ミシマ社 藤原辰史/伊原康隆対談 **Manabu-toha No18**/伊原原稿の補足

このファイルは補足というより補充で、項目番号も本文での番号にそっています。

(1) 本文の、店と品目による値段の比較に関する話の補足です。この数学的な内容は理系では大学 1 、 2 年で学習する「線形代数」という科目のテーマですが、一応述べておきましょう。はて、線形代数の授業でこう教わったかなあ？

一般に店の個数が $m$ で品目の個数が $n$ の場合でも、この種の関係性の有無は「行列の階数」の言葉で表現されます。任意の行列（$m$ 行 $n$ 列とする）が与えられると、その行ベクトルの中で 1 次独立なものの個数と列ベクトルの中で 1 次独立なものの個数とが一致する、という命題が成り立ち、その等しい個数を行列の「階数」とよびます。店は $1 \leq i \leq m$、品目は $1 \leq j \leq n$ と番号づけられているとし、$i$ 店での $j$ の値段を $r_{ij}$ と書くとき、行列

$$R = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \cdots\cdots\cdots\cdots & & \\ r_{m1} & \cdots & r_{mn} \end{pmatrix}$$

の階数が注目です（$r_{ij}$ すべてが 0 でない限り階数は 1 以上)。そして「行列 $R$ の階数が 1 」、「店だけで決まる数 $p_i$、品目だけで決まる数 $q_j$ があって、各 $r_{ij}$ は $= p_i q_j$ と分解する」、「任意の 2 次小行列式は 0」、の 3 つは同値な命題です。 3 つ目の命題は、任意に $i$ 店と $k$ 店、 $j$ 品と $l$ 品を選んだとき、それらと対応する小行列式である

$$r_{ij} r_{kl} - r_{il} r_{kj} = 0$$

が成り立つ、ということですから、本文の $m = n = 2$ の場合の一般化です。階数の小ささや、概数でいうとこれら小行列式の絶対値の小ささは

「画一化の指標」

として注視しないとつまらない社会になってしまいそうですね。この稿を推敲している段階で気がついたことですが追加しました。

(2-1) 回転、回転群という言葉を本文で用いましたが、本来の用語は、自己同型射、自己同型群です。とくに幾何学では、回転は自己同型射の一部ですから紛らわしい。それで数学では使いません。本文では（幾何的対象は出てこないので）イメージ重視で「回転」とよびました。

(3-1) 群の話に入る前に、数学での慣用記号を一つだけ説明しましょう。まず $g \in G$ とは、$g$ は集合 $G$ の元（要素）という意味です。また $\{g \in G;\ \cdots\}$ と書いたら $\cdots$ の中身は $g$ が満たすべき要件のことです。

数学で「群」といえば動的な対象の代表です。高校数学でも動的な対象として、合同変換（幾何）

とか「関数」（解析）が登場しますが、後者も（もとは function ＝機能、なのに）数の一種のような和訳でよばれてしまっています。動かしてみるということを表現する日本語がどうも乏しいですね。

群の定義

集合 $G$ が群 (group) であるとは、任意 $a, b \in G$ に対してその積 $ab \in G$ が定まり、次の性質が満たされること。

(i) 任意の $a, b, c \in G$ に対して $(ab)c = a(bc)$、（$ab$ に $c$ を掛けても $a$ に $bc$ を掛けても同じ）

(ii) 次の条件をみたす元 $e \in G$ がただ 1 つ存在する「任意の $a \in G$ に対して $ae = ea = a$」。
この元 $e$ を $G$ の単位元とよび、しばしば 1 と記す。

(iii) 任意の $a \in G$ に対して、「$aa' = a'a = e$ を満たす $a' \in G$ がただ一つ存在」。
$a$ に依存して唯 1 つ定まるこの元を $a$ の逆元とよび $a^{-1}$ と記す。

(3-2) 群らしい群

何といってもまずは幾何学における変換群でしょう。必要に応じで新種の空間をいろいろ考える数学では、「空間」とその「許される変換群」とは切り離せない「対」をなしています。ユークリッド幾何学での「平面」も「合同変換、相似変換とは何か」を問うことから始まっています。これらの変換は、変換の合成に関して群をつくっていて、本来の群論の発祥地の筈です。ガロアという天才がまず代数学で認識していなければ。。。

代数での例としては、本文でもふれた $n$ 次対称群（記号 $S_n$) が挙げられます。高校時代、私もガロアの話からこういうものも数学の対象なんだと驚いたものでした。構造を持たない単に $n$ 個の元の集合 $A$ に対して、$A$ から $A$ への 1 対 1 対応 $f : A \to A$（置換とよぶ）全体　$S_n$ に、置換の合成 $(fg)a = f(g(a))$ によって積を入れたものです。

通常よく用いられる表示方は「互いに素なサイクル表示」です。例で説明するほうが分かりやすいと思います。$A = \{1, 2, \cdots 6\}$ として $S_6$ の元 $g$ を $(123)(56)$ と書いたら、$g$ は $1, 2, 3$ を $1 \to 2 \to 3 \to 1$ と回し、書かれていない 4 は固定し、$5, 6$ は入れ替える置換、という意味です。

(3-3) 部分群、正規部分群と商群

群 $G$ の部分群とは、$G$ の $e$ を含む部分集合 $H$ であって $G$ の積によってそれ自身が群になる —つまり $H$ の元の積や逆元が $H$ からはみ出さない—もののことです。$G$ 自身と $e$ だけというのが両極端の部分群ですが、一般にはそれらの中間にいくつもあります。部分群 $H$ は、その外側もこめて $G$ を分割しますが、分割は左右 2 通りあります。一般に $Hg = \{hg; h \in H\},\ gH = \{gh; h \in H\}$ と書き、単に集合としての寄せ集めの意味で記号 $+$ を使うとき

$$G = H + Hx + Hy + \cdots \tag{1}$$
$$= H + x'H + y'H + \cdots \tag{2}$$

この分解によってさまざまな量が群の位数（元の個数）の約数になることもわかります。この分

解の項の和が有限ならそれはどちらも等しく（一方に対応 $g \to g^{-1}$ を施すと他方の分解を得るから)、それを $H$ の「指数」とよびます。

任意の $x \in G$ に対して $Hx = xH$、いいかえると $x^{-1}Hx = H$、が成り立つとき $H$ を $G$ の正規部分群とよびます。このときは (1)(2) の分解は $x' = x,\ y' = y, \cdots$ だから同じで、その分解の「成分の」集合 $G/N = N\backslash G$ に $G$ の積構造が自然に誘導され $G/N$ も群になります。$G$ の $N$ による「商群」です。

(3-4) アーベル群、可解群

アーベル群（または可換群）とは積が可換な群のことです。群 $G$ の 2 つの元 $a, b$ に対して、それらの積の可換性の「テスト」である第 3 の元　$[a, b] = (ab)(ba)^{-1} = aba^{-1}b^{-1}$ を $a, b$ の交換子といい、交換子たち全てで「生成」（それらの逆元や積で表せる元をすべてとるという意味）される $G$ の部分群を $G$ の「交換子群」$[G, G]$ とよびます。これは $G$ の正規部分群です。そして $G$ のある商群 $G/N$ がアーベル群になるための必要十分条件は $N$ が $[G, G]$ を含むことです。

群 $G$ から出発して、その交換子群、そのまた交換子群、という列を作るとき、途中で止まらずあるところで $\{1\}$ だけの群になる場合、その群 $G$ を可解群といいます。方程式の代数的可解性と対応するガロア群の性質からの命名です。

対称群 $S_n$ の交換子群は、$S_n$ の元のうち「置換の符号が正」のものだけからなる指数 2 の正規部分群で、交代群 $A_n$ とよばれています。ところが $n \geq 5$ では、$A_n$ の交換子群はそれ自身になってしまうので $n \geq 5$ では、$S_n$、$A_n$ は共に可解群になりません（次項)。

(3-5) 群の内部自己同型と共役類

群 $G$ の元 $g_0$ を 1 つとり、$G$ から $G$ 自身への写像

$$g \to g_0^{-1} g g_0$$

を考えると、これは 1 対 1 対応であり、積を積にうつし、逆元を逆元にうつします（一度自分で書いて納得すれば群についての理解が 1 分間で高まるかと思います)。これは群構造に関する自己同型射、われわれが回転とよんでいるものの一種で、群論では内部自己同型とよばれるものです。おわかりのようにこれら自体、$G$ のある商群と同型な群になります。

内部自己同型で互いにうつりあえる $G$ の元同志は一つの類、共役類を定めます。つまり $g, g' \in G$ が互いに共役とは $g' = g_0^{-1} g g_0$ となる $g_0 \in G$ が存在することです。

群の元の性質に対する普遍性のある命題は、すべて共役類に関する命題だと言えるでしょう。

対称群 $S_n$ の共役類は、互いに素なサイクル分割に現れるサイクルの長さだけを並べたものと対応します。

交代群 $A_5$ の交換子群がそれ自身になることの検証。まず 3 文字のサイクル $a = (123),\ b = (345)$ $c = (234)$ はいずれも 3 乗して 1 だが、$S_5$ の最初のアーベル化が位数 2 だからそこでは潰れる、つまりいずれも $A_5$ に属する。次に、簡単な手計算で $[a, b] = (143)$、$[a, c] = (14)(23)$ だが、

これらの共役類を集めると個数が既に $20+15$ となり、これは $A_5$ の位数 60 の過半数を超える。だから $A_5$ の交換子群は $A_5$ 全体でしかあり得ない（右から順に掛けることに注意）。

(3-6) 既約剰余類群 $(\mathbf{Z}/n)^\times$ とは

整数全体 $\mathbf{Z}$ という無限集合における和と積の構造を調べるため、しばしば、それを有限個の元からなる構造体に落として考えます。自然数 $n>1$ をあたえるごとに、整数を「$n$ で割った余りだけ」によって類別し、和や積も類同志に対して考えるのです。それが可能なのは、$n$ の倍数を（どういう倍数であれ）一括りに $(n)$ と記すとき

$$(a+(n))+(b+(n))=(a+b)+(n) \tag{3}$$
$$(a+(n))(b+(n))=ab+(n) \tag{4}$$

が成り立つからです。類全体がつくる有限集合に和と積の構造をもたせた構造体を

$$\mathbf{Z}/n$$

で表します。$\mathbf{Z}/n$ の元を 1 つとり、$a\in\mathbf{Z}$ をその類に属する整数とすると、$a$ と $n$ との最大公約数は元の類だけで定まりますが、それが 1 となる類のことを mod n の既約剰余類とよびます。たとえば $n=6$ ならそれは $\equiv 1,5\ mod\ 6$ の 2 つの類だけ、$n=p$ が素数なら $\equiv 1,2\cdots p-1$ まで $p-1$ 個あります。なお、mod n の既約剰余類の個数はオイラーの関数とよばれています。ここでは必要ありませんが、念のため記しておくと

$$\phi(n)=n\prod_{p|n}(1-1/p)$$

です（$n$ を割るすべての素数 $p$ にわたる積）。既約剰余類全体が積に関してなす群は mod n の既約剰余類群 $(\mathbf{Z}/n)^\times$ とよばれます。

(4-1) ガロア理論の基本定理。

分解体 $K$ のガロア群を $G$ とするとき、$G$ の部分群 $H$ たちと $K$ の「中間体」$k$ とよばれる和と積と（0 以外の元による）商に関して閉じた集合体たちとの間に自然な 1 対 1 対応がつけられます。

部分群 $H$ と対応する中間体 $k$ とは、任意の $H$ の元の作用で固定される $K$ の元全体、逆に $k$ と対応する部分群 $H$ は、$G$ の元のうちでその作用が $k$ のすべての数を固定するものたち全体です。$k$ が有理数全体のときと $k=K$ のときが両極端でそれぞれ $H=G$、$H=\{e\}$ と対応します。$n$ 次方程式のガロア群を対称群 $S_n$ に埋め込んで考えた場合、1 根 $\alpha_i$ だけの有理数係数の多項式として表せる $K$ の元全体 $k_i$ と $n$ 文字の置換として $i$ を固定するものの作る $G$ の部分群 $H_i$ とが対応します。中間体 $k$ に属する元と共役な元、つまりそれが満たす既約方程式の根たちが必ず $k$ に属するのは、対応する $H$ が正規部分群になることです。ガロアが残したメモアールの最初の方で強調されていたことです。

(4-2) 円周等分方程式 $f(x)=x^n-1$（$n$ は正の整数）のガロア群 $G^n$ の記述。これは古典的整

数論の基礎といってよいでしょう。まず $x^n-1=0$ の根（複素数の根）は、そのうちの「原始根」—$n$ の真の約数 $d$ に対する $x^d-1=0$ の根を除いた根—の 1 つ $\zeta$ の冪としてすべて表せること、ガロア群の元 $\sigma$ は $f(x)=0$ の原始根を原始根にうつすから、特に $\zeta$ もその冪の 1 つ $\zeta^a$ にうつし、$a$ は $n$ と互いに素でなくてはならないこと、そして $a$ は $\zeta$ の選び方によらないことがそれぞれ簡単に分かりますから $\sigma$ は $a$ で代表される $(\mathbf{Z}/n)^\times$ の元を定めます。実は

この対応 $\sigma\to$ は群 $G^n$ から群 $(\mathbf{Z}/n)^\times$ への同型射

になります。しかもこの「円の $n$ 分体」の数論的性質をきれいに反映する射です（後述）。

実は有理数係数方程式のガロア群がアーベル群になるのは、分解体がこれら「円分体」のどれかに含まれる場合に限られるのです（クロネッカーの定理）。

(4-3) 方程式の代数的可解性のガロアによる判定

アーベルに始まりガロアが根本的解決を与えた方程式論の 1 つの結果は

方程式が代数的に解けるための必要十分な条件はそのガロア群が可解群であること

でした。これらの意味ですが、まず代数的に解けるとは「すべての根が、係数から出発して四則と根号をとる操作の有限回の組み合わせによって、それぞれ（他の根と）区別して表せること」です。

これを感じ取るために、方程式 $x^5-2=0$ に注目してみてください。この根を一括りに $2^{1/5}$ と書いたのではだめです。それでは 5 個の根の区別もできておらず、全部の根を考えることのプラスも生かせていません。 2 月の書簡で書いた式

$$\zeta=\left(\sqrt{5}-1\ +i.\sqrt{10+2\sqrt{5}}\ \right)/4$$

によって 1 の原始 5 乗根の 1 つ $\zeta$ を定め、2 の実数の 5 乗根だけを $2^{1/5}$ と表し、上の方程式の 5 根を $2^{1/5}\zeta^k,\ (k=0,1,\cdots 4$ と区別してで表すのが代数的解です。これで見えるように $x^5-2=0$ の分解体は $x^5-1=0$ の分解体を含む 2 重の塔になっていて、それらの間の相対的なガロア群がアーベル群なのです。$x^3-2=0$ のガロア群自体はアーベル群ではありません。これは代数的に解ける 5 次方程式の例で、解ける理由がこの塔構造です。

対称群 $S_n$ は $n\le 4$ の時に限り可解群で、これが 4 次方程式までは代数的に解けるが 5 次以上はそうでないことの構造的な原因でした。

実はガロアはもっと印象的な定理を述べています。素数次の既約な方程式が（四則と）根号で解けるためには、すべての根がそのうちの任意の 2 根によって有理的に（有理数係数の多項式のよって）表せることが必要十分である。

分からない根たち同志の間の関係性が解けるかどうかの鍵だという命題は、それまでの計算手法の数学と一線を画していたわけです。

(5-1) $GF(p^n)$ の計算に適した表示法は、既約 $n$ 次式 $g(x)$（を任意に一つとった上で）の分解体としての構成です。これは $x$ の $Z/(p)$ 係数の $n-1$ 次以下の多項式全体の集合に、「和」はそのままの和、「積」は「掛けてから $g(x)$ で割った余りをとる」を入れたものです。たとえば $p=2$、$n=2$ とすると $g(x)=x^2+x+1$、$GF(4)=\{a+b\omega,\ \omega^2=\omega+1,\ a,b=0,1\}$ です。

(5-2) 分解体の整数論を考える際の最初のポントは、実際は「判別式」からのガロア群への情報、そして素数の分岐情報なのですが、今回は判別式の話は割愛します。分解体には判別式という整数が付随し、それを割らない素数 $p$ はそこで分岐せず（もとの方程式で大雑把に言えば係数を $\mathbf{Z}/p$ に落としても重根を持たず)、「フロベニウス射 $\phi_p$ なる $G$ の共役類を定める」ということに留めます。円周等分方程式の場合、それは（何とも気持ちの良いことに）$p$ の $n$ による剰余類自体と対応し、複素共役が定める $G^n$ の元は $-1$ が定める $(Z/(n))^\times$ の類となります。

(5-3) $n$ 次方程式 $f(x)=0$ のガロア群 $G$ は対称群 $S_n$ になるのが（ある意味で）一般的ですが、個々の場合そうなっていることを示すには、精妙な工夫が必要です。

たとえば $f(x)=x^5-x+1$。この場合は $p=2,3$ での簡易化で十分です。

まず $p=3$ のとき $f(x)$ は既約、従って $\phi_3$ は (12345) 型、他方 $p=2$ での既約分解は $f(x)\equiv(x^2+x+1)(x^3+x^2+1)$、だから $\phi_2$ は $(ij)(klm)$ 型、従って $\phi_2^3$ は $(ij)$ 型の置換になります。そしてこれら双方を含むことから、群のちょっとした計算で、$S_5$ 全体にならざるを得ないと分かります。

これを見ると、この係数に 6 の倍数を増減（たとえば $f(x)=x^5-7x+1$）しても全く同じ結論が出る、また 3 の倍数の増減でも、上の $\phi_2^3$ の代わりが虚根の関連で見つかればよい。その例として $g(x)=x^5-4x+1$ をとってみます。$g(-\infty)<0,\ g(0)=1>0,\ g(1)=-2<0,\ g(\infty)>0$ で、$g(x)$ は $x$ が実軸を右に走るとき 3 回符号が変わりますから、3 個の実数の根と 2 個の虚数の根を持ちます。従って複素共役射 $a+bi\to a-bi$ が分解体に作用し、それは 3 根を動かさず 2 根を入れ替えるという互換を引き起こすからこの役割を果たし、この場合もガロア群は $S_5$ になるのです。

ここで述べたかったのは、「素数の一つ」として複素数へのうめこみもあり、フロベニウス射の代わりとして複素共役射がある、というバランスのとれた見方、これによってやっと

全方位を見た、フル・サークルが描けた、

という調和感です。

(5-4) $p$ ガロア群のガロア群の部分群としてのパターンが $p$ にどう依存するか。言いかえると整数係数の多項式 $f(x)$ の mod p での既約分解のパターンは、「$p$ にどう依存するか」？　根が 1 の $n$ 乗根の有理数係数多項式で表せる場合は、それは $p$ を $n$ で割った余りだけで決まったのですが、それ以外の場合は大変難しく、現代数学の最前線と結びついています。

ここでは最初に、類体論で知られている場合のうちごく簡単な例を、次いで（類体論によっても）分かっているとは言い切れない例を、いずれも 3 次方程式で 1 つずつご覧ください。

1）$x^3-7x+7=0$。この 3 根は　$\theta=2\pi/7$ と置くとき、$2\cos(\theta), 2\cos(2\theta), 2\cos(4\theta)$ となります（$\cos(8\theta)=\cos(\theta)$、と循環します）。任意の 1 根を $\alpha$ とすると、他の 2 根は、コサインの 2 倍角の公式から　$\alpha^2-2$ と $-\alpha^2-\alpha+2$ になります。このように 3 根の間の関係性は対称ではなく、ガロア群は交代群 $A_3$ です。また、これは $n=7$ の円分体の中の実数だけの部分なので、上記のフロベニウス射の記述から直接従うこととして、$x^3-7x+7$ は $\mathbf{Z}/p$ では

3 重根をもつ　($p\equiv 0 \bmod 7$ のとき)
3 つの 1 次式の積に分解　($p\equiv \pm 1 \bmod 7$ のとき)
既約　(その他の $p$ の場合)

となります。

2）$f(x)=x^3+x+1$ 。ガロア群は対称群 $S_3$ です。その $\phi_p$ が素数 $p$ によってどう変わるかの様子をご覧ください。なお 31 が現れるのは、この判別式が $-31$ であることの反映で、実はこの分解体は「虚 2 次体 $\mathbf{Q}(\sqrt{-31})$ の絶対類体」とよばれる古典整数論の華の一例です。

(i) $f(x)$ mod p が既約 $\Longleftrightarrow$ $\phi_p$ の共役類は (123) 型 $\Longleftrightarrow$ $p \bmod 31$ は $Z/31$ の非平方数
(ii) $f(x)$ mod p は 1 次式と既約な 2 次式の積 $\Longleftrightarrow$ $\phi_p$ の共役類は (12) 型 $\Longleftrightarrow$ $p \bmod 31$ は $Z/31$ の平方数だが $p=a^2+31b^2$ となる整数 $a,b$ は存在しない
(iii) $f(x)$ mod p は 3 つの 1 次式の積 $\Longleftrightarrow$ $\phi_p=e \Longleftrightarrow p=a^2+31b^2$ となる整数 $a,b$ が存在。

素数は無限個ありますが、その部分集合のチェボタレフ密度というのが定義されており、上記 (i)(ii)(iii) それぞれに属する素数のチェボタレフ密度は存在し、それぞれが $\phi_p$ が属する $S_3$ の共役類の大きさに比例した $2/6, 3/6, 1/6$ であることなどは一般論でわかっています。
（註）$(a+\sqrt{-31b})/2,\ a.b\equiv 1 (\bmod\ 2)$ も「整数」ですが、これらのノルムは 2 で割れ、素数にはなりません。

その一方、(ii)(iii) の最後の判別法が明示的に至っていないこと、これがこの問題の難しさを端的に表しています。双対性によって重さ 1 の保型形式、保形表現という言葉に翻訳してみても、(i)(ii) の区別は同じことの言い換えに過ぎなくなってしまうようです。これは、素数を分解体に延長して素因子分解するとき、「素因子」が数の範囲で存在する場合と、数の範囲ではもはや「素」と呼べるものは存在せず「素イデアル」という集合まで考えなくてはいけない場合との相違でもあり、基本的な区別と関わっています。

補足原稿とはいえ、振り向けば誰もいない？ 処にまで来てしまいました。もしここまでお読みくださった方がおられたら感激です。是非編集部さんにご一報下さい。では夏休みに入らせていた

だきましょう。皆様もどうぞお元気で。