標数

Joh @物理のかぎプロジェクト

2006-06-25

体の拡大に関連して，幾つか重要な概念や用語を紹介します．この記事の内容は，基本的には 素体 の続きです．

標数が零でない体ではちょっと不思議な計算が行われますから，体をより深く理解するには重要な概念だと思います．しかし，標数が零でない体を考えるのは，この記事と次の 分離拡大体 だけで，それ以降は基本的に標数が 0 の体ばかりを扱います．ですから，少し難しい部分もあると思いますが，ここで 100 %分からなくても大丈夫です．

先を急ぐ読者の人は，この記事と分離拡大体は読み飛ばしても大丈夫でしょう．

標数

体 F に，正の整数 m があり，任意の元 $a \in F$ に対して $ma = 0$ がなりたつとします．このような m で最小のものを **体の標数** と呼びます．

有理数体，実数体，複素数体では，このような m は 0 だけですから，これらの体の標数は 0 です．この定義だけでは，標数が 0 ではない体がどんなものか想像しにくいと思いますが，例えば 体 の例 7 で取り上げたブール体では，$1 + 1 = 0$ と演算を決めましたので標数は 2 になります．このように，整数の剰余体や，**剰余体に同型な体*** には，一般的に零でない標数があります．

素数 p に対する整数の剰余体 $Z_p = \{[0], [1], [2], ..., [p-1]\}$ の標数は p です．どの元に対しても，p を掛ければ $p[k] = [0]$ $(k = 1, 2, ..., p-1)$ がなりたつからです．逆に言えば，任意の素数 p に対して，標数

p の体が一つ存在します.

体の含む素体で決まる標数

体 F が素体 F_0 を含むとします. 素体 の記事の最後で『任意の体は唯一つだけ素体を含む』という定理を証明しました. つまり, ある体に対して, 素体が一つ決まります.

さて, もう一つ『任意の素体は, 有理数体 Q (標数 0) か, 剰余体 Z_p (標数 p) に同型である』という定理がありました. これらを使うと, **任意の体の標数は, 素体の標数で表せる** ことになります.

体の構造に関して, 素体, 標数など新しい概念が急に色々と出てきましたが, 次に紹介する定理によって, これらの概念が組み合わさり, 素体や標数が体の構造を特徴付けるのに重要な概念であることが見えてきます. 繰り返しになりますが, 体の拡大をベクトル空間だと見ると定理の意味が直観的に少し分かりやすくなると思います.

有限体の位数

元の数が有限である体を **有限体** と呼びます. 有理数体, 実数体, 複素数体などはどれも **無限体** ですので, いままで有限体はあまり出てきませんでした. 有限体になりたつ美しい定理を二つ紹介します. どちらも重要な定理です.

theorem

有限体 F の位数を $|F| = q$, 標数を p, 素体を F_0 とします. $[F : F_0] = n$ のとき, $q = p^n$ がなりたちます.

proof

素体は有理数体か剰余類体に同型ということでしたが, 有理数体は無限体ですので有限体の素体になるはずがなく, 素体は剰余類体に同型 $F_0 \sim Z_p$ ということになります. F を F_0 上のベクトル空間と見ることも出来ますので, $F = a_1F_0 + a_2F_0 + ... + a_nF_0$ のように表すと (これが $[F : F_0] = n$ の意味することなので当然ですが), $|F| = |F_0| \times |F_0| \times \cdots |F_0| = p^n$ が言えます. ■

有限体 F の標数を p とします. ここで $F^p = F$ が成り立つ場合, F を **完全体** と呼びます. 標数が 0 の体も完全体だとします.

---

*1 標数が零でない体上では, 要するに 1 を幾つか足していくと, m 回足したところで 0 になってしまうわけです. これは, 普通に知っている数の性質から言えば, 極めて異常なことです. このあと 分離拡大体 では, このような算法規則が方程式論に与える影響を考えます. やはり, 今まで慣れていた方程式の性質とは違うので, 少し驚くことと思います. しかし, ガロア理論の章では基本的に標数 0 の体しか考えません. 標数を考え出すと話が全てややこしくなりますから, 初学者の間は抽象的な理解を深めるための頭の体操程度に思って読む程度で良いと思います.

*2 素体は, 体の部分群の中で最小のものです. また, 前節で標数の定義として, 体の元 a にたいし, $ma = 0$ を満たす「最小のものを」標数とすると定義しました. この定義を『素体の標数を体の標数とする』と定義する立場だと読み換えることも出来ます.

theorem

有限体は完全体です．

proof

写像 $\phi : F \to F$ を $\phi(x) = x^p \ (x \in F)$ と定めると，これは単射の準同型写像となります．単射であることに注意すると，位数に関して $|F| = |\phi(F)| = |F^p| < \infty$ がなりたちますので，$F = F^p$ が言えます．■

例題

標数が零でない体上では，どのような計算がなりたつのかを少し見てみます．通常，$(x+y)^n$ を展開すると，二項定理を使って次のように書けるのは大丈夫ですね．

$$\begin{aligned}(x+y)^n &= x^n + {}_nC_1 x^{n-1}y + \ldots + {}_nC_{n-1}xy^{n-1} + y^n \\ &= \sum_{k=0}^{n} {}_nC_k x^{n-k}y^k\end{aligned}$$

$${}_nC_k = \frac{n!}{(n-k)!k!}$$

ところが，標数 $p\ (>1)$ の体上で $(x+y)^p$ を展開すると，二項係数 ${}_pC_k = \frac{p!}{(n-k)!k!}$ は，${}_pC_0$ と ${}_pC_p\ (=1)$ を除いて，分子に現れた p によって全て零になってしまいます．従って，標数 p の体上では，次の計算が成り立ちます．

$$(x+y)^n = x^n + y^n \tag{1}$$

まるで『のび太算』のような結果ですね．この結果は 分離拡大体 でまた出てきますので覚えておいて下さい．