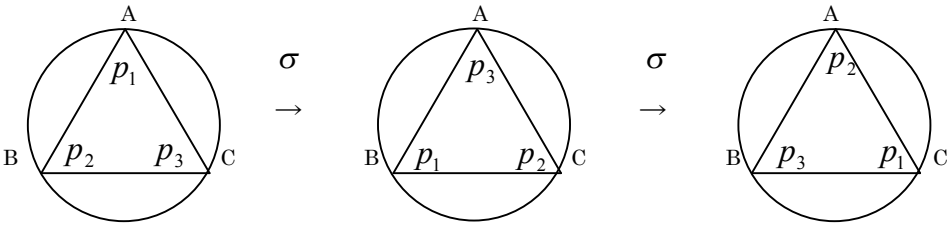
§1. 復習(群・剰余群)

今回は「群」の利用がカギになります．そこで，まずはこれまで学んできた群の復習から始めましょう．

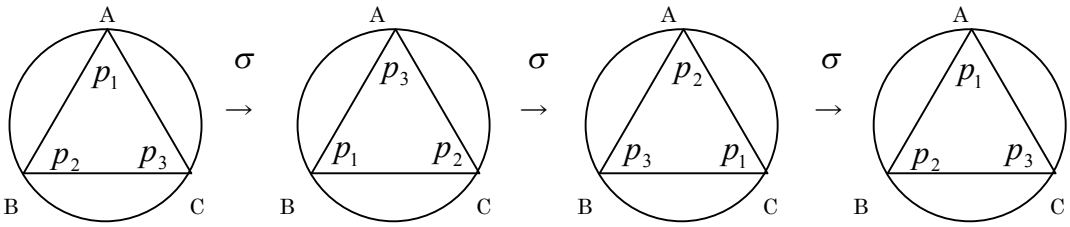
【群の例】

固定された 3 つの点 A, B，C があり，正三角形 $p_1p_2p_3$ が，p_1 は A に，p_2 は B に，p_3 は C に置かれているとします．この△ $p_1p_2p_3$ の重心を中心に 120° 回転させる操作を σ とします． また，∠A の二等分線に関する対称移動を τ とします．これらにより，いくつかの“操作の合成”をしてみましょう．

まず，$\sigma^2=\sigma\cdot\sigma$ は，

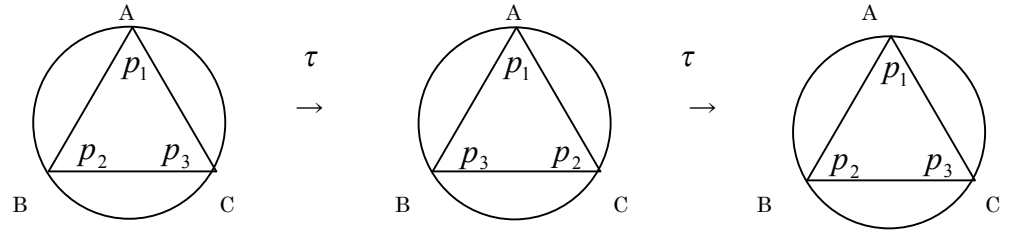


となり，これは，△ $p_1p_2p_3$ の重心を中心に 240° 回転させる操作です．また，$\sigma^3=\sigma\cdot\sigma\cdot\sigma$ なら，



となり，これは何の操作もしないことと同じです．

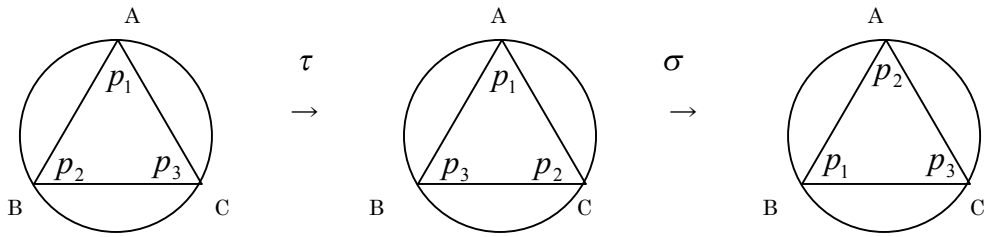
次に，$\tau^2=\tau\cdot\tau$ はどうなるでしょうか．これは，



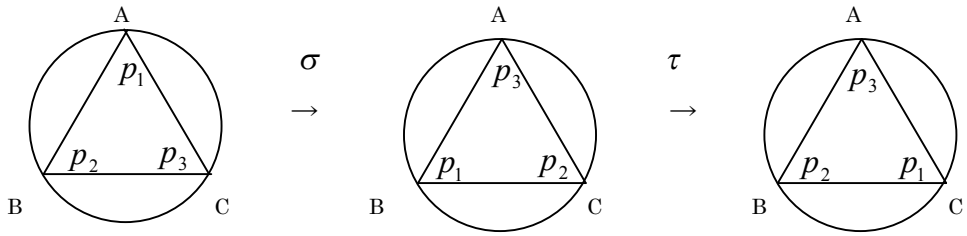
となるので，何の操作もしないことと同じです．

では，$\sigma\cdot\tau$ と $\tau\cdot\sigma$ はどうなるでしょうか.

$\sigma\cdot\tau$ は、



であり，$\tau\cdot\sigma$ は,



です.

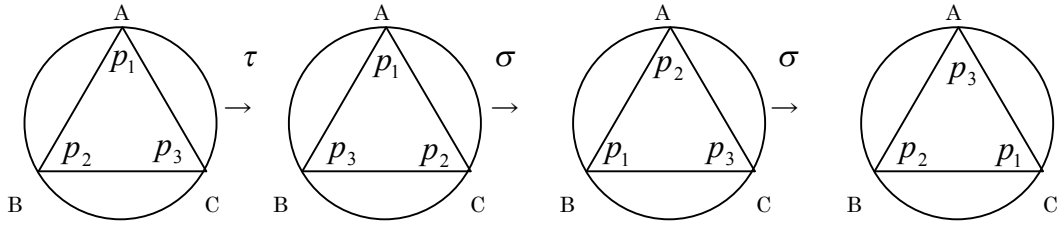
つまり，$\sigma\cdot\tau$ は∠C の二等分線に関する対称移動を表しており，$\tau\cdot\sigma$ は∠B の二等分線に関する対称移動を表しています.

重要なこと（と後で分かるのですが）は,

$$\sigma\cdot\tau\neq\tau\cdot\sigma$$

であるということです.

さらに，$\sigma^2\cdot\tau$ は,



となり，これは∠B の二等分線に関する対称移動となっているので，$\sigma^2\cdot\tau=\tau\cdot\sigma$ であることが分かります.

以上により，e を“何もしない”操作（何もしないのに操作とは違和感がありますが，“操作”という観点で以下を考察したいのでこの表現をお許しあれ）であると考えれば,

$$\left\{e,\sigma,\sigma^2,\tau,\sigma\cdot\tau,\sigma^2\cdot\tau\right\}$$

は，固定された 3 つの点 A，B，C に頂点がある正三角形 $p_1p_2p_3$ を，固定された 3 つの点 A，B，C に頂点がある正三角形に移す

“合同変換”

全体を表します．そしてこの集合は，操作の合成を演算として，“群”をなします．それを確かめるには，以下のような乗積表が重宝します：

$\cdot$	e	σ	σ^2	τ	$\sigma\cdot\tau$	$\sigma^2\cdot\tau$	逆元
e	e	σ	σ^2	τ	$\sigma\cdot\tau$	$\sigma^2\cdot\tau$	e
σ	σ	σ^2	e	$\sigma\cdot\tau$	$\sigma^2\cdot\tau$	τ	σ^2
σ^2	σ^2	e	σ	$\sigma^2\cdot\tau$	τ	$\sigma\cdot\tau$	σ
τ	τ	$\sigma^2\cdot\tau$	$\sigma\cdot\tau$	e	σ^2	σ	τ
$\sigma\cdot\tau$	$\sigma\cdot\tau$	τ	$\sigma^2\tau$	σ	e	σ^2	$\sigma\cdot\tau$
$\sigma^2\cdot\tau$	$\sigma^2\cdot\tau$	$\sigma\cdot\tau$	τ	σ^2	σ	e	$\sigma^2\tau$

この群は，“３次対称群”とよばれ，S_3 と表されます．また，

$$\sigma^3=\tau^2=e,\ \tau\cdot\sigma=\sigma^2\cdot\tau$$

なる関係式が成立っています．これ迄に学んだ“置換”を用いると，

$$\sigma\text{ には}\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\quad \tau\text{ には}\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$$

が対応することが分かり，これらを用いて次のように計算できます：

$$\sigma^2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\quad \sigma^3=\sigma\cdot\sigma^2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e,$$

$$\tau^2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}=e,$$

$$\tau\cdot\sigma^2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\quad \sigma\cdot\tau=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\tau\cdot\sigma^2,$$

$$\tau\cdot\sigma=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\quad \sigma^2\cdot\tau=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}=\tau\cdot\sigma$$

【部分群】

ここで，つぎのような問題を考えてみましょう．

3次対称群 S_3 の部分集合が群になることはあるか．あれば，それを全て求めよ．

まずは，群の定義により“単位元”eがなければ群にはならないことを確認しておきましょう．そのうえで，

（1） $H_1=\{e\}$とすると，これは群になるでしょうか．

・	e	逆元
e	e	e

この表から分かるようにこれは群になっています．

（2） $H_2=\{e,\sigma\}$とすると，これは群になるでしょうか．

・	e	σ
e	e	σ
σ	σ	σ^2

$\sigma^2\notin H_2$なので，群にはなりません（演算が閉じていない）．

（3） $H_3=\{e,\sigma,\sigma^2\}$とすると，これは群になるでしょうか．

・	e	σ	σ^2	逆　元
e	e	σ	σ^2	e
σ	σ	σ^2	e	σ^2
σ^2	σ^2	e	σ	σ

この表から分かるようにこれは群になっています．このH_3は３次巡回群”Z_3となっています．

（4） $H_4=\{e,\tau\}$とすると，これは群になるでしょうか．

・	e	τ	逆　元
e	e	τ	e
τ	τ	e	τ

この表から分かるようにこれは群になっています．このH_4は“２次巡回群”Z_2となっています．

同様にして，$H_5=\{e,\sigma\cdot\tau\}$, $H_6=\{e,\sigma^2\cdot\tau\}$も“２次巡回群”$Z_2$となることが分かります．

★ （問）それを確かめてみましょう．

このような作業を続けていくと，S_3の部分群は，（S_3自身も含めて）

$$\{e\},\ \{e,\tau\},\ \{e,\sigma\cdot\tau\},\ \{e,\sigma^2\cdot\tau\},\ \{e,\sigma,\sigma^2\},\ S_3$$

の６つあることが分かります.

【軌道分解（剰余分解）】

さて，今，

$H=\{x_1,x_2,\cdots,x_n\}\subset G$（**$G$は群とし，$H$はGの部分群であるとします**），$y\in G$ **のとき，$y\cdot H, H\cdot y$ はそれぞれ，**

$$y\cdot H=\{y\cdot x_1,\ y\cdot x_2,\cdots,\ y\cdot x_n\},\ H\cdot y=\{x_1\cdot y,\ x_2\cdot y,\cdots,\ x_n\cdot y\}$$

を表す

ものとします．すると，S_3の部分群のうち，例えばH_4に対して，

“左から”σをかける

と，$\sigma\cdot H_4=\sigma\cdot\{e,\tau\}=\{\sigma,\sigma\cdot\tau\}$となることが分かるでしょう.

また，

“左から”σ^2をかける

と，$\sigma^2\cdot H_4=\sigma^2\cdot\{e,\tau\}=\{\sigma^2,\sigma^2\cdot\tau\}$となることも分かるでしょう.

従って，

$$S_3=H_4\cup\sigma\cdot H_4\cup\sigma^2\cdot H_4$$

となっています（下図参照）：

H_4	$\sigma\cdot H_4$	$\sigma^2\cdot H_4$
$\{e,\ \tau\}$	$\{\sigma,\ \sigma\cdot\tau\}$	$\{\sigma,\ \sigma^2\cdot\tau\}$

～S_3の部分群H_4による右軌道分解～

いわば，

S_3が3つの“軌道（剰余類ともいう．昨日の講義ノートを参照）”に分割

されており，しかも，

これらの軌道は互いに交わらない

ようにできています．このような方法で，S_3 を分割することを，

S_3 の部分群 H_4 による右軌道分解

といいます．次に，H_4 に対して，

“右から” σ をかける

と，$H_4\cdot\sigma=\{e,\tau\}\cdot\sigma=\{\sigma,\tau\cdot\sigma\}=\{\sigma,\sigma^2\cdot\tau\}$ となることが分かるでしょう．また，

“右から” σ^2 をかける

と，$H_4\cdot\sigma^2=\{e,\tau\}\cdot\sigma^2=\{\sigma^2,\tau\cdot\sigma^2\}=\{\sigma,\sigma\cdot\tau\}$ となることも分かるでしょう．

従って，

$$S_3=H_4\cup H_4\cdot\sigma\cup H_4\cdot\sigma^2$$

となっています：

H_4	$H_4\cdot\sigma$	$H_4\cdot\sigma^2$
$\{e,\ \tau\}$	$\{\sigma,\ \tau\cdot\sigma=\sigma^2\cdot\tau\}$	$\{\sigma^2,\ \tau\cdot\sigma^2=\sigma\cdot\tau\}$

～S_3 の部分群 H_4 による左軌道分解～

これまた，これらの軌道は互いに交わることがありません．このような方法で，S_3 を分割することを，

S_3 の部分群 H_4 による左軌道分解

といいます．

今，S_3 の部分群 H_4 による右と左の軌道分解を比較してみると，これらは異なるものであることが分かります：

H_4	$\sigma\cdot H_4$	$\sigma^2\cdot H_4$
$\{e,\ \tau\}$	$\{\sigma,\ \sigma\cdot\tau\}$	$\{\sigma,\ \sigma^2\cdot\tau\}$

この軌道↑と同じ軌道はある↓　　けれど，他の２つの軌道は下の２つの軌道のいずれとも同じでない

H_4	$H_4\cdot\sigma$	$H_4\cdot\sigma^2$
$\{e,\ \tau\}$	$\{\sigma,\ \tau\cdot\sigma=\sigma^2\cdot\tau\}$	$\{\sigma^2,\ \tau\cdot\sigma^2=\sigma\cdot\tau\}$

★　（問）S_3 の部分群 H_5 による右軌道分解と左軌道分解をしてみましょう．上記と同様、左右で軌道分解が異なることが分かるはずです．また，H_6 による右軌道分解と左軌道分解をしてみましょう．これまた，左右で軌道分解が異なることが分かるはずです．

次に,

S_3 の部分群 H_3 による右軌道分解

および,

S_3 の部分群 H_4 による左軌道分解

をしてみましょう．すると，前者は,

$$S_3 = H_4 \cup \tau \cdot H_4$$

H_4	$\tau \cdot H_4$
$\{e, \sigma, \sigma^2\}$	$\{\tau, \tau\cdot\sigma = \sigma^2\cdot\tau, \tau\cdot\sigma^2 = \sigma\cdot\tau\}$

～S_3 の H_4 による右軌道分解～

となり，後者は,

$$S_3 = H_4 \cup H_4 \cdot \tau$$

H_4	$H_4 \cdot \tau$
$\{e, \sigma, \sigma^2\}$	$\{\tau, \sigma\cdot\tau, \sigma^2\cdot\tau\}$

～S_3 の H_4 による左軌道分解～

となることが分かります.

この二つの軌道分解を比較してみると，これらは

同じものである

ことが分かるでしょう．それもそのはずで，$\tau \cdot H_3 = H_3 \cdot \tau$ だからです：

このように,

左右の軌道分解が一致するようにできる部分群

を特に,

“正規部分群”

と呼びます.

先走りますと,

Galois 理論とはこの正規部分群に支えられた理論

なのです.

S_3の正規部分群は，このH_3と，$\{e\}$と，S_3の 3 つです.

★（問）これを確かめてみましょう.

【剰余群(商群)】

さて，ここでGaloisの天才ぶりの一端をご覧いただきましょう．

Galois によれば，正規部分群による軌道分解で生ずる軌道同士で演算を定義することができて，各軌道をひとつの元と見て

新しい群

を誕生させることができるというのです．これは一体，どういったことでしょうか．

今，$N=\{x_1, x_2, \cdots, x_n\}$（$x_1=e$とする）を群$G$の正規部分群であるとします．

このとき，ここまでで見てきたように，

$$\boxed{G=N\cdot y_1 \cup N\cdot y_2 \cup \cdots \cup N\cdot y_m}$$

のように軌道分解することができます（ただし，$y_1=e$とします）．

これらm個の軌道は全て同じ個数の元からなり，かつ各軌道は互いに交わりがありませんので，Gの元の個数は，mnです（Laglangeの定理といいます）．

また，

$$N\cdot y_i=\{x_1\cdot y_i, x_2\cdot y_i, \cdots, x_n\cdot y_i\},\ N\cdot y_j=\{x_1\cdot y_j, x_2\cdot y_j, \cdots, x_n\cdot y_j\}$$

であり，これらn個の元同士で作ったn^2個の元からなる集合

$$\{(x_1\cdot y_i)\cdot(x_1\cdot y_j),\ (x_1\cdot y_i)\cdot(x_2\cdot y_j),\ \cdots,\ (x_1\cdot y_i)\cdot(x_n\cdot y_j)$$

$$(x_2\cdot y_i)\cdot(x_1\cdot y_j),\ (x_2\cdot y_i)\cdot(x_2\cdot y_j),\ \cdots,\ (x_2\cdot y_i)\cdot(x_n\cdot y_j)$$

$$\cdots$$

$$(x_n\cdot y_i)\cdot(x_1\cdot y_j),\ (x_n\cdot y_i)\cdot(x_2\cdot y_j),\ \cdots,\ (x_n\cdot y_i)\cdot(x_n\cdot y_j)\}$$

を考えると，実は，これは，n個の元からなる集合

$$(N\cdot y_i)\cdot y_j=\{(x_1\cdot y_i)\cdot y_j, (x_2\cdot y_i)\cdot y_j, \cdots, (x_n\cdot y_i)\cdot y_j\}$$

と

一致する

のです．つまり，

“見かけ”

はn^2個の元から成っているのですが，実は元はn個しかないというわけです（つまりダブって登場する）．ちょっと不思議な感じがするかもしれませんが，実際，そうなるのです．

このことを，今考えている３次対称群S_3を例として見てみましょう．

① $H_3 \cdot e\ (=H_3)$の３個の元と，$H_3 \cdot e\ (=H_3)$の３個の元との演算で作られる９個の元からなる集合は，$H_3 \cdot e = \{e, \sigma, \sigma^2\}$ゆえ，

$$\{e, \sigma, \sigma^2, \sigma, \sigma^2, e, \sigma^2, e, \sigma\}$$

ですが，ダブりが確認できますから，やはりこれは見かけ上は９個の元からなる集合ではあるものの，実際は，

$$(H_3 \cdot e) \cdot e = \{e, \sigma, \sigma^2\} (= H_3)$$

と一致していることが分かるでしょう．

② $H_3 \cdot e\ (=H_3)$の３個の元と，$H_3 \cdot \tau$の３個の元との演算で作られる９個の元からなる集合は，$H_3 \cdot e = \{e, \sigma, \sigma^2\}$，$H_3 \cdot \tau = \{\tau, \sigma \cdot \tau, \sigma^2 \cdot \tau\}$ゆえ，

$$\{\tau, \sigma \cdot \tau, \sigma^2 \cdot \tau, \sigma \cdot \tau, \sigma^2 \cdot \tau, \tau, \sigma^2 \cdot \tau, \sigma\tau, \tau\}$$

ですが，これまたダブりが確認できますから，やはりこれは見かけ上は９個の元からなる集合ではあるものの，実際は，

$$(H_3 \cdot e) \cdot \tau = \{\tau, \sigma \cdot \tau, \sigma^2 \cdot \tau\}\ (= H_3 \cdot \tau)$$

と一致していることが分かるでしょう．

③ $H_3 \cdot \tau$の３個の元と，$H_3 \cdot \tau$の３個の元との演算で作られる９個の元からなる集合は，$H_3 \cdot \tau = \{\tau, \sigma \cdot \tau, \sigma^2 \cdot \tau\}$ゆえ，

$$\{e, \sigma^2, \sigma, \sigma, e, \sigma^2, \sigma^2, \sigma, e\}$$

ですが，これまたダブりが確認できますから，やはりこれは見かけ上は９個の元からなる集合ではあつものの，実際は，

$$(H_3 \cdot \tau) \cdot \tau = \{e, \sigma, \sigma^2\} (= H_3)$$

と一致していることが分かるでしょう．

なるほど，どうやら成り立っていそうだなと実感してもらえればここでは十分です．今日は，群の話はあくまでも復習ですので，深入りをしないでおきます．ここでは，証明は省略して先を急ぎます．

さて，そうすると先ほど作った（見かけ上）n^2 個の元からなる集合は，

$$(N\cdot y_i)\cdot(N\cdot y_j)$$

と表記されるのが自然なことでしょう（事実，一般にこのように表記されます）．
すると，

$$\boxed{(N\cdot y_i)\cdot(N\cdot y_j)=(N\cdot y_i)\cdot y_j}$$

ということになり，これすなわち，

軌道同士の演算が定義された

ということになります．
この定義によって得られる

$S_3=H_3\cup H_3\cdot\tau$ の軌道分解における各軌道同士の演算

は次のようになります：

・	H_3	$H_3\cdot\tau$	逆　元
H_3	H_3	$H_3\cdot\tau$	H_3
$H_3\cdot\tau$	$H_3\cdot\tau$	H_3	$H_3\cdot\tau$

なるほど，

$\{H_3, H_3\cdot\tau\}$ が群をなしている

ことが分かるでしょう．そして，この場合，これは 2 次の巡回群 Z_2 となっていることも分かると思います．
このようにして作られる群を，

群 G の正規部分群 N による剰余群（商群）

と呼び，

$$G/N$$

と表します．
ここでの例ですと，

$$S_3/H_3\cong Z_2$$

というわけです．

では，次の問題を演習することで理解の定着を図りましょう．

【問題】

固定された 4 つの点 A, B, C, D があり，正方形 $p_1p_2p_3p_4$ が，p_1 は A に，p_2 は B に，p_3 は C に，p_4 は D に置かれているとします．このとき，この正方形の合同変換の操作は，操作の合成を演算として群 G をなします（この群 G は“二面体群”と呼ばれます）．

（1）それを乗積表を作ることにより示してみましょう．

（2）G の正規部分群は全部で 10 個あります．それを全て見つけてみましょう．その 10 個の内，1 つの軌道が 4 つの元からなる正規部分群（どれでもよい）と，1 つの軌道が 2 つの元からなる正規部分群（これもどれでもよい）とによる剰余群はどのようなものとなっているか調べてみましょう．

（解答）

（1）何もしない操作を e，対角線の交点 I の周りに $90^\circ n$ $(n=1,2,3)$ 回転する操作を σ_n，辺 AB, BC, CD, DA の中点をそれぞれ E, F, G, H とするとき，直線 EG に関する対称移動を τ_1，直線 FH に関する対称移動を τ_2，直線 AC に関する対称移動を τ_3，直線 BD に関する対称移動を τ_4 とする（図示してみましょう）と，$\{e, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2, \tau_3, \tau_4\}$ は，操作の合成を演算として群をなすことが次の乗積表によって分かる：

・	e	σ_1	σ_2	σ_3	τ_1	τ_2	τ_3	τ_4	逆　元
e	e	σ_1	σ_2	σ_3	τ_1	τ_2	τ_3	τ_4	e
σ_1	σ_1	σ_2	σ_3	e	τ_4	τ_3	τ_1	τ_2	σ_3
σ_2	σ_2	σ_3	e	σ_1	τ_2	τ_1	τ_4	τ_3	σ_2
σ_3	σ_3	e	σ_1	σ_2	τ_3	τ_4	τ_2	τ_1	σ_1
τ_1	τ_1	τ_3	τ_2	τ_4	e	σ_2	σ_1	σ_3	τ_1
τ_2	τ_2	τ_4	τ_1	τ_3	σ_2	e	σ_3	σ_1	τ_2
τ_3	τ_3	τ_2	τ_4	τ_1	σ_3	σ_1	e	σ_2	τ_3
τ_4	τ_4	τ_1	τ_3	τ_2	σ_1	σ_3	σ_2	e	τ_4

（2）G の 10 個の正規部分群は以下の通り：

$$G,\ \{e\},\ N_1=\{e,\sigma_2\}, N_2=\{e,\tau_1\}, N_3=\{e,\tau_2\}, N_4=\{e,\tau_3\}, N_5=\{e,\tau_4\},$$
$$N_6=\{e,\sigma_1,\sigma_2,\sigma_3\},\ N_7=\{e,\sigma_2,\tau_1,\tau_2\}, N_8=\{e,\sigma_2,\tau_3,\tau_4\}$$

このうち, 例えば, 4 個の元からなる正規部分群 N_6 によって, 剰余群 G/N_6 は,

下のような剰余分解（軌道分解）

$$G = N_6 \cup N_6 \cdot \tau_1$$

N_6	$N_6 \cdot \tau_1$
$\{e, \sigma_1, \sigma_2, \sigma_3\}$	$\{\tau_1, \sigma_1 \cdot \tau_1 = \tau_4, \sigma_2 \cdot \tau_1 = \tau_2, \sigma_3 \cdot \tau_1 = \tau_3\}$

～G の正規部分群 N_6 による軌道分解～

により，乗積表は,

・	N_6	$N_6 \cdot \tau_1$	逆　元
N_6	N_6	$N_6 \cdot \tau_1$	N_6
$N_6 \cdot \tau_1$	$N_6 \cdot \tau_1$	N_6	$N_6 \cdot \tau_1$

となり，$G/N_6 \cong Z_2$（2 次巡回群）となっていることが分かる.

また，例えば，2 個の元からなる正規部分群 N_2 によって，剰余群 G/N_2 は,
下のような軌道分解

$$G = N_2 \cup N_2 \cdot \sigma_1 \cup N_2 \cdot \sigma_2 \cup N_2 \cdot \sigma_3$$

N_2	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_3$
$\{e, \tau_1\}$	$\{\sigma_1, \tau_1 \cdot \sigma_1 = \tau_3\}$	$\{\sigma_2, \tau_1 \cdot \sigma_2 = \tau_4\}$	$\{\sigma_3, \tau_1 \cdot \sigma_3 = \tau_2\}$

～G の正規部分群 N_2 による軌道分解～

により，乗積表は,

・	N_2	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_3$	逆　元
N_2	N_2	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_3$	N_2
$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_3$	N_2	$N_2 \cdot \sigma_3$
$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_3$	N_2	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$
$N_2 \cdot \sigma_3$	$N_2 \cdot \sigma_3$	N_2	$N_2 \cdot \sigma_1$	$N_2 \cdot \sigma_2$	$N_2 \cdot \sigma_1$

となり，$G/N_2 \cong Z_4$（4 次巡回群）となっていることが分かる.

（注意）この二面体群 G は，D_4 と書かれます．昨日の春木先生の講義録の 1.3 を参照してください.

§2. E. Galois の示したこと

フランスの数学者 E.Galois（1811～1832）は

５次以上の代数方程式には根の公式が存在しない

ことを証明しました。

同時代人のノルウェーの数学者 N.Abel（1802～1829）は，体（たい）の理論を用いてこのことを証明しました.

（注意：イタリアの P.Ruffini（1765～1822）が最初にこのことを主張したようで（ただし，証明は不十分），今日，“Abel-Ruffini の定理”と呼ばれているようです).

Galois が Abel と異なるのは，Galois は，このことを

“群”

の問題に置き換えてそれを明らかにしたことです. いわば,

群と体とのからみあい

が

Galois 理論

の中核をなすのです.

ところで，体とはどのようなものでしょうか. それを次章で学びましょう.

§3. 体とはなんだろうか？

2つの自然数を足すと，その結果は必ず自然数になります.

ところが，引く場合はどうでしょうか．この場合は自然数にならないことがあります．たとえば，1と2を考えてみましょう.

2−1なら答えは1で，自然数になっていますが，1−2ですと，答えは−1ですから，自然数になっていません．ここで用語の復習をしておきましょう：

数の集合Xとその上で定義されている演算・に対し，

任意の$x, y \in X$に対して，$x \cdot y \in X$のとき，Xは演算・に関して閉じている

といい，

$x \cdot y \notin X$となるx, yが存在するとき，Xは演算・に関して閉じていない

といいます.

従って，$X = N$，・を＋や−とすると，

自然数は加法に関しては閉じているが，減法に関しては閉じていない

となります.

$X = N, Z, Q$ で，・を＋，−，×，÷としたときの閉じている場合は○，閉じていない場合は×で表すと，次のようになります：

・	＋（加法）	−（減法）	×（乗法）	÷（除法）
N（自然数）	○	×	○	×
Z（整数）	○	○	○	×
Q（有理数）	○	○	○	○

一般に，集合Xが，加減乗除全てに関して閉じているとき，Xは

体

をなしているといいます.

つまり，有理数は体をなしているというわけです（有理数体と呼ぶ).

この他には，有理数を含む実数や，実数を含む複素数も体になります（実数体，複素数体)．また，これらの体から新しい体を作ることもできます．例えば，

有理数体Qに$\sqrt{2}$を付け加えて，なおかつ加減乗除に関して閉じる

ようにしてできる集合などがそうです．ここで，注意して欲しいのは，

Qに$\sqrt{2}$を付け加えただけの集合$Q \cup \{\sqrt{2}\}$は体にはならない

ということです．これは次のことからすぐ分かります．たとえば，

$$-\frac{1}{3},\sqrt{2}\in Q\cup\left\{\sqrt{2}\right\}$$

ですが,

$$-\frac{1}{3}+\sqrt{2},-\frac{1}{3}-\sqrt{2},-\frac{1}{3}\sqrt{2},-\frac{1}{3\sqrt{2}}=-\frac{\sqrt{2}}{6}\quad\cdots\quad(※)$$

はいずれも$Q\cup\left\{\sqrt{2}\right\}$に入っていません．では，$Q$に$\left\{\sqrt{2}\right\}$を付け加えるだけでなく，加減乗除に関して閉じるようにした集合はどのように表されるでしょうか．これは,

$$a+b\sqrt{2}\ (a,b\in Q)$$

の形で表される集合になります. なぜ，このような形で表すことができるのかを示すには相当の準備が必要になりますので，ここでは省略します．ただし，(※)を見ると，なるほどそんな感じがするな，と思ってもらえるのではないでしょうか（例えば，$-\frac{1}{3\sqrt{2}}\left(=-\frac{\sqrt{2}}{6}\right)$なら$a=0,\ b=-\frac{1}{6}\ (a,b\in Q)$です）．

★（問）このような形の数（つまり，$a+b\sqrt{2}\ (a,b\in Q)$）の集合が加減乗除に関して閉じていることを確認してみましょう．

さて，一般に，有理数体Qに，$\alpha\in Q$を付け加えて作られる体のうち，最小のものを$Q(\alpha)$と表すとき,

$Q(\alpha)$は，Qにαを添加してできるQの拡大体

と呼ばれます.

さて，さきに Galois 理論の構造の中核をなすのは

群と体とのからみあい

であるといいました．このことをお話することとしましょう．

Galois の理論を，体の理論によって整理したのは，ドイツの数学者 R.Dedekind（1831～1916）やオーストリアの数学者 E.Artin（1898～1962）です．とりわけ重要な役を担うのが,

体の自己同型写像

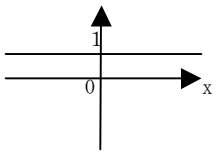
といえます.

この体の自己同型写像こそが，群と体とをからみ合わせる役を担っているのです.

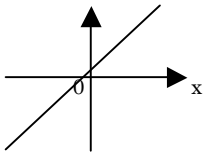
§4. 体の自己同型写像とは？

まず，簡単にこれまで体験してきたであろう写像の例を挙げて，復習してみましょう．以下で，R は実数体とします．

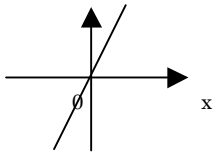
① $f:R\to R\ \ f(x)=1$



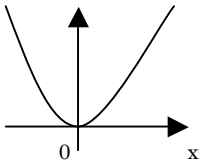
② $f:R\to R\ \ f(x)=x$



③ $f:R\to R\ \ f(x)=2x$

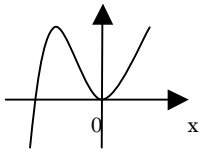


④ $f:R\to R\ \ f(x)=x^2$



これに，高校数学で学ぶものも加えておきます：

⑤ $f:R\to R\ \ f(x)=(x+1)x^2$



これらを考察してみましょう．

①は，x が変化しても $f(x)$ は１のまま変化しない，いわば“足踏み”です．

②，③は，x が実数全体を動くと，$f(x)$ も実数全体を動いて，なおかつ，$x\neq y$ なら $f(x)\neq f(y)$ です．いわば，スタートが異なればゴールも異なっています．

④は，xが実数全体を動くと，$f(x)$は非負の実数を動きます．そして，スタートが異なってもゴールが同じことがあります．例えば，$f(1)=1=f(-1)$です．

⑤は，xが実数全体を動くと，$f(x)$も実数全体を動きますが，スタートが異なってもゴールが同じことがあります．例えば，$f\left(-\frac{2}{3}\right)=\frac{4}{27}=f\left(\frac{1}{3}\right)$です（これは高校数学で極値や変曲点を学ぶと分かります）．

一般に，集合Xの数を集合Xの数に対応させる写像fの中で，

Ⅰ．$x\neq y$なら$f(x)\neq f(y)$であるものを

「単射」

といいます．　～単射とはスタートが異なればゴールも異なる写像～

また，

Ⅱ．任意のyに対し，$f(x)=y$となるxが存在するものを

「全射」

といいます．

Ⅲ．「全射」であり，なおかつ「単射」であるものは

「全単射」

と呼ばれます．

したがって，さきに挙げた写像は，

① ④は全射でも単射でもない　②，③は全単射　⑤は単射ではありませんが，全射ではある，ということになります．因みに，自然現象の記述によく用いられる写像である$f:R\to R\ \ f(x)=e^x$は全射ではありませんが，単射ではあります．

さて，次に，①から⑤までの写像で，

“加減乗除を保存する”

ものはあるでしょうか．つまり，和（差，積，商）の写像は写像の和（差，積，商）になるでしょうか，例えば，

①では，$x,y\in R$に対し，$f(x+y)=1,\ f(x)+f(y)=1+1=2$により，保存してい

ないことがすぐにわかります．このようにしてみると，$f(x)=x$だけは，和差積商全てを保存することが分かります．

★ （問）実際にそれを確認してみましょう．

一般に，体Xに対し，全単射写像$f:X\to X$が和差積商全てを保存する場合，fを体Xの**自己同型写像**といいます．

さきの例ですと，$f(x)=x$は実数体Rの自己同型写像というわけです．こんな例もあります．有理数体Qの拡大体における自己同型です：

（例）

$X=Q(\sqrt{2})=\{a+b\sqrt{2}\,|\,a,b\in Q\}$に対し，$f(a+b\sqrt{2})=a+b\sqrt{2}$は$X$の自己同型写像になっています．また，$g(a+b\sqrt{2})=a-b\sqrt{2}$も$X$の自己同型写像になっています．

これらの事柄を示すために，有理数体Qの拡大体（これを）K（とおく）の自己同型写像fに関する性質はどのようなものがあるのかを調べることにしましょう．

有理数体Qの拡大体Kの自己同型写像f に関する重要な3性質：

（性質１） $f(0)=0$

（性質２） $f(1)=1$

（性質３）任意の$x\in Q$（有理数）に対して， $f(x)=x$

（注意１）（性質３）は（性質１）と（性質２）の２つから導き出されます．

（注意２）（性質３）の見方は，

QはKの自己同型の不変元の集合（固定体）

であるということです．（性質１）は，$0=0+0$で，この両辺に自己同型写像fを

施すことにより示されます．（性質２）は$1=1\times1$の両辺にfを施すこと，およびfの単射性により示されます．（性質３）は，$n\in N$に対して，$n=1+1+\cdots+1$ゆえ，fを両辺に施すことにより$f(n)=n$が，また，$-n=0-n$ゆえ，fを両辺に施すことにより，$f(-n)=-n$を示すことができます．よって，$m(\neq 0), n\in Z$に対し，

$$f\left(\frac{n}{m}\right)=\frac{f(n)}{f(m)}=\frac{n}{m}$$

となるわけです．これらの性質によって，$X=Q\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\mid a,b\in Q\right\}$に対し，

$$f\left(a+b\sqrt{2}\right)=a+b\sqrt{2} \text{ と } g\left(a+b\sqrt{2}\right)=a-b\sqrt{2}$$

がXの自己同型写像になっていることを示すことができます．

★ （問）それを示してみましょう．

示す過程で，$X=Q\left(\sqrt{2}\right)=\left\{a+b\sqrt{2}\mid a,b\in Q\right\}$の自己同型写像は，$f$と$g$だけしかないことも同時に分かります．そして，写像の合成を演算として，自己同型写像の集合$\{f, g\}$は次の表から分かるように，２次巡回群Z_2をなします：

・	f	g	逆　元
f	f	g	f
g	g	f	g

（単位元はf）

このように，体の自己同型写像の集合が群をなすことが分かり，なるほど，群と体とが絡み合う様子が垣間見ることができました．ここまでの種々の準備によって，ようやくお待ちかねの

Galois 理論

そのものに触れることができます．では，本編の始まりです．

§５．代数方程式の根の公式が存在するとはどういうことか

そもそも，

“代数方程式 $f(x)=0$ に根の公式が存在する“

とはどういったことを指すのでしょうか.

（注意）本稿では，解ではなく，“根”ということにします.

それは,

> **係数の加減乗除とべき根（$\sqrt[n]{a}\ (a\in F)$ の形の数）をとるという操作だけで根を求めることができれば，公式が存在するといい，そうでなければ存在しない**

ということです．これをノルウェーの数学者 Abel は体の拡大という視点で次のように言い換えました：

> **方程式 $f(x)=0$ の係数を含む体を F_0（係数体と呼ぶ）とし，この係数体 F_0 から始めて，以下のような，べき根を添加して作った体（巡回拡大体という）の列**
>
> $$F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_l$$
>
> $$F_{j+1}=F_j\left(\sqrt[m_j]{a_j}\right),\quad a_j\in F_j,\ \sqrt[m_j]{a_j}\notin F_j$$
>
> **に対して，その方程式の全ての根が体 F_l（根体という）に見出すことができること**

です．記号に圧倒されそうですが，まずは，2 次方程式 $x^2+ax+b=0$ の場合で確かめて納得しましょう．ご承知の通り，この方程式の根の公式は，$x=\dfrac{-a\pm\sqrt{a^2-4b}}{2}$ です.

今，係数体 F_0 は Q としておきます（すなわち，$a,b\in Q(=F_0)$）

(1st STEP) $a,b\ (\in F_0)$ に対し，a^2-4b を計算する（加減乗除）.

(2nd STEP) a^2-4b の 2 乗根を計算する（べき根）.

(3rd STEP) $\sqrt{a^2-4b}$ に $-a$ を足す，又は，$-a$ から引く．（加減乗除）

(4th STEP) $-a\pm\sqrt{a^2-4b}$ を 2 で割る（加減乗除）

すなわち， $a, b\ (\in F_0)$ に対し， $a^2-4b(\in F_0)$ のべき根 $\sqrt{a^2-4b}$ を F_0 に添加して作った拡大体 $F_1=F_0\left(\sqrt{a^2-4b}\right)$ の中に，2 次方程式 $x^2+ax+b=0$ の 2 つの根が収まる，ということです.

Abel は，4 次方程式までなら，このような作り方で，方程式全ての根を含むような拡大体に到達することができるけれど, 5 次以上の方程式についてはそれができない，と主張しました.

その主張を Galois は“群”の問題に置き換えて明確にしました（いわゆる Galois 理論）. まずは，2 次方程式の Galois 理論を眺めてみましょう.

尚，以降では係数体を F，根体を K と書くことにします.

§6. 2次方程式の Galois 理論

2 次方程式 $px^2+qx+r=0$ は，両辺を $p\ (\neq 0)$ で割ることにより，

$$x^2+ax+b=0\cdots①$$

とすることができます．今，係数体を F とします．すなわち，$a,b\in Q(=F)$ とし，①の異なる 2 根を α,β とすると，

“①の根体（すなわち，①の全ての根を含む最小の体）”

K は，

$$K=F(\alpha,\beta)=Q(\alpha,\beta)$$

となります．ここで，（$x=\alpha$ は①の根ゆえ）

$$\alpha^2+a\alpha+b=0\cdots②$$

が成り立つので，

K の“F 上の自己同型”（すなわち，$F(=Q)$ を固定体とする K の自己同型）f を②の両辺に施すと，

（注意）先に述べた（性質 3）により，f は Q を不変にする（つまり，$f(q)=q,q\in Q)$ ので，単に“K の自己同型 f ”を②に･･･，でもよいのですが，あえて書いている理由は後述（§8 にて）します.

$$f(\alpha^2+a\alpha+b)=f0)$$
$$\therefore f(\alpha^2)+f(a\alpha)+f(b)=f(0)$$
$$\therefore \{f(\alpha)\}^2+f(a)f(\alpha)+b=0$$
$$\therefore \{f(\alpha)\}^2+af(\alpha)+b=0$$

となり，$f(\alpha)$ も①の根であることが分かります．よって，f は，次表のように，f_1 または f_2 となります：

	f_1	f_2
α の行き先（像）	α	β
β の行き先（像）	β	α

ここで，

$$f\left((\alpha-\beta)^2\right)$$

を考えると，f が f_1 であろうと，f_2 であろうと，

$$\begin{aligned}f\left((\alpha-\beta)^2\right)&=\{f(\alpha-\beta)\}^2\\&=\{f(\alpha)-f(\beta)\}^2\\&=(\alpha-\beta)^2(=(\beta-\alpha)^2)\end{aligned}$$

となります．つまり，

$(\alpha-\beta)^2$ は K の自己同型写像 f の不変元である

というわけです．ここで，さきの（性質 3）の逆である

$f_2(x)=x$ ならば $x\in Q$（有理数）である

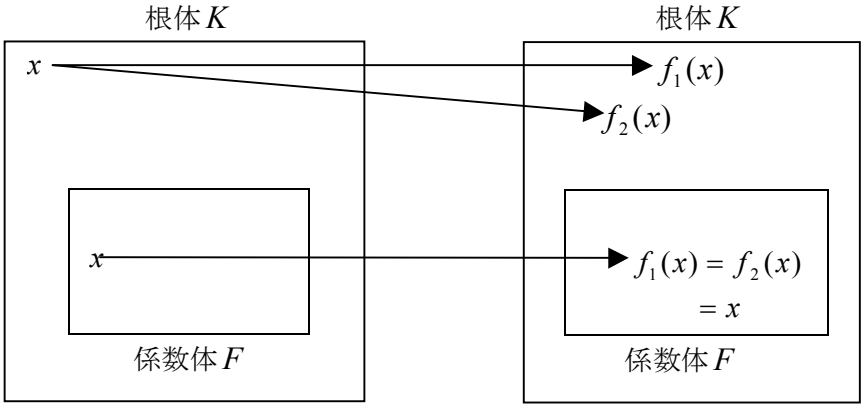
も成り立ちます．

（証明） $x=p\alpha+q\in K$, $p,q\in Q$ に対し，

$$\begin{aligned} f_2(x) &= f_2(p\alpha)+f_2(q) \\ &= f_2(p)\,f_2(\alpha)+q \\ &= p\beta+q \end{aligned}$$

$$\therefore\ p\alpha+q=p\beta+q$$

$\therefore\ p(\alpha-\beta)=0$ となるが，$\alpha\neq\beta$ ゆえ，$p=0$　$\therefore\ x=q\in Q$　■



「$x\in K-F$ の場合の $Aut(K/F)$ の元の像（行き先）」と，
「$x\in F$ の場合の $Aut(K/F)$ の元の像（行き先）」のイメージ図

このことから，今，$f_2\left((\alpha-\beta)^2\right)=(\alpha-\beta)^2$（すなわち，$(\alpha-\beta)^2$ が f_2 の不変元である）なので，

$$(\alpha-\beta)^2\in Q$$

であることが分かります．つまり，f_2 によって，$(\alpha-\beta)^2$ の正体が判明したというわけです．もとより，根と係数の関係から，$\alpha+\beta=-a$ で，$a\in Q$ ゆえ，

$$\begin{cases} \alpha+\beta=\text{有理数} \\ \alpha-\beta=\sqrt{\text{有理数}} \end{cases}$$

となり，この連立方程式を解くと，

$$\{\alpha,\ \beta\}=\left\{\frac{-a+\sqrt{\text{有理数}}}{2},\ \frac{-a-\sqrt{\text{有理数}}}{2}\right\}$$

を得ます．すなわち，

α が，有理数のべき根と有理数との加減乗除から求められる

ことが判明しました．$\beta=-a-\alpha$ なので，$Q(\alpha,\beta)=Q(\alpha)$ となり，

$$K=Q(\alpha,\ \beta)=Q(\alpha)=Q\left(\sqrt{\text{有理数}}\right)$$

であることも同時に判明し，なるほど，2 次方程式には根の公式が存在するというわけです．これが

2 次方程式の Galois 理論

というわけです．ここで，$\{f_1,\ f_2\}$は，写像を合成する操作を演算として，次の乗積表により群をなしていることが分かります（単位元は，f_1 です）：

・	f_1	f_2	逆元
f_1	f_1	f_2	f_1
f_2	f_2	f_1	f_2

すなわち，

$K=F(\alpha)$ の“F 上の自己同型”写像全体の集合 $Aut(K/F)$ は，写像の合成を演算として 2 次巡回群 Z_2 をなす

ことがわかりました．すなわち，

$$Aut(K/F)\cong Z_2$$

です．ここで，≅は“群として等しい”という意味での等号です．

以上をまとめて，自己同型群と体との関係は，つぎのように表せます：

【群と体は次のように1：1に対応する】

体←・・・・・→群

$K=F(\alpha,\beta)=F(\alpha)$ ←・・・・・→ K は $\{f_1\}$ の固定体

| である

・・・♯ $Aut(K/F)(=2)$ 次拡大

$F=Q$ ←・・・・・→ F は $Aut(K/F)=\{f_1,f_2\}\cong Z_2$ の固定体

重要なこと（と後で分かりますが）は，

$\{f_1,\ f_2\}$ が巡回群である

ということです．

§7. 3次方程式の Galois 理論

3 次方程式 $p_0y^3+p_1y^2+p_2y+p_3=0$ は，両辺を $p_0\ (\neq 0)$ で割ることにより，

$y^3+q_1y^2+q_2y+q_3=0$ とすることができます．さらに，$y=x-q_1/3$ とおくことにより，$x^3+ax+b=0$ とできる（つまり 2 次の項を消去できる）ので，3 次方程式といえば，はじめから

$$x^3+ax+b=0\cdots①$$

としてよいことになります．

★（問）実際に確かめてみましょう．

今，$a,b\in Q(\omega)\ (=F)$ とします．ここで，ω は 1 の 3 乗根のひとつで，1 とは異なるものとします（**係数体 F を，$F=Q$ ではなく，$F=Q(\omega)$ としておくのが“便利”なのは§8 にて解説します**）．

今，①の異なる 3 根を，$x=\alpha,\beta,\gamma$ とすると，①の根体 K は，$K=F(\alpha,\beta,\gamma)$ となります．

ここで，（$x=\alpha$ は①の根ゆえ）

$$\alpha^3+a\alpha+b=0\cdots②$$

が成り立つので，

K の“F 上の自己同型”（つまり，$F(=Q(\omega))$ を固定体とする K の自己同型）f を②の両辺に施すことにより，

$$f(\alpha^3+a\alpha+b)=f(0)\text{ より，}\quad f(\alpha^3)+f(a\alpha)+f(b)=0$$

$$\therefore\quad (f(\alpha))^3+f(a)f(\alpha)+b=0$$

$$\therefore\quad (f(\alpha))^3+af(\alpha)+b=0$$

となり，

$f(\alpha)$ も①の根である

ことが分かります．当然，

$f(\beta),\ f(\gamma)$ も①の根である

ことが分かります．

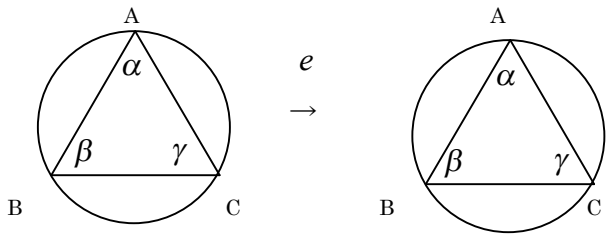
よって，f は，α, β, γ を入れ替える 6 つの写像のいずれかであることが分かります：

	e	f_1	f_2	g_1	g_2	g_3
α の像	α	γ	β	α	γ	β
β の像	β	α	γ	γ	β	α
γ の像	γ	β	α	β	α	γ

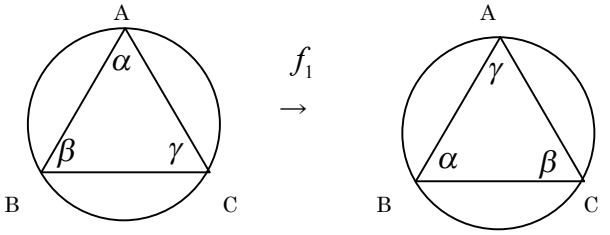
この 6 つの写像は，以下のような操作であると解釈できます：

固定された 3 つの点 A，B，C があり，正三角形$\alpha\beta\gamma$ が，α は A に，β は B に，γ は C に置かれているとすると，

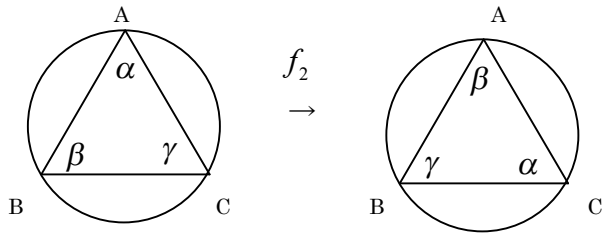
写像eは，正三角形$\alpha\beta\gamma$ に“何もしない”操作と考えられます.



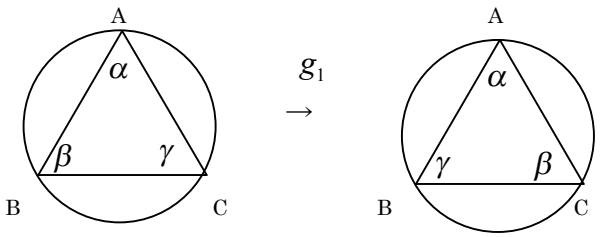
写像 f_1 は，正三角形$\alpha\beta\gamma$ を“重心を中心として，反時計回りに 120° 回転させる”操作と考えられます.



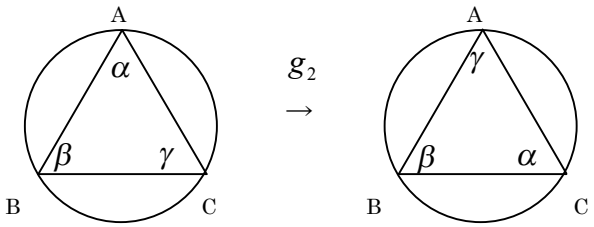
写像 f_2 は，正三角形$\alpha\beta\gamma$ を“重心を中心として，反時計回りに 240° 回転させる”操作と考えられます.



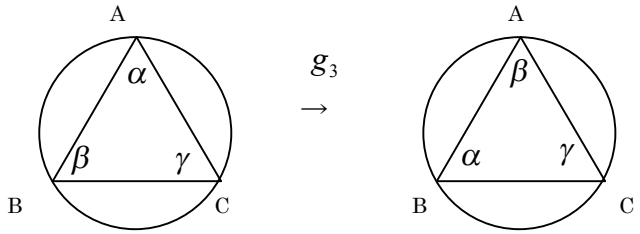
写像 g_1 は，正三角形 $\alpha\beta\gamma$ を“∠A の二等分線に関して対称移動させる”操作と考えられます.



写像 g_2 は，正三角形 $\alpha\beta\gamma$ を“∠B の二等分線に関して対称移動させる”操作と考えられます.

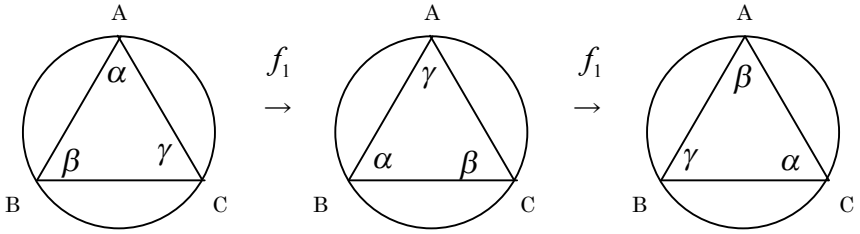


写像 g_3 は，正三角形 $\alpha\beta\gamma$ を“∠C の二等分線に関して対称移動させる”操作と考えられます.

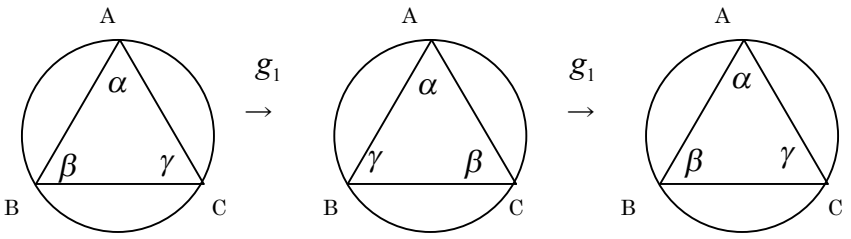


これらの操作に関して，写像の合成・を演算としてつぎのことが分かります. 例えば,

（1） f_1 ・ $f_1 = f_2$ となります（つまり，120° 回転を 2 回施せば 240° 回転になる）:



（2） $g_1 \cdot g_1 = e$ となります（つまり，同一の線対称移動を 2 回施せば，何もしていないことと同じになる）：



★（問） $f_1 \cdot g_1$ と $g_1 \cdot f_1$ はそれぞれどのような操作であるといえるでしょうか．
また，$f_1 \cdot g_1 \neq g_1 \cdot f_1$ であることを確認しましょう．

これらにより，“乗積表”を作ると，次のようになります：

$\cdot$	e	f_1	f_2	g_1	g_2	g_3	逆元
e	e	f_1	f_2	g_1	g_2	g_3	e
f_1	f_1	f_2	e	g_2	g_3	g_1	f_2
f_2	f_2	e	f_1	g_3	g_1	g_2	f_1
g_1	g_1	g_3	g_2	e	f_2	f_1	g_1
g_2	g_2	g_1	g_3	f_1	e	f_2	g_2
g_3	g_3	g_2	g_1	f_2	f_1	e	g_3

これは３次対称群 S_3 の場合と同じ乗積表となります．つまり，

３次方程式①の根体（＝全ての根を含む最小の体）K の“F 上の自己同型”写像の集合 $Aut(K/F)$ は，写像の合成・を演算として3次対称群 S_3 をなす

ことが分かりました．すなわち，

$$Aut(K/F) \cong S_3$$

です．ここで，≅は“群として等しい”という意味での等号です．今，$Aut(K/F)$ の“部分群”を考えてみましょう．S_3 の部分群は，全部で６つあります．それを，今の場合で見てみると，次のようになっています：

$$S_3 \text{自身},\ \{e\},\ H_1 = \{e, g_1\},\ H_2 = \{e, g_2\},\ H_3 = \{e, g_3\},\ N = \{e, f_1, f_2\}$$

ここで問題です：

“３次巡回群” $N = \{e, f_1, f_2\}$ の元で不変となる K の元はどのような集合か？

今，そのような集合をMと表すことにすると，

（答・その１）　Mは体をなす

ことが分かります．なぜなら，任意の$x, y \in M$と任意の$f \in N$に対して，

（ｉ）　$f(x+y)=f(x)+f(y)=x+y$　　$\therefore\ x+y \in M$

（ⅱ）　$f(x-y)=f(x)-f(y)=x-y$　　$\therefore\ x-y \in M$

（ⅲ）　$f(xy)=f(x)f(y)=xy$　　$\therefore\ xy \in M$

（ⅳ）　$f\left(\dfrac{x}{y}\right)=\dfrac{f(x)}{f(y)}=\dfrac{x}{y}\quad (y \neq 0)$　　$\therefore\ \dfrac{x}{y} \in M$

となり，Mは四則演算に関して閉じているからです．さらに，

（答・その２）　任意の$x \in M$に対して，$g_1(x)=g_2(x)=g_3(x) \in M$であり，

さらに，任意の$x \in M-F$に対して，$g_1(x) \neq x$である

ことも分かります．何故でしょうか？実は，これを考えることが，

３次方程式の Galois 理論の「幹」

にあたります．まずは，さきほど作った乗積表をながめつつ，次を確認してみましょう．例えば，

$$f_1 \cdot g_1 = g_1 \cdot f_2$$

が成り立っていますから，任意の$x \in M$に対して，$f_1(g_1(x))=g_1(f_2(x))$であることが分かります．ここで，$f_2(x)=x$ですから，結局，$f_1(g_1(x))=g_1(x)$であることが分かります．つまり，

$g_1(x)$はf_1によって不変な数である

わけです．また，

$$f_2 \cdot g_1 = g_1 \cdot f_1$$

が成り立っていますから，任意の$x \in M$に対して，$f_2(g_1(x))=g_1(f_1(x))$であることが分かり，$f_1(x)=x$により，$f_2(g_1(x))=g_1(x)$であることが分かります．同様にして，

$$f_1(g_2(x))=g_2(x), f_2(g_2(x))=g_2(x), f_1(g_3(x))=g_3(x), f_2(g_3(x))=g_3(x)$$

を示すことが出来ます．

★（問）では，これらを実際に示してください．

もとより，$e(g_1(x))=g_1(x), e(g_2(x))=g_2(x), e(g_3(x))=g_3(x)$です．よって，

$$g_1(x),\ g_2(x),\ g_3(x) \in M$$

であることが分かりました.

また， $x = f_1(x)$ ゆえ， $g_1(x) = g_1(f_1(x)) = g_3(x)$ であり， $x = f_2(x)$ でもあるので，

$g_1(x) = g_1(f_2(x)) = g_2(x)$ と分かります．さらに，もし， $x \in M - F$ に対して $g_1(x) = x$ であれば， $g_1 \in N$ となってしまうので $g_1(x) \neq x$ となり，結局，

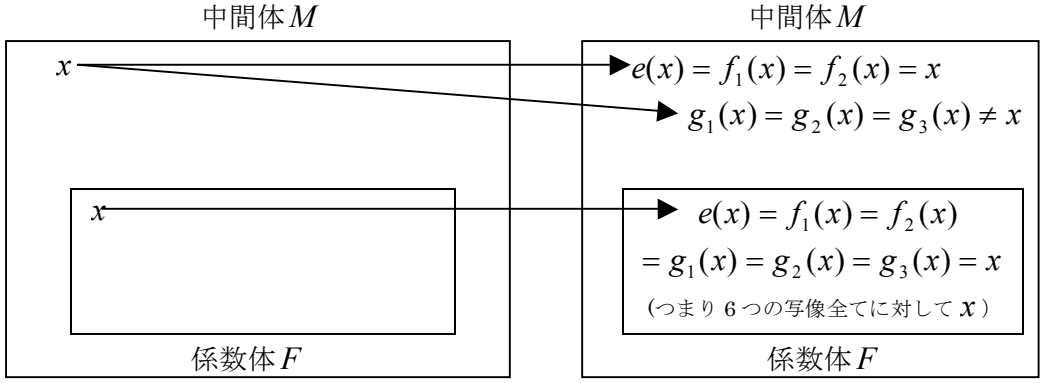
$$x \neq g_1(x) = g_2(x) = g_3(x) \in M - F$$

であることが分かります.

ここまで見てきたように，

$$\{e, f_1, f_2, g_1, g_2, g_3\} \text{は} M \text{に制限しても自己同型写像}$$

になっています.



「$x \in M - F$ の場合の $Aut(K/F)$ の元の像（行き先）」，
「$x \in F$ の場合の $Aut(K/F)$ の元の像（行き先）」のイメージ図

すると，一見， $Aut(K/F) \cong S_3$ であると同様に，

$$Aut(M/F) \cong S_3$$

のようですが，任意の $x \in M$ に対して，

$$f_1(x) = f_2(x) = f_3(x) \in M \text{ ， } g_1(x) = g_2(x) = g_3(x) \in M, f_1(x) \neq g_1(x),$$

ですので， $\sharp\, Aut(M/F) = 6$（$= \sharp\, S_3$）ではなく， $\sharp\, Aut(M/F) = 2$ であることに注意してください.

次に， $s \in M - F$ とし， $g_i(s) = t$ $(i = 1, 2, 3)$ とします（当然， $s \neq t$ です）.

今， $g_i(g_i(s)) = g_i(t)$， $g_i(g_i(s)) = s$ より， $g_i(t) = s$ と分かります.

$$\therefore g_i(s+t)=g_i(s)+g_i(t)=t+s$$

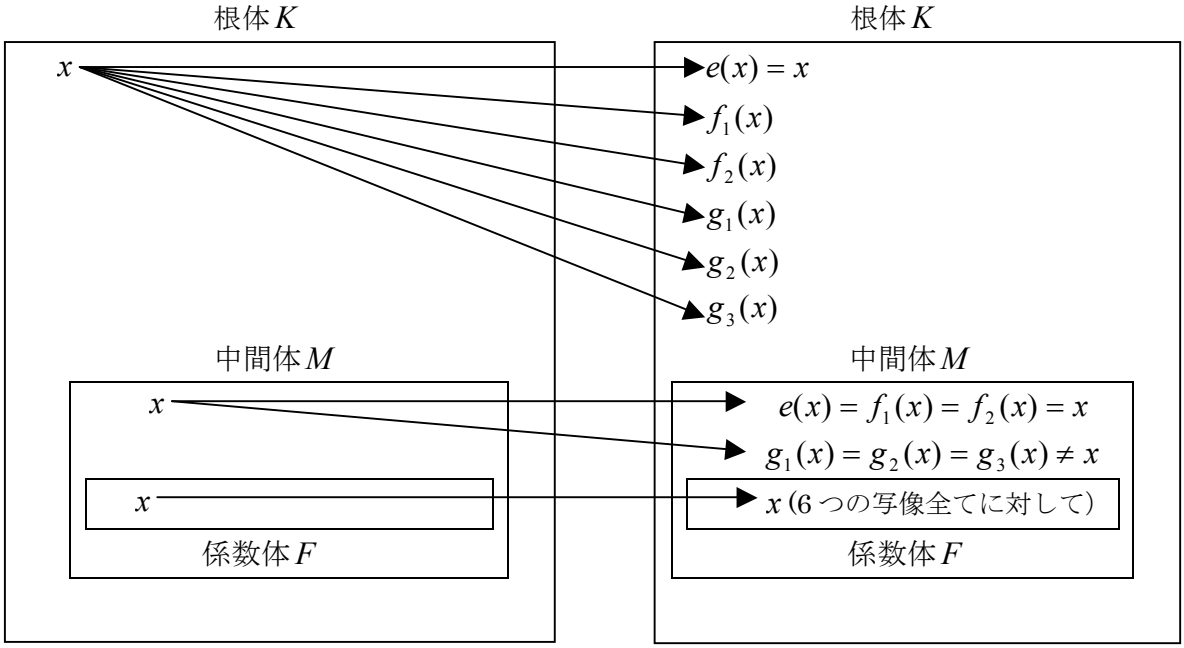
$$\therefore s+t \text{ は } g_i \text{ の不変元である}$$

となり，これにより，$s+t\in F=Q(\omega)$と分かります.

これは，先ほど述べたように，$x\in M$ に対して

$$g_i(x)\begin{cases}=x\ (x\in F\subset M)\\ \neq x\ \ (x\in M-F)\end{cases}$$

であることによります.



「$x\in K-M$ の場合の $Aut(K/F)$ の元の像（行き先）」，「$x\in M-F$ の場合の $Aut(K/F)$ の元の像（行き先）」，「$x\in F$ の場合の $Aut(K/F)$ の元の像（行き先）」のイメージ図

※それぞれの場合について，どの写像が x を不変元としているかを見てみましょう.

さらに，

$$\begin{aligned}g_i\left((s-t)^2\right)&=\left(g_i(s-t)\right)^2\\&=\left(g_i(s)-g_i(t)\right)^2\\&=(t-s)^2\\&=(s-t)^2\end{aligned}$$

なので，

$(s-t)^2$ は g_i の不変元

と分かり，先程の議論同様，$(s-t)^2 \in F = Q(\omega)$ であることが分かります．

よって，$\begin{cases} s+t = Q(\omega) \text{ の元} \\ s-t = \sqrt{Q(\omega)} \text{ の元} \end{cases}$ なる連立方程式を得て，これを解いて，

$$s = \left(Q(\omega) \text{の元} + \sqrt{Q(\omega) \text{の元}}\right)/2, \quad t = \left(Q(\omega) \text{の元} - \sqrt{Q(\omega) \text{の元}}\right)/2$$

を得ます．したがって，

$$M = F\left(\sqrt{n}\right),\ n \in F = Q(\omega)$$

であることが分かります．すなわち，

M は F のべき根拡大体である

ことが分かりました．これが M の正体というわけです．

さて，ここまでくればいよいよ，$K = F(\alpha, \beta, \gamma)$ の正体を知る態勢が整いました．つまり，つぎのような問題を解くことになります：

K は M のどのような拡大体になっているのか？

今，

$$\boxed{p = \left(\alpha + \beta\omega + \gamma\omega^2\right)^3,\ q = \left(\alpha + \beta\omega^2 + \gamma\omega\right)^3} \qquad \cdots (☆)$$

を考えます．もちろん，$p, q \in K = F(\alpha, \beta, \gamma)$ です．

ここで，$N = \{e, f_1, f_2\}$ の元による，p, q の行き先（像）を調べてみましょう．まず，明らかに，

$$e(p) = p,\ e(q) = q$$

です．また，

$$f_1(p) = p,\ f_1(q) = q,\ f_2(p) = p,\ f_2(q) = q$$

であることが示せます．例えば，$f_2(q) = q$ なら次のように示されます：

$$f_2(q) = f_2\left(\left(\alpha + \beta\omega^2 + \gamma\omega\right)^3\right) = \left(f_2(\alpha) + f_2(\beta) f_2\left(\omega^2\right) + f_2(\gamma) f_2(\omega)\right)^3$$

$$= \left(\gamma + \alpha\omega^2 + \beta\omega\right)^3 \omega^3 = \left(\alpha + \beta\omega^2 + \gamma\omega\right)^3 = q \quad (\because\ \omega^3 = 1)$$

★（問） $f_1(p) = p,\ f_1(q) = q,\ f_2(p) = p$ であることを実際に示してみましょう．

つまり，

$$p, q \in M$$

というわけです．ところで，さきほど示したように，$M = F\left(\sqrt{n}\right), n \in F$ でした．

すなわち，

p, q は，F の元と，その平方根とからなる数の加減乗除で作られる数

です．さらに，

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha + \beta\omega + \gamma\omega^2 = \sqrt[3]{p} \\ \alpha + \beta\omega^2 + \gamma\omega = \sqrt[3]{q} \end{cases}$$

（第一式は，根と係数の関係による）なので，この連立方程式を解くと，

$$\begin{cases} \alpha = \left(\sqrt[3]{p} + \sqrt[3]{q}\right)/3 \\ \beta = \left(\sqrt[3]{p}\omega + \sqrt[3]{q}\omega^2\right)/3 \\ \gamma = \left(\sqrt[3]{p}\omega^2 + \sqrt[3]{q}\omega\right)/3 \end{cases}$$

とできます．ここから分かることは，

α, β, γ は M の元と，その 3 乗根とからなる数の加減乗除で作られる数

であるということです．すなわち，

$$K = M\left(\sqrt[3]{m}\right), m \in M$$

であり，

K は M のべき根拡大体になっている

ことが分かりました．以上をまとめてみます：

3 次方程式 $x^3 + ax + b = 0$ の根は，係数体である $F = Q(\omega)$ のべき根拡大（拡大次数は，一般には 2×3＝6）により得られる．すなわち，

3 次方程式には，根の公式が存在する

これが **3 次方程式の Galois 理論**というわけです．塔の形で書いておきます：

$$K = M\left(\sqrt[3]{m}\right),\ m \in M$$

$$\Big|\quad \cdots\cdots \text{3 次拡大}$$

$$M = F\left(\sqrt{n}\right),\ n \in F$$

$$\Big|\quad \cdots\cdots \text{2 次拡大}$$

$$F = Q(\omega)$$

こうして当座の目標であった 3 次方程式には根の公式が存在することが判明しましたが，これを解明できた最大のカギは，

$$\boxed{Aut(K/F) \cong S_3 \text{に“正規部分群”} N \text{が存在する}}$$

ことによるものだということは繰返し強調しておきたいことです.

最後に，2 次方程式のときと同様に，群と体との対応を考えておきましょう.

N は S_3 の単なる部分群ではなく，正規部分群でした．それゆえ，

剰余群（商群）S_3/N

を考えることができます.

つまり， N と $g_1 \cdot N (= g_2 \cdot N = g_3 \cdot N = N \cdot g_1 = N \cdot g_2 = N \cdot g_3)$ の交わりなく，

$$S_3 = N \cup g_1 \cdot N$$

とでき（下図参照），

N	$g_1 \cdot N$
$\{e, f_1, f_2\}$	$\{g_1, g_2, g_3\}$

～ S_3 の正規部分群 N による軌道分解～

$S_3/N \cong Z_2$ の乗積表は次のようになります：

$\cdot$	N	$g_1 \cdot N$	逆 元
N	N	$g_1 \cdot N$	N
$g_1 \cdot N$	$g_1 \cdot N$	N	$g_1 \cdot N$

よって， $S_3/N \cong Z_2$ （2 次巡回群）であることが分かります.

これが $Aut(M/F)$ なのです．つまり，

$$Aut(M/F) \cong S_3/N \cong Z_2$$

というわけです．さきの「$x \in K-M$ の場合の $Aut(K/F)$ の元の像（行き先）」，「$x \in M-F$ の場合の $Aut(K/F)$ の元の像（行き先）」，「$x \in F$ の場合の $Aut(K/F)$ の元の像（行き先）」のイメージ図を再度見て理解を深めてください．

先程，具体的な計算により F から M へのべき根拡大の拡大次数が 2 であることと，M から K へのべき根拡大の拡大次数が 3 であることを示しました．一方，

$$\#(S_3/N)=2,\ \#(N/\{e\})=3$$

（もちろん，$N/\{e\} \cong N$）

です．すなわち，

$\#(S_3/N)$とFからMへのべき根拡大の拡大次数とが，

そして，

$\#(N/\{e\})$とMからKへのべき根拡大の拡大次数とが

それぞれ一致していることが分かります．

重要なことは，

正規部分群の列$\{e\} \subset N \subset S_3$が存在し，

剰余群$S_3/N,\ N/\{e\}(\cong N)$がいずれも巡回群（$S_3/N \cong Z_2,\ N/\{e\}\ (\cong N) \cong Z_3$）

であるということです．

（復習）2 次方程式でも，**正規部分群の列$\{f_1\} \subset \{f_1,\ f_2\} \cong Z_2$が存在し，**
剰余群$Z_2/\{f_1\}(\cong Z_2)$が巡回群でした．

ここで，洞察力鋭い皆さんは，

「おや！2 次と 3 次の場合で似ているな．ここに公式の存在の有無のカギがあるのだろうか？」

と思ったのではないでしょうか．その予想が一層はっきりする様に，群と体との関係を“塔”の形で表しておきます：

（3 次方程式）　　【群と体は次のように1：1に対応する】

体　←・・・・・→　群

$K = M\left(\sqrt[3]{m}\right),\ m \in M$ ←・・・・・→ K は $\{e\}$ の固定体

・・・・・ ＃ $Aut(K/M)\ (=3)$ 次拡大

$M = F\left(\sqrt{n}\right),\ n \in F$ ←・・・・・・・・→ M は $N = \{e,\ f_1,\ f_2\} \cong Z_3$ の固定体

である

・・・・・ ＃ $Aut(M/F)(=2)$ 次拡大

$F = Q(\omega)$ ←・・・・・・・・・・・・→ F は $Aut(K/F) \cong S_3$ の固定体

（注意） $Aut(M/F) \cong S_3/Z_3 \cong Z_2,\ Aut(K/M) \cong Z_3/\{e\} \cong Z_3$

再録（3 次の場合との類似を強調したい）

（2次方程式）　　【群と体は次のように1：1に対応する】

体　←・・・・・→　群

$K = F(\alpha,\ \beta) = F(\alpha)$ ←・・・・・→ K は $\{f_1\}$ の固定体である

・・・・ ＃ $Aut(K/F)(=2)$ 次拡大

$F = Q$　←・・・・・→ F は $Aut(K/F) \cong Z_2$ の固定体

（注意） $Aut(K/F) \cong Z_2/\{f_1\} \cong Z_2$

ここまで見てきた中で,

集合の正体を知りたければ写像を調べよ

というのは非常に有効な手段であることが了解されたことと思います．ここまでの議論を再度読み返してそれを味わってください.

§8. 3 次方程式の係数体 F を $Q(\omega)$ にしておく理由

なぜ，3 次方程式 $x^3+ax+b=0$ の係数体 F を， $F=Q$ ではなく， $F=Q(\omega)$ として考えるのが“便利”なのでしょうか.

それは，例えば， $p=\left(\alpha+\beta\omega+\gamma\omega^2\right)^3$ に対する $f_1(p)$ の計算において，

$$f_1(p)=(f_1(\alpha)+f_1(\beta)f_1(\omega)+f_1(\gamma)\{f_1(\omega)\}^2)^3=\cdots=p$$

を示したいのですが，$F=Q(\omega)$ を固定体とする $f\in Aut(K/F)$ としておかないと，

$f_1(\omega)$ が ω のみならず ω^2 の可能性

もでてきます.

（Θ） $f(1)=f(\omega^3)=\{f(\omega)\}^3=1$ より， $f(\omega)=1,\omega,\omega^2$ のいずれかとなりますが，

f の単射性より $f(\omega)\neq 1$ と分かることによります. ■

ここで， $f(\omega)=\omega^2$ とすると， $f(p)\neq p$ となってしまうのです.

よって， $f(\omega)=\omega$ としておくというわけです.

（注意） §7 における $\boxed{p=\left(\alpha+\beta\omega+\gamma\omega^2\right)^3,\ q=\left(\alpha+\beta\omega^2+\gamma\omega\right)^3}$ ・・・(☆)

を考えることができたので，3 次方程式の根の公式の存在に関する議論がスムーズに進んだわけですが，果たして“(☆）の出自はいずこ”でしょうか. これは“Laglange Resolvent（ラグランジュ分解式)”と呼ばれるものです. 初日の平山先生の講義録をご覧ください. 気になる読者には専門書を紐解くきっかけになると思われます.

§9.　3 次方程式の係数体 F を Q としても不便ではない例

では，3 次方程式の場合に，$F=Q$ として考えても不便ではないケースというのはないのでしょうか.

$$p=\left(\alpha+\beta\omega+\gamma\omega^2\right)^3,\quad q=\left(\alpha+\beta\omega^2+\gamma\omega\right)^3$$

において，$p\in Q, q\in Q$ であれば $F=Q(\omega)$ としなくとも $F=Q$ として不便はありません．なぜなら，根体 $K=F(\alpha,\beta,\gamma)$ の自己同型 f に対し，

$$f(p)=p, f(q)=q$$

が成り立つからです．　このような場合の例を考えてみましょう.

【例 1】$\alpha=1,\beta=\omega,\gamma=\omega^2$（すなわち，方程式 $x^3-1=0$ の場合）

$p=\left(1+\omega^2+\omega\right)^3=0\in Q, q=\left(1+1+1\right)^3=27\in Q$ となっています．この場合，$F=Q$ とすると，$K=Q\left(1,\omega,\omega^2\right)$ ですが，$Aut(K/F)$ の元は，下表の 6 つ

	e	f_1	f_2	g_1	g_2	g_3
$\alpha=1$ の像	$\alpha=1$	$\gamma=\omega^2$	$\beta=\omega$	$\alpha=1$	$\gamma=\omega^2$	$\beta=\omega$
$\beta=\omega$ の像	$\beta=\omega$	$\alpha=1$	$\gamma=\omega^2$	$\gamma=\omega^2$	$\beta=\omega$	$\alpha=1$
$\gamma=\omega^2$ の像	$\gamma=\omega^2$	$\beta=\omega$	$\alpha=1$	$\beta=\omega$	$\alpha=1$	$\gamma=\omega^2$

ではないのです．それは，f_1，f_2，g_2，$g_3\notin Aut(K/F)$ だからです．というのも，$Aut(K/F)$ の元によって，$\alpha=1$ の像は 1 でなければならないにも関らず，これら 4 個の写像はそのようになっていないからです.
従って，$\{e,g_1\}\in Aut(K/F)$ ゆえ，$Aut(K/F)\cong Z_2$ ということになり，

$$Aut(K/F)\cong S_3 \text{ でない場合もある}$$

という例になっています（“一般に” S_3 になる，としてきた所以です）.

思えば，$\omega^2=-1-\omega$ ゆえ，$K=Q\left(1,\omega,\omega^2\right)=Q(\omega)$ なので，$Aut(K/F)$ を求める場合，K の自己同型による ω の像だけを考えればよいわけです.
K の自己同型 f による ω の像は，ω または ω^2 のいずれかなので,

(i)　$f(\omega)=\omega$ なら，$f(\omega^2)=\left(f(\omega)\right)^2=\omega^2$，$f(1)=f(\omega^3)=\left(f(\omega)\right)^3=\omega^3=1$

となります．これは表における e のことであり，

(ii)　$f(\omega)=\omega^2$ なら $f(\omega^2)=\left(f(\omega)\right)^2=\omega^4=\omega$，$f(1)=f(\omega^3)=\left(f(\omega)\right)^3=\omega^6=1$

となり，これは表における g_1 のことであるというわけです.
よって， $Aut(K/F)=\{e, g_1\}\cong Z_2$ となります．（乗積表は省略します）.

（3次方程式） $x^3-1=0$ での群と体は次のように1:1に対応する

体　←・・・・・→　群

$K=F(1, \omega, \omega^2)=Q(\omega)$ ←・・・・・→ K は $\{e\}$ の固定体

| である

| ・・・♯ $Aut(K/F)(=2)$ 次拡大

$F=Q$　←・・・・・→ F は $Aut(K/F)=\{e, g_1\}\cong Z_2$ の固定体

【例 2】 $\alpha=\sqrt[3]{2}, \beta=\sqrt[3]{2}\omega, \gamma=\sqrt[3]{2}\omega^2$ （すなわち，方程式 $x^3-2=0$ の場合）

$p=\left(\sqrt[3]{2}+\sqrt[3]{2}\omega^2+\sqrt[3]{2}\omega\right)^3=2\in Q$, $q=\left(\sqrt[3]{2}+\sqrt[3]{2}+\sqrt[3]{2}\right)^3=54\in Q$ となっています．この場合， $F=Q$ とすると， $K=Q\left(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\omega^2\right)$ ですが， $\omega^2=-1-\omega$ ゆえ，

$K=Q\left(\sqrt[3]{2}, \sqrt[3]{2}\,\omega, \sqrt[3]{2}\omega^2\right)=Q\left(\sqrt[3]{2}, \omega\right)$ なので， $Aut(K/F)$ を求める場合， K の自己同型による $\sqrt[3]{2}$ と ω の像だけを考えればよいことになり，それは下表のように 6 つの元が考えられます：

	e	f_1	f_2	g_1	g_2	g_3
$\sqrt[3]{2}$ の像	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\omega$	$\sqrt[3]{2}\omega^2$
ω の像	ω	ω	ω	ω^2	ω^2	ω^2

この 6 つの元の，操作の合成による乗積表はつぎの通りです：

・	e	f_1	f_2	g_1	g_2	g_3	逆元
e	e	f_1	f_2	g_1	g_2	g_3	e
f_1	f_1	f_2	e	g_2	g_3	g_1	f_2
f_2	f_2	e	f_1	g_3	g_1	g_2	f_1
g_1	g_1	g_3	g_2	e	f_2	f_1	g_1
g_2	g_2	g_1	g_3	f_1	e	f_2	g_2
g_3	g_3	g_2	g_1	f_2	f_1	e	g_3

すなわち，$Aut(K/F)\cong S_3$ で，$\{e, f_1, f_2\}\cong Z_3$ が $Aut(K/F)$ の正規部分群をなしています．また，$e(\omega)=f_1(\omega)=f_2(\omega)=\omega$（すなわち，$\{e, f_1, f_2\}$ は ω を不変元としている）ゆえ，$\{e, f_1, f_2\}$ の固定体は $Q(\omega)$ であることが分かり，次の対応を得ます：

（3 次方程式）　$x^3-2=0$ での群と体は次のように１：１に対応する

体　←・・・・・→　群

$K=Q(\sqrt[3]{2}, \omega)$ ←・・・・・→ K は $\{e\}$ の固定体

・・・・・＃ $Aut(K/M)$ $(=3)$ 次拡大

$M=Q(\omega)$ ←・・・・・・・・→ M は，$N=\{e, f_1, f_2\}\cong Z_3$ の固定体である

・・・・・＃ $Aut(M/F)$ $(=2)$ 次拡大

$F=Q$ ←・・・・・・・・・・・・→ F は $Aut(K/F)\cong S_3$ の固定体

（注意）$Aut(M/F)\cong S_3/Z_3\cong Z_2$，$Aut(K/M)\cong Z_3/\{e\}\cong Z_3$

(注意)一般の 3 次方程式について，根の公式が存在するか否かを考える際，係数体 F を $F=Q(\omega)$ とするのが“便利”であることを見ました．これは，“便利”ということであって，$F=Q$ では考えることができない，ということではありません．

実際，上記で見たように $x^3-2=0$ は $F=Q$ から出発して，根体 K に到達し，$Aut(K/F)\cong S_3$ でした．

§10. 今日の復習，明日への予習

まずは今日の復習をしてみましょう：

【3 次方程式】根の公式は存在する

Ⅰ．係数体を $F=Q(\omega)$ とし，
Ⅱ．異なる 3 つの根を α,β,γ として，根体（3 つの根全てを含む最小の体）を $K=F(\alpha,\beta,\gamma)$ とすると，
Ⅲ．一般に， $Aut(K/F)\cong S_3$ となるので，
Ⅳ．この 3 次対称群 S_3 に**正規部分群の列** $S_3\supset Z_3\supset\{e\}$ **が存在し，**
Ⅴ．その正規部分群で作られる**剰余群の列** $S_3/Z_3, Z_3/\{e\}$ が**全て巡回群**になっていました．

【2 次方程式】根の公式は存在する

Ⅰ．係数体を $F=Q$ とし，
Ⅱ．異なる 2 つの根を α,β として，根体（2 つの根全てを含む最小の体）を $K=F(\alpha,\beta)$ とすると，
Ⅲ． $Aut(K/F)\cong Z_2$ となり，
Ⅳ．この Z_2 に**正規部分群** $\{e\}$ **が存在**し，
Ⅴ．その正規部分群で作られる**剰余群** $Z_2/\{e\}$ が**巡回群**になっていました．

以上の議論に倣い明日への予習といきましょう．
まず，４次方程式に公式が存在するか否かは次のように予想できます：

Ⅰ．係数体を F とし，
Ⅱ．異なる 4 つの根を $\alpha,\beta,\gamma,\delta$ として，根体（４根全てを含む最小の体）を $K=F(\alpha,\beta,\gamma,\delta)$ とすると，
Ⅲ．一般に， $Aut(K/F)\cong S_4$ となるので，
Ⅳ．この 4 次対称群 S_4 に**“正規部分群の列が存在するかどうか”**を調べ，
Ⅴ．存在する場合，その正規部分群で作られる
剰余群の列が全て巡回群になるかどうか
を見ることになります．

果たして，S_4には

$$\{e\} \subset Z_2 \subset V_4 \subset A_4 \subset S_4$$

なる正規部分群の列（前の群が後の群の正規部分群になっている）が存在します．ここに，A_4は4次交代群，V_4はKleinの4元群とよばれるもの（これらについても前回の春木先生の講義録を参照してください）です．

さらに，実は，

$$S_4/A_4 \cong Z_2,\ A_4/V_4 \cong Z_3,\ V_4/Z_2 \cong Z_2,\ Z_2/\{e\} \cong Z_2$$（全て巡回群！！）

となります．

★ （問）このことを確認してみましょう．

よって，KはFの2×2×3×2＝24次の巡回拡大となり，4次方程式の場合も

根の公式が存在することが予想

されるように思われます．

また，5次方程式に根の公式が存在するかどうかを調べたい場合は，

5次対称群であるS_5に正規部分群の列が存在するかどうかを調べればよい

ことになると推測されます．果たして，

$$\{e\} \subset A_5 \subset S_5$$

なる正規部分群の列は存在します．ここで，A_5は5次の交代群を表します．

次に，剰余群の列が全て巡回群になるかどうかを調べることになりますが，実は，

$S_5/A_5 \cong Z_2$**ではあるが，**$A_5/\{e\} \cong A_5$**は巡回群ではない**

のです．

従って，巡回拡大を行うことができないので，

根の公式は存在しないことが予想

されます．

実際，これらの予想は全て正しく，それを保障するのが Galois 理論であるというわけです.

5 次以上の方程式については,

n 次交代群 A_n は,
① $n \geq 4$ のとき，巡回群と同じ群とはならない.
② $\{e\}$ と自分自身以外に正規部分群をもたない（このような群は“単純群”と呼ばれます）

ことが知られていますので，根の公式が存在しないことが分かります.

$Z_3 \cong A_3$ であり，$Z_2 \cong S_2$ （2 次対称群）であることに注意してください.

ともあれ，詳しくは次回の網谷先生の講義録をご覧ください.

いかがでしたか．今回までの話で Galois 先生の天才ぶりがお分かりいただけたでしょうか.

私見では，３次方程式の Galois 理論が“実感”できれば，もはや Galois 理論は我々の掌中にあるも同然，と考えます.

では明日（次回）のフィナーレをお楽しみに.

参考文献

☆天才ガロアの発想力　　小島寛之著　　（技術評論社刊　2011 年）

ガロア生誕 200 年に花を添えたと言ってよい名著です. 泉下の Galois 先生も，ご自身の記念すべき年に，故国フランスから離れた東洋にてこのような書が出現したことを喜んでおられることと思われてなりません.

今回の講義は，本書を大いに参考にさせていただきました．かえって本書の珠玉の筆致及び内容が分かりづらいものになっていないことを祈るばかりです.

もともと私は，「高校への数学」（東京出版刊）に連載されていた小島先生によるガロア理論入門の記事を毎月読むのを楽しみにしており，単行本になるといいな，と思っていたところ，より平易に，しかも充実した内容となって本書が刊行されたので嬉しさも一入でした.

どの本をベースに講義をしようかと迷いに迷いましたが，最終的に本書しかない，という結論に達しました．皆さんも是非，入手されご一読頂くと得るところが少なくないと思われます.

☆代数学のレッスン　　雪田修一著　（サイエンティスト社・絶版）

ともすると，初学者には難解と思われがちな剰余群（商群）について，きわめて明解かつ分かりやすく書かれた快著です.

“軌道分解”なる用語は本書からの転用で，これは，本書の雰囲気を損ないたくなかった私の気持ちの現れです．ただし，現在，絶版になっているようで実に惜しい限りです．古書店などで見つけることが出来れば入手しておくことを強くお勧めします.

この他，以下の書物も大いに参考にさせて頂きました．お礼申し上げます.

☆環と体の理論（酒井文雄著・共立出版）
☆群と幾何学（難波誠著・現代数学社）
☆ガロワと方程式（草場公邦著・朝倉書店）
☆ガロアと群論（リリアン・リーバ著・みすず書房）
☆13 歳の娘に語る ガロアの数学 （金重明著・岩波書店）
☆現代思想（特集　ガロアの思考　第 39 巻 5 号・上野健爾ほか・青土社）
☆数学の視点（上野健爾著・東京図書）
☆ガロア理論（ジョセフ・ロットマン著・関口次郎訳・シュプリンガーフェアラーク東京）