体の基本

1 導入

この講義で最重要なのは、**体とは「0 以外では割り算ができる環」であり、そのおかげで方程式や線形代数が非常に扱いやすくなる**ことです。
整数では $2x = 1$ を整数の中で解けません。しかし有理数や実数では $x = 1/2$ と解けます。この「割り算ができること」の差を構造として表したものが体です。

2 用語と定義

体 とは、単位元を持つ可換環 F であって、0 でないすべての元が逆元を持つものです。
Field
つまり $a \neq 0$ なら

$$aa^{-1} = 1$$

となる a^{-1} が存在します。

3 方針

まず、なぜ環の次に体を考えるのかを見ます。そのあと、$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ と $\mathbb{Z}/p\mathbb{Z}$ を例にして、割り算ができる条件を整理します。

→ 講義 **環の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/環の基本-講義/

→ 講義 **合同式と mod 演算の基本** lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-講義/

4 直感的な説明

体では、0 でない数を「縮尺」のように自由に掛けたり戻したりできます。だから一次方程式や行列の計算が安定します。

5 厳密な説明

5.1 1. なぜ体が必要か

環だけでは掛け算の逆元があるとは限りません。すると

$$ax = b$$

を解きたくても、a^{-1} を掛けて

$$x = a^{-1}b$$

とする操作ができません。
したがって線形方程式や多項式を系統的に扱うには、0 以外の元に逆元がある世界が欲しくなります。

5.2 2. 典型例

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}$$

は体です。0 でない数なら逆数があるからです。
一方で $\mathbb{Z}$ は体ではありません。2 の逆元が整数の中にないからです。

5.3 3. mod 演算で体になるのはいつか

→ 講義 合同式と mod 演算の基本 lecture math abstract-algebra
https://study.bem130.com/lecture/math/abstract-algebra/合同式と mod 演算の基本-講義/

$\mathbb{Z}/n\mathbb{Z}$ が体になるのは、n が素数のときです。
まず $n = p$ を素数とします。$[a] \neq [0]$ なら $p \nmid a$ です。素数の性質から

$$\gcd(a, p) = 1$$

なので、$ax + py = 1$ を満たす整数 x, y が存在します。これを $\bmod p$ で見ると

$$ax \equiv 1 \pmod{p}$$

だから $[a]$ は逆元 $[x]$ を持ちます。
逆に n が合成数で、$n = ab$ と分解できるなら

$$[a][b] = [0]$$

で、$[a]$ も $[b]$ も $[0]$ ではありません。すると零因子があり、0 でないすべての元が可逆という条件を満たせません。したがって $\mathbb{Z}/n\mathbb{Z}$ は体ではありません。

5.4 4. 体の上で線形代数が動く理由

連立一次方程式で掃き出し法を使うとき、主成分を 1 にするために割り算をします。これは係数が体の中にあるから正当化できます。
つまり体は、代数や線形代数を滑らかに進めるための基盤です。

6 別の見方

6.1 方程式の見方

割り算ができるから方程式が解きやすい世界として見る見方です。

6.2 構造的な見方

環のうち、0 以外で割り算ができるものを抜き出した構造として見る見方です。

6.3 有限体の見方

$\mathbb{Z}/p\mathbb{Z}$ のように、元の数が有限でも体になれると見る見方です。ここから符号理論や暗号へもつながります。

7 見分け方

- 割り算を構造的に正当化したいときは、体を考えます。
- $\mathbb{Z}/n\mathbb{Z}$ が体かどうかを見るときは、まず n が素数かどうかを確かめます。

8 どこまで成り立つか

ここでは $\mathbb{Z}/p\mathbb{Z}$ を例にしましたが、有限体はそれだけではありません。ただし初学では、まず「素数で割った mod 演算は体になる」という事実が最重要です。

9 最終形

$$\boxed{\text{体} = 0 \text{ 以外で割り算のできる可換環}}$$

$$\boxed{\mathbb{Z}/p\mathbb{Z} \text{ は } p \text{ が素数なら体}}$$

10 一言でいうと

- 体とは、環のうち 0 以外で割り算ができるようにした世界で、方程式や線形代数の基盤になります。