有限体を係数体とする二次行列の位数についての研究

牧石 晃利
学習院大学理学部数学科

1. 目的

$p = 2, 3, 5, 7, 11$ について、有限体 F_p に係数を持つ行列が正則の時、その位数を調べる。

これら全体は一般線形群 $\mathrm{GL}(2, p)$ になる。

また、行列式Dが1のものに限ると、特殊線形群 $\mathrm{SL}(2, p)$ になる。

これらの位数も数え挙げる。

2. 手順

$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ において、mod p で p は 2 以上の素数として、各 a, b, c, d に $0, 1, ..., p-1$ (pは2以上の素数) をそれぞれ代入し、

$$A^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (= E)$$

を満たす n をprologを使い、求める。

$GL(2,p), SL(2,p)$ についてのデータの量が膨大な為、例として使う $GL(2,3)$ の表の一部省略したものを載せ、他は結果だけを纏めた表を載せた。
そのデータに基づき、位数が最大の時、又は位数が最大でない時、

$$\varphi_A(t) = t^2 - (a+d)t + (ad - bc)$$

が mod p で既約となっているか、調べる。

TABLE 1. GL(2,3)

matrix	order	list
$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	[1]
$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	[2]
$\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$	2	[2]
$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	2	[2]
$\begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$	2	[2]
$\begin{pmatrix} 1 & 0 \\ 2 & 2 \end{pmatrix}$	2	[2]
$\vdots$	$\vdots$	$\vdots$

matrix	order	list
⋮ ⋮	⋮ ⋮	⋮ ⋮
$\begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$	3	[3]
⋮ ⋮	⋮ ⋮	⋮ ⋮
$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	8	[2, 2, 2]
⋮ ⋮	⋮ ⋮	⋮ ⋮
$\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$	8	[2, 2, 2]

3. 例

例えば、$\mathrm{GL}(2,3)$において、最大の位数は8であり、

$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$の時、$\mathrm{mod}\ p$で、

$$\varphi_A(t) = t^2 - (0+1)t + (0-1)$$
$$\varphi_A(t) = t^2 - t - 1$$

となる。

$\mod p$で

$t = 0$の時、

$$\varphi_A(0) = -1 = 2$$

$t = 1$の時、

$$\varphi_A(1) = -1 = 2$$

$t = 2$の時、

$$\varphi_A(2) = 1$$

となり、

$\varphi_A(t) = 0$は、$t = 0, 1, 2$では、0にならない。

よって、この場合は、

$\varphi_A(t)$は位数が最大の時、既約である事が分かる。

また、$\mathrm{GL}(2,3)$において、位数が3の時（位数が最大でない）、

$A = \begin{pmatrix} 2 & 2 \\ 1 & 0 \end{pmatrix}$の時、

$$\varphi_A(t) = t^2 - (2+0)t + (0-2)$$
$$\varphi_A(t) = t^2 - 2t - 2$$

となり、$\mathrm{mod}\ p$で、

$$\varphi_A(t) = t^2 + t + 1$$

となる。

$\mathrm{mod}\ p$で、
$t = 0$の時、

$$\varphi_A(0) = 1$$

$t = 1$の時、

$$\varphi_A(1) = 3 = 0$$

$t = 2$の時、

$$\varphi_A(2) = 7 = 1$$

となり、
$\varphi_A(t) = 0$は、$t = 1$で、成り立つ。

よって、この場合は、
$\varphi_A(t)$は、位数が最大でない時、根を持ち、既約でない事が分かる。

4. $\mathrm{GL}(2,p)$

$GL(2,p)$で位数が最大なら、その位数はp^2-1である。

$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ において、Aの位数が最大ならば、

$$\varphi_A(t)=t^2-(a+d)t+(ad-bc)$$

が $\mathrm{mod}\ p$で既約となっている。

5. $\mathrm{GL}(2,p)$の位数と行列の最大位数

群	位数	行列の最大位数	その個数
$\mathrm{GL}(2,2)$	6	3	2
$\mathrm{GL}(2,3)$	48	8	12
$\mathrm{GL}(2,5)$	480	24	80
$\mathrm{GL}(2,7)$	2016	48	336
$\mathrm{GL}(2,11)$	13200	120	1760
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\mathrm{GL}(2,p)$	$(p-1)^2p(p+1)$	p^2-1	

6. $\mathrm{SL}(2,p)$ の位数と行列の最大位数

群	位数	行列の最大位数	その個数
$\mathrm{SL}(2,2)$	6	3	2
$\mathrm{SL}(2,3)$	24	6	8
$\mathrm{SL}(2,5)$	120	10	24
$\mathrm{SL}(2,7)$	336	14	48
$\mathrm{SL}(2,11)$	1320	22	120
⋮	⋮	⋮	⋮
$\mathrm{SL}(2,p)$	$(p-1)p(p-1)$		

$\mathrm{SL}(2,p)$ の時、位数が最大の時、その位数を一般に表す事は出来なかった。

7. 結果

TABLE 2. GL(2,p) と SL(2,p) の群の位数の比

p	$\mathrm{GL}(2,p)$の位数	$\mathrm{SL}(2,p)$の位数	群の位数の比
2	6	6	1 : 1
3	48	24	2 : 1
5	480	120	4 : 1
7	2016	336	6 : 1
11	13200	1320	10 : 1
⋮	⋮	⋮	⋮
p	$(p-1)^2p(p+1)$	$(p-1)p(p-1)$	$p-1:1$

途中でこれは赤とします
これは緑
これはカーネーションCarnationPink
これはForestGreen
これはLimeGreen
これはLimeGreen
これはLimeGreen
枠緑 背景は青色
枠赤　背景黄色
字の背景に色をつけましょう
これは黄色
これは赤