イデアル

Joh・丹下@物理のかぎプロジェクト

2006-05-27

イデアルは部分環の一種ですが，とても重要な概念ですので，わざわざ記事を一つ設けました．しかし，この後しばらくは体論をやりますので，イデアルの概念を使う内容は当面出てきません．

それでも，ざっと考え方に触れておくと良いと思います．

イデアルの定義

環 R の部分環 I が次の性質を満たすとき，I を **イデアル** と呼びます．

$$I \subset R$$

Important

環 R の任意の元 x と，I の任意の元 a に対し $xa \in I$ がなりたちます．

一般に環の乗法は非可換なので，ここで定義したイデアルを特に **左イデアル** と言います．逆に $x \in R, a \in I \longrightarrow ax \in I$ を満たすものを **右イデアル** と呼びます．イデアルが，左イデアルと同時に右イデアルでもあるとき，これを **両イデアル** もしくは単にイデアルと呼びます．

イデアルは既に部分環なので，加法に関しては環 R の部分群になっています．乗法の条件が，すこぶる変わっています．『環 R に属するどんな元を取って来ても，イデアルの元との積はイデアルに含まれてします』というのですね．

例１

環 R の零元 0 はそれだけでイデアルになります．R のどんな元も，0 を掛ければ 0 になってしまいますし，0 だけで加法も乗法も作れるからです．環 R 自身も，イデアルになります．零元と環自身の二つは **自明なイデアル** と呼ばれます．自明なイデアル以外のイデアルを，**純イデアル** と呼んで区別する場合もあります．

---

*1 イデアルとはなんとも奇妙な名前です．英語では *ideal* と書きますので，英語式に発音すれば “アイディール” となります．日本語の用語はドイツ語の *Ideal* から入って来ていますので，「イデアル」と読むのです．ドイツ語の発音には旧制高校風の趣があり，私はなかなか好きです．

*2 積を取れば何でも自分の元になってしまう，という代数的性質を吸収律と呼びます．そのままの命名ですね．

例２

整数環 Z で，偶数全体からなる集合はイデアルです．偶数同士の和，偶数同士の積は偶数になり，偶数だけで部分環になります．さらに，偶数でも奇数でも，偶数を掛ければ偶数になりますから，イデアルの定義を満たしています．

一般に，整数環 Z で整数 m の倍数の全体 $[m]$ はイデアルになります．

例３

R上の多項式環 $R[x]$ で，$x=1$ を代入すると 0 になる多項式の全体 $I=\{f(x)|f(1)=0\in R[x]\}$ は，イデアルになります．確認してみて下さい．

単項イデアル

単位元を持つ環 R のある元 a を取り，R の全ての元 x_i に関して集合 $I=\{x_1a,x_2a,....,x_na,...\}$ を考えると，I は R の左イデアルになります．

実際，この I に R の任意の元 x_i を掛けてみると，x_ix_j という形の積が出てきますが，環が乗法について閉じていることから，これは何か一つの x_k に等しいはずで，$x_ix_ja=x_ka$ が成り立つはずですので，確かに I の元と任意の R の元の積は I に含まれます．

これを a **で生成された単項左イデアル** と呼びます．同様に $I=\{ax_1,ax_2,....,ax_n,...\}$ を a **で生成された単項右イデアル** と呼びます．単項イデアルのことを **主イデアル** と呼ぶ場合もあります．

元 a から生成されたイデアルを記号で (a) のように書くことにします．

$$(a)=\{ax_1,ax_2,....,ax_n,...\}=aR \tag{1}$$

環には加法と乗法があったわけですが，加法と乗法とで表わせる a と x_i の組合わせは，式 (1) で表わされるもので網羅されています．(x_i には 0 や 1 も含まれることに注意してください．)

例

整数環 Z で, ある素数 p を取ります．p から生成する単項イデアルは $I=\{,...,-3p,-2p,-p,0,p,2p,3p,...\}$ のように p の倍数全体からなる集合 $[p]$ になります．確かに，どんな整数も p の倍数を掛けたら p の倍

[*3] 定義と例の羅列だけでは，実感のある理解は難しいかも知れません．イデアルのような抽象概念には，使い慣れて実態が分かるようになってから，自分なりの解釈を加えていくものだと思います．例えば，集合と定義したイデアルが，慣れてくると一つの数に見えてきたりします．代数幾何をやっている人なら，イデアルによって一つの図形を思い浮かべるでしょう．このように，今後，勉強する分野によって色々なイメージが膨らむ可能性があり，咀嚼の仕方は人それぞれで良いのです．また，意味が分からなくなってしまったら，いつでも最初の定義に戻って考え直すことが出来ます．イメージを膨らまし過ぎて危険に陥っても，戻ってくるところ，つまり『定義』がある，というのは数学の素晴らしいところです．

数になってしまいますから，$[p]$ はイデアルになっています．

集合から生成されたイデアル

単項イデアルは一つの元から作ったイデアルでしたが，元を集合にまで拡張し，環 R の部分集合 $\{a_1, a_2, ..., a_n\}$ からイデアルを生成することを考えます．式 (1) から，次のように拡張できることが分かります．

$$(a_1, a_2, ..., a_n) = a_1R + a_2R + ... + a_nR \tag{2}$$

これを，集合 $\{a_1, a_2, ..., a_n\}$ から生成されたイデアルと呼びます．

図 1　(理想数を考え付いたクンマー)

体のイデアル

体のイデアルは自明なイデアル，つまり $\{0\}$ と体自身のみです．

theorem

体のイデアルは，自明なイデアル ($\{0\}$ と体自身) だけです．

*4 特に，整数環のイデアルは，整数 m の倍数集合 $[m]$ という単項イデアルだけからなります．全てのイデアルが単項イデアルであるような環を，単項イデアル環と呼びます．全てのイデアルが単項イデアルである整域は，単項イデアル整域と呼びます．このあたりの用語はごちゃごちゃしていますが，最初から全部覚えようとしなくても大丈夫です．

*5 ドイツの数学者クンマー (Ernst Eduard Kummer (1810-1893)) は，フェルマーの大定理に取り組み，砲弾の弾道計算にも功績を残しました．有理整数 (要するに普通の整数) を素数で素因数分解する仕方は，例えば $6 = 2 \times 3$ のようにただ一通りに決まりますが，代数的整数 (有理整数を係数とする代数方程式の解になる数．例えば $\frac{-1+\sqrt{3}i}{2}$ は $x^2 + x + 1 = 0$ の解なので代数的整数です) を使って素因数分解しても良いことにまで話を拡張すると，$6 = (1 + \sqrt{5}i) \times (1 - \sqrt{5}i)$ のようなものまで出てきて，一般には素因数分解の仕方が一通りには決まりません．有理整数の因数分解でも，きちんと最後まで素因数分解しなければ，$24 = 8 \times 3$ と $24 = 6 \times 4$ のように分解の仕方が一通りに決まりません．クンマーはこの例の類推に基づき，代数的整数を含めた素因数分解が非一意的になるものも，因数分解の仕方が不十分なためだと考え，とことん因数分解を行えば，代数的整数による素因数分解であっても一通りに決まる数に行き着くのではないかと考えました．つまり，数の概念を拡張して行けば，素数に相当する『これ以因数上分解できない数』に行き当たるだろうと考えたのです．クンマーはこれを理想数 ($idealnumber$) と名づけました．クンマーの研究自体は当時の数論の延長といったものでしたが，デデキントがクンマーの理想数を抽象的概念にまで拡張しました．その時にイデアルという名前をそのまま継承したのが，この奇妙な名前の由来です．この脚注で理想数の話題に深入りすることはできませんが，単項イデアルは整数に，単項イデアル以外のイデアルは理想数に対応し，整数の素因数分解の概念はイデアルを素イデアルに分解することに対応した抽象概念です．

proof

体 F のイデアル I が，0 以外の元 a を含むとします．どんな元を a に掛けても，その積はイデアルの定義によりイデアルの元になるのですから，a^{-1} を掛けると，$aa^{-1} = e \in I$ が要請されます．つまり単位元はイデアルに含まれることになります．すると，F の任意の元 x に対して，$ex = x \in I$ がなりたつはずですから，結局 $I = F$ となってしまいます．■

逆に，環が $\{0\}$ と環自身以外にイデアルを持たないとき，この環は体になります．この定理は環が体になる条件として重要です．

Important

環が自明なイデアル ($\{0\}$ と環自身) しか持たないとき，この環は体になります．

proof

環 R のイデアルが $\{0\}$ と R 自身のみだとします．すると任意の R の元 $a\ (\neq 0)$ に対し，a で生成された単項イデアル (a) を考えると，$a \in (a)$ より少なくとも $(a) \neq 0$ ですから，最初の仮定により $(a) = R$ となります．よって $e \in (a)$ となるはずで，必ず $aa' = e \in (a) = R$ となる a' が存在することになりますので，R は全ての元に対して乗法の単位元と逆元を持つことになり，体となります．■