ガロア理論の基本定理

Joh @物理のかぎプロジェクト

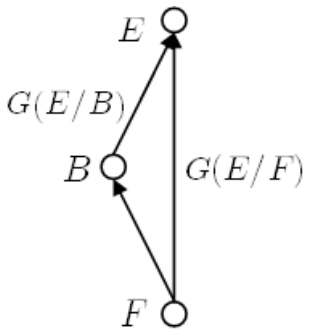
2007-03-03

いよいよガロア理論です．ここまでに，体の自己同型写像 と ガロア群の例 を通じて，体の自己同型写像群（つまりガロア群）というものを考えることで，正規拡大体の拡大次数をガロア群の位数で表すことができ，体の拡大と群という二つの概念が，美しく関係することを勉強しました．この考えを少し発展させると，正規拡大体の列を順次考えていくのに対応して，ガロア群の正規部分群の列が対応するのではないか，と想像できるでしょう．（ ガロア群の例 の最後の例に，ガロア群が部分群を持つ例があります．）この記事で考える **ガロア理論の基本定理** というのは，そのような体の拡大とガロア群の部分群の関係に関する定理です．今後の話題（作図可能な正多角形だとか，可解な方程式だとか）は，全て，この定理を中心に展開していきます．よく，定理の意味を理解して下さい．

ガロア理論の基本定理

theorem

体 F とそのガロア拡大 E の間に，中間体 B があるとします．このとき，E は B のガロア拡大にもなっており，ガロア群 $\mathcal{G}(E/B)$ は $\mathcal{G}(E/F)$ の部分群になっています．また，$\mathcal{G}(E/B)$ が $\mathcal{G}(E/F)$ の正規部分群の場合に限り，B は F のガロア拡大になります．



$$F \subset B \subset E$$

$$G(E/B) \subset G(E/F)$$

体の包含関係 $F \subset B \subset E$ と，群の包含関係 $\mathcal{G}(E/B) \subset \mathcal{G}(E/F)$ が逆になる点に注意してください．（これを，体と群の包含関係が **反変的** と言ったりします．慣れるまで，一番よく混乱するのは，この反変的包含関係かも知れません．）これは『ガロア理論の基本定理』と呼ばれる大事な定理で，体の昇鎖列と部分群の組成列の関係を示した点が斬新であるだけでなく，中間体が関係している点が秀逸です．

一般に，体とその拡大体があったとき，その中間体にはどのようなものがあるのかを調べるのは容易ではありません．それは，体は一般的に無限集合であることが多く，無数に中間体を決められる可能性があるからです．ところが，拡大体がガロア拡大体である場合に限り，間にある中間体の構造はガロア群の構造に反映され，ガロア群を調べることで中間体の個数や様子をいとも簡単に知ることが出来るわけです．ガロア群はちょうど，中間体を調べるためのモニターのような役割を果たしています．ですから，今後の話題でも，中間体を考えることがとても重要です．このような隠されたカラクリを見破ったガロアの慧眼に，改めて畏怖の念を感じます．

少し長くなりますが，以下に証明を示します．

proof

【 E が B のガロア拡大体であることの証明】拡大体 E は，F 上のある分離多項式の最小分離体になっていますので，E の元 θ を使って $E = F(\theta)$ と書けるはずです．このとき $E = B(\theta)$ も明らかです．解 α を E 上に持つ, B 上で既約な多項式 $f(x)$ を考えるとき，$f(x)$ は，α を解に持つ F 上の多項式 $g(x)$ を割るはずです．ここで，ガロア拡大とガロア群 で考えた【補足-1】より，$g(x)$ は E 上に全ての解（個数は g の次数）を持ち，全ての解は相異なります．これより E は B のガロア拡大体になっていると言えます (ガロア拡大とガロア群 の定義 3. 参照)． $F \subset B \subset E$ より，$\mathcal{G}(E/B) \subset \mathcal{G}(E/F)$ は明らかです．$\mathcal{G}(E/B)$ と $\mathcal{G}(E/F)$ はどちらも $\mathcal{G}(E)$ の部分群になっています．■

proof

【 B がガロア拡大体→ $\mathcal{G}(E/B)$ は $\mathcal{G}(E/F)$ の正規部分群の証明】 B が F のガロア拡大体ならば，B のある元 ξ を使って $B = F(\xi)$ と書けるはずです．ξ の F 上の最小多項式を g とすると，g は全ての解を B 上に持ちます．$g(\xi) = 0$ ですが，ある同型写像 $\phi \in \mathcal{G}(E/F)$ に対して $\phi(g(\xi)) = g(\phi(\xi)) = 0$ を満たすはずですので，$\phi(\xi)$ は g の解の一つで，$\phi(\xi) \in B$ が要請されます．この結果は，ϕ が $B \to B$ を満たす同型写像だということです．また，ϕ は F を不動に保ちますので，$\phi \in \mathcal{G}(E/F)$ の元で B にも属するもの (ϕ_B と書きます) は，$\phi_B \in \mathcal{G}(B/F)$ を満たします．これより，写像 $h : h(\phi) = \phi_B$ を考えると，h によって $\mathcal{G}(E/F) \longmapsto \mathcal{G}(B/F)$ なる写像がなされ，h は準同型写像の群になります．準同型定理によって $\mathrm{Ker}h = \mathcal{G}(E/B)$ が成り立ちます．準同型写像の核は常に正規部分群ですから，$\mathcal{G}(E/B) \triangleright \mathcal{G}(E/F)$ が示されました．■

proof

【$\mathcal{G}(E/B)$ は $\mathcal{G}(E/F)$ の正規部分群の証明→ B がガロア拡大体】いま $\mathcal{G}(E/B) \triangleright \mathcal{G}(E/F)$ とします．このとき，二つの同型写像 $\phi \in \mathcal{G}(E/B), \psi \in \mathcal{G}(E/F)$ に対し，$\psi^{-1}\phi\psi \in \mathcal{G}(E/B)$ を得ます．B の元 β に対し $\psi^{-1}\phi\psi(\beta) = \beta$ が成り立ちますので，これを変形して $\phi\psi(\beta) = \psi(\beta)$ と見ると，$\psi(\beta)$ は変換 ϕ に対して不動を保ち，$\psi(\beta) \in B$ が言えます (B は $\mathcal{G}(E/B)$ の元に対す固定体でした)．ここで，写像 $h : \mathcal{G}(E/F) \longmapsto \mathcal{G}(B,F)$ を考えます．$\mathcal{G}(B,F)$ という変な記号を使いましたが，これは『 B に属する同型写像で，B の部分集合 F を不動に保つもの』という意味だとします．まだ F が部分体になることが示せていないので，$\mathcal{G}(B/F)$ と書くのは早計です．さて，写像の核は $\mathrm{Ker}h = \mathcal{G}(E/B)$ です．いま，第三同型定理 (同型定理 参照) より $\mathcal{G}(E/F)\mathcal{G}(E/B) \sim \mathcal{G}(B,f)$ が言えますので，拡大次数について $[B:F] = [E:F]/[E:B] = |\mathcal{G}(E/F)||\mathcal{G}(E/B)| \leq |\mathcal{G}(B,F)|$ が言えます．一方，F は $\mathcal{G}(B,F)$ に対する固定体に含まれるはずですので，$[B:F] \geq |\mathcal{G}(B,F)|$ が成り立ちます．従って $[B:F] = \mathcal{G}(B,F)$ あって $\mathcal{G}(B,F) = \mathcal{G}(B/F)$ であり，B は F のガロア拡大体になっています．■

最後の証明より，$\mathcal{G}(E/F)\mathcal{G}(E/B) \longmapsto \mathcal{G}(B/F)$ を満たす同型写像の存在が示されます．ふう．