Lean による GL(2, Q) の有限位数の決定

北海道大学理学部数学科4年 学生番号 02220077 森下 善
指導教員 : 松下 大介

2026 年 1 月 25 日

1 はじめに

本稿では, 証明支援系Leanを用いて, 有理数体上の2次一般線型群 GL(2, Q) の有限位数を決定していく.
具体的には, GL(2, Q) の有限位数元は, 位数 1, 2, 3, 4, 6 のいずれかであり, 各位数に対して標準的な代表元が存在することを示す. 元 g が有限位数元であるとは, $g^n = I$ (単位元) となるような正の整数 n が存在するということである.

2 主定理

定義 2.1 (有限位数元).
G を群, I を G の単位元とする.
G の元 g が有限位数元であるとは, ある正の整数 n に対して $g^n = I$ となることである.
また, そのような最小の正の整数 n を g の位数と呼ぶ.

補題 2.1. M を *GL(2, Q)* の有限位数元とする. このとき, M の固有多項式の次数は *2* 以下.

```
lemma charpoly_deg_eq_two : (charpoly M.val).natDegree = 2 :=  -- 固有多項式の次数は以下2
  charpoly_natDegree_eq_dim M.val
```

補題 2.2. M を *GL(2, Q)* の有限位数元とする. このとき, M の最小多項式は固有多項式を割り切る.

```
lemma minpoly_deg_le_two : (minpoly ℚ M.val).natDegree ≤ 2 :=  -- 最小多項式の次数は以下2
  calc
    _ ≤ (charpoly M.val).natDegree := by
      apply natDegree_le_of_dvd
      · apply minpoly_dvd_charpoly M.val
      · apply ne_zero_of_natDegree_gt
        show 1 < (charpoly M.val).natDegree
        rw [charpoly_deg_eq_two]
        norm_num
    _ = 2 := by rw [charpoly_deg_eq_two]
```

補題 2.3. M を *GL(2, Q)* の有限位数元とする. このとき, M の最小多項式の次数は *2* 以下.

```
lemma minpoly_dvd_charpoly : minpoly ℚ M.val  M.val.charpoly := by -- 最小多項式は固有多項式を割り切る
  apply dvd ℚ M.val
  exact aeval_self_charpoly M.val
```

定義 2.2 (トーシェント関数). 自然数 n に対して,

$$\varphi(n) = \#\{k \in \mathbb{N} \mid 1 \leq k \leq n, \gcd(k, n) = 1\}$$

をトーシェント関数という.

```
def totient (n : ℕ) : ℕ := Finset.card {a ∈ Finset.range n | n.Coprime a}
```

定義 2.3 (円分多項式). 自然数 n に対して, 円分多項式 $\Phi_n(x)$ を次で定義する.

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \zeta_n^k)$$

ただし, ζ_n は n 番目の原始 n 乗根である.

補題 2.4. 円分多項式の次数はトーシェント関数と等しい.

```
lemma cyclotomic_deg_eq_totient (n : ℕ) :
    (cyclotomic n ℚ).natDegree = totient n := by  -- 円分多項式の次数はトーシェント関数
  exact natDegree_cyclotomic n ℚ
```

補題 2.5. M を *GL(2, Q)* の有限位数元とする. このとき, 円分多項式は M の最小多項式を割り切る.

補題 2.6. n を M の位数とする. このとき, トーシェント関数 $\varphi(n)$ は *2* 以下である.

補題 2.7. トーシェント関数 $\varphi(n)$ が *2* 以下となる自然数 n は, $n = 1, 2, 3, 4, 6$ のいずれかである.

定理 2.1. $GL(2, Q)$ の有限位数元の位数は $1, 2, 3, 4, 6$ のいずれかである.

定理 2.2. $n = 1, 2, 3, 4, 6$ に対して, $GL(2, Q)$ の有限位数元で位数が n であるものが存在する.

定理 2.3. $GL(2, Q)$ の有限位数元は, 位数 $1, 2, 3, 4, 6$ のいずれかであり, 各位数に対して標準的な代表元が存在する.

3 おわりに

本稿では, 証明支援系Leanを用いて, 有理数体上の2次一般線型群 GL(2, Q) の有限位数元の分類を行った. 具体的には, GL(2, Q) の有限位数元は, 位数 1, 2, 3, 4, 6 のいずれかであり, 各位数に対して標準的な代表元が存在することを示した. 今後の課題として, より高次元の一般線型群に対する有限位数元の分類や, 他の体上での類似の問題に取り組むことが挙げられる.

4 参考文献