正(有限個点が増えている)したものが絶対既約、滑らかで完備な代数曲線です。

(例1) $K=F_{p^2}$, $f(x,y)=y^p+y-x^{p+1}$

このとき, 無限遠点以外は滑らかで, 無限遠点も滑かではないが1個

K有理点は p^3+1 ケです. ($a,b\in F_{p^2}$ のとき a^p+a, $b^{p+1}\in F_p$ となることに注意し, 各 $c\in F_p$ に対して $a^p+a=c$ となる $a\in F_{p^2}$ は p ケ, 各 $c\in F_p$, $c\neq 0$ に対して $b^{p+1}=c$ となる $b\in F_{p^2}$ は $p+1$ ケであることを示せ.)

さて, 一般に上のように $f(x,y)=0$ で定まる絶対既約, 滑らかで完備な代数曲線 V を考えると, K係数有理関数 $\frac{f(x,y)}{g(x,y)}$ であって g が与えられた f で割れないものは, V 上の関数と考えることが出来, V 上の K′有理点でとる値は, K′の数又は ∞ となります.

(例えば $\frac{y-b}{x-a}$ が点 "$Y-\alpha_i X$" でとる値は $\frac{0}{0}$ の不定ではなく, α_i である)

こうして得られる V 上の関数を V 上の有理関数と呼びます.

それが V のある点 P で ∞ になるときも, その点での極の位数が自然に定義されます (例えば $\frac{y-b}{x-a}$ が "X" でとる値は ∞, 極の位数は r_0.) ($r_0>0$ なら)

代数曲線 V に対して, その種数 g と呼ばれる 0 または正の整数が定まります. V の点 P を任意にとって, P だけで丁度 m 位の極をもち, その他では極をもたない有理関数があるかどうかを調べ, そういう関数の存在しない $m(\geq 1)$ の値を $m_1(P)<\cdots<m_g(P)$ とするとき, g は P によらず V だけで定まる $(0\leq g<\infty)$. これが種数です. (上の例では $g=\frac{1}{2}(p^2-p)$.)

§4 Goppa符号

V を F_q 上の絶対既約, 滑らか完備な代数曲線とし, その種数を g とします. また V は相異る F_q 有理点 $P_0, P_1, \cdots, P_n$ をもつとします。m を自然数とし, これらの資料によって定まる Goppa 符号 $C \subset (F_q)^n$ を,

$$C = \{ (f(P_1), \cdots, f(P_n)) \mid \begin{array}{l} f \text{ は } V \text{ 上の } F_q \text{ 係数の有理関数で,} \\ P_0 \text{ で } m \text{ 位以下の極をもつ他は} \underline{\text{正則}} \\ \qquad\qquad (\text{有限値をとること}) \end{array} \}$$

と定義します。 $2g-2 < m < n$ とすると, Riemann-Roch の定理を用いることによって,

$$\dim(C) = \dim(f \text{の空間の次元}) = m-g+1.$$

また $f \neq 0$ なら $f(P_i)=0$ となる i の個数 $\leq m$ ゆえ,

$$d(C) \geq n-m.$$

よって,

$$R(C) = \frac{m-g+1}{n}, \qquad \delta(C) \geq 1 - \frac{m}{n}$$

$$\therefore \quad \delta(C) + R(C) \geq 1 - \frac{g-1}{n}$$

が得られます. よって, n が $g-1$ に比べて大きい程, $(\delta(C), R(C))$ は より右上の方にあることになります. n は, V の F_q-有理点の個数マイナス 1 にとれますから, F_q を固定したとき $g-1$ に比べて F_q-有理点の著しく多い F_q 上の代数曲線の系列を見つけることが問題になります.

定量的には,

$$A(q) = \overline{\lim_{g\to\infty}} \left(\frac{\mathbb{F}_q\text{上の代数曲線 } V \text{の } \mathbb{F}_q \text{有理点の個数}}{V\text{の種数 } g} \right)$$

とおくとき, Goppa符号により(mは $2g-2 < m < n$ の範囲ですべての値を用いる), 線分

$$(G_P) \qquad \delta + R = 1 - \frac{1}{A(q)}, \quad \frac{1}{A(q)} \le R \le 1 - \frac{1}{A(q)}$$

は U_q に属することがすぐわかります. 一方, §2(注意 GV)より,

$$A(q) > \left(\log_q \left(\frac{2g-1}{g} \right) \right)^{-1} \fallingdotseq \log_2 q$$

なら, 線分 (G_P) の少くも一部が GV 下限曲線の上にはみ出す事になります. そこで, 各素数巾 q に対して $A(q)$ の値, またはそのよい下限を求めることが問題になります.

5 沢山の有理点をもつ F_q 上の代数曲線

これについては次の事が知られています.

定理5 $q=p^{2n}$ 型のとき, F_q 上絶対既約, 滑らかで完備な代数曲線の可算無限系列 $\{V_i\}_{i\geq 1}$ であって, V_i の種数 g_i は $g_i\geq 2$ $(i=1,2,\cdots)$, $g_i\to\infty$ $(i\to\infty)$ を満し, 各 V_i は少くも

$$(p^n-1)(g_i-1)$$

個の F_q-有理点をもつものが存在する.

系 $q=p^{2n}$ 型のとき, $A(q)\geq \sqrt{q}-1$ (実は $=$ になる)

これを $\left(\log_q \frac{2q-1}{q}\right)^{-1}$ と比べると, $q\geq 7^2$ なら確かに $\sqrt{q}-1$ の方が大きくなるので, 線分 (Gp) の一部分が GV曲線の上にはみ出る事になります。 上の定理5は伊原によって1970年代示されたものですが, 証明には志村曲線と呼ばれる曲線系の理論が使われます. Tsfasman-Vladut-Zink も $q=p^2$ のときの別証を与え, 又その後 Garcia-Stichtenoth は定理5の条件を満す $\{V_i\}$ を具体的に構成した.

V_i は変数 $x_1,\cdots,x_{i+1},y_2,\cdots,y_{i+1}$ の間の連立方程式

$$x_jx_{j+1}=y_{j+1},\quad y_{j+1}^{p^n}+y_{j+1}=x_j^{p^n+1}\quad (1\leq j\leq i)$$

によって 定まる F_q 上の代数曲線です. ($i=1$ が既に出た例)。

$q=p^{2n-1}$ 型のときの $A(q)$ の値は $\leq \sqrt{q}-1$ であること(Drinfeld-Vladut)

以外は あまりわかっていませんが, Niederreiter, Xing 等による かなり

よい結果もあるので; これらについても (なるべく公開講座の時点での

最新情報を) 報告したいと思います.

線型符号と有理点の結びつきは Goppa 符号による

結びつきだけではなく, 又上の話は $(\delta(C), R(C))$ の集積点が

どの位 右上にありうるかという問題にしぼられていましたが, 有理点の

応用として具体的な よい線型符号をつくる事も 勿論なされ

ています. よい符号の構成には 日本人の寄与も大きく, とに

笠原正雄氏のグループは 現在世界で使われている符号の

何割かの符号を発明されたそうです。

ここでは, 有限体, その上の代数曲線の有理点,

つまり F_q 係数の方程式 $f(x,y)=0$ の解の研究という, 元来

純数学的興味の対象として研究されていた成果が、「よい符号の

構成 (又は構成の可能性の追究)」という応用上の問題と

(まず Goppa によって) 結びつき, 純粋, 応用 双方のその後の

活発な発展を促した事に注目していただきたかったわけです.