体の自己同型写像

Joh @物理のかぎプロジェクト

2007-03-03

体 E から体 E 自身への同型写像を，**自己同型写像** と言います (参考). 体には加法と乗法がありますから，自己同型写像 $\phi : E \longmapsto E$ は次の二式を満たすものと定義できます.

$$\phi(\alpha + \beta) = \phi(\alpha) + \phi(\beta)$$

$$\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$$

つまり，ここで考えているのは，加法群としての E の自己同型写像と，乗法群としての E^* の自己同型写像を，どちらも保つように一つに併せたものです.

自己同型写像の群

二つの自己同型写像 ϕ, ψ の合成写像 $\phi\psi$ は，やはり自己同型写像になります. また，自己同型写像の逆写像も自己同型写像です. そこで，全ての元を自分自身に移す自己同型写像 (つまり恒等写像) を単位元とすれば，E の **自己同型写像全体は群をなします**.

この群を $\mathcal{G}(E)$ と書きます.

特に，自己同型写像 ϕ が E の部分体 F を動かさないとき，すなわち $\phi(a) = a$ $(\forall a \in F)$ が成り立つとき，F を E の **固定体** と呼びます.

反対に，E の部分体 F を不動に保つ自己同型写像の集合 $\{\phi_1, \phi_2, ..., \phi_n | \phi_1(a) = \phi_2(a) = ... = \phi_n(a) = a \ (\forall a \in F)\}$ は，$\mathcal{G}(E)$ の部分群となります. これを $\mathcal{G}(E/F)$ と書くことにします. $\mathcal{G}(E/F)$ は F の 固定部分群 になっているわけです.

}

自己同型写像の一次独立・一次従属

体 E の自己同型写像 $\{\phi_1, \phi_2, ..., \phi_n\}$ が，E 上次式を満たす場合を考えます.

$$c_1\phi_1 + c_2\phi_2 + ... + c_n\phi_n = 0$$

この式が成りたつのが $c_1 = c_2 = ... = c_n = 0$ の場合だけならば，ϕ_i は E 上 **一次独立** だと言います. 逆に，上式を満たす $c_i \neq 0$ が存在するとき，ϕ_i は E 上 **一次従属** だと言います.

この用語は線形代数からの便宜的な借用で，実際に ϕ_i をベクトル空間の元だとは考えない方が良いと思います．**一次独立な自己同型写像は，相異なる** ということだけ覚えておきましょう．

重要な定理

体の自己同型写像を元とする群を考えました．何でこんな変チクリンな群を考えるのでしょうか？実は，この群を考えると，次に示すように，いままで別々に勉強してきた群論と体論の間に密接な関係が見えてくるのです．ここでは定理を二つ示しますが，最初の定理は二個目の定理を示すための補題です．とても大事な定理なので，少し長くなりますが証明も考えてみてください．

lemma

体 E の相異なる n 個の自己同型写像 $\phi_1, \phi_2, ..., \phi_n$ が，E の部分体 F を動かさないとき，$[E:F] \geq n$ が言えます．

proof

背理法を使って示します．仮に $[E:F] = r < n$ とし，E を F 上のベクトル空間と見たときの基底を $\{\sigma_1, \sigma_2, ..., \sigma_r\}$ とします．これらを使って，r 本の連立一次方程式 $(\phi_1\sigma_i)x_1 + (\phi_2\sigma_i)x_2 + ... + (\phi_n\sigma_i)x_n = 0$ $(i = 1, 2, ..., r)$ を考えます．この方程式系は，n 個の未知数 x_j $(j = 1, 2, ..., n)$ に対して式が r 本しかありませんので，x_j は一次独立ではなく，非零解 $x_j = c_j$ が存在します．一方，E に含まれる任意の元 α は，適当な係数 a_i と基底 $\{\sigma_1, \sigma_2, ..., \sigma_r\}$ の線形結合で $\alpha = \sum_{k=1}^{r} a_k\sigma_k$ の形に書けますが，任意の α に対して，c_j $(\neq 0)$ を $(\phi_1\alpha)c_1 + (\phi_2\alpha)c_2 + ... + (\phi_n\alpha)c_n = 0$ となるように選べます．（c_j の中に 0 があっても構いませんが，全て 0 ということはありません．なぜなら $\phi_j\alpha$ が一次従属だからです．）そこで，$0 = \sum_{j=1}^{n}(\phi_j\alpha)c_j$ という式を考えてみると，これは次のように変形できます． $0 = \sum_{j=1}^{n}(\phi_j\alpha)c_j = \sum_{j=1}^{n} c_j[\phi_j(\sum_{k=1}^{r} a_k\sigma_k)] = \sum_{k=1}^{r} a_k(\sum_{j=1}^{n} c_j(\phi_j\sigma_k))$. **ここで，左辺 $= 0$ より，$\sum_{j=1}^{n} c_j(\phi_j\sigma_k) = 0$ $(k = 1, 2, ..., r)$ が要請されますが，これは ϕ_i が一次従属という主張に他なりません．これは仮定に反しますので，$[E:F] = r \geq n$ でなければなりません．■**

自己同型写像の群，固定体など，目新しい話題が出てきましたが，次の定理はこれらの間になりたつ，驚くほど美しい結果の一つです．先ほどの定理は，この定理の証明に使うために紹介しました．いままで別々に勉強してきた群と体が，互いに密接に関係していそうだという衝撃の事実を，よく感じてみて下さい．

theorem

体 E と，E の自己同型写像の群 G を考えます．G に対する E の固定部分体を F とするとき，$[E:F] = |G|$ が成り立ちます．

*1 ガロア理論とは，正規部分群の列と正規拡大体の列の間にある密接な関係に関するものです．群論と体論は，既習の範囲ではあまり関係なさそうに見えたわけですが，これから，その隠された関係に肉迫していきます．この記事の定理は，そのための第一歩です．

proof

背理法を使って示します．仮に $[E:F]=r>n$ **とし，**$G=\{\phi_1,\phi_2,...,\phi_n\}$ **だとします．また，**E **を** F **上のベクトル空間と見たときの基底を** $\{\sigma_1,\sigma_2,...,\sigma_r\}$ **とします．これらを使って，**n **本の連立一次方程式** $(\phi_j\sigma_1)x_1+(\phi_j\sigma_2)x_2+...+(\phi_j\sigma_r)x_r=0\ (j=1,...,n)$ **を考えます．この方程式系には，**r **個の未知数** $x_i\ (i=1,2,...,r)$ **に対して式が** n **本しかなく，未知数が** $r-n$ **個余計です．よって，**x_i **は一次独立ではなく，非零解** $x_i=c_i$ **が存在し，**$(\phi_j\sigma_1)c_1+(\phi_j\sigma_2)c_2+...+(\phi_j\sigma_r)c_r=0$ **と書けるはずです** $(*)$**．いま，この** c_i **を使って** $b_i=\phi_1c_i+\phi_2c_i+...+\phi_nc_i\ (i=1,...,r)$ **を考えてみると，式** $(*)$ **により，**b_i **は** ϕ_j **の作用に対して不動だと見ることができますので，定義より** $b_i\ (i=1,...,r)$ **は** F **の元だと言えます．これを使うと，**$\sum_{i=1}^{r}b_i\sigma_i=\sum_{i=1}^{r}\sigma_i(\sum_{k=1}^{n}\phi_kc_i)=\sum_{k=1}^{n}\phi_k(\sum_{i=1}^{r}c_i(\phi_k^{-1}\sigma_i))$ **が示せますが，右辺** $=0$ **より，**$\sum_{i=1}^{r}b_i\sigma_i=0$ **が要請されます．これは** σ_i **が一次従属という主張であり，問題の条件に反しますので** $[F:E]=r\leq n$ **でなければなりません．一方，前定理より** $[F:E]=r\geq n$ **ですので，結局** $[F:E]=n$ **が示されます．■**

体 E の部分体 F が，E の自己同型写像による有限群 G に対して固定部分体になるとします．このとき，E を F の **ガロア拡大体** と呼びます．また，G を『E の F 上の **ガロア群** 』と呼び，$\mathcal{G}(E/F)$ のように書きます．

いま定めた用語と記号をさっそく使えば，先ほどの定理は $[E:F]=|\mathcal{G}(E/F)|$ と書け，『ガロア拡大体の拡大次数は，ガロア群の位数に等しい』と要約できます．なんだか，拡大体の話と群論が急に関係し始めました！

[*2] 体と群が急に一緒に出てきて，面食らっている人がいるかも知れません．何を隠そう（何も隠していませんが），ガロア理論の真髄は，体の拡大を群に結び付けてしまう点にあるのです．群論も体論も無かった 200 年近くも前に，ガロア拡大とガロア群の関係を見抜いたガロアは，まさに時代を数十年は先取りした超級の天才だったのでしょう．体より群の方が扱いやすく，計算もわかり易いですし，群論の豊富な成果を援用できます．また，体は無限集合であることが多く，無限体の拡大体も無限集合なので，それらの計算は一般に面倒ですが，もしもこれがガロア拡大体ならば，間に有限個の中間体しか存在せず，それらのガロア群を調べることで体の性質を調べることが出来るのです．ガロア群とは，拡大体（往々にして無限体）の構造を，分かりやすいように輪切りにして見せてくれる MRI のようなものです．次の記事では，拡大体の列と，ガロア群の部分群の列が対応していることを見ます．