有限体の入口

1 導入

この講義で最重要なのは、**有限体とは「元の数が有限なのに、0 以外では割り算ができる世界」であり、mod 演算の最も自然な完成形の 1 つだ**ということです。
高校数学では $\mathrm{mod}\ p$ は余りの計算として使います。しかし大学数学では、$\mathbb{Z}/p\mathbb{Z}$ を有限体として見ることで、線形代数や暗号、符号理論への入口が開けます。

2 用語と定義

有限体 (Finite field) とは、元の数が有限である体です。
もっとも基本的な例は

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

で、p は素数です。

3 方針

まず、なぜ $\mathbb{Z}/p\mathbb{Z}$ が有限体になるのかを見ます。そのあと、p が素数でないと何が壊れるかを確認し、有限体の意味を整理します。

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

有限個しか元がない世界では、表を作れば全部の計算を確認できます。それなのに、0 以外ではちゃんと割り算もできるので、有限体は「小さいが非常に整った数の世界」です。

5 厳密な説明

5.1 1. なぜ $\mathbb{Z}/p\mathbb{Z}$ は体になるのか

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

p が素数なら、$[a] \neq [0]$ のとき

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

です。したがって $ax + py = 1$ を満たす x, y があり、

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

となります。つまり $[a]$ は逆元を持ちます。だから $\mathbb{Z}/p\mathbb{Z}$ は体です。

5.2 2. なぜ素数でないとだめか

もし $n = ab$ が合成数なら、

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

ですが、$[a] \neq [0]$、$[b] \neq [0]$ です。すると零因子があり、0 以外の元すべてに逆元があることは期待できません。

したがって $\mathbb{Z}/n\mathbb{Z}$ が体になるのは、n が素数のときだけです。

5.3 3. 有限体で何がうれしいか

体なので割り算ができ、しかも元が有限個しかありません。したがって

- 線形代数を有限個の元で行える
- 誤り訂正符号や暗号で計算しやすい
- mod 演算が構造的に理解できる

という利点があります。

5.4 4. 加法群と乗法群

$\mathbb{F}_p$ の元は足し算については加法群をなし、0 を除いた元は掛け算について乗法群をなします。

つまり 1 つの有限体の中に、

- 足し算の構造
- 掛け算の構造
- 体としての構造

が重なって見えます。

6 別の見方

6.1 高校数学に近い見方

mod 演算で割り算ができる条件を整理する見方です。

6.2 代数的な見方

$\mathbb{Z}/p\mathbb{Z}$ を体として見て、零因子の有無や逆元の存在を中心に考える見方です。

6.3 応用的な見方

有限体を符号理論や暗号の計算基盤として見る見方です。

7 見分け方

- mod 演算で割り算まで自然に扱いたいときは、$\mathbb{Z}/p\mathbb{Z}$ を有限体として見ます。
- $\mathbb{Z}/n\mathbb{Z}$ が体かどうかを問うなら、まず n が素数かを確認します。

8 どこまで成り立つか

ここでは $\mathbb{F}_p$ だけを扱いました。より一般の有限体 $\mathbb{F}_{p^m}$ もありますが、まずは「mod 演算の中に体が潜んでいる」という見方を押さえるのが大事です。

9 最終形

$$\boxed{\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \text{ は有限体}}$$

$$\boxed{\mathbb{Z}/n\mathbb{Z} \text{ が体} \iff n \text{ が素数}}$$

10 一言でいうと

- 有限体とは、有限個の元しかないのに 0 以外では割り算ができる、非常に整った mod 演算の世界です。