代数 / 群・環・体

蟹江幸博

この日，頭棲(とうすむ)先生は少し機嫌が悪かった．

「いくら，算数・数学の質問箱を開いていると言ったって，こんな質問はないだろう．第一，質問になってやしない．だろう？」

だろう？と訊かれたって，我が輩には質問が見えないのだから，返事の仕様がない．見えても読めないだろうって？　うーん……[1]

「代数 / 群・環・体とは何なのか説明してください，だってさ．こういうの，質問ていうのか？　本を読めば分かるだろう．本はそのためにあるのだし，こういう質問をする以上はどこかで聞いたことがあるのだろうし，講義で聴いたんだったら，ちゃんと聞いてりゃ分かるだろう？」

読めなくったって，先生のボヤキを聞いてりゃ分かってしまう．

「ま，講義を聴いて分かるくらいなら，他人に質問なんかしないだろうけどな．たしかに大学の講義には親切とは言えんところがある．定義すりゃいいだろうなんて調子だからな．

定義されても，それだけで分かるような親切なもんじゃないし．だがまた，それが大学らしくていいんだという気分も，少しはほしいって気もするが．

そう言えば，僕が大学に入ったころは，ブルバキが幅を利かせていたせいか，何もかもがそういう調子の講義だったな．

●大学数学は線形代数から

大学で受けた一番最初の講義が線形代数だった．いつ倒れても不思議がないくらいの古い木造校舎だったな．黒板の前に立った教授が,「ベクトルとは何か」という質問を学生にするところから始まったものだ．誰も答えないので，たまたま一番前に座っていた僕が指されて，仕方がないので高校で習った通りに答え

[1]［犬註］わが輩は先生の家の同居犬である．詳しく知りたければ本誌の 2000 年の 1 月号を見るがよい．

たわけだ．長さと向きのある...，と言いかけて困った．長さと向きのある何だったんだ？　言い淀んでいると，はにかむように先生は「ん，ベクトルというのは多次元の量なのだよ」と言葉を引き取ってくれた．そして，ベクトル空間の公理的定義が始まった．

$K = \mathbb{R}$ を実数の全体，V を集合とする．和と呼ばれる演算 $+ : V \times V \to V,\ (v, w) \mapsto v + w$ とスカラー倍と呼ばれる演算 $\cdot : K \times V \to V,\ (\lambda, v) \mapsto \lambda v$ があって，

1)	$u + (v + w) = (u + v) + w$	$(^\forall u, v, w \in V)$	結合律
2)	$u + v = v + u$	$(^\forall u, v \in V)$	交換律
3) $^\exists 0 \in V$	$0 + v = v = v + 0$	$(^\forall v \in V)$	零元の存在
4) $^\forall v \in V$	$^\exists w \in V$	$v + w = 0 = w + v$	逆元の存在
5)	$\lambda(\mu v) = (\lambda\mu)v$	$(^\forall \lambda, \mu \in K, ^\forall v \in V)$	結合律
6)	$1v = v$	$(^\forall v \in V)$	スカラー倍の正規化
7)	$(\lambda + \mu)v = \lambda v + \mu v$	$(^\forall \lambda, \mu \in K, ^\forall v \in V)$	左分配律
8)	$\lambda(u + v) = \lambda u + \lambda v$	$(^\forall \lambda \in K, ^\forall u, v \in V)$	右分配律

を満たすとき，V を K 上の線形空間と言う．V の元 v をベクトルと言い，K の元をスカラーと言う．K をまた係数体と言う．

淡々と黒板が埋まって行く．教室の中はエネルギーの高い静寂が満ちてきて，チョークの黒板を叩く音と，ノートに鉛筆の擦れる音だけが聞こえていた．実にスマートで恰好良かった．戦前からの老朽木造校舎とブルバキ風な公理的展開のモダンさとのアンバランスが，ぞくぞくするほど嬉しかった．大学に来たんだ，大学にいるんだ！

ブルバキの名前も知らなければ，使われている記号も分かっちゃいなかったが.」

陶酔する先生の様子にわが輩は少しあっけにとられていた．先生は昔からミーハーだったわけだ．え，ミーハーって何だって？

「自分でも講義をするようになるまで，線形代数が分かったという気持ちになれなかったが，こういう構成の講義だったからかも知れんな．公理的定義なんてのは，教師の側から言えば，こんなに楽なことはない．項目を少々忘れていても，書きながら説明していれば，思い出しても来るし，忘れてたことを学

生には知られないで済む．しかも，完全無欠，誰にも文句は言わせないってわけだ.」

いやはや，教師は楽な商売と見える．

「たしかに楽と言えば楽なんだが，それだけじゃないんだ．2 次元や 3 次元の実ベクトルならある程度は直観も効く．平行四辺形や平行 6 面体が自由に想像できればそれでもいい．だが，四次元以上になると直観は効きにくい．しかもスカラーを複素数にとることにしたら，もう駄目だろうね．そんなときには，この公理主義的定義というのは便利だ．というより，これ以外に術(て)がないわけだ．

力なんかの物理的な意味から，2,3 次元のベクトルの性質が分かる．その性質をまとめて公理的定義にしてみると，物理的な計算にはその性質しか使わないことが分かる．そこまではただの便利だね．だけど，相対論もあることだから 4 次元は必要となり，もっと高次元での計算が簡単なら，高次元の空間を使って表わすほうが便利な（物理）現象もある．そこで，エイヤッと，任意次元のベクトルを定義してしまう．そのとき，重要なのは任意次元のベクトルを直接定義するんじゃなく，任意次元の線形空間を（公理的に）定義して，その元をベクトルと呼ぶことなんだ．つまりね，個々のベクトルを定義せず，無定義用語としてのベクトルをその関係概念だけで認識しようということなんだな．わかるか？」

あ，やっぱり我が輩相手に話していたつもりらしい．こんな風に理屈に陶酔している先生には逆らわないことだ．とりあえず，一声ワンとないておこう．

ともかく定義を

「わかるわけないか．で，まあ，スカラーを複素数まで広げると，単にスカラーの集合というわけにはいかなくなる．実数も複素数もそれぞれ体になっていて，体であることが線形代数の計算に重要になる．定義の式から見て，任意の体上の線形空間も同じように定義できる．だけど，当然のことだが，体が変われば，成り立つことも変わってくる．それが線形空間の個性というものだ．ともかくスカラーが重要だとなれば，それに名前を付けることになり，係数体という．係数体が F のとき，F 上の線形空間という.」

語尾に微妙な間が聞こえる．先生，大丈夫かな．で，合の手に，ワン．

「スカラーが体をなさない線形代数もできるが，この質問に答える程度じゃ，要らんだろう．お前もウルサイな．

ともかく，複素係数で考えるまでには，というか，行列式の議論をする頃には，そんなに重要な体の性質をはっきりさせとかなきゃ，不便で困る．そこで，大学1年の夏までには，体の定義をすることになってしまう．それを講義できる余裕のカリキュラムが走っていれば，群と環と体を順に定義して，その都度簡単な性質と例を示すというようにゆっくりやれば，下手をすると1年でも終わらない．

時間がないときは，ともかく体の定義をしてしまうのがてっとり早い．裏技めいて気が引けるが，覚えるならこの方が楽だ．

集合 K に2種類の2元算法 $+ : K\times K \to K,\ (x,y) \mapsto x+y$ と $\cdot : K \times K \to K,\ (x,y) \mapsto xy$ があって，

1)	$x+(y+z)=(x+y)+z$	$(^\forall x,y,z \in K)$	結合律
2)	$x+y=y+x$	$(^\forall x,y \in K)$	交換律
3) $^\exists 0 \in K$	$0+x=x=x+0$	$(^\forall x \in K)$	零元の存在
4) $^\forall x \in K$	$^\exists y \in V$	$x+y=0=y+x$	逆元の存在
5)	$x(yz)=(xy)z$	$(^\forall x,y,z \in K)$	結合律
6)	$xy=yx$	$(^\forall x,y \in K)$	交換律
7) $^\exists 1 \in K$	$1x=x=x1$	$(^\forall x \in K)$	単位元の存在
8) $^\forall x(\neq 0) \in K$	$^\exists y \in K$	$xy=1=yx$	逆元の存在
9)	$(x+y)z=xz+yz$	$(^\forall x,y,z \in K)$	左分配律
9′)	$x\,(y+z)=xy+xz$	$(^\forall x,y,z \in K)$	右分配律

を満たし，$0 \neq 1$ のとき，K を「体」と言う．$0 \neq 1$ という条件は重要で，$0=1$ だと，上の条件から $K=\{0\}$ となってしまう．それは詰まらない．

6) を満たさないとき「斜体」と言う．斜体が有効な分野もあって，そういうときには，斜体を単に「体」と呼び，上の意味での体を「可換体」と呼ぶ．

6) があるから，9) から 9') が出るが，6) のないときは（つまり斜体のときは）9') は別に定義に入れておく必要がある．そう呼ぶ必然性はないが，習慣上便利だから，$+$ を加法と呼び，$\cdot$ を乗法と呼ぶ．

さて，そこで，8) 以外は満たす集合を「可換環」と呼ぶ．6) と 8) 以外を満たす集合を単に「環」と呼ぶ．6) を満たさないことが強調したい場合には「非可換環」と言う．

7) を満たさない代数系を考えることもあるので，そういう場合には単に環と呼んで，7) を満たす場合を強調して「単位元を持つ環」とか「単位的環」と言う．

算法が 1 つしかなくて，そのときは必ずしも $+$ で書く必要はないが，1), 2), 3), 4) を満たす集合を「可換群」とか「アーベル群」と言う．そのとき特に演算を $+$ で書くときは「加法群」と言う．

1), 3), 4) を満たす集合を単に「群」と言う．2) を満たさないとき，演算は $+$ で書いてはいけない．

1) を満たす集合を「半群」と言い，1), 3) を満たす集合を「単位的半群」と言い，1), 2) を満たす集合を「可換半群」と言う．

さらに，結合律をゆるめた「準群」もある．」

わが輩は聴いているだけでしっかり疲れた．先生という種族はこういうことには疲れないものなのだろうか．

定義の陰には周知の事実がある

「定義を見て気になることがいくつかあるだろう．3) や 7) で単位元が存在するとあるがいくつもあるかも知れない，4) や 8) での逆元だってそうだ．1 つしかないと言わなくてもいいのだろうか．それは，言う必要がないんだ．そうなってしまうから．

たとえば，$0'$ が 3) の性質を満たすとすれば，$0 = 0 + 0' = 0'$ というわけ．乗法の方も同じ．逆元も，x に対して 4) を満たす元が 2 つ y, y' とあったとすれば．$x + y = 0$ の両辺に左から y' を足せば，左辺は $y' + (x + y) = (y' + x) + y = 0 + y = y$ で，右辺は $y' + 0 = y'$ となり，$y = y'$ となるからね」

我が輩が聴いてやっているというのに，自分で質問して，自分で答えている．まったく，2 重人格というか，精神分裂というか，こうでないと先生をやってられないのなら，我が輩はお断りだ．真っ当な犬生を生きて行きたいじゃないか．

「たとえば，半群の場合，左単位元というものが考えられる．任意の x に対して $1x = x$ を満たすものと定義するのだが，これだと無限に多くの左単位元があったっていい．同じように右単位元というものも一意的とは言えない．ところが，上の証明をじっと見ればわかるが，1 つの代数系に右単位元と左単位元が存在することになると，この多義性が凝縮して，右単位元は左単位元でもあり，両側単位元，つまり通常の意味の単位元になってしまう．

逆元でも，左逆元や右逆元が定義できて，同じことが言える．そんなわけで，3), 4), 7), 8) では，不必要に見える（実際に可換なら不必要だが）等式が書いてある．

たとえば R が環で，x に左逆元 y, y' があったとする．つまり，$yx = 1 = y'x$ だな．左分配律から $(y - y')x = 1 - 1 = 0$ になる．$y \neq y'$ だから，0 でない元の掛け算で 0 が出てくることになる．こういう元を「零因子」と言う．

0 の約数ということだな．英語じゃ，約数も因数も因子も区別はない．どれも factor だ．区別したがるのは，日本文化の幼児性なのかもしれん．山ほど数詞があるのとおんなじで,「因」と言うだけじゃ，落ち着かない.「数」なのか，もっと抽象的な何かなのか，はっきりしてほしいという,... 気分かな．

ともかく，体ならありそうもないわけで，その根拠は逆元の存在だ．それは実際，簡単に証明できる．体には零因子がない．

内算法しかない（抽象）代数系はこんなものだが，外算法も考慮するなら，加群や代数も重要だ．最初に挙げた K 上の線形空間の定義は，K 加群の定義そのものだ．有限次元の線形空間は次元が同じなら同型になって，つまり，次元が n なら数ベクトル空間 K^n と同型なわけだ．この空間上のすべての線形写像の全体は，K を係数とする n 次正方行列の全体で $M_n(K) = M(n; K)$ などと書かれるが，これが K 代数になる．

K はスカラー．K 代数は，K 加群に積を導入したものと言ってもよいし，環にスカラー倍を定義したものといってもよい．本によっては K 代数のことを

K 多元環とも言う.」

そんなこと，定義だけで分かれって言うの？　凄まじいね．これだけ話が進んでも，定義だけなんだよ．先生という種族は，疲れも飽きも感じないのかねぇ．我が輩の知ったことじゃないが...

まず例より始めよ

「一般論的には，同型の概念と，既知のものから新しいものを作る方法へと進むのだが，手短に済まそうと思えば，そろそろ例をやらないといけない．学生が飽きるからな.」

聴衆のことも気にかけてはいるんだ...

「体は何より実数を表わすためにあるようなものだが，まず，体の定義だけでどこまで迫れるかを見てみよう.

0 と 1 がある．$+$ と $\cdot$ をやって新しいものが出るのは $1+1$ だけで，これを 2 と呼ぶ．$0,1,2$ でやっても，$2+1=1+2$ しか新しいものはなく，これを 3 と呼ぶ．n に 1 を足して $n+1$ を作ることを順にやっていけば，数学的帰納法で自然数の全体 $\mathbb{N}$ が得られる．$\mathbb{N}$ 全体に自然に $+$ と $\cdot$ が定義できる．が，これは $+$ に関しても $\cdot$ に関しても単位的可換半群にしかならない.

元が足らない．$+$ に関して逆元をすべて追加すると，整数全体の集合 $\mathbb{Z}$ が得られる．$+$ に関しては可換群，$\cdot$ に関しては単位的可換半群，で，可換環になる．それを忘れないように，$\mathbb{Z}$ はいつも「整数環」という方がよい.

$\mathbb{N}$ に $\cdot$ に関する逆元を付け加えると，非負の有理数の全体 $\mathbb{Q}_+$ になる．$\cdot$ に関しては可換群，$+$ に関しては単位的可換半群，だが，可換環ではない．分配律が成り立たないからだ．可換群になっている演算の方で分配しないといけないので，$x+(yz)=(x+y)\cdot(x+z)$ が要求される．が，これは成り立たない.

$\mathbb{Z}$ に $\cdot$ に関する逆元を付け加えると，有理数の全体 $\mathbb{Q}$ が得られるが，これでやっと体が得られるわけだ．忘れないように $\mathbb{Q}$ を「有理数体」と呼ぶ.

ここまでの構成は，代数では標準的な議論で，たとえば「付け加える」という言葉も何度か使ったが,

それぞれの場合に，それぞれきちんとした定義がある．それを学生に話すこともあるが，覚えて欲しいってわけじゃない．日常的な言葉でふわっと述べた事柄にも，厳密な裏づけがある，と言うか，あり得るということなんだが，面白くないのかなあ．

ま，分数を作って「商体」を定義する操作より，たとえば $\mathbb{Z}$ を作るときに，直積集合 $\mathbb{N}\times\mathbb{N}$ に $+$ を定義して，さらにそれと同調する同値関係を導入して，それで割るときちんと環の構造が得られるというあたり，実に堅牢なゴチックというかガウディ的な建築物が組み上がって行くようで....」

ちょっと陶酔し過ぎる．ゴチックだのガウディだの，話が滑らか過ぎてウソっぽい．ここらで一つ，ワン．も一つ，ワン，ワン．

「何だ，クレームか？　数学は分からんくせに，鼻の利く奴だ．

実数に進む前にちょっと反省！　$1+1$ が新しいと言ったあたり，たしかに勇み足．そのあたりの議論が正しければ，任意の体は $\mathbb{N}$ を含み，自動的に $\mathbb{Z}$ も $\mathbb{Q}$ も含むことになる．

何がいけなかったか？　答えを言ってから質問をするようなもんだが，うちの学生あたりだとこれ位しないと分かっちゃくれん．何？　しても分からないだろうって？　失敬な！　そんなことは言っちゃおらん．

環や体が自動的に $\mathbb{N}$ を含むわけではないが，$\mathbb{N}$ 加群にはなる．だから，$\mathbb{N}$ 代数にもなる．そこで，$n\in\mathbb{N}$ に対して，$n1$ がいつでも 0 にならないという保証がない，ということだ．ここで，体に零因子がないことに矛盾しないか，気になるところだが，外算法だから矛盾ではない．つまり，$n\notin K$ だから，構わないんだ．

そこで，$n1=0$ となることが起る場合があるということだ．体 K で考えることにすると，$\varphi:\mathbb{Z}\ni n\mapsto n1\in K$ は準同型だが単射とは限らないということである．核 N は $\mathbb{Z}$ のイデアルで，もちろん正規部分群でもある．$\mathbb{Z}$ の加法群としての（0 でない）部分群は $p\mathbb{Z}$ $(p\in\mathbb{N}\setminus\{0\})$ という形であることが分かるので，上の準同型は商準同型 $\bar{\varphi}:\mathbb{Z}/p\mathbb{Z}\to K$ を導く．

ここで，p が素数であることも分かる．$p=k\ell$ だ

とすると，$0 = \varphi(p) = \varphi(k\ell) = \varphi(k)\varphi(\ell)$ となるが，p の最小性から $\varphi(k), \varphi(\ell) \neq 0$ だから K に零因子があることになり，矛盾．

p が素数なら，商環 $\mathbb{Z}/p\mathbb{Z}$ にも零因子はなく，体になる．これを F_p と書いて標数 p の素体と言う．元の体 K も標数 p と言う．$\mathbb{Q}$ の時は，$N = \mathrm{Ker}\,\varphi = \{0\}$ となるわけで，$N = p\mathbb{N}$ と書くなら，$p = 0$ となるので，標数 0 と言う．

普通は標数 0 だけ考えていればよい，と言っては居られない時代になっている．コンピュータの発達で，$p = 2$ は基本だし，一般有限標数の計算が楽に行えることになったため，色んな応用も生れている．が，当面，勉強するのはまず，標数 0 で感じを掴んでからの方がいいだろう．」

息つく暇もない．喋ってる方は快感だろうが，聴いてる方は堪らん．でもまだまだ入り口だ．これからどうするつもりだろう...

「普通は有理数体 $\mathbb{Q}$ から実数体 $\mathbb{R}$ や複素数体 $\mathbb{C}$ へ拡張するのだが，今は止めておこう．$\mathbb{Q}$ から $\mathbb{R}$ へは完備化というか連続体化というべきもので，有理数の間の隙間を埋める作業で，極限操作が自由にできるようにするためのものだ．解析や位相の問題といった方がよい．$\mathbb{R}$ や $\mathbb{C}$ では，$+$ と $\cdot$ は連続になっているが，逆元をとる操作も連続で，そういう体を「位相体」と言う．

大きくすればよいわけじゃなく，$\mathbb{C}$ を含む局所コンパクトなハウスドルフ位相体が存在しないことが知られている．可換を捨てれば四元数体 $\mathbb{H}$ にまでは拡張できるが，実 8 次元のケイリー代数 $\mathcal{C}a$ まで広げると，$\cdot$ の結合律さえ成り立たない.」

説明のない言葉が乱舞するようになったな．さすがに先生もお疲れなご様子だ．

「$\mathbb{C}$ は $\mathbb{R}$ の代数的閉包だが，虚数単位 i を付け加えただけとも考えられる．$\mathbb{R}$ 上の線形空間として 2 次元で，1 と i が基底になっている．$\mathbb{C} = \mathbb{R} + \mathbb{R}i$ とも書かれる．$\mathbb{R}$ 上の多項式環 $\mathbb{R}[x]$ の $x^2 + 1$ で生成されるイデアルによる商環を考えると，それが体でもあったとも言える．

多項式環 $\mathbb{R}[x]$ 自身の商体は有理関数体 $\mathbb{R}(x)$ だか

ら可換体なんだが，無限次元になっている．もう代数というより，関数の世界の話だな．

代数的なことだけなら，$\mathbb{Q}$ で考えても同じだ．$\alpha \in \mathbb{C}$ が（$\mathbb{Q}$ 上）代数的なら，$\mathbb{Q}$ に α を添加した体 $\mathbb{Q}(\alpha)$ は有限次元だが，超越数なら無限次元になる．$\mathbb{R}$ を $\mathbb{Q}$ 上のベクトル空間と見ると，これは大変で，基底を選ぶことも難しい.」

また脱線してるよ．

「一応，群論，環論，体論と言って，それぞれのタイトルでたくさんの本が書かれている．が，互いに絡み合っていて別々のやれるというものではない．群の研究をすすめようとすれば，加群も環（代数）も必要になる．もっとも基本的な非可換群である対称群も，代数方程式の可解性と関連して体の拡大との対応で数学的な価値が定まったとも言える．環からは体を作れるかどうかを問うのが基本問題だし，加群の写像列からホモロジー群やコホモロジー群が作られる．

体の（代数）拡大の理論はまた代数関数の理論でもあり，複素関数論とも関係し，リーマン面の理論へ，代数多様体の理論へと広がって行く．

代数も幾何も解析もみな絡まり合っている．何かだけとり出して，これだけ勉強すればよい，ということはない.」

….. もう止めようもない．お題のことを忘れてしまったようだ．

●この後は本で

「ふぅう，何を言ってるのか分からなくなってきたぞ．代数/群・環・体を説明するとなると，せめて本が 1 冊必要だな．定義から厳密に構成されているのが好きなら，ファン・デル・ヴェルデンの『現代代数学』(銀林浩訳，東京図書) だろうし，意味に興味があって，沢山の例が知りたければ I.R. シャファレヴィッチ『代数学とは何か』（シュプリンガー・フェアラーク東京）がいいだろう．シャファレヴィッチが言ってることだが，本は初版がよい．版を改訂していくと，正確さは増して行くが，著者のパッションが失われていく.」

ブルバキの手本になったファン・デル・ヴェルデン

と，ブルバキ主義とは対極にあるシャファレヴィッチを挙げるなんぞ，思想ってものがあるのかね．

「あーあ，困った．口で言えばこうなんだが，どういう書けばいいかまるで分からん．質問が届かなかったことにして，返事をしないでおこうかな...」

どうやら，頭棲先生の，頭の中に棲んでいる怠け虫がまた活動を始めたらしい…

よこがお

専門は表現論.

http://www.com.mie-u.ac.jp/~kanie/tosm/

円周率の 3 は論外だが，これまでの文教政策に従っていては，数学を愛する心が若い人たちに育ちそうもない．この所，多くの時間をとられている良い数学の輸入にしても，読者が育たなければ困ってしまう．

だから，公教育とは別に，初等数学教育のあり方と教材についても考えてきた．少しは論文風の発表もしたが，成書を作らないと普及は覚束ない．と言って，怠け者．で，時に触れて，自分を拘束する約束をしている．力学グラフの本を書くぞ !!!