

ガロア拡大とガロア群

Joh @物理のかぎプロジェクト

2007-03-03

この記事と次の [ガロア群の例](#) では、[体の自己同型写像](#) で勉強したガロア拡大とガロア群について、もう少し理解を深めることを目的とします。目新しい概念は出てきませんが、役に立つ定理を幾つか考えます。また、ここまで既習の事柄も、このあたりで一度頭の整理をしてみてください。

ガロア群

ガロア群の元を求める際に、次の定理が便利です。

Important

ζ を 1 の素数乗根 $e^{\frac{\alpha\pi i}{p}}$ (p は素数) とします。有理数体 Q に ζ を添加してできる拡大体 $Q(\zeta)$ に対し、ガロア群は整数の剰余群と同型となり、 $\mathcal{G}(Q(\zeta)/Q) \sim Z_p$ がなりたちます

proof

いま p は素数としていますので、剰余群 Z_p は p 次の巡回群 $\{[0], [1], \dots, [p-1]\}$ になります。 $x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \dots + 1) = 0$ を考えると、 ζ は $x^{p-1} + x^{p-2} + \dots + 1 = 0$ の解ですが、この方程式は Q 上既約で、 Q 上には解を持たず、体 $Q(\zeta)$ は $x^{p-1} + x^{p-2} + \dots + 1 = 0$ の最小分解体 $Q(x_1, x_2, \dots, x_{p-1})$ になっており、拡大次数は p です。よって定理が成り立ちます。■

例 1

有理数体 Q に、 $x^5 - 1 = 0$ の解の一つである $\zeta = e^{\frac{2\pi i}{5}}$ を添加して作った拡大体 $Q(\zeta)$ はガロア拡大になっています。 $Q(\zeta)$ の元は $a + b\zeta + c\zeta^2 + d\zeta^3 + e\zeta^4$ ($a, b, c, d, e \in Q$) の形をしており、拡大次数は 5 です。一方、ガロア群 $\mathcal{G}(Q(\zeta)/Q)$ は、 Z_5 に同型ですので位数は 5 です。よって、 $Q(\zeta)$ は Q のガロア拡大になっています。

ガロア拡大とガロア群に関しては、体の拡大次数が、ガロア群の位数で表されてしまうわけです。とて

*1 前定理より、拡大次数が 2, 3, 5, 7, 11, ... の代数的拡大体は、全てガロア拡大だと言えます。

も美しい関係です．

ガロア拡大の別の定義

ここまでで、ガロア拡大とは『 F の拡大体 E が、 E の F 上自己同型写像群 $\mathcal{G}(E/F)$ が E を固定体とし、 $[F : E] = |\mathcal{G}(E/F)|$ の場合』と定義しました．この定義は分かりやすいものですが、全く同値な定義に言い換えることも出来ます．

【ガロア拡大の定義】

1. $[E : F] = |\mathcal{G}(E/F)|$
2. E は F の有限次分離正規拡大体です．
3. E は、 F 上のある分離多項式 $f(x)$ の最小分解体になっています．

これらが同値な条件であることは、以下に証明します．場合に応じて、分かりやすい定義を使えば良いと思います．二番目の定義を最初に挙げる教科書が多いようです．(2. $\rightarrow$ 3.) の証明は [体の元の共役と正規拡大体](#) で示してありますので、ここでは (1. $\rightarrow$ 2.) の証明を示します．

proof

(1. $\rightarrow$ 2.) E の任意の元 α に対し、 α の最小多項式が重解を持たず、かつ E 上で一次式の積に分解できることを示せばよいわけです． $\mathcal{G}(E/F)$ は有限群ですので、 $\mathcal{G}(E/F)$ の元の中で異なるものを集めた集合 $\{\tau_1, \tau_2, \dots, \tau_n\}$ を考えます ($n \leq |\mathcal{G}(E/F)|$)． E の任意の元 α にたいし、この集合の元による写像を $\tau_i(\alpha)$ と書き、多項式 $f(x) = (x - \tau_1(\alpha))(x - \tau_2(\alpha)) \cdots (x - \tau_n(\alpha))$ を考えます．まず各 τ_i は全て異なるので、 $f(x)$ は重解を持ちません．また、 $f(x)$ を展開した際の係数は全て $\tau_i(\alpha)$ ($i = 1, 2, \dots, n$) の和と積で表現されますが、これらは固定体 F の元になっているはずで、これより、 α の F 上の最小多項式 $q(x)$ ($q(x) = x - \alpha$ とは限りません) は $f(x)$ を割るので、 $q(x)$ は重解を持ちません．よって $q(x)$ は E 上一次式の積に分解できます．これより、 E は F の分離正規拡大体になっています．■

ガロア拡大の表現には、他にも色々なものがあり、教科書によって取り上げ方が様々だと思います．例えば、次の二つの条件が成り立つことも、 E が F のガロア拡大であることと同値であることを示すことが出来ます．

【補足】

1. F 上既約な m 次方程式 g が、もし一つでも E 上に解を持てば、 g は結局 m 個の解を E 上に持ちます．
2. E は F の代数的単純拡大体として表現できます．(つまり、 F 上にある代数的元 θ があって、 $E = F(\theta)$ と書けるということ．)

後で使う都合上、1. だけ、簡単に証明しておきます．あまり、証明の細かいところにはまらずに、結果だけを承して先に進んでも良いと思います．

proof

まず必要条件を証明します． E が F のガロア拡大だとすれば，ガロア群を $G(E/F) = \{\phi_1, \phi_2, \dots, \phi_n\}$ のように決めることができ， $\alpha \in E$ に対し $\phi_1\alpha, \phi_2\alpha, \dots, \phi_n\alpha \in E$ が言えます．これらの中から， $r (> m)$ 個を選んで，多項式 $g(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$ を作ると， g の係数は $G(E/F)$ によって動かされませんから（ガロア群の元は α_i を置換するだけなので）， g は F 上の多項式だということが出来ます．ここで α を解とする F 上既約な多項式 f を考えると（ m 次多項式とします）， $g(\alpha) = 0$ より， f は g を割るはずですが， g の最小分解体が E なので， f の最小分解体も E になり，既約という仮定より， f の解は全て異なるはずでです．■

proof

次に十分条件を示します． $E = F(\theta)$ と書け， $[E : F] = n$ とします．いま， θ の最小分解多項式は n 個の解持つはずですので，それを θ_i ($i = 1, 2, \dots, n$) とすると，拡大体 $F(\theta_i) \subset E$ は，全ての i に対して $[F(\theta_i) : F] = n$ を満たし，結局 $F(\theta_i) = E$ が言えます．ここで，写像 ϕ_i ($i = 1, 2, \dots, n$) を $\phi_i(\theta_1) = \theta_i$ と定義すると， $\{1, \phi_1, \phi_2, \dots, \phi_{n-1}\}$ は E を F 上のベクトル空間とみたときの基底になっており， F 上の多項式 g に対して $\phi_i g(\theta_1) = g(\theta_i)$ が成り立ちます．これより， ϕ_i は F を固定体とする E の自己同型写像だということが出来て， E は F のガロア拡大だと言えます．■

例 2

$Q(\sqrt[3]{2})$ は Q のガロア拡大ではありません． $Q(\sqrt[3]{2})$ の任意の元は $a + b\sqrt[3]{2} + c\sqrt[3]{2^2}$ の形に書けますが， $\sqrt[3]{2}$ の共役元である $\sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$ (ω は 1 の三乗根で $\omega = \frac{1+i\sqrt{3}}{2}$ とします) を含まないため，正規拡大にはなっていないからです．

アーベル拡大体と巡回拡大体

特に，ガロア群が可換群である場合のガロア拡大体を アーベル拡大体，ガロア群が巡回群である場合のガロア拡大体を 巡回拡大体 と呼びます．