整数と図形の深い関係

現代代数幾何に触れる

高校生のための公開講座（２０２２年１１月）

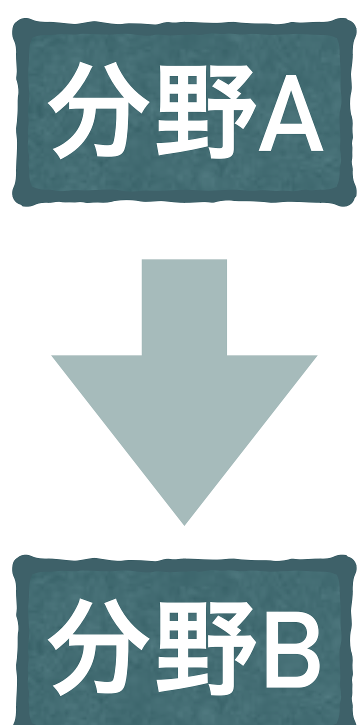
by 安田健彦

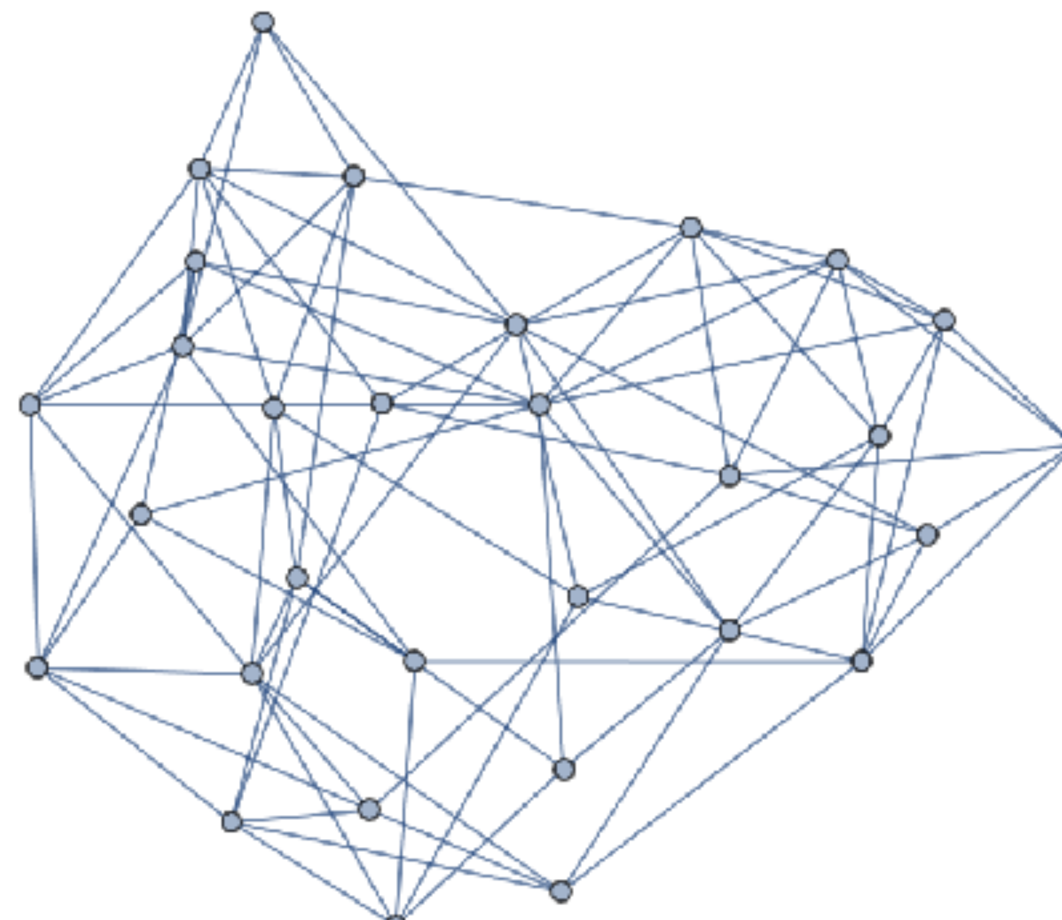
数学者なら誰でも知っているように，**ある理論から別の理論への曖昧な類推や不明瞭な考察**ほど豊穣なものはない

-アンドレ・ヴェイユ *(1906-1998)*

«De la métaphysique aux mathématiques»,
Œuvres, t. II, p. 408. 講演者訳

Konrad Jacobs - https://opc.mfo.de/detail?photo_id=4448, CC BY-SA 2.0 de, https://commons.wikimedia.org/w/index.php?curid=6079745による





分野間のネットワーク

数

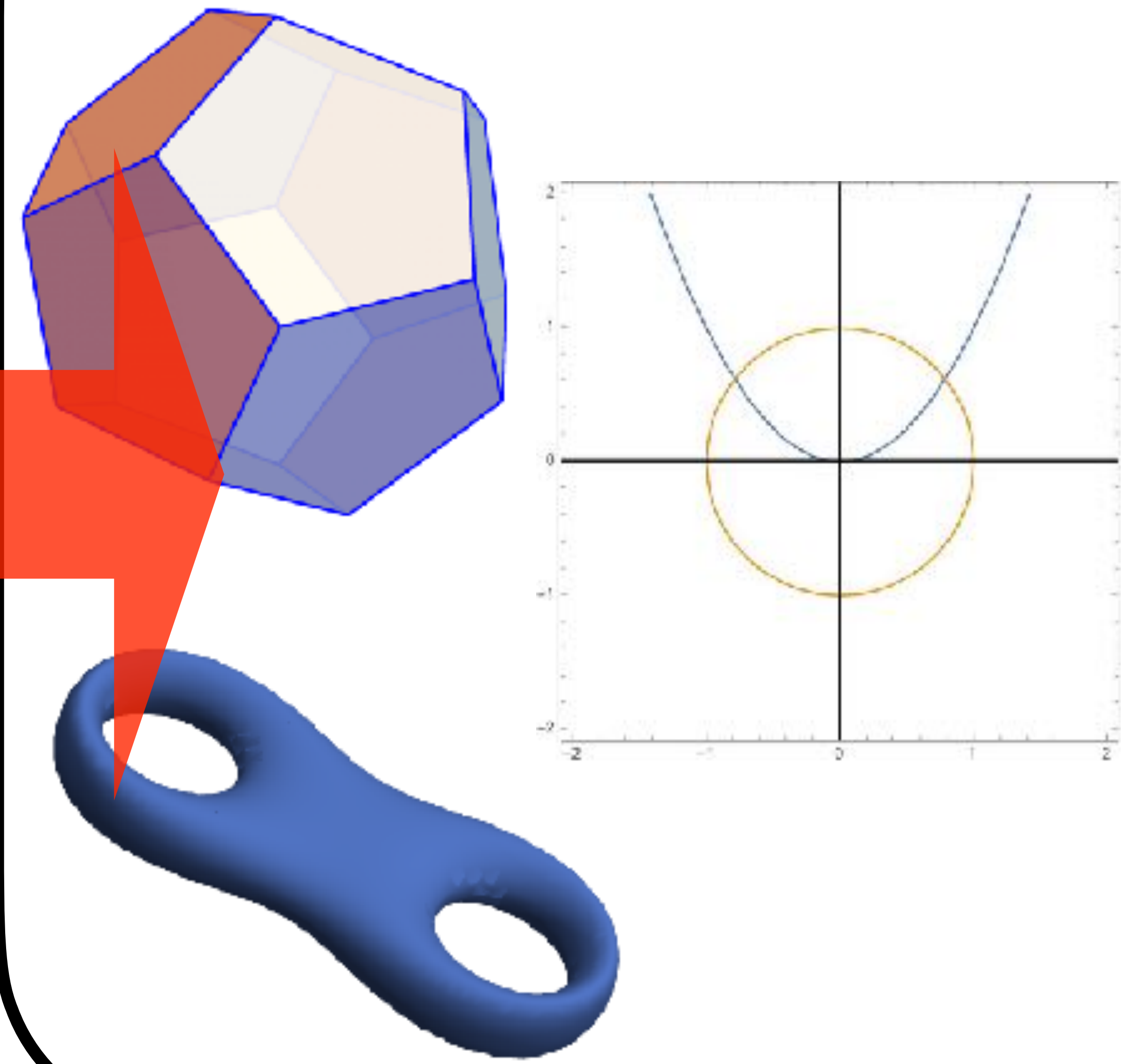
3

-7

$\sqrt{31}$

$2+5i$

形



整数論

幾何（トポロジー）

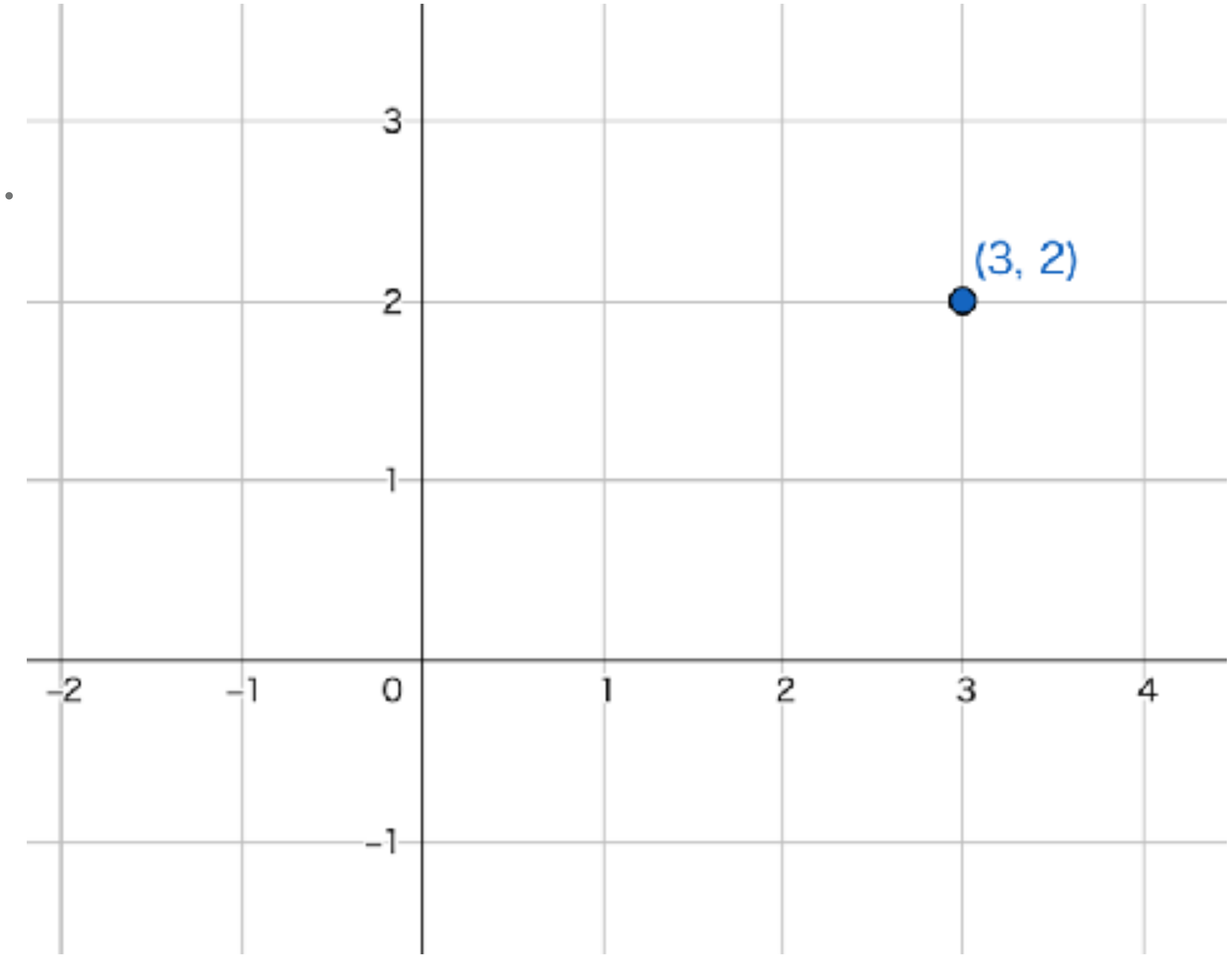
代数幾何

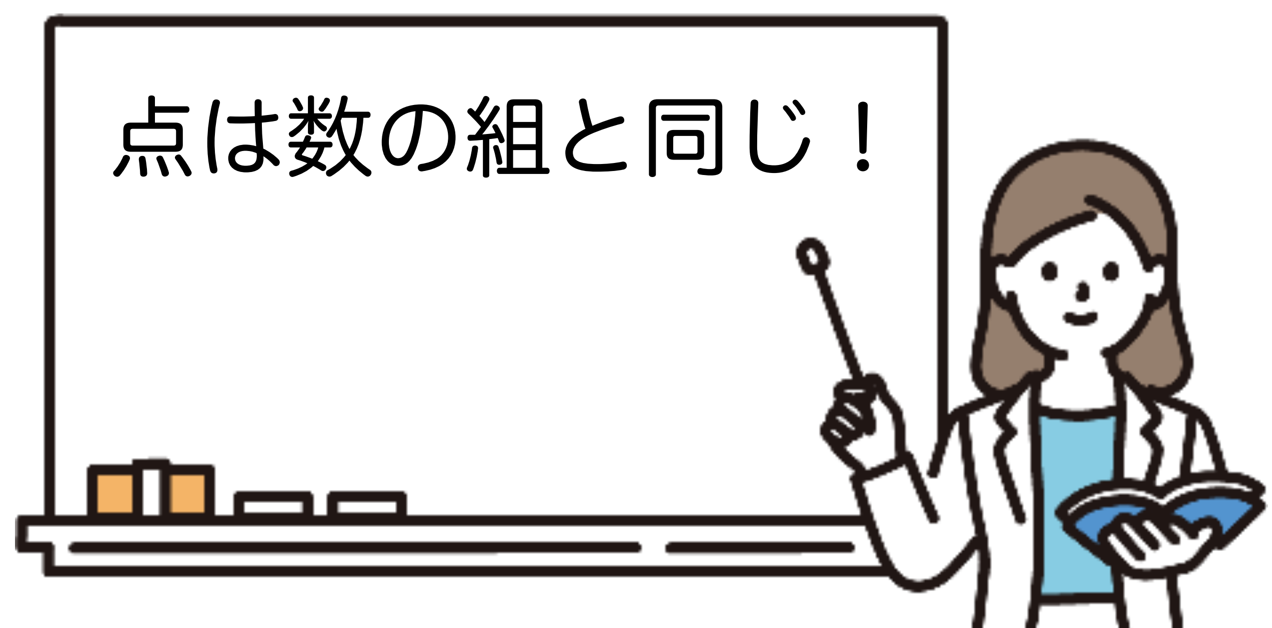
Algebraic Geometry

代数幾何とは

デカルトが「座標」を導入

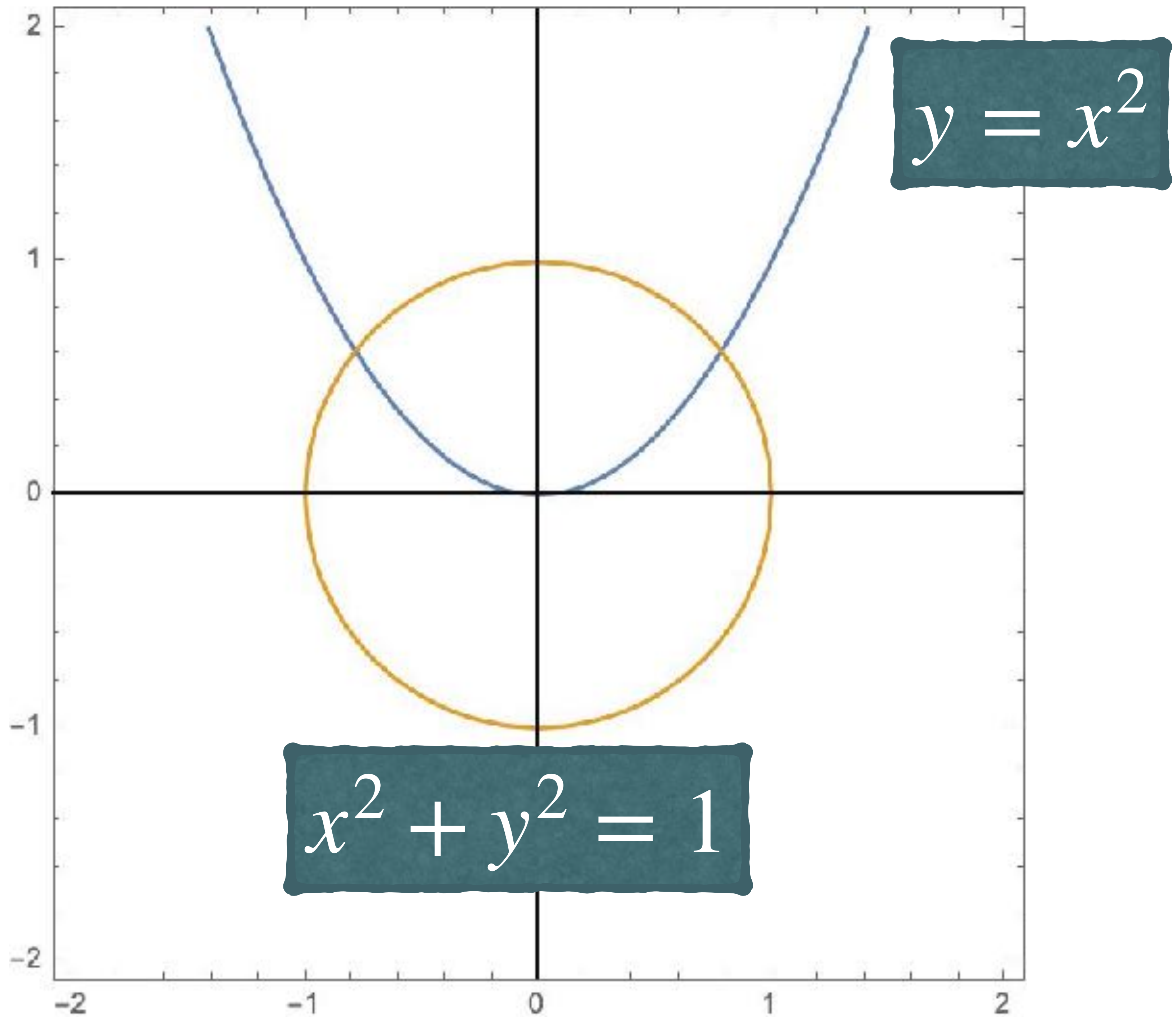
ルネ・デカルト
（1596-1650）





方程式と図形

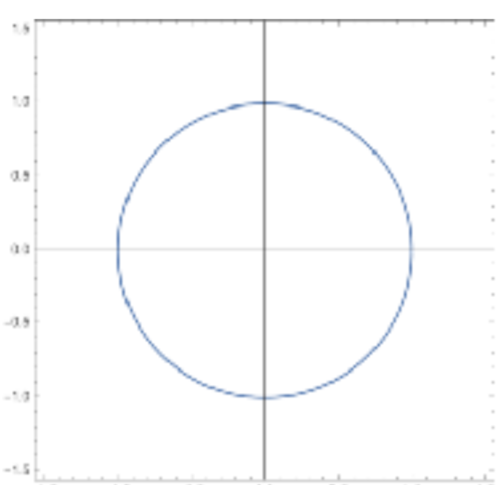
- 代数幾何では方程式が定める図形を調べる。



いくらでも複雑に

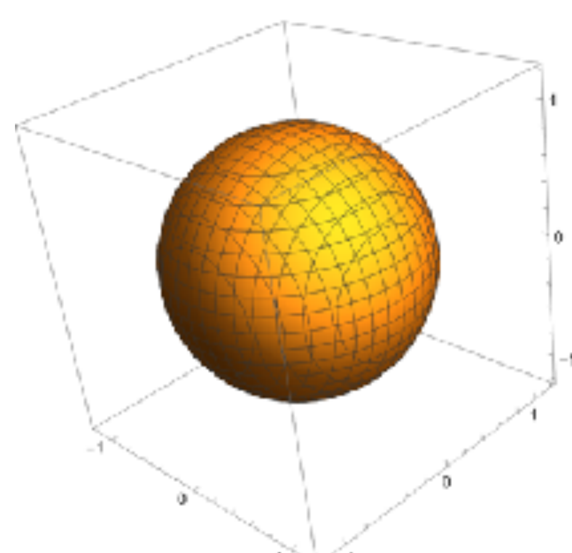
- 方程式でいくらでも複雑な図形を作れる。
- 連立方程式を考える、変数の数を増やす、式の次数を上げる、などの方法
- 図形の次元もいくらでも大きく出来る。（４次元の図形、２３次元の図形、２８７１次元の図形）

１次元



$x^2 + y^2 = 1$

２次元



$x^2 + y^2 + z^2 = 1$

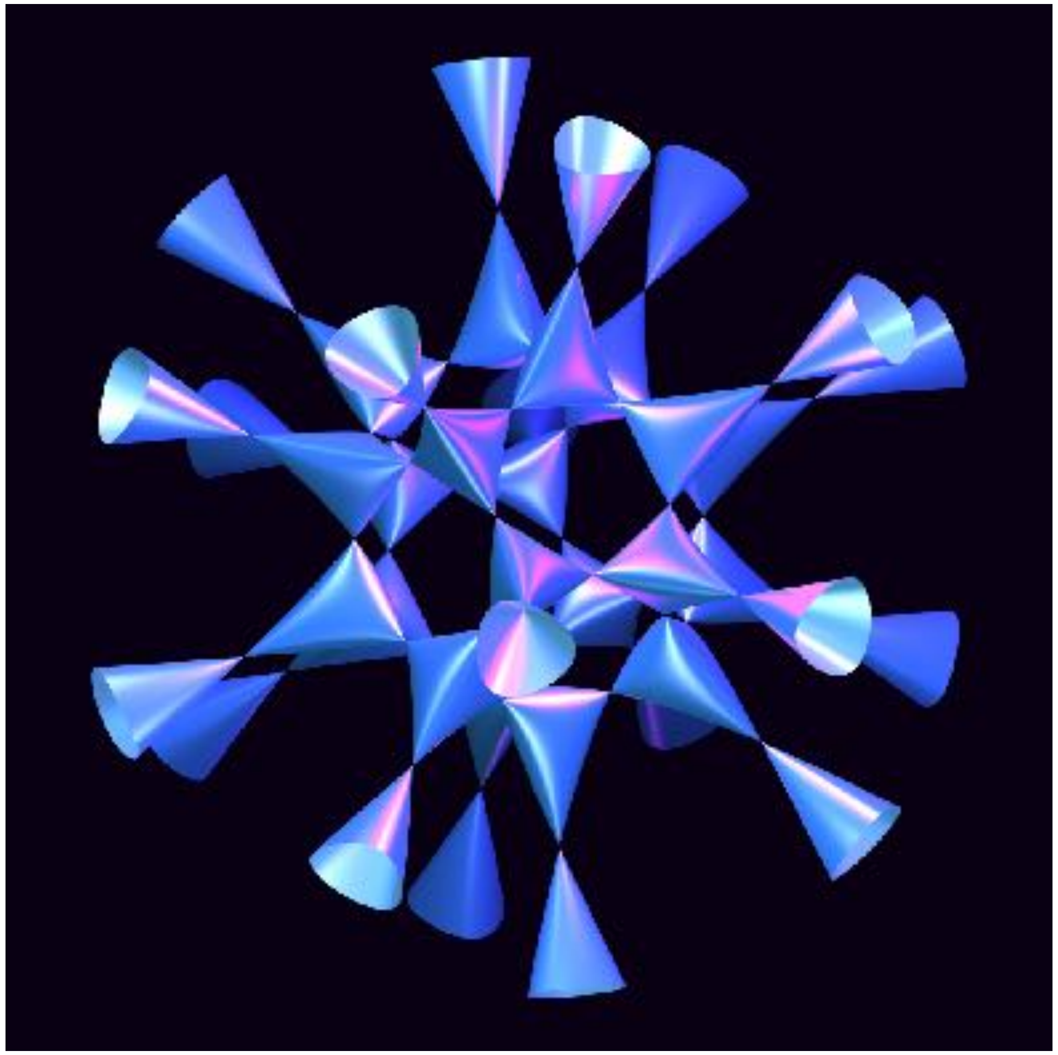
９次元

$x_1^2 + x_2^2 + \cdots + x_{10}^2 = 1$

BARTHの6次曲面

$$(a^2x^2 - y^2)(a^2y^2 - z^2)(a^2z^2 - x^2) - \frac{2a+1}{4}(x^2 + y^2 + z^2 - 1)^2 = 0$$

$$\left(a = \frac{1+\sqrt{5}}{2}\right)$$



Author: Oliver Labs
downloaded from www.imaginary.org

合同方程式

Congruence Equation

一つの方程式から

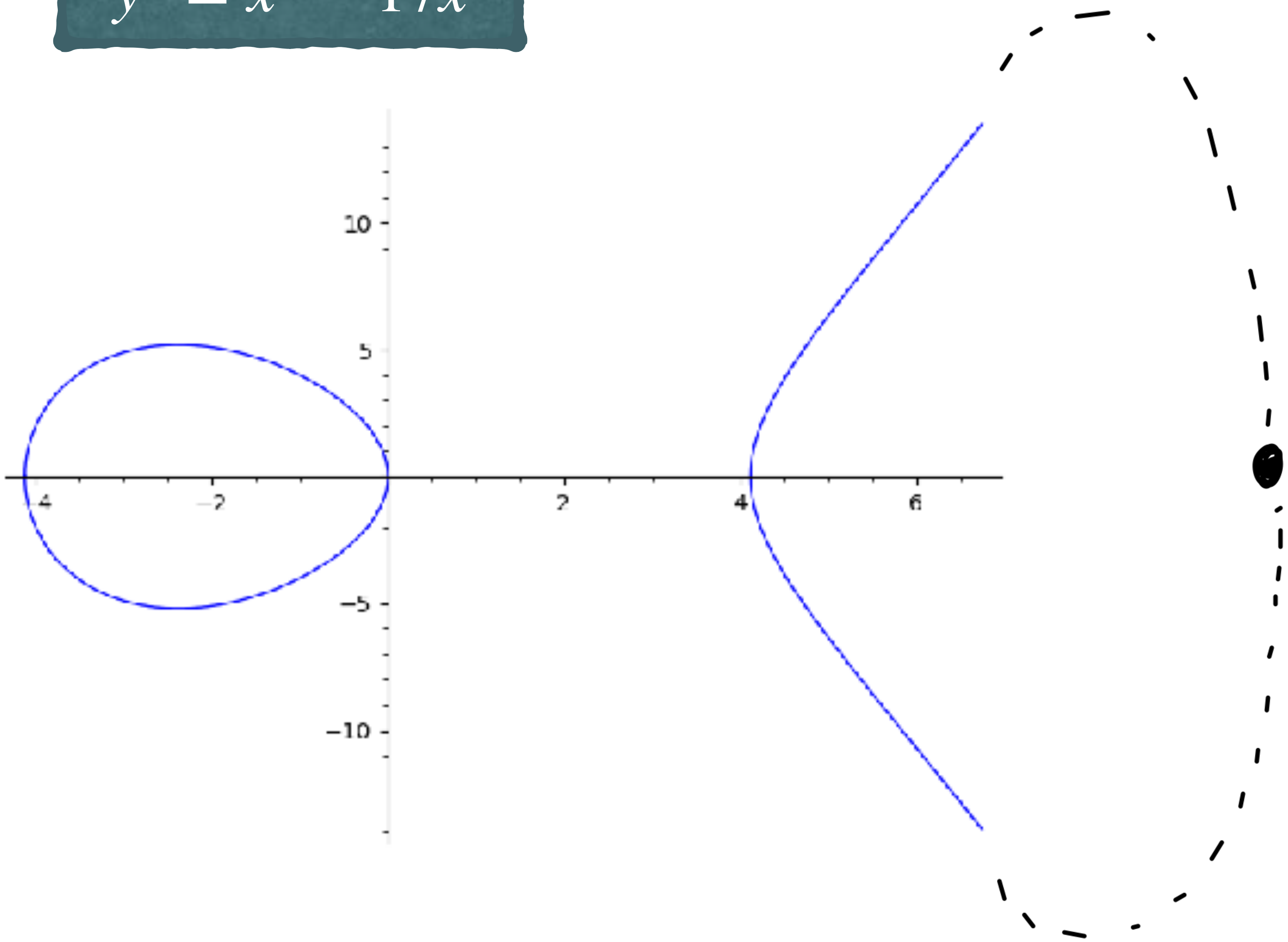
- 今日は次の方程式に注目！

$$y^2 = x^3 - 17x$$

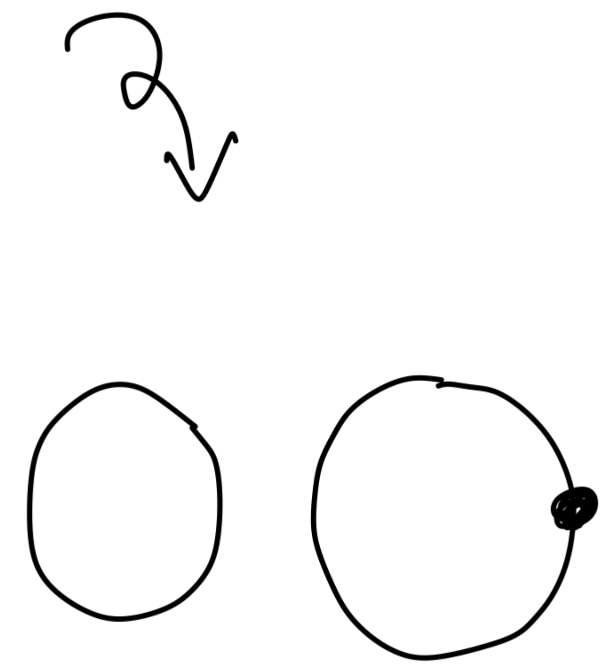
- 解をどの範囲から探す？
- 考える数の範囲によって、解全体の様子が変わる。

実数

$$y^2 = x^3 - 17x$$



無限遠点



遠近法

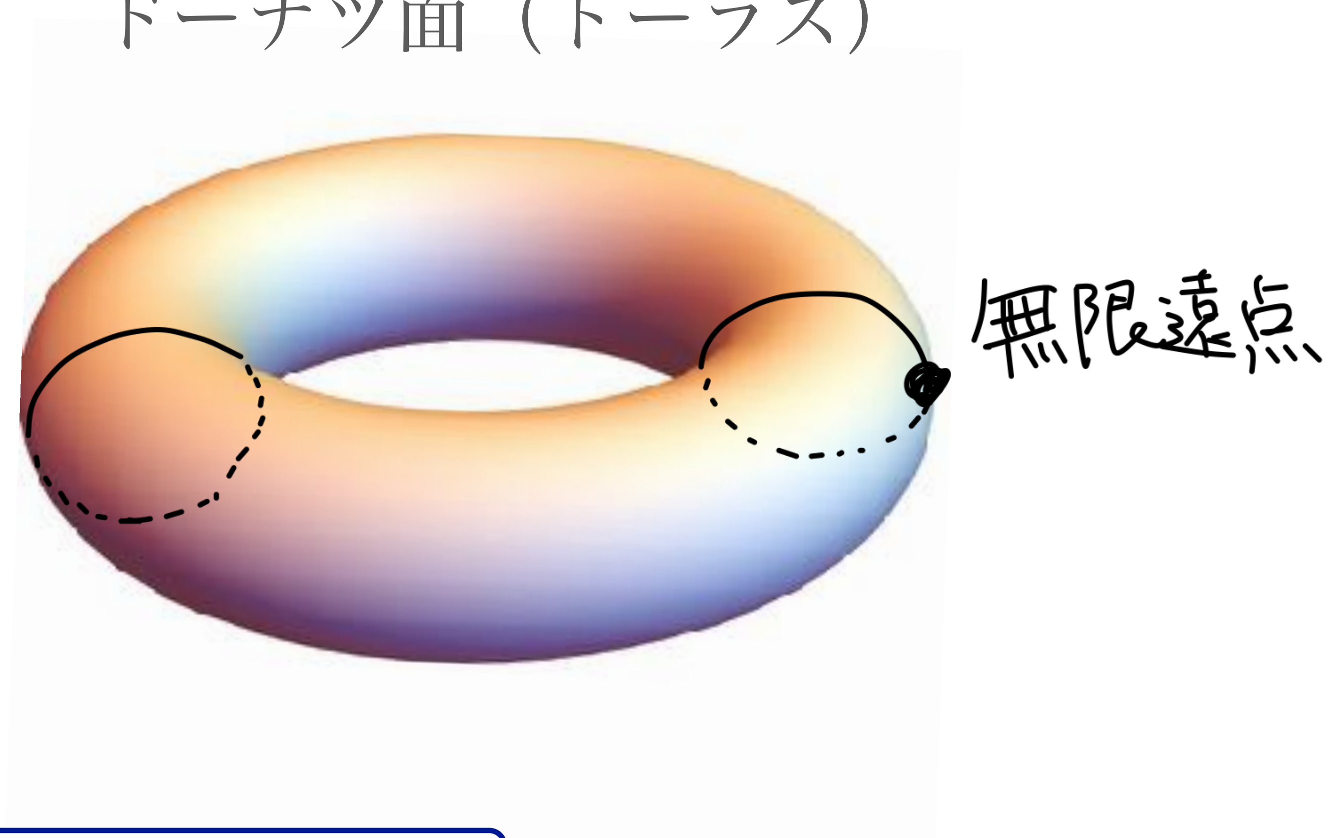
消失点

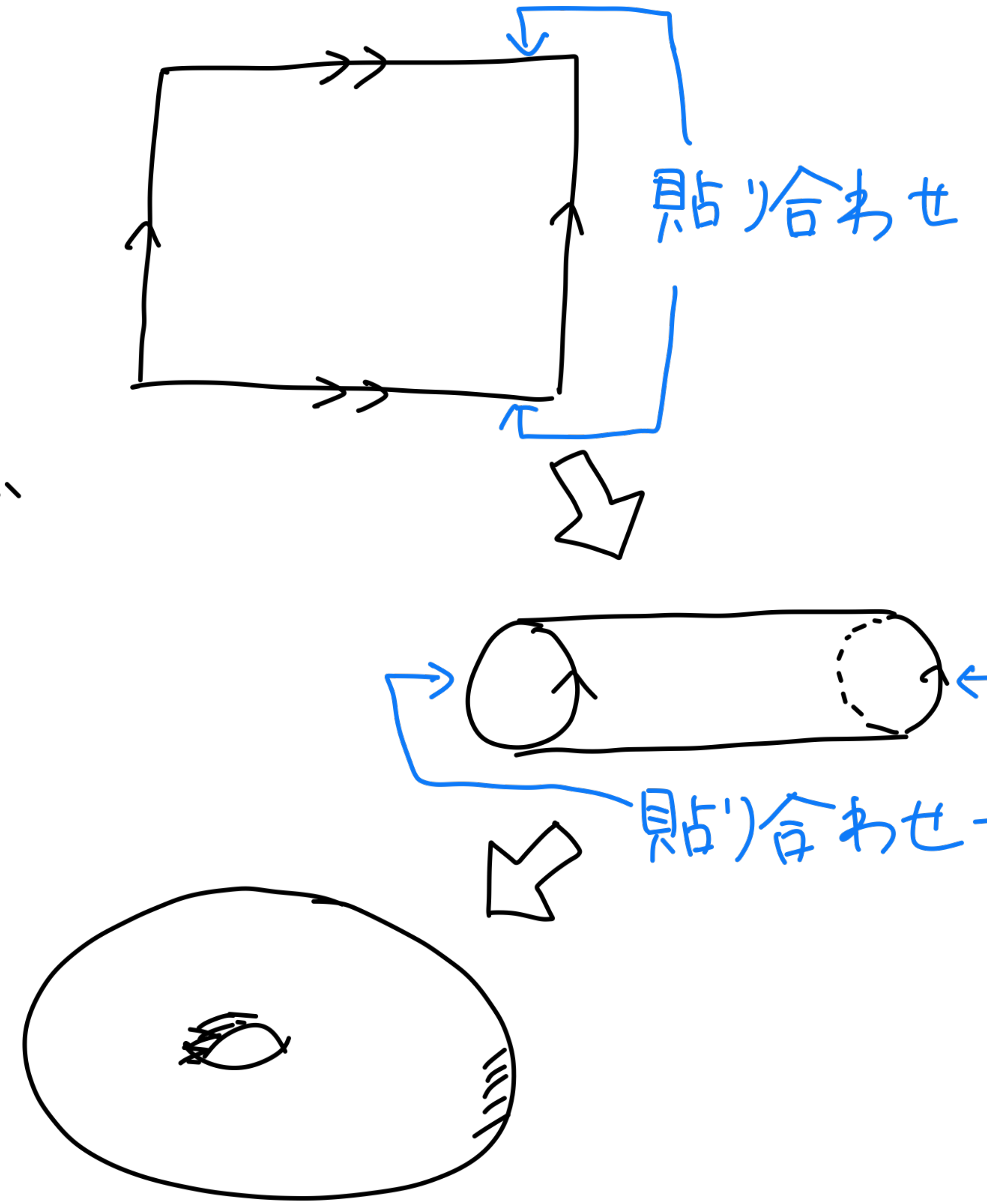
無限遠点を付け
足すと便利

複素数

$$y^2 = x^3 - 17x$$

ドーナツ面（トーラス）

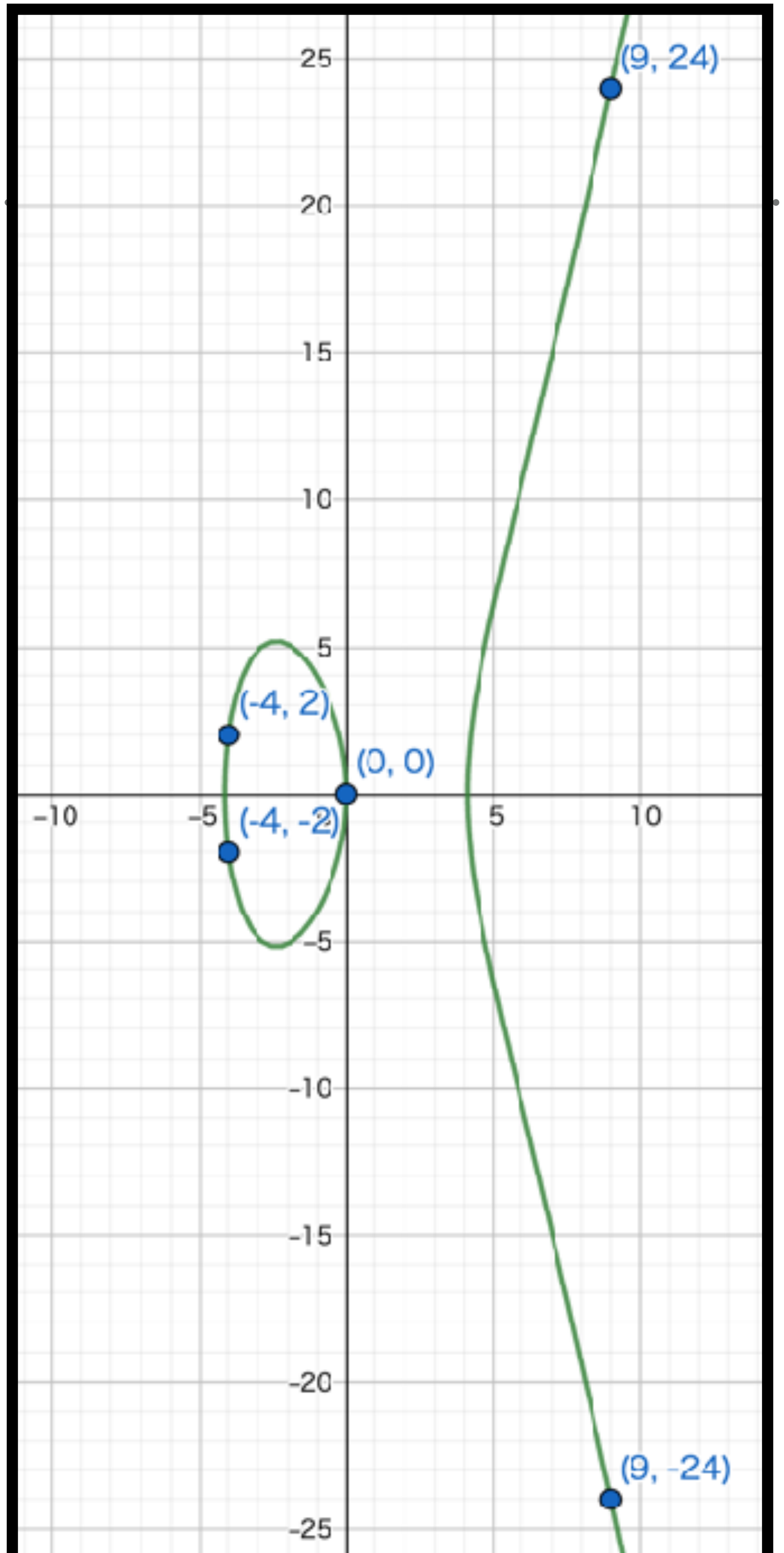




曲面（２次元）
になった！！

整数

$$y^2 = x^3 - 17x$$



合同式：MOD N

- 合同式の解を考えても良い。
- 合同式について少し復習しよう。
- 自然数nを固定し、nで割った**余りだけ**に注目して足し算、引き算、掛け算をする。これを「**nを法とした(mod n)合同式**」という。
- $3 + 11 \equiv 4 \mod 5$

mod 2

+	偶	奇
偶	偶	奇
奇	奇	偶

-	偶	奇
偶	偶	奇
奇	奇	偶

×	偶	奇
偶	偶	偶
奇	偶	奇

mod 3

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

-	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

合同方程式

- 「$2x + 1 \equiv 0 \mod 3$」の唯一つ解は「$x \equiv 1$」
- 3で割った余りが1の整数は全て解となるが、それらは同じグループなので、一つと数える。
- 「$2x + y \equiv 0 \mod 3$」の解は「$(x, y) \equiv (0,0), (1,1), (2,2)$」の三つ。

方程式「$y^2 = x^3 - 17x$」を合同式(MOD 5)で考えると

mod 5：

(0,0), (1,2), (1,3), (2,2), (2,3), (3,1), (3,4), (4,1), (4,4)

x \ y	0	1	2	3	4
0	●				
1			●	●	
2			●	●	
3		●			●
4		●			●

$y^2 \equiv x^3 - 17x \mod 5$

＋無限遠点 → １０個の点

ハッセの不等式

- **問題**：素数 p を法とした $y^2 = x^3 - 17x$ の解の個数 N_p はいくつ？（無限遠点を含む）
- **確率で考えると、、、**
- ランダムに選んだ組 (x, y) が解になる確率は$1/p$。
- 考える組(x, y)は全部で p^2 個。
- その中で解になるは p 個ぐらい？

無限遠点も入れると
$p+1$ 個ぐらいかな？

ハッセの不等式（続き）

➤ ハッセの不等式：下の不等式が常に成り立つ。

$$|N_p - (p+1)| \leqq 2\sqrt{p}$$

前の例 (mod 5)：$|10-6| = 4 \leq 2\sqrt{5} = 4.47\cdots$

不等式が成り立つのは分かったけど、これが形を扱う幾何学と関係ある？

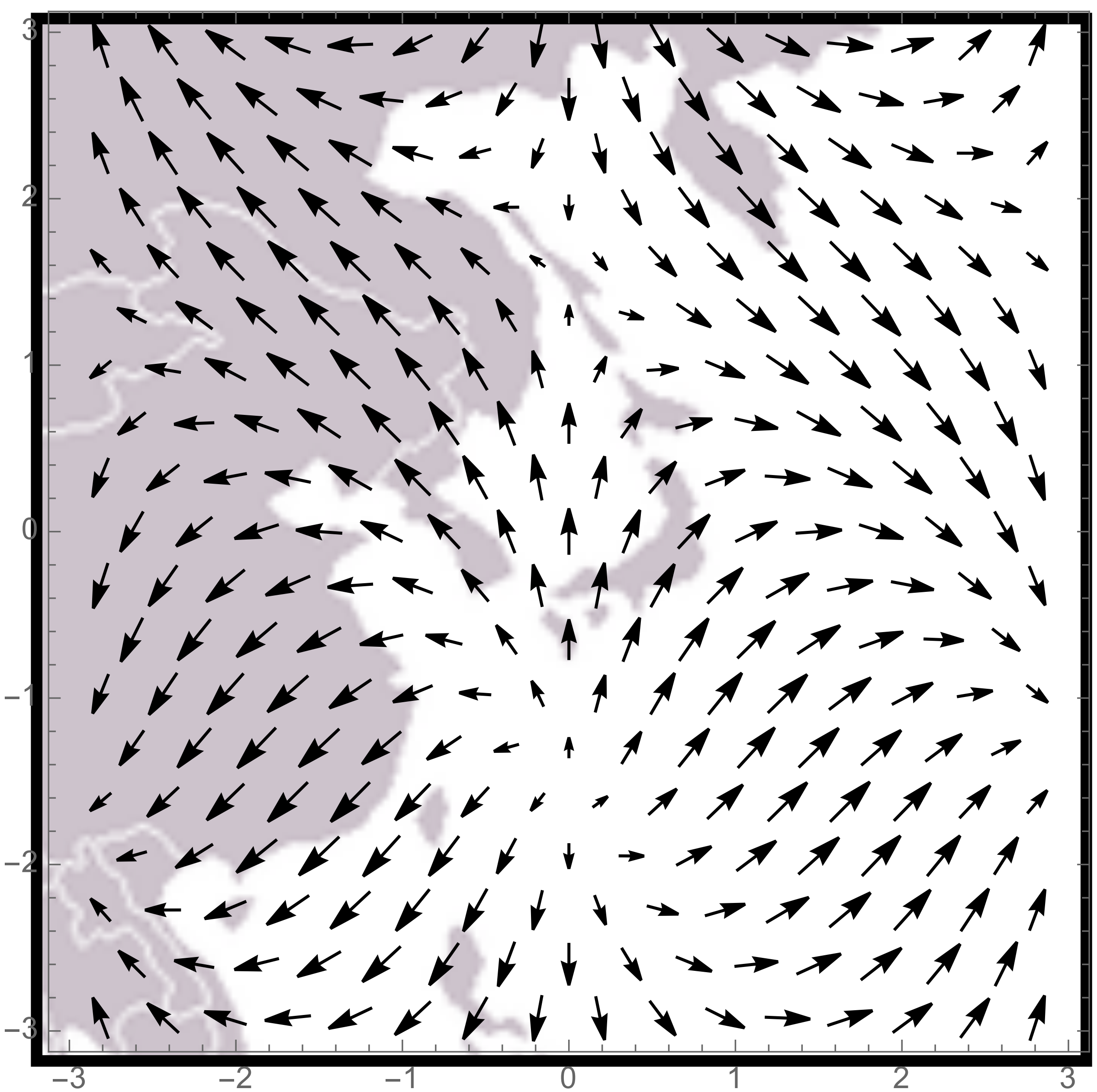
それを次のパートで見てみよう！

幾何を使って数える

Counting Points by Using Geometry

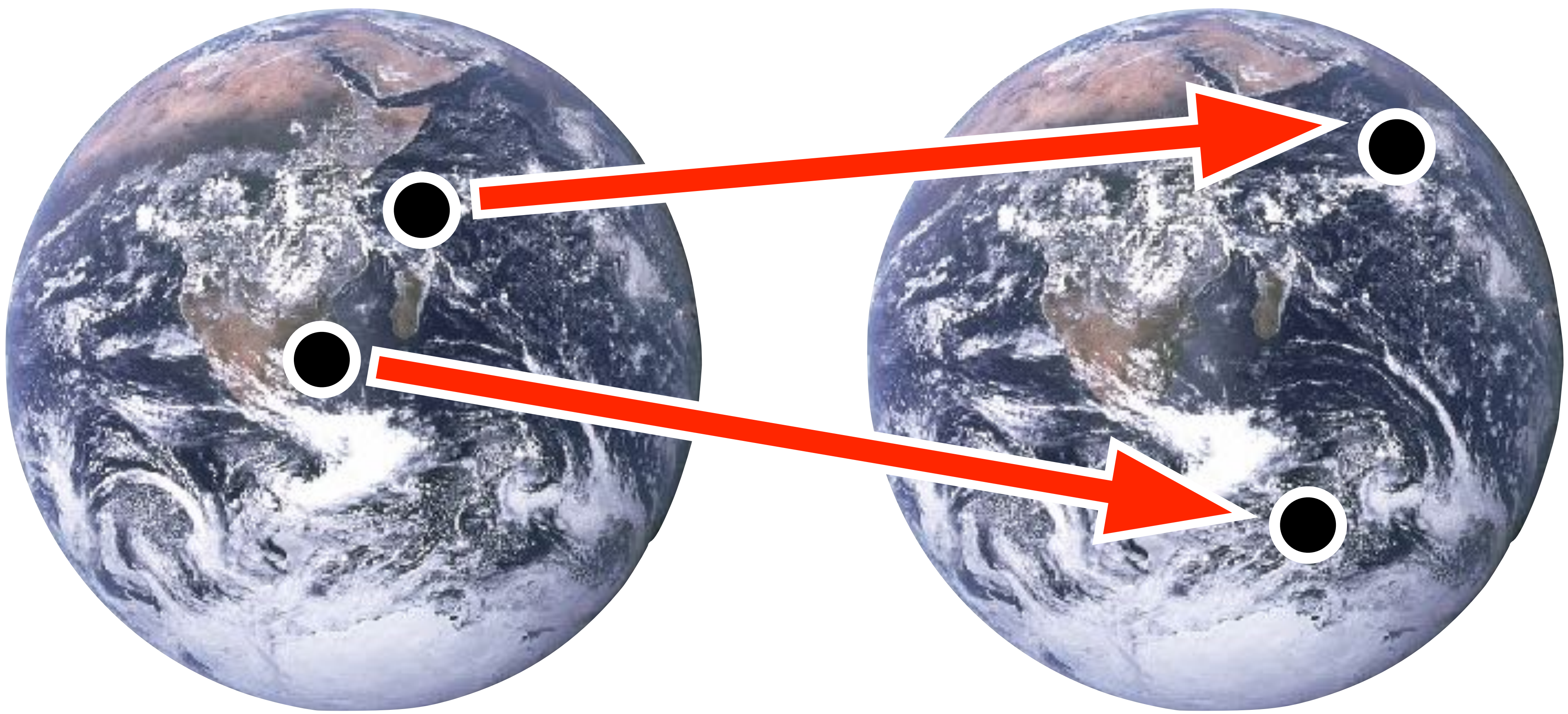
台風の目と不動点

風向・風速図



矢印は点の移動と解釈すると、、、

球面内の点の移動

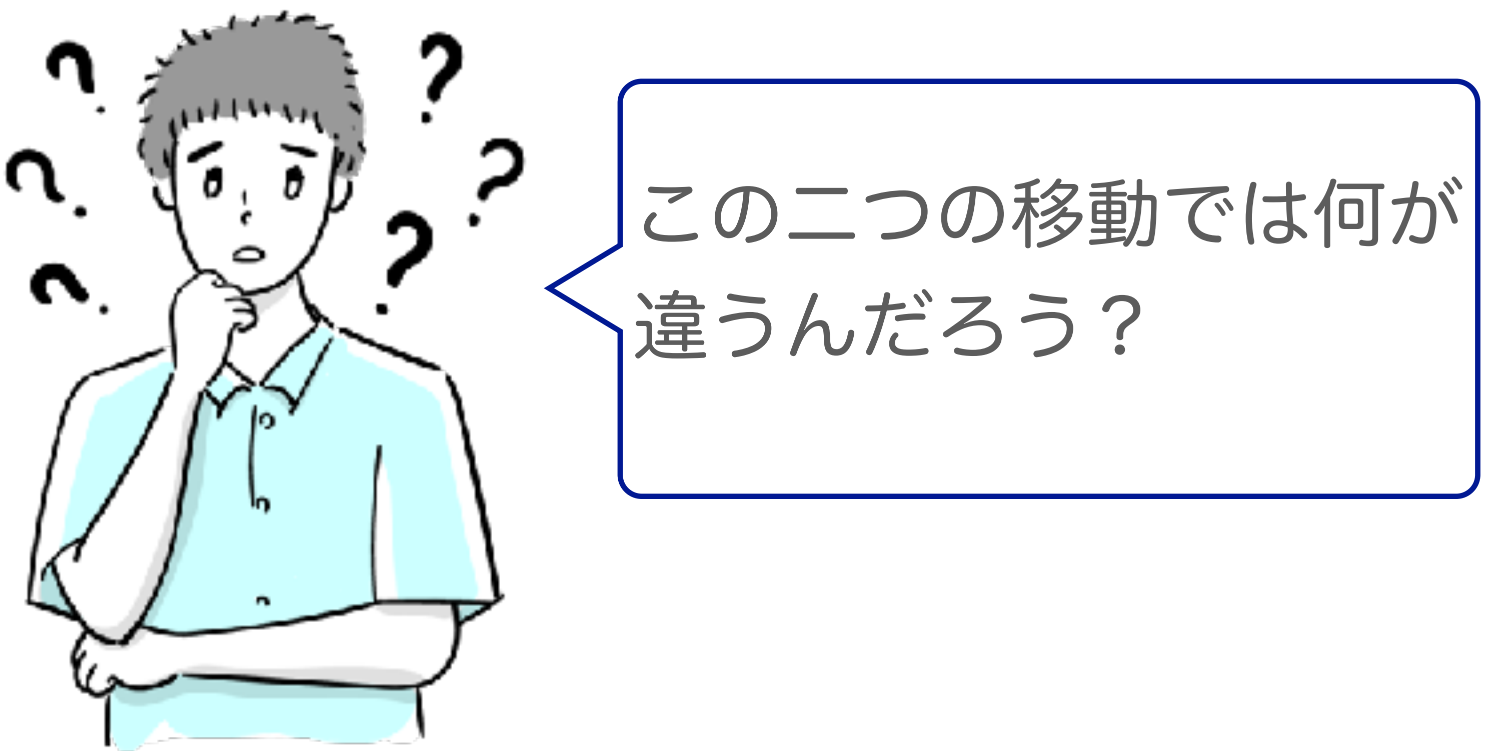


単位時間での点の移動を追いかけると、球面内の各点が別の点に移動している。

問題：不動点（移動しない点）はあるか？

答え

- 風による点の移動では不動点は存在する。
- 球面をひっくり返す点の移動（北極を南極に、日本をブラジルに移動）では不動点はない。



ソロモン・レフシェッツ
(1884-1972)

- **レフシェッツの定理**で説明できる！

行列（正方行列）

- 縦横にn個ずつ数を並べたものをn次行列（正方行列）という。
- 例：2次行列 $\begin{pmatrix} 3 & 0 \\ -1 & 4 \end{pmatrix}$

表みたいなものですね。

- n次行列はn次ベクトルの1次式による変化を表す。
- 上の2次行列はベクトル $\begin{pmatrix} x \\ y \end{pmatrix}$ を $\begin{pmatrix} 3 \cdot x + 0 \cdot y \\ -1 \cdot x + 4 \cdot y \end{pmatrix}$ に送る。

1次式なら簡単だぜ！

行列の跡（セキ）

- 左上から右下への対角線部分を足し合わせたものを**跡（せき）**という。

$$\begin{pmatrix} 1 & 5 & -6 \\ 0 & -3 & 1 \\ 7 & 2 & 15 \end{pmatrix} \qquad \text{跡：} 1 + (-3) + 15 = 13$$

- 跡はn^2個の数という大きな情報から、重要な一つの数を取り出す。

レフシェッツの定理

- 曲面の点の移動に対し、3つの行列が定まる：

$$A_0 = (1) \qquad A_1 = \begin{pmatrix} ? & ? & \cdots \\ ? & ? & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix} \qquad A_2 = (?)$$

1次行列　　n次行列　　1次行列

0次元（点）の移動の情報　**1次元（曲線）の移動の情報**　**2次元（曲面）の移動の情報**

- $L =$（A_0の跡）－（A_1の跡）＋（A_2の跡）　の値に注目する

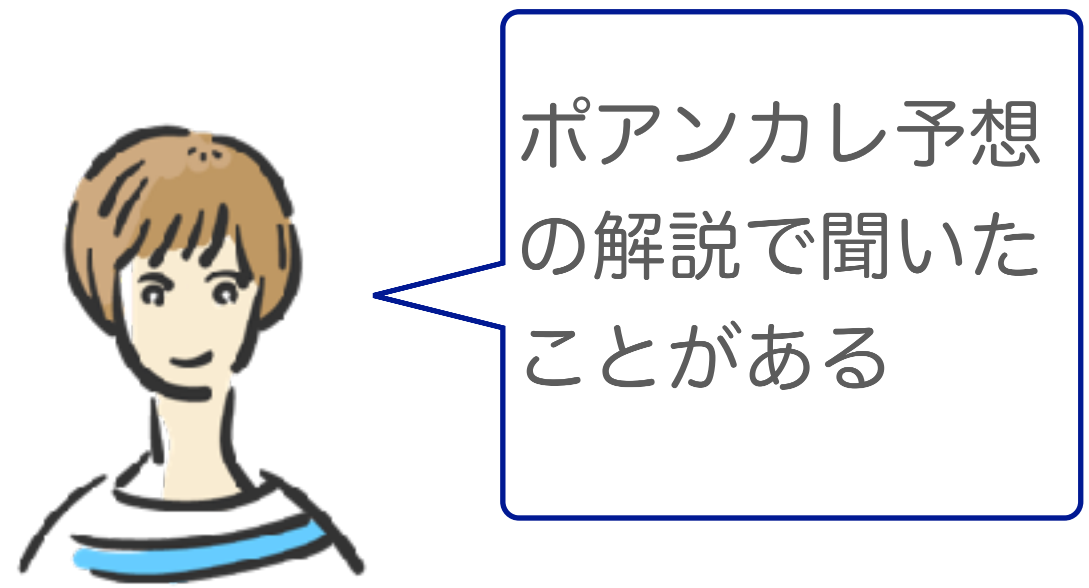
レフシェッツ数

レフシェッツの定理（続き）

- $L =$（A_0の跡）$-$（A_1の跡）$+$（A_2の跡）$\neq 0$　**ならば不動点有り。**
- （不動点が有限個のとき、）L **は不動点を重複度込みで数えた個数になる。**

地球（球面）の場合：風による移動

- $A_0 = (1)$
- A_1は0次行列。（球面上の輪っかは1点に縮められるから）
- $A_2 = (1)$
- $L = 1 - 0 + 1 = 2 \neq 0 \quad \Rightarrow$ 不動点有り
- 地球の自転の場合、不動点は北極と南極の2個



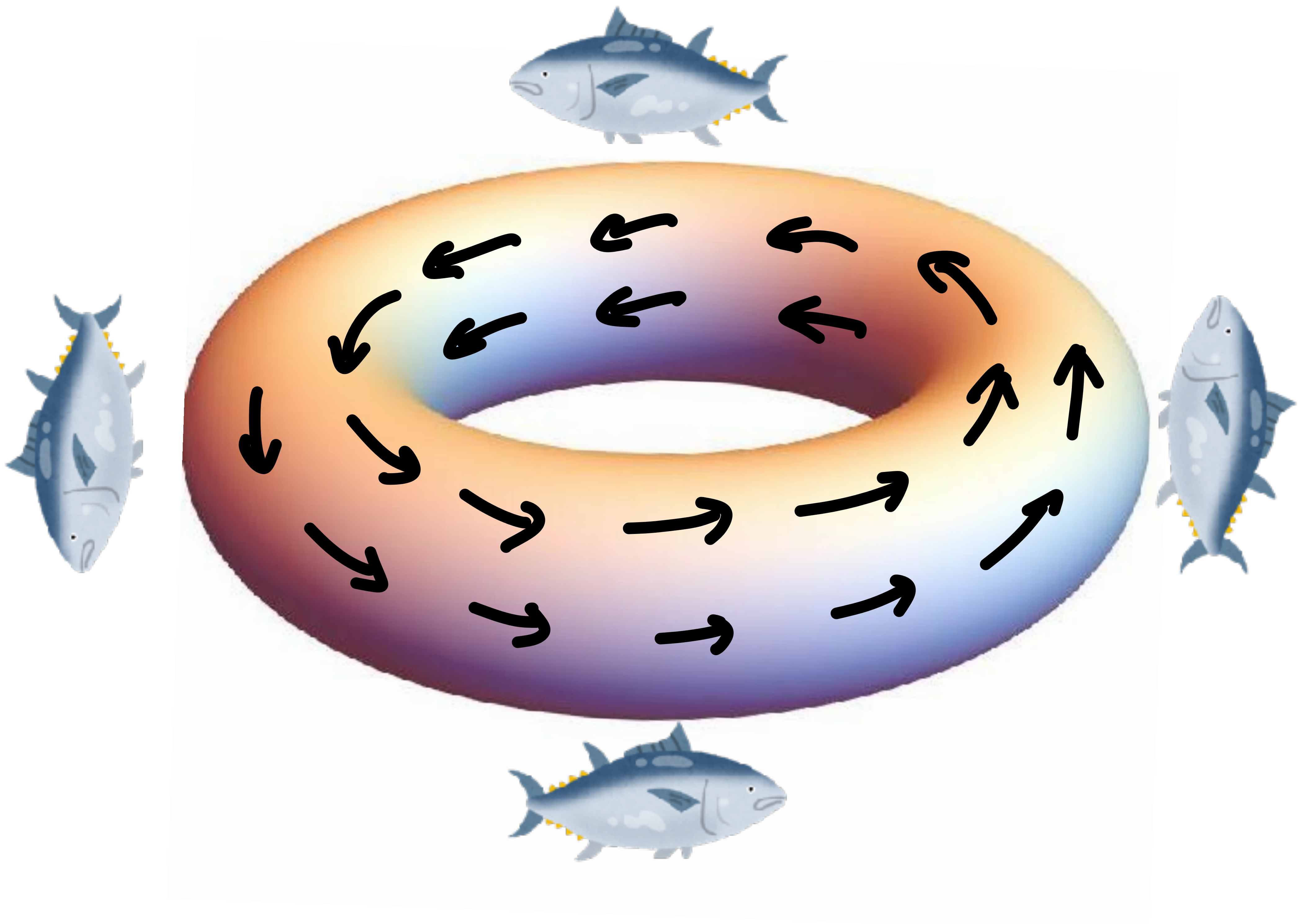
地球（球面）の場合：ひっくり返し

- $A_0 = (1)$
- A_1は0次行列。（球面上の輪っかは1点に縮められるから）
- $A_2 = (-1)$
- $L = 1 - 0 + (-1) = 0$ なので、不動点がなくてもいい 。
- ひっくり返し移動では、実際に不動点がない。

ひっくり返るから、マイナス1倍するのか

ドーナツ面の場合

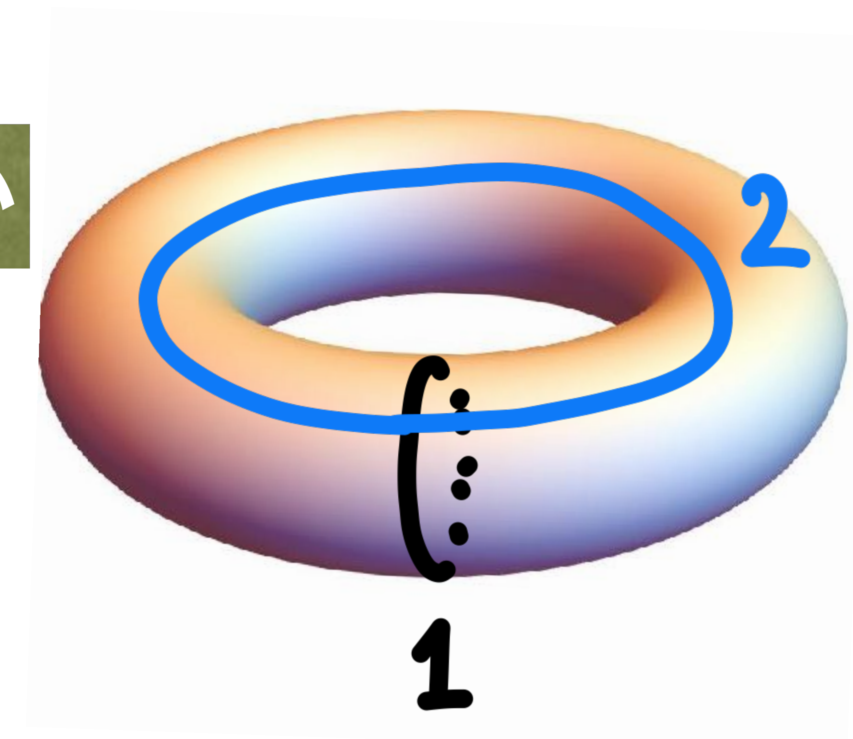
- ドーナツ型惑星では、不動点無しの風移動が可能



ドーナツ面のレフシェッツの定理

2次行列 $\Leftarrow$ 2つの輪っか

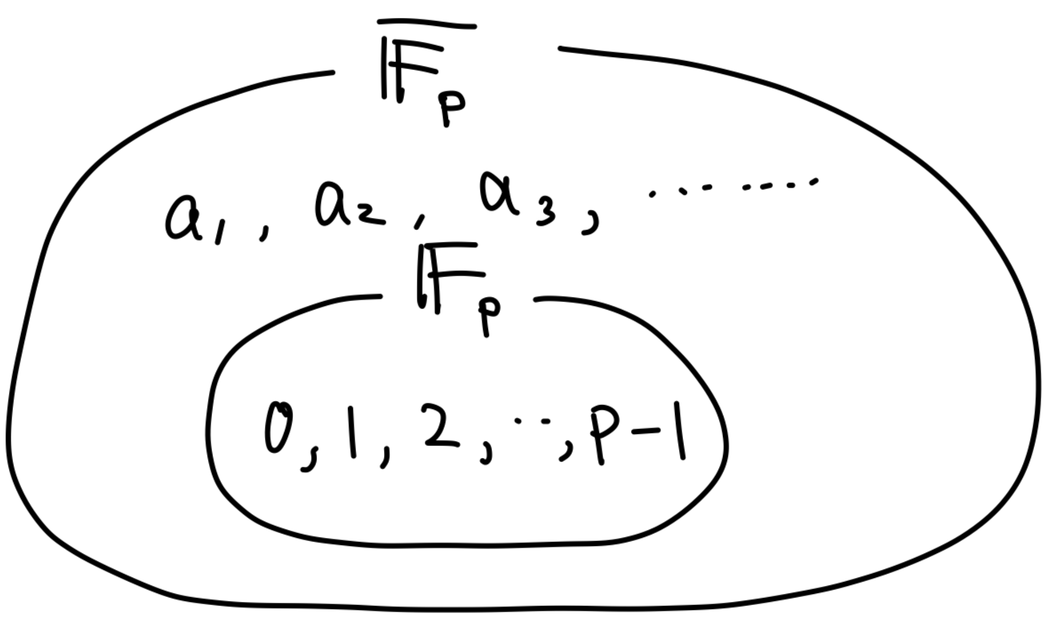
- $A_0 = (1)$
- $A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- $A_2 = (1)$
- $L = 1 - 2 + 1 = 0$ となり、不動点はなくても良い。

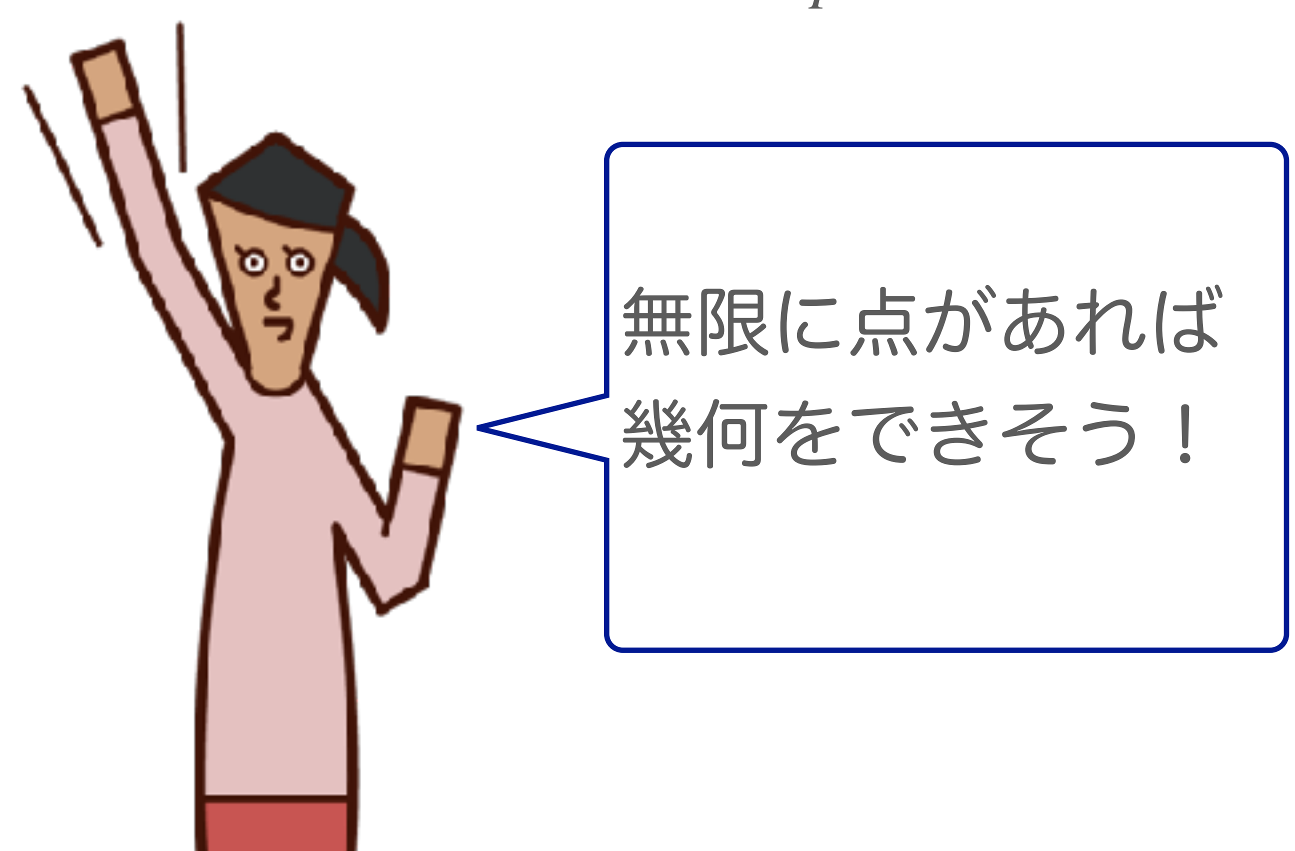


１タイプのループは１タイプのループへ移動
２タイプのループは２タイプのループへ移動

p 元体 $\mathbb{F}_p$

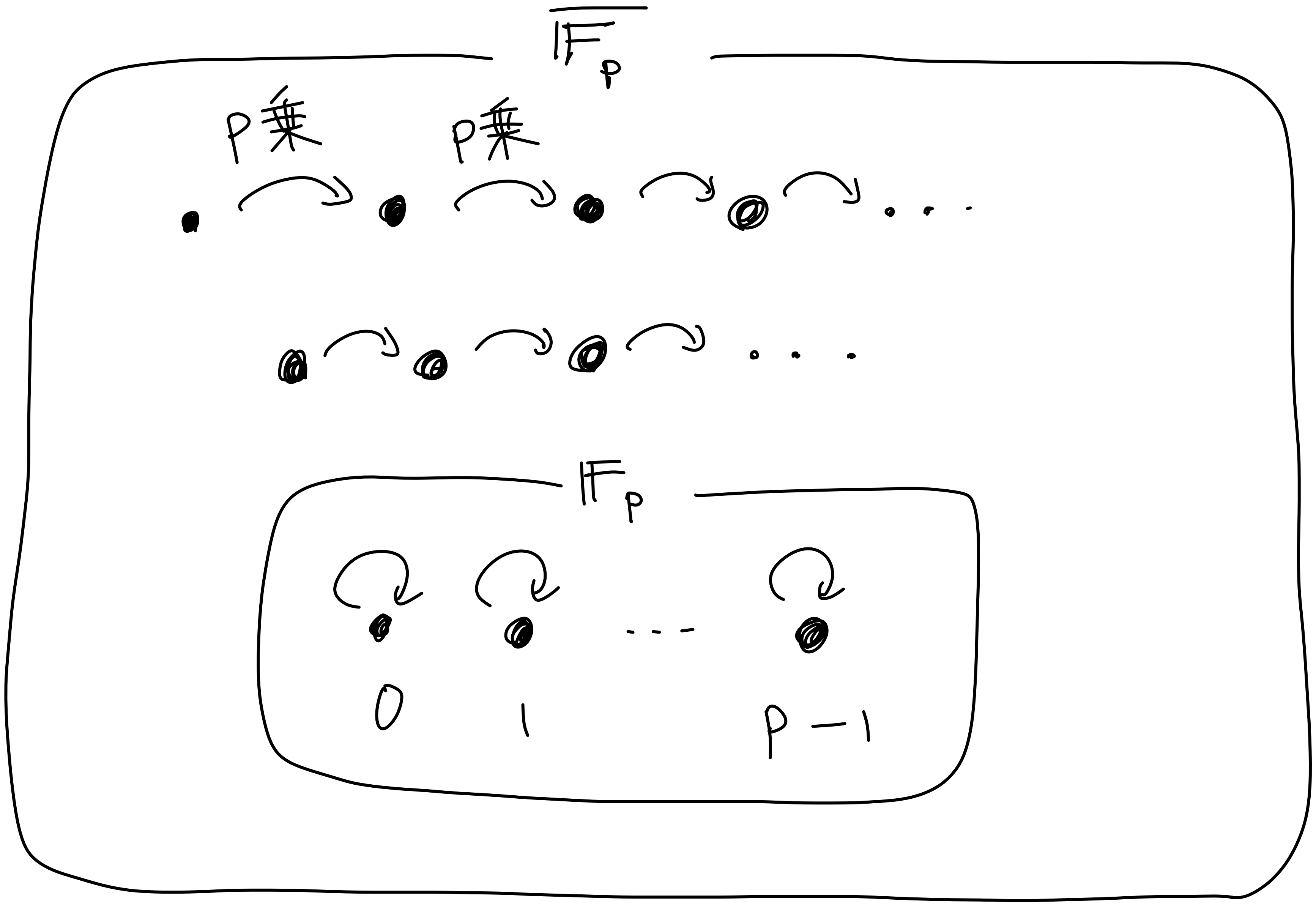
- 素数 p で合同式を考える → p 個のグループ $\{0,1,2,\ldots,p-1\}$
- $\{0,1,2,\ldots,p-1\}$は p 元体 $\mathbb{F}_p$ という「数」の集まりになる
- 有限個しか「数」がないと図形（曲面など）を考えられないので、無限個の「数」を含む、より大きな集まり $\overline{\mathbb{F}_p}$ を考える。





フェルマーの小定理

- p が素数のとき、全ての整数 n に対し $n^p \equiv n \mod p$ が成り立つ。（フェルマーの小定理）
- p 元体 $\mathbb{F}_p = \{0,1,\ldots,p-1\}$ においては、数を p 乗しても元の数と等しい。
- 大きな数の集まり $\overline{\mathbb{F}_p}$ において、$\mathbb{F}_p = \{0,1,\ldots,p-1\}$ はp乗しても変わらない数全体。
- $\overline{\mathbb{F}_p}$ の点（数）を p 乗する移動において、$\mathbb{F}_p$のp個の点 $0,1,\ldots,p-1$が不動点になる。



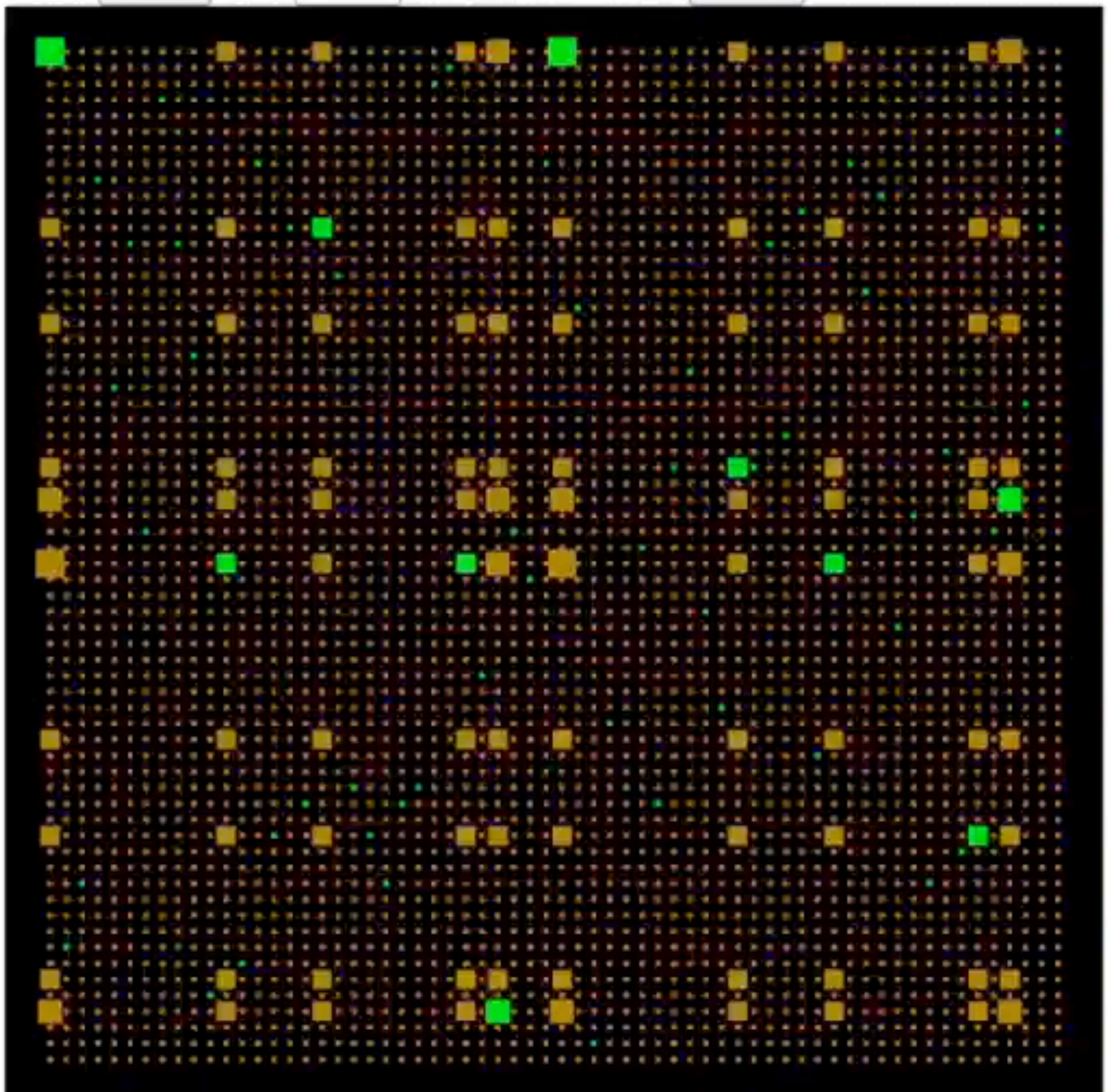
$\mathbb{F}_p$の点がp乗移動の不動点になってる！

p 乗移動の不動点

- 方程式 $y^2 = x^3 - 17x$ の解を $\overline{\mathbb{F}_p}$ の中で考えると、「図形」ができる。
- 座標をp乗する点の移動 $(x, y) \to (x^p, y^p)$ は、図形の点の移動を定める。
- 合同式 $y^2 \equiv x^3 - 17 \mod p$ の解は、この移動の不動点。

In case the action is slow, please try this small version. Editing the JavaScrip
to enter a polynomial used to define a finie field by oneself.

Apply the 1 -times iterated Frobenius map.
(cf. Apply the 2 -th power map. Reset)



$$y^2 \equiv x^3 + x^2 \mod 2$$

明るい点が、方程式の解

一番大きい点が $\mathbb{F}_2$

一番小さい点が $\mathbb{F}_{64} = \mathbb{F}_{2^6}$

http://www4.math.sci.osaka-u.ac.jp/~takehikoyasuda/Frobenius/Frobenius-en.html

グロタンディーク・レフシェッツの定理

- 図形「$y^2 = x^3 + ax + b$」の点のp乗移動に対し、3つの行列が定まる。

$$A_0 = (1) \qquad A_1 = \begin{pmatrix} ? & ? \\ ? & ? \end{pmatrix} \qquad A_2 = (p)$$

- 不動点（合同式の解）の個数 N_p（無限遠点含む）は次の値に等しい：

- （A_0の跡）－（A_1の跡）＋（A_2の跡)

＝ $p + 1 -$（A_1の跡)

アレクサンドル・グロタンディーク
（*1928-2014*）

Konrad Jacobs, Erlangen, Copyright by MFO

グロタンディーク・レフシェッツの定理（続き）

- $N_p =$（A_0の跡）$-$（A_1の跡）$+$（A_2の跡）$= p + 1 -$（A_1の跡）
- ハッセの不等式を思い出そう！　$|N_p - (p+1)| \leqq 2\sqrt{p}$
- 上の式を使うと、これは $|(A_1\text{の跡})| \leqq 2\sqrt{p}$ と同等

ドリーニュの定理

- $(A_1$の跡$)$ は大きさが$\sqrt{p}$の複素数

  $z = x + yi$とその共役$\bar{z} = x - yi$により、$(A_1$の跡$) = z + \bar{z} = 2x$と書ける。

リーマン予想の類似

- したがって、$|(A_1$の跡$)| \leqq 2\sqrt{p}$

- ハッセの不等式

  $|N_p - (p+1)| \leqq 2\sqrt{p}$ を「幾何学」で説明できた！

この講義の最初に登場したヴェイユがハッセの不等式を大幅に改良、一般化し、幾何学的に説明するプログラムを構想。

グロタンディークはヴェイユの構想を実現するために、代数幾何を基礎から書き換え、代数幾何に革命を起こした。

グロタンディークの弟子ドリーニュは、ヴェイユの構想の最後の部分（リーマン予想の類似）を証明した。

幾何を数える

Counting Geometry

オイラーの多面体公式

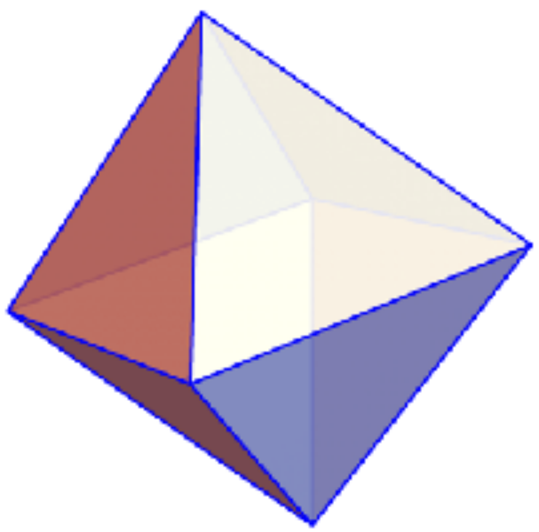
- 凸多面体にたいし、次の等式が成り立つ。
- （頂点の数）−（辺の数）＋（面の数）＝ 2

正8面体

頂点：6

辺：12

面：8

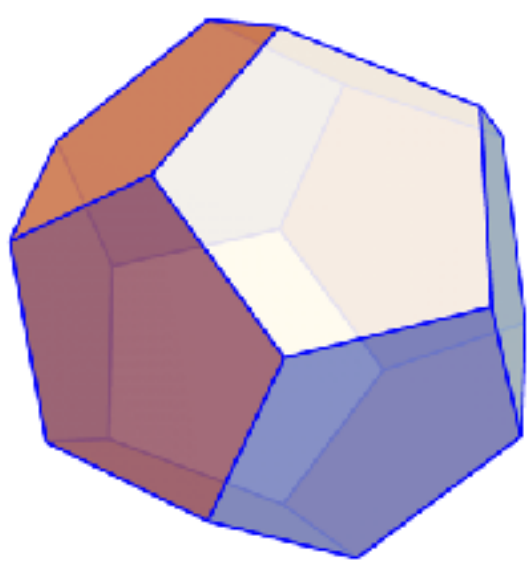


正12面体

頂点：20

辺：30

面：12

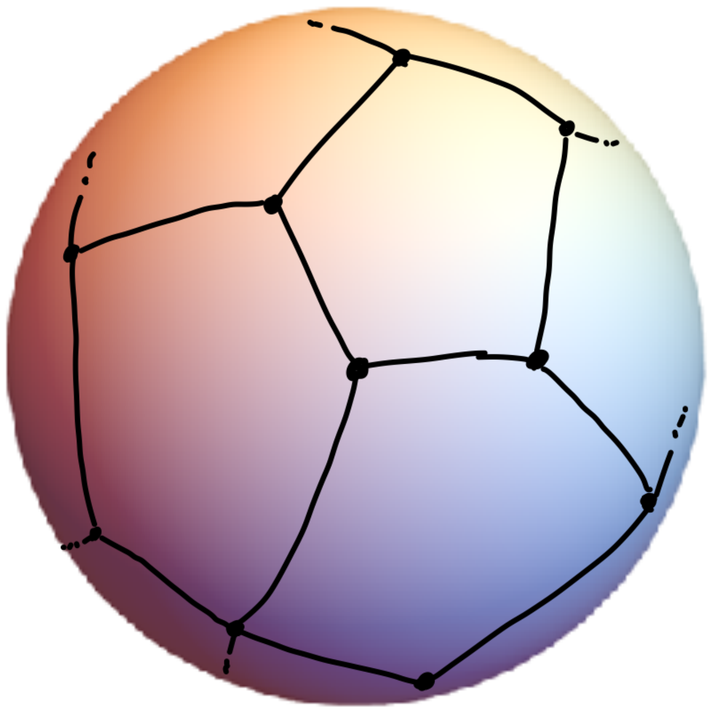


レオンハルト・オイラー

1707-1783

オイラーの多面体公式

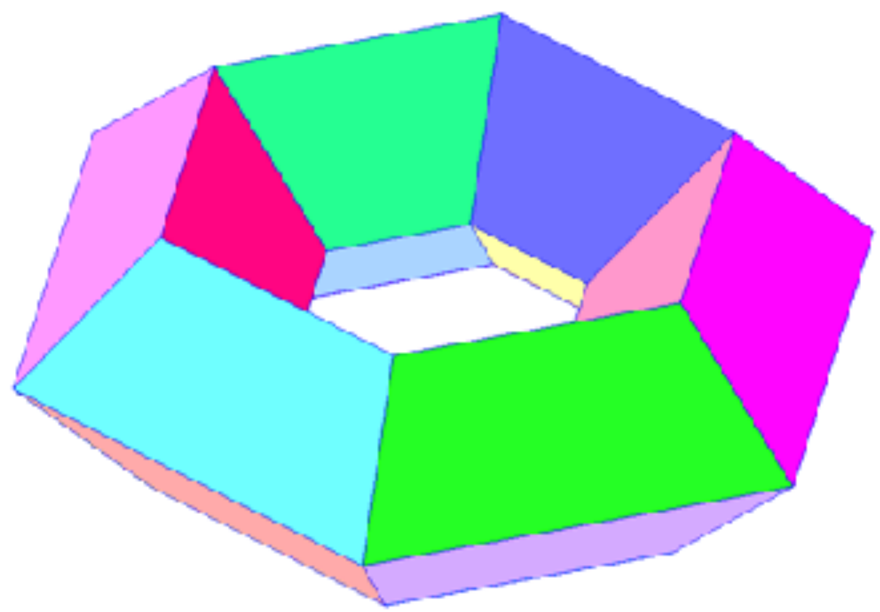
- これは実は「球面」の性質！
- 球面のオイラー数は2。



ドーナツ面のオイラー数

- ドーナツ面では
- （頂点の数）−（辺の数）＋（面の数）＝　0

頂点：24
辺：48
面：24



- ドーナツ面のオイラー数は0

曲面のオイラー数は（A_0のサイズ）−（A_1のサイズ）＋（A_2のサイズ）という式でも計算できる。

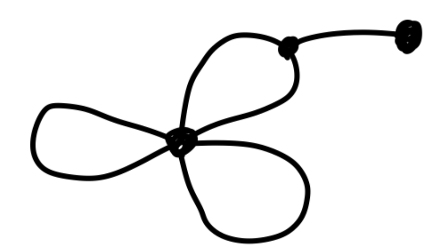
多面体であることや、頂点や辺の数よりも、穴が空いているかどうかが重要なのか？

そうか、これが前の講座で久野先生が解説したトポロジーってやつだな！

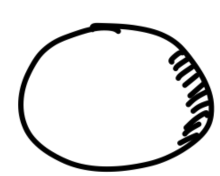
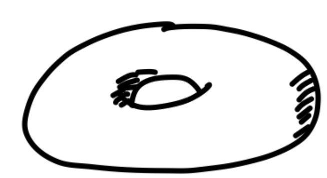
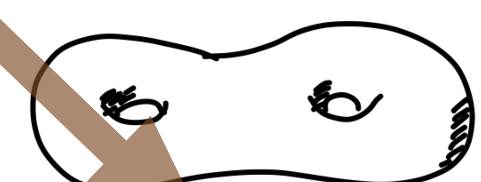
オイラー数は曲面のトポロジーで決まる数なんだ！

いろんな図形のオイラー数

0次元	図形	1点 	2点 	3点 
	オイラー数	1	2	3

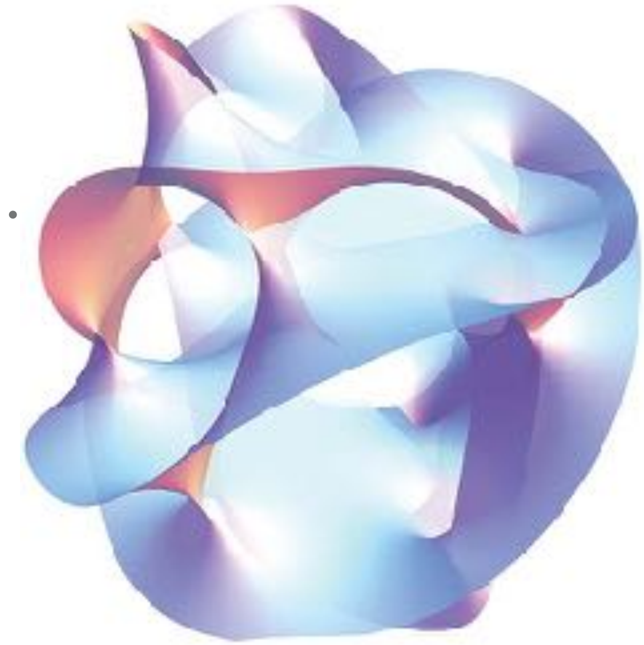
1次元	図形	線分 	円 	
	オイラー数	1	0	-2

マイナスになることもある！！

2次元	図形	球面 	ドーナツ面 	二重ドーナツ面 
	オイラー数	2	0	-2

オイラー数と素粒子

- 一説（超弦理論）によると宇宙は１０次元らしい。
- ４次元の時空（空間３次元＋時間１次元）に加えて、小さくたたまれた６次元があるらしい。
- その６次元はカラビ・ヤウ多様体という形をしているらしい。
- 素粒子が３世代あるのは、そのカラビ・ヤウ多様体のオイラー数が６だかららしい。

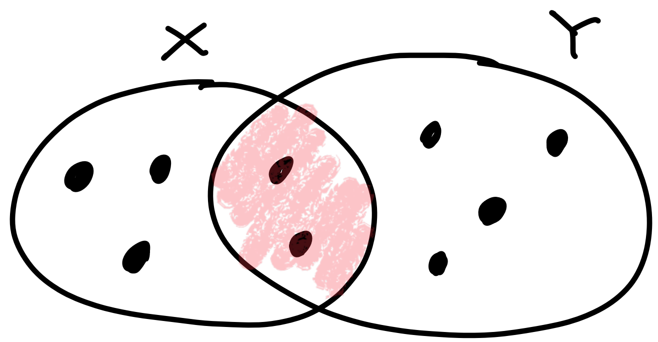


カラビ・ヤウ多様体

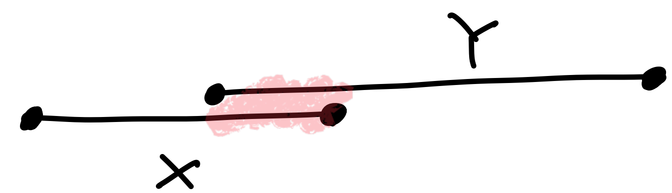
	第1世代	第2世代	第3世代
クオーク	アップダウン	チャーム ストレンジ	トップ ボトム
レプトン	eニュートリノ 電子	μニュートリノ ミューオン	τニュートリノ タウ

大きさの尺度

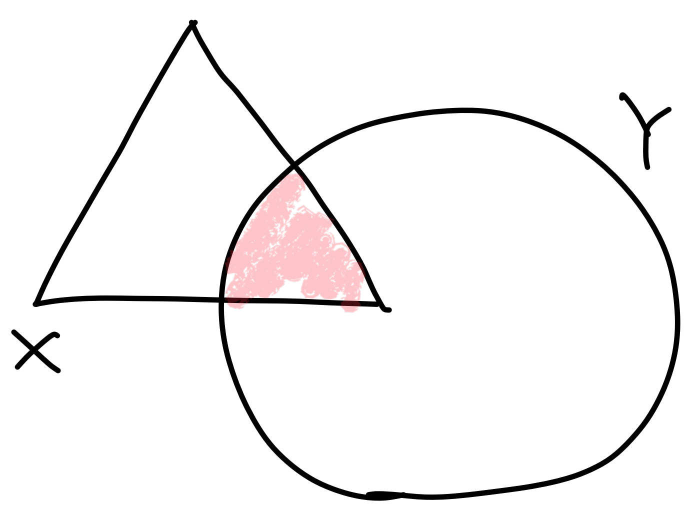
1. 個数



2. 長さ



3. 面積



4. オイラー数

?

確かに、いろんな物を測るときに、包除原理を使ってた。

包除原理

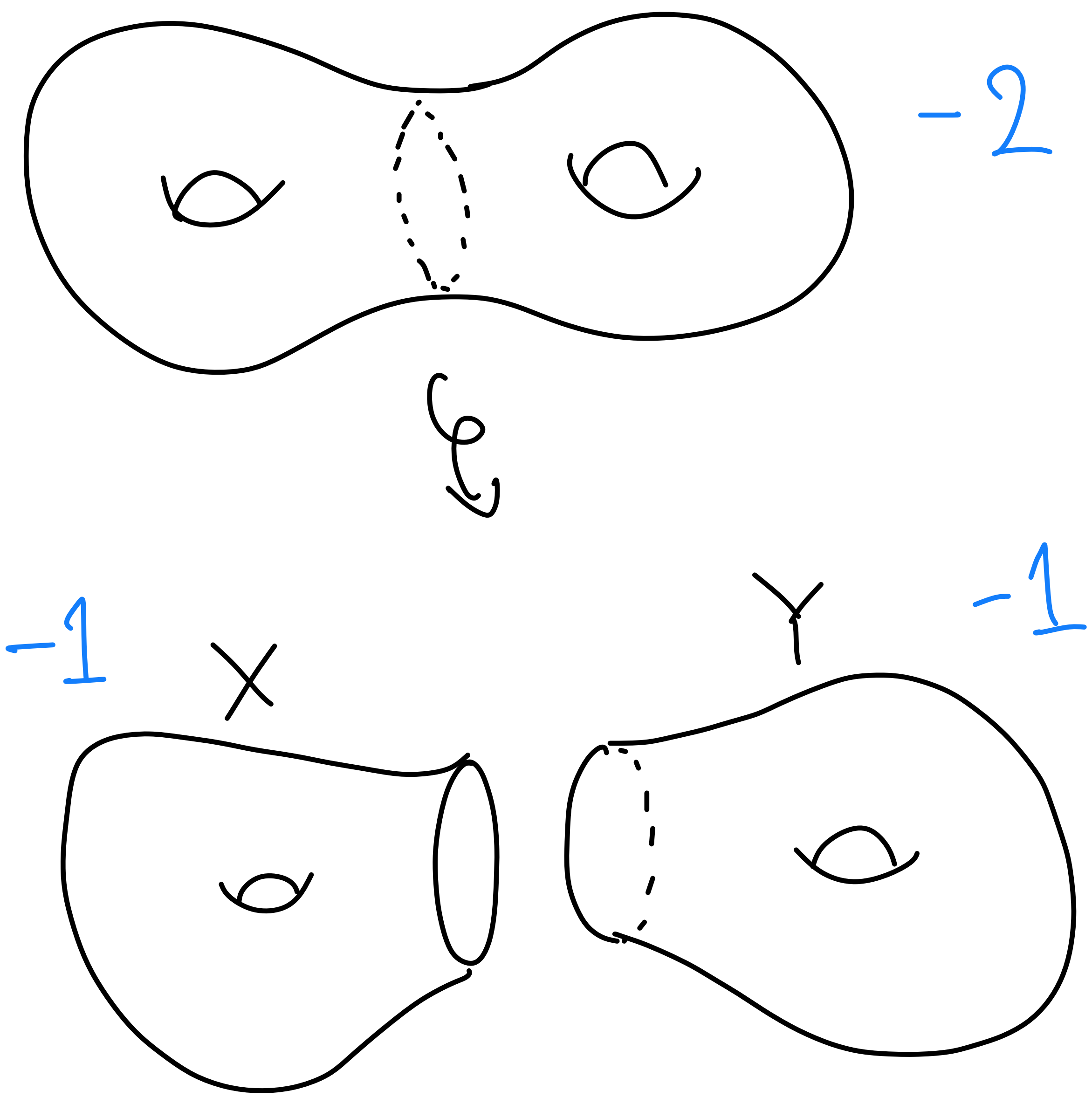
(X∪Y の？) = (Xの？) + (Yの？) - (X∩Yの？)

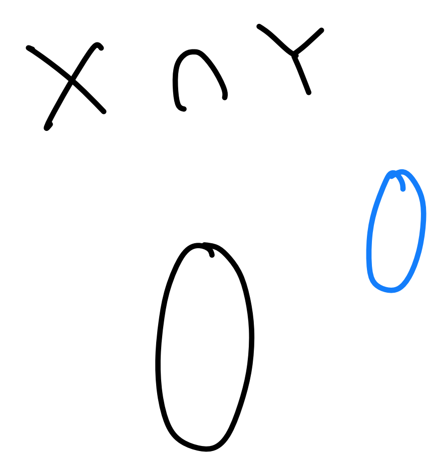
オイラー数の包除原理

(X∪Yのオイラー数) ＝
(Xのオイラー数) + (Yのオイラー数) - (X∩Yのオイラー数)

$-2 =$

$(-1) + (-1) - 0$





包除原理が成り立つから、オイラー数も図形の「大きさ」を測っていると思って良いのかな。

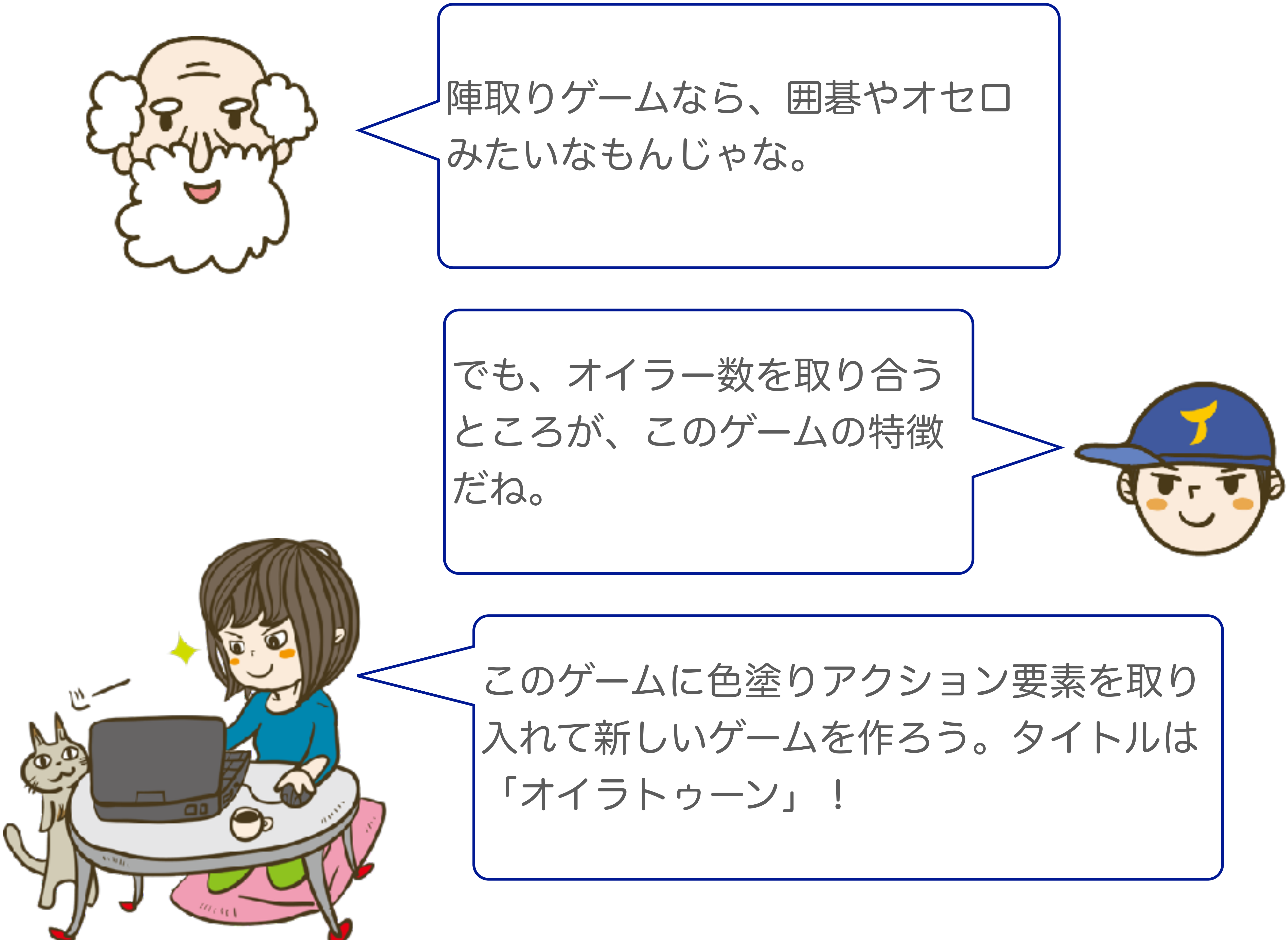
値が負（マイナス）になるのが違和感があるけど、「お金」という大きさでも、借金という負の数が現れるな。

形の大きさを測るのに、整数という飛び飛びの値を取るのが面白いな。

オイラー数と点の個数の間の類似の背後には、グロタンディークが構想した「モチーフ」の理論があるらしい、、、

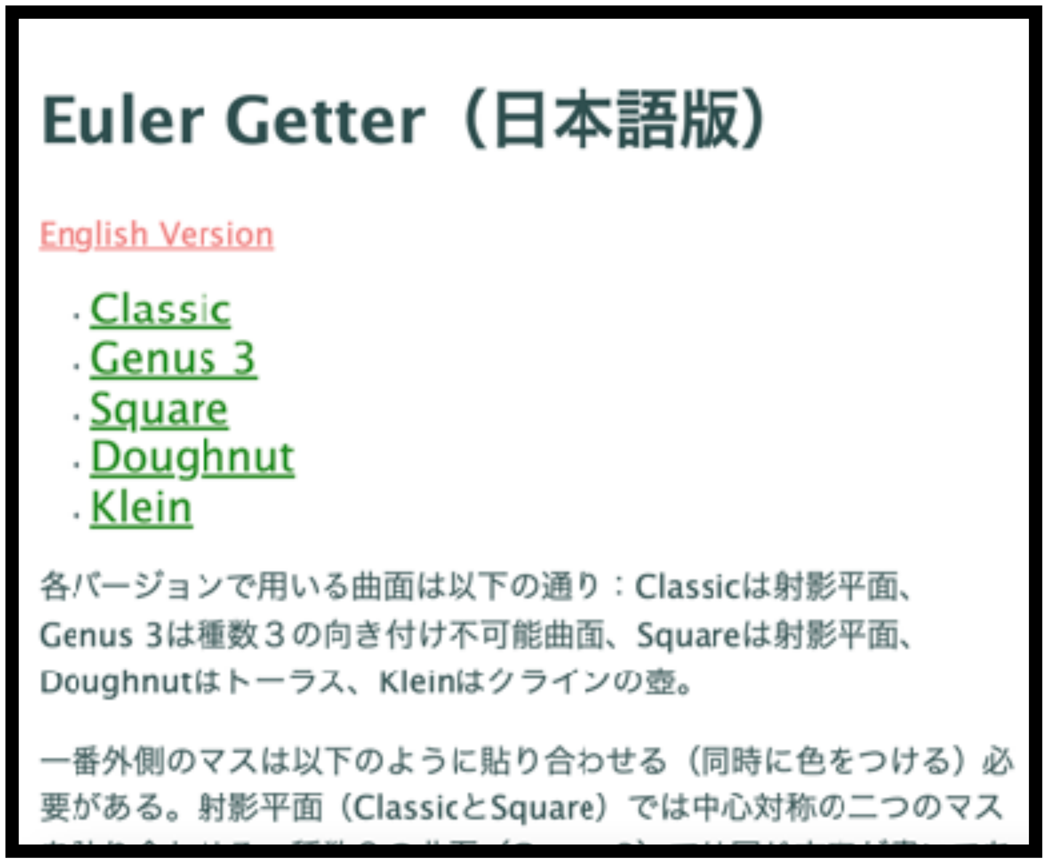
オイラー・ゲッター

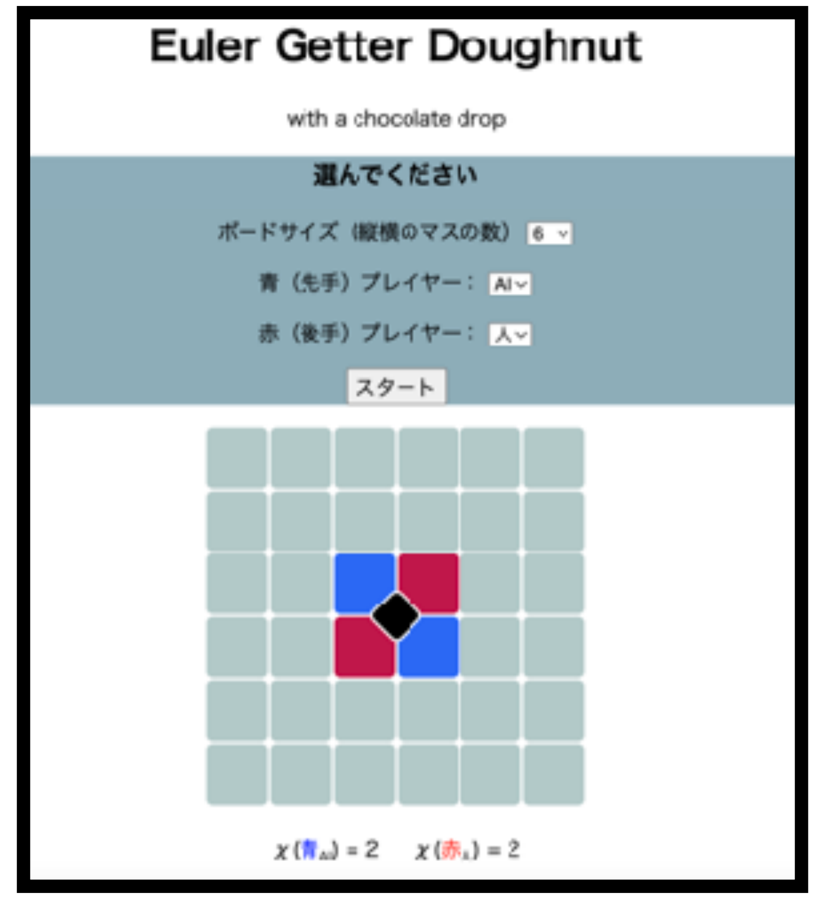
- 曲面上でオイラー数を取り合うゲーム。
- ドーナツ面、射影平面、クラインの壺などの曲面がある。


陣取りゲームなら、囲碁やオセロみたいなもんじゃな。
でも、オイラー数を取り合うところが、このゲームの特徴だね。
このゲームに色塗りアクション要素を取り入れて新しいゲームを作ろう。タイトルは「オイラトゥーン」！

ウェブページと参考図書

http://www4.math.sci.osaka-u.ac.jp/~takehikoyasuda/EulerGetterJP/





参考図書：安田健彦「ゲームで大学数学入門：スプラウトからオイラー ゲッターまで」（共立出版）

本日は、「幾何を使って数え」たり、「幾何を数え」たりする、整数論と幾何学の交わりを見てきました。

数学では、他にも驚くような分野間のつながりがたくさんあり、現在も新しい発見がどんどん出てきています。

数学の奥深さは果てしないですが、今日はここで終わりにしたいと思います。

ありがとうございました。