

ラマヌジャングラフの構成について

教科教育専攻 数学教育専修

篠永小百合

平成25年2月4日

目次

1	序	2
1.1	グラフの隣接行列と固有値	2
1.2	固有値の gap の不等式	3
1.3	family of expanders での固有値の近似的なふるまい	4
1.4	近似的なふるまいの証明	6
1.5	非隣接数と彩色数	8
1.6	大きな girth と大きな彩色数	9
2	整数論と $\mathrm{PSL}_2(q)$	14
2.1	2 つの平方数の和	14
2.2	平方剰余の相互法則と 4 つの平方数の和	16
2.3	四元数環	17
2.4	整四元数環における整数論	18
2.5	$\mathrm{PGL}_2(q)$ と $\mathrm{PSL}_2(q)$	21
2.6	部分群の構造	22
2.7	有限群の表現論	24
3	グラフ $X^{p,q}$	32
3.1	ケーリーグラフ	32
3.2	$X^{p,q}$ の構成	33
3.3	girth と連結性	36
3.4	固有値の評価	41
4	グラフ $H \backslash X^{p,q}$	50
4.1	商ケーリーグラフ	50
4.2	グラフ $H \backslash X^{p,q}$	51
4.3	$H \backslash X^{p,q}$ の固有値の評価	53
4.4	$H \backslash X^{p,q}$ の girth と彩色数	53

1 序

1.1 グラフの隣接行列と固有値

V を頂点の集合, E を辺の集合とし, グラフ $X = (V, E)$ を考える. 特に断りのないときはグラフ X は無向で, 多くの場合有限グラフである. X の頂点の集合を $V = \{v_1, v_2, \dots\}$ とする. このときグラフ X の隣接行列 A は

$$A_{ij} = v_i \text{ と } v_j \text{ をつなげている辺の個数}$$

とすると, $A = (A_{ij})$ である. X が単純であるとは隣接した頂点が多くとも 1 つの辺でつながっている, すなわちすべての $v_i, v_j \in V$ に対し $A_{ij} \in \{0, 1\}$ となることをいう. X が単純のときには $v_i, v_j \in V$ をつないでいる辺を $\{v_i, v_j\}$ と表す. 隣接行列 A によりグラフ X は完全に決定し, X が無向のときは A は対称行列である. グラフ X にループがないとは, すべての $v_i \in V$ に対し, $A_{ii} = 0$ であることと必要十分である. 2 頂点 $v_i, v_{i+1} \in V$ が辺 $e_i \in E$ により隣接しているとき, 列 $v_1 e_1 v_2 e_2 v_3 \dots v_k$ を X の経路という. 特に X が単純のときには $v_1 v_2 \dots v_k$ とかく. グラフ X のすべての 2 頂点が経路によりつなぐことができたなら連結しているという.

定義 1.1.1. $k \geq 2$ を整数とする. すべての $v_i \in V$ に対し, $\sum_{v_j \in V} A_{ij} = k$ が成り立つとき, X は k -正則という.

X にループがないとき, k -正則であることと, すべての頂点がちょうど k 個の頂点と隣接していることは等しい.

X を n 頂点を持つ有限グラフとする. このとき隣接行列 A は n 行 n 列の対称行列であり, n 個の実固有値が存在する. 重複も数に入れ, 値が減少するように並べると,

$$\mu_0 \geq \mu_1 \geq \dots \geq \mu_{n-1}$$

となる. A の固有値の集合を X の固有値という. μ_0 の重複度が 1 であることは, $\mu_0 > \mu_1$ であることと必要十分である.

グラフ $X = (V, E)$ に対し, 関数 $f: V \rightarrow \mathbb{C}$ を考え,

$$l^2(V) = \{f: V \rightarrow \mathbb{C} : \sum_{v \in V} |f(v)|^2 < +\infty\}$$

を定義する. $l^2(E)$ も同様に定義する.

V が有限のとき $|V| = n$ とすると, すべての関数 $f: V \rightarrow \mathbb{C}$ は $l^2(V)$ に含まれる. このような関数を \mathbb{C}^n 上のベクトルと考える. これに隣接行列を作用させると,

$$\begin{aligned} Af &= \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ \vdots & \vdots & & \vdots \\ A_{i1} & A_{i2} & \dots & A_{in} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} f(v_1) \\ f(v_2) \\ \vdots \\ f(v_n) \end{pmatrix} \\ &= \begin{pmatrix} A_{11}f(v_1) + A_{12}f(v_2) + \dots + A_{1n}f(v_n) \\ \vdots \\ A_{i1}f(v_1) + A_{i2}f(v_2) + \dots + A_{in}f(v_n) \\ \vdots \\ A_{n1}f(v_1) + A_{n2}f(v_2) + \dots + A_{nn}f(v_n) \end{pmatrix} \end{aligned}$$

となる。したがって、 $(Af)(v_i) = \sum_{j=1}^n A_{ij}f(v_j)$ となる。添字を頂点の組そのままにすると、 A は $(A_{xy})_{x,y \in V}$ によって表され、すべての $x \in V$ に対し、 $(Af)(x) = \sum_{y \in V} A_{xy}f(y)$ となる。

命題 1.1.2. X を有限で、 n 頂点を持つ k -正則グラフとする。このとき次が成り立つ；

- (a) $\mu_0 = k$.
- (b) $1 \leq i \leq n-1$ に対し、 $|\mu_i| \leq k$.
- (c) μ_0 の重複度が 1 であることと、 X が連結であることは同値である。

定義 1.1.3. グラフ $X = (V, E)$ はある頂点の分割 $V = V_+ \cup V_-$ により $A_{xy} \neq 0$ となるすべての 2 頂点 x, y を $x \in V_+(V_-)$ かつ $y \in V_-(V_+)$ とすることができたならば、**2 彩色可能** という。このグラフを **2 部グラフ** という。

言い換えると、どの 2 つの隣接する頂点も同じ色にならないように頂点を 2 色でぬることができたならば、グラフは 2 彩色可能である。

命題 1.1.4. X を連結で n 頂点を持つ k -正則グラフとする。次は同値となる：

- (i) X は 2 彩色可能である；
- (ii) X の固有値は 0 で対称となる；
- (iii) $\mu_{n-1} = -k$.

すべての有限で連結な k -正則グラフ X は最大固有値 $\mu_0 = k$ を持ち、2 彩色可能ならば最小固有値は $\mu_{n-1} = -k$ となる。固有値 $k, -k$ を X の**自明な固有値**という。差 $k - \mu_1 = \mu_0 - \mu_1$ を X の**固有値の gap** という。

1.2 固有値の gap の不等式

$X = (V, E)$ をグラフとする。 $F \subset V$ のとき、 F の**境界** ∂F を F と $V - F$ をつなぐ辺の集合とする。すなわち、 ∂F は F と $V - F$ を連結している辺の集合である。 $\partial F = \partial(V - F)$ である。

定義 1.2.1. グラフ X の **expanding constant** を

$$h(X) = \inf \left\{ \frac{|\partial F|}{\min\{|F|, |V - F|\}} : F \subset V, 0 < |F| < +\infty \right\}$$

とする。 X が n 頂点を持つ有限グラフのとき、 $h(X) = \min \left\{ \frac{|\partial F|}{|F|} : F \subset V, 0 < |F| \leq \frac{n}{2} \right\}$ となる。

グラフ X を情報伝達ネットワークとすると、expanding constant $h(X)$ は X の**質**を測定している。 $h(X)$ が大きいことは、情報伝達がよいことを意味している。

定義 1.2.2. グラフ族 $(X_m)_{m \geq 1}$ が有限で連結していて k -正則であり、 $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ をみたすとする。このとき、

$$\exists \varepsilon > 0, \forall m \geq 1 \quad \text{such that} \quad h(X_m) \geq \varepsilon$$

をみたすならば、**family of expanders** という。

X_m が完全グラフ（すべての頂点が他のすべての頂点と隣接しているグラフ）ならば，確かに情報伝達
はよいがコストがかかることから，最小の辺によって最適な相互通信能力が与えられるグラフが最もよい．

定理 1.2.3. $X = (V, E)$ を有限で連結していて，ループのない k -正則グラフとする． μ_1 を X の自明でない最大固有値とすると，

$$\frac{k - \mu_1}{2} \leq h(X) \leq \sqrt{2k(k - \mu_1)}$$

が成り立つ．

定義 1.2.2 と定理 1.2.3 から次がわかる．

系 1.2.4. $(X_m)_{m \geq 1}$ を有限で連結していて，ループのない k -正則グラフ族とし， $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ をみたすとする．このとき，族 $(X_m)_{m \geq 1}$ が family of expanders であることは，

$$\exists \varepsilon > 0, \forall m \geq 1 \quad \text{such that} \quad k - \mu_1(X_m) \geq \varepsilon$$

をみたすことと，必要十分である．

系 1.2.4 から k -正則なグラフ族が family of expanders であることは固有値の gap に 0 から離れた下限が存在することと必要十分であることがわかる．また，定理 1.2.3 から固有値の gap が大きいほど expanding constant $h(X)$ が大きく， X の質がよいことがわかる．

1.3 family of expanders での固有値の近似的なふるまい

この節でのグラフはすべてループなしとする．次の定理より k -正則グラフの固有値の gap の大きさには限りがあることがわかる．

定理 1.3.1. $(X_m)_{m \geq 1}$ を有限で連結している k -正則グラフ族とし， $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ をみたすとする．このとき，

$$\liminf_{m \rightarrow +\infty} \mu_1(X_m) \geq 2\sqrt{k-1}$$

が成り立つ．

定理 1.3.1 より強い結果を 1.4 節で見えていく．

定義 1.3.2. X を連結グラフとする． X の **girth** $g(X)$ を X の最小の閉路の長さとする． X が tree である，すなわち X に閉路がないとき， $g(X) = +\infty$ とする．

有限で連結している k -正則グラフにおいて， $\mu(X)$ を X の最小非自明固有値とする．

定理 1.3.3. $(X_m)_{m \geq 1}$ を有限で連結している k -正則グラフ族とし， $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ をみたすとする．このとき，

$$\limsup_{m \rightarrow +\infty} \mu(X_m) \leq -2\sqrt{k-1}$$

が成り立つ．

定理 1.3.3 も同様に強い結果を 1.4 節で見ていく．定理 1.3.1 と定理 1.3.3 から主定義が導かれる．

定義 1.3.4. X を有限で連結している k -正則グラフとする． X のすべての非自明固有値 μ において、

$$|\mu| \leq 2\sqrt{k-1}$$

が成り立つとき、 X をラマヌジャングラフという．

$(X_m)_{m \geq 1}$ をループなしの k -正則なラマヌジャングラフ族とし、 $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ だとする．このとき、 X_m の固有値の gap は可能な限りの最大となり、family of expanders について最適となる．

命題 1.3.5. X を有限な k -正則グラフとする．頂点 x_0 を固定し、自然数 r を $r < \frac{g(X)}{2}$ とする． X に中心 x_0 、半径 r の円をかく．この円の中に頂点は $\frac{k((k-1)^r - 1)}{k-2} + 1$ 個ある．

証明. 中心 x_0 、半径 r の円をかくと、この円の内部にあるグラフの部分は k -正則な tree と同型である．よって、頂点の個数は

$$1 + k + k(k-1) + \cdots + k(k-1)^{r-1} = \frac{k((k-1)^r - 1)}{k-2} + 1$$

となる． □

命題 1.3.6. $k \geq 3$ とする． $(X_m)_{m \geq 1}$ を連結している k -正則グラフ族とし、 $m \rightarrow +\infty$ のとき $|V_m| \rightarrow +\infty$ をみたすとする．このとき、

$$g(X_m) \leq 2 + 2 \log_{k-1} |V_m|$$

となる．

証明. 自然数 r_m を $r_m < \frac{g(X_m)}{2}$ とする．中心 x_0 、半径 r_m の円を考えると、命題 1.3.5 より

$$\begin{aligned} \frac{k((k-1)^{r_m} - 1)}{k-2} + 1 &\leq |V_m|, \\ \frac{k((k-1)^{r_m} - 1)}{k} + 1 &\leq |V_m|, \\ (k-1)^{r_m} &\leq |V_m|, \\ r_m &\leq \log_{k-1} |V_m| \end{aligned}$$

となる． $\frac{g(X_m)}{2} - 1 \leq r_m < \frac{g(X_m)}{2}$ とできるので、

$$\begin{aligned} \frac{g(X_m)}{2} - 1 &\leq \log_{k-1} |V_m|, \\ g(X_m) &\leq 2 + 2 \log_{k-1} |V_m| \end{aligned}$$

となる． □

1.4 近似的なふるまいの証明

この節では定理 1.3.1 と定理 1.3.3 よりも強い結果を見ていく.

定理 1.3.1 の不等式は k -正則グラフでの頂点 v から v への長さが m になる経路の数は, k -正則な tree の v から v への経路の数以上であるということからきている.

$X = (V, E)$ を k -正則な単純グラフとする ($|V|$ は無限でもよい). $x_i \in V (i = 0, 1, \dots, r)$ に対し, x_i と $x_{i-1} (i = 0, 1, \dots, r-1)$ が隣接していて $x_{i+1} \neq x_{i-1} (i = 1, 2, \dots, r-1)$ が成り立つとき,

$$\underline{e} = x_0 x_1 \cdots x_r$$

を長さ r の後戻りのない経路という. \underline{e} の始点は x_0 は, 終点は x_r である. $r \in \mathbb{N}$ に対し A_r を

$$(A_r)_{xy} = \text{始点 } x, \text{ 終点 } y \text{ の後戻りなしの長さ } r \text{ の経路の数}$$

と定義する. このとき, $A_0 = \text{Id} (= A^0)$ と $A_1 = A$ が成り立つことは明らかである.

補題 1.4.1.

$$(a) \ A_1^2 = A_2 + k \cdot \text{Id}.$$

$$(b) \ r \geq 2 \text{ に対し, } A_1 A_r = A_r A_1 = A_{r+1} + (k-1)A_{r-1}.$$

補題 1.4.1 から A_r の生成関数を計算することができる. すなわち, A_r を係数の形式的べき級数にできる.

補題 1.4.2.

$$\sum_{r=0}^{\infty} A_r t^r = \frac{1-t^2}{1-At+(k-1)t^2}$$

が成り立つ. すなわち,

$$\left(\sum_{r=0}^{\infty} A_r t^r \right) (\text{Id} - At + (k-1)t^2 \cdot \text{Id}) = (1-t^2)\text{Id}$$

となる.

補題 1.4.2 の右辺の分子の $1-t^2$ を消去するために多項式 T_m を

$$T_m = \sum_{0 \leq r \leq \frac{m}{2}} A_{m-2r} \quad (m \in \mathbb{N})$$

と定義する. T_m の生成関数は補題 1.4.3 で与えられる.

補題 1.4.3.

$$\sum_{m=0}^{\infty} T_m t^m = \frac{1}{1-At+(k-1)t^2}.$$

定義 1.4.4. 第 2 種のチェビシエフ多項式を

$$U_m(\cos \theta) = \frac{\sin(m+1)\theta}{\sin \theta} \quad (m \in \mathbb{N})$$

と定義する.

U_m と T_m の関係は命題 1.4.5 で与えられる.

命題 1.4.5. $m \in \mathbb{N}$ に対し,

$$T_m = (k-1)^{\frac{m}{2}} U_m \left(\frac{A}{2\sqrt{k-1}} \right)$$

が成り立つ.

$X = (V, E)$ を有限で n 頂点を持つ k -正則グラフとする. X の固有値を

$$\mu_0 = k \geq \mu_1 \geq \cdots \geq \mu_{n-1}$$

で表す. $x \in V$ に対し, $f_{l,x}$ を X の始点 x , 終点 x の後戻りなしの長さ l の経路の数とする. すなわち, $f_{l,x} = (A_l)_{xx}$ である. T_m のトレースを 2 つの方法で考えることで, 次の trace formula が成り立つことがわかる.

定理 1.4.6. すべての $m \in \mathbb{N}$ に対し,

$$\sum_{x \in V} \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r,x} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{k-1}} \right)$$

が成り立つ.

X の自己同型群 $\text{Aut } X$ が頂点集合 V 上で推移的に動くとき, X は**頂点推移**という. すなわち, すべての頂点の組 x, y に対し, ある $\alpha \in \text{Aut } X$ が存在し, $\alpha(x) = y$ が成り立つことをいう. 頂点推移であるとき, $f_{l,x}$ は単に f_l としてよい.

系 1.4.7. X を頂点推移で有限で n 頂点を持つ k -正則グラフとする. このときすべての $m \in \mathbb{N}$ に対し,

$$n \cdot \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r} = (k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{k-1}} \right)$$

が成り立つ.

定理 1.4.6 の右辺 $(k-1)^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{k-1}} \right)$ からだけではこれが非負整数になるかはわからない. しかし, 左辺が正となるということからこれが正になることがわかり, これより非自明な結果を得る. そのために, まずチェビシエフ多項式のテクニカルな結果を用意する.

命題 1.4.8. $L \geq 2$ と $\varepsilon > 0$ を実数とする. $[-L, L]$ 上の任意の確率測度 ν に対し, すべての $m \in \mathbb{N}$ において $\int_{-L}^L U_m \left(\frac{x}{2} \right) d\nu(x) \geq 0$ となるならば

$$\nu([2-\varepsilon, L]) \geq C$$

をみたす定数 $C = C(\varepsilon, L) > 0$ がある. (ν は C 以上の速度を $[2-\varepsilon, L]$ に与える.)

有限で連結な k -正則グラフの固有値の話に戻り, 定理 1.3.1 よりもよい定理を与える. 定理 1.3.1 のように非自明でない最大の固有値 μ_1 が近似的に $2\sqrt{k-1}$ より大きいだけでなく, 区間 $[(2-\varepsilon)\sqrt{k-1}, k]$ にある正の固有値でもそうであることが次でわかる.

定理 1.4.9. すべての $\varepsilon > 0$ に対し定数 $C = C(\varepsilon, k) > 0$ があり, すべての有限で連結な n 頂点を持つ k -正則グラフ X の固有値は, 区間 $[(2-\varepsilon)\sqrt{k-1}, k]$ に少なくとも $C \cdot n$ 個存在する.

定理 1.4.9 に類似した定理 1.3.3 の改善を行っていく． X をグラフとするととき， $|X|$ をグラフの頂点数とする． δ_a を $a \in [-L, L]$ のディラック測度とする．これは $[-L, L]$ 上の確率測度である．すなわち， $[-L, L]$ 上の連続関数 f に対し， $\int_{-L}^L f(x) d\delta_a(x) = f(a)$ となる．

定理 1.4.10. $(X_m)_{m \geq 1}$ を有限で連結な k -正則グラフ族とし， $m \rightarrow \infty$ のとき $g(X_m) \rightarrow \infty$ をみたすとする． $\nu_m = \nu(X_m)$ を

$$\nu_m = \frac{1}{|X_m|} \sum_{j=0}^{|X_m|-1} \delta_{\frac{\mu_j(X_m)}{\sqrt{k-1}}}$$

によって定義される $[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}]$ 上の測度とすると， $[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}]$ 上のすべての連続関数 f について

$$\lim_{m \rightarrow \infty} \int_{-\frac{k}{\sqrt{k-1}}}^{\frac{k}{\sqrt{k-1}}} f(x) d\nu_m(x) = \int_{-2}^2 f(x) \sqrt{4-x^2} \frac{dx}{2\pi}$$

となる．言い換えると， $[-\frac{k}{\sqrt{k-1}}, \frac{k}{\sqrt{k-1}}]$ 上の測度列 $(\nu_m)_{m \geq 1}$ は $d\nu(x) = \frac{\sqrt{4-x^2}}{2\pi} dx$ を与えることで $[-2, 2]$ 上の測度 ν に弱収束する．

系 1.4.11. $(X_m)_{m \geq 1}$ を有限で連結な k -正則なグラフ族とし， $m \rightarrow \infty$ のとき $g(X_m) \rightarrow \infty$ をみたすとする．すべての $\varepsilon > 0$ に対し，定数 $C = C(\varepsilon) > 0$ が存在し，区間 $[-k, (-2+\varepsilon)\sqrt{k-1}]$ 上の X_m の固有値の数は少なくとも $C|X_m|$ である．

1.5 非隣接数と彩色数

$X = (V, E)$ をループのない有限グラフとし， X の隣接行列を A とする．

定義 1.5.1.

- (a) **彩色数** $\chi(X)$ をすべての $i = 1, 2, \dots, \chi$ に対し，すべての $x, y \in V_i$ が $A_{xy} = 0$ となるような分割 $V = V_1 \cup V_2 \cup \dots \cup V_\chi$ の組の最小数とする．
- (b) **非隣接数** $i(X)$ をすべての $x, y \in F$ に対し， $A_{xy} = 0$ となるような部分集合 $F \subset V$ の要素の最大数とする．

補題 1.5.2. X をループなしの n 頂点を持つ有限グラフとする．このとき， $n \leq i(X)\chi(X)$ が成り立つ．

有限で連結している k -正則グラフ X の固有値

$$k = \mu_0 > \mu_1 \geq \dots \geq \mu_{n-1}$$

と $i(X)$ には次の関係がある．

命題 1.5.3. X を有限で連結な n 頂点を持つ k -正則グラフとする．このとき， $i(X) \leq \frac{n}{k} \max\{|\mu_1|, |\mu_{n-1}|\}$ が成り立つ．

補題 1.5.2，命題 1.5.3，命題 1.1.4，定義 1.3.4 から次がわかる．

系 1.5.4. X を有限で連結な n 頂点を持つループなしの k -正則グラフとする．このとき

$$\chi(X) \geq \frac{k}{\max\{|\mu_1|, |\mu_{n-1}|\}}$$

が成り立つ。特に、 X が 2 彩色可能でないラマヌジャングラフならば

$$\chi(X) \geq \frac{k}{2\sqrt{k-1}} \sim \frac{\sqrt{k}}{2}$$

となる。

1.6 大きな girth と大きな彩色数

一般に辺の数が増えると彩色数は増加し（少なくとも減少はしない）、girth は減少する。大きな girth と大きな彩色数を同時に持つグラフの存在という問題には長い歴史がある。なぜなら大きな girth と大きな彩色数を同時に持つと通信効率の面でもコストの面でもよいからだ。次は Erdős によって最初に示されたものである。

定理 1.6.1. k と c を大きな数とする。 $g(X) \geq k$ と $\chi(X) \geq c$ をみたす単純なグラフ X が存在する。

証明. n を自然数とする。頂点数が n 、辺の数が m のグラフの集合を考える。この集合を $\mathcal{X}_{n,m}$ と表す。 $0 < \varepsilon < \frac{1}{k}$ をみたす ε を固定し、 $m = \lfloor n^{1+\varepsilon} \rfloor$ と定める（ $\lfloor \cdot \rfloor$ はガウス記号）。

First Step. まず、 $\mathcal{X}_{n,m}$ の元の個数を数える。頂点 n 個から辺は $\binom{n}{2}$ 本引くことができるので、 m 辺を選ぶと

$$|\mathcal{X}_{n,m}| = \binom{\binom{n}{2}}{m}$$

となる。

Second Step. 次に、 $\mathcal{X}_{n,m}$ の中で非隣接数が小さいものを考える。 $0 < \eta < \frac{\varepsilon}{2}$ をみたす η を固定し、 $p = \lfloor n^{1-\eta} \rfloor$ とする。 X の頂点集合から p 個の元をもつ任意の部分集合をとる。その頂点で作った完全グラフ K_p の辺が X と n 個（かなり大きい数）より多い辺と共有しているものを非隣接数が小さいとする。そうでない悪いグラフとはある完全グラフ K_p と共有している辺が少ししかないときであり、この悪いグラフを考えていく。

p 個の元を固定して考える。 K_p が $0 \leq l \leq n$ をみたす l 辺だけ共有している $X \in \mathcal{X}_{n,m}$ の数は

$$\binom{\binom{p}{2}}{l} \binom{\binom{n}{2} - \binom{p}{2}}{m-l}$$

となる。したがって n 個以下の辺が K_p と共有している $X \in \mathcal{X}_{n,m}$ の数を $\tilde{N}(n, m)$ とすると、

$$\tilde{N}(n, m) = \sum_{l=0}^n \binom{\binom{p}{2}}{l} \binom{\binom{n}{2} - \binom{p}{2}}{m-l}$$

となる。 $n \leq \frac{N}{2}$ かつ $0 \leq l \leq n$ のとき、一般に

$$\binom{N}{l} \leq \binom{N}{n}$$

となるので, 大きな n と $0 \leq l \leq n$ に対し,

$$\binom{\binom{p}{2}}{l} \leq \binom{\binom{p}{2}}{n}, \quad \binom{\binom{n}{2} - \binom{p}{2}}{m-l} \leq \binom{\binom{n}{2} - \binom{p}{2}}{m}$$

がわかる. よって

$$\begin{aligned} \tilde{N}(n, m) &\leq (n+1) \binom{\binom{p}{2}}{n} \binom{\binom{n}{2} - \binom{p}{2}}{m} \leq (n+1) \left(\frac{p(p-1)}{2} \right)^n \binom{\binom{n}{2} - \binom{p}{2}}{m} \\ &\leq \frac{p^{2n}}{2^n} (n+1) \binom{\binom{n}{2} - \binom{p}{2}}{m} \leq p^{2n} \binom{\binom{n}{2} - \binom{p}{2}}{m} \\ &= \frac{p^{2n}}{m!} \left[\binom{n}{2} - \binom{p}{2} \right] \left[\binom{n}{2} - \binom{p}{2} - 1 \right] \cdots \left[\binom{n}{2} - \binom{p}{2} - m + 1 \right] \end{aligned}$$

となる. $0 \leq l \leq m$ のとき

$$\binom{n}{2} - \binom{p}{2} - l \leq \left(\binom{n}{2} - l \right) \left(1 - \frac{\binom{p}{2}}{\binom{n}{2}} \right)$$

より,

$$\begin{aligned} \tilde{N}(n, m) &\leq \frac{p^{2n}}{m!} \binom{n}{2} \left[\binom{n}{2} - 1 \right] \cdots \left[\binom{n}{2} - m + 1 \right] \left(1 - \frac{\binom{p}{2}}{\binom{n}{2}} \right)^m \\ &= p^{2n} \binom{\binom{n}{2}}{m} \left(1 - \frac{\binom{p}{2}}{\binom{n}{2}} \right)^m \\ &\leq p^{2n} \binom{\binom{n}{2}}{m} \left(1 - \left(\frac{p-1}{n-1} \right)^2 \right)^m \end{aligned}$$

となる. $0 < x < 1$ のとき $(1-x)^m < e^{-mx}$ となるので, First Step より

$$\tilde{N}(n, m) \leq p^{2n} e^{-m \left(\frac{p-1}{n-1} \right)^2} |\mathcal{X}_{n,m}|$$

となる.

Third Step. $N(n, m)$ をある K_p と n 辺以下の辺を共有している $X \in \mathcal{X}_{n,m}$ の数とする. K_p は $\binom{n}{p}$ 通りあるので

$$N(n, m) \leq \binom{n}{p} \tilde{N}(n, m)$$

となる.

Fourth Step. $p = \lceil n^{1-\eta} \rceil$ より $\binom{n}{p} \leq n^p \leq p^n$ であるので, Second Step と Third Step より

$$N(n, m) \leq p^{3n} e^{-m \left(\frac{p-1}{n-1} \right)^2} |\mathcal{X}_{n,m}|$$

となる.

Fifth Step. $0 < \eta < \frac{\varepsilon}{2}$, $m = \lceil n^{1+\varepsilon} \rceil$, $p = \lceil n^{1-\eta} \rceil$ であることを使うと,

$$\begin{aligned} \frac{N(n, m)}{|\mathcal{X}_{n,m}|} &\leq p^{3n} e^{-m \left(\frac{p-1}{n-1} \right)^2} \\ &= e^{3n \log p - m \left(\frac{p-1}{n-1} \right)^2} \end{aligned}$$

となる。さらに

$$\begin{aligned}
m \left(\frac{p-1}{n-1} \right)^2 &\geq (n^{1+\varepsilon} - 1) \left(\frac{n^{1-\eta} - 2}{n} \right)^2 \\
&= \frac{n^{3-2\eta+\varepsilon} - 4n^{2-\eta+\varepsilon} + 4n^{1+\varepsilon} - n^{2-2\eta} + 4n^{1-\eta} - 4}{n^2} \\
&\doteq n^{1-2\eta+\varepsilon} \quad (n \text{ が大きいとき})
\end{aligned}$$

であり, $0 < \varepsilon' < -2\eta + \varepsilon$ により $\log p = \varepsilon'$ とできるので

$$\begin{aligned}
3n \log p - m \left(\frac{p-1}{n-1} \right)^2 &\doteq 3n\varepsilon' - n^{1-2\eta+\varepsilon} \\
&\rightarrow -\infty \quad (n \rightarrow \infty)
\end{aligned}$$

となる。よって

$$\frac{N(n, m)}{|\mathcal{X}_{n, m}|} \rightarrow e^{-\infty} = 0 \quad (n \rightarrow \infty)$$

が成り立つ。 $n \rightarrow \infty$ のとき $A(n) = o(B(n))$ とは, $n \rightarrow \infty$ のとき $\frac{A(n)}{B(n)} \rightarrow 0$ が成り立つことと同値であるので, $n \rightarrow \infty$ のとき

$$N(n, m) = o(|\mathcal{X}_{n, m}|)$$

となる。これは $\mathcal{X}_{n, m}$ の中で**すべての** K_p と n 辺より多く共有しているグラフ X の割合が $n \rightarrow \infty$ のとき 1 となることを表している。すなわち, 非隣接数が**小さい** X が存在することを表している。

Sixth Step. これから girth について考える。今まで考えてきた K_p と n 辺より多く共有している X が大きな girth をもつとは限らないからである。 $\mathcal{X}_{n, m}$ 上の整数値関数 F を定義する。最初に固定した k に対し, 長さ $l \leq k$ の X の閉路の数を $F(X)$ とする。 $A(n, k)$ を F の値の平均とすると

$$A(n, k) = \frac{1}{|\mathcal{X}_{n, m}|} \sum_{X \in \mathcal{X}_{n, m}} F(X)$$

となる。

Seventh Step. $A(n, k)$ を別の方法で計算していく。 $3 \leq l \leq k$ のとき, l を固定して $C_l : x_1 \rightarrow x_2 \rightarrow \dots \rightarrow x_l \rightarrow x_1$ となる長さ l の閉路を考える。 C_l を含むグラフの個数は $\binom{\binom{n}{2} - l}{m - l}$ 個であり, $\sum_{X \in \mathcal{X}_{n, m}} F(X)$ では $X \in \mathcal{X}_{n, m}$ の中でこの条件をみたすものは 1 個ずつ数えてある。 $n(n-1)\dots(n-l+1)$ は長さ l の閉路の数である。したがって

$$\begin{aligned}
A(n, k) &= \frac{1}{|\mathcal{X}_{n, m}|} \sum_{l=3}^k n(n-1)\dots(n-l+1) \binom{\binom{n}{2} - l}{m - l} \\
&\leq \sum_{l=3}^k n^l \frac{\binom{\binom{n}{2} - l}{m - l}}{\binom{\binom{n}{2}}{m}} \quad (\text{First Step より}) \\
&= \sum_{l=3}^k n^l \frac{m(m-1)\dots(m-l+1)}{\binom{n}{2} \left(\binom{n}{2} - 1 \right) \dots \left(\binom{n}{2} - l + 1 \right)}
\end{aligned}$$

$$\begin{aligned}
&\leq \sum_{l=3}^k \frac{n^l m^l}{\binom{n}{2} \left(\binom{n}{2} - 1\right) \cdots \left(\binom{n}{2} - l + 1\right)} \\
&= \sum_{l=3}^k \frac{n^l m^l}{\binom{n}{2}^l} \left[1 + \left(\frac{\binom{n}{2}^l}{\binom{n}{2} \left(\binom{n}{2} - 1\right) \cdots \left(\binom{n}{2} - l + 1\right)} - 1 \right) \right]
\end{aligned}$$

となる. () の項は $n \rightarrow \infty$ のとき $o(1)$ となる. これより, $m = \lfloor n^{1+\varepsilon} \rfloor$ と $\varepsilon < \frac{1}{k}$ から

$$\begin{aligned}
A(n, k) &\leq (1 + o(1)) \sum_{l=3}^k \frac{n^l m^l}{\binom{n}{2}^l} \\
&= (1 + o(1)) \sum_{l=3}^k \left(\frac{2m}{n-1} \right)^l \\
&\leq (1 + o(1)) \cdot k \cdot \left(\frac{2m}{n-1} \right)^k \\
&\rightarrow o(n) \quad (n \rightarrow \infty)
\end{aligned}$$

となる.

Eighth Step. $n \rightarrow \infty$ のとき

$$\frac{1}{|\mathcal{X}_{n,m}|} \sum_{X \in \mathcal{X}_{n,m} : F(X) \geq \frac{n}{k}} \frac{n}{k} \leq \frac{1}{|\mathcal{X}_{n,m}|} \sum_{X \in \mathcal{X}_{n,m}} F(X) = A(n, k) = o(n)$$

が成り立つ. よって $n \rightarrow \infty$ のとき

$$\frac{|\{X \in \mathcal{X}_{n,m} : F(X) \geq \frac{n}{k}\}|}{|\mathcal{X}_{n,m}|} = o(1)$$

となる.

Coda. $X \in \mathcal{X}_{n,m}$ に対し, 次の 2 つの性質を考える:

- (1) X は n 辺より多く, すべての K_p と共有している;
- (2) $F(X) < \frac{n}{k}$.

Fifth Step と Eighth Step より $n \rightarrow \infty$ のとき $X \in \mathcal{X}_{n,m}$ が (1), (2) をみたす割合が 1 となる. そこで十分大きな n (k, ε, η により決まる) に対し, (1), (2) をみたす X を選ぶ. X から長さが l 以下の閉路を作る辺すべてを消したものを X' とする. 明らかに $g(X') > k$ である. (2) より X から X' にするのに消した辺は n 辺より少ないので, X' は少なくとも 1 辺がすべての K_p と共有しているので $i(X') \leq p$ が成り立つ. 補題 1.5.2 より $\chi(X') \geq \frac{n}{p}$ であり,

$$\chi(X') \geq \frac{n}{n^{1-\eta}} = n^\eta$$

となる. これは十分大きな n に対して c より大きくなる. よって X' が必要な条件をみたすグラフである. \square

Erdős によって示された定理 1.6.1 は確率論的方法を使っている. この証明方法では大きな girth と大きな彩色数をもつグラフの存在は明らかとなるが, 具体例を見つける手掛かりとはならない. p, q を異なる奇

素数としたとき, Lubotzky と Phillips と Sarnak は $\mathrm{PGL}_2(q)$ または $\mathrm{PSL}_2(q)$ を頂点集合とし, $S_{p,q}$ により辺を構成するグラフ $X^{p,q}$ がラマヌジャンであり, ルジャンドル記号 $\left(\frac{p}{q}\right) = 1$ のときは大きな girth と大きな彩色数をもつことを示した. このことは 3 節にある. なお, この論文の 1 節から 3 節は参考文献 [2] を基本的にまとめたものである.

この論文では部分群 $H \subset \mathrm{PGL}_2(q)$ による, $\mathrm{PGL}_2(q)$ または $\mathrm{PSL}_2(q)$ の剰余類を頂点集合とし, $S_{p,q}$ により辺を構成するグラフ $H \backslash X^{p,q}$ もラマヌジャンであることを示す. このグラフ $H \backslash X^{p,q}$ はどの $h \in H, s \in S_{p,q}$ も共役でなく, m を任意の $h \in H$ に対し, $h^m = 1$ となる最小の自然数としたとき, $X^{p,q}$ の girth が $2m$ より大きいときにループがなく単純である. ループがなく単純のときには, $H \backslash X^{p,q}$ は $X^{p,q}$ に比べ, 頂点数は少なくなるが girth はそれほど小さくはならないことがわかる. すなわち, $H \backslash X^{p,q}$ は大きな girth をもつことがわかる. また, $H \backslash X^{p,q}$ の彩色数は, $X^{p,q}$ が 2 彩色可能でないときは同様の下限をもつことがわかる. 特に, ルジャンドル記号 $\left(\frac{p}{q}\right) = -1$ のときは, $X^{p,q}$ は 2 彩色可能となってしまうが, $H \backslash X^{p,q}$ は部分群 H をうまくとることで 2 彩色可能でなくなり, この場合も他の場合と同様の下限をもつことがわかる. すなわち, 大きな彩色数をもつことがわかる. これによりラマヌジャンで, ループがなく単純な大きな girth と大きな彩色数をもつグラフの具体的な例を増やすことができる.

2 整数論と $\mathrm{PSL}_2(q)$

2.1 2つの平方数の和

この節ではガウスの整数環 $\mathbb{Z}[\mathbf{i}]$ と整四元数環 $\mathbb{H}(\mathbb{Z})$ の様々な性質を見ていく。特に、2.4 節の S_p は $X^{p,q}$ や $H \setminus X^{p,q}$ の構成に必須のものである。また、2.5 節からは $X^{p,q}$ の頂点集合になる $\mathrm{PGL}_2(q)$ や $\mathrm{PSL}_2(q)$ について見ていく。

$k \geq 2$, $n \in \mathbb{Z}$ に対し, $r_k(n)$ を n を k 個の平方数の和で表す方法の個数とする。すなわちディオファントス方程式 $x_0^2 + x_1^2 + \cdots + x_{k-1}^2 = n$ の解の個数である：

$$r_k(n) = \left| \left\{ (x_0, \dots, x_{k-1}) \in \mathbb{Z}^k : \sum_{i=0}^{k-1} x_i^2 = n \right\} \right|.$$

\mathbf{i} を虚数単位とする, すなわち $\mathbf{i}^2 = -1$ をみたすとする。ガウスの整数環 $\mathbb{Z}[\mathbf{i}]$ を

$$\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} : a, b \in \mathbb{Z}\}$$

と定義する。 $\mathbb{Z}[\mathbf{i}]$ が複素数体 \mathbb{C} の部分環であることはすぐわかる。ノルム $N(\alpha)$ を $N(\alpha) = \alpha\bar{\alpha} = |\alpha|^2 = a^2 + b^2$ とすると $N(\alpha)$ は有理整数であるから, 有理整数が2つの平方数の和となることと, あるガウス整数のノルムであることは同値である。ノルムは乗法について

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad (\alpha, \beta \in \mathbb{Z}[\mathbf{i}])$$

となることから, 2つの平方数の和の積が2つの平方数の和となることがわかる。 $\alpha \in \mathbb{Z}[\mathbf{i}] - \{0\}$ とする。 $\alpha^{-1} = \frac{1}{\alpha} \in \mathbb{Z}[\mathbf{i}]$ のとき, α を単元という。 $1 = N(\alpha \cdot \frac{1}{\alpha}) = N(\alpha)N(\frac{1}{\alpha})$ かつ $N(\alpha), N(\frac{1}{\alpha}) \in \mathbb{N} \cup \{0\}$ より α が $\mathbb{Z}[\mathbf{i}]$ の単元となることは $N(\alpha) = 1$ であることと同値である。さらに $N(\alpha) = 1$ は $\alpha \in \{1, -1, \mathbf{i}, -\mathbf{i}\}$ と同値である。

定義 2.1.1.

- (a) 2つのガウス整数 α, β が**同伴**であるとは, ある単元 $\varepsilon \in \mathbb{Z}[\mathbf{i}]$ があり $\alpha = \varepsilon\beta$ が成り立つことである。
- (b) ガウス整数 $\pi \in \mathbb{Z}[\mathbf{i}]$ が**素元**であるとは, π が $\mathbb{Z}[\mathbf{i}]$ の単元でなく, すべての因数分解 $\pi = \alpha\beta \in \mathbb{Z}[\mathbf{i}]$ に対して α または β が $\mathbb{Z}[\mathbf{i}]$ の単元であることである。

同伴である2つの元は $\mathbb{Z}[\mathbf{i}]$ 上で同値関係が成り立ち, 逆元や素元の有無や整除性といった特性を保つ。可換環では定義2.1.1(b)は普通**既約**の定義であり, 素元の定義は命題2.1.5のものである。この2つが同値であることを見ていく。

命題 2.1.2. $\alpha, \beta \in \mathbb{Z}[\mathbf{i}], \beta \neq 0$ とする。 $\gamma, \delta \in \mathbb{Z}[\mathbf{i}]$ があり, $\alpha = \beta\gamma + \delta$ かつ $N(\delta) < N(\beta)$ とできる。

定義 2.1.3. $\alpha, \beta \in \mathbb{Z}[\mathbf{i}]$ を固定する。

- (a) α が β を**割り切る**とは, $\gamma \in \mathbb{Z}[\mathbf{i}]$ があり $\beta = \gamma\alpha$ となることである。
- (b) $\delta \in \mathbb{Z}[\mathbf{i}]$ が α と β の**最大公約数**とは, δ が α と β を割り切り, α と β を割り切るすべての $\gamma \in \mathbb{Z}[\mathbf{i}]$ が δ を割り切ることである。 $(\alpha, \beta) = \delta$ とかく。

明らかに, 最大公約数が存在するとき, 同伴なものを無視すればただ1つである。 $(\alpha, \beta) = \pm 1, \pm \mathbf{i}$ ならば α と β を**互いに素**という。この場合は $(\alpha, \beta) = 1$ とする。

命題 2.1.4. $\alpha, \beta \in \mathbb{Z}[\mathbf{i}] - \{0\}$ に対し, 最大公約数 $(\alpha, \beta) \in \mathbb{Z}[\mathbf{i}]$ が存在する. また, ベズーの等式が成り立つ, すなわち $\gamma, \delta \in \mathbb{Z}[\mathbf{i}]$ があり, $(\alpha, \beta) = \alpha\gamma + \beta\delta$ とできる.

命題 2.1.5. $\pi \in \mathbb{Z}[\mathbf{i}]$ が素元であることは, π が積 $\alpha\beta$ ($\alpha, \beta \in \mathbb{Z}[\mathbf{i}]$) を割り切るとき, π が α または β を割り切ることと同値である.

これから, $\mathbb{Z}[\mathbf{i}]$ の因数分解の一意性が示される.

命題 2.1.6. すべての 0 でない $\mathbb{Z}[\mathbf{i}]$ の元は $\mathbb{Z}[\mathbf{i}]$ の素元の積で単数倍を除いて一意にかける. すなわち $\alpha \in \mathbb{Z}[\mathbf{i}] - \{0\}$ とすると, 素元 $\pi_1, \dots, \pi_k, \sigma_1, \dots, \sigma_l \in \mathbb{Z}[\mathbf{i}]$ があり $\alpha = \pi_1 \cdots \pi_k$ とかけ, さらに $\alpha = \pi_1 \cdots \pi_k = \sigma_1 \cdots \sigma_l$ と α に素元による因数分解が 2 つあるならば, $k = l$ かつ $1 \leq i \leq k$ に対して添字を置換することで π_i と σ_i は同伴となる.

q を素数のべき乗とする. \mathbb{F}_q を元を q 個持つ有限体とする. q 個の元を持つ有限体は 1 種類しかない. \mathbb{F}_q^\times は \mathbb{F}_q の 0 でない元の乗法群を意味する.

定理 2.1.7. p を \mathbb{N} 上の奇素数とする. 次は同値となる:

- (i) $p \equiv 1 \pmod{4}$;
- (ii) -1 が \mathbb{F}_q で平方, すなわち $x^2 \equiv -1 \pmod{p}$ は \mathbb{Z} に解をもつ;
- (iii) p は 2 つの平方数の和となる ($r_2(p) > 0$ である).

次は Fermat と Euler の有名な結果である.

系 2.1.8. 整数 $n \geq 2$ が 2 つの平方数の和でかける ($r_2(n) > 0$) ことは, すべての $p \equiv 3 \pmod{4}$ となる素数が n の素因数分解の中に偶数乗で現れることと同値である.

補題 2.1.9. $n \in \mathbb{Z}, \alpha \in \mathbb{Z}[\mathbf{i}]$ とする. $(m, \alpha) = 1$ と $(m, N(\alpha)) = 1$ は同値である.

命題 2.1.10. ガウス整数 $\pi \in \mathbb{Z}[\mathbf{i}]$ が素元であることは, 次の 3 つのうちの 1 つが成り立つことと同値である:

- (i) $N(\pi) = 2$ (すなわち $\pi = \{1 \pm \mathbf{i}, -1 \pm \mathbf{i}\}$);
- (ii) p を \mathbb{Z} の素元で $p \equiv 1 \pmod{4}$ とする. $N(\pi) = p$ となる;
- (iii) q を \mathbb{Z} の素元で $q \equiv 3 \pmod{4}$ とする. π と q が同伴となる.

$n \in \mathbb{N}$ とし, 次を定義する:

- $d_1(n)$ を法 4 で 1 と合同になる n の約数の個数とする;
- $d_3(n)$ を法 4 で 3 と合同になる n の約数の個数とする;
- $d(n)$ を n の約数の個数とする.

定理 2.1.11. $n \in \mathbb{N}, n > 0$ とする. $r_2(n) = 4(d_1(n) - d_3(n))$ が成り立つ.

$\varepsilon > 0$ を固定する. $n \in \mathbb{N}$ に対し, $f(n) = O_\varepsilon(n^\varepsilon)$ であるとは, ある定数 $C = C(\varepsilon) > 0$ によりすべての $n \in \mathbb{N}$ が

$$|f(n)| \leq Cn^\varepsilon$$

となることである. これを使い, $r_2(n)$ と $r_3(n)$ の増大度を求める.

系 2.1.12. すべての $\varepsilon > 0$ に対し, $r_2(n) = O_\varepsilon(n^\varepsilon)$ となる.

系 2.1.13. すべての $\varepsilon > 0$ に対し, $r_3(n) = O_\varepsilon(n^{\frac{1}{2}+\varepsilon})$ となる.

2.2 平方剰余の相互法則と4つの平方数の和

p を奇素数とする. 定理 2.1.7 は「 -1 が法 p で平方になるのはどんなときか」という問の答えであった. ルジャンドル記号 $\left(\frac{m}{p}\right)$ を

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & (p \text{ が } m \text{ を割り切るとき}) \\ 1 & (p \text{ が } m \text{ を割り切らず, } m \text{ が法 } p \text{ で平方のとき}) \\ -1 & (p \text{ が } m \text{ を割り切らず, } m \text{ が法 } p \text{ で平方でないとき}) \end{cases}$$

と定義する. $Q = \{\alpha^2 : \alpha \in \mathbb{F}_p^\times\} \subset \mathbb{F}_p^\times$ とすると

$$\mathbb{F}_p^\times = Q \cup xQ \quad (x \in \mathbb{F}_p^\times, x \notin Q)$$

より $(\mathbb{F}_p^\times : Q) = 2$ となる. なぜなら

$$\begin{aligned} f : \mathbb{F}_p^\times &\rightarrow \mathbb{F}_p^\times \\ x &\mapsto x^2 \end{aligned}$$

を考えると f は準同型である. よって準同型定理を使うと, $\text{Ker} f = \{\pm 1\}$ より

$$\mathbb{F}_p^\times / \{\pm 1\} \simeq Q$$

であるので

$$|Q| = \frac{|\mathbb{F}_p^\times|}{|\{\pm 1\}|} = \frac{p-1}{2}.$$

よって $(\mathbb{F}_p^\times : Q) = 2$ である. これより

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right) \left(\frac{n}{p}\right) \quad (m, n \in \mathbb{Z})$$

がわかる.

補題 2.2.1. $n \in \mathbb{Z}$ に対し, $n^{\frac{p-1}{2}} \equiv \left(\frac{n}{p}\right) \pmod{p}$ が成り立つ.

ルジャンドル記号の乗法公式より, 任意の m について $\left(\frac{m}{p}\right)$ を求めるためには \mathbb{Z} の素数や -1 のときのルジャンドル記号の値を求めればよい. 次は Gauss により与えられた有名な平方剰余の相互法則である.

定理 2.2.2. p を奇素数とする. このとき, 次が成り立つ;

- (i) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$
- (ii) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$
- (iii) q が p と異なる奇素数のとき, $\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right).$

次に, Jacobi によって与えられた定理 2.2.6 を見ていく.

補題 2.2.3. すべての $n \in \mathbb{N}$ に対し, $r_4(2n) = r_4(4n)$ が成り立つ.

補題 2.2.4. 奇数 $n \in \mathbb{N}$ に対し, $r_4(2n) = 3r_4(n)$ が成り立つ.

$k \geq 2$, $n \in \mathbb{N}$ に対し, $N_k(n)$ を n を k 個の正の奇数の平方の和で表す方法の個数とする:

$$N_k(n) = \left| \left\{ (x_0, \dots, x_{k-1}) \in \mathbb{N}^k : \sum_{i=0}^{k-1} x_i^2 = n, \quad x_i \equiv 1 \pmod{2}, \quad 0 \leq i \leq k-1 \right\} \right|.$$

補題 2.2.5. 奇数 $n \in \mathbb{N}$ に対し, $N_4(4n) = \sum_{d|n} d$ が成り立つ.

補題 2.2.3, 補題 2.2.4, 補題 2.2.5 を使うと Jacobi によって示された次の定理がわかる.

定理 2.2.6. n を正の奇数とする. このとき $r_4(n) = 8 \sum_{d|n} d$ が成り立つ.

2.3 四元数環

2.1 節で 2 つの平方数の和についてガウスの整数環を使い調べたように, 4 つの平方数の和についても整四元数環を使い, 調べていく. しかし, 整四元数は交換可能ではないためより難解である. R を乗法の単位元を持つ任意の可換環とする. この節では R 上の四元数についての性質を述べる. 整四元数環については 2.4 節で見えていく.

定義 2.3.1. R 上のハミルトンの四元数環を $\mathbb{H}(R)$ とかき, 次のように定義する:

- (i) 1 を乗法的単位元とする;
- (ii) $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$;
- (iii) $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$; $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$; $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$;
- (iv) $\mathbb{H}(R)$ を $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$ 上の自由 R -加群とする. すなわち,

$$\mathbb{H}(R) = \{a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} : a_0, a_1, a_2, a_3 \in R\}.$$

$q = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ が四元数のとき, q と共役な四元数を $\bar{q} = a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}$ とする. q のノルムは $N(q) = q\bar{q} = \bar{q}q = a_0^2 + a_1^2 + a_2^2 + a_3^2$ である. 四元数のノルムはガウス整数のノルムと同様に乗法でわけられる. すなわち, $q_1, q_2 \in \mathbb{H}(R)$ のとき

$$N(q_1q_2) = N(q_1)N(q_2)$$

である. したがって 4 つの平方数の和の積はまた 4 つの平方数の和となることがわかる. これからすべての自然数が 4 つの自然数の和でかけられるかという問題は素数についてわかればよい.

ある四元数環と体上の 2×2 行列を同一視していく. 特に有限体 \mathbb{F}_q について必要となるが一般の体について定めることができる.

環の標数とは

$$0 = m \cdot 1 = 1 + 1 + \dots + 1$$

をみたす最小の正の数 m である．もしこのような m が存在しないときは標数は 0 とする．整域，特に体上では標数は 0 または素数である．有理数体 \mathbb{Q} ，実数体 \mathbb{R} ，複素数体 \mathbb{C} の標数はすべて 0 であり，素数のべき乗 $q = p^l$ のよる有限体 \mathbb{F}_q の標数は p である．

K を体とする．写像 $\psi : \mathbb{H}(K) \rightarrow M_2(K)$ を

$$\psi(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) = \begin{pmatrix} a_0 + a_1x + a_3y & -a_1y + a_2 + a_3x \\ -a_1y - a_2 + a_3x & a_0 - a_1x - a_3y \end{pmatrix}$$

と定義する．これは準同型写像である．

命題 2.3.2. K を体とし，標数が 2 でないとする． $x, y \in K$ により $x^2 + y^2 + 1 = 0$ とできるとする．このとき， $\mathbb{H}(K)$ と $M_2(K)$ は同型である．

命題 2.3.2 は明らかに代数閉体だけでなく， q が奇素数のべき乗の有限体 \mathbb{F}_q でも成り立つことが次の命題によりわかる．

命題 2.3.3. q を素数のべき乗とする．このとき， $x, y \in \mathbb{F}_q$ が存在し $x^2 + y^2 + 1 = 0$ となる．

補題 2.3.4. K を体とし，標数が 2 でないとする． $x, y \in K$ により $x^2 + y^2 + 1 = 0$ とできるとする．写像 $\psi : \mathbb{H}(K) \rightarrow M_2(K)$ について次が成り立つ；

- (a) $q \in \mathbb{H}(K)$ に対し， $\det \psi(q) = N(q)$ ， $\text{Tr} \psi(q) = q + \bar{q}$ となる．
- (b) 写像 ψ で実四元数 ($q = \bar{q}$ のとき) はスカラー行列になる．

命題 2.3.5. $q \in \mathbb{H}(\mathbb{Z})$ に対し，次の 3 つは同値である：

- (a) q は $\mathbb{H}(\mathbb{Z})$ に可逆元を持つ；
- (b) $N(q) = 1$ ；
- (c) $q \in \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ ．

2.4 整四元数環における整数論

この節では $\mathbb{H}(\mathbb{Z})$ に制限し，この特別な環の整数論的性質について見ていく．有理整数が 4 つの平方数の和でかけることと $\mathbb{H}(\mathbb{Z})$ のある四元数のノルムとなることは同値である．2.3 節の命題 2.3.5 より $\mathbb{H}(\mathbb{Z})$ の可逆元，すなわち単元が $\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}$ であることがわかる．整四元数の素元による因数分解はできるが \mathbb{Z} や $\mathbb{Z}[\mathbf{i}]$ のように一意的ではない．交換可能ではない環 $\mathbb{H}(\mathbb{Z})$ はユークリッドの互除法を修正したものを持ち，類似の最大公約右 (左) 因子は同伴なものを除くと一意的である． \mathbb{Z} の素数は $\mathbb{H}(\mathbb{Z})$ では素元ではなく，2 つの共役な素四元数の積に因子分解できる．また， $\mathbb{H}(\mathbb{Z})$ の素元かどうかは $\alpha \in \mathbb{H}(\mathbb{Z})$ のノルム $N(\alpha)$ が \mathbb{Z} の素数かどうかにより決まり， $\mathbb{Z}[\mathbf{i}]$ と対照的である ($\mathbb{Z}[\mathbf{i}]$ では素数 $q \equiv 3 \pmod{4}$ は素数となるがノルムは $N(q) = q^2$ であった) ．

定義 2.4.1.

- (a) 四元数 $\alpha \in \mathbb{H}(\mathbb{Z})$ は， $N(\alpha)$ が偶数 (奇数) のとき，**偶数 (奇数)** という．
- (b) 四元数 $\alpha \in \mathbb{H}(\mathbb{Z})$ は， $\mathbb{H}(\mathbb{Z})$ の単元ではなく，すべての $\alpha = \beta\gamma$ について β, γ の一方が必ず単元となるとき，**素元 (素四元数)** という．
- (c) 2 つの四元数 $\alpha, \alpha' \in \mathbb{H}(\mathbb{Z})$ は，ある単元 $\varepsilon, \varepsilon' \in \mathbb{H}(\mathbb{Z})$ により $\alpha' = \varepsilon\alpha\varepsilon'$ となるとき，**同伴** という．
- (d) $\delta \in \mathbb{H}(\mathbb{Z})$ は， $\gamma \in \mathbb{H}(\mathbb{Z})$ により $\alpha = \gamma\delta$ とできるとき， $\alpha \in \mathbb{H}(\mathbb{Z})$ の**右因子** という．

単元 ε に対し $N(\varepsilon) = 1$ より同伴であることは同値関係であり、同伴なものは偶数である、奇数である、素元である、単元であるといった性質を保つ。

\mathbb{Z} や $\mathbb{Z}[\mathbf{i}]$ では素元の定義からベズーの等式を使うことで既約元を定義することができた (命題 2.1.5 より π が素元であることは π が積 xy を割り切るとき、 x または y を割り切ることと同値である)。しかし、明らかに xy の右因子は一般に x の右因子ではないから、交換可能でない環 $\mathbb{H}(\mathbb{Z})$ にはこのような既約元の定義は使えない。したがって $\mathbb{H}(\mathbb{Z})$ ではこの素元の性質なしで進めていく。しかし、定義 2.4.1(b) の素元の定義は素四元数の因子分解の存在を与える。

命題 2.4.2. すべての四元数 $\alpha \in \mathbb{H}(\mathbb{Z})$ は素元の積でかける。

命題 2.4.2 の因子分解は必ずしも一意的ではない (同伴ですらない)。例えば、

$$13 = (1 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k})(1 - 2\mathbf{i} - 2\mathbf{j} - 2\mathbf{k}) = (3 + 2\mathbf{i})(3 - 2\mathbf{i})$$

は素四元数での 13 の 2 種類の因子分解となっている。

奇数の四元数による右からの乗法に限定したユークリッド互除法を考えていく。左からの乗法も同様だが対応する γ_1 と δ_1 は必ずしも一致しない。さらに右からのユークリッド互除法を使い、最大公約右因子を構成する。最大公約左因子についても同様である。

補題 2.4.3. $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ とし、 β を奇数とする。ある $\gamma, \delta \in \mathbb{H}(\mathbb{Z})$ が存在し、

$$\alpha = \gamma\beta + \delta \quad \text{かつ} \quad N(\delta) < N(\beta)$$

となる。

左からのユークリッドの互除法は $\gamma_1, \delta_1 \in \mathbb{H}(\mathbb{Z})$ が存在し、 $\alpha = \beta\gamma_1 + \delta_1$ かつ $N(\delta_1) < N(\beta)$ となることから与えられる。

定義 2.4.4. α, β を整四元数とする。 $\delta \in \mathbb{H}(\mathbb{Z})$ は次をみたすとき、 α と β の**最大公約右因子**という；

- (a) δ は、 α と β の右因子である。
- (b) $\delta_0 \in \mathbb{H}(\mathbb{Z})$ が α と β の右因子であるとき、 δ_0 は δ の右因子である。

δ は $(\alpha, \beta)_r$ によって表す。 $(\alpha, \beta)_r$ は存在するならば同伴なものを除いて一意的である。すなわち、 δ, δ' を α と β の最大公約右因子とすると、ある単元 $\pi \in \mathbb{H}(\mathbb{Z})$ により $\delta = \pi\delta'$ とかける。

補題 2.4.5. $\alpha \in \mathbb{H}(\mathbb{Z})$ とする。このとき α は一意に因子分解できる：

$$\alpha = 2^l \pi \alpha_0,$$

ただし、 $l \in \mathbb{N} \cup \{0\}$ 、 $\pi \in \{1, 1 + \mathbf{i}, 1 + \mathbf{j}, 1 + \mathbf{k}, (1 + \mathbf{i})(1 + \mathbf{j}), (1 + \mathbf{i})(1 - \mathbf{k})\}$ 、 $\alpha_0 \in \mathbb{H}(\mathbb{Z})$ は奇数である。

$\mathbb{Z} \left[\frac{1}{2} \right]$ は有理数の部分環で

$$\mathbb{Z} \left[\frac{1}{2} \right] = \left\{ \frac{k}{2^n} : k \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

と定義する。

定理 2.4.6. $\alpha, \beta \in \mathbb{H}(\mathbb{Z})$ 、 β を奇数とする。このとき $(\alpha, \beta)_r$ が存在し、 $(\alpha, \beta)_r$ はベズーの等式の形でかける。すなわち、 $\gamma, \delta \in \mathbb{H} \left(\mathbb{Z} \left[\frac{1}{2} \right] \right)$ が存在し、 $(\alpha, \beta)_r = \gamma\alpha + \delta\beta$ とできる。

次に \mathbb{Z} と $\mathbb{Z}[\mathbf{i}]$ のときに使ったように最大公約右因子, すなわち $\mathbb{H}(\mathbb{Z})$ の素元でのベズーの等式と $\mathbb{H}(\mathbb{Z})$ での因子分解の定理を発展させて使う. その過程で \mathbb{Z} の素数は自明でない 2 つの共役な四元数の積に因子分解されることがわかる. さらに, α が $\mathbb{H}(\mathbb{Z})$ の素元であることは $N(\alpha)$ が \mathbb{Z} の素数であることと同値であることを見ていく.

まず $\mathbb{Z}[\mathbf{i}]$ のように四元数の整除性とそのノルムの整除性を関係づける. これは補題 2.1.9 とよく似ている.

補題 2.4.7. $\alpha \in \mathbb{H}(\mathbb{Z})$, $m \in \mathbb{Z}$ を奇数とする. $(m, \alpha)_r = 1$ と $(m, N(\alpha))_r = 1$ は同値である.

補題 2.4.8. $p \in \mathbb{N}$ を奇素数とする. ある $\alpha \in \mathbb{H}(\mathbb{Z})$ が存在し, α が p で割り切れず, $N(\alpha)$ が p で割り切れるとする. $(\alpha, p)_r = \delta$ とする. このとき δ は $\mathbb{H}(\mathbb{Z})$ の素元となり, $N(\delta) = p$ である.

定理 2.4.9. すべての奇素数 $p \in \mathbb{N}$ に対し, ある $\delta \in \mathbb{H}(\mathbb{Z})$ が存在し, $p = N(\delta) = \delta\bar{\delta}$ となる. すなわち p は $\mathbb{H}(\mathbb{Z})$ の素元でない.

系 2.4.10. $\delta \in \mathbb{H}(\mathbb{Z})$ が $\mathbb{H}(\mathbb{Z})$ の素元であることは, $N(\delta)$ が \mathbb{Z} の素数であることと同値である.

$\mathbb{H}(\mathbb{Z})$ における整数論から, 有名な Lagrange の 4 つの平方数の和についての結果が得られるが, これは定理 2.2.6 から同様にわかる.

系 2.4.11. すべての自然数は 4 つの平方数の和でかける.

命題 2.4.2 の下の例により, $\mathbb{H}(\mathbb{Z})$ の素元による因子分解の一意性は期待できない. しかし, $p \in \mathbb{N}$ を奇素数とし $N(\alpha) = p^k$ となる整四元数 α に制限すると, 一意性のようなものを取り戻す.

p を奇素数とする. Jacobi の定理 2.2.6 より,

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

は $8(p+1)$ 個の整数解をもち, それぞれノルムが p となる整四元数 $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ に一致する. 解を同伴な 8 個ずつ $p+1$ 組に分類して考える. $p \equiv 1 \pmod{4}$ のとき a_i の 1 つは奇数で残りは偶数となり, $p \equiv 3 \pmod{4}$ のとき a_i の 1 つは偶数で残りは奇数となる. 各場合で 1 つのものを a_i^0 とする.

$p \equiv 1 \pmod{4}$ のときは $a_i^0 \neq 0$ となり, 同伴な 8 個の $\varepsilon\alpha$ 中に $a_0 = |a_i^0|$ となる解が存在する. それを α_i とすると, $\alpha_i \equiv 1 \pmod{2}$ となる. 一方, $p \equiv 3 \pmod{4}$ のときは $a_i^0 \neq 0$ と $a_i^0 = 0$ の可能性があり, $a_i^0 \neq 0$ のときは $p \equiv 1 \pmod{4}$ のときと同様に α_i とすると, $\alpha_i \equiv \mathbf{i} + \mathbf{j} + \mathbf{k} \pmod{2}$ となる. $a_i^0 = 0$ のときは同伴な 8 個の $\varepsilon\alpha$ の中に $a_0 = |a_i^0| = 0$ となる解が存在し, それを β_j とすると $\beta_j \equiv \mathbf{i} + \mathbf{j} + \mathbf{k} \pmod{2}$ となる. β_j となる解はそれぞれ 2 個ずつ存在するが, どちらかを β_j とする. α_i となる解には別の組に共役な $\bar{\alpha}_i$ が存在し, $\bar{\alpha}_i$ も同様の条件をみたしている. ここで,

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

の解の部分集合 S_p を考える. S_p には $\alpha_i, \bar{\alpha}_i$ は共に入れ, β_j と $-\beta_j$ はどちらかを入れる. 言い換えると,

$$S_p = \{\alpha_1, \bar{\alpha}_1, \dots, \alpha_s, \bar{\alpha}_s, \beta_1, \dots, \beta_t\}$$

となる. ただし α_i は $a_0^{(i)} > 0$, β_j は $b_0^{(j)} = 0$ となり, $\alpha_i \bar{\alpha}_i = -\beta_j^2 = p$ をみたす ($a_0^{(i)}, b_0^{(j)}$ はそれぞれ α_i, β_j の a_0 を表す). $2s+t = |S_p| = p+1$ である. (すなわち S_p は $a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$ の解を同伴な 8 個ずつ $p+1$ 組に分類した中から 1 つずつ選んできたものの集合である.)

定義 2.4.12. S_p 上の既約語とは S_p の元の積で $\alpha_i \bar{\alpha}_i, \bar{\alpha}_i \alpha_i, \beta_j^2$ ($i = 1, \dots, s, j = 1, \dots, t$) という部分語がないものをいう. 単語の長さとは単語を構成する記号の数をいう.

定理 2.4.13. $k \in \mathbb{N}$ とし, $\alpha \in \mathbb{H}(\mathbb{Z})$ を奇素数 $p \in \mathbb{N}$ に対し, $N(\alpha) = p^k$ をみたすものとする. このとき α の一意分解 $\alpha = \varepsilon p^r w_m$ が存在する. ただし, ε は $\mathbb{H}(\mathbb{Z})$ の単元, w_m は長さ m の S_p 上の既約語, $k = 2r + m$ である.

$\mathbb{H}(\mathbb{Z})$ の部分集合 Λ' を

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod{2} \text{ または } \alpha \equiv \mathbf{i} + \mathbf{j} + \mathbf{k} \pmod{2}, \quad N(\alpha) \text{ は } p \text{ のべき乗}\}$$

と定義する. Λ' は積について閉じていて, $S_p \subset \Lambda'$ である.

系 2.4.14. すべての $N(\alpha) = p^k$ をみたす $\alpha \in \Lambda'$ は一意分解 $\alpha = \pm p^r w_m$ をもつ. ただし $r \in \mathbb{N}$, w_m は S_p 上の長さ m の既約語, $k = 2r + m$ である.

2.5 $\mathrm{PGL}_2(q)$ と $\mathrm{PSL}_2(q)$

3 節で定義されるラマヌジャングラフ $X^{p,q}$ はこの節で定義する有限群 $\mathrm{PGL}_2(q)$ または $\mathrm{PSL}_2(q)$ を頂点集合として構成される.

K を体とする. $\mathrm{GL}_2(K)$ を係数が K で正則, すなわち行列式が 0 とならない 2×2 行列の群とし, $\mathrm{SL}_2(K)$ を $\mathrm{GL}_2(K)$ のうち行列式が 1 となる部分群とする:

$$\begin{aligned} \mathrm{GL}_2(K) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K, ad - bc \neq 0 \right\}; \\ \mathrm{SL}_2(K) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in K, ad - bc = 1 \right\}. \end{aligned}$$

行列式の写像

$$\det : \mathrm{GL}_2(K) \rightarrow K^\times$$

を考えると $\mathrm{SL}_2(K) = \mathrm{Ker}(\det)$ より $\mathrm{SL}_2(K)$ は $\mathrm{GL}_2(K)$ の正規部分群となる. また $\mathrm{PGL}_2(K)$ と $\mathrm{PSL}_2(K)$ は剰余群で,

$$\begin{aligned} \mathrm{PGL}_2(K) &= \mathrm{GL}_2(K) / \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in K^\times \right\}, \\ \mathrm{PSL}_2(K) &= \mathrm{SL}_2(K) / \left\{ \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon \end{pmatrix} : \varepsilon = \pm 1 \right\} \end{aligned}$$

と定義される.

$P^1(K) = K \cup \{\infty\}$ を K 上の射影直線とする. $\mathrm{PGL}_2(K)$ と $\mathrm{PSL}_2(K)$ は $P^1(K)$ の対称群 $\mathrm{Sym} P^1(K)$ にうめこむことができる. 分数一次変換 (またはメビウス変換) のように, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(K)$ に対し,

$$\varphi_A : P^1(K) \rightarrow P^1(K)$$

を

$$\varphi_A(z) = \frac{az + b}{cz + d}$$

により定義する．ただし， $\varphi_A(\infty) = \begin{cases} \frac{a}{c} & (c \neq 0) \\ \infty & (c = 0) \end{cases}$ ， $\varphi_A\left(\frac{-d}{c}\right) = \infty$ とする．このとき φ_A は全単射となる．
これより，写像

$$\begin{aligned}\varphi : \mathrm{GL}_2(K) &\rightarrow \mathrm{Sym}P^1(K), \\ \varphi(A) &= \varphi_A\end{aligned}$$

を得るが，これは準同型写像である．準同型定理を用いると

$$\mathrm{GL}_2(K)/\mathrm{Ker}(\varphi) \simeq \mathrm{Im}(\varphi)$$

であり， $\mathrm{Ker}(\varphi) = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} : \lambda \in K^\times \right\}$ と $\mathrm{Im}(\varphi) = \varphi(\mathrm{GL}_2(K))$ から $\mathrm{PGL}_2(K)$ と $\varphi(\mathrm{GL}_2(K))$ は同一視できる． $\mathrm{PSL}_2(K)$ と $\varphi(\mathrm{SL}_2(K))$ も同様である．

$K = \mathbb{F}_q$ ，つまり位数 q の有限体のとき，この 4 つの群は $\mathrm{GL}_2(q)$ ， $\mathrm{SL}_2(q)$ ， $\mathrm{PGL}_2(q)$ ， $\mathrm{PSL}_2(q)$ とかく．

命題 2.5.1.

- (a) $|\mathrm{GL}_2(q)| = q(q-1)(q^2-1)$.
- (b) $|\mathrm{SL}_2(q)| = |\mathrm{PGL}_2(q)| = q(q^2-1)$.
- (c) $|\mathrm{PSL}_2(q)| = \begin{cases} q(q^2-1) & (q \text{ が偶数}) \\ \frac{q(q^2-1)}{2} & (q \text{ が奇数}) \end{cases}$.

命題 2.5.2. 写像 $f : \mathrm{SL}_2(q) \rightarrow \mathrm{PGL}_2(q)$ は $q = 2^k$ のとき同型写像となるが， q が奇数のときは同型写像ではない．

命題 2.5.3. 写像 $\varphi : \mathrm{GL}_2(K) \rightarrow \mathrm{PGL}_2(K)$ を考える． $\varphi(A) \in \mathrm{PSL}_2(K)$ となる必要十分条件は $\sqrt{\det A} \in K^\times$ である．

3 節のラマヌジャングラフ $X^{p,q}$ の性質は $\mathrm{PSL}_2(q)$ のある構造上の性質に依存する．単純性はどの $X^{p,q}$ が 2 彩色可能かを決めるのと， $X^{p,q}$ の expanding constant の性質を評価するのに使われる．

補題 2.5.4. 体 K に対し，群 $\mathrm{SL}_2(K)$ は 2 つの部分群 $\left\{ \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} : \lambda \in K \right\}$ と $\left\{ \begin{pmatrix} 1 & 0 \\ \mu & 1 \end{pmatrix} : \mu \in K \right\}$ の和集合により生成される．すなわち，すべての $\mathrm{SL}_2(K)$ の行列は対角成分が 1 となる上三角と下三角の行列の有限積でかける．

群 G が単純であるとは正規部分群が $\{1\}$ か G のみのとき，すなわちすべての群準同型写像 $\pi : G \rightarrow H$ が 1 点 (単位元) のみにいく，または単射であることをいう．次は 1861 年に Jordan によって証明された．

定理 2.5.5. K を体とし， $|K| \geq 4$ とする．このとき $\mathrm{PSL}_2(K)$ は単純群である．

2.6 部分群の構造

3 節でラマヌジャングラフを構成するために必要な連結性を示すために， $\mathrm{PSL}_2(q)$ の部分群の構造をいくつか知る必要がある．

σ を集合 X の置換とし， $x \in X$ とすると σ での x の軌道を $\Omega_x = \{\sigma^k(x) : k \in \mathbb{Z}\}$ と定義する．

補題 2.6.1. σ を集合 X の置換とする. σ が素位数 p をもつとき, すべての X 上での σ の軌道は 1 点のみ, または p 個の元を持つどちらかだけである.

次は補題 2.6.1 を応用したもので Cauchy によって示された.

定理 2.6.2. G を有限群とし, p を素数とする. p が $|G|$ を割り切るとき, G には位数 p となる元が存在する.

定義 2.6.3. 群 G に対し正規部分群 N があり, N と G/N がともにアーベルのとき, G を**メタアーベル**という.

補題 2.6.4. 群 H が指数 2 のアーベル部分群を持つとき, H はメタアーベルである.

G がアーベル群ならば, 明らかに G はメタアーベル群となる. またメタアーベル群は solvable である. すなわち, $G \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\}$ を $G/G_1, G_1/G_2, \dots, G_{n-1}/G_n$ がアーベル群となるようにとれる ($G \triangleright N$ は N が G の正規部分群であることを表す). さらに, 部分群 $H \subset G$ は G がメタアーベルならば H もメタアーベルとなる.

1901 年に Dickson が q が素数のべき乗のときの $\text{PSL}_2(q)$ のすべての部分群のリストを与えた (同型なものを除く). q が素数のときに限定した Dickson のリストをみると, $\text{PSL}_2(q)$ のすべての真部分群は次の 2 つの例外を除いてメタアーベルである:

- 位数 24 の $\text{Sym}(4)$ は solvable だがメタアーベルではない;
- 位数 60 の $\text{Alt}(5)$ は単純群でアーベル群でない.

定理 2.6.5. q を素数とする. H を $\text{PSL}_2(q)$ の真部分群で, $|H| > 60$ とする. このとき H はメタアーベルである.

定理 2.6.5 は次の 2 つの結果からわかる.

命題 2.6.6. q を素数とし, H を $\text{PSL}_2(q)$ の真部分群とする. q が $|H|$ を割り切るとき, H はメタアーベルである.

定理 2.6.7. q を素数とし, H を $\text{PSL}_2(q)$ の部分群とする. $|H| > 60$ で q が $|H|$ を割り切らないとき, H は多くても指数 2 のアーベル部分群を持つ. 特に補題 2.6.4 より H はメタアーベルである. (命題 2.5.1(c) から q が $|H|$ を割り切らないとき, H は真部分群である.)

命題 2.6.6 の証明には $\text{PSL}_2(q)$ の位数 q の元の説明が必要である. $\varphi : \text{SL}_2(q) \rightarrow \text{PSL}_2(q)$ は $\varphi(A) = \varphi_A$ を意味する写像によって定義された. C_b を行列 $C_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ を表すとする.

補題 2.6.8. q を素数とする. $A \in \text{SL}_2(q)$ に対し, 次は同値となる:

- (i) φ_A は位数 q である;
- (ii) A または $-A$ が各点を固定するような \mathbb{F}_q^2 の 1 次元部分空間 D は唯一つである;
- (iii) φ_A はある φ_{C_b} ($b \in \mathbb{F}_q^\times$) と $\text{PGL}_2(q)$ で共役である.

補題 2.6.8 から次がわかる: $A, B \in \text{SL}_2(q)$ を φ_A と φ_B が位数 q となるものとする. A, B が \mathbb{F}_q^2 上の同一直線 D を集合として固定したとすると, φ_A と φ_B は $\text{PSL}_2(q)$ で位数 q の同じ部分群を生成する. これから命題 2.6.6 が示される.

命題 2.6.7 を証明するにはさらに専門用語が必要である.

定義 2.6.9. G を群とする. $J \subset H \subset G$ を部分群とし, $g \in H$ とする.

(a) H の g での**中心化群** $C_H(g)$ とは H の元で g と交換可能な元でできた部分群のことをいう:

$$C_H(g) = \{h \in H : hg = gh\}.$$

(b) H の J での**正規化群** $N_H(J)$ とは H の元で J を正規化する元でできた部分群のことをいう:

$$N_H(J) = \{h \in H : hJh^{-1} = J\}.$$

補題 2.6.10. G を有限群とし, Z を G の中心とする. すべての $g \in G - Z$ に対し, 中心化群 $C_G(g)$ は可換とする. J, K を G の極大アーベル部分群とする. $J \neq K$ のとき $J \cap K = Z$ となる.

補題 2.6.10 の仮定は Z を含む G のすべての部分群に引き継がれる. この仮定は $SL_2(q)$ (q は素数) でもみたされる.

補題 2.6.11. q を素数とする. $SL_2(q)$ のすべてのスカラー行列でない行列はアーベルな中心化群をもつ.

補題 2.6.12. q を奇素数とする. H を $SL_2(q)$ の部分群でスカラー行列を含み, q が $|H|$ を割り切らないものとする. J を極大アーベル部分群とすると, $[N_H(J) : J] \leq 2$ となる.

以上から命題 2.6.7 が示される.

命題 2.6.13. G を群とする. $g_1, g_2 \in G$ に対し, g_1, g_2 の交換子を $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$ と定める. G がメタアーベルであることは, すべての $g_1, g_2, g_3, g_4 \in G$ に対し,

$$[[g_1, g_2], [g_3, g_4]] = 1$$

が成り立つことと同値である.

2.7 有限群の表現論

実または複素ベクトル空間 V 上の群 G の表現は G から V の線形群への準同型写像で, すなわち可逆元を持つ V 上の線形変換の群である. V が有限次元で V の基底が固定されているとき, これは G の表現は V に作用する行列式が 0 でない行列の群への準同型写像を意味する.

G が X に作用するとき X は G -空間という, すなわち G から X の対称群への準同型写像が与えられるとき G -空間という. このとき G は特に X 上の関数空間に作用する. X 上の複素数値関数のベクトル空間を $\mathbb{C}X$ とすると, $\mathbb{C}X$ 上の G の表現 λ_X が

$$(\lambda_X(g)f)(x) = f(g^{-1}x) \quad (g \in G, x \in X)$$

により定義される.

$\mathbb{C}X$ 上の表現 λ_X と可換な 1 次変換 $T : \mathbb{C}X \rightarrow \mathbb{C}X$ が存在するとする, すなわちすべての $g \in G$ に対し,

$$\lambda_X(g)T = T\lambda_X(g)$$

となる T が存在するとする。関数 f を T の固有関数としその固有値を μ とすると $\lambda_X(g)f$ も固有関数となる、すなわち

$$T\lambda_X(g)f = \lambda_X(g)Tf = \mu\lambda_X(g)f$$

が成り立つ。 T の固有空間 V_μ も μ と同様に λ_X で不変な $\mathbb{C}X$ の部分空間である、言い換えると交換可能な 1 次変換の固有空間は表現をより小さな部分空間にわけることができる。

特に $X = (V, E)$ が有限グラフだとする。 G を X の同型写像の群とし、 λ_V を $\mathbb{C}X$ 上の G の表現だとする。 G は辺を辺に移すから λ_X は隣接行列 A と交換可能である。 A は対角化可能であるから A の固有空間をわけることで λ_X を既約にできる。 逆にいえば直感的に G の表現として A の固有値の空間への表現を使うことができる。 その後、 $\mathrm{PSL}_2(q)$ の自明でない表現は少なくとも $\frac{q-1}{2}$ 次元をもつことを見ていく。 これにより 3 節でグラフ $X^{p,q}$ の自明でない固有値の重複度が少なくとも $\frac{q-1}{2}$ 個であることがわかる。

定義 2.7.1. G を群とする。 G の**表現**とは複素ベクトル空間 V と準同型写像 $\pi: G \rightarrow GL(V)$ のことをいい、 (π, V) とかく。 $(GL(V))$ とは V の線形変換の群である。 (π, V) の**次数**を V の次元 $\dim_{\mathbb{C}} V$ とする。

関係しているベクトル空間について混乱がなければ (π, V) のかわりに π とかく。

例 2.7.2.

- (i) 定数準同型写像 $G \rightarrow GL(V)$ は V 上の G の自明な表現で定義する。
- (ii) すべての準同型写像 $G \rightarrow \mathbb{C}^\times$ は \mathbb{C} 上の次数 1 の表現を与える。
- (iii) 空でない集合 X を G -空間とする、すなわち準同型写像 $G \rightarrow \mathrm{Sym}(X)$ が与えられたとする ($\mathrm{Sym}(X)$ は X の置換群)。 $\mathbb{C}X$ を X の有限部分集合上を除いていつも 0 の関数 $X \rightarrow \mathbb{C}$ の集合とする。 $\mathbb{C}X$ 上の**置換表現** λ_X を $f \in \mathbb{C}X, g \in G, x \in X$ により

$$(\lambda_X(g)f)(x) = f(g^{-1}x)$$

と定義する。

- (iv) G を左からのかけ算による G -空間とする。 $\mathbb{C}X$ 上の**左正規表現** λ_G を

$$(\lambda_G(g)f)(x) = f(g^{-1}x) \quad (f \in \mathbb{C}G, g, x \in G)$$

と定義する。

G を右からのかけ算による G -空間とする。 $\mathbb{C}X$ 上の**右正規表現** ρ_G を

$$(\rho_G(g)f)(x) = f(xg) \quad (f \in \mathbb{C}G, g, x \in G)$$

と定義する。

表現を調べるには不変部分空間を調べる方が簡単である。

定義 2.7.3. (π, V) を G の表現とする。 V の線形空間 W はすべての $g \in G$ に対し $\pi(g)(W) = W$ となるとき**不変**という。

W が不変のとき $(\pi|_W, W)$ もまた G の表現で π の**部分表現**と呼ばれる。 部分空間 $\{0\}$ と V は自明な不変部分空間である。

例 2.7.4. X を G -空間とする。 集合

$$W_0 = \left\{ f \in \mathbb{C}X : \sum_{x \in X} f(x) = 0 \right\}$$

は λ_X の不変部分空間である。 X が有限のとき、 W_0 は G -不変な補空間をもち、それは X の定数関数の部分空間 W_1 である。 $\lambda_X|_{W_1}$ は W_1 上の次数 1 の自明な表現である。

定義 2.7.5. $V \neq \{0\}$ の表現 (π, V) は自明でない不変部分空間が存在しないとき**既約**という。

例 2.7.6.

- (i) 次数 1 のすべての表現は既約である。
- (ii) V 上の $GL(V)$ の自然な表現 (自己同型写像 $GL(V) \rightarrow GL(V)$ により与えられたもの) は既約である。なぜなら, $GL(V)$ は同一次元の線形部分空間の集合上で推移的に作用するからである。

同値関係は表現論でも重要な役割をはたす。ここで群 G の表現の同値関係を, 対応する表現の空間上のある種の線形写像の存在により定義する。

定義 2.7.7. (π, V) と (ρ, W) を G の 2 つの表現とする。

- (a) 線形写像 $T: V \rightarrow W$ が π と ρ の**絡作用素**であるとはすべての $g \in G$ に対し, $T\pi(g) = \rho(g)T$ となることをいう。 $\text{Hom}_G(\pi, \rho)$ は π と ρ の絡作用素のベクトル空間である。
- (b) π と ρ にある可逆な絡作用素 $\text{Hom}_G(\pi, \rho)$ が存在するとき, すなわちある線形写像 $T: V \rightarrow W$ がすべての $g \in G$ に対し,

$$\rho(g) = T\pi(g)T^{-1}$$

となるとき, **同値**という。

定義 2.7.7(a) は T が π と ρ の絡作用素のとき, 次の可換図式を意味する:

$$\begin{array}{ccccc} & & \pi(g) & & \\ & & \longrightarrow & & \\ V & & & & V \\ T \downarrow & \circlearrowleft & & & \downarrow T \\ W & & \longrightarrow & & W \\ & & \rho(g) & & \end{array}$$

例 2.7.8.

- (i) 写像 $T: \mathbb{C}G \rightarrow \mathbb{C}G$ を

$$(Tf)(x) = f(x^{-1}) \quad (f \in \mathbb{C}G, x \in G)$$

により定義する。このとき $T^2 = \text{Id}$ と $T \in \text{Hom}_G(\lambda_G, \rho_G)$ から λ_G と ρ_G は同値となる。

- (ii) G -空間 X に対し, 写像 $T: \mathbb{C}X \rightarrow \mathbb{C}$ を

$$f \mapsto \sum_{x \in X} f(x)$$

により定義する。このとき T は λ_X と次数 1 の自明な表現の絡作用素である。

次の結果は有名なシュアーの補題である。この証明は表現論での複素ベクトル空間の役割を説明している。

定理 2.7.9. $(\pi, V), (\rho, W)$ を有限次元で既約な G の表現とする。このとき

$$\dim_{\mathbb{C}} \text{Hom}_G(\pi, \rho) = \begin{cases} 0 & (\pi \text{ と } \rho \text{ が同値でないとき}) \\ 1 & (\pi \text{ と } \rho \text{ が同値のとき}) \end{cases}$$

が成り立つ。

シュアの補題 (定理 2.7.9) を言い換えると次のようになる: (π, V) と (ρ, W) を G の 2 つの既約な表現とし, T を π と ρ の絡作用素とする. このとき, (a) $T \equiv 0$, または (b) T は同型写像, すなわち π と ρ が同値で $V \simeq W$, のどちらかとなる. (b) のとき T は $\lambda \in \mathbb{C}$ によりスカラー写像 $T(v) = \lambda v$ となる.

これからずっと有限次元複素ベクトル空間上の有限群の表現だけを考えていく.

まず, 2 つの有限次元複素ベクトル空間 V と W のテンソル積 $V \otimes W$ を定義する. $v \in V, w \in W$ による組 (v, w) というデカルト積 $V \times W$ と複素係数上の組の有限和からなる加法群を考える. すなわち

$$G = \left\{ \sum \alpha_{ij} (v_i, w_j) : \alpha_{ij} \in \mathbb{C}, v_i \in V, w_j \in W \right\}$$

を考える. G の部分群 H を

- (i) $(v_1 + v_2, w) - (v_1, w) - (v_2, w),$
- (ii) $(v, w_1 + w_2) - (v, w_1) - (v, w_2),$
- (iii) $(v, \alpha w) - (\alpha v, w),$

の形の部分集合の和により生成されるものとする. 写像 $i: V \times W \rightarrow G/H$ を

$$i(v, w) = (v, w) + H$$

により定義する. 群 G/H は \mathbb{C} 上のベクトル空間であるがこれを V と W のテンソル積と呼び, $V \otimes W$ と表す.

$V \otimes W$ の元についてよりわかりやすく説明する. $\{v_i\}_{1 \leq i \leq n}$ と $\{w_j\}_{1 \leq j \leq m}$ をそれぞれ V と W の基底の集合とすると, 集合 $\{i(v_i, w_j)\}$ が $V \otimes W$ の基底の集合となる. くだいていうと $V \otimes W$ は積 $\sum v_r w_s$ の有限和の集合とすることができ, すべての $v \in V, w \in W$ について次が成り立つ:

$$\begin{aligned} (v_1 + v_2)w &= v_1w + v_2w, \\ v(w_1 + w_2) &= vw_1 + vw_2, \\ \alpha(vw) &= (\alpha v)w = v(\alpha w). \end{aligned}$$

さらにテンソル積は次の意味で一意的である: Y を任意のベクトル空間とし, v, w の双方について線形な任意の写像 $B: V \times W \rightarrow Y$ をとったとき, 一意的に線形写像 $\tilde{B}: V \otimes W \rightarrow Y$ が存在して $B = \tilde{B} \circ i$ をみたす.

定義 2.7.10. $(\pi, V), (\rho, W)$ を群 G の表現とする.

- (a) $V^* = \text{Hom}(V, \mathbb{C})$ を V の双対ベクトル空間とする. (π, V) の共役表現 (π^*, V^*) は V^* 上の G の表現で

$$(\pi^*(g)f)(x) = f(\pi(g^{-1})x) \quad (g \in G, x \in V, f \in V^*)$$

により定義される.

- (b) π と ρ の直和とは $V \oplus W$ 上の G の表現 $(\pi \oplus \rho, V \oplus W)$ が

$$(\pi \oplus \rho)(g)(v, w) = (\pi(g)v, \rho(g)w) \quad (g \in G, v \in V, w \in W)$$

となることをいう.

- (c) π と ρ のテンソル積は $V \otimes W$ 上の G の表現 $(\pi \otimes \rho, V \otimes W)$ が 1 つの元のテンソル積 $v \otimes w$ に対しては

$$(\pi \otimes \rho)(g)(v \otimes w) = \pi(g)v \otimes \rho(g)w \quad (g \in G, v \in V, w \in W)$$

により定義される．一般には

$$(\pi \otimes \rho)(g) \left(\sum v_i \otimes w_i \right) = \sum \pi(g)v_i \otimes \rho(g)w_i$$

となる．

例 2.7.11. $(\pi, V), (\rho, W)$ を G の表現とする． $\text{Hom}(V, W)$ 上での表現 σ を

$$\sigma(g)(T) = \rho(g)T\pi(g^{-1}) \quad (g \in G, T \in \text{Hom}(V, W))$$

により定義する． $\rho \otimes \pi^*$ が σ と同値であることを示す． $f \in V^*, w \in W$ に対し，階数 1 の作用素 $\theta_{w,f} \in \text{Hom}(V, W)$ を

$$\theta_{w,f}(v) = f(v)w \quad (v \in V)$$

により定義する．写像 $B : W \times V^* \rightarrow \text{Hom}(V, W) : (w, f) \mapsto \theta_{w,f}$ は双線形であり，これから線形写像

$$\tilde{B} : W \otimes V^* \rightarrow \text{Hom}(V, W) : w \otimes f \mapsto \theta_{w,f}$$

をえる．写像 \tilde{B} は全射で， V と W に対する基底をとることで V^* に対する基底となる． $\dim_{\mathbb{C}}(W \otimes V^*) = \dim_{\mathbb{C}} \text{Hom}(V, W)$ より写像 \tilde{B} は同型写像となる． $g \in G, w \in W, f \in V^*$ に対し

$$\sigma(g)\theta_{w,f} = \theta_{\rho(g)w, \pi^*(g)f} = \tilde{B}(\rho(g)w \otimes \pi^*(g)f)$$

すなわち， $\sigma(g)\tilde{B} = \tilde{B}(\rho \otimes \pi^*)(g)$ となり $\tilde{B} \in \text{Hom}_G(\rho \otimes \pi^*, \sigma)$ となる．

複素ベクトル空間は次の性質をみたすエルミート内積 $(\cdot | \cdot)$ をもつ：

- (i) $v \neq 0$ のとき $(v | v) > 0$,
- (ii) $(v | w) = \overline{(w | v)}$.

命題 2.7.12. (π, V) を有限群 G の表現とする．

- (i) V 上に $\pi(G)$ で不変なエルミート内積 $\langle \cdot | \cdot \rangle$ が存在する，すなわちすべての $g \in G, v_1, v_2 \in V$ に対し， $\langle \pi(g)v_1 | \pi(g)v_2 \rangle = \langle v_1 | v_2 \rangle$ となる．
- (ii) すべての π の不変部分空間 W には不変補空間が存在する，すなわち不変部分空間 W' が存在し， $W \cap W' = \{0\}$ ， $W + W' = V$ となる．
- (iii) $V \neq \{0\}$ のとき， π は G の既約な表現の直和と同値である．

G の表現 (π, V) に対し，

$$V^G = \{v \in V : \pi(g)v = v, \forall g \in G\}$$

を V での $\pi(G)$ -固定ベクトル空間という．これは π の不変部分空間である．

例 2.7.13. X を有限 G -空間とする．関数 $f \in \mathbb{C}X$ が $\lambda_X(G)$ 上で固定されることは， f が X での G の軌道上で不変であることと同値である．特に $\dim_{\mathbb{C}}(\mathbb{C}X)^G$ は X での G の軌道の個数である．

命題 2.7.14. (π, V) を有限群 G の表現とする． $P_\pi = \frac{1}{|G|} \sum_{g \in G} \pi(g)$ とする．このとき，

- (i) $P_\pi^2 = P_\pi$ ，すなわち P_π は $\text{End} V = \text{Hom}(V, V)$ でベキ等である．
- (ii) すべての $h \in G$ に対し， $\pi(h)P_\pi = P_\pi\pi(h) = P_\pi$ となる．
- (iii) $\text{Im} P_\pi = V^G$ ．
- (iv) $\frac{1}{|G|} \sum_{g \in G} \text{Tr} \pi(g) = \dim_{\mathbb{C}}(V^G)$ ．

定義 2.7.15. (π, V) を G の表現とする. π の指標とは関数 $\chi_\pi : G \rightarrow \mathbb{C} : g \mapsto \text{Tr} \pi(g)$ のことをいう.

例 2.7.16. X を有限 G -空間とする. χ_{λ_X} を求めるために $\mathbb{C}X$ の基底として点の特性関数 $(\delta_X)_{x \in X}$ からなるものを使う. $g \in G$ に対し, $\lambda_X(g)\delta_x(y) = \delta_x(g^{-1}y) = \delta_{gx}(y)$, すなわち $\lambda_X(g)\delta_x = \delta_{gx}$ から $\lambda_x(g)$ は置換行列である. $\lambda_X(g)$ のトレースは対角成分上に並ぶ 1 の数, すなわち $\chi_{\lambda_X}(g)$ は X での g の固定点の数となる. これは有限群 G の左正規表現の場合

$$\chi_{\lambda_G}(g) = \begin{cases} |G| & (g = 1 \text{ のとき}) \\ 0 & (g \neq 1 \text{ のとき}) \end{cases}$$

となる.

定義 2.7.10 で構成した表現の指標を見ていく.

命題 2.7.17. $(\pi, V), (\rho, W)$ を群 G の表現とする.

- (i) $\chi_{\pi^*}(g) = \chi_\pi(g^{-1}) \quad (g \in G).$
- (ii) $\chi_{\pi \oplus \rho} = \chi_\pi + \chi_\rho.$
- (iii) $\chi_{\pi \otimes \rho} = \chi_\pi \chi_\rho.$
- (iv) π と ρ が同値のとき, $\chi_\pi = \chi_\rho$ となる.

群 G 上の関数として指標は次の性質をもつ.

補題 2.7.18. (π, V) を有限群 G の表現とする.

- (a) $\chi_\pi(1) = \dim_{\mathbb{C}} V.$
- (b) $g \in G$ に対して, $\chi_\pi(g) = \overline{\chi_\pi(g^{-1})}$ となる.
- (c) $g, h \in G$ に対して, $\chi_\pi(g) = \chi_\pi(hgh^{-1})$ となる.

G 上の関数空間の内積 $f_1, f_2 : G \rightarrow \mathbb{C}$ に対し,

$$\langle f_1 | f_2 \rangle_G = \frac{1}{|G|} \sum_{g \in G} f_1(g) \overline{f_2(g)}$$

により定義する. シュアーの補題 (定理 2.7.9) を使うことで, 群 G の既約な表現に関連した指標がこの内積に対して正規直交であることがわかる.

定理 2.7.19. $(\pi, V), (\rho, W)$ を有限群 G の表現とする. このとき, $\langle \chi_\rho | \chi_\pi \rangle_G = \dim_{\mathbb{C}} \text{Hom}_G(\pi, \rho)$ となる.

系 2.7.20. (π, V) を $V \neq \{0\}$ の有限群 G の表現とする. G の既約な表現 ρ_1, \dots, ρ_k により $\pi = \rho_1 \oplus \dots \oplus \rho_k$ とできる (命題 2.7.12(iii) より). (ρ, W) を G の既約な表現とする. ρ と同値な ρ_i の個数は $\langle \chi_\pi | \chi_\rho \rangle_G$ と等しく, 特にこの個数は π を既約な表現の直和に分解するときの選び方に依らない.

系 2.7.21. (π, V) を $V \neq \{0\}$ の有限群 G の表現とする. 表現 π が既約であることは, $\langle \chi_\pi | \chi_\pi \rangle_G = 1$ であることと必要十分である.

表現の既約な成分への分解は順番を除いては一意的であることを示す. まず, $V = W_1 \oplus \dots \oplus W_r$ を V の既約な G -不変部分空間への分解とする. $\pi : G \rightarrow GL(V)$ とし, $\pi = \pi|_{W_1} \oplus \dots \oplus \pi|_{W_r} = \pi_1 \oplus \dots \oplus \pi_r$ とする. トレースの性質より $\chi_i = \chi_{\pi_i}$ とすると,

$$\chi_\pi = \chi_1 + \dots + \chi_r$$

となる。命題 2.7.17(ii) より、

$$\langle \chi_i | \chi_\pi \rangle = \langle \chi_i | \chi_1 \rangle + \cdots + \langle \chi_i | \chi_r \rangle$$

となる。したがって $\langle \chi_i | \chi_\pi \rangle$ はちょうど π の分解に現れる π_i と同型な表現の個数である。これは明らかに

$$\langle \chi_i | \chi_\pi \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_\pi(g^{-1})$$

より分解の仕方に依らない。これより χ_π は π の表現を決める。実際、 π はちょうどそれぞれ既約な成分 π_i を $\langle \chi_i | \chi_\pi \rangle$ 個ずつ含んでいる。これから次が示される。

定理 2.7.22. $\pi : G \rightarrow GL(V)$ を G の表現とし、 $\pi = \sum n_j \pi_j$ を G の異なる既約な表現 π_j による π の分解とする。このとき、この分解の成分は順番を除いて一意である。

定理 2.7.23. 指標が等しい 2 つの表現は同値であり、任意の既約な表現は重複度が同じである。

定理 2.7.19 より同値でない既約な表現の指標は内積 $\langle \cdot | \cdot \rangle_G$ により $\mathbb{C}G$ 上で直交する。これは G は同値なものを除いて、多くても $|G|$ 種類の既約な表現しかもたないことを意味する。次は次数公式として知られている。

系 2.7.24. $(\rho_1, W_1), \dots, (\rho_k, W_k)$ を有限群 G の既約な表現すべてとする。 $n_i = \dim_{\mathbb{C}} W_i$ を ρ_i の次数とする。このとき、 $|G| = \sum_{i=1}^k n_i^2$ となる。

次数公式は既約な表現がすべてそろっているか判断するのに便利である。

定義 2.7.25. G -空間が 2 重可移であるとは、 $X \times X$ 上の 2 つの $x_i \neq y_i$ ($i = 1, 2$) をみたす組 $(x_1, y_1), (x_2, y_2)$ に対し、ある $g \in G$ が存在し、 $gx_1 = x_2, gy_1 = y_2$ となることをいう。

X 上の G の作用が 2 重可移のとき、可移でもあることはすぐにわかる。 X を有限 G -空間とする。 λ_X^0 は λ_X を余次元 1 の部分空間

$$W_0 = \left\{ f \in \mathbb{C}X : \sum_{x \in X} f(x) = 0 \right\}$$

に制限したものと定義すると、すでに例 2.7.4 で考えたものである。

命題 2.7.26. G を有限群とし、 X を 2 重可移の有限 G -空間とする。このとき λ_X^0 は G の既約な表現である。

命題 2.7.27. G をアーベル群とする。 G のすべての既約な表現は次数 1 である。

命題 2.7.28. G を有限アーベル群で位数 n とする。このとき、次が成り立つ：

- (a) G の既約な表現は同値なものを除いてちょうど n 個あり、それは準同型写像 $\chi_i : G \rightarrow \mathbb{C}^\times$ ($i = 1, \dots, n$) により与えられる。
- (b) 内積 $\langle \cdot | \cdot \rangle_G$ による $\mathbb{C}G$ の正規直交基底として χ_1, \dots, χ_n がとれる。
- (c) $G = \mathbb{Z}/n\mathbb{Z}$ (加法群) に対し、 $\omega = e^{\frac{2\pi i}{n}}$ とする。 $a \in \mathbb{Z}/n\mathbb{Z}$ に対し、

$$e_a(z) = \omega^{az} \quad (z \in \mathbb{Z}/n\mathbb{Z})$$

とする。このとき e_a ($a \in \mathbb{Z}/n\mathbb{Z}$) が G のすべての指標となる。

次の目標は Frobenius による定理 2.7.31 を見ることである．この定理により $X^{p,q}$ の固有値の重複度がわかる． B を \mathbb{F}_q の $ax + b$ 群，すなわち \mathbb{F}_q のアフィン変換

$$z \mapsto az + b \quad (a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q)$$

による群とする． \mathbb{F}_q を B -空間とみなし， B の置換表現 $\lambda_{\mathbb{F}_q}$ を例 2.7.2(iii) のような形とする．

$$W_0 = \left\{ f \in \mathbb{C}\mathbb{F}_q : \sum_{z \in \mathbb{F}_q} f(z) = 0 \right\} \text{ 上の部分表現を } \lambda_{\mathbb{F}_q}^0 \text{ とする.}$$

補題 2.7.29. 表現 $\lambda_{\mathbb{F}_q}^0$ は次数 $q - 1$ の B の既約な表現である．

写像

$$\varphi : \mathrm{SL}_2(q) \rightarrow \mathrm{PSL}_2(q)$$

が命題 2.6.6 の証明のように自然な写像を意味するとし，

$$B_0 = \varphi \left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}$$

を $\mathrm{PSL}_2(q)$ の $\infty \in P^1(\mathbb{F}_q)$ の固定部分群とする． \mathbb{F}_q 上の B_0 の作用は

$$\varphi_A(z) = a^2 z + ab \quad \left(\begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \text{ のとき} \right)$$

により与えられる．これは B_0 が B の指標 2 の部分群と同一であることを意味する．実際， α を全射準同型

$$\alpha : B \rightarrow \mathbb{F}_q^\times : (z \mapsto az + b) \mapsto a$$

とすると， $B_0 = \alpha^{-1}(\mathbb{F}_q^{\times 2})$ とわかる ($\mathbb{F}_q^{\times 2}$ は \mathbb{F}_q^\times 上の平方根の群を意味する)．次は B_0 の表現定理である．

命題 2.7.30. q を奇素数とする． B_0 の既約な表現は $\frac{q+3}{2}$ 個あり，

- $\alpha|_{B_0}$ を経由することで得られる $\frac{q-1}{2}$ 個の群準同型写像 $B_0 \rightarrow \mathbb{C}^\times$ ，
- 次数 $\frac{q-1}{2}$ の 2 つの同値でない表現 ρ_+, ρ_-

によって構成される．

以上から定理 2.7.31 が証明される．

定理 2.7.31. $q \geq 5$ を素数とする． $\mathrm{PSL}_2(q)$ の自明でない表現の次数は少なくとも $\frac{q-1}{2}$ である．

3 グラフ $X^{p,q}$

3.1 ケーリーグラフ

この節でグラフ $X^{p,q}$ について議論をする. G を群 (有限または無限) とし, S を空でない G の有限集合とする. S を対称, すなわち $S = S^{-1}$ とする.

定義 3.1.1. ケーリーグラフ $\mathcal{G}(G, S)$ を頂点集合 $V = G$ と辺集合

$$E = \{\{x, y\} : x, y \in G; \exists s \in S : y = xs\}$$

によるグラフとする.

2 頂点は一方向がある S の元の右乗法によって他方となるととき隣接している. S は対称であるからこの隣接関係も対称であり, 結果としてグラフは無向である.

非同型群は同型ケーリーグラフをもつことができる. 一般に, n 個のシンボル a_1, \dots, a_n で生成される自由群 \mathbb{L}_n と $S = \{a_1^{\pm 1}, \dots, a_n^{\pm 1}\}$ に対し, ケーリーグラフ $\mathcal{G}(G, S)$ は $2n$ -正則な tree である.

命題 3.1.2. $\mathcal{G}(G, S)$ をケーリーグラフとし, $|S| = k$ とする.

- (a) $\mathcal{G}(G, S)$ は単純で k -正則な頂点推移グラフである.
- (b) $\mathcal{G}(G, S)$ がループを持たないことは $1 \notin S$ であることと必要十分である.
- (c) $\mathcal{G}(G, S)$ が連結であることは S が G を生成することと必要十分である.
- (d) G から乗法群 $\{1, -1\}$ への準同型写像 χ が存在して $\chi(S) = \{-1\}$ のとき, $\mathcal{G}(G, S)$ は 2 彩色可能である. 逆は $\mathcal{G}(G, S)$ が連結のとき成り立つ.

証明.

(a) $\mathcal{G}(G, S)$ の隣接行列 $A = (A_{xy})$ は

$$A_{xy} = \begin{cases} 1 & (s \in S \text{ が存在して } y = xs \text{ のとき}) \\ 0 & (\text{その他}) \end{cases}$$

となる. これから明らかに $\mathcal{G}(G, S)$ は単純で k -正則である. 一方, G は左乗法により $\mathcal{G}(G, S)$ 上で左から作用する. この作用は $V = G$ 上の推移である.

(b) 明らか.

(c) $\mathcal{G}(G, S)$ が連結であることは, すべての $x \in G$ が辺をたどることにより $1 \in G$ とつながっていることと必要十分である. これはすべての元 $x \in G$ が S の元により生成される単語として表されることと必要十分であり, すなわち S が G を生成することと必要十分である.

(d) 準同型写像 $\chi: G \rightarrow \{1\}$ が与えられたとき,

$$\begin{aligned} V_+ &= \{x \in G : \chi(x) = 1\}, \\ V_- &= \{x \in G : \chi(x) = -1\} \end{aligned}$$

が $\mathcal{G}(G, S)$ を 2 彩色可能としている. 逆に $\mathcal{G}(G, S)$ が連結で 2 彩色可能とする. V_+ を 2 彩色によって $1 \in G$ となる組とし, V_- をその他の組とする. ($S \subset V_-$ となる.) このとき, 写像 $\chi: G \rightarrow \{\pm 1\}$ を

$$\chi(x) = \begin{cases} 1 & (x \in V_+ \text{ のとき}) \\ -1 & (x \in V_- \text{ のとき}) \end{cases}$$

と定義する． χ が群準同型であることを示す． S が G を生成することから $l_S(x)$ が x に関する S の単語の長さ，すなわち $\mathcal{G}(G, S)$ における x から 1 の距離のとき

$$\chi(x) = (-1)^{l_S(x)}$$

がわかる．よって $G = V_+ \cup V_-$ となり，このとき明らかに χ は群準同型写像である． \square

命題 3.1.3. $\mathcal{G}(G, S)$ をケーリーグラフとし，隣接行列 A は $l^2(G)$ に作用しているとする ($Af(x) = \sum_{y \in G} A_{xy}f(y)$)． $f \in l^2(G)$ に対し $\lambda_G(g)f(x) = f(g^{-1}x)$ ， $\rho_G(g)f(x) = f(xg)$ とする．このとき，次が成り立つ：

$$(a) \ A = \sum_{s \in S} \rho_G(s).$$

(b) μ を A の固有値とし， V_μ を固有空間とする． V_μ は λ_G の不変部分空間である．

証明.

(a) $s \in S$ に対し $\rho_G(s)f(x) = f(xs)$ より， $\sum_{s \in S} \rho_G(s)f(x) = \sum_{s \in S} f(xs)$ である．一方，

$$\begin{aligned} Af(x) &= \sum_{y \in G} A_{xy}f(y) \\ &= \{f(y) : y = xs, s \in S\} \text{ の和} \\ &= \sum_{\substack{y=xs \\ s \in S}} f(y) = \sum_{s \in S} f(xs) \end{aligned}$$

となる．よって $A = \sum_{s \in S} \rho_G(s)$ となる．

(b) $V_\mu = \left\{ f \in l^2(G) : \sum_{s \in S} \rho_G(s)f = \mu f \right\}$ となる．また $f \in V_\mu$ に対し， $\lambda_G(g)f(x) = f(g^{-1}x)$ であるので，

$$\begin{aligned} \sum_{s \in S} \rho_G(s)\lambda_G(g)f(x) &= \sum_{s \in S} \rho_G(s)f(g^{-1}x) \\ &= \mu f(g^{-1}x) = \mu \lambda_G(g)f(x) \end{aligned}$$

となり， $\lambda_G f \in V_\mu$ となる．よって V_μ は λ_G の不変部分空間である． \square

3.2 $X^{p,q}$ の構成

p, q を異なる奇素数とする．定義 2.4.12 の前でノルム p の $p+1$ 個の整四元数の集合

$$S_p = \{\alpha_1, \bar{\alpha}_1, \dots, \alpha_s, \bar{\alpha}_s, \beta_1, \dots, \beta_t\}$$

(α_i は $a_0^{(i)} > 0$ ， β_j は $b_0^{(j)} = 0$ ， $2s+t = p+1$ をみたす) を定義した．

法 q で考える：

$$\tau_q : \mathbb{H}(\mathbb{Z}) \rightarrow \mathbb{H}(\mathbb{F}_q).$$

命題 2.3.3 よりある整数 x, y が存在し, $x^2 + y^2 + 1 \equiv 0 \pmod{q}$ となる. そのような整数を選ぶことで命題 2.3.2 の前のように同型写像 $\psi_q : \mathbb{H}(\mathbb{F}_q) \rightarrow M_2(\mathbb{F}_q)$ を

$$\psi_q(a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}) = \begin{pmatrix} a_0 + a_1x + a_3y & -a_1y + a_2 + a_3x \\ -a_1y - a_2 + a_3x & a_0 - a_1x - a_3y \end{pmatrix}$$

により定義すると, 次の 2 つの性質を持つ (補題 2.3.4 より):

- (a) $\alpha \in \mathbb{H}(\mathbb{F}_q)$ に対し, $N(\alpha) = \det \psi_q(\alpha)$;
- (b) $\alpha \in \mathbb{H}(\mathbb{F}_q)$ が実四元数 ($\alpha = \bar{\alpha}$) のとき, $\psi_q(\alpha)$ はスカラー行列となる.

$\alpha \in S_p$ に対し, $N(\alpha) = p \neq q$ より $\psi_q(\tau_q(\alpha))$ が $M_2(\mathbb{F}_q)$ の可逆群 $\mathrm{GL}_2(q)$ に属することがわかり, また $\psi_q(\tau_q(\alpha\bar{\alpha})) = \psi_q(\tau_q(\bar{\alpha}\alpha))$ は $\mathrm{GL}_2(q)$ の 0 でないスカラー行列である. さらに準同型写像

$$\varphi : \mathrm{GL}_2(q) \rightarrow \mathrm{PGL}_2(q)$$

の核はちょうどスカラー行列の部分群を構成する (2.5 節より). このとき

$$S_{p,q} = (\varphi \circ \psi_q \circ \tau_q)(S_p)$$

とする. 上記のことは $S_{p,q}$ が $\mathrm{PGL}_2(q)$ の対称な部分集合であること, すなわち $S_{p,q}^{-1} = S_{p,q}$ を示している.

補題 3.2.1. q を p に対して十分大きな数 (例えば $q > 2\sqrt{p}$) とするとき, $|S_{p,q}| = p + 1$ となる.

証明. $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$, $\beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ を S_p の 2 つの異なる元とする. すなわち, ある $i \in \{0, 1, 2, 3\}$ に対し $a_i \neq b_i$ とする. $N(\alpha) = N(\beta) = p$ よりすべての $j \in \{0, 1, 2, 3\}$ に対し, $a_j, b_j \in (-\sqrt{p}, \sqrt{p})$ となる. $q > 2\sqrt{p}$ とすると, $a_i \not\equiv b_i \pmod{q}$, すなわち $\tau_q(\alpha) \neq \tau_q(\beta)$ となる. $A = (\psi_q \circ \tau_q)(\alpha)$ かつ $B = (\psi_q \circ \tau_q)(\beta)$ とすると $\mathrm{GL}_2(q)$ で $A \neq B$ となる. ここで $\mathrm{PGL}_2(q)$ で $\varphi_A = \varphi_B$ と仮定する. このとき $\lambda \in \mathbb{F}_q^\times$ が存在して $\lambda \neq 1$ かつ $A = \lambda B$ となる. 行列式をとると $p = \det A = \lambda^2 \det B = \lambda^2 p$ となり $\lambda^2 = 1$, すなわち $\lambda = -1$ となる. $A = -B$ から $\alpha \equiv -\beta \pmod{q}$, すなわちすべての $j \in \{0, 1, 2, 3\}$ に対し $a_j \equiv -b_j \pmod{q}$ となる. $q > 2\sqrt{p}$ から $a_j = -b_j$ となり, これは $\alpha = -\beta$ を意味する. S_p の定義より $a_0, b_0 \geq 0$ より $a_0 = b_0 = 0$ となり $\beta = \bar{\alpha}$ である. しかしこれは 2.4 節での説明の中の $\alpha \in S_p$ が $a_0 = 0$ のとき $\bar{\alpha} \notin S_p$ というものに矛盾する. よって $\varphi_A \neq \varphi_B$ である. 以上から $\alpha \neq \beta$ のとき $\varphi_A \neq \varphi_B$, すなわち $\varphi \circ \psi_q \circ \tau_q$ が単射であることが示された. よって $|S_{p,q}| = p + 1$ である. \square

補題 3.2.1 の範囲 $2\sqrt{p}$ は定理 3.2.2 でのラマヌジャンの範囲の $2\sqrt{p}$ と何の関係もなく, この一致はただの偶然である.

p が法 q で平方のとき, $\left(\frac{p}{q}\right) = 1$ となり, このとき $S_{p,q} \subset \mathrm{PSL}_2(q)$ である (命題 2.5.3 より). $X^{p,q}$ を $S_{p,q}$ による $\mathrm{PSL}_2(q)$ のケーリーグラフと定義する:

$$X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q}).$$

$x' \in g\mathrm{PSL}_2(q)$ ($g \in \mathrm{PGL}_2(q)$, $g \notin \mathrm{PSL}_2(q)$) はすべての $s \in S_{p,q}$ により $x's \in g\mathrm{PSL}_2(q)$ となるので, $X^{p,q}$ と同様に $X'^{p,q} = \mathcal{G}(g\mathrm{PSL}_2(q), S_{p,q})$ を定義すると, これは $X^{p,q}$ と同型である.

p が法 q で平方でないとき, $\left(\frac{p}{q}\right) = -1$ となり, このとき $S_{p,q} \subset \mathrm{PGL}_2(q)$, $S_{p,q} \cap \mathrm{PSL}_2(q) = \emptyset$ である. $X^{p,q}$ を $S_{p,q}$ による $\mathrm{PGL}_2(q)$ のケーリーグラフと定義する:

$$X^{p,q} = \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q}).$$

次の定理により $X^{p,q}$ がラマヌジャングラフであり, girth と 2 彩色可能かどうかができる.

定理 3.2.2. p, q を異なる奇素数で $q > 2\sqrt{p}$ とする. $X^{p,q}$ は連結でラマヌジャンな $(p+1)$ -正則グラフである. さらに

$$(a) \left(\frac{p}{q}\right) = 1 \text{ のとき } X^{p,q} \text{ は } \frac{q(q^2-1)}{2} \text{ 頂点を持つ 2 彩色可能でないグラフで girth は}$$

$$g(X^{p,q}) \geq 2 \log_p q$$

をみたしている.

$$(b) \left(\frac{p}{q}\right) = -1 \text{ のとき } X^{p,q} \text{ は } q(q^2-1) \text{ 頂点を持つ 2 彩色可能なグラフで girth は}$$

$$g(X^{p,q}) \geq 4 \log_p q - \log_p 4$$

をみたしている.

注意 3.2.3.

- (a) $X^{p,q}$ の連結性の問題はとても重要なものの 1 つであり 3.3 節で示す. 命題 3.1.2(c) より $S_{p,q}$ が $\text{PSL}_2(q)$ を生成するか, $\text{PGL}_2(q)$ を生成するかは $\left(\frac{p}{q}\right) = 1$ であるかと $\left(\frac{p}{q}\right) = -1$ であるかと同値である. これは 3.3 節で $q > p^8$ という仮定より少し強い条件で証明する.
- (b) 定理 3.2.2 はなかなか示すことができない. 特に, $X^{p,q}$ に対するラマヌジャン性質は簡単には証明できず, この性質はモジュラー形式のラマヌジャン予想から導く. しかしながら固定された p に対する族 $(X^{p,q})_{q:\text{素数}}$ が family of expanders であることと, 固有値の gap の下限を 3.4 節で初等的な方法で証明する.
- (c) 定理 3.2.2 の一部の証明は簡単である. 命題 3.1.2(a) と補題 3.2.1 から $(p+1)$ -正則であることがわかる. $X^{p,q}$ の頂点の個数は 2.5.1(b) と (c) により与えられる. $\left(\frac{p}{q}\right) = -1$ のとき命題 3.1.2(d) と群準同型写像 $\text{PGL}_2(q)/\text{PSL}_2(q) \simeq \{\pm 1\}$ から $X^{p,q}$ が 2 彩色可能であることがわかる.

命題 3.2.4. $Z^{p,q}$ を次のように構成する. 頂点集合を射影直線 $P^1(\mathbb{F}_q) = \mathbb{F}_q \cup \infty$ とし, 隣接行列 $A = (A_{xy})$ を

$$A_{xy} = |\{s \in S_{p,q} : s(x) = y\}| \quad (x, y \in P^1(\mathbb{F}_q))$$

で決まるものとする. 定理 3.2.2 が示せたならば, $Z^{p,q}$ は $(p+1)$ -正則で連結なラマヌジャングラフである.

証明. $(p+1)$ -正則であることは定義より明らかである.

$\left(\frac{p}{q}\right) = 1$ とすると $\text{PSL}_2(q)$ が $P^1(\mathbb{F}_q)$ に作用している. すなわち, $z \in P^1(\mathbb{F}_q)$ に対し $z \mapsto \frac{az+b}{cz+d}$ である. $B_0 = \left\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} : a \in \mathbb{F}_q^\times, b \in \mathbb{F}_q \right\}$ とすると, $P^1(\mathbb{F}_q) = \text{PSL}_2(q)/B_0$ となる. これから定理 3.2.2 より $X^{p,q}$ は連結であることから $Z^{p,q}$ も連結である.

$X^{p,q}$ の隣接行列は命題 3.1.3 より, $A = \sum_{s \in S_{p,q}} \lambda_{\text{PSL}_2(q)}(s)$ であり, 仮定より $X^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入っている.

$\pi : X^{p,q} \rightarrow Z^{p,q}$ とし, $f \in l^2(Z^{p,q})$ とすると, $f \circ \pi(x) \in l^2(X^{p,q})$ となり, $f \circ \pi(x) = f \circ \pi(xb)$ ($b \in B_0$) となる. 逆に, $g \in l^2(X^{p,q})$ に対し, すべての $x \in X^{p,q}, b \in B_0$ が $g(x) = g(xb)$ となるならば, ある $f \in l^2(Z^{p,q})$ により $g = f \circ \pi$ となる. $W_1 = \{g \in l^2(X^{p,q}) : g(x) = g(xb), x \in X^{p,q}, b \in B_0\} \simeq l^2(Z^{p,q})$ とすると, $W_1 \subset l^2(X^{p,q})$ となる. $s \in S_{p,q}$ に対し, $g(x) \in W_1$ ならば $g(sx) \in W_1$ である. W_1 は A -不変な

ので $Z^{p,q}$ の固有値は $X^{p,q}$ の固有値の一部となる．すなわち， $Z^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入る．

$\left(\frac{p}{q}\right) = -1$ のときも同様である．よって $Z^{p,q}$ はラマヌジャングラフである． \square

3.3 girth と連結性

この節では他の $(p+1)$ -正則なグラフの族 $Y^{p,q}$ を定義し， $X^{p,q}$ への同型写像を作る． $Y^{p,q}$ は tree の商として定義されるので girth を評価することがかなり簡単である．3.4 節で固有値の評価もしやすいことがわかる．

p を奇素数とする．定理 2.4.13 の後で $\mathbb{H}(\mathbb{Z})$ の部分集合 Λ' を

$$\Lambda' = \{\alpha \in \mathbb{H}(\mathbb{Z}) : \alpha \equiv 1 \pmod{2} \text{ または } \alpha \equiv \mathbf{i} + \mathbf{j} + \mathbf{k} \pmod{2}, \quad N(\alpha) \text{ は } p \text{ のべき乗}\}$$

と定義した． Λ' 上で次の同値関係を定義する： $\alpha \sim \beta$ とはある $m, n \in \mathbb{N}$ が存在し， $p^m \alpha = \pm p^n \beta$ となることとする． $[\alpha]$ を $\alpha \in \Lambda'$ の同値類とし， $\Lambda = \Lambda' / \sim$ を同値類の集合とし，

$$Q : \Lambda' \rightarrow \Lambda$$

を商写像 $Q(\alpha) = [\alpha]$ とする．

\sim は乗法についても成り立つ，すなわち $\alpha_1 \sim \beta_1$ ， $\alpha_2 \sim \beta_2$ のとき $\alpha_1 \alpha_2 \sim \beta_1 \beta_2$ となる．このように Λ は積について結合法則をみたし，単位元を持つ．

定義 2.4.12 の前でノルム p の $p+1$ 個の整四元数の集合

$$S_p = \{\alpha_1, \bar{\alpha}_1, \dots, \alpha_s, \bar{\alpha}_s, \beta_1, \dots, \beta_t\}$$

(α_i は $a_0^{(i)} > 0$ ， β_j は $b_0^{(j)} = 0$ ， $2s+t = p+1$ をみたす) を定義した． $S_p \subset \Lambda'$ である．

命題 3.3.1.

- (a) Λ は群である．
- (b) ケーリーグラフ $\mathcal{G}(\Lambda, Q(S_p))$ は $(p+1)$ -正則な tree である．

証明.

- (a) $\alpha \in \Lambda'$ に対し $\alpha \bar{\alpha} = \bar{\alpha} \alpha \sim 1$ となる．よって $[\alpha]^{-1} = [\alpha]$ となり， Λ は群である．
- (b) $\alpha, \beta \in S_p$ に対し， $\alpha \sim \beta$ は $\alpha = \beta$ を意味する．つまり $|Q(S_p)| = p+1$ である．

系 2.4.14 の存在の部分の証明より $\alpha \in \Lambda'$ は S_p の既約語と同値である．言い換えると， Λ は $Q(S_p)$ により生成され，命題 3.1.2 よりグラフ $\mathcal{G}(\Lambda, Q(S_p))$ は $(p+1)$ -正則で連結である．tree であることを示すためには閉路を含まないことを示せばよい．長さ $g \geq 3$ の閉路 $x_0, x_1, x_2, \dots, x_{g-1}, x_g = x_0$ を含むと仮定する．頂点推移より $x_0 = [1]$ としてよい．ケーリーグラフの定義より，ある $\gamma_1, \gamma_2, \dots, \gamma_g \in S_p$ により $x_1 = [\gamma_1], x_2 = [\gamma_1 \gamma_2], \dots, x_g = [\gamma_1 \gamma_2 \dots \gamma_g]$ をえる． $1 \leq k \leq g-1$ に対し， $x_{k-1} \neq x_{k+1}$ より S_p 上の語 $\gamma_1 \gamma_2 \dots \gamma_g$ は既約である．すなわち $\alpha_i \bar{\alpha}_i, \bar{\alpha}_i \alpha_i, \beta_j^2$ ($1 \leq i \leq s, 1 \leq j \leq t$) が存在しない． $[1] = [\gamma_1 \gamma_2 \dots \gamma_g]$ は Λ' 上で

$$p^m = \pm p^n \gamma_1 \gamma_2 \dots \gamma_g$$

となる．しかし， $\gamma_1 \gamma_2 \dots \gamma_g$ は S_p 上の自明でない既約語であるから系 2.4.14 の一意性の部分に矛盾する．よって閉路は存在しない． \square

3.2 節のように法 q で考える.

$$\tau_q : \mathbb{H}(\mathbb{Z}) \rightarrow \mathbb{H}(\mathbb{F}_q)$$

は Λ' から $\mathbb{H}(\mathbb{F}_q)$ の可逆元の群 $\mathbb{H}(\mathbb{F}_q)^\times$ への写像を作る. Z_q を $\mathbb{H}(\mathbb{F}_q)^\times$ の中心とする:

$$Z_q = \{\alpha \in \mathbb{H}(\mathbb{F}_q)^\times : \alpha = \bar{\alpha}\}.$$

$\alpha, \beta \in \Lambda'$ とすると $\alpha \sim \beta$ のとき $\tau_q(\alpha)^{-1}\tau_q(\beta) \in Z_q$ となる. これは $\tau_q : \Lambda' \rightarrow \mathbb{H}(\mathbb{F}_q)^\times$ が well-defined な群準同型

$$\Pi_q : \Lambda \rightarrow \mathbb{H}(\mathbb{F}_q)^\times / Z_q$$

を作ることを意味する. Π_q の核を $\Lambda(q)$ とすると Π_q の像は商群 $\Lambda/\Lambda(q)$ だとわかる. $T_{p,q} = (\Pi_q \circ Q)(S_p)$ とする.

補題 3.2.1 より q を p に対して十分大きな数とすると (例えば $q > 2\sqrt{p}$), $|T_{p,q}| = p+1$ となる. グラフ $Y^{p,q}$ を $T_{p,q}$ による $\Lambda/\Lambda(q)$ のケーリーグラフとする:

$$Y^{p,q} = \mathcal{G}(\Lambda/\Lambda(q), T_{p,q}).$$

Λ は $Q(S_{p,q})$ により生成されるから (命題 3.3.1 の証明より), 命題 3.1.2 より $q > 2\sqrt{p}$ のときグラフ $Y^{p,q}$ は $(p+1)$ -正則で連結となる.

命題 2.3.2 の前の同型写像 $\psi : \mathbb{H}(\mathbb{F}_q)^\times \rightarrow \mathrm{GL}_2(q)$ は Z_q を $\mathrm{GL}_2(q)$ の部分群であるスカラー行列に送り, スカラー行列は $\varphi : \mathrm{GL}_2(q) \rightarrow \mathrm{PGL}_2(q)$ の核となる. したがって同型写像

$$\beta : \mathbb{H}(\mathbb{F}_q)^\times / Z_q \rightarrow \mathrm{PGL}_2(q)$$

を定義できる.

これにより $X^{p,q}$ と $Y^{p,q}$ を可換図式により比較できる.

$$\begin{array}{ccccc} S_p \subset \Lambda' & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \mathrm{GL}_2(q) \\ \downarrow Q & & \downarrow & & \downarrow \varphi \\ \Lambda & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z_q & \xrightarrow{\beta} & \mathrm{PGL}_2(q) \end{array}$$

(これらの縦矢印はすべて商写像である.) グラフ $X^{p,q}$ は $\varphi \circ \psi_q \circ \tau_q$ により定義され, $Y^{p,q}$ は $\Pi_q \circ Q$ により定義される. $X^{p,q}$ が連結かどうかはまだ分からないがどの群からなるかは知っていて, p が法 q で平方かどうかにより $\mathrm{PGL}_2(q)$ か $\mathrm{PSL}_2(q)$ からである. 対称的に $Y^{p,q}$ は定義より連結だが, 群 $\Lambda/\Lambda(q)$ はよくわからない. しかし, $\beta(T_{p,q}) = S_{p,q}$ から $Y^{p,q}$ が $X^{p,q}$ の一部となることがわかる. 両方の構成は互いに反していることからゆくゆくは $X^{p,q}$ は $q > p^8$ のとき連結であり, $X^{p,q}$ と $Y^{p,q}$ は同型であることを示していく.

補題 3.3.2.

$$\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, q \mid a_1, a_2, a_3\}.$$

証明.

$$\begin{aligned} [\alpha] \in \Lambda(q) &\Leftrightarrow \tau_q(\alpha) \in Z_q \\ &\Leftrightarrow q \text{ は } a_0 \text{ を割り切らず, } q \mid a_1, a_2, a_3 \\ &\Leftrightarrow q \mid a_1, a_2, a_3. \end{aligned}$$

2 行目から 3 行目の同値は $N(\alpha)$ は p のべき乗で $p \neq q$ であることからわかる. □

補題 3.3.3. q を奇素数とする. a, b を q で割り切れず, $a^2 \equiv b^2 \pmod{q^2}$ となる整数とする. このとき, $a \equiv \pm b \pmod{q^2}$ となる.

証明. $a^2 \equiv b^2 \pmod{q^2}$ より $a^2 - b^2 \equiv 0 \pmod{q^2}$, すなわち $(a+b)(a-b) \equiv 0 \pmod{q^2}$ となる. このとき $a+b \equiv 0 \pmod{q}$ または $a-b \equiv 0 \pmod{q}$ が成り立つ. $a+b \equiv 0 \pmod{q}$ のとき $a-b \equiv 0 \pmod{q}$ も成り立つとすると $a \equiv b \equiv 0 \pmod{q}$ となり仮定に矛盾する. よって $a-b \not\equiv 0 \pmod{q}$ から $a+b \equiv 0 \pmod{q^2}$ がわかる. $a-b \equiv 0 \pmod{q}$ のときも同様である. よって $a \equiv \pm b \pmod{q^2}$ となる. \square

$Y^{p,q}$ の girth の下限を与える.

命題 3.3.4. $g(Y^{p,q}) \geq 2 \log_p q$ となる. $\left(\frac{p}{q}\right) = -1$ のときは $g(Y^{p,q}) \geq 4 \log_p q - \log_p 4$ となる.

証明. 簡単のため $g(Y^{p,q}) = g$ とする. $x_0, x_1, \dots, x_{g-1}, x_g = x_0$ を $Y^{p,q}$ での長さ g の閉路の頂点とする. $Y^{p,q}$ の頂点推移より $\Lambda/\Lambda(q)$ で $x_0 = x_g = 1$ としてよい. $Y^{p,q}$ はケーリーグラフであるから, $t_1, t_2, \dots, t_g \in T_{p,q}$ があり

$$x_i = t_1 t_2 \cdots t_i \quad (1 \leq i \leq g)$$

とできる. $t_i = \Pi_q([\gamma_i])$ は $\gamma_i \in S_p$ ($i = 1, \dots, g$) により一意的に表される. $\alpha = \gamma_1 \gamma_2 \cdots \gamma_g \in \Lambda'$ を $\alpha = a_0 + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k}$ とする. α は S_p 上の既約語であるので命題 3.3.1(b) より $[\alpha] = [\gamma_1][\gamma_2] \cdots [\gamma_g]$ は Λ で $[1]$ と異なる. すなわち, α は Λ' で 1 と同値でなく, a_1, a_2, a_3 の中の少なくとも 1 つが 0 でないことを意味する. 一方,

$$\Pi_q([\alpha]) = t_1 t_2 \cdots t_g = x_g = 1$$

より $[\alpha] \in \Lambda(q)$ である. 補題 3.3.2 より素数 q は a_1, a_2, a_3 を割り切る. これらの中の少なくとも 1 つは 0 でないから

$$p^g = N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2 \geq q^2$$

となる. p を底にして対数をとると $g(Y^{p,q}) \geq 2 \log_p q$ となる.

$\left(\frac{p}{q}\right) = -1$ とする. $p^g \equiv a_0^2 \pmod{q^2}$ より

$$1 = \left(\frac{p^g}{q}\right) = \left(\frac{p}{q}\right)^g = (-1)^g,$$

となる. すなわち, g は偶数となり, $g = 2h$ といえ,

$$p^{2h} \equiv a_0^2 \pmod{q^2}$$

と表され, 補題 3.3.3 から

$$p^h \equiv \pm a_0 \pmod{q^2} \tag{1}$$

となる. 一方, $a_0^2 \leq p^g$, すなわち $|a_0| \leq p^h$ である. 背理法で示していく. $g < 4 \log_p q - \log_p 4 = \log_p \frac{q^4}{4}$ とすると $p^h < \frac{q^2}{2}$ となる. このとき, $|p^h \mp a_0| < q^2$ となり, (1) より $p^h = \pm a_0$ となる. $p^g = a_0^2$ から $a_1 = a_2 = a_3 = 0$ となり矛盾する. よって $g(Y^{p,q}) \geq 4 \log_p q - \log_p 4$ となる. \square

注意 3.3.5. 命題 1.3.6 から $p \geq 3$ のとき

$$g(Y^{p,q}) \leq 2 + 2 \log_p |Y^{p,q}|$$

であり, 命題 3.3.4 から

$$|Y^{p,q}| \geq \frac{q}{p}$$

となる. また, $\left(\frac{p}{q}\right) = -1$ のときは

$$|Y^{p,q}| \geq \frac{q^2}{2p}$$

となる. これは $|Y^{p,q}| = |\Lambda/\Lambda(q)|$ が少なくとも q の 1 次式となることを示している.

定理 3.3.6. $p \geq 3$ とする. $q > p^8$ に対し, グラフ $X^{p,q}$ は連結である. したがって $X^{p,q}$ と $Y^{p,q}$ は同型である.

証明. 命題 3.1.2(c) より $S_{p,q}$ は $\left(\frac{p}{q}\right) = 1$ のとき $\text{PSL}_2(q)$ を生成し, $\left(\frac{p}{q}\right) = -1$ のとき $\text{PGL}_2(q)$ を生成することを示したい. 同型写像 $\beta: \mathbb{H}(\mathbb{F}_q)^\times / Z_q \rightarrow \text{PGL}_2(q)$ があり, $\beta(T_{p,q}) = S_{p,q}$ となった. これから

$$\beta(\Lambda/\Lambda(q)) = \begin{cases} \text{PSL}_2(q) & \left(\left(\frac{p}{q}\right) = 1 \text{ のとき}\right) \\ \text{PGL}_2(q) & \left(\left(\frac{p}{q}\right) = -1 \text{ のとき}\right) \end{cases}$$

を示せばよい. 2 番目の場合, $S_{p,q} \subset \text{PGL}_2(q)$, $S_{p,q} \cap \text{PSL}_2(q) = \emptyset$ であることはすでに述べている. $H_{p,q} = \text{PSL}_2(q) \cap \beta(\Lambda/\Lambda(q))$ とする. どちらの場合も

$$H_{p,q} = \text{PSL}_2(q)$$

をいえばよい. そのために $|H_{p,q}| > 60$ かつ $H_{p,q}$ がメタアーベルでないことを示す. このとき, もし $H_{p,q} \subsetneq \text{SL}_2(q)$ ならこれは定理 2.6.5 に反する. よって $H_{p,q} = \text{PSL}_2(q)$ がいえる.

$|H_{p,q}| > 60$ であることは $q > p^8$ かつ $p \geq 3$ から, 注意 3.3.5 より

$$|\Lambda/\Lambda(q)| \geq \frac{q}{p} > \frac{p^8}{p} = p^7 \geq 3^7 > 120,$$

すなわち $|\beta(\Lambda/\Lambda(q))| > 120$ より $|H_{p,q}| > 60$ となる.

$H_{p,q}$ がメタアーベルでないことは命題 2.6.13 より, ある $g_1, g_2, g_3, g_4 \in H_{p,q}$ に対し,

$$[[g_1, g_2], [g_3, g_4]] \neq 1$$

を示せばよい. それぞれの場合で考える.

- (a) $\left(\frac{p}{q}\right) = 1$ のとき, $S_{p,q}$ の元の中から次のように g_i を選ぶ. $g_1 \in S_{p,q}$ を任意とし, $g_2 \notin \{g_1^{\pm 1}\}$, $g_3 = g_1$ とし, $g_4 \notin \{g_1^{\pm 1}, g_2^{\pm 1}\}$ とする. このように選ぶと $[[g_1, g_2], [g_3, g_4]]$ は $S_{p,q}$ の長さ 16 の既約語となる. 命題 3.3.4 より $Y^{p,q}$ の girth は

$$\begin{aligned} g(Y^{p,q}) &\geq 2 \log_p q \\ &> 2 \log_p p^8 = 16 \end{aligned}$$

をみたし, $S_{p,q}$ の長さ 16 の既約語は $H_{p,q}$ で 1 と等しくなれない.

- (b) $\left(\frac{p}{q}\right) = -1$ のとき, h_1, h_2, h_3 を $S_{p,q}$ から次のように選ぶ. $h_1 \in S_{p,q}$ を任意とし, $h_2 \notin \{h_1^{\pm 1}\}$, $h_3 \notin \{h_1^{\pm 1}, h_2^{\pm 1}\}$ とする. このとき $g_1 = h_1 h_3$, $g_2 = h_2 h_3$, $g_3 = h_1 h_2$, $g_4 = h_3 h_2$ とすると, これらは $H_{p,q}$ の元となる. このように選ぶと $[g_1, g_2] = h_1 h_3 h_2 h_1^{-1} h_3^{-1} h_2^{-1}$, $[g_3, g_4] = h_1 h_2 h_3 h_1^{-1} h_2^{-1} h_3^{-1}$ より $[[g_1, g_2], [g_3, g_4]]$ は $S_{p,q}$ の長さ 24 の既約語となる. 命題 3.3.4 より $Y^{p,q}$ の girth は

$$\begin{aligned} g(Y^{p,q}) &\geq 4 \log_p q - \log_p 4 \\ &> 4 \log_p p^8 - \log_p 4 \\ &= 32 - \log_p 4 > 24 \end{aligned}$$

をみたし, $S_{p,q}$ の長さ 24 の既約語は $H_{p,q}$ で 1 と等しくなれない.

よって $H_{p,q}$ はメタアーベルではなく, $H_{p,q} = \text{PSL}_2(q)$ がいえた. $S_{p,q}$ が生成元となるので $X^{p,q}$ は連結で, グラフ $Y^{p,q}$ はグラフ $X^{p,q}$ と等しくなることがわかった. \square

系 3.3.7. $q > p^8$ とする. $X^{p,q}$ は $(p+1)$ -正則で連結グラフである.

- (a) $\left(\frac{p}{q}\right) = 1$ のとき, $X^{p,q}$ は 2 彩色可能でなく, girth は

$$g(X^{p,q}) \geq \frac{2}{3} \log_p |X^{p,q}|$$

となる.

- (b) $\left(\frac{p}{q}\right) = -1$ のとき, $X^{p,q}$ は 2 彩色可能で, girth は

$$g(X^{p,q}) \geq \frac{4}{3} \log_p |X^{p,q}| - \log_p 4$$

となる.

証明. 連結性は定理 3.3.6 で示された. girth の評価は命題 3.3.4 と命題 2.5.1 からの $q^3 > |X^{p,q}|$ よりわかる. $\left(\frac{p}{q}\right) = 1$ のときは $g(X^{p,q}) \geq 2 \log_p q > 2 \log_p |X^{p,q}|^{\frac{1}{3}} = \frac{2}{3} \log_p |X^{p,q}|$ で, $\left(\frac{p}{q}\right) = -1$ のときは $g(X^{p,q}) \geq 4 \log_p q - \log_p 4 > 4 \log_p |X^{p,q}|^{\frac{1}{3}} - \log_p 4 = \frac{4}{3} \log_p |X^{p,q}| - \log_p 4$ となる.)

$\left(\frac{p}{q}\right) = 1$ とする. 命題 3.1.2(d) と $X^{p,q}$ の連結性から, $X^{p,q}$ が 2 彩色可能でないことは定理 2.5.5 の $\text{PSL}_2(q)$ が単純であることを使うとわかる. $\left(\frac{p}{q}\right) = -1$ のとき, $X^{p,q}$ が 2 彩色可能であることは注意 3.2.3(c) でわかっている. \square

注意 3.3.8. 族 $(X_m)_{m \geq 1}$ を有限で連結な k -正則グラフで, $m \rightarrow +\infty$ のとき $|X_m| \rightarrow +\infty$ をみたすとする. $C > 0$ が存在し, $g(X_m) \geq (C + o(1)) \log_{k-1} |X_m|$ のとき **大きな girth** をもつという. 命題 1.3.6 より $C \leq 2$ となる. Erdős と Sachs は構成的でない方法で $C = 1$ をみたす族があることを示した. $\left(\frac{p}{q}\right) = -1$ のとき, グラフ $X^{p,q}$ は $(p+1)$ -正則で大きな girth を持つ, すなわち $C = \frac{4}{3}$ をみたす族となった. これは, 構成的な方法が構成的でない方法よりも良い結果となる, グラフ理論での数少ない例の 1 つである.

補題 3.3.9. $p \equiv 1 \pmod{4}$ とする. $\Lambda(q) = \{[\alpha] \in \Lambda : \alpha = a_0 + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k}, 2q \mid a_1, a_2, a_3\}$ とする.

証明. $p \equiv 1 \pmod{4}$ から S_p の定義より a_1, a_2, a_3 は偶数である. \square

命題 3.3.10. $p \equiv 1 \pmod{4}$ で $\left(\frac{p}{q}\right) = -1$ のとき, $g(Y^{p,q}) \geq 4 \log_p q$ となる.

証明. $p \equiv 1 \pmod{4}$ で $\left(\frac{p}{q}\right) = -1$ とする. $p^g \equiv a_0^2 \pmod{q^2}$ より

$$1 = \left(\frac{p^g}{q}\right) = \left(\frac{p}{q}\right)^g = (-1)^g$$

となる. すなわち, g は偶数となり $g = 2h$ がいえ,

$$p^{2h} \equiv a_0^2 \pmod{q^2}$$

と表され, 補題 3.3.3 から

$$p^h \equiv \pm a_0^2 \pmod{q^2}$$

となり, a_0 は S_p の定義より奇数なので

$$p^h \equiv \pm a_0^2 \pmod{2q^2} \quad (2)$$

となる. 一方 $a_0^2 \leq p^g$ すなわち $|a_0| \leq p^h$ である. 背理法で示していく. $q < 4 \log_p q$ とすると $p^h < q^2$ となる. このとき $|p^h \mp a_0| < 2q^2$ となり (2) より $p^h = \pm a_0$ となる. $p^g = a_0^2$ から $a_1 = a_2 = a_3 = 0$ となり矛盾する. よって $g(Y^{p,q}) \geq 4 \log_p q$ である. \square

3.4 固有値の評価

この節では固定された p に対して族 $X^{p,q}$ が family of expanders であり, p が q に対し十分大きいときの固有値の gap の下極限を示す.

$X^{p,q}$ の頂点数を命題 2.5.2 より計算したものとし, n とおき,

$$\mu_0 = p + 1 > \mu_1 \geq \mu_2 \geq \cdots \geq \mu_{n-1}$$

を隣接行列の固有値とする. 1.4 節で f_m を後戻りなしの始点, 終点 1 の長さ m の $X^{p,q}$ 上の経路の数とした. 命題 3.1.2(a) から $X^{p,q}$ は頂点推移であり, 系 1.4.7 の trace formula を $X^{p,q}$ でとると, すべての $m \in \mathbb{N}$ に対し,

$$\sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r} = \frac{p^{\frac{m}{2}}}{n} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{p}} \right)$$

となる.

trace formula の左辺を別の解釈をしていく. このために 4 変数の 2 次形式を導入する:

$$\mathcal{Q}(x_0, x_1, x_2, x_3) = x_0^2 + q^2(x_1^2 + x_2^2 + x_3^2).$$

また, $m \geq 1$ に対し,

$$s_{\mathcal{Q}}(p^m) = |\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : \mathcal{Q}(x_0, x_1, x_2, x_3) = p^m, \\ x_0 \text{ が奇数で } x_1, x_2, x_3 \text{ が偶数, または } x_0 \text{ が偶数で } x_1, x_2, x_3 \text{ が奇数}\}|$$

と定義する.

注意 3.4.1. m が偶数または $p \equiv 1 \pmod{4}$ とする. 法 4 で考えると前の定義からわかることは現れるすべての 4 つ組 (x_0, x_1, x_2, x_3) は x_0 が奇数で x_1, x_2, x_3 が偶数となる. 2 次形式を導入する:

$$\mathcal{Q}'(x_0, x_1, x_2, x_3) = x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2).$$

m が偶数または $p \equiv 1 \pmod{4}$ のとき $s_{\mathcal{Q}}(p^m)$ はちょうど 2 次形式 \mathcal{Q}' による p^m の表現と同じになる.

一般の p に戻る.

補題 3.4.2. $m \in \mathbb{N}$ に対し, $s_{\mathcal{Q}}(p^m) = 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$ となる.

証明. 定理 3.3.6 より $X^{p,q}$ と $Y^{p,q}$ は同一視できる. $x_0 = 1, x_1, \dots, x_{l-1}, x_l = 1$ を後戻りなしの始点, 終点が 1 の長さ l の $Y^{p,q}$ の経路とする. 命題 3.3.4 の証明より, $t_1, \dots, t_l \in T_{p,q}$ があり, $x_i = t_1 t_2 \cdots t_i$ ($1 \leq i \leq l$) とできる. $\alpha \in S_p$ ($i = 1, \dots, l$) により $t_i = \Pi_q([\alpha_i])$ と一意的にかける. $[\alpha_1][\alpha_2] \cdots [\alpha_l]$ は後戻りなしの経路であるから, Λ 上の長さ l の既約語となり, $\Pi_q([\alpha_1][\alpha_2] \cdots [\alpha_l]) = x_l = 1$ となるから $[\alpha_1][\alpha_2] \cdots [\alpha_l]$ は $\Lambda(q)$ に属する. これから f_l は $\Lambda(q)$ に属する長さ l の Λ での既約語の数となる.

$(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4$ が $s_{\mathcal{Q}}(p^m)$ の条件をみたすとする. $\alpha = x_0 + q(x_1 \mathbf{i} + x_2 \mathbf{j} + x_3 \mathbf{k})$ とすると, この四元数 α は Λ' に属し, 補題 3.3.2 より同値類は $\Lambda(q)$ に入る. これから次となる;

$$s_{\mathcal{Q}}(p^m) = |\{\alpha = a_0 + a_1 \mathbf{i} + a_2 \mathbf{j} + a_3 \mathbf{k} \in \Lambda' : N(\alpha) = p^m, q \mid a_1, a_2, a_3\}|. \quad (3)$$

α が (3) の右辺の条件をみたすとする. 系 2.4.14 より α は一意分解 $\alpha = \pm p^l \omega_{m-2l}$ をもつ, ただし ω_{m-2l} は S_p の長さ $m-2l$ の既約語である. 類 $[\alpha]$ は Λ 上で長さ $m-2l$ の既約語となり $\Lambda(q)$ に属する. 反対に $\Lambda(q)$ に属する長さ $m-2l$ の既約語 ω から $\alpha = \pm p^l \omega$ のように 2 つの四元数を生成できる. これは

$$|\{\alpha \in \Lambda' : N(\alpha) = p^m, [\alpha] \in \Lambda(q)\}| = 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$$

を意味し, すなわち

$$s_{\mathcal{Q}}(p^m) = 2 \sum_{0 \leq r \leq \frac{m}{2}} f_{m-2r}$$

となる. □

$X^{p,q}$ の trace formula はすべての $m \in \mathbb{N}$ に対し,

$$s_{\mathcal{Q}}(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} U_m \left(\frac{\mu_j}{2\sqrt{p}} \right)$$

となる. ここで \mathbb{C} の部分集合 Θ_p を導入する:

$$\Theta_p = [\mathbf{i} \log \sqrt{p}, 0] \cup [0, \pi] \cup [\pi, \pi + \mathbf{i} \log \sqrt{p}].$$

複素数 $z \in \mathbb{C}$ のコサインとサインは

$$\begin{aligned} \cos z &= 1 - \frac{z^2}{2!} + \frac{z^4}{4!} - \frac{z^6}{6!} + \cdots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n}}{(2n)!} = \frac{e^{\mathbf{i}z} + e^{-\mathbf{i}z}}{2} \\ \sin z &= z - \frac{z^3}{3!} + \frac{z^5}{5!} - \frac{z^7}{7!} + \cdots = \sum_{n=0}^{\infty} (-1)^n \frac{z^{2n+1}}{(2n+1)!} = \frac{e^{\mathbf{i}z} - e^{-\mathbf{i}z}}{2\mathbf{i}} \end{aligned}$$

と定義された. 変数変換 $z \rightarrow 2\sqrt{p} \cos z$ の写像は Θ_p から $[-(p+1), p+1]$ への全単射となる. 特に, この変数変換は $[0, \pi]$ を $[-2\sqrt{p}, 2\sqrt{p}]$ に移すので $[0, \pi]$ をラマヌジャン区間とみることができる. $j = 0, 1, \dots, n-1$ に対し $\theta_j \in \Theta_p$ を Θ_p の一意的な元で $\mu_j = 2\sqrt{p} \cos \theta_j$ となるものとする. 特に $\theta_0 = \mathbf{i} \log \sqrt{p}$ で, $\left(\frac{p}{q}\right) = -1$ のとき:

$$\theta_{n-1} = \pi + \mathbf{i} \log \sqrt{p} \quad (\text{系 3.3.7 より}).$$

チェビシエフ多項式 U_m の定義より

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j}$$

となる.

$X^{p,q}$ がラマヌジャンであることを示すためには $\theta_0 = \mathbf{i} \log \sqrt{p}$ と, $\left(\frac{p}{q}\right) = -1$ のときは $\theta_{n-1} = \pi + \mathbf{i} \log \sqrt{p}$ を除いたら, すべての θ_j が実数であることを示す必要がある. これは最初に注意 3.4.7 の方法で示された. 初等的な方法では今のところできないが, その代わり十分大きな q に対し θ_j の虚数部分が p だけに依存して決まることで十分だということを示す. これにより $X^{p,q}$ が family of expanders であることがわかる.

trace formula から θ_j の重複度は固有値の重複度に一致することがわかる.

命題 3.4.3. μ を $X^{p,q}$ の非自明な固有値, すなわち $|\mu| \neq p+1$ とし, その重複度を $M(\mu)$ とする, このとき $M(\mu) \geq \frac{q-1}{2}$ となる.

証明. V_μ を μ に対応する固有空間とする. 命題 3.1.3 からベクトル空間 V_μ は $X^{p,q}$ を構成している群の表現空間である. この群は常に $\text{PSL}_2(q)$ を含んでいることから V_μ は $\text{PSL}_2(q)$ の表現空間である. 定理 2.7.31 から $\text{PSL}_2(q)$ の表現の次数は少なくとも $\frac{q-1}{2}$ である. $|\mu| \neq p+1$ のとき V_μ 上の $\text{PSL}_2(q)$ の表現が非自明であることを示せばよい. 背理法で示す. V_μ 上の $\text{PSL}_2(q)$ の表現が自明とする. 2つの場合に分ける.

$\left(\frac{p}{q}\right) = 1$ のとき, 表現が自明ならば $f(g^{-1}x) = \lambda_{\text{PSL}_2(q)}(g)f(x) = f(x)$ より $f(x)$ は定数である. $\mu f(x) = Af(x) = \sum_{s \in S_{p,q}} f(xs) = (p+1)f(x)$ から $\mu = p+1$ となる.

$\left(\frac{p}{q}\right) = -1$ のとき, 0 でない関数 $f \in V_\mu$ は $\text{PGL}_2(q)$ の $\text{PSL}_2(q)$ による 2つの剰余類となり, それぞれ定数となる, すなわち

$$f(x) = \begin{cases} a_+ & (x \in \text{PSL}_2(q) \text{ のとき}) \\ a_- & (x \in \text{PGL}_2(q), x \notin \text{PSL}_2(q) \text{ のとき}) \end{cases}$$

とできる. f は $X^{p,q}$ の隣接行列の固有関数であるので

$$\mu f(x) = Af(x) = \sum_{s \in S_{p,q}} f(xs) = \begin{cases} (p+1)a_- & (x \in \text{PSL}_2(q) \text{ のとき}) \\ (p+1)a_+ & (x \in \text{PGL}_2(q), x \notin \text{PSL}_2(q) \text{ のとき}) \end{cases}$$

から

$$\begin{cases} \mu a_+ = (p+1)a_- \\ \mu a_- = (p+1)a_+ \end{cases}$$

となる. f は 0 でないので $\mu^2 = (p+1)^2$, すなわち $|\mu| = p+1$ となり, 2つの場合とも矛盾となる.

以上から $M(\mu) \geq \frac{q-1}{2}$ となる. □

定理 3.4.4. 実数 ε を $0 < \varepsilon < \frac{1}{6}$ に固定する. 十分大きな q に対し, $X^{p,q}$ のすべての非自明な固有値 μ は

$$|\mu| \leq p^{\frac{5}{6} + \varepsilon} + p^{\frac{1}{6} - \varepsilon}$$

をみたす. 特に $X^{p,q}$ は family of expanders である.

証明. $X^{p,q}$ の trace formula から始める: すべての $m \in \mathbb{N}$ に対し,

$$s_{\mathcal{Q}}(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j}$$

となった. ここで $\mu_j = 2\sqrt{p} \cos \theta_j$ とする. μ_j がラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ にないとき

$$\begin{cases} \theta_j = \mathbf{i}\psi_j & (2\sqrt{p} < \mu_j \leq p+1 \text{ のとき}) \\ \theta_j = \pi + \mathbf{i}\psi_j & (-(p+1) \leq \mu_j < -2\sqrt{p} \text{ のとき}) \end{cases}$$

となり, どちらも $0 < \psi_j \leq \log \sqrt{p}$ である.

今後, m を偶数とする. 複素数 z のハイパボリックサインとハイパボリックコサインを

$$\begin{aligned} \sinh z &= \frac{e^z - e^{-z}}{2} = \mathbf{i} \sin(-\mathbf{i}z), \\ \cosh z &= \frac{e^z + e^{-z}}{2} = \cos(\mathbf{i}z) \end{aligned}$$

と定義する. $\mu_j \notin [-2\sqrt{p}, 2\sqrt{p}]$ のとき, どちらの場合も m は偶数だから

$$\frac{\sin(m+1)\theta_j}{\sin \theta_j} = \frac{\sin \mathbf{i}(m+1)\psi_j}{\sin \mathbf{i}\psi_j} = \frac{\sinh(m+1)\psi_j}{\sinh \psi_j} \geq 0$$

となる. このとき自明な固有値 $\mu_k \notin [-2\sqrt{p}, 2\sqrt{p}]$ を固定すると

$$\begin{aligned} s_{\mathcal{Q}}(p^m) &= \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j: \mu_j \neq \mu_k} \frac{\sinh(m+1)\theta_j}{\sinh \theta_j} \\ &\geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j: |\mu_j| \leq 2\sqrt{p}} \frac{\sinh(m+1)\theta_j}{\sinh \theta_j} \end{aligned}$$

となる. 実数 θ に対し,

$$\begin{aligned} \left| \frac{\sin(m+1)\theta}{\sin \theta} \right| &= \left| \frac{\sin(m\theta) \cos \theta + \cos(m\theta) \sin \theta}{\sin \theta} \right| \\ &\leq \left| \frac{\sin(m\theta) \cos \theta}{\sin \theta} \right| + |\cos(m\theta)| \\ &\leq \left| \frac{\sin(m\theta) \cos \theta}{\sin \theta} \right| + 1 \\ &\leq m+1 \end{aligned}$$

となるので

$$s_{\mathcal{Q}}(p^m) \geq \frac{2}{n} p^{\frac{m}{2}} M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} - 2p^{\frac{m}{2}}(m+1) \quad (4)$$

となる. 注意 3.4.1 より $s_{\mathcal{Q}}(p^m)$ を評価する. m が偶数より $s_{\mathcal{Q}}(p^m)$ は

$$x_0^2 + 4q^2(x_1^2 + x_2^2 + x_3^2) = p^m$$

の整数解の個数である．まず x_0 の選び方の個数を評価する． $|x_0| \leq p^{\frac{m}{2}}$ であり， $x_0^2 \equiv p^m \pmod{q^2}$ より補題 3.3.3 を使うと

$$x_0 \equiv \pm p^{\frac{m}{2}} \pmod{q^2}$$

となる． x_0 と p は共に奇数だから

$$x_0 \equiv \pm p^{\frac{m}{2}} \pmod{2q^2}$$

となる．これより x_0 の選び方は多くて $\left(\frac{p^{\frac{m}{2}}}{q^2} + 1\right)$ 通りとなる．いったん x_0 を固定し，

$$x_1^2 + x_2^2 + x_3^2 = \frac{p^m - x_0^2}{4q^2}$$

を整数解で解く．2.1 節の記号を使うと $r_3\left(\frac{p^m - x_0^2}{4q^2}\right)$ 通りである．系 2.1.13 より，すべての $\varepsilon > 0$ に対し

$$r_3\left(\frac{p^m - x_0^2}{4q^2}\right) = O_\varepsilon\left(\left(\frac{p^m}{q^2}\right)^{\frac{1}{2}+\varepsilon}\right)$$

となる．このとき

$$\begin{aligned} s_{\mathcal{Q}}(p^m) &= O_\varepsilon\left[\frac{p^{\frac{m}{2}+\varepsilon m}}{q^{1+2\varepsilon}}\left(\frac{p^{\frac{m}{2}}}{q^2} + 1\right)\right] \\ &= O_\varepsilon\left[\frac{p^{m(1+\varepsilon)}}{q^{3+2\varepsilon}} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q^{1+2\varepsilon}}\right] \\ &= O_\varepsilon\left[\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q}\right] \end{aligned}$$

となる．

したがって，ある定数 $C_\varepsilon > 0$ により (4) は

$$\frac{M(\mu_k)}{n} \cdot p^{\frac{m}{2}} \cdot \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon \left[\frac{p^{m(1+\varepsilon)}}{q^3} + \frac{p^{\frac{m}{2}(1+2\varepsilon)}}{q} \right] + p^{\frac{m}{2}}(m+1)$$

となる． $p^{\frac{m}{2}}$ を消して， $n \leq q^3$ を使うと，

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon \left[p^{m(\frac{1}{2}+\varepsilon)} + q^2 p^{m\varepsilon} \right] + q^3(m+1)$$

となる． m を $p^{\frac{m}{2}} \leq q^3$ となるように選んだとする．このとき

$$M(\mu_k) \frac{\sinh(m+1)\psi_k}{\sinh \psi_k} \leq C_\varepsilon [q^{3+6\varepsilon} + q^{2+6\varepsilon}] + q^3(1+6\log_p q)$$

となる． $\sinh \psi_k \leq \sinh \log \sqrt{p}$ から

$$M(\mu_k) \sinh(m+1)\psi_k = O_\varepsilon [q^{3+6\varepsilon}]$$

となる． m を $p^{\frac{m}{2}} \leq q^3$ をみたす 1 番大きな偶数とする．十分大きな q に対し，

$$\sinh(m+1)\psi_k \geq \frac{e^{(m+1)\psi_k}}{3} \geq \frac{e^{(-1+6\log_p q)\psi_k}}{3} \geq \frac{p^{-\frac{1}{2}}}{3} e^{6\log_p q \cdot \psi_k}$$

となる．最後の不等式は $\psi_k \leq \log \sqrt{p}$ を使っている．このとき

$$M(\mu_k) = O_\varepsilon \left(q^{3+6\varepsilon - \frac{6\psi_k}{\log p}} \right)$$

となる． μ_k は非自明な固有値なので命題 3.4.3 より

$$M(\mu_k) \geq \frac{q-1}{2}$$

となる．十分大きな q に対して

$$3 + 6\varepsilon - \frac{6\psi_k}{\log p} \geq 1,$$

すなわち

$$\psi_k \leq \left(\frac{1}{3} + \varepsilon \right) \log p$$

となる．

このとき， $\theta_k = \mathbf{i}\psi_k$ または $\theta_k = \pi + \mathbf{i}\psi_k$ と $\mu_k = 2\sqrt{p} \cos \theta_k$ から， q が十分大きいとき

$$\begin{aligned} |\mu_k| &= 2\sqrt{p} |\cos(\mathbf{i}\psi_k)| \\ &= 2\sqrt{p} \cosh \psi_k \\ &\leq \sqrt{p} (e^{(\frac{1}{3}+\varepsilon)\log p} + e^{-(\frac{1}{3}+\varepsilon)\log p}) \\ &= p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon} \end{aligned}$$

となる．これから $\varepsilon \in \left(0, \frac{1}{6}\right)$ を固定する．十分大きな q に対し，定理 1.2.3 より

$$h(X^{p,q}) \geq \frac{p+1 - p^{\frac{5}{6}+\varepsilon} - p^{\frac{1}{6}-\varepsilon}}{2}$$

となる．よって $X^{p,q}$ は family of expanders である． □

系 3.4.5. 実数 ε を $0 < \varepsilon < \frac{1}{6}$ に固定する． $\left(\frac{p}{q}\right) = 1$ のとき $\mu_{n-1} \neq -(p+1)$ より q が十分大きいとき，系 1.5.4 より

$$\chi(X^{p,q}) \geq \frac{p+1}{p^{\frac{5}{6}+\varepsilon} + p^{\frac{1}{6}-\varepsilon}}$$

となる．

次の系により，大きな girth と大きな彩色数を持つ有限なグラフ族の構成がわかる．これは 1.6 節の確率論的証明では解決できなかったことだ．

系 3.4.6. $N \in \mathbb{N}$ を固定する．十分大きな素数 q に対し，

$$g(X^{p,q}) \geq N \quad \text{かつ} \quad \chi(X^{p,q}) \geq N$$

となる奇素数 p が存在する．

証明. p を $\frac{p+1}{p^{\frac{11}{12}} + p^{\frac{1}{12}}} \geq N$ をみたすよう十分大きく選ぶ．このとき， q を次の 4 条件を同時にみたすように十分大きく選ぶ：

- (a) $q \geq p^8$;
- (b) $2 \log_p q \geq N$;
- (c) $\left(\frac{p}{q}\right) = 1$;
- (d) $\chi(X^{p,q}) \geq \frac{p+1}{p^{\frac{11}{12}} + p^{\frac{1}{12}}}$.

これから命題 3.3.4 と定理 3.3.6 より

$$\min\{g(X^{p,q}), \chi(X^{p,q})\} \geq N$$

をえる. □

注意 3.4.7. グラフ $X^{p,q}$ がラマヌジャンであることの証明の概略を記していく.

ラマヌジャン予想はモジュラー尖点形式の係数の増大度についての予想で, 重さ 2 でのこの予想は Eichler によって証明された.

2 次形式の Q' の θ -関数は

$$\theta(z) = \sum_{x \in \mathbb{Z}^4} e^{2\pi i Q'(x)z} = \sum_{k=0}^{\infty} r_{Q'}(k) e^{2\pi i k z}$$

により与えられる; ここで $r_{Q'}(k)$ は整数 k の形式 Q' による整数表現の個数である. このとき θ は重さ 2 のモジュラー形式で; θ をアイゼンシュタイン級数と尖点形式の和として分解すると, Eichler の結果を偶数 m に対し $r_{Q'}(p^m) = s_Q(p^m)$ と得ることができる. 特にすべての $\varepsilon > 0$ に対し

$$s_Q(p^m) = \frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} + O_\varepsilon\left(p^{\frac{m}{2}(1+\varepsilon)}\right)$$

となる. この結果と初等的な証明であった定理 3.4.4 に含まれている評価を比べることは興味深い.

$X^{p,q}$ の trace formula は

$$s_Q(p^m) = \frac{2}{n} p^{\frac{m}{2}} \sum_{j=0}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j}$$

であった. 主要な項 $\frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1}$ は自明な固有値, すなわち

$$\begin{cases} \theta_0 = i \log \sqrt{p} & \left(\left(\frac{p}{q}\right) = 1 \text{ のとき} \right) \\ \theta_0 = i \log \sqrt{p}, \theta_{n-1} = \pi + i \log \sqrt{p} & \left(\left(\frac{p}{q}\right) = -1 \text{ のとき} \right) \end{cases}$$

により与えられる. まず, $\frac{\sin(m+1)\theta_0}{\sin \theta_0} = p^{-\frac{m}{2}} \cdot \frac{p^{m+1}-1}{p-1}$ を示す.

$$\begin{aligned} \frac{\sin(m+1)\theta_0}{\sin \theta_0} &= \frac{\sinh(m+1)(-\log \sqrt{p})}{\sinh(-\log \sqrt{p})} \\ &= \frac{e^{(m+1)(-\log \sqrt{p})} - e^{(m+1) \log \sqrt{p}}}{e^{(-\log \sqrt{p})} - e^{\log \sqrt{p}}} \\ &= \frac{p^{-\frac{1}{2}(m+1)} - p^{\frac{1}{2}(m+1)}}{p^{-\frac{1}{2}} - p^{\frac{1}{2}}} \\ &= \frac{p^{\frac{m}{2}+1} - p^{-\frac{m}{2}}}{p-1} \\ &= p^{-\frac{m}{2}} \cdot \frac{p^{m+1}-1}{p-1} \end{aligned}$$

となる. $\frac{\sin(m+1)\theta_{n-1}}{\sin \theta_{n-1}} = p^{-\frac{m}{2}} \cdot \frac{p^{m+1}-1}{p-1}$ も同様である.

$\left(\frac{p}{q}\right) = 1$ のとき $n = \frac{q(q^2-1)}{2}$ であるので,

$$\begin{aligned} s_{\mathcal{Q}}(p^m) &= \frac{4}{q(q^2-1)} p^{\frac{m}{2}} \cdot p^{-\frac{m}{2}} \frac{p^{m+1}-1}{p-1} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \\ &= \frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \end{aligned}$$

となる. $\left(\frac{p}{q}\right) = -1$ のとき $n = q(q^2-1)$ であるので,

$$\begin{aligned} s_{\mathcal{Q}}(p^m) &= \frac{2}{q(q^2-1)} p^{\frac{m}{2}} \cdot 2p^{-\frac{m}{2}} \frac{p^{m+1}-1}{p-1} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j=1}^{n-2} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \\ &= \frac{4}{q(q^2-1)} \frac{p^{m+1}-1}{p-1} + \frac{2}{n} p^{\frac{m}{2}} \sum_{j=1}^{n-2} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \end{aligned}$$

となる. これから $\left(\frac{p}{q}\right) = 1$ のときを考える. $\left(\frac{p}{q}\right) = -1$ のときも同様である. ラマヌジャン-アイヒラーの評価より

$$\frac{2}{n} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j} = O_{\varepsilon}(p^{\frac{\varepsilon m}{2}})$$

となることがわかる. これより

$$\left| \frac{2}{n} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \right| \leq C_{\varepsilon} p^{\frac{\varepsilon m}{2}} \quad (5)$$

となる. θ_j が実数でないものがあるとする. 定理 3.4.4 のように $\theta_j = \mathbf{i}\psi_j$ または $\theta_j = \pi + \mathbf{i}\psi_j$ ($0 < \psi_j \leq \log \sqrt{p}$) とすると, m が偶数から

$$\frac{2}{n} \frac{\sin(m+1)\theta_j}{\sin \theta_j} = \frac{2}{n} \frac{\sinh(m+1)\psi_j}{\sinh \psi_j} > 0$$

となる. また,

$$\left| \frac{2}{n} \sum_{i: \theta_i \text{ が実数}} \frac{\sin(m+1)\theta_i}{\sin \theta_i} \right| \leq 2(m+1)$$

である. これらから

$$\begin{aligned} \left| \frac{2}{n} \sum_{j=1}^{n-1} \frac{\sin(m+1)\theta_j}{\sin \theta_j} \right| &= \left| \frac{2}{n} \sum_{i: \theta_i \text{ が実数}} \frac{\sin(m+1)\theta_i}{\sin \theta_i} + \frac{2}{n} \sum_{j: \theta_j \text{ が虚数}} \frac{\sinh(m+1)\psi_j}{\sinh \psi_j} \right| \\ &\geq - \left| \frac{2}{n} \sum_{i: \theta_i \text{ が実数}} \frac{\sin(m+1)\theta_i}{\sin \theta_i} \right| + \left| \frac{2}{n} \sum_{j: \theta_j \text{ が虚数}} \frac{\sinh(m+1)\psi_j}{\sinh \psi_j} \right| \\ &\geq -2(m+1) + \frac{2}{n} \sum_{j: \theta_j \text{ が虚数}} \frac{2e^{m\psi_j}}{3} \end{aligned} \quad (6)$$

となる. (5),(6) より

$$C_{\varepsilon} p^{\frac{\varepsilon m}{2}} \geq -2(m+1) + \frac{2}{n} \sum_{j: \theta_j \text{ が虚数}} \frac{2e^{m\psi_j}}{3}$$

となる. $\frac{\varepsilon}{2} < \psi_j$ とし, m を偶数で十分大きくとると, これは矛盾する. よって θ_j はすべて実数であり, グラフ $X^{p,q}$ はラマヌジャンであることがわかる.

4 グラフ $H \backslash X^{p,q}$

4.1 商ケーリーグラフ

この節でいよいよ $H \backslash X^{p,q}$ を定義する．まず，この節で商ケーリーグラフの基本的な性質を示し，4.2 節で $H \backslash X^{p,q}$ の性質を示す．ラマヌジャングラフであることを 4.3 節で示し，4.4 節で girth や彩色数について議論する．

定義 4.1.1. $\mathcal{G}(G, S)$ をケーリーグラフとする (G は群, S は空でない G の有限集合で対称であった)． G を部分群 H で左から割った剰余類 $H \backslash G$ を頂点集合とする． $Hx, Hy \in H \backslash G$, $s \in S$ により $Hy = Hxs$ となるとき Hx と Hy を結ぶ辺があるものとする． $s' \in S$ により $Hx = Hys'$ となるとき $s' = s^{-1}$ ならばこれは 1 つの辺とする． $s_1, s_2 \in S$, $s_1 \neq s_2$ により $Hy = Hxs_1, Hy = Hxs_2$ となるとき，どちらも Hx と Hy に辺を与えるが，これらは異なる辺とする．すなわち，多重辺となる．これらの頂点集合と辺集合によるグラフを $H \backslash \mathcal{G}(G, S)$ とかき，**商ケーリーグラフ** という．

商ケーリーグラフ $H \backslash \mathcal{G}(G, S)$ は $|S| = k$ とすると明らかに k -正則グラフである．まず， $H \backslash \mathcal{G}(G, S)$ が連結である条件を示す．

命題 4.1.2. $\langle S \rangle$ を S の元が生成する群とする．商ケーリーグラフ $H \backslash \mathcal{G}(G, S)$ が連結となることは， $H \langle S \rangle = G$ となることと必要十分である．

証明.

(\implies) $H \backslash \mathcal{G}(G, S)$ が連結とする．任意の $x \in G$ をとると Hx は辺をたどることで H とつながっている．すなわち， $s_1, \dots, s_i \in S$ が存在し， $Hx = Hs_1 \cdots s_i$ となる．このとき $h \in H$ があり $x = hs_1 \cdots s_i$ となる．よって $H \langle S \rangle = G$ となる．

(\impliedby) $H \langle S \rangle = G$ とすると，任意の $x \in G$ は $h \in H$, $s_1, \dots, s_i \in S$ が存在し， $x = hs_1 \cdots s_i$ とかける．これにより $Hx = Hs_1 \cdots s_i$ となるので Hx は辺をたどることで H とつながっている．よって任意の Hx は H とつながっているので連結である． \square

$\mathcal{G}(G, S)$ は命題 3.1.2(a),(b) のとき，ループをもたず，単純であった．しかし， $H \backslash \mathcal{G}(G, S)$ は $\mathcal{G}(G, S)$ がループをもたず，単純であっても，ループがあったり，多重辺が存在したりする． $H \backslash \mathcal{G}(G, S)$ がループをもたない条件は次の補題である．

補題 4.1.3. $H \backslash \mathcal{G}(G, S)$ がループをもたないことは，どの $h \in H$, $s \in S$ も共役でない，すなわち $xhx^{-1} = s$ となる $x \in G$ がないことと必要十分である．

証明. 明らか． \square

次の命題が $H \backslash \mathcal{G}(G, S)$ が単純である条件である．

命題 4.1.4. m を任意の $h \in H$ に対し， $h^m = 1$ となる最小の自然数とする． $\mathcal{G}(G, S)$ の girth が $2m$ より大きいとき， $H \backslash \mathcal{G}(G, S)$ は単純である．

証明. 背理法で示す．単純でない，すなわち多重辺があるとすると，ある $Hx \in H \backslash G$ に対し $s_1, s_2 \in S$, $s_1 \neq s_2$ が存在し $Hxs_1 = Hxs_2$ となる．このとき $h \in H$ があり

$$xs_1 = hxs_2$$

となる．これより $x = hxs_2s_1^{-1}$ となるから

$$\begin{aligned} xs_1 &= hxs_2 = h(hxs_2s_1^{-1})s_2 \\ &= h^2xs_2s_1^{-1}s_2 = h^2(hxs_2s_1^{-1})s_2s_1^{-1}s_2 \\ &= \cdots \\ &= h^m xs_2s_1^{-1} \cdots s_2s_1^{-1}s_2 \quad (s_1^{-1}s_2 \text{ は } m-1 \text{ 個}) \end{aligned}$$

となる．仮定より $h^m = 1$ であるので $s_1 = s_2s_1^{-1} \cdots s_2s_1^{-1}s_2$ である．すなわち

$$\begin{aligned} 1 &= s_1^{-1}s_2s_1^{-1} \cdots s_2s_1^{-1}s_2 \quad (s_1^{-1}s_2 \text{ は } m \text{ 個}) \\ &= (s_1^{-1}s_2)^m \end{aligned}$$

となる．これは $\mathcal{G}(G, S)$ の girth が $2m$ より大きいことと矛盾する．よって， $\mathcal{G}(G, S)$ の girth が十分大きいとき $H \backslash \mathcal{G}(G, S)$ は単純である． \square

4.2 グラフ $H \backslash X^{p,q}$

この節以降は $H \backslash X^{p,q}$ について考えていく． p と q を異なる奇素数とする．

定義 4.2.1. $H \subset \mathrm{PGL}_2(q)$ とする． $X^{p,q}$ による商ケーリーグラフ $H \backslash X^{p,q}$ を次のように定義する；

- (Ia) $\left(\frac{p}{q}\right) = 1$ で $H \subset \mathrm{PSL}_2(q)$ のときは， $H \backslash \mathrm{PSL}_2(q)$ を頂点集合とし，辺集合を $S_{p,q}$ によって決まるものとする商ケーリーグラフを $H \backslash X^{p,q}$ とかく．
- (Ib) $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \mathrm{PSL}_2(q)$ のときは， $X^{p,q} = \mathcal{G}(\mathrm{PSL}_2(q), S_{p,q})$ と $X'^{p,q} = \mathcal{G}(g\mathrm{PSL}_2(q), S_{p,q})$ ($g \in \mathrm{PGL}_2(q), g \notin \mathrm{PSL}_2(q)$) が同型であったことから， $\mathrm{PSL}_2(q) \cup g\mathrm{PSL}_2(q) = \mathrm{PGL}_2(q)$ より， $H \backslash \mathrm{PGL}_2(q)$ を頂点集合とし，辺集合を $S_{p,q}$ によって決まるものとする商ケーリーグラフを $H \backslash X^{p,q}$ とかく．
- (II) $\left(\frac{p}{q}\right) = -1$ のときは， $H \backslash \mathrm{PGL}_2(q)$ を頂点集合とし，辺集合を $S_{p,q}$ によって決まるものとする商ケーリーグラフを $H \backslash X^{p,q}$ とかく．

$H \backslash X^{p,q}$ は連結である．特に， $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \mathrm{PSL}_2(q)$ のときも $H \backslash X^{p,q}$ は連結となる．なぜなら， $H \langle S_{p,q} \rangle = H\mathrm{PSL}_2(q) = \mathrm{PGL}_2(q)$ となるからである．補題 4.1.3 のループの条件は $H \backslash X^{p,q}$ のとき，命題 4.2.2 のようになる．

命題 4.2.2. m を任意の $h \in H$ に対し， $h^m = 1$ となる最小の自然数とする． $X^{p,q}$ の girth が m より大きく， H の位数 2 の元が $S_{p,q}$ のどの元とも共役でないとき， $H \backslash X^{p,q}$ はループをもたない．

証明. 背理法で示す．ループをもつとすると，補題 4.1.3 より $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \mathrm{PSL}_2(q)$ または $\left(\frac{p}{q}\right) = -1$ のときは $Hx \in H \backslash \mathrm{PGL}_2(q)$ ， $\left(\frac{p}{q}\right) = 1$ で $H \subset \mathrm{PSL}_2(q)$ のときは $Hx \in H \backslash \mathrm{PSL}_2(q)$ に対し， $s \in S_{p,q}$ が存在し $Hx = Hxs$ となる．このとき $h \in H$ があり

$$x = hxs$$

となる。これより

$$\begin{aligned}
x &= hxs = h(hxs)s \\
&= h^2xs^2 = h^2(hxs)s^2 \\
&= \dots \\
&= h^m xs^m
\end{aligned}$$

となる。仮定より $h^m = 1$ であるので

$$1 = s^m$$

となる。また $x = hxs$ より $s = x^{-1}h^{-1}x$ であるから、 s と h^{-1} は共役となり特に位数は等しい。すなわち、 s は位数 2 でないので $s^2 \neq 1$ となり、 s^m は後戻りをもたない。これは $X^{p,q}$ の girth が m よりも大きいことに矛盾する。よって $X^{p,q}$ の girth が十分大きいとき $H \setminus X^{p,q}$ はループをもたない。□

命題 4.2.2 により $H \setminus X^{p,q}$ がループをもたない条件は補題 4.1.3 よりは詳しくなった。命題 4.2.2 は $p \not\equiv 3 \pmod{8}$ に限定すると、さらに系 4.2.4 となる。そのために補題 4.2.3 を示しておく。

補題 4.2.3. $p \not\equiv 3 \pmod{8}$ のとき、 p は 3 つの奇数の平方の和でかけない。このとき $q > 2\sqrt{p}$ ならば、すべての $s \in S_{p,q}$ は $s^2 \neq 1$ である。

証明. 背理法で示す。 a_1, a_2, a_3 を奇数とし、 $p = a_1^2 + a_2^2 + a_3^2$ をみたすとする。このとき、

$$\begin{aligned}
p &= a_1^2 + a_2^2 + a_3^2 \\
&\equiv 1 + 1 + 1 \pmod{8} \\
&\equiv 3 \pmod{8}
\end{aligned}$$

となり矛盾する。よって、 $p \not\equiv 3 \pmod{8}$ のとき、 p は 3 つの奇数の平方の和でかけない。

S_p の定義より、 p が 3 つの奇数の和でかけるときだけ、 $\beta_j \in S_p$ ($b_0 = 0$) が存在する。 $\varphi \circ \psi_q \circ \tau_q(\beta_j) = s$ とすると、このような s だけ $s^2 = 1$ となる。もし $\alpha_i \in S_p$ ($a_0 \neq 0$) がこのような s を行き先とすると、 $s^2 = 1$ となることは $\varphi \circ \psi_q \circ \tau_q$ が補題 3.2.1 の証明より単射であったことと矛盾する。以上から、 $p \not\equiv 3 \pmod{8}$ のとき $q > 2\sqrt{p}$ ならば、すべての $s \in S_{p,q}$ は $s^2 \neq 1$ である。□

系 4.2.4. $q > 2\sqrt{p}$ とする。 m を任意の $h \in H$ に対し、 $h^m = 1$ となる最小の自然数とする。 $X^{p,q}$ の girth が m より大きく、 $p \not\equiv 3 \pmod{8}$ のとき、 $H \setminus X^{p,q}$ はループをもたない。

証明. 補題 4.2.3 より、 $p \not\equiv 3 \pmod{8}$ のとき、すべての $s \in S_{p,q}$ は $s^2 \neq 1$ であるから、命題 4.2.2 の証明より $H \setminus X^{p,q}$ はループをもたない。□

命題 4.1.4 と系 4.2.4 から、 $q > 2\sqrt{p}$ で m を任意の $h \in H$ に対し $h^m = 1$ となる最小の自然数としたとき、 $X^{p,q}$ の girth が $2m$ より大きく、 $p \not\equiv 3 \pmod{8}$ のとき、 $H \setminus X^{p,q}$ はループをもたず、単純である。しかし、注意 4.4.3 の後より $p \equiv 3 \pmod{8}$ のときでも $H \setminus X^{p,q}$ がループをもたない H が存在することがわかる。

4.3 $H \backslash X^{p,q}$ の固有値の評価

次により, 新たに $H \backslash X^{p,q}$ もラマヌジャングラフであることがわかる.

定理 4.3.1. p と q を異なる奇素数とする. $H \backslash X^{p,q}$ はラマヌジャングラフである.

証明. $X^{p,q}$ はラマヌジャングラフであった. $X^{p,q}$ の隣接行列は命題 3.1.3 より, $\left(\frac{p}{q}\right) = 1$ のときは $A =$

$\sum_{s \in S_{p,q}} \rho_{\text{PSL}_2(q)}(s)$, $\left(\frac{p}{q}\right) = -1$ のときは $A = \sum_{s \in S_{p,q}} \rho_{\text{PGL}_2(q)}(s)$ であり, $X^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入っていた.

$\left(\frac{p}{q}\right) = 1$ で $H \subset \text{PSL}_2(q)$ または $\left(\frac{p}{q}\right) = -1$ とする. $\pi : X^{p,q} \rightarrow H \backslash X^{p,q}$ とし, $f \in l^2(H \backslash X^{p,q})$ とすると $f \circ \pi \in l^2(X^{p,q})$ となり, $f \circ \pi(x) = f \circ \pi(hx)$ ($h \in H$) となる. 逆に, $g \in l^2(X^{p,q})$ に対し, すべての $x \in X^{p,q}, h \in H$ が $g(x) = g(hx)$ となるならば, ある $f \in l^2(H \backslash X^{p,q})$ により $g = f \circ \pi$ となる. $W_1 = \{g \in l^2(X^{p,q}) : g(x) = g(hx), x \in X^{p,q}, h \in H\} \simeq l^2(H \backslash X^{p,q})$ とすると, $W_1 \subset l^2(X^{p,q})$ となる. $s \in S_{p,q}$ に対し, $g(x) \in W_1$ ならば $g(xs) \in W_1$ である. W_1 は A -不変なので $H \backslash X^{p,q}$ の固有値は $X^{p,q}$ の固有値の一部となる. すなわち, $H \backslash X^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入る.

$\left(\frac{p}{q}\right) = 1$ で $H \not\subset \text{PSL}_2(q)$ とする. $X^{p,q} = \mathcal{G}(\text{PSL}_2(q), S_{p,q})$ と $X'^{p,q} = \mathcal{G}(g\text{PSL}_2(q), S_{p,q})$ ($g \in \text{PGL}_2(q), g \notin \text{PSL}_2(q)$) は同型であるので, 隣接行列は同じである. このとき $X^{p,q}$ と $X'^{p,q}$ の隣接行列を A とすると, グラフ $X''^{p,q} = \mathcal{G}(\text{PSL}_2(q) \cup g\text{PSL}_2(q), S_{p,q}) = \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ の隣接行列は $\begin{pmatrix} A & O \\ O & A \end{pmatrix}$ となる. これから, $X''^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入り, 他の場合と同様に考えると $l^2(H \backslash X^{p,q}) \subset l^2(X''^{p,q})$ がわかるので $H \backslash X^{p,q}$ の自明でない固有値はラマヌジャンの範囲 $[-2\sqrt{p}, 2\sqrt{p}]$ に入る. また命題 4.1.2 より $H \backslash X^{p,q}$ は連結である.

以上から $H \backslash X^{p,q}$ はラマヌジャングラフである. □

4.4 $H \backslash X^{p,q}$ の girth と彩色数

まず, グラフ $H \backslash X^{p,q}$ の girth の下限を求める.

定理 4.4.1. グラフ $H \backslash X^{p,q}$ がループがなく単純とし, t を H の元の位数の最大値とする. このとき, $g(H \backslash X^{p,q}) \geq \frac{g(X^{p,q})}{t}$ となる.

証明. 簡単のため $g(H \backslash X^{p,q}) = g$ とする. 仮定より $g \geq 3$ である.

$\left(\frac{p}{q}\right) = 1$ で $H \subset \text{PSL}_2(q)$, または $\left(\frac{p}{q}\right) = -1$ とする. $Hx_0, Hx_1, \dots, Hx_{g-1}, Hx_g = Hx_0$ を $H \backslash X^{p,q}$ での長さ g の閉路の頂点とする. $i \neq j (1 \leq i, j \leq g)$ のとき $Hx_i \neq Hx_j$ であり, 特に $Hx_1 \neq Hx_{g-1}$ である. $H \backslash X^{p,q}$ はケーリーグラフであるから, $s_1, s_2, \dots, s_g \in S_{p,q}$ があり

$$Hx_i = Hx_0 s_1 s_2 \cdots s_i \quad (1 \leq i \leq g)$$

とできる. 特に $Hx_g = Hx_0 s_1 s_2 \cdots s_g = Hx_0$ となるので, $h \in H$ があり

$$h x_0 s_1 s_2 \cdots s_g = x_0$$

となる．仮定より $h^r = 1$ となる自然数 $r \leq t$ が存在する．このとき

$$\begin{aligned} x_0 &= hx_0s_1s_2 \cdots s_g = h(hx_0s_1s_2 \cdots s_g)s_1s_2 \cdots s_g \\ &= h^2x_0s_1s_2 \cdots s_gs_1s_2 \cdots s_g = h^2(hx_0s_1s_2 \cdots s_g)s_1s_2 \cdots s_gs_1s_2 \cdots s_g \\ &= \cdots \\ &= h^rx_0(s_1s_2 \cdots s_g)^r \end{aligned}$$

となる． $h^r = 1$ であるので

$$1 = (s_1s_2 \cdots s_g)^r$$

となる．今， $s_g \neq s_1^{-1}$ である．もし $s_g = s_1^{-1}$ ならば

$$\begin{aligned} Hx_0s_1s_2 \cdots s_{g-1}s_g &= Hx_0, \\ Hx_0s_1s_2 \cdots s_{g-1}s_1^{-1} &= Hx_0, \\ Hx_0s_1s_2 \cdots s_{g-1} &= Hx_0s_1, \\ Hx_{g-1} &= Hx_1 \end{aligned}$$

となり矛盾する．よって

$$\begin{aligned} g(X^{p,q}) &\leq g(H \backslash X^{p,q}) \cdot r \\ &\leq g(H \backslash X^{p,q}) \cdot t \end{aligned}$$

となる．すなわち

$$g(H \backslash X^{p,q}) \geq \frac{g(X^{p,q})}{t}$$

となる．

$\left(\frac{p}{q}\right) = 1$ で $H \notin \text{PSL}_2(q)$ とする．このとき， $S_{p,q} \subset \text{PSL}_2(q)$ であるので $s \in S_{p,q}$ とすると，すべての $x \in \text{PSL}_2(q)$ に対し $xs \in \text{PSL}_2(q)$ となり，すべての $x' \in g\text{PSL}_2(q)$ ($g \in \text{PGL}_2(q), g \notin \text{PSL}_2(q)$) は $x's \in g\text{PSL}_2(q)$ となる．これから， $Hx_0, Hx_1, \dots, Hx_{g-1}, Hx_g = Hx_0$ を $H \backslash X^{p,q}$ での長さ $g(H \backslash X^{p,q})$ の閉路の頂点とすると， $x_0, x_1, \dots, x_g \in \text{PSL}_2(q)$ か $x_0, x_1, \dots, x_g \in g\text{PSL}_2(q)$ のどちらか一方とできる．よって，他の場合と同様に考えると

$$g(H \backslash X^{p,q}) \geq \frac{g(X^{p,q})}{t}$$

となる． □

$X^{p,q}$ は $\left(\frac{p}{q}\right) = 1$ のときは 2 彩色可能でなかったのに，明らかに $\left(\frac{p}{q}\right) = 1$ のときは $H \backslash X^{p,q}$ も 2 彩色可能でない．次の定理により $\left(\frac{p}{q}\right) = -1$ のときも $H \backslash X^{p,q}$ には 2 彩色可能でないものが存在することがわかる．

定理 4.4.2. $\left(\frac{p}{q}\right) = -1$ とする． $H \notin \text{PSL}_2(q)$ のとき， $H \backslash X^{p,q}$ は 2 彩色可能でない．

証明. $\left(\frac{p}{q}\right) = -1$ のとき $X^{p,q}$ は 2 彩色可能であった．命題 3.1.2(d) より， $x \in \text{PGL}_2(q)$ に対し $\chi(x) = \left(\frac{\det x}{q}\right)$ と定義すると， $x \in \text{PSL}_2(q)$ のとき $\chi(x) = \left(\frac{\det x}{q}\right) = 1$ ， $x' \in g\text{PSL}_2(q)$ ($g \in \text{PGL}_2(q), g \notin$

$\mathrm{PSL}_2(q)$ のとき $\chi(x') = \left(\frac{\det x'}{q}\right) = -1$ より, $X^{p,q}$ は $\mathrm{PSL}_2(q)$ と $\mathrm{PGL}_2(q)$ で 2 色にわかれている. また 2 彩色可能であることは, 明らかにすべての閉路の頂点数が偶数であることと同値である.

$H \not\subset \mathrm{PSL}_2(q)$ より $hx = x'$ となるような $h \in H, x \in \mathrm{PSL}_2(q), x' \in g\mathrm{PSL}_2(q)$ が存在する. このよう
な x, x' を含む $X^{p,q}$ の閉路を考える. $x_0, x_1, \dots, x_{2u-1}, x_{2u} = x_0$ を $X^{p,q}$ での長さ $2u$ の閉路の頂点とす
る. ただし, $x_0, x_2, \dots, x_{2u} \in \mathrm{PSL}_2(q), x_1, x_3, \dots, x_{2u-1} \in g\mathrm{PSL}_2(q)$ とし, ある $h \in H$ により $hx_{2i} =$
 x_{2j-1} ($0 \leq i < j \leq u$) となるとする. 必要ならば閉路の番号付けを逆向きにすることで, $i < j$ としても
一般性を失わない. このとき, $Hx_0, Hx_1, \dots, Hx_{2i-1}, Hx_{2i} = Hx_{2j-1}, Hx_{2j}, \dots, Hx_{2u-1}, Hx_{2u} = Hx_0$
を考えると, これは $H \setminus X^{p,q}$ の閉路の頂点である. 頂点数は $2u - (2j - 1 - 2i) = 2(u + i - j) + 1$ となり,
奇数である. 以上から $H \setminus X^{p,q}$ は 2 彩色可能でない. \square

$\left(\frac{p}{q}\right) = -1$ で $H \subset \mathrm{PSL}_2(q)$ のときは $H \setminus X^{p,q}$ は 2 彩色可能のままである. なぜならすべての $h \in H, x \in$
 $\mathrm{PSL}_2(q)$ に対し, $hx \in \mathrm{PSL}_2(q)$ となるからである.

注意 4.4.3. Beauville[1] は無限に多くの q に対しての $\mathrm{PGL}_2(q)$ に共通に入る有限部分群のリスト, およ
び共役類を与えている. それは次の通りである: q を奇素数とする. C_r を位数 r の巡回群, D_{2r} を位数 $2r$
の二面体群とする.

$\mathrm{PSL}_2(q)$ ($q \geq 3$) すべてに共通の部分群は以下の通りである;

群	$\mathrm{PGL}_2(q)$ での 共役類の個数	部分群の共役類の代表元	$\mathrm{PSL}_2(q)$ の部分群のとき S , そうでないとき G
C_2	2	$\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$	S
		$\langle \begin{pmatrix} 0 & x \\ 1 & 0 \end{pmatrix} \rangle (-x \notin \mathbb{F}_q^{\times 2})$	G
C_3	1	$\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	S
C_4	1	$\langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	$S \quad (q \equiv \pm 1 \pmod{8})$
			$G \quad (q \equiv 3, 5 \pmod{8})$
$C_2 \times C_2$	2	$\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix} \rangle (x^2 + y^2 + 1 = 0)$	S
		$\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix} \rangle (-x^2 - y^2 \notin \mathbb{F}_q^{\times 2})$	G
D_6 ($q = 3$)	1	$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	G
D_6 ($q > 3$)	2	$\langle \begin{pmatrix} -x-y & x-y \\ 2x & x+y \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle (3x^2 + y^2 + 4 = 0)$	S
		$\langle \begin{pmatrix} -x-y & x-y \\ 2x & x+y \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle (-3x^2 - y^2 \notin \mathbb{F}_q^{\times 2})$	G
D_8 ($q \equiv \pm 1(8)$)	2	$\langle \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle (x^2 + y^2 + 1 = 0)$	S
		$\langle \begin{pmatrix} x & -y \\ -y & -x \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle (-x^2 - y^2 \notin \mathbb{F}_q^{\times 2})$	G
D_8 ($q \equiv 3, 5(8)$)	1	$\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	G
$\mathrm{Alt}(4)$	1		S
$\mathrm{Sym}(4)$	1		$S \quad (q \equiv \pm 1 \pmod{8})$
			$G \quad (q \equiv 3, 5 \pmod{8})$

$\mathrm{PGL}_2(q)$ ($q \geq 5$) すべてに共通の部分群は上の表と以下の通りである；

群	$\mathrm{PGL}_2(q)$ での 共役類の個数	部分群の共役類の代表元	$\mathrm{PSL}_2(q)$ の部分群のとき S , そうでないとき G
C_6	1	$\langle \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	S ($q \equiv \pm 1 \pmod{12}$) G ($q \equiv 5, 7 \pmod{12}$)
D_{12} ($q \equiv \pm 1 \pmod{12}$)	2	$\langle \begin{pmatrix} x+y & x-y \\ 2x & -x-y \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \rangle (3x^2 + y^2 + 4 = 0)$ $\langle \begin{pmatrix} x+y & x-y \\ 2x & -x-y \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \rangle (-3x^2 - y^2 \notin \mathbb{F}_q^{\times 2})$	S G
D_{12} ($q \equiv 5, 7 \pmod{12}$)	1	$\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix} \rangle$	G

$\mathrm{PGL}_2(q)$ ($q \equiv \pm 1 \pmod{5}$) すべてに共通の部分群は上の 2 つの表と以下の通りである．このとき，条件の q は $\left(\frac{5}{q}\right) = 1$ となる．2 乗して 5 になる元の 1 つを λ_5 と表す；

群	$\mathrm{PGL}_2(q)$ での 共役類の個数	部分群の共役類の代表元	$\mathrm{PSL}_2(q)$ の部分群のとき S , そうでないとき G
C_5	1	$\langle \begin{pmatrix} 1+\lambda_5 & -2 \\ 2 & 2 \end{pmatrix} \rangle$	S
D_{10}	2	$\langle \begin{pmatrix} (-1+\lambda_5)x-2y & (1+\lambda_5)x+(-1+\lambda_5)y \\ 4x & (1-\lambda_5)x+2y \end{pmatrix}, \begin{pmatrix} 1+\lambda_5 & -2 \\ 2 & 2 \end{pmatrix} \rangle ((5+\lambda_5)x^2 + 2y^2 + 8 = 0)$ $\langle \begin{pmatrix} (-1+\lambda_5)x-2y & (1+\lambda_5)x+(-1+\lambda_5)y \\ 4x & (1-\lambda_5)x+2y \end{pmatrix}, \begin{pmatrix} 1+\lambda_5 & -2 \\ 2 & 2 \end{pmatrix} \rangle (-2\{(5+\lambda_5)x^2 + 2y^2\} \notin \mathbb{F}_q^{\times 2})$	S G
$\mathrm{Alt}(5)$	1		S

考える q の下限を大きくすると共通に含まれる部分群は増えていくが，これ以降は C_r , D_{2r} のタイプのものしかない．

$p \equiv 3 \pmod{8}$ で $\left(\frac{p}{q}\right) = -1$ のとき， $H = C_4$ とすると C_4 の位数 2 の元は $\mathrm{PSL}_2(q)$ に入ることから， $g \in \mathrm{PGL}_2(q)$, $g \notin \mathrm{PSL}_2(q)$ とは共役にはならない．特に $S_{p,q} \subset \mathrm{PGL}_2(q)$, $S_{p,q} \cap \mathrm{PSL}_2(q) = \emptyset$ より， $S_{p,q}$ の元と共役にはならない．このとき， $X^{p,q}$ の girth は 4 より大きいので，命題 4.2.2 よりこれは $p \equiv 3 \pmod{8}$ のときに $H \backslash X^{p,q}$ がループをもたない例である．

次の命題より， $H \backslash X^{p,q}$ は H が共役のときはグラフとして同型であることがわかる．

命題 4.4.4. $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \mathrm{PSL}_2(q)$ または $\left(\frac{p}{q}\right) = -1$ のときは $g \in \mathrm{PGL}_2(q)$, $\left(\frac{p}{q}\right) = 1$ で $H \subset \mathrm{PSL}_2(q)$ のときは $g \in \mathrm{PSL}_2(q)$ とする．このとき， $H \backslash X^{p,q}$ と $(gHg^{-1}) \backslash X^{p,q}$ はグラフとして同型である．

証明. $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \mathrm{PSL}_2(q)$ または $\left(\frac{p}{q}\right) = -1$ のときを示す． $\left(\frac{p}{q}\right) = 1$ で $H \subset \mathrm{PSL}_2(q)$ のときも同様である．

(a) まず， $H \backslash \mathcal{G}(\mathrm{PGL}_2(q), S_{p,q})$ と $(gHg^{-1}) \backslash \mathcal{G}(\mathrm{PGL}_2(q), gS_{p,q}g^{-1})$ がグラフとして同型であることを示す． g の共役による写像

$$\begin{aligned} H \backslash \mathrm{PGL}_2(q) &\longrightarrow (gHg^{-1}) \backslash \mathrm{PGL}_2(q) \\ Hx &\longmapsto gHg^{-1}gxg^{-1} (= gHxg^{-1}) \end{aligned}$$

は同型である．この写像はグラフの頂点間に全単射を与える．2 点 $Hx, Hy \in H \backslash \mathrm{PGL}_2(q)$ が $S_{p,q}$ の元の積 $s = s_1 \cdots s_n$ による辺で結ばれている，すなわち $Hxs = Hy$ とする．このとき $gHxsg^{-1} = gHyg^{-1}$

であり、両辺はそれぞれ $gHxsg^{-1} = gHg^{-1}gxg^{-1}gs_1g^{-1}\cdots gs_n g^{-1}$ と $gHyg^{-1} = gHg^{-1}gyg^{-1}$ となる。よって、2 点 $gHg^{-1}gxg^{-1}, gHg^{-1}gyg^{-1} \in (gHg^{-1}) \backslash \text{PGL}_2(q)$ は $gS_{p,q}g^{-1}$ の元の積 $gs_1g^{-1}\cdots gs_n g^{-1}$ による辺で結ばれている。同様に逆もいえるので、対応する頂点は同じように結ばれている。すなわち、 $H \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $(gHg^{-1}) \backslash \mathcal{G}(\text{PGL}_2(q), gS_{p,q}g^{-1})$ はグラフとして同型である。

(b) 次に、 $H \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $H \backslash \mathcal{G}(\text{PGL}_2(q), gS_{p,q}g^{-1})$ がグラフとして同型であることを示す。写像

$$\begin{aligned} H \backslash \text{PGL}_2(q) &\longrightarrow H \backslash \text{PGL}_2(q) \\ Hx &\longmapsto Hxg^{-1} \end{aligned}$$

は同型である。この写像はグラフの頂点間に全単射を与える。2 点 $Hx, Hy \in H \backslash \text{PGL}_2(q)$ が $S_{p,q}$ の元の積 $s = s_1 \cdots s_n$ による辺で結ばれている、すなわち $Hxs = Hy$ とする。このとき $Hxsg^{-1} = Hyg^{-1}$ であり、 $Hxsg^{-1} = Hxg^{-1}gs_1g^{-1}\cdots gs_n g^{-1}$ より、2 点 $Hxg^{-1}, Hyg^{-1} \in H \backslash \text{PGL}_2(q)$ は $gS_{p,q}g^{-1}$ の元の積 $gs_1g^{-1}\cdots gs_n g^{-1}$ による辺で結ばれている。同様に逆もいえるので、対応する頂点は同じように結ばれている。すなわち、 $H \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $H \backslash \mathcal{G}(\text{PGL}_2(q), gS_{p,q}g^{-1})$ はグラフとして同型である。

(a) から $H \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $(gHg^{-1}) \backslash \mathcal{G}(\text{PGL}_2(q), gS_{p,q}g^{-1})$ はグラフとして同型であり、(b) を部分群 gHg^{-1} に用いると $(gHg^{-1}) \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $(gHg^{-1}) \backslash \mathcal{G}(\text{PGL}_2(q), gS_{p,q}g^{-1})$ はグラフとして同型である。よって、 $H \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ と $(gHg^{-1}) \backslash \mathcal{G}(\text{PGL}_2(q), S_{p,q})$ 、すなわち $H \backslash X^{p,q}$ と $(gHg^{-1}) \backslash X^{p,q}$ はグラフとして同型である。□

定理 4.4.5. p, q を奇素数とし、 $q > p^8$ をみたすとする。 H を注意 4.4.3 の群とし、(i) $p \not\equiv 3 \pmod{8}$ 、または (ii) ルジャンドル記号 $\left(\frac{p}{q}\right) = 1$ かつ H の位数 2 の元はどれも $\text{PSL}_2(q)$ に入らない、または (iii) ルジャンドル記号 $\left(\frac{p}{q}\right) = -1$ かつ H の位数 2 の元はどれも $\text{PSL}_2(q)$ に入る、のいずれかをみたすとする。さらに $v = |H|$ 、 m を任意の $h \in H$ に対し $h^m = 1$ となる最小の自然数、 t を H の元の位数の最大値とする。

(Ia) $\left(\frac{p}{q}\right) = 1$ で $H \subset \text{PSL}_2(q)$ とする。 $X^{p,q}$ の girth が $2m$ より大きい、例えば $2\log_p q \geq 2m$

とする。このとき $H \backslash X^{p,q}$ は $\frac{q(q^2-1)}{2v}$ 頂点をもつ、連結で $(p+1)$ -正則なラマヌジャングラフで

$$g(H \backslash X^{p,q}) \geq \frac{2}{t} \log_p q, \quad \chi(H \backslash X^{p,q}) \geq \frac{p+1}{2\sqrt{p}}$$

をみたしている。

(Ib) $\left(\frac{p}{q}\right) = 1$ で $H \not\subset \text{PSL}_2(q)$ とする。 $X^{p,q}$ の girth が $2m$ より大きい、例えば $2\log_p q \geq 2m$

とする。このとき $H \backslash X^{p,q}$ は $\frac{q(q^2-1)}{v}$ 頂点をもつ、連結で $(p+1)$ -正則なラマヌジャングラフで

$$g(H \backslash X^{p,q}) \geq \frac{2}{t} \log_p q, \quad \chi(H \backslash X^{p,q}) \geq \frac{p+1}{2\sqrt{p}}$$

をみたしている。

(IIa) $\left(\frac{p}{q}\right) = -1$ で $H \subset \text{PSL}_2(q)$ とする。 $X^{p,q}$ の girth が $2m$ より大きい、例えば $4\log_p q -$

$\log_p 4 \geq 2m$ とする。このとき $H \backslash X^{p,q}$ は $\frac{q(q^2-1)}{v}$ 頂点をもつ、連結で $(p+1)$ -正則なラマヌジャングラフで

$$g(H \backslash X^{p,q}) \geq \frac{4}{t} \log_p q - \frac{1}{t} \log_p 4, \quad \chi(H \backslash X^{p,q}) = 2$$

をみたしている.

(IIb) $\left(\frac{p}{q}\right) = -1$ で $H \not\subset \text{PSL}_2(q)$ とする. $X^{p,q}$ の girth が $2m$ より大きい, 例えば $4\log_p q - \log_p 4 \geq 2m$ とする. このとき $H \setminus X^{p,q}$ は $\frac{q(q^2-1)}{v}$ 頂点をもつ, 連結で $(p+1)$ -正則な ラマヌジャングラフで

$$g(H \setminus X^{p,q}) \geq \frac{4}{t} \log_p q - \frac{1}{t} \log_p 4, \quad \chi(H \setminus X^{p,q}) \geq \frac{p+1}{2\sqrt{p}}$$

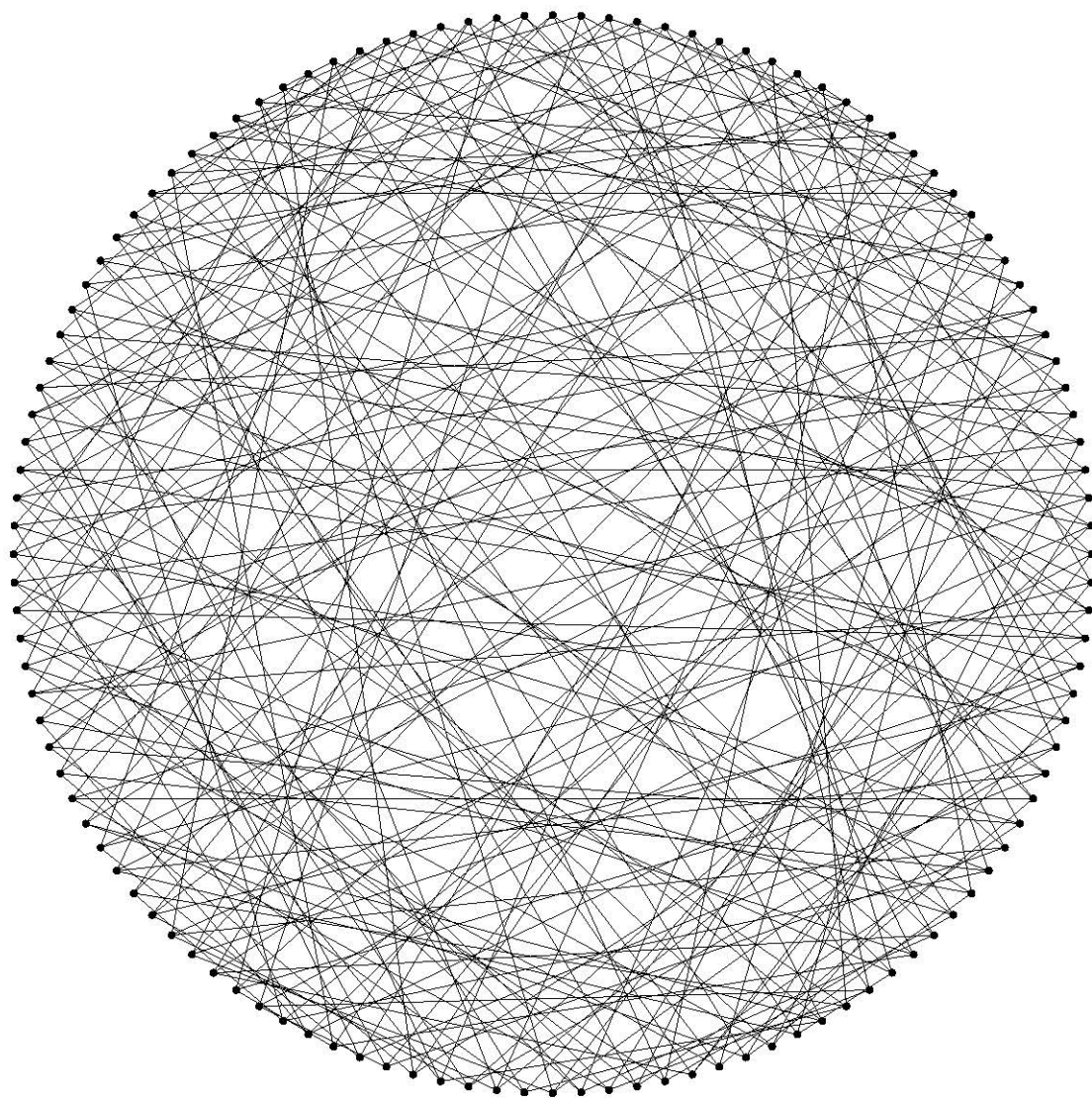
をみたしている.

証明. 条件のとき, $H \setminus X^{p,q}$ がループがなく単純であることは, 命題 4.1.4, 命題 4.2.2, 系 4.2.4, 注意 4.4.3 の後からわかり, 頂点数は定義 4.2.1 と命題 2.5.1 からわかる. $H \setminus X^{p,q}$ が連結で $(p+1)$ -正則であることは定義 4.2.1 とその後からすぐわかり, ラマヌジャングラフであることは定理 4.3.1 からわかる. また, $H \setminus X^{p,q}$ の girth は命題 3.3.4, 定理 3.3.6, 定理 4.4.1 からわかり, 彩色数は定理 4.4.2 とその前後, 系 1.5.4 からわかる. \square

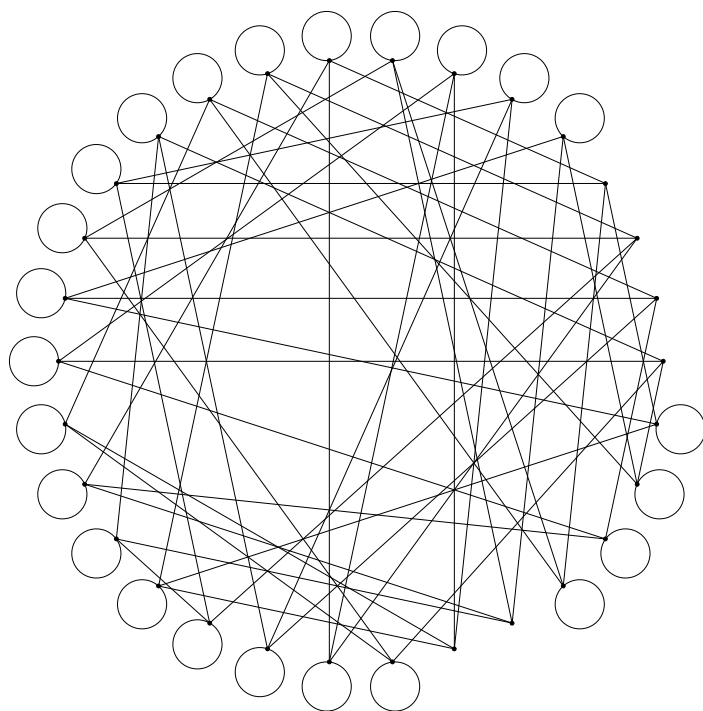
すなわち, $H \setminus X^{p,q}$ は定理 4.4.5 の (Ia), (Ib), (IIb) のとき, 連結なラマヌジャングラフで, p, q を十分大きくとれば大きな girth と大きな彩色数をもつことがわかる.

最後に $X^{p,q}$ と $H \setminus X^{p,q}$ の例をいくつか挙げておく.

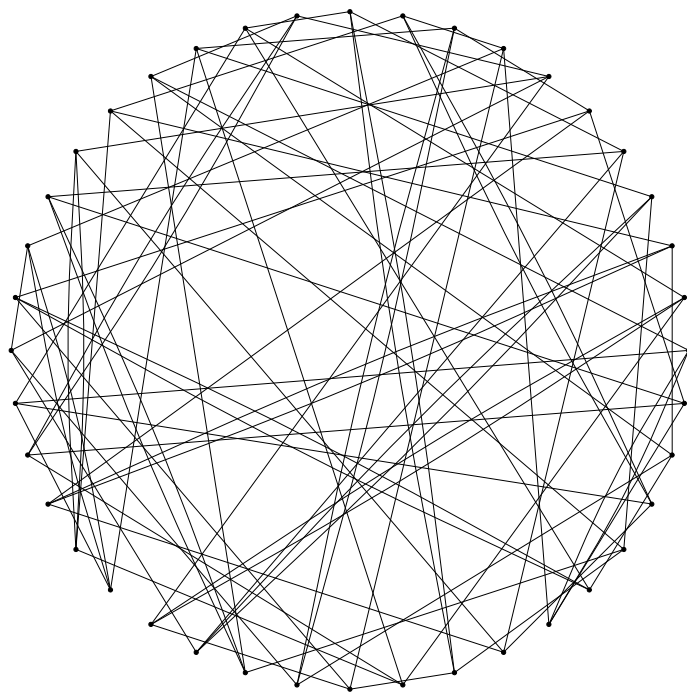
$X^{3,5}$ 頂点数 120 girth 6 2 彩色可能



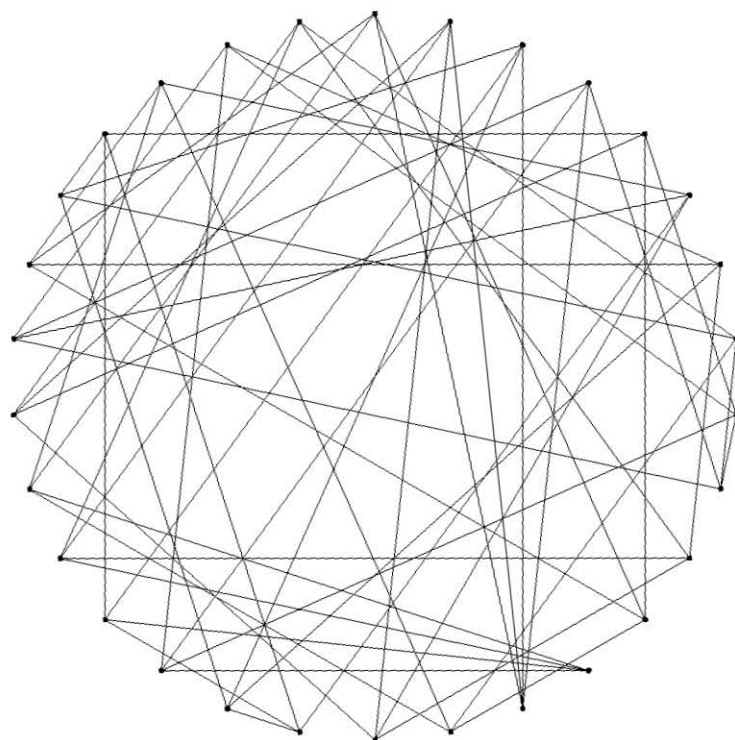
$$H \backslash X^{3,5}, H = C_2 \times C_2 = \left\langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \right\rangle \quad \text{頂点数 } 30 \quad \text{ループあり}$$



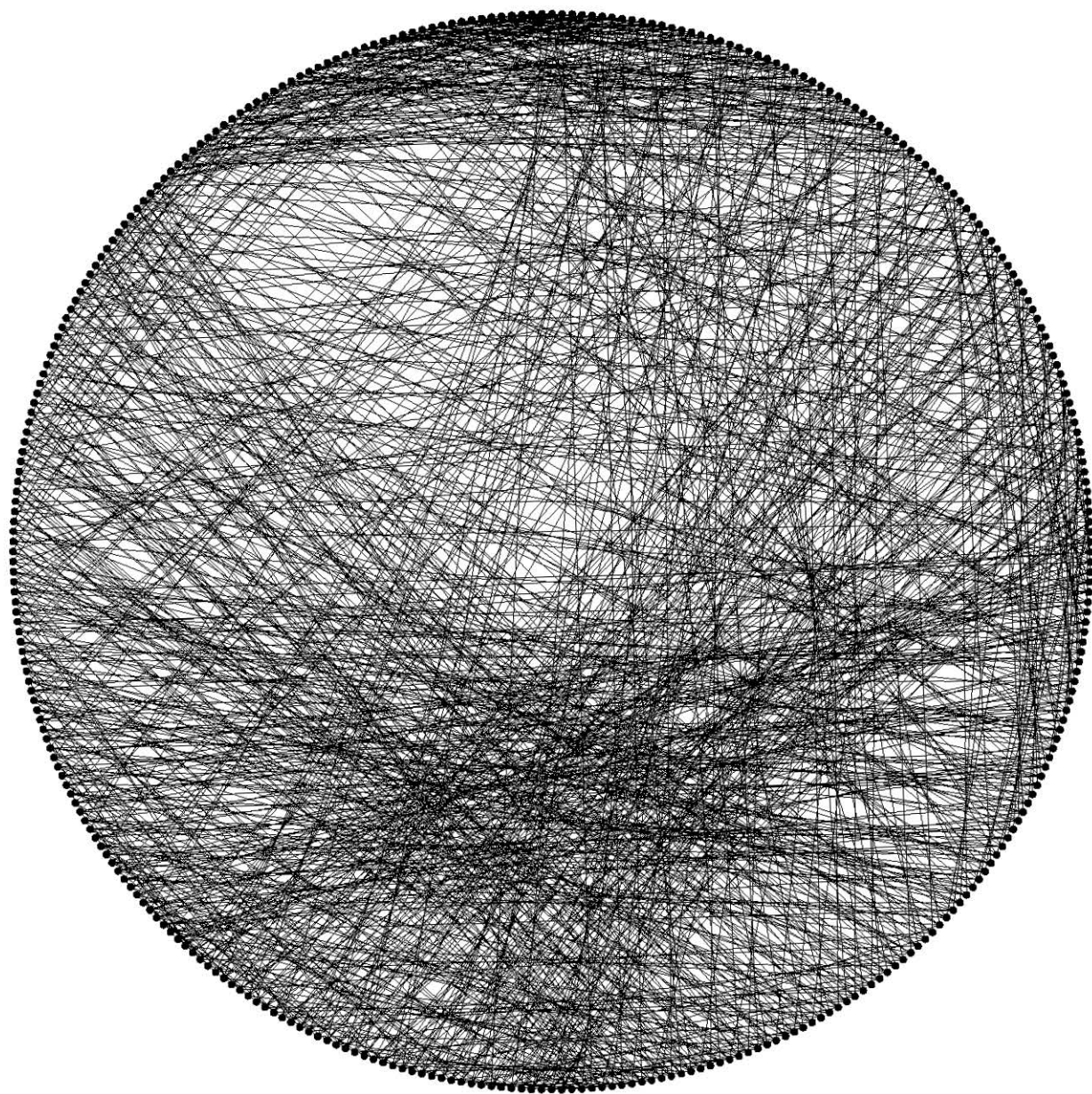
$$H \backslash X^{3,5}, H = C_3 = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle \quad \text{頂点数 } 40 \quad \text{多重辺あり}$$



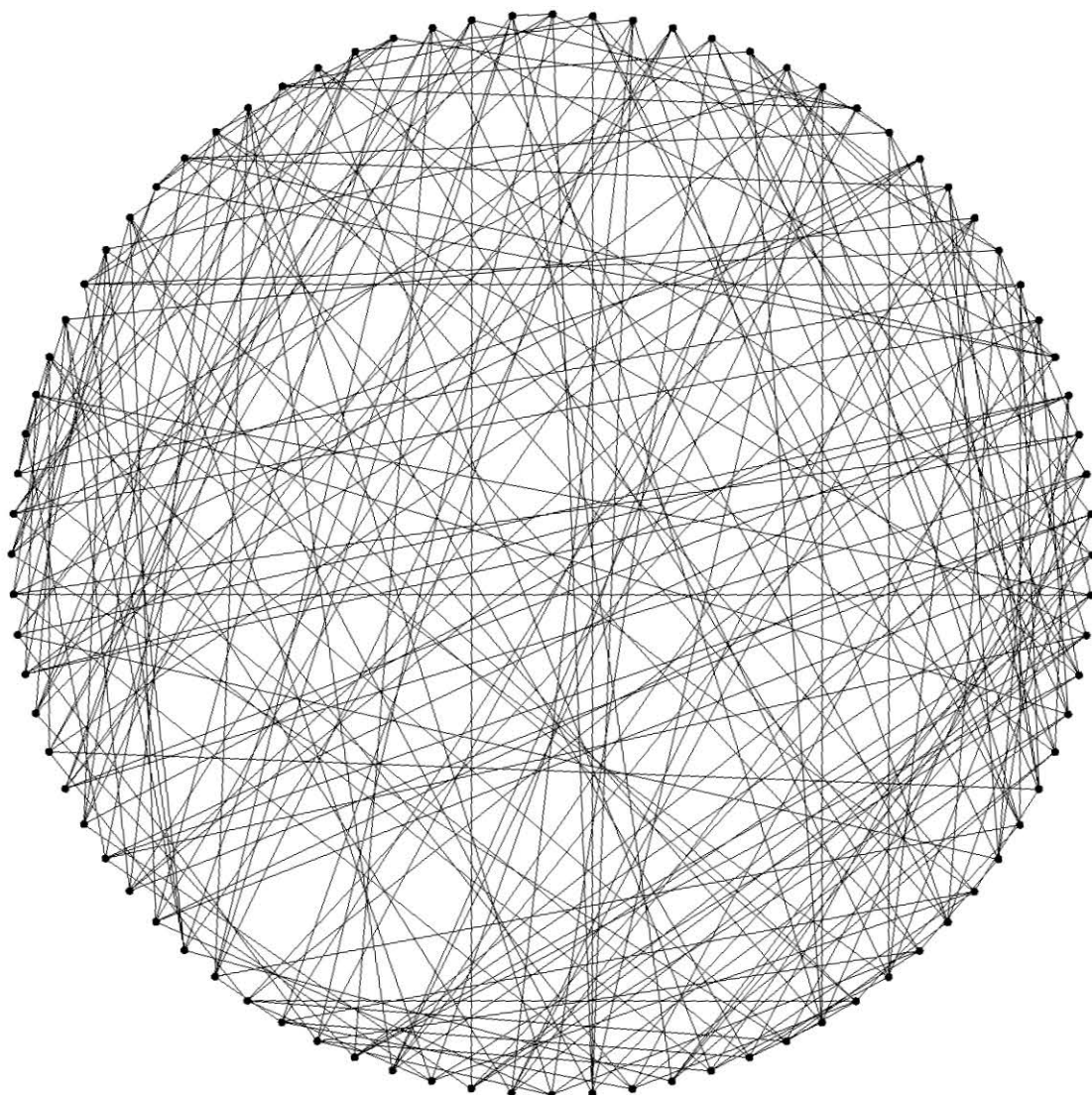
$H \setminus X^{3,5}$, $H = C_4 = \langle \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \rangle$ 頂点数 30 girth 3 2 彩色可能でない



$X^{5,7}$ 頂点数 336 girth 6 2 彩色可能



$H \setminus X^{5,7}$, $H = C_2 \times C_2 = \langle \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \rangle$ 頂点数 84 girth 3 2 彩色可能でない



参考文献

- [1] Arnaud Beauville, *Finite subgroups of $\mathrm{PGL}_2(K)$* , Contemporary Mathematics, 23–29, **522** (2010)
- [2] Guiliana Davidoff, Peter Sarnak and Alain Valette, *Elementary number theory, group theory and Ramanujan graphs*, London Mathematical Society Student Texts **55**, 2003