対称性の数理

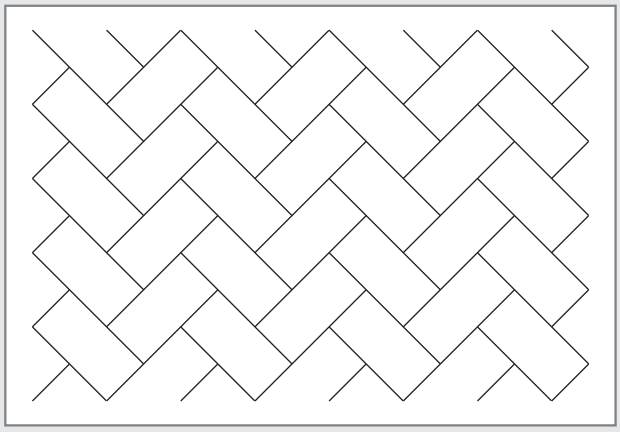
東京理科大学 創域理工学部 数理科学科 准教授 大橋（おおはし） 久範（ひさのり）

■1 はじめに

対称性と聞いて何を思い浮かべますか？ 点対称，線対称，また面対称といった言葉から想像を膨らませると，正多角形や円，正多面体，真上から見た花の形，万華鏡の景色などが思い浮かびます．壁の幾何学模様や，舗装された道路を埋めるタイルを思い出す人もいると思います．後者のように，タイルを敷き詰めた結果生じる規則性も，数学では対称性と呼ばれます．蜂の巣の断面，整然と配列された商品棚など，身の回りには対称性や規則性がたくさんあります**【図 1，図 3】**．

非対称なもの，不規則なものよりも，対称なもの，規則的なもののほうが少し美しく見えることが多いですね．この稿では対称性を定量化する**「群」**という構造を中心に，数学の一部を紹介したいと思います．わからない計算は飛ばして，雰囲気を読んでみてください．

第 2 節では，小学校以来の図形の対称性について見てみます．第 3，4 節では，方程式の対称性を紹介します．図形の対称性は目で見えるのでわかりやすいですが，方程式にも対称性の構造があるというのは 19 世紀の数学者ガロアの発見で，そのアイデアは現代のコンピュータ理論にまで大きな影響を与えています．第 5 節では群の中でも特に「硬い」構造を持つ単純群について，2 つの大きな分類定理を紹介します．



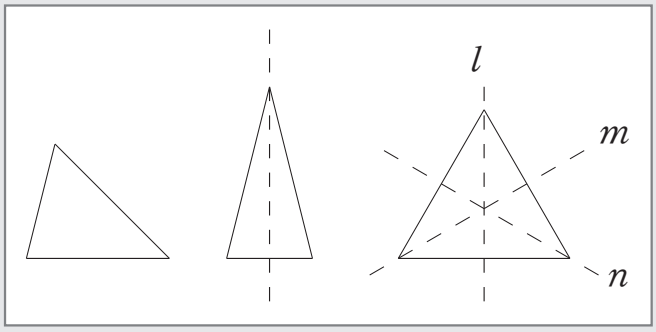
【図 1】檜垣（ひがき）模様

■2 平面図形

小中学校では三角形や円の基本性質を学びます．任意の三角形において 3 つの内角の和は常に 180 度であること，これが二等辺三角形になると 2 つの角の大きさが一致すること，正三角形では全ての角の大きさが一致すること，などなど．実は，三角形のこのような類別は，三角形の対称性による類別に他なりません．

ここで言う対称性とは，平面の合同変換で図形を保つもののことです．**合同変換**とは平面から平面への全単射（点の集合としての一対一対応）で，任意の 2 点間の距離を保つもののことです．平面内の何らかの直線に関する対称移動や，ある点に関する回転移動などが合同変換の例になっています．

【図 2】を見てわかるように，二等辺三角形には対称軸（底辺の垂直二等分線）があります．正三角形においては対称軸が 3 つ存在し，さらに 0 度，120 度，240 度の回転対称性も考えられます．ここで「0 度の回転」は実質的に平面を変換していないのですが，こういうものも「自明な」合同変換としてきちんと数えておくことが重要です．これを踏まえると，正三角形には合計 6 つの，それ以外の二等辺三角形には 2 つの，さらに一般の三角形には（自明なもの）1 つだけの合同変換が作用できることがわかりました．これらの合同変換はまた，合成することができます．図の正三角形で，反時計回りに 120 度回転する合同変換を R，l に関する対称移動の合同変換を L と書くと，



【図 2】三角形の対称性

$R\circ L$（対称移動してから回転）は n に関する対称移動であり，$L\circ R$（回転してから対称移動）は m に関する対称移動となります．どちらも正三角形を保つ合同変換であり，しかも $R\circ L\neq L\circ R$，つまり合成は非可換な二項演算となっています．このような，対称性のなす集合とその上の合成（二項演算）が，群と呼ばれるものの原型です．

定義. 集合 G とその上の二項演算＊が結合法則，単位元の存在，逆元の存在を満たすとき，$(G,*)$ を群という．

集合が含む元の個数を位数と言いました．したがって，正三角形，二等辺三角形，一般の三角形の対称性は位数がそれぞれ 6,2,1 の群となっている，と言えます．

円についても考えてみましょう．正三角形の３つの回転対称性と比べると，円は任意の角度の回転で保たれるため，無限に多くの回転対称性を持ちます．線対称についても，中心を通る任意の直線に関して円は線対称性を持ちます．このように円は正三角形よりも豊富な対称性を持ちます．合同変換を二次正方行列を用いた平面の一次変換として表すと，円の対称性のなす群は次の二次直交群になります．

$$O(2)=\{A:\text{二次正方行列}\mid {}^tAA=E\}$$

これは正三角形のときの有限群とは異なり，滑らかな空間の構造も併せ持つリー群となります．$O(2)$ は非連結な１次元のリー群です．

ここまで図形自身の対称性について調べましたが，これらの図形には規則的な拡張の可能性にも違いがあります．円板だけを用いて平面を敷き詰めることはできませんが，正三角形だけを使って平面を敷き詰めることはできます．

道路にも正三角形や菱形のタイルで敷き詰められている場所が多くあります．用の美という言葉があるように，日常における使いやすさも人間の美的感覚の１つの基準であり，対称性の多さだけで重要性が測られるわけではないのかもしれません．

練習　正三角形ではない二等辺三角形を用いても，平面を敷き詰められることを確かめよ．また，そのように敷き詰めた平面の対称性が一番小さくなるような敷き詰め方を見つけよ．

ユークリッド空間の合同変換のなす離散群（で余コンパクトなもの）は結晶群と呼ばれ，古くからの研究対象です．現代の数学ではユークリッド空間の代わりに種々のリー群や等質空間においても，その合同変換のなす離散群（格子）が研究されています．

■ 3　代数方程式

復習から始めましょう．二次方程式

$$ax^2+bx+c=0 \tag{1}$$

の２つの解は

$$x=\frac{-b\pm\sqrt{b^2-4ac}}{2a} \tag{2}$$

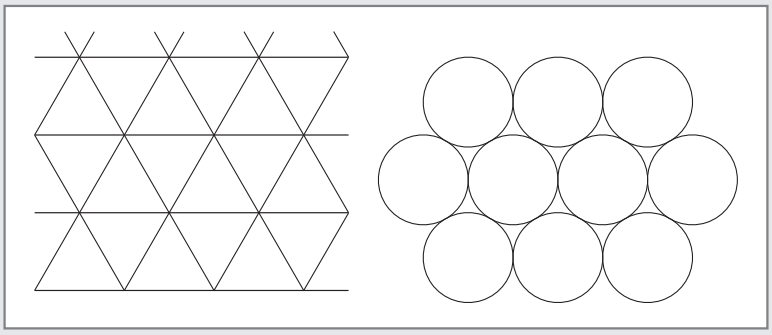
で与えられ，これらを x_1,x_2 とすると

$$x_1+x_2=-\frac{b}{a}\ ,\ x_1x_2=\frac{c}{a}$$

という解と係数の関係が成り立ちます．解それ自身の形は少し複雑に見えますが，それに比して解の対称式は非常に簡単な式で表されるというのがポイントです．また，これを使って，解の差積の平方 Δ を係数で表した式

$$\Delta=(x_1-x_2)^2=\frac{b^2-4ac}{a^2}$$

のことを，(1) の**判別式**と呼びます（皆さんが覚えて



【図 3】円板と正三角形を並べる

いるものと少し違うかもしれませんが，a^2 はひとまず気にしないでいてください）．これは，a,b,c が実数のときには，Δ の値の正・ゼロ・負に応じて解が実数解・重解・虚数解と判別できることからこう呼ばれますが，係数が実数でない場合にも大切な意味を持つ量です．

このあたりの事情は方程式の次数を高くしても同様に成り立ちます．三次方程式で見てみましょう．

$$ax^3+bx^2+cx+d=0 \tag{3}$$

の場合，これは（四則と）べき根で表示できる解を持ち，それは

$$p=\frac{-2b^3+9abc-27a^2d}{54a^3},\qquad q=\frac{27a^2d^2-18abcd+4b^3d+4ac^3-b^2c^2}{108a^4} \tag{4}$$

とおいたとき，$i=1,2,3$ に対して

$$x_i=-\frac{b}{3a}+\zeta^i\sqrt[3]{p+\sqrt{q}}+\zeta^{-i}\sqrt[3]{p-\sqrt{q}},\qquad \text{ただし } \zeta=\frac{-1+\sqrt{-3}}{2} \tag{5}$$

という形をとります．二次方程式の場合よりもずいぶん複雑です．一方，解と係数の関係は

$$x_1+x_2+x_3=-\frac{b}{a},\qquad x_2x_3+x_3x_1+x_1x_2=\frac{c}{a},\qquad x_1x_2x_3=-\frac{d}{a}$$

となり，解自身に比べていかにシンプルかわかります．ここでも，判別式は解の中で根号の中に入っている量を使って

$$\Delta=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2=-108q \tag{6}$$

となることが確認できます．

練習　n 次方程式

$$a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$$

の解 $x_1,\ldots,x_n$ に対する解と係数の関係を書け．

練習　a,b,c,d が実数のとき，三次方程式 (3) の解の様子と Δ の符号がどう対応するだろうか？

この先四次，五次，… と進むにつれて，係数を用いて解を表す公式がどのように複雑化していくかを類推するのは至難の業です．実は，四次方程式の解もべき根を使って表示する公式がありますが（余白が足りないのでここには記しません），五次以上の方程式では一般には四則とべき根で解を表す公式が存在しないという定理が知られています．このように，方程式の解の複雑さを定量的に表す理論は 19 世紀の数学者ガロアにより確立されました．大学の代数学の授業で習う内容ですが，現代ではウェブサイトや動画などでも解説を多く目にするようになりました．興味のある人は見てみてください．

ガロア理論では，方程式の対称性のなす群（ガロア群）の構造が重要な役割を果たします．この対称性とは，解 $x_1,\ldots,x_n$ の置換（全単射による置き換え）のうち，四則演算と両立するようなもののことです．方程式の係数が十分に一般（ランダム）であれば，解と係数の関係が $x_1,\ldots,x_n$ についての対称な連立方程式であることから $x_1,\ldots,x_n$ の役割には差異がなく，置換できるものだということはわかると思います．こうして，一般の n 次方程式のガロア群は n 次対称群 S_n であることがわかります．S_n は偶置換からなる正規部分群 A_n を持ちますが，$n\geq 5$ であれば A_n はこれ以上可換群で分解できない（単純群である）ため，その解がべき根で構成できないことがわかります．

他方で，方程式の係数が特別な値の場合には，その解をべき根で表示できることもあります．そのような特別な係数を探す試みは代数学の 1 つの分野として研究されています．次の節ではべき根とはまた違う観点から，特別なガロア群を持つ方程式について考えてみたいと思います．

練習　方程式 $x^5+750x+3750=0$ の 1 つの解が，$x=-\sqrt[5]{432}-\sqrt[5]{24}+\sqrt[5]{324}-\sqrt[5]{18}$ で与えられることを確かめよ．また，他の 4 つの解の形を類推し，求めてみよ．（ヒント：1 の 5 乗根を使う．）

■ 4　最小ガロア群を持つ多項式

既約 n 次多項式 $f(x)$ のガロア群は n 個の根の集合に推移的に作用するので少なくとも n 個の元を持ちます．ここで等号が成り立つとき，つまりガロア群が位数 n を持つときに，この稿では $f(x)$ **が最小ガロア群を持つ**，ということにしたいと思います．これは，$f(x)$ の最小分解体が 1 つの根だけで（体として）生

成されることと同値です．この場合にはガロア群は具体的な多項式の代入操作によって理解することができます．以下，$f(x)$ は既約なものを考えます．

はじめに，最小ガロア群を持つような多項式がどれくらいあるか考えてみます．前節で説明したように，方程式の係数を一般的にとればそのガロア群は対称群 S_n となり，位数は $n!$，これは大抵の場合に n よりずっと大きくなります．こう見ると最小ガロア群を持つ多項式は極めて特別なものだという印象になります．一方で，任意の有限次ガロア拡大は単拡大で書けること，またその生成元として拡大体の一般的な元を使えることがよく知られていますので，そのような生成元の最小多項式は最小ガロア群を持つことになります．つまり，最小ガロア群を持つ多項式はありふれています．これらの推論はどちらも正しいですが，計算量の観点から見て，ここでの感覚は前者を持ってくれると良いと思います．ガロア拡大の一般の生成元の最小多項式が，印象に残るような簡潔な式になることはあまり期待できません．

最小ガロア群を持つ方程式を実際に探しましょう．まず，前節の二次方程式 (1) の場合は，既約であれば常に最小ガロア群を持ちます（$2!=2$ による）．放物線の軸に関する対称変換

$$x\mapsto -x-\frac{b}{a}$$

を施すと，(1) の左辺は不変，つまり

$$f\left(-x-\frac{b}{a}\right)=f(x)$$

が成り立ち，この変換がガロア群の非自明な元となります．言い換えると，x が (1) の解のとき，もう 1 つの解が $-x-\frac{b}{a}$ で表される，ということです．（$\frac{c}{ax}$ と言っても良いのですが，ここでは x についての多項式となるものを優先します．）

三次方程式 (3) の場合には，最小ガロア群が現れるのはそれが交代群 A_3 となるとき，つまり (6) に現れる Δ の値が有理数 e の平方 e^2 となるときです．これを満たす三次方程式を探すのはなかなか大変です．適当に a,b,c,d を決め打ちしても，まず $\Delta=e^2$ とはならないでしょう．問題は，$\Delta(a,b,c,d)=e^2$ となるような有理数 a,b,c,d,e をできるだけたくさん求めることです．実は今の場合には，幸運にも完全解を求めることができます．

命題. 有理数 $a\neq 0,b,m,n$ を任意にとる．方程式 $\Delta(a,b,c,d)=e^2$ の有理数解が，次のように c,d,e を決めることで構成できる．

$$ac=-m^2-3n^2+\frac{1}{3}b^2$$

$$a^2d=-\frac{1}{3}(2n+b)(m^2+3n^2)+\frac{1}{27}b^3$$

$$a^3e=2m(m^2+3n^2)$$

逆に，全ての有理数解は適当な a,b,m,n から上の操作により得られる．

例えば $a=1,b=0,m=3/2,n=-1/2$ とおいて計算すると最小ガロア群を持つ多項式 x^3-3x+1 が得られます．$a=1,b=0,m=-9/2,n=1/2$ とすれば $x^3-21x-7$ となります．

練習　命題を次のようにして証明せよ：方程式 $\Delta(a,b,c,d)=e^2$ の分母を払い，左辺をまず d について平方完成し，残りを立方完成する．出来上がった式を鍵となる量 $ac-b^2/3$ で 2 度割り，係数を調整して m,n を見出す．

こうして得られた $f(x)=x^3-3x+1$ の場合に，ガロア群を具体的に見ておきましょう．$x=\alpha$ が 1 つの解のとき，

$$f(x)-f(\alpha)=(x-\alpha)(x^2+\alpha x+\alpha^2-3)$$

となるので，残り 2 つの解は

$$x=\frac{-\alpha\pm\sqrt{-3\alpha^2+12}}{2}$$

となります．ここで，関係式

$$-3\alpha^2+12=(2\alpha^2+\alpha-4)^2$$

を見つけることで，因数分解が

$$(x-\alpha)(x-(\alpha^2-2))(x-(-\alpha^2-\alpha+2))$$

と完成します．f のガロア群は根に対する置換

$$\sigma\colon \alpha\mapsto\alpha^2-2,\tau\colon \alpha\mapsto-\alpha^2-\alpha+2$$

と恒等置換 id からなり，$\sigma^2=\tau,\sigma^3=\mathrm{id}$ が成り立つことを確認してみてください．

命題で与えられる，他の三次方程式に対しても同様にガロア群を具体的な式で表すことができます．一般的に行おうとすると，計算量はなかなかのものです．興味のある人は，具体例をやってみることをお勧めし

ます．いくつかの例を下の練習に挙げておきます．

問題　四次以上の方程式で，最小ガロア群を持つ条件を具体的に書き下せ．

一般的に計算するのは大変だと思いますので，特別な形の多項式から考えてみるのが良いかもしれません．よく使われるのは x^n+ax+b という形をした三項式（英語では trinomial）ですが，もっと簡単にした二項式 x^n+b や，別の三項式 x^n+ax^m+b なども考えられます．位数 4 の群が 2 種類あることから，解もおそらく 2 系列存在することになります．

最小ガロア群が現れる方程式の別の系列として，円分多項式 $\Phi_n(x)$ が挙げられます．これは 1 の原始 n 乗根（n 乗根のうち，n 乗してはじめて 1 になる複素数）のみを解とする，次数 $\varphi(n)$ の多項式（φ はオイラーの totient 関数）で，

$$\Phi_5(x)=x^4+x^3+x^2+x+1,$$
$$\Phi_8(x)=x^4+1,$$

などが挙げられます．この場合のガロア群は $\varphi(n)$ 個の変換

$$x\mapsto x^m\ (m \text{ は } n \text{ と互いに素})$$

で与えられ，ガロア群は環 $\mathbb{Z}/n\mathbb{Z}$ の単元群になります．これらの最小分解体（円分体）の部分体を考えることで，可換であるような最小ガロア群を持つ多項式がたくさん構成できます．

練習　(1) $x^3-21x+28=0$ の 1 つの解を α とするとき，$(\alpha^2+2\alpha-28)^2=-3\alpha^2+84$ を確認し，他の 2 つの解 β,γ を α で表せ．ガロア群の元となる置換 $\sigma\colon \alpha\mapsto\beta,\tau\colon \alpha\mapsto\gamma$ に対して，$\sigma^2=\tau,\sigma^3=\mathrm{id}$ が成り立つことを確認せよ．
(2) $x^3-7x+7=0$ の 1 つの解を α とするとき，他の解を α を使って表し，ガロア群の元を書き下せ．
(3) $x^4-70x^2-120x+445=0$ の 1 つの解を α とするとき，この方程式のガロア群は

$$\sigma\colon \alpha\mapsto\frac{-\alpha^2+2\alpha+35}{4}$$

で生成される群になることを確認せよ．
(4) $x^6+3=0$ の一つの解を α とするとき，この方程式のガロア群は

$$\alpha\mapsto-\alpha,\alpha\mapsto\frac{\alpha+\alpha^4}{2}$$

で生成される群になることを示せ．ガロア群はどんな群か？

問題　最小ガロア群を持つような多項式で，項の数が少ないものを見つけよ．特に，円分多項式と直接関係しないようなもの，ガロア群が非可換になるものをたくさん作ることができるだろうか？

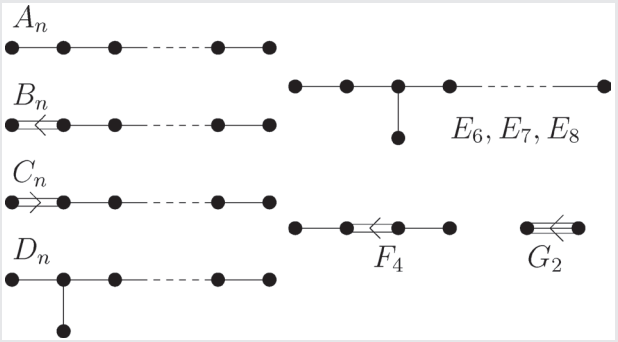
■ 5　単純群

対称群 S_n の中の交代群 A_n のように，ほかの群への準同型写像の核となるような部分群のことを正規部分群というのでした．正規部分群が自明なもの，つまり単位群と自分自身しかないような群を単純群と呼びます．単純群は群の構成要素としての位置づけが単純ではあるものの，複雑で繊細な構造を持っています．それでも，調べ続けることで人間が全体像を理解していけるというのがその魅力になっています．最後に，2 種類の単純群の分類定理を紹介します．

まずは幾何学的な対象である単純リー群の分類定理を紹介します．リー群とは行列群に代表される，可微分（多様体）構造を持った群のことで，群であると同時に豊富な幾何構造を持ちます．例えば，リー群 G の各点での接空間は正則表現（平行移動）により自然に同一視され，不変ベクトル場の全体とも対応します．これにより，接空間は括弧積 $[X,Y]$ の構造を持ち，これは G のリー環と呼ばれます．単純リー群のリー環は非自明なイデアルを持たないという意味で単純リー環になり，単純リー環はそのカルタン部分環の作用により定義されるルート系から決まります．ルート系の性質は右のページに挙げるディンキン図形に集約されます．このようにして得られる単純リー群の分類（20 世紀初頭）は，数学における最も美しい定理の 1 つと言われています．ここでは簡単のため，複素数体上のリー群を考え，表では，単純リー群の「同種」類を挙げています．

定理. 単純リー群とそのディンキン図形は以下の通りに分類される．ここで，ディンキン図形の頂点数は，ルート系の記号の添え字 n に等しい（階数と呼ばれる）．A 型から D 型は無限系列で，古典型と呼ばれる．E 型から G 型は合わせて 5 つしかなく，例外型と呼ばれる．

		構成	複素次元
A_n	$n \geq 1$	$\mathrm{SL}(n+1,\mathbb{C})$	$n(n+2)$
B_n	$n \geq 2$	$\mathrm{SO}(2n+1,\mathbb{C})$	$n(2n+1)$
C_n	$n \geq 3$	$\mathrm{Sp}(2n,\mathbb{C})$	$n(2n+1)$
D_n	$n \geq 4$	$\mathrm{SO}(2n,\mathbb{C})$	$n(2n-1)$
E_n	$6,7,8$		$78,133,248$
F_4		（アルバート代数）	52
G_2		（八元数体）	14



複素単純リー群に続いて，一般の体上の単純リー群（代数群）が 20 世紀中ごろには分類されました．その後，抽象的な有限群論の発展により，幾何構造を持たない有限単純群の分類が潮流となり，1981 年には有限単純群の分類定理が発表されました．

定理. 有限単純群は，次の（i)—(iv）のどれかに現れるものと同型である．

（i）素数位数の巡回群 C_p,p=2,3,5,7,…
（ii）交代群 A_n,n=5,6,7,…
(iii）リー型の単純群，つまり有限体上の単純リー群の有理点から作られる群とその亜種
(iv）26 個の散在型単純群

26 個の散在型単純群はさらに，Mathieu 群 M_{24} に含まれる第一世代，Conway 群 Co_1 に含まれる第二世代，モンスター群 $\mathbb{M}$ に含まれる第三世代とその他に分類されます．3 つの世代の群をまとめて happy family と呼ぶ人もいます．3 つの世代に共通して現れる 24 次元という数字は，今なお神秘的で，数学研究者の興味をひいています．モンスター群はこの分類の中ではじめて認識された巨大な対象で，その位数は

$$|\mathbb{M}| = 808,017,424,794,512,875,886,459,904,$$
$$961,710,757,005,754,368,000,000,000$$

にもなります．オーダーでは 10^{53} であり，アボガドロ定数やプランク定数（の逆数）よりも大きく，単独で意味のある最大の数字の 1 つです．この群を行列で表示するには，196,883 次の正方行列が必要です．

これらの群は，その位置づけが確立された後，他分野との密接な関係も浮かび上がってきていて，興味が持たれています．Mathieu 群と Conway 群は代数幾何学に現れる特別な多様体，$K3$ 曲面やシンプレクティック多様体の理論と深い関係を持っています．モンスター群に対しては，ムーンシャイン現象という楕円関数との不思議な関係が予想され，Borcherds が頂点作用素代数を用いてこれを証明してフィールズ賞を受賞しました．直近のフィールズ賞受賞者の Viazovska は，一般次元のユークリッド空間において中身の詰まった単位球をできるだけ密に置くとき，最良となる置き方は何かという球充塡問題を 8 次元と 24 次元で解決しました．これらの次元でのみ問題が解決されていることの背景には，上で出てきた例外 E_8 型単純リー群や散在型の Conway 群があります．

問題　単純群が惹起する数学的現象を探せ．