関数体の紹介
Riemann 予想と ABC 予想の類似

グミ

自己紹介

一時期主食がグミだったので、グミと名乗っています。

(今はグミをあまり食べないため、汁なし担々麺と名乗るべき)

数学科の修士卒で、専攻は整数論でした。

今は数学とあまり関係ない仕事をしてしまっています。

図 1: https://x.com/GummyCandy1206

有限体上の 1 変数多項式環

$\mathbb{F}_q$を位数がqの有限体とする。

$\mathbb{F}_q$上の 1 変数多項式環$\mathbb{F}_q[T]$を、以降は単にAと表記する。

Aの元の具体例

$$T+2 \in \mathbb{F}_3[T]$$

$$2T+3 \in \mathbb{F}_7[T]$$

整数環$\mathbb{Z}$と有限体上の多項式環Aは似ていることが知られている。

以降のスライドで、その類似点を紹介する。

整数環$\mathbb{Z}$と有限体上の多項式環Aの類似点

Theorem 1.

$\mathbb{Z}$は単項 ideal 整域である。

Theorem 2.

Aは単項 ideal 整域である。

ざっくり説明

Iはある元の倍数全体の集合 $\Rightarrow$

（Iの元同士を足してもIの元　かつ　Iの元を何倍にしてもIの元）

逆も成り立つのが単項 ideal 整域。

整数環$\mathbb{Z}$と有限体上の多項式環Aの類似点 (ii)

Theorem 3.

$m \neq 0$のとき、剰余環$\mathbb{Z}/m\mathbb{Z}$は有限環である。

Theorem 4.

$f \neq 0$のとき、剰余環A/fAは有限環である。

整数環$\mathbb{Z}$と有限体上の多項式環Aの類似点 (iii)

Theorem 5.

pが素数のとき、剰余環の乗法群$(\mathbb{Z}/p\mathbb{Z})^*$は位数$p-1$の巡回群である。

Theorem 6.

Pが既約多項式のとき、剰余環の乗法群$(A/PA)^*$は位数$|P|-1$の巡回群である。

※ $|P|$はA/PAの位数を表す。

整数環$\mathbb{Z}$と有限体上の多項式環Aの類似点 (iv)

Theorem 7: Euler の定理.

$n \in \mathbb{Z}, \mathbb{Z} \neq 0$とする。また、$a \in \mathbb{Z}$を$n$と互いに素な元とする。 このとき、次が成り立つ。

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$$

Theorem 8.

$f \in A, A \neq 0$とする。また、$a \in A$をfと互いに素な元とする。 このとき、次が成り立つ。

$$a^{\Phi(f)} \equiv 1 (\mathrm{mod}\, f)$$

※ $\varphi(n)$は Euler のトーシェント関数、$\Phi(f)$はそのAでの類似の関数。

従って、Fermat の小定理も同様に成り立つ。

整数環$\mathbb{Z}$と有限体上の多項式環Aの類似点 (v)

Definition 1: Riemann zeta 関数.

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Definition 2: A の zeta 関数.

$$\zeta_A(s) := \sum_{f \in A,\, f \text{ monic}} \frac{1}{|f|^s}$$

関数体の対応関係

整数環$\mathbb{Z}$と有限体上の多項式環Aの対応と同様に、次の対応関係がある。

有理数体$\mathbb{Q}$	有限体上の1変数有理関数体$\mathbb{F}_q(T)$
代数体（$\mathbb{Q}$の有限次拡大体）	関数体（$\mathbb{F}_q(T)$の有限次拡大体）

では、相違点は……？

相違点

整数の場合より、証明が容易なケースがある。

例えば……

関数体バージョンの Riemann 予想は 1948 年に Weil によって既に証明されている。

Theorem 9: 関数体バージョンの Riemann 予想.

Kを$\mathbb{F}_q(T)$の有限次拡大体とする。 $\zeta_K(s)$の零点の実部は$\frac{1}{2}$である。

Bombieri による、より初等的な証明が院生向けの教科書に載っている。[1]

→頑張れば修士・学部生でも理解できるかも？

さらに……

関数体バージョンの Fermat の最終定理も証明済み。

Theorem 10: 関数体バージョンの Fermat の最終定理.

Kを関数体とし、その定数体Fは完全であるとする。 NをFの標数pを割り切らない数とする。

次の場合は$X^N + Y^N = 1$は定数以外の解を持たない。

- Kの種数g_Kが0で、$N \geq 3$のとき。
- $g_K \geq 1$で、$N > 6g_K - 3$のとき。

※ $x^n + y^n = z^n$の両辺をz^nで割れば、$X^n + Y^n = 1$の形になる。

誰が最初に証明したかはリサーチ不足……

さらにさらに……

関数体バージョンの ABC 予想も証明済み。

Theorem 11: 関数体バージョンの ABC 予想（定理）.

Kを関数体とし、その定数体Fは完全であるとする。 $u, v \in K^*$を$u+v=1$を満たすものとする。 このとき、次が成り立つ。

$$\deg_s u = \deg_s v \leq 2g_K - 2 + \sum_{P \in \operatorname{Supp}(A+B+C)} \deg_K P$$

ここで、AとBはそれぞれuとvのKにおける zero divisor で、CはそれらのKにおける polar divisor である。

※ 元の ABC 予想は次のように書きなおせる。

$$u := \frac{A}{C}, v := \frac{B}{C}, \operatorname{ht}\left(\frac{m}{n}\right) := \max(\log|m|, \log|n|)$$

$$\max(\operatorname{ht}(u), \operatorname{ht}(v)) \leq m_\varepsilon + (1+\varepsilon) \sum_{p \mid ABC} \log p$$

まとめ

- 関数体は代数体と似ている。
- 関数体バージョンの Riemann 予想、Fermat の最終定理、ABC 予想は証明済み。
- それらの証明は院生向けの教科書に載っている。[1]

整数論に興味のある方は、関数体も学んでみるとこれらの証明を理解できるかも？

（補記）

- 関数体では整数論の定理だけでなく、他にも Riemann-Roch の定理や、Riemann-Hurwitz の定理も同様に成り立つ。
- 関数体バージョンの ABC 定理の証明は Riemann-Huwitz の定理を用いる。
- 関数体バージョンの Fermat の最終定理の証明は ABC 定理を用いる。
- 円分体に対応する円分関数体が定義できる。
- ideal 類群も同様に定義できる。
- 関数体バージョンの Kronecker-Weber の定理も成り立つ。

（補記）年表

西暦	出来事
1670	Fermat 予想が提示される
1859	Riemann 予想が提示される
1948	Weil が関数体バージョンの Riemann 予想を証明する
1985	ABC 予想が提示される
（不明）	関数体バージョンの ABC 予想、Fermat の最終定理が証明される
1995	Wiles が Fermat の最終定理を証明する
2020	望月氏の ABC 予想の証明論文が『RIMS』に掲載される

すべて関数体バージョンが先行して証明されている（と思う）。

※ 年表のソースは Wikipedia です。

（補記）その他の整数論との類似点

以下の定理の類似も同様に成り立つ

- Wilson の定理
- 平方（n 乗）剰余の相互法則
- 素数定理
- Dirichlet の定理

（補記）関数体の他の例

本スライドでは有限体上の 1 変数有理関数体を扱ったが、有限体に限らず一般の体上の 1 変数有理関数体も定義できる。

例：$\mathbb{C}$上の 1 変数有理関数体

$\mathbb{C}$上の 1 変数有理関数体の圏は、以下と圏同値。[2]

- 閉 Riemann 面の圏
- 非特異射影曲線の圏

全くの余談

$$11^{\ln 11} = 314.159789...$$

100πに近い。なんで？

参考文献

[1] M. Rosen, Number theory in function fields, vol. 210. Grad. Texts Math., vol. 210. New York, NY: Springer, 2002.

[2] 柳田伸太郎, 「代数学 IV/代数学概論 IV 講義ノート」. [Online]. 入手先: https://www.math.nagoya-u.ac.jp/~yanagida/18W/20181220.pdf