MATHEMATICAL
April 2007 SCIENCES Number 526

特集／現代数学はいかに使われているか [代数編]

現代数学が繰り広げる世界

(代) 数学はいかに使われているか

中村　郁

1. はじめに

現代社会の中で数学は，どのように使われているか？　これは，数学を学ぼうとする人々が等しく疑問に思うことであるだろう.「いや，面白くてそれで十分だ」と思ってくださる方は，そのままでいい.「面白い」というのは学問の重要な要素である．しかし，数学を教える立場の人の中には,「何で数学なんか，勉強しなきゃいけなんですか？ 僕は数学なんかいりません」と言う反発に出会ったことのある人もいるだろう.「教える」ということは，本来学ぶ意味の（基本的な）説明も含まれていると解すべきである．しかし，実のところ，数学者でも，どこにどう使われているか，すべてよく知っているわけではない.

筆者は最近，線形代数の教科書を執筆し，その中でいくつか線形代数の応用についても述べた．量子力学から題材をひいたり，マルコフ連鎖の例を挙げた．たとえば，シャーレの中に 2 種類の細菌 A, B があり，それぞれの細菌が毎秒 1 回変化して，また細菌 A,B を生成する．細菌 A はその 70% が A になり，30% が B になる．細菌 B はその 40% が A になり，60% が B になる．(こんなことが実現できるかどうか知りませんが) 総量 $A+B$ は変化しないものとする．シャーレを数日間放置したら，その中の細菌 A, B の割合はどうなっているか？ これはマルコフ連鎖の一番簡単な例である.

最初の時点での A,B の量を A_0,B_0 とする．そうすると，1 秒後の A,B の量 A_1,B_1 はそれぞれ

$$A_1 = 0.7A_0 + 0.4B_0, \quad B_1 = 0.3A_0 + 0.6B_0$$

となる．2 秒後には

$$A_2 = 0.7A_1 + 0.4B_1, \quad B_2 = 0.3A_1 + 0.6B_1$$

となる．行列を使って表せば,

$$\begin{bmatrix} A_1 \\ B_1 \end{bmatrix} = \begin{bmatrix} 0.7 & 0.4 \\ 0.3 & 0.6 \end{bmatrix} \begin{bmatrix} A_0 \\ B_0 \end{bmatrix}$$

これを無限回繰り返すと (収束は仮定しておくが) 答えが求まる.

$$\begin{bmatrix} A_\infty \\ B_\infty \end{bmatrix} = \begin{bmatrix} 0.7 & 0.4 \\ 0.3 & 0.6 \end{bmatrix}^\infty \begin{bmatrix} A_0 \\ B_0 \end{bmatrix}$$

行列 P を

$$P = \begin{bmatrix} 0.7 & 0.4 \\ 0.3 & 0.6 \end{bmatrix}$$

とする．このとき,

$$P \begin{bmatrix} A_\infty \\ B_\infty \end{bmatrix} = P^{\infty+1} \begin{bmatrix} A_0 \\ B_0 \end{bmatrix} = \begin{bmatrix} A_\infty \\ B_\infty \end{bmatrix}$$

だから，$\begin{bmatrix} A_\infty \\ B_\infty \end{bmatrix}$ は行列 P の固有値 1 に対応する固有ベクトルである．一方，行列 P の固有値 1 に対応する固有ベクトルは容易に計算できて，

$$\begin{bmatrix} 4 \\ 3 \end{bmatrix} \quad \text{または，その定数倍}$$

となる．したがって，$A_\infty : B_\infty = 4 : 3$，すなわち，$A_\infty : B_\infty$ は最初の A, B の割合によらず行列 P で決定される．線形代数では，必ず，行列の固有値や固有ベクトルの計算と行列の対角化を教える．そういう計算が役に立つことが，マルコフ連鎖の問題を解くとよく分かる．

あるいは，世界で最初の X 線 CT スキャンは，その原理の本質的な部分が，線形代数で説明できる．一言で言うと，非常に変数の多い連立 1 次方程式を短い時間で解く問題である．ところが，この方程式は一般に解を持たない方程式である．そこで,「最小 2 乗解」という近似解を求める．これは，体重や身長を測定するとき，複数回測定して平均値をとるのと本質的に同じである．X 線 CT スキャンでは 1 度に 90 万個もデータがとれるので，こういう求め方が必要になる．これは計算量が多いので，計算機を用いて初めて可能になる線形代数である．なお，歯科用であれば，理論的には「最小 2 乗解」CT スキャンで十分であることが知られている．

また，コンパクト・ディスクの再生には，ほこりや傷を受けたときも，正しいデータを推定して再生する技術が必要である．誤り訂正符号の理論は，そのような問題を扱う数学の理論である．そのなかでも線形符号理論は，線形代数を学習したあとなら説明は容易なので，ハミング符号を紹介した．符号理論のもとのアイディアは簡単なので，これについては，§ 5 で初歩的な部分を解説する．線形代数という教科のほんの少し先に，こういう面白い応用がある．学生の一部からは「数学がどう使われているか，分かって面白かった」という反応があった．

2. 数学は役に立つか？

いろいろな人と話すと，意外なことを教えられることがある．

大学 1 年生「先生，受験勉強の中で「考える」のは数学くらいしかないんだぜ，長い解答書くのも数学しかないし，ほかのはほとんど暗記だよ」

文学部の歴史の先生「いや，高校時代，図形の講義は楽しかったですな．こんな問題もありましたよ，缶詰の缶を作るのに，一定の面積のアルミ板を使って最大の容量にするには，半径と高さの比率をどうすればいいか，微分を使うとできるんです．この問題を出されたとき，数学って役に立つんだなーって思いましたね」

数学教育法の講義の受講生「数学は，論理的にものを考える訓練として適している」

という具合である．

「役に立つか」という問にどう答えるか？　それは,「役に立つ」とは何か，どのようなことなのか？　あるいは，どういう視点から「役に立つ」と考えるのか？　ここを分岐点として，答えは個人差が大きくなる．数学者は多くの場合,「自分のいつもやっている最先端の数学」を「数学」だと思っているから，算数や微積分が役に立っても，それではなにか物足りない．だから，心情的には「数学は役に立ちます」とは答えにくい．しかし，それでも訊かれたら，数学者は職業である以上，役に立つ実例を見つけて説明できた方がいい．

「数学は役に立つか？」という問を，もっと強く「先端の数学研究がすぐ社会的な応用に結びつくか?」と解釈する立場もないわけではないが，ここではそこまで堅くは考えたくない．私の「数学の役立ち方」に対する答えは，以下のようになる．

(i)　そもそも，定量的な答えを導く（つまり，数字で答えを出せる）科学的な手段は数学しかなく，その意味で社会の全般で役立っている．

(ii)　論理的な思考の訓練として最適であって，教育的にも大切である．論理的な思考は，自然科学，社会科学の最も基本的な考察手段である．

(iii) 実用化された数学的アイディアは沢山ある．たとえば，計算機（これだけで大変な寄与である），通信手段 (携帯電話など)，位置確認手段（カーナビなど），画像処理，医療診断装置，100 年前には想像も付かなかったものが（ハードウェアの進歩，他の技術の進歩により）現在実用化されたものがあるように，今後何十年後かに，それが，何であるかは現在予言することはできないが，数学の中に実用化されるものが必ずあると信じてよい．1683 年 (おそらくそれ以前に) ニュートンは「惑星の軌道は太陽をその焦点のひとつとする楕円である」ことを証明した．その結果，当時の誰一人おそらく夢想すらしなかったようなことが，今起きている．静止衛星を用いて世界中の人々が携帯電話で話し，カーナビで車を運転する．ニュートンの発見から実に 300 年が経過している．同じことが将来別の数学で必ず起きる，と信じてよい．

もちろん，これらの応用技術は常に軍事的な利用の可能性をもつが，その逆も起きる．たとえば，人工衛星の偵察撮影写真の画像処理は，その後，ハッブル望遠鏡による天文観測の画像処理を経て，現在では医療診断の画像処理として役立っている．トマホーク・ミサイルの誘導装置は，その後カーナビとなった．カーナビが可能なのは，静止衛星のお陰であるが，静止衛星はレーガン大統領のときに，スター・ウォーズならぬ核攻撃迎撃システムとして利用されそうになったこともある．静止衛星はほかにも携帯電話，気象観測で威力を発揮している．これらは，高速大規模計算が可能なためであって，それは計算機の発明のお陰であり，それは数学の２進法のお陰である．もちろん，それは，電子の電荷がプラスとマイナスの二つであることのお陰でもある．数学的事実だけが，何かの発明を可能にするのではなく，物理的な，あるいは，化学的な別の現象と有効に結びついてはじめて可能になる．

ここにあげた数学の応用はそれでも高度な部類である．もっと理論的に高度な例は，本特集の記事をごらんいただけばよい．しかし，私が (i) で述べたのはそんな高度なものを意味していない．

日本に本格的に数学が輸入されたのは，7 世紀遣隋使，9 世紀遣唐使による律令制度の輸入の時期と重なる．それは，この時期に暦，数詞，測量技術，班田収受の法などの租税の制度が導入されるからである．数学教育は唐の制度を導入し，(人数も唐と同じ）算博士 2 名，算生 30 名の学制が作られ，唐の教科書『九章算術』などが使われた．いまで言えば，学生 30 名の学部数学科と合計 2 名の修士・博士課程に，教科書は「解析概論」というところであろう．これが，日本で測量・租税の技術官僚を養成した最初と思われる．当時の最先端の数学が，当時としての近代化，官僚制度により国家財政を管理・運営し，平城京・平安京をはじめとする都市開発・建設を行うために必要であったことがうかがえる．これは，明治初頭，菊池大麓を先頭に西洋数学を導入した東京帝国大学数学科の発足を思わせるものがある.『古地図から見た古代日本』(岩波新書) によれば，東大寺開田図と呼ばれる古代荘園の地図のあるものには,「算師」という役職の人物の署名が残されている．租税や寺の造営に関わる官僚と推定されるが,「算師」という名前からも，算生・算博士コースの卒業生であろう.「造東大寺司」という役所が発注して「東大寺写書所」の「画師」に荘園図を作製させたこと，さらにその報酬額の記録が残されている．この「造東大寺司」には「算師」が所属していたことが知られている．筆者の想像だが,「造東大寺司」の「算師」による測量結果を，荘園図として作製・浄書するよう「画師」に依頼した，と見るのが自然であろう．しかし，この点はまだ解明されていないようである．

奈良平安時代の数学なら，現在の中学生の知識で十分であろう．しかし，これが当時としての最先端の数学であった．時代とともに，人々の理解できる数学の領域は拡大していく．現在の中学の数学では，２次方程式の解の公式を学ぶ．ピタゴラスの定理や円周や球の体積を学ぶ．高校では，３角関数や等比数列，３次関数やそのグラフ，最大

最小や行列を学ぶ．かなりの生徒が計算機の小さなプログラムを書ける．優秀な生徒なら大人に負けないプログラムを書く．中学生や高校生の学ぶ数学で，相当難しい事ができるのである．しかし，それは少しも不思議ではない．

それはつぎのことを考えてみれば分かるだろう．様々な機会に (たとえば，岩波の『図書』の野上弥生子記念) 読書感想文コンクールがあるが，一見して中学生や高校生の作品はきわめて高度である．あるいは，中学生や高校生の日本語能力でも，もう充分文学作品を読み，味わうことができるし，小説を書くことさえもできる．そういうレベルの日本語能力を備えている．あるいは，中学，高校で学ぶ英語が完璧ならば，それでも相当の英語力である．英会話の能力なら，この年齢で十分高いレベルに到達する．

数学もそうである．高校生数学オリンピックの問題は数学者でも解けないことが多い．それくらい難しい．そういう出題が可能なほどに，高校までの数学は十分高度なレベルまで教える．専門家になるためには，たしかにまだたくさん勉強しなければならないのは当然だが，にもかかわらず，高校までで学ぶことは，すでに相当のレベルになる．

だから，社会のさまざまな分野で役立てられている数学が，高校までの数学を学んだひとびとに十分理解できる水準の数学に依存しているのは, 少しも不思議でない．

3. 思考手段としての数学

にもかかわらず，数学が役に立たない，と言われれば，数学者は「たまには数学も役に立ちます」と防戦一方になりがちである．しかし，実際は「数学は大変役に立っている」．数学は，数学者の頭脳の中だけで活動しているわけではない．社会ではそれをもはや数学とは意識しない程に，数学を自らの一部としているために，気づかなくなっているだけである．

大切なのはまさにこの点である．前節 (ii) で述べたように，数学は思考手段である.「考え方として，あるいは考える手段として，数学を頭脳の中に持っているか否か」その差に気づくか否か，この点で数学の大切さの評価は大きく変わる．自動車，テレビ，電気洗濯機や掃除機のように目に見える便利さはない．有効に使いうる人間にしかその重要さは気づかれない．より正確にいえば，余りに当たり前のものとして使っていれば，その人間でさえ，重要さに気づかないこともある．

しかし，こういう数学の役割，思考手段としての数学の役割こそ強調されなければならない．数学の有用性とは，まず第一に，思考手段としての有用性である．数学者のひとつの役割は，そのような数学の潜在的な力を次代に伝えていくことである．定理を増やすことだけが，数学者の役割ではないし業績なのでもない．

その一方で，先端の数学がそのまますぐ役に立つか，と言われれば，たいていの数学者は答えに窮する．しかし，100 年，200 年のスパンで見れば，必ず，今ある数学のどれかが役に立つと信じてよい．しかも，その役立ち方は，ひとつふたつの工場ができると言う規模ではなく，一つの産業が生まれたり，社会全体が恩恵を受けるような大きな影響の可能性がある．これが基礎科学の持つ力である．しかし，逆に言えば，だからそんな強力なアイディアが，そうたびたび出てくる筈もない．

たびたび出て来なくても，数学は社会の様々なところで思考手段として役立っている．

4. アメリカ数学会による分類

つぎの表は，アメリカ数学会による数学分野の分類の一部である．アメリカ数学会では，数学研究者の便宜をはかって，論文の内容を数百字程度にまとめた要約集 (Mathematical Reviews) を発行している．Reviews では，おのおのの論文に，論文がどのようなテーマを扱っているかを示すために，14K10,11G10 と言うような分類番号が付く．14 は代数幾何学を表し，K10 は「アーベル多様体」という幾何学的対象を表す．一般には，最初の 2 桁の数字が粗い分野を表し，次の 1 文字 2 数

字が細分されたテーマやキーワードを表す．分類番号は現在 00 から 97 まであり，今後増える可能性もある．04 以降 57 までは数学固有のテーマで，そのほとんどには，(若干の飛び番号はあるが）代数学，幾何学，解析学の分野が並ぶ．それらを説明するのは，この序文ではほとんど不可能に近いので，具体的な名称も省略した．以上が，現在の世界の数学分野の標準分類番号の概略である．

以下では，タイトルから内容が想像がつきそうなものだけを列挙した．

00　一般
01　歴史と伝記
03　数理論理，および数学基礎論
14　代数幾何学
49　変分法、最適制御、最適化
58　大域解析，多様体上の解析
60　確率論と確率過程
62　統計学
65　数値解析
68　計算機科学
70　質点と質点系の力学
74　変形可能な固体力学
76　流体力学
78　光学、電磁気学
80　古典的熱力学、熱の移動
81　量子論
82　統計力学、物質の構造
83　相対論と重力理論
85　天文学と宇宙物理学
86　地球物理学
90　OR 理論、数理計画法
91　ゲーム理論、経済学、
　社会科学および行動科学
92　生物学およびその他の自然科学
93　システム理論、制御
94　情報と通信、回路
97　数学教育

大学で言えば，理学部の他の学科，工学部で扱われるテーマが，ここに登場している．これらはみな数学者の研究テーマである．49 や 58 以降の多くについては，説明なしでも大体の内容が想像つくと思う．おそらく，相当数の読者が，このようなテーマが数学であつかわれていることを意外に思うかもしれない．数学のテーマは，一般の人々とが想像するよりも，はるかに広範で深い．定性的な問題はともかく，定量的に数値を求める問題で数学が使われないということは，おそらくないだろう．

たとえば，94 では，筆者の専門分野である代数幾何学の同僚たちが，暗号理論に代数幾何学を用いて研究している．このほか，整数論研究者でも，すぐれた擬似乱数発生の方法を考案した松本真氏や，詳細な数論の研究成果が偶然にも，本質的に高性能の暗号を与えていた，伊原康隆氏の例がある．92 の生物学は，これも数学のテーマとしてかなり有望視されている．DNA の組み合わせ論的研究は，簡単ではないが興味あるテーマであるし，非常に多くの個体からなる系の運動や行動は，視点の置き方によって，数学のトポロジー，微分幾何学の問題ともなる．あるいは，粘菌のコロニーの示す運動も興味深い．大脳がないにもかかわらず，餌に近づくために最短距離を選択できるなど，全体として一つの生物のように行動する．そのメカニズムの解明は，今なお (数学的にも) 興味深い問題であり，熱心に研究されている．あるいは，動物の皮膚模様はどのように決定されるか？　これについては，反応拡散方程式のひとつ，チューリング (イギリスの数学者，チューリング・マシーンを発明したことでも知られる) の方程式が有名である．この方程式は．実験的にも正しいことが確認されている．こういうことが，数学のテーマたりうるのである．

分野の話をしたついでに，もう一言付け加えると，「代数学」と「幾何学」は一般に思われているほどに違うものではない．筆者の専門分野は「代数幾何学」と言う，「代数学」と「幾何学」の中間の分野である．「代数幾何学」とは，「幾何学」を研究するために代数的な手法を用いる分野，という

意味である.「幾何学」も「数論幾何学」,「代数幾何学」,「複素解析幾何学」,「微分幾何学」とほぼ連続的に変化する．その手法も，代数的なものから,「多変数関数論を用いた複素解析的」,「微分方程式を用いた解析的な方法」へと連続的に，ときにアイディアは全く別の世界から援用されて混然一体となる．それでは,「代数的」なものと「解析的」なものはどうかと言えば，ソリトン方程式と呼ばれる特殊な系列の微分方程式 (解析的な対象) は代数的にすべての解が求まる．この場合には，それらの方程式と解全体を完全に代数的に統制する原理，大きな対称をもつ変換群が存在する (佐藤理論)．と言うわけで,「代数学」と「解析学」も全く違う分野と言い切れないものがある．

5. 符号理論の初歩

坂内氏の論説の予備知識として，符号理論を簡単な場合に説明する．長さ 2 の情報ビット (a_1, a_2), $(a_i \in \{0,1\})$ を送信したいとしよう．つまり，4 種類の情報を送信したいとしよう．0 と 1 は送信の際にそれぞれ 1 と 0 に誤って送信されるかも知れない．もちろん，送信システムが全く信頼できないレベルであれば，どんな誤送信があるか分からないので，そもそも情報の送信自体が無理である．しかし，かなり信頼できるレベルの送信が可能であるとしよう．つまり，間違いはかなり低い頻度でしか起きないとしよう．その場合には，その誤りを突き止めて，正しい情報を再現できる可能性がある．それでは，そのためにはどうしたらよいだろう？　それがこの節で考える問題である．

最初にもっと簡単な場合を考える．長さ 1 の情報ビット 0 または 1 を送り，誤って受信された場合には訂正できるようにしたい，とすれば，長さを 3 にして，つぎのように送ればよい：

$$0 \text{ の代わりに } 0\quad 0\quad 0$$
$$1 \text{ の代わりに } 1\quad 1\quad 1.$$

こうすれば，受信した 3 個の信号の『多数派』が正しい元の情報と推定されるから，誤りが高々 1 つならかならず誤りを訂正できる（と考えてよい）．しかし，この方法では情報ビットをいつも 3 倍の長さにしなければならないから，効率が余り良くない．

今度は，2 つの情報を正しく送信することを考える．以下，

$$\mathbf{F}_2 = \{0,1\} = \{ \text{ 偶数のクラス，奇数のクラス } \}$$

とする．$\mathbf{F}_2$ は整数を 2 で割った余りのなす集合とみなしてもよい．2 進法で考える，と言ってもよい．こう考えると，$-1 = 1$, $-0 = 0$ だから，$x \in \mathbf{F}_2$ ならば，いつも $-x = x$ が成り立つ．これを

$$-x = x \mod 2$$

と表す．以下，誤解のおそれのない限り，簡単のために $\mod 2$ を省略するが，計算規則は単純で，

$$0+0=0,\quad 0+1=1+0=0,\quad 1+1=0$$
$$0\cdot 0=0,\qquad 0\cdot 1=1\cdot 0=0,\qquad 1\cdot 1=0$$

となる．送信すべき情報は

$$0\quad 0$$
$$0\quad 1$$
$$1\quad 0$$
$$1\quad 1$$

の 4 通りとする．まず最初に少し簡単な問題から考えよう．これを送信して，間違いがあったら，気が付くようにするにはどうしたらいいだろうか？　ただし，間違いは送信したコードのうち，高々1 ビットまでと仮定する．それには，つぎのように，パリティと呼ばれるもう 1 ビットを付け加えばよい：

$$0\quad 0\quad 0$$
$$0\quad 1\quad 1$$
$$1\quad 0\quad 1$$
$$1\quad 1\quad 0$$

3 番目の項は，(1 番目の項) + (2 番目の項) $\mod 2$ で与えられる．こうすれば，どれか一つが間違うと，関係式

$$(3\text{番目の項}) = (1\text{番目の項}) + (2\text{番目の項}) \mod 2$$

がくずれるので，誤りが何であるかは分からないが，ともかく，誤りであることは分かる．

さて，もっと進んで，ひとつの誤りまでは訂正できるようにするには，どうすればよいだろう？ ひとつの情報のときと同じようにすると，6 個の情報ビットで

$$\begin{array}{cccccc} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{array}$$

のように送ることになるが，もっと効率的にして，5 個で済ますことはできないだろうか？ それにはつぎのようにすればよい：

$$\begin{array}{ccccccccc} 0 & 0 & \mapsto & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & \mapsto & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & \mapsto & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & \mapsto & 1 & 1 & 1 & 1 & 0 \end{array} \qquad (1)$$

最後の項は，やはりパリティ項で，この場合は，はじめの情報が (x_1, x_2) ならば $x_1 + x_2 \mod 2$ $(= (x_1 + x_2)$ を 2 で割った余り$)$ を対応させる．この対応を一般的に表わせば

$$(x_1, x_2) \mapsto (x_1, x_2, x_1, x_2, x_1 + x_2 \mod 2)$$

となる．こうすると，どうしてひとつの誤りまでは訂正できるのか，考えてみよう．

たとえば，$\mathbf{x} = [\,0\,0\,0\,0\,0\,]$ を送ると，受信の誤りが高々ひとつなら，受信された信号は

$$\begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array} \qquad (2)$$

のどれかになる．仮に (1) の中の

$$1 \quad 0 \quad 1 \quad 0 \quad 1 \qquad (3)$$

も誤って受信されたとする．しかし，(3) の受信の誤りがひとつなら，それが (2) のどれかと一致することはない．したがって，(2) のように受信された信号は，正しくは

$$0 \quad 0 \quad 0 \quad 0 \quad 0$$

である確率が最も高いと判断してよい．このように考えれば，2 ビットの送信情報を 5 ビット (これを送信ビットと呼ぼう）で送ることにより，誤りを訂正できることが分かる．

つぎに，これを線形代数の見方で見てみよう．以後，$\mathbf{x} = [x_1, x_2, x_3, x_4, x_5] \in \mathbf{F}_2^5$，つまり，$x_i \in \mathbf{F}_2$ とする．いま構成した「誤り訂正符号」(1) は，集合としては

$$V = \left\{ \mathbf{x} \in \mathbf{F}_2^5 \,;\, \begin{array}{c} x_3 = x_1,\ x_4 = x_2 \\ x_5 = x_1 + x_2 \end{array} \right\}$$
$$= \left\{ \mathbf{x} \in \mathbf{F}_2^5 \,;\, \begin{array}{c} x_1 + x_3 = x_2 + x_4 = 0 \\ x_1 + x_2 + x_5 = 0 \end{array} \right\}$$

と同じである．これは，$\mathbf{F}_2$ 上の 2 次元ベクトル空間にほかならない．

行列 H を

$$H = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

とすれば，

$$V = \left\{ \begin{array}{l} \mathbf{x} \in \mathbf{F}_2^5 \,; \\ \mathbf{x}H = [\,0,\ 0,\ 0\,] \end{array} \right\}$$

と表すことができる．これは，典型的なベクトル空間の構成方法で，線形代数を学んだ人なら覚えているかも知れない．

上の述べた通り，送信ビット $\mathbf{x}$ は V に含まれる．これが $\mathbf{z}$ として受信されたとしよう．$e = \mathbf{z} - \mathbf{x}$ とすると，仮定により，e は成分が高々ひとつ 1 で，あとはゼロに等しい $\mathbf{F}_2^5$ のベクトルである．しかし，$\mathbf{x} \in V$ だから

$$\mathbf{z}H = (\mathbf{x} + e)H = \mathbf{x}H + eH = eH$$

となる．つぎの表を見よう：

e	eH
$[1\ \ 0\ \ 0\ \ 0\ \ 0]$	$[1\ \ 0\ \ 1]$
$[0\ \ 1\ \ 0\ \ 0\ \ 0]$	$[0\ \ 1\ \ 1]$
$[0\ \ 0\ \ 1\ \ 0\ \ 0]$	$[1\ \ 0\ \ 0]$
$[0\ \ 0\ \ 0\ \ 1\ \ 0]$	$[0\ \ 1\ \ 0]$
$[0\ \ 0\ \ 0\ \ 0\ \ 1]$	$[0\ \ 0\ \ 1]$
$[0\ \ 0\ \ 0\ \ 0\ \ 0]$	$[0\ \ 0\ \ 0]$

この表により，eH を見ると，誤り e が分かる．したがって，$\mathbf{x} = \mathbf{z} - e$ として最初の送信ビットとが再現される．こうして再現された $\mathbf{x}$ の最初のふたつの座標が，最初に送りたかった情報である．これが，線形代数的に考えたときに，V が「誤り(一つの) 訂正符号」である理由である．線形代数が巧妙に用いられている．

この考えを推し進めると，4 個の情報を送るには，3 個のパリティビットを加えて合計 7 個の情報として送れば，誤りが高々一つまでなら訂正可能である．これが (7,4,3) ハミング符号である．

以上が誤り訂正符号のもとのアイディアである．簡明ではあるが，発展性のあるアイディアであることが分かる．

6. 他の論説へのコメント

まず，この特集野記事の中にしばしば現れる「グラフ」とは何であるか，説明しておきたい.「グラフ」とは，点と点を線分で結んだ, (多くの場合有限個の) 折れ線の全体のことである．関数のグラフのことではない．以下の図 1 がそのグラフの例である．砂田氏の論説の 六角格子の実現もグラフの例であるが，一般には，周期的（規則的）である必要はない．

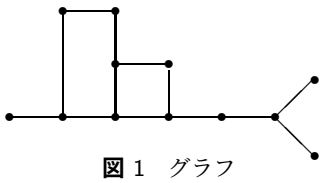

図 1　グラフ

砂田氏の論説は結晶について論ずる．結晶は空間の変換（自己同型）で不変であるとき，その自己同型が多ければ多いだけ美しい形をとる．結晶をそれ自身に重ね合わせる変換全体は群をなす．この群の構造と結晶には深い関係がある．代数的な観点から結晶を論ずるときは，この群を用いることが多い．論説は結晶を離散的なグラフの (3 次元ユークリッド) 空間内での周期的な実現として，幾何学的に興味深い解説を与える．

坂内氏の論説は，組み合わせ論，グラフ理論，符号理論，線形計画法，デザインなどの問題が他のテーマ・領域とどのように関わるか，最新の結果を交えながら幅広く解説する．

秦泉寺氏，菅野氏の論説は量子力学，場の量子論における線形代数的なものの見方について解説する.「表現論」という言葉が登場するが，これは，与えられた作用素（線形写像）を行列表示する (表現する) 理論であると思えばよい．行列表示する仕方は一通りではないので，表示方法の本質的でない差を無視すると，比較的都合のよい理論ができる．こうしてできた表示方法のなかで，もはや分解されないものを既約表現と呼ぶが，これは，物理の理論のなかでしばしば素粒子などに対応する．したがって,「表現論」とは，素粒子を研究するための線形代数的な方法を与える理論である，と言っても間違いではない．

二つの論説に行列は登場していないように見えるが，それは，行列ではなく線形写像として書かれているためである．秦泉寺氏の論説をみると，わずかに，$(X)_{nm}$, $(P)_{nm}$ と言う部分が，行列の (n, m) 成分として現れている．これを行列表示していないのは，実は行列のサイズが無限であるためである．二人の論説によって物理の量子論における数学の重要性が分かる．

河原林氏の論説は，グラフ理論のネットワーク解析への応用についての解説である．論説の目的を一口で言えば，道路網を交差点と交差点を結んだグラフとみなしたとき，どの経路を選べばいちばん早く目的地にたどりつけるか，というカーナビの原理の説明である．論説はこの問題について

の最新の結果を紹介する．

高山氏の論説はグレーブナー基底と呼ばれる，数学的に非常に有用で基本的な，(ベクトル空間の) 基底とその応用についての解説である．数学ではしばしば具体的な計算が重要になる．その計算を実行しようとすると，原理的にはできることが分かっている場合でも，具体的に求めるのは時間がかかって大変な場合が多い．ある程度一般的な状況でそういう計算を実行するアルゴリズムがあると，非常に役に立つ．論説はグレーブナー基底の研究と応用の現状を紹介する．

佐藤氏の論説は公開鍵暗号のたいへん具体的な解説である．ここでは，有名な「Fermat の小定理」が使われる．3 進法で (正確には，3 で割った余りを) 考えると，どんな数の 2 乗も 1 に等しい．

$$1^2 = 1, \quad 2^2 = 4 \equiv 1 \quad (3 \text{ 進法})$$

5 進法で考えると，どんな数の 4 乗も 1 に等しい．

$$2^4 = 16 \equiv 1, 3^4 = 81 \equiv 1, 4^4 = 256 \equiv 1 \ (5 \text{ 進法})$$

p を勝手な素数とする．このとき，どんな数の $(p-1)$ 乗も，p で割った余りは 1 に等しい．これが「Fermat の小定理」である．4051 は素数であり，$\mathbf{F}_{4051}^{\times}$ は集合としては，1 から 4050 までの数からなる．それらの積を 4051 進法で考えることにすると，積はまた 1 から 4050 までの数になる．「Fermat の小定理」によれば，どの数も 4050 乗すると 4051 で割った余りは 1 に等しい．

寺杣氏の論説は，線形代数の高度の数学的応用例である．整数論や代数幾何学の観点から重要な「代数的対応」と呼ばれる「線形写像」がある．元来，その「線形写像」は保型形式という関数の整数論的な研究にとって非常に大切な役割を果たす．この論説では「代数的対応」の類似物の理論物理学への応用について解説される．

（なかむら・いく，北海道大学）