ガロア理論とその活用 1

蠣崎　瞬　16-00-006

稚内北星学園大学 情報メディア学部 数学ゼミ

稚内北星学園大学
Wakkanai Hokusei Gakuen University

はじめに

私は数学ゼミで2年間に渡り，ガロア理論とその予備知識を学んできた．そこで本ポスターでは，ガロア理論とその活用を細かいことには目をつぶりつつ紹介させていただく．

数学者ガロア

エヴァリスト・ガロア(1811-1832)とはフランスの数学者である．政治活動にも参加しており，最後は決闘に敗れ亡くなった．ガロアの残した論文の内容は後にガロア理論とよばれ，群論や体論の基礎になった．これは数学界に大きな発展をもたらした．

体と群

右の表は数の範囲と四則演算の対応表である．○は計算がその範囲で常に出来る場合，×は常に出来るとは限らない場合を表している．ただし，÷において0で割ることは考えない．他にも条件はあるが四則演算が可能な下の3つは体とよばれる．また，下の4つは群とよばれる．群は四則でなく+，−か×，÷のどちらかが成り立っている．

	+	−	×	÷
$\mathbb{N}$	○	×	○	×
$\mathbb{Z}$	○	○	○	×
$\mathbb{Q}$	○	○	○	○
$\mathbb{R}$	○	○	○	○
$\mathbb{C}$	○	○	○	○

※$\mathbb{N}$は自然数全体の集合，$\mathbb{Z}$は整数全体の集合，
$\mathbb{Q}$は有理数全体の集合，$\mathbb{R}$は実数全体の集合，
$\mathbb{C}$は複素数全体の集合を表している．

拡大体

体$\mathbb{R}$の中には体$\mathbb{Q}$がある．このようなとき，$\mathbb{R}$は$\mathbb{Q}$の拡大体とよび，$\mathbb{R}/\mathbb{Q}$と書く．逆に$\mathbb{Q}$は$\mathbb{R}$の部分体とよぶ．$\mathbb{C}/\mathbb{R}/\mathbb{Q}$のようになっているとき，体$\mathbb{R}$を$\mathbb{C}/\mathbb{Q}$の中間体とよぶ．

最小分解体

$\mathbb{R}/\mathbb{Q}$について，$x^4-5x^2+6=(x^2-2)(x^2-3)=0$の係数$1,-5,6$は$\mathbb{Q}$にあり，この方程式の解$\sqrt{2},-\sqrt{2},\sqrt{3},-\sqrt{3}$は$\mathbb{R}$にある．このようなとき，$\mathbb{R}$を$x^4-5x^2+6$の$\mathbb{Q}$上の分解体とよぶ．また，$\mathbb{Q}$に4つの解を加えた$\mathbb{Q}(\sqrt{2},\sqrt{3},-\sqrt{2},-\sqrt{3})$を最小分解体とよぶ．$-1\times\sqrt{2}=-\sqrt{2},-1\times\sqrt{3}=-\sqrt{3}$のようにすれば$-\sqrt{2},-\sqrt{3}$をつくれるから
$\mathbb{Q}(\sqrt{2},\sqrt{3},-\sqrt{2},-\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$となる．

ガロア拡大とガロア群

拡大E/Fについて，EがF上の多項式の最小分解体でF上分離的であるとき，E/Fをガロア拡大とよぶ．ガロア拡大E/Fに対し，EのF上の自己同型を集めたものは写像の合成に関して群となり，ガロア群とよばれる．例えば，$\mathbb{Q}(\sqrt{2},\sqrt{3})$は$x^4-5x^2+6$の$\mathbb{Q}$上の最小分解体であり，分離的でもあるので$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$はガロア拡大である．このときのガロア群は$\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$と書く．
この中には$\sigma:\sqrt{2}\mapsto\sqrt{2},\sqrt{3}\mapsto-\sqrt{3}$,
$\tau:\sqrt{2}\mapsto-\sqrt{2},\sqrt{3}\mapsto\sqrt{3}$,
$\sigma\tau:\sqrt{2}\mapsto-\sqrt{2},\sqrt{3}\mapsto-\sqrt{3}$,
$id:\sqrt{2}\mapsto\sqrt{2},\sqrt{3}\mapsto\sqrt{3}$という自己同型がある．
ガロア群が$\langle\sigma\rangle=\{\sigma,\sigma^2,\ldots,\sigma^n=id\}$と表せるとき，$E/F$を$n$次巡回拡大とよぶ．

ガロアの基本定理

E/F:ガロア拡大，$G=\mathrm{Gal}(E/F)$，$H\leq G$,
$K:E/F$の中間体．
$\mathcal{F}(H)=\{\alpha\in E\mid\forall\tau\in H,\tau(\alpha)=\alpha\}$,
$\mathcal{G}(K)=\{\sigma\in G\mid\forall r\in K,\sigma(r)=r\}$とおく．
このとき，$\mathcal{F}(H)$はE/Fの中間体，$\mathcal{G}(K)\leq G$であり，次が成り立つ．

1. $[E:F]=|G|$
2. E/K:ガロア拡大，$\mathrm{Gal}(E/K)=\mathcal{G}(K)$
3. $\{E/F$の中間体$\}\underset{\mathcal{F}}{\overset{\mathcal{G}}{\rightleftarrows}}\{\mathrm{Gal}(E/F)$の部分群$\}$
$$K\mapsto\mathcal{G}(K)$$
$$\mathcal{F}(H)\mapsfrom H$$
は互いに逆の1対1対応である．
4. $K_1,K_2:E/F$の中間体．
このとき，次が成り立つ．
   - 4.1 $K_1\supset K_2\Leftrightarrow\mathcal{G}(K_1)\subset\mathcal{G}(K_2)$
   - 4.2 $\langle\mathcal{G}(K_1)\cup\mathcal{G}(K_2)\rangle=\mathcal{G}(K_1\cap K_2)$
   - 4.3 $\mathcal{G}(K_1)\cap\mathcal{G}(K_2)=\mathcal{G}(K_1K_2)$
   - 4.4 $\forall\sigma\in G,\mathcal{G}(\sigma(K))=\sigma(\mathcal{G}(K))\sigma^{-1}$
5. K/F:ガロア拡大$\Leftrightarrow\mathcal{G}(K)\lhd G$
このとき，$\mathrm{Gal}(K/F)\cong G/\mathcal{G}(K)$

ガロア理論の活用

ガロア拡大の中間体や解の公式の存在を調べる，ギリシャの3大作図不可能問題のうち2つの問題の証明ができるなどが有名である．また，無限次ガロア拡大の議論等，他にも様々な応用がある．

syun@wakhok.ac.jp

ガロア理論とその活用２

蠣崎　瞬　16-00-006

稚内北星学園大学 情報メディア学部 数学ゼミ

稚内北星学園大学
Wakkanai Hokusei Gakuen University

ガロア拡大の中間体

拡大E/Fの中間体がいくつありどのような体があるかを調べるのは難しい．しかし，前節で述べたガロアの基本定理から，E/Fがガロア拡大であればガロア群の部分群を調べることですべての中間体を求めることが出来る．
例えば，$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$の中間体を探してみよう．
$G=\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$は4つの自己同型
$\sigma,\tau,\sigma\tau,id$からなり，$G$には5つの部分群
$G,\langle\sigma\rangle,\langle\tau\rangle,\langle\sigma\tau\rangle,\langle id\rangle$があることがわかる．ガロアの基本定理の3番を用いて左から順に
$\mathbb{Q},\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{2},\sqrt{3})$が対応することがわかる．なので$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$の中間体は$\mathbb{Q},\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3}),\mathbb{Q}(\sqrt{6}),\mathbb{Q}(\sqrt{2},\sqrt{3})$の5種類のみである．

解の公式の存在

$n\geq 5$でn次方程式の解の公式は存在しないことを主張するアーベル・ルフィニの定理という有名な定理がある．これはガロア理論を用いて証明することが出来る．また，ガロア理論から4次以下の方程式の解の公式を求めることも出来る．

2次方程式の解の公式

2次方程式$x^2+bx+c=0$の解の公式を求めよう．求める解をα,βとし，b,cは不定元とする．解と係数の関係を用いると$s_1=\alpha+\beta=-b, s_2=\alpha\beta=c$となる．このとき，$F(\alpha,\beta)/F(s_1,s_2)$はガロア拡大になり，ガロア群は2文字の置換全体を表す対称群S_2と同型となる．解の差積を$\Delta=\alpha-\beta$，判別式を$D=\Delta^2$とする．S_2の部分群である交代群A_2と対応する中間体は$F(s_1,s_2,\Delta)=F(\alpha,\beta)$となり，
$F(s_1,s_2,\Delta)/F(s_1,s_2)$は2次巡回拡大となる．
$\alpha,\beta\in F(s_1,s_2,\Delta)$となるから，$\alpha,\beta$は$F,s_1,s_2,\Delta$でつくれる．連立方程式$\begin{cases}\Delta=\alpha-\beta=\sqrt{D}\\ \alpha+\beta=-b\end{cases}$を解けば，$\alpha=\dfrac{-b+\sqrt{D}}{2}$，$\beta=\dfrac{-b-\sqrt{D}}{2}$となる．
$D=\Delta^2=(\alpha-\beta)^2=b^2-4c$となるから，
$x=\dfrac{-b\pm\sqrt{b^2-4c}}{2}$となる．

3次方程式の解の公式

3次方程式$z^3+bz^2+cz+d=0$の解の公式を求めよう．$z=x-\dfrac{1}{3}b$とおく．b,c,dの多項式をp,qとすれば，$x^3+px+q=0$となる．この方程式を解けばzを求められるのでこの方程式を解いていく．解をα,β,γとする．$F(\alpha,\beta,\gamma)/F(p,q)$はガロア拡大になり，ガロア群は$S_3$と同型となる．解の差積を$\Delta=(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)$，判別式を$D=\Delta^2=-4p^3-27q^2$とする．$S_3$の部分群である交代群$A_3$と対応する中間体は$F(p,q,\Delta)$となり，$F(\alpha,\beta,\gamma)/F(p,q,\Delta)$はガロア拡大になる．
$\omega=\dfrac{-1+\sqrt{-3}}{2}$として，$F(\omega,\alpha,\beta,\gamma)/F(\omega,p,q,\Delta)$を考える．ガロアの推進定理を用いると
$F(\omega,\alpha,\beta,\gamma)/F(\omega,p,q,\Delta)$はガロア拡大でガロア群が$A_3$と同型となるから3次巡回拡大となる．
$K=F(\omega,p,q,\Delta)=F(\sqrt{-3},p,q,\Delta)$とすれば
$F(\omega,\alpha,\beta,\gamma)=K(\alpha)$となる．このとき，ラグランジュの分解式$(1,\alpha)=0,(\omega,\alpha),(\omega^2,\alpha)$の3乗は$K$に入り，$(\omega,\alpha)=\sqrt[3]{-\dfrac{27}{2}q-\dfrac{3\sqrt{-3}\sqrt{D}}{2}}$,
$(\omega^2,\alpha)=\sqrt[3]{-\dfrac{27}{2}q+\dfrac{3\sqrt{-3}\sqrt{D}}{2}}$と書け，
$\alpha=\dfrac{1}{3}((\omega,\alpha)+(\omega^2,\alpha))$となる．
$\sigma(\alpha)=\beta,\sigma(\beta)=\gamma,\sigma(\gamma)=\alpha$となる$\sigma\in A_3$で$\alpha$を写せば，$\beta=\dfrac{1}{3}(\omega(\omega,\alpha)+\omega^2(\omega^2,\alpha))$,
$\gamma=\dfrac{1}{3}(\omega^2(\omega,\alpha)+\omega(\omega^2,\alpha))$を得る．これをカルダノの公式といい，これを用いればzが求まる．

参考文献

1. 石井俊全，「ガロア理論の頂を踏む」，ベレ出版，2013.
2. 桂利行，「代数学III 体とガロア理論」(大学数学の入門③)，東京大学出版会，2005.
3. 雪江明彦，「代数学2 環と体とガロア理論」，日本評論社，2010.
4. 京都産業大学，「ガロアが広げた数学の自由―革命を志した青年が起こした数学上の一大革命―」，2020年1月22日参照，https://www.kyoto-su.ac.jp/project/st/st08_01.html.

syun@wakhok.ac.jp