ガロア群の例

Joh @物理のかぎプロジェクト

2007-03-03

ガロア群の定義はそれほど難しくありませんでしたが，ガロア群が具体的にどのような群であるか，すなわち，その元である自己同型写像がどのようなものであるかが，まだあまりピンと来ていないと思います．

実は，ガロア群の元は体によって簡単に決まる場合もあれば，なかなか求めるのが難しいような場合もあり，一般にはなかなか簡単に決まりません．特に，拡大次数が大きい場合には大変です．ガロア群を決定するための万能の方法はありませんが，幾つかの例と定理を見ながら，ガロア群に少しずつ慣れていきましょう．

まず，体の自己同型写像の定義を復習しましょう．

$$\phi(\alpha+\beta)=\phi(\alpha)+\phi(\beta) \tag{1}$$

$$\phi(\alpha\beta)=\phi(\alpha)\phi(\beta) \tag{2}$$

有理数体 Q を Q に写す自己同型写像には，恒等写像しかないことが分かります．これは背理法ですぐに示せますが，もしも，ある有理数が違う有理数に写される場合があれば，式 (1)(2) が成り立たない反例をすぐに示せるからです．

Important

有理数体 Q を Q に移す自己同型写像には恒等写像しかありません．

例１（二次拡大体）

最初に，Q の二次拡大体の例として $Q(\sqrt{2})$ のガロア群 $\mathcal{G}(\sqrt{2})$ を考えます．$Q(\sqrt{2})$ の元が全て $a+b\sqrt{2}$ の形に書けるのはもう大丈夫だと思います．

まず，明らかに恒等写像 I は自己同型写像で，$\mathcal{G}(\sqrt{2})$ の元です．

$$I:\ a+b\sqrt{2}\ \longmapsto\ a+b\sqrt{2}$$

これは自明な元です．実は，もう一つそれほど明らかではない自己同型写像に，$a+b\sqrt{2}$ を $a-b\sqrt{2}$ に写す写像があります．

$$J:\ a+b\sqrt{2}\ \longmapsto\ a-b\sqrt{2}$$

この写像 J が確かに自己同型写像の定義を満たすことを確認してみましょう．式 (1)(2) に J を代入してみます．

$$\begin{aligned} J((a+b\sqrt{2})+(c+d\sqrt{2})) &= J((a+c)+(b+d)\sqrt{2}) \\ &= (a+c)-(b+d)\sqrt{2} \\ &= (a-b\sqrt{2})+(c-d\sqrt{2}) \\ &= J(a+b\sqrt{2})+J(c+d\sqrt{2}) \end{aligned}$$

$$\begin{aligned} J((a+b\sqrt{2})\cdot(c+d\sqrt{2})) &= J((ac+2bd)+(ad+bc)\sqrt{2}) \\ &= (ac+2bd)-(ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2}) \\ &= J(a+b\sqrt{2})J(c+d\sqrt{2}) \end{aligned}$$

確かに J も自己同型写像の定義 (1)(2) を満たすことが分かりました．$J^2 = I$ ですから，この自己同型写像群は I と J だけで閉じた位数 2 の群を作れます．

また，I も J も $a+b\sqrt{2}$ の形の元の有理数部分，つまりこの例の a を不変に保ちますから，ガロア群 $\mathcal{G}(Q(\sqrt{2})/Q) = \{I, J\}$ が分かります．

例2

もう一つ，Q の拡大体 $Q(\sqrt{2},\sqrt{3})$ を考えてみましょう．$Q(\sqrt{2},\sqrt{3})$ の元は，全て $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$ の形で表わすことができます．

二つの $Q(\sqrt{2},\sqrt{3})$ の元の積を考えて，恒等写像以外の自己同型写像の可能性を考えてみましょう．計算はけっこう大変です．

$$\begin{aligned} (a_1+b_1\sqrt{2}+c_1\sqrt{3}+d_1\sqrt{6})(a_2+b_2\sqrt{2}+c_2\sqrt{3}+d_2\sqrt{6}) &= (a_1a_2+2b_1b_2+3c_1c_2+6d_1d_2) \\ &\quad +(a_1b_2+b_1a_2+3c_1d_2+3d_1c_2)\sqrt{2} \\ &\quad +(a_1c_2+c_1a_2+2b_1d_2+2d_1b_2)\sqrt{3} \\ &\quad +(a_1d_2+b_1c_2+c_1b_2+d_1a_2)\sqrt{6} \end{aligned}$$

じっと両辺を見ていると，まず左辺の b と d の符号を $+$ から $-$ に変える写像 K が，右辺でも二行目と四行目（つまり b と d に相当）の符号だけを変えることが分かります．

$$K:\ a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \ \longmapsto\ a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$

よって，K は式 (2) を満たしています．K が式 (1) を満たすのは明らかですから，K は $Q(\sqrt{2},\sqrt{3})$ の自己同型写像になっています．同様に，b と c の符号だけを変える写像 L，c と d の符号だけを変える写像 M も自己同型写像になります．

有理数の部分 a を不変に保つ自己同型写像（つまり Q を固定体とする $Q(\sqrt{2},\sqrt{3})$ の自己同型写像）はこの四つだけですが，この四つの自己同型写像は確かに群をなします．群表は次のようになります．

[*1] のちほど，ガロア理論の応用として，定規とコンパスで作図可能な図形の問題や，代数方程式の可解性も問題を考えますが，そうした場合に二次拡大が非常に大事です．

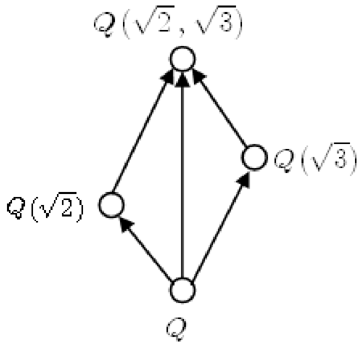
	I	**K**	**L**	**M**
I	I	K	L	M
K	K	I	M	L
L	L	M	I	K
M	M	L	K	I

これより，ガロア群 $\mathcal{G}(Q(\sqrt{2},\sqrt{3})/Q)=\{I,K,L,M\}$ が分かります．この群が，クラインの四元群と同型であることを，群表を比較して確認してください．ここで行った計算はやや面倒でしたが，自己同型写像を具体的に決めるには，定義式 (1)(2) を満たすように地道に探すしかありません．

補足

例 2 に出てきた I,M の二つは，$Q(\sqrt{2},\sqrt{3})$ の元で $a+b\sqrt{2}$ の部分の符号を変えませんので，$\mathcal{G}(Q(\sqrt{2},\sqrt{3})/Q(\sqrt{2}))=\{I,M\}$ が言えます．このガロア群は，明らかに例 1 で見た $\mathcal{G}(Q(\sqrt{2})/Q)=\{I,J\}$ に同型です．

これは少し考えてみればもっともなことです．ガロア群は，二つの体の間にある，拡大の関係だけで決まってくる群ですので，Q に $\sqrt{2}$ を添加した体と，$Q(\sqrt{3})$ に $\sqrt{2}$ を添加した体とで，ガロア群 $\mathcal{G}(Q(\sqrt{2},\sqrt{3})/Q(\sqrt{2}))$ と $\mathcal{G}(Q(\sqrt{2})/Q)$ が同型になっていることに不思議はありません．このような関係を，よく次のような図で書く人もいます．図中，下の Q から上の $Q(\sqrt{2},\sqrt{3})$ に到るのに，添加する元と中間体を示しているわけです．



矢印の横には，ガロア群の元や位数など，追加情報を書き込みましょう．物理のかぎしっぽでは，このような図はあまり使わないと思いますが，演習問題を解く際に自分で考えるのには，きっと役に立つと思います．ここまでに 体の自己同型写像 で『ガロア拡大の拡大次数は，ガロア群の位数に等しい』という定理を導きましたが，例 1 と例 2 をもう一度振り返って，この関係を確認してみてください．

例 3

有理数体 Q の拡大体 $Q(\sqrt[4]{2},i)$ を考えてみます．$Q(\sqrt[4]{2}),i)$ は，x^4-1 の解 $\pm\sqrt[4]{2},\pm i\sqrt[4]{2}$ を Q に添加して得られる体で，Q 上 x^4-1 は既約ですから，$Q(\sqrt[4]{2},i)$ は x^4-1 の最小分解体になっています．

*2 具体的に自己同型写像を探すしかないと書きましたが，たいていは例題のように，$\pm$ の符号を入れ替える写像を考えれば良いです．複素共役を取る操作に似てますね．