$$\sigma_1=\begin{pmatrix} Q(\sqrt{2}) & Q(-\sqrt{2}) \\ Q(\sqrt{2}) & Q(-\sqrt{2}) \end{pmatrix},\quad \sigma_2=\begin{pmatrix} Q(\sqrt{2}) & Q(-\sqrt{2}) \\ Q(-\sqrt{2}) & Q(\sqrt{2}) \end{pmatrix}.$$

見通しよくするには，$Q(\sqrt{2})$ を１番目の体，$Q(-\sqrt{2})$ を２番目の体というほどの意味にすれば，

$$\sigma_1=\begin{pmatrix} 1\,2 \\ 1\,2 \end{pmatrix}=1,\quad \sigma_2=\begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix}=(12)$$

この２つの置換を G_2 で表わそう．

$$G_2=\{\sigma_1,\ \sigma_2\}$$

この G_2 は群の定義を満たす．G_2 のことを**２次対称群**という．

こうして正則拡大体 $Q(\sqrt{2})$ に置換を定義することができた．２個のものの置き換えはすべて２次対称群を作る．２次対称群を直接図形で表現するならば，線分 AB の対称移動に例えることができる．線分 AB を線分 AB に移すのが恒等置換**１**，線分 AB を線分 BA に移すのが互換(AB)であり，これらは２次対称群{**１**，(AB)}を作る．

さて，正則拡大体の中には，当然いくつかの部分体が含まれているのであるが，これらは正則拡大体の部分体であるとともに，**中間体**とも呼ばれる．中間体とは，基礎体と正則拡大体の「中間に」ある体という意味である．

以上の議論を一般化しよう．k を基礎体とし，$K=k(\theta)$ を n 次方程式[11]の解 $\theta=\theta_1,\theta_2,\ \cdots\ ,\theta_n$ をすべて含んだ単純正則拡大体とする．すなわち，k に n 次方程式[11]のある解 $\theta=\theta_1$ で拡大したらそのまま正則拡大体になったとする．$Q(\sqrt{2})$ などもそうである．このとき，$k(\theta_1)$ から $k(\theta_i)$ への n 個の k-同型対応ができるが，これをそのまま $K=k(\theta)$ の k-自己同型対応としたならば．この k-自己同型対応によってそれぞれの中間体の置換が引き起こされる．この置換をガロア置換という．ガロア置換の個数は正則拡大体の次数に等しい．例えば $Q(\sqrt{2})$ の（Q に対する）次数は２なので，そのガロア置換（=Q-自己同型対応）は２個ある．

正則拡大体 K に属する k-自己同型対応（ガロア置換）は，群を作る．これを K/k のガロア群といい，$G(K/k)$ と表わす． $Q(\sqrt{2})$ の例で言えば $G_2(\ Q(\sqrt{2})\ /Q)$ がガロア群である．

ここでもう一度「ガロア理論の基本定理」を述べる．K/k を取り入れて少し表現を変えてある．

【定理１】（基本定理）K/k を正則拡大体，G をそのガロア群とする．K の中間体と G の部分群は１対１に対応し，相対応する中間体の次数と部分群の位数は等しい．

この中間体と部分群の対応をもう少し詳しく説明すると，K のある中間体 L に対して，G の元による k-自己同型対応で L がまったく変化しないような G の元が作る集合（G の部分集合）が部分群となって対応し，逆に G のある部分群の元による k-自己同型対応によってまったく変化しない K の元が作る集合が中間体として対応するのである．

この対応のことをガロアの対応（ガロア対応）という．この対応によって正則拡大体の性質が群に反映されるのである．

正則拡大体をガロア拡大体といい，その群をガロア群，そしてガロア置換，ガロア対応等々というのは，すべてガロアが初めて実質的に用いたところからその名が冠されている．

ガロア群の最大の部分群は G 自身であるから，その位数は K の（k に対する）次数に等しい．またガロア群の最小の部分群は単位群 E={**１**}であるから，その位数は基礎体 Q の Q に対する次数（=1）に等しい．

次章でガロア群の例を挙げる．

5．ガロア群の例

まず，2次体についてはすでに $Q(\sqrt{2})$ のガロア群として2次対称群をあげた．ここではそれ以外のいくつかの例をあげる．まず，

$$x^4-10x^2+1=0 \quad . \qquad [13]$$

これは4次方程式ではあるが，実は2次方程式が重なった複2次方程式なので高校数学でも解を求められる． $X=x^2$ とおいて，

$$\begin{aligned} &X^2-10X+1=0 \\ &X=5\pm 2\sqrt{6} \\ &\therefore\ x^2=5\pm 2\sqrt{6} \\ &\therefore\ x=\pm(\sqrt{3}\pm\sqrt{2}) . \end{aligned}$$

よって方程式[13]の解は，

$$x=\sqrt{3}+\sqrt{2},\sqrt{3}-\sqrt{2},-\sqrt{3}+\sqrt{2},-\sqrt{3}-\sqrt{2} \quad .$$

の4つである．

この方程式[13]の基礎体は係数も有理数なので有理数体 Q である．しかも Q を正則拡大体にするために Q に追加する数は，解のどれかひとつ，たとえば $\sqrt{3}+\sqrt{2}$ だけで十分である．なぜなら他の解は以下のようにこの解と有理数との四則計算から導かれるからである．

$$\sqrt{3}-\sqrt{2}=\frac{1}{\sqrt{3}+\sqrt{2}},\ -\sqrt{3}+\sqrt{2}=-(\sqrt{3}+\sqrt{2}),\ -\sqrt{3}-\sqrt{2}=-(\sqrt{3}+\sqrt{2}) .$$

すなわち， $Q(\sqrt{3}+\sqrt{2})$ は，方程式[13]の正則拡大体である． $Q(\sqrt{3}+\sqrt{2})$ の Q に対する次数はもちろん4である．$[\ Q(\sqrt{3}+\sqrt{2})\ :Q\ ]=4$．

$Q(\sqrt{3}+\sqrt{2})$ の共役体は， $Q(-\sqrt{3}+\sqrt{2})$ ， $Q(\sqrt{3}-\sqrt{2})$ ， $Q(-\sqrt{3}-\sqrt{2})$ であり，これらの体の置換によってガロア置換を求めることができる．

$Q(\sqrt{3}+\sqrt{2})$ のガロア対応は次の4つである．

$$\begin{aligned} \sigma_1 &:\ Q(\sqrt{3}+\sqrt{2}) \to Q(\sqrt{3}+\sqrt{2}) \qquad \text{(恒等置換)} \\ \sigma_2 &:\ Q(\sqrt{3}+\sqrt{2}) \to Q(-\sqrt{3}+\sqrt{2}) \\ \sigma_3 &:\ Q(\sqrt{3}+\sqrt{2}) \to Q(\sqrt{3}-\sqrt{2}) \\ \sigma_4 &:\ Q(\sqrt{3}+\sqrt{2}) \to Q(-\sqrt{3}-\sqrt{2}) \end{aligned}$$

これらを(123)のような巡回置換で表現してみよう． $\sqrt{3}+\sqrt{2}$ を1番目の解， $-\sqrt{3}+\sqrt{2}$ を2番目の解，$\sqrt{3}-\sqrt{2}$ を3番目の解， $-\sqrt{3}-\sqrt{2}$ を4番目の解とすると，まず，σ_1 は恒等置換で何も変わらないのであるから，他の解もまったく変化しない．それを次のように表わそう．

$$\sigma_1=\begin{pmatrix}1234\\1234\end{pmatrix} \quad .$$

これは恒等置換なので，**1**とする．

次の σ_2 は $Q(\sqrt{3}+\sqrt{2})$ に $Q(-\sqrt{3}+\sqrt{2})$ を対応させるのだから， $\sqrt{3}+\sqrt{2}$ が $-\sqrt{3}+\sqrt{2}$ に変わる．これは $\sqrt{3}$ の符号だけが変わっていると見ることができる．すなわち，σ_2 によって1番目の $\sqrt{3}+\sqrt{2}$ は2番目の $-\sqrt{3}+\sqrt{2}$ に変わり，2番目の $-\sqrt{3}+\sqrt{2}$ は1番目の $\sqrt{3}+\sqrt{2}$ に変わり，3番目の $\sqrt{3}-\sqrt{2}$ は4番目の $-\sqrt{3}-\sqrt{2}$ に変わり，4番目の $-\sqrt{3}-\sqrt{2}$ は3番目の $\sqrt{3}-\sqrt{2}$ に変わる．ゆえに，

$$\sigma_2=\begin{pmatrix}1234\\2143\end{pmatrix}=(12)(34) \quad .$$

同様に，σ_3 では $\sqrt{2}$ の符号が変わっているので，1→3，2→4，3→1，4→2という置換になる．ゆえに，

$$\sigma_3=\begin{pmatrix}1234\\3412\end{pmatrix}=(13)(24)$$

σ_4では，$\sqrt{3}$ と $\sqrt{2}$ の両方の符号が変わっているので，１→４，２→３，３→２，４→１という置換になる．ゆえに，

$$\sigma_4=\begin{pmatrix}1234\\4321\end{pmatrix}=(14)(23)\ .$$

こうして，ガロア置換を方程式の解の置換としてとらえることができるのである．この置換の集合にB_4という名をつけよう．

$$B_4=\{1,(12)(34),(13)(24),(14)(23)\}\ . \qquad [14]$$

このB_4は群を作る．群表は次の通り．

B_4	1	(12)(34)	(13)(24)	(14)(23)
1	1	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	1	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	1	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	1

これが方程式[13]のガロア群である．B_4にはクラインの４元群という名前が付いている（クラインはドイツの数学者の名）．B_4はアーベル群である（アーベル群は群表では対角線に対して対称になる）．

この群を導くときに，方程式[13]の４つの解の置換を利用したが，一般に，方程式のガロア体における一つひとつのガロア置換に対して方程式の解のある置換が対応する．ただし，この逆は成り立たない．すべての解の置換に対応するガロア置換があるわけではない．n次の正則拡大体のガロア置換はn個であるが，方程式の解の置換は$n!$個あり，$n>3$の時には$n<n!$だからである．

今の例では，ガロア対応として体 $Q(\sqrt{3}+\sqrt{2})$ から他の中間体へのk-自己同型対応を取ったが，これを $Q(\sqrt{3}+\sqrt{2})$ 以外の，例えば $Q(-\sqrt{3}+\sqrt{2})$ から他の中間体への対応としても同じガロア群が得られるのはいうまでもない．

方程式[13]では，解の置換として４つの置換が出てきてクラインの４元群を構成したが，４つのものの置換には一般に４!=24通りがあり，それらは４次対称群[10]という群を成す．クラインの４元群はその部分群のひとつである．ある方程式のガロア群がどういう群になるかはそれぞれの方程式の個性に依るものであり，一般的に論じることは非常に困難である．

さて，基本定理によれば，「正則拡大体の中間体とガロア群の部分群とが１対１に対応する」のであるが，まずB_4の部分群を数え上げてみよう． $Q(\sqrt{3}+\sqrt{2})$ の中の中間体の個数を調べるよりもB_4の部分群の個数を調べる方が簡単である．有限群の部分群は有限個しかなく，その位数はもとの群の位数の約数であるからである．そしてこのこと自体がすでに基本定理の威力を示しているのである．

さて，B_4の部分群は次の５つしかないことは自明である．

B_4自身，

H_1={**1**，(12)(34)},

[10] ４次対称群についてはB_4がその部分群の一つであることを述べるにとどめ，詳述しない．

H_2={**1**，(13)(24)}，

H_3={**1**，(14)(23)}，

E ={**1**}（単位群）．

そこで，まず H_1 に対応する K= $Q(\sqrt{3}+\sqrt{2})$ の中間体を求めてみよう．

ガロアの対応によれば，「G の部分群の元による k-自己同型対応（=解の置換）によってまったく変化しない K の元が作る集合が中間体として対応する」のであるが，H_1 の元である**1**，及び (12)(34) によってまったく変化しない K の元とは何であろうか．

1 がすべての部分群に含まれるのは群であることから当然であり，また恒等置換なので K の元はすべてまったく変化しない．H_1 のもうひとつの元 (12)(34) とは，解の置換においては $\sqrt{3}+\sqrt{2}$ → $-\sqrt{3}+\sqrt{2}$ のように $\sqrt{3}$ の符号だけが変わる置換であった．言い換えれば，$\sqrt{2}$ の方は変わらないのだ．だから，もし K の中に $\sqrt{2}$ と Q だけからなる体すなわち $Q(\sqrt{2})$ が存在すれば，それは置換 (12)(34) によってまったく変化しない中間体といえるであろう．そして，$\sqrt{2}$ が $Q(\sqrt{3}+\sqrt{2})$ の元であることは，

$$\sqrt{2}=\frac{(\sqrt{3}+\sqrt{2})+(-\sqrt{3}+\sqrt{2})}{2}\ .$$

となることから明らかである．従って $Q(\sqrt{2})$ は $Q(\sqrt{3}+\sqrt{2})$ の部分体で，置換 (12)(34) によって変わらない中間体である．

このことを別の角度から見るために，【定理２】に依って $Q(\sqrt{3}+\sqrt{2})$ の一般項を計算してみよう．

$[\ Q(\sqrt{3}+\sqrt{2})\ :Q\ ]=4$ と【定理２】から，

$$a+b(\sqrt{3}+\sqrt{2})+c(\sqrt{3}+\sqrt{2})^2+d(\sqrt{3}+\sqrt{2})^3$$

となるが，これを展開･整理してみると，

$$\begin{aligned}&a+b(\sqrt{3}+\sqrt{2})+c(\sqrt{3}+\sqrt{2})^2+d(\sqrt{3}+\sqrt{2})^3\\=&a+b\sqrt{3}+b\sqrt{2}+5c+2c\sqrt{6}+3\sqrt{3}d+9d\sqrt{2}+6\sqrt{3}d+2\sqrt{2}d\\=&(a+5c)+(b+9d+2d)\sqrt{2}+(b+9d)\sqrt{3}+(2c+6d)\sqrt{6}\\=&a'+b'\sqrt{2}+c'\sqrt{3}+d'\sqrt{6}\ .\end{aligned}$$

この最後の式の a', b',c',d' はもちろん Q の元である．つまり，$Q(\sqrt{3}+\sqrt{2})$ のどんな元も a, b,c,d を Q の元として，

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \qquad [15]$$

の形に表せるのである．

この式は恒等置換 **1** によってもちろん全く変化しない．また，置換 (12)(34) によって解 $\sqrt{3}+\sqrt{2}$ は $-\sqrt{3}+\sqrt{2}$ に変わるが，同様の計算によって，体 $Q(-\sqrt{3}+\sqrt{2})$ の元は，

$$a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}\ . \qquad [16]$$

となる．[15]の最後の式と[16]を比べてみると，恒等置換 **1** と置換 (12)(34) の両方によっても $a+b\sqrt{2}$ は変わっていないのである．これはすなわち，体 $Q(\sqrt{2})$ を成す元である．

すなわち体 $Q(\sqrt{2})$ が H_1 にガロア対応する K= $Q(\sqrt{3}+\sqrt{2})$ の中間体である．

このやり方で他の部分群にガロア対応する中間体を求めてみよう．

部分群 H_2 の置換 (13)(24) とは $\sqrt{2}$ だけの符号を変えることであったから，一般項は，$a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$ となり，恒等置換とともに変化しないのは $a+c\sqrt{3}$，すなわち H_2 にガロア対応する中間体は $Q(\sqrt{3})$ である．

さらに，部分群 H_3 の置換 (14)(23) では $\sqrt{2}$ と $\sqrt{3}$ の両方の符号が変わり，一般項は $a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$ となる．よって恒等置換とともに変化しないのは $a+d\sqrt{6}$，すなわち H_3 に対応する中間体は $Q(\sqrt{6})$ である．

また，ガロア群 B_4 のすべての置換によってまったく変化しない $K=\ Q(\sqrt{3}+\sqrt{2})$ の元は Q しかないので，B_4 にガロア対応する K の中間体とは基礎体 Q であり，最後に，単位群 E の元 **1** によって K のすべての元はまったく変化しないので部分群 E にガロア対応する中間体は K 自身ということになる．

こうしてガロア群 B_4 のすべての部分群に対して正則拡大体 $K=\ Q(\sqrt{3}+\sqrt{2})$ の中間体が対応することがわかった．

基本定理は，この反対も成り立つことを述べている．すなわち，正則拡大体 K の任意の中間体 L に対しては，ガロア群の部分群がただ一つ対応する．そしてこの部分群にガロア対応する中間体がもとの中間体 L である．

今の例でいえば，正則拡大体 $K=\ Q(\sqrt{3}+\sqrt{2})$ の中間体として，例えば $Q(\sqrt{2})$ をあげたとする（ $\sqrt{2}$ が K に属することは前に述べた）．K のガロア群 B_4 の元のうち，K の元である $a+b\sqrt{2}$ を変えないものは，恒等置換 **1** のほかには $\sigma_2=$ (12)(34) しかない．σ_2 は解の置換としては $\sqrt{3}$ を $-\sqrt{3}$ に変えるものであり，$\sqrt{2}$ の符号は変えないからである．こうしてガロア群 B_4 の元のうち，**1** と (12)(34) だけが中間体 $Q(\sqrt{2})$ を変化させない．そしてこの二つは B_4 の部分群 $H=\{$**1**，(12)(34) $\}$を作る．以下同様．

これら部分群と中間体の対応は１対１の対応を示す．これがガロア対応である．ガロア理論の基本定理とは，ガロア対応が成り立つことを述べているのである．

B_4 と $K=\ Q(\sqrt{3}+\sqrt{2})$ のガロア対応

ガロア群の部分群	$K=\ Q(\sqrt{3}+\sqrt{2})$ の中間体
B_4	Q
$H_1=\{$**1**，(12)(34)$\}$	$Q(\sqrt{2})$
$H_2=\{$**1**，(13)(24)$\}$	$Q(\sqrt{3})$
$H_3=\{$**1**，(14)(23)$\}$	$Q(\sqrt{6})$
$E\ =\{$**1**$\}$	K

次の例は，前にも出てきた３次方程式，

$$x^3-2=0 \qquad [17]$$

である．この方程式の３つの解は，$\sqrt[3]{2}$ ，$\sqrt[3]{2}\,\omega$ ，$\sqrt[3]{2}\,\omega^2$ であり，正則拡大体は $K=\ Q(\omega,\sqrt[3]{2})$ （$=\ Q(\omega+\sqrt[3]{2})$ ）という６次の体であることを前に述べた．この方程式のガロア群を求めてみよう．

この場合は前の例と違ってやや複雑である．方程式[13]の場合のように Q に解のひとつを追加するだけで正則拡大体を作るというわけにはいかない．Q に $\sqrt[3]{2}$ だけを追加して作った体 $Q(\sqrt[3]{2})$ が ω や $\sqrt[3]{2}\,\omega$ を含んでいないためである．

そこでまず，Q に ω を追加してを作り，これを Q'とし，これに $\sqrt[3]{2}$ を追加して $Q'(\sqrt[3]{2})\ =\ Q(\omega,\sqrt[3]{2})$ としたのであった．これで正則となり，方程式[17]のガロア群を作ることが可能になる．

ここでひとつ新たな約束を設ける．それは，**方程式が基礎体に対して p 次既約である場合には，基礎体には１の虚数 p 乗根を含むことにする（ただし p は奇数の素数）**というものである．こうすることで理論が透明になるのである．この約束は，３次以上の既約方程式の場合に重要となる[11]．

この約束によって，方程式[17]の基礎体を初めから $Q'=\ Q(\omega)$ とすることが出来る．方程式[17]は Q に対して３次既約だから，上の約束によって初めから１の３乗根を含ませておくことができる．そして，$K=$

[11] 方程式[12]の $x^2-2=0$ の場合にも，この基礎体は Q であるが，１の２乗根（すなわち ±1 ）を既に含んでいると考えることができる．

$Q(\omega,\sqrt[3]{2})$ のガロア群として，$G(K/Q)$ ではなくて，$G(K/Q')$ を求めるのである．

こうして基礎体 $Q'=Q(\omega)$ 上に作られた正則拡大体 $Q'(\sqrt[3]{2})$ に対してガロア置換を定義するのであるが，ここから先は前の例と同様にすればよい．すなわち $Q'(\sqrt[3]{2})$ のガロア置換は次の3つである．

$$\begin{aligned}&\tau\ :\ Q'(\sqrt[3]{2})\ \rightarrow\ Q'(\sqrt[3]{2})\ :\ \text{（恒等置換）}\\&\tau_2\ :\ Q'(\sqrt[3]{2})\ \rightarrow\ Q'(\sqrt[3]{2}\,\omega)\\&\tau_3\ :\ Q'(\sqrt[3]{2})\ \rightarrow\ Q'(\sqrt[3]{2}\,\omega^2)\ .\end{aligned}\qquad [18]$$

（τ は「タウ」という，σ と同じギリシア文字）

例によって解 $\sqrt[3]{2}$ を1番目の解，$\sqrt[3]{2}\,\omega$ を2番目の解，$\sqrt[3]{2}\,\omega^2$ を3番目の解として式[18]の共役体の対応は次の解の置換に置き換えることが出来る．

τ_1 は言わずと知れた恒等置換であるから，

$$\tau_1=\begin{pmatrix}\sqrt[3]{2} & \sqrt[3]{2}\,\omega & \sqrt[3]{2}\,\omega^2\\ \sqrt[3]{2} & \sqrt[3]{2}\,\omega & \sqrt[3]{2}\,\omega^2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=1\ .$$

同様に，置換[18]によれば τ_2 は $\sqrt[3]{2}$ が $\sqrt[3]{2}\,\omega$ に，つまり $\sqrt[3]{2}$ に ω が掛けられているのであるから，$\sqrt[3]{2}\,\omega$ は $\sqrt[3]{2}\,\omega^2$ に，$\sqrt[3]{2}\,\omega^2$ は $\sqrt[3]{2}$ になる．よって1が2に，2が3に，3が1になっている．よって τ_3 は，

$$\tau_2=\begin{pmatrix}\sqrt[3]{2} & \sqrt[3]{2}\,\omega & \sqrt[3]{2}\,\omega^2\\ \sqrt[3]{2}\,\omega & \sqrt[3]{2}\,\omega^2 & \sqrt[3]{2}\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=(123)\ .$$

次の τ_3 は $\sqrt[3]{2}$ が $\sqrt[3]{2}\,\omega^2$ に，つまり $\sqrt[3]{2}$ に ω^2 が掛けられているのであるから，$\sqrt[3]{2}\,\omega$ は $\sqrt[3]{2}$ に，$\sqrt[3]{2}\,\omega^2$ は $\sqrt[3]{2}\,\omega^4=\sqrt[3]{2}\,\omega$ になる．よって1が3に，3が2に，2が1になっている．よって τ_3 は，

$$\tau_3=\begin{pmatrix}\sqrt[3]{2} & \sqrt[3]{2}\,\omega & \sqrt[3]{2}\,\omega^2\\ \sqrt[3]{2}\,\omega^2 & \sqrt[3]{2} & \sqrt[3]{2}\,\omega\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=(132)\ .$$

以上から求めるガロア群は，{1,(123),(132)}となる．これは前述3次対称群 G_3 の正規部分群 A_3 と同じ形をしているので名前も A_3 としておこう．

$$A_3=\{1,(123),(132)\}\ .\qquad [19]$$

この A_3 については，新たな群の概念である交代群という性質を持つことを述べる．3つのものの置き換えを示す置換 (123) は次のように2つの互換の積に分解するることができる．すなわち，

$$(123)=(12)(13)=(23)(12).\qquad [20]$$

あるいはさらに長さ4の巡回置換で (1423) というのがあったときには，

$$(1423)=(14)(12)(13)=(23)(24)(14).\qquad [21]$$

このようにどんなに長い巡回置換でもすべて互換の積に分解できる．その分解は上記のように一通りではないが，互換の個数は一定となる．そのときの互換の個数が偶数である場合には最初の巡回置換を偶置換，奇数であるならば奇置換という．そして対称群の中で偶置換だけを集めるとそれは群になるのである．上の A_3 にがまさにそうで，これを3次交代群という．ちなみに恒等置換は偶置換と定めることになっているので，奇置換だけを集めても群にはならない（恒等置換がないから）．

さて，ここまで議論を進めてきたので，次に巡回群を導入しよう．

今，解の置換 τ_1,τ_2,τ_3 を使って A_3 を構成したが，このとき τ_2 とは $\sqrt[3]{2}$ に ω を掛けることであり，τ_3 とは $\sqrt[3]{2}$ に ω^2 を掛けることであった．ところで ω^2 を掛けるとは ω を2回掛けることであるから，置換 τ_2 を2回行なうことでもある．すなわち τ_3 とは $\tau_2\tau_2$ のことである（$\tau_2\tau_2$ のことを τ^2 と表わす ついでに(123)(123)も$(123)^2$と表わす）．

$$\tau_2\tau_2=\tau^2=(123)(123)=(123)^2=(132)=\tau_3\ .$$

さらにもう一度 τ_2 を掛けてみると，これは ω を 3 回掛けることになり，ω^3=1 になるから $\sqrt[3]{2}$ は変わらない．すなわち τ_2 を 3 回掛けると恒等置換になる．

$$\tau^3=(123)^3=(132)(123)=1$$

これで A_3 のすべての元がそろってしまった．なにを意味するかというと，A_3 という（置換）群は，ある一つの置換，例えば(123)を 2 回 3 回と累乗することですべての元が得られるということである．このときには，A_3 を，(123)を生成元とする巡回群と呼ぶことがある．A_3 では，τ_2 =(123)を順に 3 回掛けて（累乗して）A_3 のすべての元を形成したが，この 3 のことを「置換(123)の位数」という．3 以上の数で累乗しても新たな元を得ることはない．

巡回群の生成元を σ ，任意の元を τ ， υ （ υ は「ウプシロン」という， σ と同じギリシア文字）とすると，これらはいずれも σ の何乗かで表わされるから， $\tau = \sigma^m$ ， $\upsilon = \sigma^n$ と表せる．よって $\tau\upsilon$ は，

$$\tau\upsilon=\sigma^m\sigma^n=\underbrace{(\sigma\sigma..\sigma)}_{m個}\underbrace{(\sigma\sigma...\sigma)}_{n個}=\underbrace{\sigma\sigma\sigma.....\sigma\sigma\sigma}_{(m+n)個}=\underbrace{(\sigma\sigma...\sigma)}_{n個}\underbrace{(\sigma\sigma..\sigma)}_{m個}=\sigma^n\sigma^m\ .$$

ゆえに任意の元の積について交換法則が成り立つ．すなわち，巡回群はすべてアーベル群である[12]．

今求めたガロア群 A_3 は $G(K/Q')$，つまり K の $Q'=Q(\omega)$ に対するガロア群であったが，では K の Q に対するガロア群：$G(K/Q)$ は求められないのか，という疑問が残る．多少複雑になるが，当然可能ではある．

まず K は Q に対して，$K=Q(\omega,\sqrt[3]{2})$ というように ω と $\sqrt[3]{2}$ という二つの超数を持っているのでガロア置換も 2 種類を考える．まず ω は方程式 $x^2+x+1=0$ の解で，その共役数は ω^2 であるから その K の中での k-同型対応は，

$$\sigma_1:\omega\to\omega$$
$$\sigma_2:\omega\to\omega^2$$

である．次に $\sqrt[3]{2}$ の共役数は当然， $\sqrt[3]{2}\omega$ ， $\sqrt[3]{2}\omega^2$ であるから，その K の中での k-自己同型対応は，

$$\tau_1:\sqrt[3]{2}\to\sqrt[3]{2}$$
$$\tau_2:\sqrt[3]{2}\to\sqrt[3]{2}\omega$$
$$\tau_1:\sqrt[3]{2}\to\sqrt[3]{2}\omega^2$$

である．従って K の Q に対するガロア置換はこれらを「組み合わせた」ものになる．

$$\upsilon_1:\omega\to\omega\ ,\sqrt[3]{2}\to\sqrt[3]{2}\ （恒等置換）$$
$$\upsilon_2:\omega\to\omega\ ,\sqrt[3]{2}\to\sqrt[3]{2}\omega$$
$$\upsilon_3:\omega\to\omega\ ,\sqrt[3]{2}\to\sqrt[3]{2}\omega^2$$
$$\upsilon_4:\omega\to\omega^2,\sqrt[3]{2}\to\sqrt[3]{2}$$
$$\upsilon_5:\omega\to\omega^2,\sqrt[3]{2}\to\sqrt[3]{2}\omega$$
$$\upsilon_6:\omega\to\omega^2,\sqrt[3]{2}\to\sqrt[3]{2}\omega^2\ .$$

これらを方程式[17]の解の置換としてみるならば， $\upsilon_1,\upsilon_2,\upsilon_3$ は ω が変わらないので上の A_3 の元と同じものである．すなわち， $\upsilon_1=1$ ， $\upsilon_2=(123)$ ， $\upsilon_3=(132)$ ．

次の υ_4 は，解 $\sqrt[3]{2}$ は変わらないが，解 $\sqrt[3]{2}\omega$ は $\omega\to\omega^2$ によって， $\sqrt[3]{2}\omega^2$ に換わり，解 $\sqrt[3]{2}\omega^2$ は $\omega\to\omega^2$ によって $\sqrt[3]{2}(\omega^2)^2=\sqrt[3]{2}\omega$ になる．よって，1→1，2→3，3→2．ゆえに，

$$\upsilon_4=\begin{pmatrix}\sqrt[3]{2} & \sqrt[3]{2}\omega & \sqrt[3]{2}\omega^2\\ \sqrt[3]{2} & \sqrt[3]{2}\omega^2 & \sqrt[3]{2}\omega\end{pmatrix}=\begin{pmatrix}123\\132\end{pmatrix}=(23)$$

[12] この計算からわかる通り，群の元の累乗については指数法則が成り立つ．

となる．

次の υ_5 は $\omega\to\omega^2$ と，$\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega$ によって，

まず，解 $\sqrt[3]{2}$ は $\omega\to\omega^2$ には関係ないが，$\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega$ によって $\sqrt[3]{2}\omega$ になる．つまり１→２．

次に，解 $\sqrt[3]{2}\omega$ は $\omega\to\omega^2$ によって $\sqrt[3]{2}\omega^2$ になり，それが $\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega$ によって $\sqrt[3]{2}\omega\cdot\ \omega^2\ =\ \sqrt[3]{2}$ ．従って２→１．

最後の解 $\sqrt[3]{2}\omega^2$ は $\omega\to\omega^2$ によって $\sqrt[3]{2}(\omega^2)^2=\sqrt[3]{2}\omega$ になり，それが $\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega$ によって $\sqrt[3]{2}\omega^2$ ．

つまり，３→３．ゆえに，

$$\upsilon_5=\begin{pmatrix}123\\213\end{pmatrix}=(12)$$

最後に υ_6 は $\omega\to\omega^2$ と，$\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega^2$ によって，

まず，解 $\sqrt[3]{2}$ は $\omega\to\omega^2$ には関係ないが，$\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega^2$ によって $\sqrt[3]{2}\omega^2$ になる．すなわち，１→３．

次に，解 $\sqrt[3]{2}\omega$ は $\omega\to\omega^2$ によって $\sqrt[3]{2}\omega^2$ になり，それが $\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega^2$ によって $\sqrt[3]{2}\omega^2\cdot\ \omega^2\ =\ \sqrt[3]{2}\omega$ ．すなわち，２→２．

最後の解 $\sqrt[3]{2}\omega^2$ は $\omega\to\omega^2$ によって $\sqrt[3]{2}(\omega^2)^2=\sqrt[3]{2}\omega$ になり，それが $\sqrt[3]{2}\ \to\ \sqrt[3]{2}\omega^2$ によって $\sqrt[3]{2}\omega^2\cdot\ \omega=\sqrt[3]{2}$ ．ゆえに，３→１．よって，

$$\upsilon_6=\begin{pmatrix}123\\321\end{pmatrix}=(13)$$

以上の結果，$\upsilon_1\ \sim\ \upsilon_6$ の集合は，A_3 の元 **1**，(123)，(132) と(23)，(12)，(13)とからなる３次対称群 G_3 そのものである．これが方程式[17]のガロア群 $G(K/Q)$ である．

これまでの結果，$K=\ Q(\omega,\sqrt[3]{2})$ の Q に対するガロア群が３次対称群 G_3 であり，K の $Q'=\ Q(\omega)$ に対するガロア群はその正規部分群 A_3 であることがわかった．また Q' は Q に対して２次の体になることから正則であり，そのガロア群は２次対称群 G_2 である．ここでひとつ疑問となるのは，K の $Q'=\ Q(\omega)$ に対するガロア群 A_3 は G_3 の（正規）部分群として G_3 の「中に　」存在しているのだが，Q' の Q に対するガロア群 G_2 は G_3 の「中に」はないことである．G_3 から A_3 を「取り除いたもの」（={ (12),(23),(13) }）が G_2 になるわけではない．しかし，実はこの G_2 を，G_3 と A_3 から「作り出す」ことができる．G_3 の位数が 6，A_3 の位数が 3 で，G_2 の位数は 2 であることから思いつくことは，6÷3=2 という計算である．ここから剰余群の思想にたどり着く．

しかし，その前に，$K=\ Q(\omega,\sqrt[3]{2})$ の Q に対するガロア群 G_3 での中間体と部分群の対応，すなわちガロア対応を片付けておこう．ここでも G_3 での部分群を先に調べる方が早道である．

G_3 での部分群は次の通り．

G_3 自身，

H_1={**1**，(12)}，

H_2={**1**，(13)}，

H_3={**1**，(23)}，

A_3={**1**，(123)，(132)}，

E ={**1**}（単位群）．

G_3 自身と単位群 E はまず置いといて，H_1 から考えてみよう．H_1 の恒等置換はともかく，互換 υ_5 =(12) によって変わらない体とは何か．１番目の解 $\sqrt[3]{2}$ と２番目の解 $\sqrt[3]{2}\omega$ が入れ替わるのが (12) であるから，３番目の解 $\sqrt[3]{2}\omega^2$ は変わらない．解 $\sqrt[3]{2}\omega^2$ が変わらないということは，これに対応する中間体はこの３番目の解の追加によってできる体 $Q(\sqrt[3]{2}\omega^2)$ ということである．この調子でいけば，H_2 に対応する中間体は (13) で変わらないのだから，１番目の解 $\sqrt[3]{2}$ と３番目の解 $\sqrt[3]{2}\omega^2$ が入れ替わっても変わらない体なので２

番目の解 $\sqrt[3]{2}\omega$ によって作られる $Q(\sqrt[3]{2}\omega)$ ということになる．そして H_3に対応する中間体は (23) によって変わらない，すなわち２番目の解 $\sqrt[3]{2}\omega$ と３番目の解 $\sqrt[3]{2}\omega^2$ の入れ替わりによって変わらないのであるから，１番目の解 $\sqrt[3]{2}$ によって作られる中間体 $Q(\sqrt[3]{2})$ ということになる．

次に，A_3によって変わらないKの中間体とは何か．A_3は前述の通り $K=Q(\omega,\sqrt[3]{2})$ の$Q'=Q(\omega)$ に対するガロア群であり，Q'の上に築かれる拡大体に対する置換の集まりであるから，当然 A_3は Q' を変えることはない．A_3の元が変えるのは Q' の上に築かれた $Q'(\sqrt[3]{2})$ の共役体である．すなわち A_3によって変わらない $K=Q(\omega,\sqrt[3]{2})$ の中間体とは $Q'=Q(\omega)$ のことである．実際，ω を３つの解を使って表わしたとき，

$$\omega=\frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}\ ，\text{または}\ \frac{\sqrt[3]{2}\omega^2}{\sqrt[3]{2}\omega} \qquad [22]$$

のようになるが，これらの式に置換 (123) を行なうと１番目の解は２番目に，２番目は３番目に，３番目は１番目の解に変わる．ゆえに，置換の結果：(123)(ω)の値は，

$$(123)(\omega)=\frac{\sqrt[3]{2}\omega^2}{\sqrt[3]{2}\omega}=\omega\ ，\text{または}\ \frac{\sqrt[3]{2}}{\sqrt[3]{2}\omega^2}=\frac{\sqrt[3]{2}\cdot\ \omega}{\sqrt[3]{2}\omega^2\cdot\ \omega}=\frac{\sqrt[3]{2}\omega}{\sqrt[3]{2}}=\omega\ .$$

すなわち，ω は置換 (123) によっては変わらない．ゆえに体 $Q(\omega)$ としても変わらないのである．もちろん置換 (132) についても ω は変わらない．

以上から，A_3の元である**1**，(123)，(132)によって変わらない体，言い換えればガロア対応する中間体は $Q(\omega)$ である．

では $Q(\omega)$ はA_3以外部分群H_1の元によって変わるだろうか，試してみよう．H_1の元である恒等置換**1**によって変わらないのは当然であるが，もう一つの置換 (12) による式[22]の置換の結果：(12)(ω)は，

$$(12)(\omega)=\frac{\sqrt[3]{2}}{\sqrt[3]{2}\omega}=\frac{\sqrt[3]{2}\cdot\ \omega^2}{\sqrt[3]{2}\omega\cdot\ \omega^2}=\omega^2\ ，\text{または}\ \frac{\sqrt[3]{2}\omega^2}{\sqrt[3]{2}}=\omega^2$$

となるから，ω は ω^2 に変わるのである． $Q(\omega)$ と $Q(\omega^2)$ とは集合としては同じものであるが，体としては異なり，互いに共役体であるが，中間体としては別物である．従って $Q(\omega)$ は置換 (12) によって体としては変わるのである．よってH_1は $Q(\omega)$ にガロア対応しているとはいえない．

部分群H_2にやH_3についても同様にωは ω^2 に変わってしまう．ゆえに， $Q(\omega)$ にガロア対応しているのは $Q(\omega)$ 以外にはない．

最後に， G_3自身と単位群Eにガロア対応する「中間体」とは，それぞれQ及びK自身となる．G_3のどの元によっても変わらない体とは基礎体Qだけであり，単位群Eによって変わらない体，すなわち恒等置換だけで変わらない体は，K以外にはない．Kより「小さい」中間体はみな G_3のどれかの元で変わるからである．

さて，ここでいよいよ前に持ち出しておいた「剰余群」について述べよう．

剰余群を正式に定義するためには，群の元と部分群の「掛け算」，あるいは群の部分集合同士の「掛け算」を定義しなくてはならない．

群Gのある元 σ とGの部分群Hがあるとき，その積 σH とはHの各元に（左から） σ を掛けたものの集合を表わすものとする．例えば，G_3の部分群 H={**1**，(12)} に G の元 (123) を左側から掛けた (123)Hとは，

$$(123)H=(123)\{\ 1,\ (12)\ \}=\{(123),\ (123)(12)\ \}=\{\ (123),\ (23)\ \}\ .$$

σ をHの右側から掛けた $H\sigma$ も同様に定義される．H(123)を示すと，

$$H(123)=\{\ 1,\ (12)\ \}(123)=\{(123),\ (12)(123)\ \}=\{\ (123),\ (13)\ \}\ .$$

σH や $H\sigma$ のことを副群と呼ぶこともある．

この例のように，一般には $\sigma H\neq H\sigma$ となるが，これが成り立つとき，HはGの正規部分群となる．あ

る部分群 H が正規部分群であるかを見分ける最も有効な方法は，群の任意の任意の元 σ について，$\sigma H=H\sigma$ または（この両辺に右側から σ^{-1} を掛けて） $\sigma H\sigma^{-1}=H$ を示すことである．

これが正規部分群の本質的な特徴である．また，アーベル群では任意の部分群について $\sigma H=H\sigma$ が成り立つことから，すべての部分群が正規部分群である．

もうひとつの，「部分集合の積」とは，各集合の元同士をすべて掛け合わせた積のすべてからなる集合とするのである．もし元の積に同じものが出てきたらそれはひとつと数える（以下，積の演算記号「·」は出来るだけ省略するが，1と(123)の積のようなときは·を用いる）．

例えば， G_3 の任意の部分集合として適当に {1,(12),(23)}と{(123),(132)} を選んだときの積は，

$$\begin{aligned}\{1,(12),(23)\}\{(123),(132)\}&=\{1\cdot(123),\ 1\cdot(132),\ (12)(123),\ (12),(132),\ (23)(123),\ (23)(132)\}\\&=\{(123),(132),(13),(23),(12),(13)\}\\&=\{(12),(13),(23),(123),(132)\}.\end{aligned}$$

とするのである．

以上を前置きとして，実際に G_3 と A3 から「剰余群」なるものを構成する．

まず， A_3 に G_3 のすべての元を左から掛けてみると，

$$\begin{aligned}1\cdot A_3&=\{1,(123),(132)\}\\(12)\cdot A_3&=\{(12),(13),(23)\}\\(13)\cdot A_3&=\{(13),(23),(12)\}\\(23)\cdot A_3&=\{(23),(12),(13)\}\\(123)\cdot A_3&=\{(123),(132),1\}\\(132)\cdot A_3&=\{(132),1,(123)\}.\end{aligned}$$

結果を見ると，これらの副群はまったく同じか全然別物かのどちらかであり，G_3 は 2 種類の同じ個数を持った副群に分けられる．A3 の元が 3 個なので当然である．一つは A_3 自身で，もう一つは {(12),(13),(23)} である． A_3 でない方を M ととすると，$M=$ {(12)，(13)，(23)} ．

なぜ A_3 と M が同じかまったく別物になるのか． A_3 にないもの，例えば (12) を掛けたとき，その積は A_3 にないものになる．もし積が A_3 の元になれば (12) は A_3 の元ということになる， A_3 は群だからである．ゆえに (12)· A_3 はすべて A_3 の元以外のものになる．逆に A_3 の元，例えば (123) を A_3 に掛ければそれは A_3 自身になるのは当然である．

もうひとつ，副群が 2 個できる訳は，各副群の元の個数はすべて A_3 の位数(=3)であり，それらがまったく同じか全然別物に分けられるのだから， $6\div3=2$ ということである[13]．

このように群をある部分群をもとにいくつかの副群に分けることができる．その副群の元の個数はもとになった部分群と同じである．互いの副群はまったく同じか全然異なっている．異なる副群の個数は（群 G の位数）÷（部分群 H の位数）によって決まる．これを部分群の指数といい，（G : H）と表わす．今の例では，

$$(G_3:A_3)=2$$

である．

今，対象としている群は G_3（位数 6）であり，その正規部分群は A_3（位数 3）である．A_3 をもとにして作られた副群は A_3 と $M=\{(12),(13),(23)\}$ だけであった．この A_3 と M とで「部分集合の積」を求めてみよう．

[13] ちなみに，G_3 を A_3 以外の部分群，例えば $H_1=\{1,(12)\}$ をもとに副群に分解することもできる．この場合は 3 種の副群ができる．

$$
\begin{aligned}
&A_3\cdot A_3=A_3,\\
&A_3\cdot M=\{1,(123),(132)\}\{(12),(13),(23)\}\\
&\qquad=\{(12),(13),(23),(23),(12),(12),(13),(23),(12)\}\\
&\qquad=\{(12)(13),(23)\}\\
&\qquad=M,\\
&M\cdot A_3=M,\\
&M\cdot M=\{(12),(13),(23)\}\{(12),(13),(23)\}\\
&\qquad=\{1,(123),(132),(132),1,(123),(123),(132),1\}\\
&\qquad=\{1,(123),(132)\}\\
&\qquad=A_3\quad .
\end{aligned}
$$

このようにA_3とMとの積は結果がA_3とMのどちらかになり，従って「演算」として閉じているのである．すなわちA_3とMは部分集合の積を演算として群を構成する．群表は次の通り．

	A_3	M
A_3	A_3	M
M	M	A_3

これをG_3のA_3に対する剰余群といい，G_3/A_3と表わす．明らかに２次対称群と同じ形をしている．剰余群の位数（元の個数）はG_3のA_3に対する指数（$G_3:A_3$）に等しい．

注意すべきことは副群を作るのは他の部分群でも可能だが，剰余群を構成できるのは正規部分群に限るのである．例えばG_3の正規部分群でない部分群として，$H_1=\{1,(12)\}$を取れば，他の副群は$\{(13),(132)\}$，$\{(23),(123)\}$となるが，仮にH_1と$\{(13),(132)\}$を掛けてみると，

$$H_1\cdot\{(13),(132)\}=\{(13),(132),(123),(132)\}=\{(13),(123),(132)\}$$

となって3つの副群のどれでもないものになるので，部分集合の積を演算としては閉じていない．従って群にはならない．

こうして剰余群G_3/A_3を構成したからには，それが晴れてG_3とA_3における，$Q'=Q(\omega)$のQに対するガロア群となることを宣言することができる．

一般に，Gを正則拡大体$K=Q(\theta)$のガロア群，HをGの正規部分群とし，Hにガロア対応する$Q(\theta)$の部分体をQ'とするとき，Q'は正則であり，Q'のQに対するガロア群が剰余群G/Hになるのである．

剰余群に関しては身近な例を挙げることができる．

整数の集合Z={0，±1，±2，…}は加法を演算として群を成すが，これをもとに，ある自然数nをZの元に掛けてできる整数全体の集合を考える．例えばZに5を掛けると5の倍数の集合ができるが，これを5Zと表わすと，5ZはZの正規部分群になる．そこで5ZにZの各元（つまり整数）を足すと（Zは加法についての群なので掛け算ではなく足し算をとる），

$$
\begin{aligned}
&\vdots\\
5\mathbb{Z}+(-2)&=\{\ldots,-12,-7,\ 2,\ 3,\ \ldots\}=(3),\\
5\mathbb{Z}+(-1)&=\{\ldots,-11,-6,\ 1,\ 4,\ \ldots\}=(4),\\
5\mathbb{Z}+\ 0\ \ &=\{\ldots,-10,-5,\ 0,\ 5,\ \ldots\}=(0),\\
5\mathbb{Z}+\ 1\ \ &=\{\ldots..,-9,-4,\ 1,\ 6,\ \ldots\}=(1),\\
5\mathbb{Z}+\ 2\ \ &=\{\ldots..,-8,-3,\ 2,\ 7,\ \ldots\}=(2),\\
5\mathbb{Z}+\ 3\ \ &=\{\ldots..,-7,-2,\ 3,\ 8,\ \ldots\}=(3),\\
5\mathbb{Z}+\ 4\ \ &=\{\ldots..,-6,-1,\ 4,\ 9,\ \ldots\}=(4),\\
5\mathbb{Z}+\ 5\ \ &=\{\ldots,-10,-5,\ 0,\ 5,\ \ldots\}=(0),\\
5\mathbb{Z}+\ 6\ \ &=\{\ldots..,-9,-4,\ 1,\ 6,\ \ldots\}=(1),\\
&\vdots\\
&\vdots
\end{aligned}
$$

という 5 種類の集合ができる．この(0)，(1)，(2)，(3)，(4)と表わしたものが結局，整数を 5 で割ったときの余りが同じ整数を一つにまとめたものと考えればよい．これを $\mathbb{Z}/5\mathbb{Z}=\{(0),(1),(2),(3),(4)\}$ と表わせば，これは文字通り「剰余群」になる!

Z / 5Z に属する 2 つの元を「足す」とは，それぞれに属する整数をどれか代表して足し，それをまた 5 で割ったときの余りがその結果であるとすると， Z / 5Z はこの「加法」について閉じていることになる．例えば (3)+(4)の場合は 3+4=7 で，7 を 5 で割った余りは 2 なので(3)+(4)=(2)．ただしこの「加法」は普通の加法よりは拡張されている．