

環 (かん)

Joh @物理のかぎプロジェクト

2006-05-27

環と呼ばれる代数構造も大事なものです。環は英語やドイツ語で *ring* ですので、頭文字をとって R で表わすことが多いようです。環には加法と乗法の二つの演算が与えられますので、群よりは強い構造です。しかし、乗法に逆元や単位元は必ずしも必要ないので、体よりは弱い構造だと言えます。

群や体と比較しつつ、環とはどのような構造なのかを見ていきましょう。

環の公理

以下の条件を満たす集合を環と呼びます。

1. 加法について可換群になっています。(加法が閉じており、単位元 0 、逆元 $-a$ があります)。
加法の単位元を特に 零元 と呼びます。
2. 結合則を満たす乗法があります。
3. 加法と乗法について分配法則がなりたちます。 $(a + b)c = ac + bc$, $a(b + c) = ac + bc$

環は、加法については群になっていますが、乗法については群になっていません。[半群](#) を知っている人ならば『環は加法について可換群、乗法について半群である』と覚えてもいいでしょう。

幾つかの例

例 1：整数環

有理数、実数、複素数、四元数は全て体をなしましたが ([体](#) を参照)、整数は割り算について閉じておらず、体にはならないのでした。

しかし、整数の全体 $\mathbb{Z}$ は加法に関しては群になりますし、乗法も閉じおり、結合則を満たします。そこ

*1 乗法の演算について結合則を満たすことにしましたが、結合則は必ずしも必要ない考える人もいます。例えば、八元数 (ケーリー数ともいう) という、八次元の超複素数の集合は結合則を満たしませんが、環に似た構造を持ちます。これを環だと言い切ってしまう流派の人もあるようです。しかし、これはあまりにも例外的な例です。とりあえず普通は結合則もなりたつものだと思います、あまり気にせず先へ進んでください。教科書によっては、はっきりと乗法の結合則を環の公理に明記していますので、ここでもそのようにしました。

で整数全体は環になります．これを 整数環 と呼びます．

環の乗法には単位元が存在しなくても良かったので，単位元が存在する環を特に 単位元を持つ環 と区別して呼ぶことがあります．整数環は単位元を持つ環です．

例 2：全行列環

実正方形行列の全体は，加法に関して群になりますし (零元は零行列

$$\begin{pmatrix} 00 \\ 00 \end{pmatrix}$$

です)，乗法の結合法則も満たすので環になります．そこで， $n \times n$ 実正方形行列の全体を， R 上の n 次全行列環 と呼びます．この R は実数体の意味の R です．

以下は，今すぐ重要なことではありませんが，環の興味深い性質に関わる事柄なので補足しておきます．例えば R 上の 2 次全行列環の乗法を考えましょう．いま行列

$$A = \begin{pmatrix} 10 \\ 10 \end{pmatrix}, B = \begin{pmatrix} 00 \\ 11 \end{pmatrix}$$

はどちらも零行列ではありませんが， $AB = O$ となります．このように，どちらも零ではないものの積が，環上では零になることがあります．これを 零因子 と呼びます．

また $BA \neq O$ にも注意してください．積の順番によっても答えが変わってくるのです．(そこで左右を区別して， A を B の 左零因子 だと言います．もしくは B を A の 右零因子 と言うことも出来ます．)

例 3：準同型写像の集合

加法群 M を加法群 M に移す自己準同型写像の全体集合 R を考えます． R の二つの元 f, g に対し，加法を $(f + g)(x) = f(x) + g(x)$ ，乗法を $(f \circ g)(x) = f(g(x))$ と定めれば R は環になります．

加法の零元は， M の各元を 0 に移す写像 f_0 です．下の二式を確認してください．

$$(f + f_0)(x) = f(x) + f_0(x) = f(x) + 0 = f(x)$$

$$(f_0 + f)(x) = f_0(x) + f(x) = 0 + f(x) = f(x)$$

加法の逆元は， M の各元 x を $f'(x) = -f(x)$ に移す写像です．

$$(f + f')(x) = f(x) + f'(x) = f(x) - f(x) = 0$$

$$(f' + f)(x) = f'(x) + f(x) = -f(x) + f(x) = 0$$

環の歴史

整数全体は環になるということでしたが，そもそも環という概念自体が，整数を一般的に拡張したものです．『加法については可換群だけど乗法には逆元が無い』なんていうアンバランスな定義も，整数のことを念頭に置けば納得がいくと思います．環の定義を忘れそうになったら，整数を思い出しましょう．しかし最初の人には，何が嬉しくて整数を抽象化するようなことを始めたのでしょうか？

ラグランジュ (Joseph-Louis Lagrange (1736-1813)) やガウス (Johann Carl Friedrich Gauss (1777-1855)) による整数の合同式の研究から，最初に環の概念が生まれてきたと考えられます (整数の剰余類は **イデアル** の記事で勉強するように環になります) ，環論を大きく発展させた動機の一つが，有名な『フェルマーの最終定理』を解決しようという試みです．フェルマーの定理と環は切っても切れない関係にあり，環の歴史には，超大物数学者の名前がたくさん出てきます．少し長くなりますが，その歴史を概観してみましょう．

フェルマーの最終定理とは，フェルマー (Pierre de Fermat (1601-1665)) が 1630 年頃に考えたと言われる『3 以上の整数 n に対し， $x^n + y^n = z^n$ を満たす整数 x, y, z の組は存在しない』という有名な問題で，1995 年にワイルズ (Andrew John Wiles (1953-)) によってようやく証明されたものです．フェルマー自身は，本の余白に『驚くべき証明を見つけたが，ここには書き込む余白がない』と書き残したそうです．フェルマーの最終定理の証明には現代数学の粋が集められており，本の余白がたとえ十分大きくても，フェルマーが証明できたとは思えません．おそらく負け惜しみか，勘違いだったでしょう．

その後 $n = 3, 4, 5, 14, 7$ の場合がフェルマー，オイラー (Leonhard Euler (1707-1783)) ，ルジャンドル (Adrian-Marie Legendre (1752-1833)) ，ディリクレ (Johann Peter Gustav Lejeune Dirichlet (1805-1859)) ，ラメ (Gabriel Lamé (1795-1870)) 等によって個別に証明されていきました．オイラーはこの過程で， $n = 3$ の場合の証明を $n = a + ib\sqrt{3}$ の場合にまで拡張して考えてみました．ここで，読者のみなさんは $a + ib\sqrt{3}$ の形をした数 (a, b は整数とします) の全体が，環を作ることを確認してください．



図 1 (フェルマーの最終定理で有名なフェルマー．本職は医者だった．)

その後，ラメがフェルマーの最終定理の証明に成功したと発表し，ラメ，コーシー (Augustin Louis Cauchy (1789-1857))

*2 単なる恒等写像 e も R の元のはず (M の元をそのまま M に移す) なので， R には e が含まれ， e と他の写像との合成には $ef = fe = f$ がなりたちます．つまり R は『単位元を持つ環』だと言えます．

), リュービル (Joseph Liouville (1809-1882)) 等の間でその証明について議論が起こりました．議論の末，ラメの証明が正しいかどうかの要点は『通常の素因数分解を $a + ib\sqrt{3}$ の形の数にまで拡張した場合，果たして一意的に素因数分解が決まるといえるのかどうか』という一点に絞られてきました．

素因数分解の概念を通常の整数より広げると，その一意性は必ずしも自明ではありません．例えば 4 は通常の有理整数の範囲では $4 = 2 \times 2$ と，一意的に素因数分解できますが，複素数にまで考える範囲を広げれば $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ のような他の分解も可能です．

その後，クンマー (Ernst Eduard Kummer (1810-1893)) は，必ずしも $a + ib\sqrt{3}$ の形の数による素因数分解は一意的でないことを示し，ラメの証明は否定されました．フェルマーの定理の証明は振り出しに戻りました．クンマーは， $n = a + ib\sqrt{3}$ の形の数による素因数分解が一意的に決まらない理由は，分解の仕方が不十分なためではないかと考えました．例えば 24 は $24 = 2 \times 2 \times 2 \times 3$ と一意的に素因数分解できますが，途中で素因数分解をやめてしまうと $24 = 8 \times 3$ と $24 = 6 \times 4$ のように，異なる因数分解の仕方が可能です．有理整数の範囲では一通りに $4 = 2 \times 2$ のように決まった素因数分解が，複素数まで数の概念を広げると $4 = (1 + i\sqrt{3})(1 - i\sqrt{3})$ のようなものも現われてきましたが，一般に数の概念を広げていくと，今まで出来なかった素因数分解の可能性が広がっていきます．そこで，数の概念を行き着くところまで広げ，とことん因数分解を行っていけば，いつか素因数分解が一通りに決まる数に行き着くのではないかと考え，これを理想数 (*idealnumber*) と名づけました (理想数については [イデアル](#) の記事でまた触れます) ．



図 2 (講義中，三掛ける七を忘れてしまって学生に聞いたというクンマー．計算が苦手でも数学者にはなれる．)

クンマーは，初等整数論の延長として理想数を考えただけでしたが，後にデデキント (Richard Julius Wilhelm Dedekind (1831-1916)) によって，クンマーの理想数 (*idealnumber*) はイデアルという抽象概念にまで高められ，有理整数における素数は，素イデアルという概念に，素因数分解はイデアルを素イデアルに分解することにまで抽象化されました．イデアルは次に勉強しますが，一種の部分環ですので，普通の教科書では環を定義したあとにイデアルが出てきます．しかし，歴史的には逆で，素因数分解論の拡張としてイデアルの抽象化の方が先に進んだようです．

環という奇妙な用語はドイツ語の *Zahlring* (数の輪の意味) から来ており，英語では *ring* ，フランス語では *anneau* と，各国語でもリングを直訳した用語が使われています．この命名者はヒルベルト (David Hilbert (1862-1943)) です．ヒルベルトは $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ という形をした数の集合を考ましたが， $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ に $\sqrt[3]{2}$ を一回掛けると $2c + a\sqrt[3]{2} + b\sqrt[3]{4}$ になり，二回掛けると $2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}$ にな

*3 ガウスは $a + ib$ (a, b は整数) の形の数による素因数分解は一意的であることを証明し，1 の三乗根である $\omega = \frac{1+i\sqrt{3}}{2}$ を使った $a + b\omega + c\omega^2$ という形で表わされる数による素因数分解も一意的なことを証明されました． ω を使った素因数分解が一意的であることを使って， $n = 3$ の場合のフェルマーの定理を示すことができます．なお，素因数分解という用語を有理整数以外に使うのは少し不正確ですが，ここではあまり細かな用語には拘らないことにします．

り，というように，この操作を続けていくと (a, b, c) の位置がグルグル回っているように見えることが輪のようだと思い，このように命名したのだということです．



図 3 (20 世紀最大の数学者の一人・ヒルベルト)

この辺りの話題の内容は，もう少し勉強を進めて，代数的数，超越数，体の拡大などの概念が分かってくると，もう少し見通しよくなり，面白くなってきます．