

曲線上の点とねじれた数の世界 ~ Brauer 群へ至る道

植松 哲也

豊田高専 一般学科

March 15, 2017./ 第2回一般学科コロキウム @ 豊田高専

お伝えしたいこと

整数論
素数の不思議

↓
幾何的視点・一般化

曲線上に
「すてきな」点
があるかどうか

結びつき

ねじれた数の世界で
割り算
ができるか

↓
Brauer 群

素数 (1)-Quiz

素数とは？

- 1 と自分自身以外に約数を持たない数.
- 2, 3, 5, 7, 11, 13, 17, ...
- 素数は無数に存在する (Euclid).

Quiz 1

(奇数の) 素数を次のように分けました . **規則性**はなんでしょう？

グループ 1	グループ 2
5, 13	3, 7
17, 29	11, 19
37, ...	23, ...

素数 (2)-規則性の答

答

- グループ 1 の素数たちは 4 で割ると 1 余る
- グループ 2 の素数たちは 4 で割ると 3 余る

グループ 1	グループ 2
$5 = 4 \times 1 + 1$	$3 = 4 \times 0 + 3$
$13 = 4 \times 3 + 1$	$7 = 4 \times 1 + 3$
$17 = 4 \times 4 + 1$	$11 = 4 \times 2 + 3$
$29 = 4 \times 7 + 1$	$19 = 4 \times 4 + 3$
$37 = 4 \times 9 + 1$	$23 = 4 \times 5 + 3$
...	...

もうひとつ質問

他に規則性が見つかったひと・・・？

素数 (3)-不思議な規則性

もうひとつの規則性？

グループ 1	グループ 2
$5 = 1^2 + 2^2$	$3 = ???$
$13 = 2^2 + 3^2$	$7 = ???$
$17 = 1^2 + 4^2$	$11 = ???$
$29 = 2^2 + 5^2$	$19 = ???$
...	...
$97 = 4^2 + 9^2$...
...	...

定理 (Fermat)

- 4 で割って 1 余る素数は, 2 つの平方数の和に (ただ一通りに) 書き表すことができる.
- 一方, 4 で割って 3 余る素数には, このような分解は (分数の利用を認めても) 存在しない.

注意

- 手作業 (あるいはコンピュータ) で調べていけば, 小さな素数については, 確かにこうなっていることが確認できる. しかしながら, **素数は無数に存在する**ので, いくら速いコンピュータを使っても, この定理は証明できない.
無限には **論理** をもって立ち向かうしかない.
- この定理は, それ自体は整数のはなしであるが, より広い数の世界である複素数の世界で捉えることによってはじめて, 明快な証明を得ることができる.

方程式(1)-Quiz

Quiz 2

鶴と亀がたくさんいます。頭の数进行数えると、10個あり、足の数进行数えると、34本ありました。鶴と亀は何匹ずついるでしょう？

答 (こんなことしなくても、頭の数进行数える途中で、分かるはず...)

鶴が x 羽、亀が y 匹いるとすると、頭の数について、 $x + y = 10$ が成り立つ。

また、足の数について、 $2 \times x + 4 \times y = 34$ が成り立つ。

つまり、

$$\begin{cases} x + y = 10 \\ 2x + 4y = 34 \end{cases}$$

の2つの式をともに満たす(自然)数 x, y を求めればよく、 $x = 3, y = 7$ 。

方程式 (2)

方程式とは？

- 等号の入った式を成り立たせる数を求める問題. 答を**解**とよぶ.
- $2x + 3y = 7$ のように, 変数が 2 つ, 式が 1 つだけ, という方程式 (**不定方程式**) も考えられる.
- 整数論の立場からは, **整数や有理数の解**に興味がある.

方程式 (3)-Fermat の定理の書き換え

素数の最後に出てきた定理を思い出す：

定理 (Fermat)

- 4 で割って 1 余る素数は、2 つの平方数の和に (ただ一通りに) 書き表すことができる。
- 一方、4 で割って 3 余る素数には、このような分解は (分数の利用を認めても) 存在しない。

この定理は、方程式を用いて表現すれば、次のようになる：

Fermat の定理の方程式による表示

p を素数とする。このとき、次の 2 条件は同値：

- 不定方程式 $x^2 + y^2 = p$ は有理数解をもつ。
- $p = 2$ または p は 4 で割ると 1 余る。

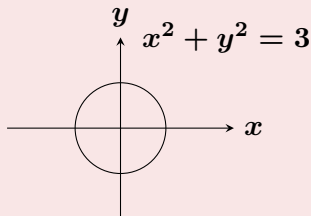
方程式(4)-代数幾何学

方程式の図形的解釈

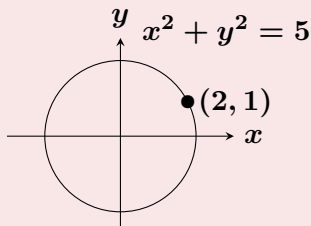
- さらに読み替えると, これは,

xy 平面上の原点中心, 半径 \sqrt{p} の円 $x^2 + y^2 = p$

の上に有理点 (x 座標も y 座標も有理数である点) が存在するかしないか, という図形の問題とも解釈できる (代数幾何学のアイデア).



ひとつも有理点がない



有理点が(無数に)存在する

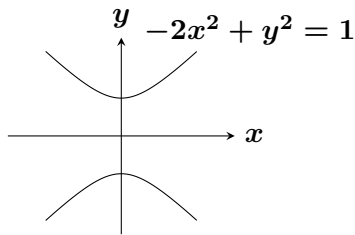
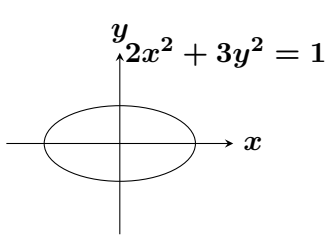
方程式(5)-曲線上の有理点

$x^2 + y^2 = p$ の両辺を p で割り、 $\frac{1}{p}x^2 + \frac{1}{p}y^2 = 1$ としても、有理点が存在するかどうかは変わらないので、 x^2 と y^2 の係数を一般にして次のような問題を考えたい。

Question 1

a, b は有理数とする。

曲線 $ax^2 + by^2 = 1$ 上に有理点が存在するような a, b の条件は？



四元数環 (1)

数の世界の広がり

- 自然数 : $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.
この中では, 足し算と掛け算はできるが, 引き算ができない.
例 : $1 - 3 = ?$
- 整数 : $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.
この中では, 足し算引き算掛け算はできる (こういう数の集まりを環という) が, 割り算はできない.
例 : $-3 \div 5 = ?$
- 有理数 : $\mathbb{Q} = \left\{ \frac{a}{b} \text{ (} a \text{は整数, } b \text{は} 0 \text{以外の自然数)} \right\}$
このなかでは, 四則が全てできる (こういう数の集まりを体という) が, 方程式 $x^2 = 2$ はこの中では解けない.

四元数環 (2)

数の世界の広がり

- 実数： $\mathbb{R} = \{\text{小数表示できる数}\}$
実数全体の集まりは体であるが、方程式 $x^2 = -1$ はこの中では解けない。
- 複素数： $\mathbb{C} = \{a + bi \text{ (} a, b \text{は実数) と表される数}\}$
ここで、 i は $i^2 = -1$ を満たす仮想的な数 (虚数単位)

数の世界

- 演算 (足し算や割り算など) で閉じていることが大切。
- うまく数を付け加えて広げることができる。
- 今見た数の世界は可換 (掛け算の順序を逆にしてもよい)。
例： $3 \times 5 = 5 \times 3$
- 一方で、非可換な数の世界もある。
例：行列の世界は $AB = BA$ は一般には成立しない。

非可換な数の世界を作ってみる

- 有理数体 \mathbb{Q} から拡張する.
- 2つの有理数 a, b を持つてくる.
- i, j を $i^2 = a, j^2 = b$ となる**仮想的な数**とする.
注: i, j は \sqrt{a} や \sqrt{b} という実数 (複素数) ではない!
- **非可換にしたい**ので, 仮想的な数 i と j の掛け算を

$$i \cdot j = -j \cdot i$$

と決める. 簡単のため $k = i \cdot j$ とおく.

- 有理数と, 仮想的な数 i, j, k たちの掛け算は可換とする.

四元数環 (4)-四元数環の構成

四元数環

- 有理数 a, b を固定する.
- 仮想的な数 i, j, k の決め方は前のおりとする.
- p, q, r, s を有理数として,

$$p + q \cdot i + r \cdot j + s \cdot k$$

の形に表される数を**四元数**という.

- 四元数全体の集まりを**四元数環**といい, 記号 $\left(\frac{a, b}{\mathbb{Q}}\right)$ で表す.

四元数環 (5)-例 1 : $\left(\frac{-2,5}{\mathbb{Q}}\right)$ の世界の計算

Example ($i^2 = -2, j^2 = 5, k = ij = -ji$)

- 和 : $(1 + 2i - j + 5k) + (-2 + 3j) = -1 + 2i + 2j + 5k$
- 積 :

$$\begin{aligned}(2 + 3i)(1 - j + k) &= 2 - 2j + 2k + 3i - 3ij + 3ik \\ &= 2 - 2j + 2k + 3i - 3k + 3i^2j \\ &= 2 - 2j + 2k + 3i - 3k + 3(-2)j \\ &= 2 + 3i - 8j - k,\end{aligned}$$

$$\begin{aligned}(1 - j + k)(2 + 3i) &= 2 + 3i - 2j - 3ji + 2k + 3ki \\ &= 2 + 3i - 2j - 3(-k) + 2k + 3(-ji)i \\ &= 2 + 3i - 2j + 3k + 2k + 6j \\ &= 2 + 3i + 4j + 5k\end{aligned}$$

- これからも分かるように, 掛け算は**非可換**である.

四元数環 (6)-例 1 : $\left(\frac{-2,5}{\mathbb{Q}}\right)$ の世界の計算

Example ($i^2 = -2, j^2 = 5, k = ij = -ji$)

- 実は, この数の世界では**割り算もできる!** (=0以外のどんな数にも逆数がある!)

例: 分子分母に**共役四元数**をかけると...

$$\begin{aligned}\frac{1}{1 + 2i + 3j + 4k} &= \frac{1 - 2i - 3j - 4k}{1^2 - (-2)2^2 - 5 \cdot 3^2 - (-10)4^2} \\ &= \frac{1}{196} - \frac{1}{98}i - \frac{3}{196}j - \frac{1}{49}k\end{aligned}$$

- したがって, 四元数環 $\left(\frac{-2,5}{\mathbb{Q}}\right)$ は四則が全てできる体になっている (ただし, 掛け算は非可換). 通常, 可換な体と区別して, **斜体**とよぶ.

四元数環 $(\frac{1,1}{\mathbb{Q}})$ の世界の計算

Example $(i^2 = 1, j^2 = 1, k = ij = -ji)$

- この世界でも、足し算引き算と、(非可換な) 掛け算が同様に考えられるが、この数の世界では割り算はできない(=0以外にも逆数がない数がある)ので、**斜体にはならない**.

例： $1 + i$ には逆数がない。

証明：背理法で示す。 $1 + i$ の逆数 $x = p + qi + rj + sk$ があるとすると、 $(1 + i)x = 1$ となる。ここで、両辺に**左から** $1 - i$ をかけると、 **$(1 - i)(1 + i)x = 1 - i$** となるが、

$$(1 - i)(1 + i) = 1^2 + i - i - i^2 = 1 - 1 = 0$$

なので、 $0 = 1 - i$ となって矛盾。

- 実は、四元数環 $(\frac{1,1}{\mathbb{Q}})$ は**2次正方形行列全体からなる環 $M_2(\mathbb{Q})$ と同じ構造を持っている**ことが知られている。

四元数環 (8)-2 種類の四元数環

注意

いままでの例を通して分かるように, 四元数環 $\left(\frac{a, b}{\mathbb{Q}}\right)$ には,

- 斜体の構造をもつ (割り算もできる) もの
- 行列環と同じ構造をもつ (割り算ができない) もの

という 2 種類があることがわかった.

そこで, 次のような問題を考えたい.

Question 2

a, b は有理数とする.

四元数環 $\left(\frac{a, b}{\mathbb{Q}}\right)$ が斜体となるような a, b の条件は?

まとめ-曲線上の点と数の拡張の結びつき

Question 1(曲線上の有理点に関する問題)

a, b は有理数とする.

曲線 $ax^2 + by^2 = 1$ 上に有理点が存在するような a, b の条件は?

Question 2(非可換な数の世界の構造の問題)

a, b は有理数とする.

四元数環 $\left(\frac{a, b}{\mathbb{Q}}\right)$ が斜体となるような a, b の条件は?

定理

a, b を有理数とする. 次の2条件は同値である.

- 曲線 $ax^2 + by^2 = 1$ 上に有理点が存在しない.
- 四元数環 $\left(\frac{a, b}{\mathbb{Q}}\right)$ は斜体となる.

ご清聴ありがとうございました

体の Brauer 群とは？

- 体 K (四則ができる数の集まり) からどれくらいの種類の**中心的単純環** (四元数環の一般化) が作れるかを表すもの. $\text{Br}(K)$ で表す.
- $\text{Br}(\mathbb{C}) = \{[\mathbb{C}]\}$ (=複素数から出発して, 非可換な数の世界は広げられない).
- $\text{Br}(\mathbb{R}) = \left\{ [\mathbb{R}], \left[\left(\frac{-1, -1}{\mathbb{R}} \right) \right] \right\}$.
- $\text{Br}(\mathbb{Q})$ の構造は非常に複雑 (=有理数上, 非可換な世界はたくさんある).

代数多様体の Brauer 群

- 円 $x^2 + y^2 = 1$ や平面 $2x + y - 3z = 0$ のように, 多項式で定義される図形を代数多様体という.
- 代数多様体 X の上に, 「非可換な関数」がどれくらいあるか, ということを表すものとして, Brauer 群 $\text{Br}(X)$ を作ることができる.
- 四元数環の構造が, 方程式の解の情報と結びついていたように, $\text{Br}(X)$ の様子から, 元の図形 X の性質を読み解くことができる.
- 曲線 $C : ax^2 + by^2 = 1$ の Brauer 群 $\text{Br}(C)$ は体の Brauer 群 $\text{Br}(\mathbb{Q})$ ともっている情報がちょっと少ない(か同じか)なので, 曲線 C 上の有理点を調べる上では, 体の Brauer 群 $\text{Br}(\mathbb{Q})$ のごく一部を解析すれば十分だった.

代数多様体の Brauer 群

- 一般には, 図形の Brauer 群 $\text{Br}(X)$ のほうが, 体の Brauer 群 $\text{Br}(K)$ よりもその図形に固有の情報を持っていることが多い.

Example (対角的 3 次曲面の場合 (U-, 2014))

- $a, b, c, d \in K$
 - $X : x^3 + by^3 + cz^3 + dw^3 = 0$ で定義される射影曲面
- (1) $b = 1$ の場合, $\text{Br}(X)$ が $\text{Br}(K)$ より, どれくらい多い情報を持っているかを定量的に計算し, その差分を係数 c, d から明示的に表す公式を求めた.
 - (2) b, c, d が一般に動く場合, どれくらい多い情報を持っているかは決定できるが, b, c, d を用いて明示的には表示できないことを示した.

四元数と回転

\mathbb{R} を元にして作られる四元数環 $\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}} \right)$ (ハミルトンの四元数環) は, 空間における回転を表すのに, 利用されることがある.
(参考 URL: 和歌山大床井氏の講義ノート
(<http://www.wakayama-u.ac.jp/tokoi/lecture/gg/ggbook04.pdf>))

四元数を使った回転の表示

- 空間の点 $A = (a_x, a_y, a_z)$ を四元数 $a = a_x i + a_y j + a_z k$ と同一視する.
- 回転の軸を表すベクトルを $\vec{d} = (d_x, d_y, d_z)$ とする.
- \vec{d} を軸として θ 回転させるとき, 四元数 x を $x = \cos \frac{\theta}{2} + (d_x i + d_y j + d_z k) \sin \frac{\theta}{2}$ と定める.
- 点 A を \vec{d} を軸として θ だけ回転させて得られる点 B に対応する四元数 b は $x a x$ に対応する.