第 34 回数学史シンポジウム (2024)　報告集

ガロアの「群」とは何を指すのか

梅田 亨　(**大阪公立大学数学研究所**)

はじめに：

本稿は，基本的に「数学史シンポジウム」での講演 (2024.10.12) に基づく．但し，そこで言及しきれなかった事柄についても，紙幅の許す限り補足したいと思う．

講演では，講演に至る経緯などにもそれなりに触れたが，ここでは立ち入らない．その代わり，関連する情報をいくつか記す．

まず，主催者の一人である佐藤文広氏の翻訳『代数学の歴史』(V.J. Katz・K.H. Parshall 著 / 佐藤勝造・佐藤文広訳 共立出版 2023) と，その正誤表 (特に注釈)：

`https://hondana-storage.s3.amazonaws.com/1040/files/11493_seigo.pdf`

そして，昨年度 (2023) の数学史シンポジウムの講演と報告集 (杉本遥菜氏).

これらが直接のきっかけだが，私自身が，ガロアについて過去に書いたものを一つだけ挙げておくと，“評伝・ガロア”『数学セミナー』 **40**-4 (2001), 24–27．ここには基本的な考え方を述べた．今回の内容は，それを敷衍・詳述するものではある．但し，講演および報告集原稿を準備する現在までの過程で，改めてガロアの論文を読み込み，よりガロア自身の思考に近づけた (まだまだ完全からは遠いが) と信ずる．このような機会を与えていただいた研究会関係者の方々に謝意を表したい．

[**注記**：主要人名は原綴でなくカタカナで書いた．講演タイトルで，深く考えずにガロアと書いてしまったので，それに引きずられる形になった．尤も，完全にそれを貫いたわけではない．]

要約：

扱う論文は，ガロアの「第一論文」と言われる “Sur les conditions de résolubilité des équations par radicaux” で，ガロアの全集 (二種類ある) には当然あるが，現在はネット上でも見ることができる：

https://www.gutenberg.org/files/40213/40213-pdf.pdf

特に，この前半部の，理論上の柱である主要な定理を，ガロア自身がどのように述べているか，そして我々がそれをどう読むべきかについて詳しく見たい．通常，そこに，現在の我々の知る「群概念」がでてきて，それを援用して方程式論が組み立てられると，つい想像してそう思い込む．そして，実際，数学史の本だけでなく，いくつかある「ガロア解説本」には，そのような形に “ガロア” が構成されてしまっている．だが，素直に読めば，決してそうは読めない．ヘタをすると，当時すでに「置換群」の概念が流布・発展していて，ガロアはそれを応用したかの如くに思い込むあまり，そう断定してしまっている本もある．が，実際は，ガロアはこの論文において，最初の基本定理を述べるのに,「順列」を用いているが,「置換」を用いたわけではない．では，ガロアは今日謂うところの「群」，特に「置換」のなす群に対応するものを全く得ていないのかというと，そうではなく，この論文において，初めてその概念が形作られる原初のさまが観察できる．我々は，まさにその姿を見る．その貴重な機会を目の前にしながら，最初から，現代の常識である「置換群」を密輸入してガロアを読むのでは，数学的創造のさまを感知できる折角の機縁をあたら放擲するに等しく，いかなる数学的感興にも到達しえない．

もちろん，先行するラグランジュの方程式論や，コーシーの置換論 (の一部) は存在していたが，ガロアの論文の最初の主要定理の理解には，その影響を (それがあるとしても) 無理に考慮する必要はない．独立して一貫した思想がガロアにはあるのだ．先行研究の影響を調べることとガロアを理解することは切り離して考えるべきものである．

[注：第 VII 節にはコーシーを引用する箇所がある]

講演および本稿の動機は，すべて，これらを改めて示したいという点にある．

方法：

「第一論文」は，基本的に完成したと考えてよい．従って，虚心坦懐に読むに限る．但し，決闘前夜に加筆し訂正した箇所もあるので，その点は考慮する必要がある．Bourgne-Azra

“Écrits et Mémoires Mathématiques D’Évariste Galois” (Gauthier-Villars 1962) には手稿にある異同等まで詳しく，必読の文献であるが，定年の引っ越しに伴い，手元に現物がすぐに取り出せない状態なので，目下徹底した検討ができない．ともかく，原稿への書き込みについての位置なども，出版物によって異なる場合もあり (そういう注意もなく出版されていることが多いから)，そういった事柄については，通常の論文より注意深く扱わなくてはいけないだろう．[ことに，論文の最初 Principes (用いる原理) という節で，補題 I の手前にある言明 (順列や置換の説明の箇所) については，この位置で適切なのかどうかは検討の余地が大いにある].

この点については，タヌリ (J. Tannery) の発表したガロアの遺稿 (1908) のメモが，ネット上で読めるので，それを参考にした：

https://archive.org/details/OeuvresMathmatiquesDvaristeGalois/page/n8/mode/1up

『ガロアの生涯』のインフェルトは，追記で，参考にした文献等の説明もかなり詳しく述べている．その中で，タヌリの公刊したものは，リウヴィルのものに比べて学問的価値は低いと断じる．たしかにそうではあるが，ガロアの言い回しの細かい点の解釈に悩む時，手稿の雑然とした記録ですら，それ自体に数学的な意味はなかったとしても，ガロアの普段の，言葉や記号の使い方，のようなものを知る上では有用だ．そのような細かすぎることは，単なる興味というより，ガロアの真意を知るための助けとして必要である．

紙幅もないのに，余談を付け加えるのは気がひけるが，このインフェルトの追記では，次のベルトランの証言が引かれている：

ポアソンが曖昧だと断じた論文を公表するにあたって，リウヴィルは彼にしては珍しい解説をつけたのである．その証明はきわめて理解し易い，と彼が言っているのを私は聞いたが，彼は私の驚きを見てとると言った.「なあに，一，二カ月ほかのことは何も考えずに，こればかりに没頭していればすぐにわかるさ.」

結論・主張：

ガロアの記述の細部すべてについて，逐語的に説明するだけの余裕はないので，以下にまず，重要な点を主張として挙げる：

(0)　ガロアの「第一論文」の主要部分を読んで，ガロアの書いていることを素直に読み解くとき，多くの解説が，ガロアが「順列」と書いているところを無理に「置換」と読み直して，現代風解釈を施している．しかし，ガロアの主張どおり,「順列」は「順列」のままで論文を読むことに何ら無理はなく，そう読むことでガロアの考えが自然に理解できる．

(1)　この「順列」の「あつまり」(groupe) からどのようにして現在われわれのいう**群**が導き出されるのか，その機構もガロアの書いていることから自然に読み取れる．

これらには，従来の解説と対立する部分もある一方，類似の主張をする解説もあるかと思う．先行する研究についての調査をするのも，本来の「数学史研究」の範囲だろうが，そこまで本格的に立ち入ることはできなかった．[この点は，ガロアが受容され，理論が変容していく歴史の一部としても重要だろうが，別の課題と考える].

いずれにしろ，上の主張の根拠は，ガロアの論文を読むことで得られるので，部分的には，逐語的にガロアを読むことを含む．従来の解釈と反する箇所については，その分，説明を丁寧にする必要がでてくる．

注意点：

以上を概要として，もう少し具体的に言葉の注意を述べよう．当然のことながら，同じ言葉がガロアに見られるからと言って，それが現代の我々が用いる意味であるかどうかは，検討を要する．大きなキーワードは permutation, substitution, groupe である．これらの意味は，ガロアの論文の用法を忠実にたどれば，誤解の余地は少ない．論文の重要な概念を，書いた本人が，混同すると考える理由はない．[にも拘らず，ガロアが混同すると断じる解説が多いのは何故なのだろうか].

他に，équation と fonction が，それぞれ，今日言う多項式と有理式の意味で用いられているのは，文脈からほぼ明らかである．無理に，方程式と函数と訳して解釈すると辻褄があわなくなる．

これらは，目立つ (何度も使われるから) ので判りやすい．それほど目立たないが，数学的に微妙な使い分けとして，racine, lettre がある．意味は文字どおり，根と文字ではあるが，これらを「入れ替える」という場面では，区別をする厳密性が要求されることがある．そして，ガロアは，その最も微妙な局面においては，繊細な区別をしているように見える．現代なら，すでに基礎が確立した事柄を述べるだけだろうが，ガロアに於いては，自分の

新理論を正確に伝える慎重さが要求される局面である．おのずと，誤解の生じない言葉を選ぶ細やかさが働いたと解釈できる．

文字 (不定元) とそこに数を代入したものの区別は，現代でも，文脈で判断できるような場合なら，煩わしいのでいちいち区別しないことが多い．ガロアにおいても，そのような書き方をしている箇所が少なくないが，区別が必要であれば言葉を変えているように読める．ついでに，論文中には現われないが，残っているメモの中には fonction de m indéterminée などと書かれている定理がある．これが現在の不定元と全く同じかどうかは断定的には言えないが，そういう意味があると考えても妥当性を損わないだろう．文字と数の区別が重大な問題を扱っているという注意は論文中の脚注にもあるのだから，これらの区別は注意して読むべきである．

これらが実際にどういう場面で使われているかは，あとで見る．

第一論文の中心部分とその概要：

既に述べたが，本稿の目的は，ガロアにおいて，主要な定理がどのように述べられ，証明され，その中から現在我々の知る「群概念」が析出してくるのか，という点であり，そこに絞って見る．「第一論文」の全部ではなく，詳しく見るのは Principes, Proposition I, Proposition II (用いる原理，第 I 節，第 II 節) に限る．それ以外に，関連してシュヴァリエへの遺書 (Lettre testamentaire: Lettre a Auguste Chevalier) の一部の解釈についても触れる．それらが，ガロアにおける「群」の意味を知る手がかりだからである．

数学的な内容としては，Principes の中で，定義などの説明を除くと，補題 I から補題 IV という主張と，第 I 節と第 II 節の主定理である．

このガロア論文の第一の眼目は，代数方程式の根から作られた未知の量の中から，既知の量を判別する明快な手段を与えることである．その手段が「根の順列の群」というものである (定義はあとで述べる)．現代では “群” は，演算をもった代数系だが，それはガロアの用語法ではない．

論文に即して読む前に概要を述べる．記号等はできるだけガロアに従うが，それが判りにくい場合には，少し変えることがある．いずれにしろ，ガロアを読むのだから，ガロアの書き方を尊重したい．[函数の記号も $f(V)$ と括弧をつけたり ψV とつけなかったりするが，基本は原文のままにする；もちろん，ガロアにない記号を補う場合は，その限りではない].

(i)　まず，既知の量とは，現代の言葉で，基礎に設定する体 (四則演算=有理演算が自由にできる世界) である．既知の量を係数にもつ代数方程式の根を $a, b, c, \cdots$ として，それらを既知の量に付け加え有理的に書けるもの (=体) が未知の量の全体と設定される．ここで，$a, b, c, \cdots$ の有理式 $V = \varphi(a, b, c, \cdots)$ で根 $(a, b, c, \cdots)$ (の順番) を並べ替えたとき，異なる並べ方で，すべて異なる値をとるようなものをとる (それが取れることが補題 II)．このとき，すべての根 $a, b, c, \cdots$ は V の有理式 (係数は既知量) で書けるというのが全ての鍵となる事実である (補題 III)．ここで考えている根 $a, b, c, \cdots$ の数を m として，V によって根 $a, b, c, \cdots$ を書く有理式を $\varphi, \varphi_1, \cdots, \varphi_{m-1}$ とする．[ここのところは，φ という記号が上で V を定めるものとして使われているから，混乱をもたらす不適切なものと思われるかもしれない．でも，ガロアはそのように書いている；但し，実は単なる混乱ではなく，理由があると考えられる．現在の常識から言えば，適切ではない記号を何故ガロアが使ったのかという推測は後で述べる．]

(ii)　一方，この V の満たす既約方程式の根を $V, V', \cdots, V^{(n-1)}$ とする．つまり，V の満たす，既知量係数の既約方程式 (現在の言葉では「ガロア分解式」) の共軛根を $V, V', \cdots$ として，方程式の次数を n とした．このとき，V によって根 $a, b, c, \cdots$ を表わす有理式 $\varphi, \varphi_1, \cdots, \varphi_{m-1}$ に，V の共軛 $V^{(l)}$ を代入すると，やはり元の方程式の根となる (補題 IV)．それを並べて**根の順列**

$$\varphi V^{(l)}, \quad \varphi_1 V^{(l)}, \quad \cdots, \quad \varphi_{m-1} V^{(l)}$$

ができる．それを簡単に $(V^{(l)})$ と書く．このようにして V の共軛から，n 箇の根の順列ができるが，その**全体** (集まり=groupe) が，ガロアの謂うところの「方程式の群」であり，時に略して「群」という．現代数学の用語のモトになった語であるが，それとは意味合いが異なる．後世の数学者 (特にデデキント) が借用し換骨奪胎して代数系の群の名前にしてしまった．以下，本家のガロアの用語の場合はカギカッコをつけ「群」と書いて区別する (充分紛らわしいし，心苦しいが，最小限のとりつくろい策である)．

この「順列の群」を用いてガロアは，未知量の中から既知量をとりだす判定基準を確立した．それが最初の主定理 (第 I 節) である．主張を述べておこう．まず，未知量とは，定義によって $a, b, c, \cdots$ の有理式で書けるもので，それを $F(a, b, c, \cdots)$ と書く．この並びを，上に述べた「根の順列」で置き換えて代入するという操作を考える．このとき，全ての「方程式の群」に対する置き換えによって値を変えない (同じ値をとる) ということと，その量が既知量であることが一致する．これが定理であり，簡潔にして明快な主張である．

「置き換え」と言っているので，置換群を考えているように思うかもしれないが，置き換え自体の操作がここに現われているのではない．代入する根の並びが，すでに「順列の群」として提示されているので，順列から順列への入れ替え操作自体に焦点は置かれていない (この時点では，そういう視点は全く必要ない)．つまり，現代の意味の群は，この定理の内容には関わってこない．

ここで大きな問題は，Principes で，補題に入る前に順列 (permutation) と，その「置換」(substitution) に言及した箇所である．これがあるので，最初から置換が重要な役割をするのかと思ってしまうが，実は，この箇所はあとから付け加えられたもので，一旦完成した論文に (決闘前夜だろうか) 加筆したものである．

順列から置換に考察の軸を移し，さらに現在いう群概念をとりだす動機は，おそらく次の節 (Proposition II) の定理に関わる．第 II 節の定理は，既知量に別の方程式の根を付け加えたときに順列の群がどう縮小するかという記述で，縮小した「順列の群」の性質を見ると，順列の置換という概念が自然に現われる．そのことと，そもそも，上に述べた「方程式の群」というのは，定義としては単なる順列の集まりではあるが，本来はそれにとどまらず，そこに内在的な構造 (特徴づけ) があるべきだ．そういう視点と認識が,「方程式の群」に属する順列について，それらの置換とその合成という観点を顕在化させ，現代的な意味での群概念を形作らせたと考えられる．

ガロアの言う「順列」は，現在謂う群の元としての置換ではなく，文字どおりの順列と解釈すべきである．この点の補足としてシュヴァリエへの手紙の最初の方にある,「群」G と「部分群」H の関係を書いた

$$G = H + HS + HS' + \cdots$$

と

$$G = H + TH + T'H + \cdots$$

という二種類の分解の仕方についての解釈についても補足したい．これを，G を現代の群と考えて，剰余類への分解だとする人が多いが，それでは右と左の区別がどこからでてくるのか理由が判然としない．しかし，G も H も順列のあつまりだと考えるなら，右と左の作用は，順列の二通りの入れ替えの仕方と見ると自然である．これも，当然のことながら，第 II 節の定理の内容の観察から見えてくる．無論，$S, S', \cdots$ と $T, T', \cdots$ は置換であって，こちらは順列ではない．

論文を読む：

では，論文の数学的内容に入って説明していく．

ここで文献について補足しておきたい．冒頭部分に挙げたネット上の，ガロア論文自体とタヌリの発表したもの，に加えて，ガロアの論文 (手書き) そのものの全体の写真を含む

`https://uberty.org/wp-content/uploads/2015/11/`
`Peter_M._Neumann_The_Mathematical_Writings.pdf`

の存在を知ることになった．これによって，加筆した部分の位置などが確認できる．ガロアの筆跡そのままに読める本当に貴重な文献である．著者は Peter M. Neumann で，タイトルは The mathematical writing of Évariste Galois である．英訳にあたって，フランス語原文とともに，語の用法などの詳細な検討が施され，コメントも微に入り細を穿つ．迂闊にも，そういう文献が 2011 年にヨーロッパ数学会 (European Mathematical Society) から出版されていることを知らなかった．400 ページに及ぶこの文献を，紙の本を手に入れたわけではないので，全体をパラパラとめくることすら果たしていないが，必読である．ただ，私は，上記のガロアの手稿自体に迫れるだけで，とりあえず満足である．

いずれにしろ，Bourgne-Azra のもの以上に詳しい情報が得られることになったのは望外の幸運であった [原稿を書き始めてかなり経ってから，この文献を知ることになったが，基本的な考えを補強してくれるものが得られた].

• Principes (用いる原理)：

ここでは定義と補題 (すべて知られているとガロアは書く) がまとめられている．[証明はやさしいので省略すると書いて，そこは消している．実際，補題 III と補題 IV には，証明をつけている．] ガロアは，このように自分の一貫した思考を「原理」としてまとめている．現在なら高校生が理解できる簡単な事実だけで済むという明澄な境地の提示である．

最初の定義は多項式 (原語は équation) が既約ということ．また，有理的などの言葉の説明があるが，このあたりは，現代人にとって何も頭を悩ますところはない．直ちに現代的な用語に翻訳できる．現代用語で，基礎の体をはっきりさせて多項式の既約性などを考えるという点への注意事項と言える．上ではガロアに忠実という基本態度を表明したが，それをやりすぎると却って判りづらくなる箇所である．

問題なのは，それに続く「順列」と「置換」の説明だが，これは，最初から論文にあっ

たのではなく，あとで付け加えられたものである (原稿の写真を見ると確認できる)．さらに，公表時になぜこのように編集され，この位置に置かれたのか，それが適切かどうかを含めて検討すべきである．従って，説明はあと (適切な場所) に廻す．[ここは，普通に読んでも異質な感じがするので，当然，注意深く読まないといけないと気づく筈だ．]

補題 I は既約多項式が，多項式と共通根を持った場合には，その多項式を割り切る，という言明．ここでは係数の体は決められている (既知の量) としている．

続く補題 II は次のような言明である：方程式が任意に与えられて，重根を持たないとする．その根を $a, b, c, \cdots$ とするとき，これらの根の有理式 V で，根のあらゆる並べ替え (動詞は permute の分詞形 permutant) に対し，すべての値が異なるものがある．証明は書いていないが，たとえば一次式で取れるという補足的注意がある．

補題 I, II の証明は省略している．ちょっと考えればできる程度のものだから．[補題 II は，無限体だからどうやってもできる．有限体の場合は今は考慮の外である．]

次の補題 III が議論の根幹となる命題である．補題 III と IV は，証明を見てこそガロアが何を考えていたか判る．証明は思考過程を知る重要なヒントである．ここは，丁寧に，数学的解説をしたい．

一つ注意すると，ちょっと奇妙なことにガロアは，考えている根 $a, b, c, \cdots$ の満たす方程式を全く書かない．ガロアの頭の中には，それを必要としないほど澄み切った世界が広がっていたのだろうと想像するが，説明のためには，それがないと不便なので，原論文にない記号を導入しておく：

$$\Phi(x) = (x-a)(x-b)(x-c)\cdots$$

とする．この $\Phi(x)$ の係数は，もちろん既知量としている．他の記号 F, f, φ などはガロアが使っているから，それ以外を選んだ．また，文字 x もあまり使わないようだ [定理の注では使っている] が，とりあえず普通の記号として選んだ．後では，根の数を m とするので，$\Phi(x)$ の次数は m としておく．また，$\Phi(x)$ は重根をもたないと仮定するが，既約性は仮定しない．既知量を増やした場合，一般に方程式は既約でなくなる．その様子が主題になるのだから，既約性を課さないのは当然である．

補題 III： 補題 II のように $V = \varphi(a, b, c, \cdots)$ をとると，最初に与えられた根 $a, b, c, \cdots$ は V の有理式 (係数は既知量) で書ける．

証明についてのコメントは後で述べるとして，まずは証明を書く．その中で，対称式の

基本定理に関係した一つの事実を使っているので，それを取り出して書いておく：ガロアにはないので，手っ取り早く現代的記法を使う．体 k 上の m 変数多項式環 $k[x_0,\cdots,x_{m-1}]$ に対称群 $\mathfrak{S}_m$ が変数の入れ替えで働くが，そのうち x_0 を動かさず残りの $x_1,\cdots,x_{m-1}$ だけに働くものを $\mathfrak{S}_{m-1}$ と書く．このとき，不変式環の関係として

$$k[x_0,\cdots,x_{m-1}]^{\mathfrak{S}_{m-1}}(=k[x_1,\cdots,x_{m-1}]^{\mathfrak{S}_{m-1}}[x_0])=k[x_0,\cdots,x_{m-1}]^{\mathfrak{S}_m}[x_0]$$

が成り立つ．この事実の証明は今は省略するが，これを用いれば，変数の数 m に関する帰納法で対称式の基本定理も証明できる．対称式に対する認識として，効率的であり，実用的でもある．[私はガロアを読むことで，この明快な機序を学んだ．ここは高校での学習範囲には入らないが，説明すれば理解可能な範囲だ．] なお，対称式の基本定理は，多項式に対するものだが，それが判れば，有理式に対する言明が従うのもやさしい (一般の傾向として，不変式に関する命題は，環に対するものの方が体に関するものより精密である).

さて，まず，ガロアに従った証明を述べる．ガロアの書き方が判りにくいと文句をつける「解説本」があるので，最小限の補いをして述べる．補題 II の性質をもつ $a,b,c,\cdots$ の有理式を

$$V=\varphi(a,b,c,d,\cdots)$$

とする．ここで，別に v という文字 (=不定元) を用意して

$$v-\varphi(a,b',c',d',\cdots)$$

で $(a,b',c',d',\cdots)$ は根 a を固定して残り $b,c,d,\cdots$ のあらゆる並べ替えをとって積を考える：

$$\begin{aligned}\Psi(v)&=\prod_{b',c',d',\cdots}\big(v-\varphi(a,b',c',d',\cdots)\big)\\&=\big(v-\varphi(a,b,c,d,\cdots)\big)\big(v-\varphi(a,c,b,d,\cdots)\big)\big(v-\varphi(a,b,d,c,\cdots)\big)\cdots.\end{aligned}$$

これは v の多項式だが，その係数は a 以外の $b,c,d,\cdots$ に関する対称式である．対称式の基本定理に関する注意で見た事実 (すぐ上) から，その係数は $a,b,c,\cdots$ の対称式と，a で書ける．ここで，$a,b,c,\cdots$ は既知量 k を係数とする方程式 $\Phi(x)=0$ の根であり，その対称式として表わされる量は既知量である．したがって，$\Psi(v)$ は k に a を付け加えた量を係数とする v の多項式になっている．それを $F(v,a)$ と書く．これは，a の方から見れば，既知量 k に文字 v をつけくわえたものを係数とする a の有理式である．[ガロアは k などとはもちろん書かない．文字 v も別に立てない．これらが最小限の補足である．]

ここで，k に $V=\varphi(a,b,c,\cdots)$ を付け加えた有理域 (=体) を考えて，それを係数とする x の有理式 $F(V,x)$ と $\Phi(x)$ の共通根を考える [ガロアは文字 x を用いず a のまま書く]. 主張は，この共通根は a のみということである．

そうでないとすると，$\Phi(x)$ は単根のみをもつから，別の根 b で，$F(V,b)=0$ を満たす. しかし，これは不可能．実際，上の議論で，$F(v,a)$ を出すところを，a の代わりに b を使って考えると，積 $\Psi(v)$ は，

$$\Psi_1(v)=\big(v-\varphi(b,a,c,d,\cdots)\big)\big(v-\varphi(b,c,a,d,\cdots)\big)\big(v-\varphi(b,a,d,c,\cdots)\big)\cdots$$

と a の代わりに b にしたものに変わる．この v の係数のうち，$a,b,c,\cdots$ の対称式は a を b に変えても同じだから，置き換えた $\Psi_1(v)$ を b の式と見たものは $F(v,b)$ になる．ここで $v=V$ と代入すると $F(V,b)$ とは，$\Psi_1(V)$ となり，各因子は，補題 II の条件より，すべて 0 ではない．従って，$F(V,b)\neq 0$.

以上より，$F(V,x)$ と $\Phi(x)$ の共通根は x について 1 次 (互除法で有理的に求まる x は a のみ) で，それを書けば，a は V と既知量 k を係数にもつ有理式で書けることになる．これが補題 III である．[$F(v,a)$ は a については，有理式だから，共通根と言う時は，有理式の分子だけとって考えるべきである．]

コメント：この補題 III はいろいろと議論を引き起こす箇所なので，注意をいくつか書く.

まず，インフェルト『ガロアの生涯』(市井三郎訳) には，決闘前夜，論文を読み返すところ (8 章 5 節) で補助定理 II に対する査読者ポアソンの書き込み「この補助定理の証明不十分なり．しかし，ラグランジュの論文第百号，ベルリン 1775 年によれば正しい」と，それに対するガロアの書き込み「これは 1830 年に発表されたある論文の証明を，原文のまま書き写したものである．ポアソン氏が記入する義務を感じた上記の覚え書きは，ここに一個の歴史的文書として残しておく」がある．ここは，ガロア論文の内容を見るなら,「補助定理 II」は「補助定理 III」の間違いだろうと，当然思う．今回，翻訳ミスや誤記の可能性などを確かめるためにインフェルトの原著を見ると (ネット上で少しの時間貸し出せる), Lemma II となっている．詳しく書けばいろいろ面白い話もあるのだが，省略せざるを得ない．ただ，これはインフェルトの理解不足ではなく，挿入の矢印の指示から，Bourgne もそう判断しているようだ (上記 Neumann の本 p.154)．ちなみにインフェルトの “Whom the Gods Love” は 1948 年の刊行で，Bourgne-Azra は 1962 年である．

ラグランジュの論文の年についても，1770 か 1771 か 1775 か，鉛筆書きは薄くて写真からは正確には読み取れない．いずれにしろ，内容から言っても補題 III であることは間違いない (Edwards も Neumann もそう思っているし，さらに補強する材料もあるらしい)．日本語訳で問題なのは,「ある論文」というところで，インフェルトの英語原文は This proof is a textual transcription of one by us in a paper in 1830．つまり，ガロア自身の論文を指しているのだが，そこが曖昧になっているので，一方でアーベルが証明**なし**に書いているということとの関係が読み取れず，とまどう．ちなみに，ガロアが書いたフランス語は Nous avons transcrit textuellement la démonstration que nous avons donnée de ce lemme un mémoire présenté en 1830.

ラグランジュの 1770/71 のベルリン論文とは，全集の 3 巻にある有名な “Réflexions sur la résolution algébrique des équations” のことだろうと思われる．解説本は，これを紹介しつつ，デデキントのベルリン講義録 (1856/57) の証明を紹介したりする．一種定番である．そして，なぜガロアがラグランジュを引用しなかったのかという謎も同時に語られる．私も長年疑問で，仮にガロアがラグランジュを知っていたとしても，証明が気に喰わなかったのだろうと単純に思っていた．もっと言えば，ラグランジュはなぜあんな証明をしているのか．それ自体は構わない．いかにもラグランジュ風ではある．しかし，自身の名のついた補間公式を使えば，一発で書けるのになぜ使わないのか，とも思っていた．解説本だってどうしてそうしないのか不思議だ [私は自分の『代数の考え方』で補間公式を用いた．ついでに，そこに対称式の基本定理の証明も書いた]．最近になって，ラグランジュの補間公式は，上記 Réflexions よりだいぶ後になって，しかも代数方程式とは全く別の文脈で発表されたらしいと知り，ちょっとだけ納得した (完全にいろいろなことが判ったわけではない)．ガロアは補題 III をアーベルの遺稿にある (証明なしに述べられた) と注しているところから，ラグランジュのことを知らなかった可能性もあるだろうと，今は考えている [原文は Cette proposition est citée sans démonstration par Abel, dans le Mémoir posthume sur les fonctions elliptique. だが，この citée とはどういうことなのか，Abel の論文を見るまで訳せない．また，さらに遺稿はどういう形で公表され，ガロアが読めたのか．派生した疑問は拡がるが，時間がない].

ここで，次の補題 IV にも関係するので，ラグランジュの補間公式を用いた補題 III の証明を書いておく．ここは現代記法で $V = \varphi(a, b, c, \cdots)$ の $(a, b, c, \cdots)$ の入れ替えを $\sigma \in \mathfrak{S}_m$

を用いて $V^\sigma = \varphi(a^\sigma, b^\sigma, c^\sigma, \cdots)$ と書くとして

$$\Xi(x) = \prod_{\sigma \in \mathfrak{S}_m} (x - V^\sigma)$$

と置くと，仮定から重根をもたない．そこで $\rho \in \mathfrak{S}_m$ に対し

$$\Lambda_\rho(x) = \sum_{\sigma \in \mathfrak{S}_m} \frac{a^{\rho\sigma}}{\Xi'(V^\sigma)} \frac{\Xi(x)}{x - V^\sigma}$$

と置く．但し，$\Xi'(x)$ は $\Xi(x)$ の微分 (導函数) を表わす．重根をもたないから $\Xi'(V^\sigma)$ はゼロにならないことに注意しておく．また，$\Lambda_\rho(x)$ は根の入れ替えで不変だから係数は既知量 k に入る．ここで　$x = V$ とすると，和は $\sigma = 1$ だけ生き残り，$\Lambda_\rho(V) = a^\rho$ となる．つまり，もとの根のどれもが V の有理式 (実際は多項式) で書けることが判る．ついでに $x = V^\tau$ とすると $\sigma = \tau$ だけが生き残り，$\Lambda_\rho(V^\tau) = a^{\rho\tau}$ となる．

このように具体的に書くことができるのだが，ガロアの方法も，やろうと思えば実行は可能である．しかし，計算をするまでもなく判る，というところにガロアの透徹した思考方法を見る．これはサント・ペラジー監獄で書いた「序文」: “Deux Mémoires d’Analyse pure par E. Galois” の Préface の一節：

Sauter à pieds joints sur les calculs; grouper les opérations, les classer suivant leurs difficultés et non suivant leurs formes; telle est, suivant moi, la mission des géomètres futurs; telle est la voie où je suis entré dans cet ouvrage.

にある**「両足を揃えて計算を跳びこえる」**という思想であり，逆に自分の証明をこの序文で説明しているということなのだろう．ちなみに，このフランス語の言い回しについては，高橋礼司先生が，この箇所に印象深く思ったということを (口頭で) 言われていた．文章では，この序文を読むためにでもフランス語を勉強すべきだと書かれていた (本稿冒頭の『数学セミナー』の記事を参照；なお，高橋先生の書評は 1988 年 1 月号 p.96).

ついでに横道だが，この序文にはロンスキー (Wronski) の名前もでてきて，このような訳のわからぬ怪しい奴と一緒くたに見られることへの忌避が表明されている．ロンスキーは元ポーランドの軍人で (『アンナ・カレーニナ』の登場人物はこの設定を借りたのか), 退役後パリで自分の哲学に従ったいろいろ (数学も) を発表していた．アルゴリズムの技法 (technie de l’algorithmie) の提唱もある．上のガロアの序文にアルゴリズムという言葉が

でてきて批判の対象となっているのも偶然でないのかもしれない．ロンスキーはラグランジュの級数展開の方法を批判し，代数方程式に関しても発表しているので，同類と見做される危険性もあったのだろう．京大数学の図書には彼の書いたものが二冊か三冊所蔵されていたので，借り出してパラパラ見たことがある．覚えているのは，数学記号にヘブライ文字を使っている箇所だけで，カントールより早い使用だと思ったことくらいだ．

なお，多くの「解説」では，この補題 III のことを「単拡大定理」と呼ぶ．数学的な内容は，たしかにそうかもしれない．しかし，ガロア論文の肝をそう名付け，代数の教科書にある他の定理と同列の目立たぬ存在に埋没させ，さらには，どのような形でも証明さえ与えればそれが理解されたかの如くに扱うのは，不当な処遇であるように感じる．というのは，次の補題 IV とともに，ガロアの考えそれ自体が，証明を通じて，定理の言明の上っ面を突き破り，背景に浮かび上がってくるからである．

補題 IV：　補題 II のように V をとり，それを根にもつ (既知量係数の) 既約方程式を考え，その根を $V, V', V'', \cdots$ とする．このとき，$a = f(V)$ として V がもとの方程式の根をあらわすなら，$f(V')$ ももとの方程式の根となる．[言うまでもないが，f は既知量係数とする．]

この主張を額面通りにとって証明するのなら，それは補題 I からすぐに出る．以下はガロアの証明ではない．まず，$a, b, c, \cdots$ の満たす方程式を $\Phi(x) = 0$ とし，$\Phi(f(x)) = 0$ という方程式を考える．仮定より $x = V$ は，その方程式を満たす．補題 I から，$\Phi(f(x))$ は V の満たす既約方程式で割り切れる．つまり，その式で $x = f(V')$ としたものは $\Phi(x) = 0$ になって，これはつまり，もとの方程式の根だということ．

証明だけなら，これはこれでスッキリしているが，ガロアは別の行き方をする．少し上，ラグランジュの補間公式のところで使った $\Xi(x)$ を $x - \varphi(a, b, c, \cdots)$ で $(a, b, c, \cdots)$ の全ての並べ替えについての積を取ったものとする．係数はすべて既知量である．このうち $x - \varphi(a, b, c, \cdots)$ を含む既約因子を考えれば，その根 V' が $V = \varphi(a, b, c, \cdots)$ の共軛根 (この言葉をガロアは使っていないが，便利なので使う；V を根にもつ既約多項式の根を指す) なわけだが，それは，$\varphi(a, b, c, \cdots)$ で $(a, b, c, \cdots)$ を並べ替えた形で得られる．それを $V' = \varphi(a', b', c' \cdots)$ とすると，補題 III の証明で $F(V, a)$ の作り方を思い出せば，$F(V', a') = 0$ となる．補題 III の結論を言い換えて，$F(V, a) = 0$ と $\Phi(a)$ の共通根を書いて $a = f(V)$ となるのだから，$F(V', a') = 0$ と $\Phi(a') = 0$ とから $a' = f(V')$ となる．

これが論文の証明である．ガロアは，もっと何か言いたかったのだろう．例えば，重要に思える次の一文は，線で消されている：Ces principes posés, nous allons passer à l'exposition de notre théorie hors la première. この前には Car V' doit s'obtenir par l'échange des lettres dans la fonction V. つまり，V をその共軛に変えるのは $V = \varphi(a, b, c, \cdots)$ で，根 $a, b, c, \cdots$ の並べ替えに移ることで得られる，のはもちろんのこと，未知量の背後にこの根の並べ替えという単純な原理を，より一般的に見出していて，補題 IV はその適用例だと言いたいかのようにも思える．どこかに書いておくべきことがらだったはずだ．Neumann の注記 (p.155) によると，この削除については Bourgne-Azra には記録されていないらしい．ともかく，ここは書き換えるならたくさんのことがあったのだろうと推測される．

手稿の写真を見ると，今見ている補題 IV の証明は，言明のすぐ後から書かれていず，欄外から始まっている (補足のように見える)．証明は，元々もっとそっけなく書いているようだ．つまり，証明は，上に書いた Car V' doit s'obtenir... からが当初の出だしのようで，その移行はガロアにとっては，当然の「原理」だったのを,「原理」は消して，より丁寧に証明を書き始めたみたいだ [書き換えに伴って，Car は消された形で公表された]．この節のタイトルが Principes なのも，実はそのあたりが意図だったのかもしれない．

それとは関係がないかもしれないが，一つ補足的事項をここにメモしておく (補題 IV をそのように書いたとて，役に立つ訳ではないものの，一応注意しておく)：たとえば，$U = \varphi(a', b', c', \cdots)$ を必ずしも V の共軛とは限らないが，根の入れ替えで得られるものだとする．このとき $a = f(V)$ のとき，$a' = f(U)$ である．これは，ガロアの証明なら，補題 IV の証明で既約因子ということは効いてきていないから判る．また，U が V を含む既約因子に属さなくても，V と同じ性質をもつから，補題 IV からも言えないことはない．別の視点からは，上で述べた，ラグランジュの補間公式経由の証明でも判る．

注意： 補題 IV の述べるところを少し敷衍する．上でラグランジュの補間公式がらみで述べた形で言い尽くしてはいるが，述べ方と記号を変えてみる．補題 III で証明された V で根を表わす有理式で，表わす根を明示的に書くとして，根の書き方を $a, b, c, \cdots$ ではなくて現代風に $a_0, a_1, \cdots, a_{m-1}$ のように書く時

$$a_i = f_i(V) = f_i(\varphi(a_0, a_1, \cdots, a_{m-1}))$$

とする．このとき $V^\sigma = \varphi(a_{\sigma(0)}, a_{\sigma(1)}, \cdots, a_{\sigma(m-1)})$ となっているなら

$$f_i(V^\sigma) = a_{\sigma(i)}$$

である．つまり，V の共軛根 $V^{(l)}$ を f_i に代入したときの値は $V^{(l)}$ の中で，パラメータとして入っている根の順列で，i 番目の根を拾うことで得られる，ということだ．つまり，重要なのは，パラメータの中の根の並びであって，計算はそれで支配されているということなのだ．おそらく，この事実が，次の定理での順列に関する函数の記号 (素直に見ると若干の混乱か誤用に感じる) の由来なのではないかと，私は思う．

これから連想されることは多い．現代の目から見ても示唆的である．が，書き出すと，とめどなくなるので，深入りはしないことにする．

• 第 I 節 (Proposition I)：

いよいよ主要定理が述べられる．補題 IV で仄めかされた「根の並び」=「根の順列」が定理の形で，その本質を顕わす．

定理： 方程式とその根 $a, b, c, \cdots$ は今までどおりの設定だとする．このとき，次の条件を満たす**文字** (lettres) $a, b, c, \cdots$ の「並びの集まり」が存在する [原文は Il y aura toujours un groupe de permutations des lettres $a, b, c, \cdots$ qui jouira la propriété suivante. 「順列の群」と訳すものをここでは丁寧に述べた].

1° 根の有理式で，この「群」の並びに従って根を代入 (subtitutions) して不変 (値を変えない) なら，それは既知量である．

2° 逆に，根の有理式で表わされる量が既知量であるなら，この「群」の並びに従う根の代入で値を変えない．

定理についてのコメントはあとにして，証明を書く [最小限の補足は付け加える].

まず，定理に述べられた「根の順列」は以下のように作られる．準備した補題を前提として，記号 V などはそのまま使う．

(i) 補題 III によって存在が保証された，根 $a, b, c, \cdots$ を V によって表わす有理式を $\varphi, \varphi_1, \cdots, \varphi_{m-1}$ とする [さきに注意したが，記号 φ はもともと V を $a, b, c, \cdots$ で表わすものだったから適切な使用とは言えないが，変数の数が違うので区別は一応つく．とは言うものの，単なる混乱ではなく，或る種の同一性を指し示す記号として意図的に使われた

“記号の濫用”なのかもしれない].

(ii)　一方，V の共軛 (n 箇あるとして) を $V, V', \cdots, V^{(n-1)}$ とする．V で根を表示する $\varphi, \varphi_1, \cdots, \varphi_{m-1}$ に共軛根 $V^{(l)}$ を代入しても，やはりもとの方程式の根である (補題 IV). 従って，その代入によって $a, b, c, \cdots$ の並び替え (**根**の順列)

$$\varphi V^{(l)}, \quad \varphi_1 V^{(l)}, \quad \cdots, \quad \varphi_{m-1} V^{(l)}$$

ができる．それを簡単に $(V^{(l)})$ と書く [この記号は下の表を書いた後で，表の欄外に付け足した]．ガロアは，この n 箇の順列の集まり (「順列の群」groupe de permutations) を

(V)	φV	$\varphi_1 V$	$\varphi_2 V$	$\cdots$	$\varphi_{m-1} V$
(V')	$\varphi V'$	$\varphi_1 V'$	$\varphi_2 V'$	$\cdots$	$\varphi_{m-1} V'$
(V'')	$\varphi V''$	$\varphi_1 V''$	$\varphi_2 V''$	$\cdots$	$\varphi_{m-1} V''$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(V^{(n-1)})$	$\varphi V^{(n-1)}$	$\varphi_1 V^{(n-1)}$	$\varphi_2 V^{(n-1)}$	$\cdots$	$\varphi_{m-1} V^{(n-1)}$

と表に書くが，これが定理の主張の「順列の群」である．これをもとに定理の証明を続ける：

1°　根 $a, b, c, \cdots$ は補題 III から V の有理式で書けるから，$a, b, c, \cdots$ の (既知量係数の) 有理式 F は，V の有理式 ψ を以って $F = \psi V$ と書ける．従って，F で，根の並びを上の「順列」に従って入れ替えるとは V をその共軛にすることとなるから，その入れ替えで値が変わらないというのは

$$\psi V = \psi V' = \psi V'' = \cdots = \psi V^{(n-1)}$$

ということである．ガロアはここで，もう結論だと言ってしまう．V の共軛根の対称式だから，有理的になるという意味だろう．それはそれで構わないが，蛇足ながら，念の為，老婆 (爺) 心で [解説の中には筋の悪い議論を付け足すものがあったので] 補足しておく．有理式 ψ を (既知量係数) 多項式 α, β の商で $\psi = \beta/\alpha$ と書いたとする．ここで，今まで記号を出さなかったが，V の満たす既知量係数の (n 次) 多項式を ϕ とし，この α, β を ϕ で割り算して，余りを α_0, β_0 とすると，$\alpha V^{(l)} = \alpha_0 V^{(l)}$, $\beta V^{(l)} = \beta_0 V^{(l)}$ である．従って，ψ は β_0/α_0 で置き換えてもよい．ここで $\gamma = \beta_0 - F \cdot \alpha_0$ という多項式を考える．割り算の余りだから，この次数は高々 $n-1$ である．但し $F = \psi V$ は式ではなく (仮定によって共通の) 値を表している．このとき，上の仮定は

$$\gamma V = \gamma V' = \gamma V'' = \cdots = \gamma V^{(n-1)} = 0$$

で，高々 $n-1$ 次の γ が異なる n 箇の零点をもつことを意味し，$\gamma=0$ となる．よって，$F=\beta_0/\alpha_0$ だが，右辺の係数はすべて既知量だから F も既知量となる．この補足=蛇足部分は，(本稿では証明しなかった) 対称式の基本定理のツメの部分に対応する議論である．

2° 逆に F が根 $a,b,c,\cdots$ の既知量係数の有理式で書けて，かつその値が既知量になっているとする．このとき，上のとおり $F=\psi V$ の形になる．もちろん ψ は既知量係数の有理式．上の 1° の証明と同じ記号を使うとして，$\psi=\beta/\alpha$ と (既知量係数) 多項式の商とするとき，$\psi-F=(\beta-F\cdot\alpha)/\alpha$ で，分子の $\beta-F\cdot\alpha$ は既知量係数の多項式である．これに V を代入すると 0 である．補題 I により，それは V の満たす既約多項式で割り切れて，従って，他の共軛根 $V^{(l)}$ を代入しても 0．つまり，$\psi V^{(l)}=F$ と不変性が出る．

• ガロア自身の補足とコメント： 以上，定理の証明は，私の蛇足を除けば，とても短く明快である．以下，定理を補足しようとするガロアの注意などについて少し見る．定理自体には，何の疑義もないと思われるのに，ガロアが説明を加えるのは，その応用としての次節の定理に関係するのが一つ．さらに，定理に述べられた「順列の群」としての「方程式の群」についての本質を見ようとしているという点が，もう一つの理由だろう．

まず，原論文にある (注)．それは，定理自体の主張の「不変」invariable という語につけられている．これは，式の形が変わらないというのでなく，値が変わらないというものを考えているという注意である [その主張のあとの「たとえば」以下の補足解説のおかしい本があるが，見てすぐ判るだろうし，正す価値はあまりないので省略する]．式 (多項式，有理式) と，その変数に「数」を代入した数値的な観点の峻別がされているのだが，これを簡単な言葉で十全に言い切るのは難しい．ガロアの論文では，多変数の (根の) 函数で，根の (或る種の) 入れ替え操作が問題となっている点が重要である．

定理の後に二つの注釈 (Scolie) がある．これは次の節 (Proposition II) の定理の理解の助けのためという側面もあるだろうが，それを読み取るのは難しい．Scolie I, II を原文で挙げ，やや説明的な私訳を書く [原稿には番号はついていないが，印刷公表されたものには，便宜上 I, II とつけている：I は本文に続いているので，本来はそれだけが Scolie のつもりだったのだろう；II は欄外にある]．イタリックにした substitutions (Scolie I) は手稿で下線が引かれている．

Scolie I. Il est évident que dans le groupe de permutations dont il s'agit ici, la

disposition des lettres n'est point à considérer, mais seulement les *substitions* de lettres par les quelles on passe d'une permutation à l'autre.

ここで扱う順列の群では，その文字の並べ方は本質的でなく，文字間の**入れ替え方**のみが問題なのは明らかなことだ.

Ainsi l'on peut se donner arbitrairement une première permutation, pourvu que les autres permutations s'en d'éduisent toujours par les mêmes substitutions de lettres. Le nouveau groupe ainsi formé jouira évidemment des mêmes propriétés que le premier, puisque, dans le théorème précédent, il ne s'agit que des substitutions (de lettres) que l'on peut faire dans les fonctions.

従って，最初に与える順列は任意に採って構わない．同じ仕方で文字を並べ替えをしさえすればよいのだから．そのように置き換えられた順列も，上述の定理では全く同じ役割を果たす．というのも，有理式での (文字の) 入れ替えのみを問題にしているのだから [de lettres はシュヴァリエが書き写し損なったらしい].

Scolie II. Les substitutions sont indépendantes même du nombre des racines.

「入れ替え」に注目するなら，最初の根の箇数にさえ依存しない.

Scolie II は欄外にあるが，その直前に，線で消したような二つの文があって，しかも，消し方自体はそれほど (他の消し方に比べて) 強くない．重要と思われるので，それを書く：

Ce qui characterise un groupe. On peut partir d'une des permutations quelconques du groupe.

「(方程式の) 群」の本質 (特徴).「群」の順列のどこからでも出発できる.

あと，上で紹介を省いたので，Principes の補題 I の前の「置換」に関わる "問題の数行" を，ここに書いてみる (Neumann のものでは，Princepes でなく，定理の言明のあとに置いている．但し，ガロアは定義のあとに置く (移動する) よう指示をしているとある．いずれにしろ，後から書き加えたことに間違いはない)：

Les substitutions sont le passage d'une permutation à l'autre.

「置換」(置き換え) とはひとつの順列からもうひとつの順列への移行 (passage) である．

La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions; car il n'y a aucune raison pour que, dans une fonction de plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.

有理式を扱うとき，変数の「置き換え」を指定する際に，最初の文字 (=変数) の「並べ方」は全く任意である．というのも，複数変数の有理式でひとつの文字がどこか特別の位置に置かれなくてはならないという理由は全くないから．[文末の un autre は名詞 (冠詞) の性からして rang を指し (lettre でも permutation でもない)，rang が「位置」を意味するのは，ガロアの他のメモ書きからかなり確かだ.]

Cependant, comme on ne peut guère se former l'idée d'une substitution sans se former celle d'une permutation, nous ferons, dans le langage, un emploi fréquent des permutations, et nous ne considérons les substitutions que comme le passage d'une permuation a une autre.

そうではあるが，文字の並び (=「順列」) を設定することなしに,「置換」の意味を理解することなど殆ど不可能だから，説明として「順列」の語をしばしば使うことになる．そして,「置換」はもっぱら順列から順列への移行の場合にのみ考える．

Quand nous voudrons grouper des substitutions, nous les ferons toutes provenir d'une même permutation.

「置換」のいくつかをまとめて考えたいときには，最初にとる順列は同じものとする．

Comme il s'agit toujours de questions où la disposition primitive des lettres n'influe en rien dans les groupes que nous considérons, on devra avoir les mêmes substitutions, quelle que soit la permutation d'où l'on sera parti. Donc, si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST.

我々の考える「群」に於いて，最初の文字の配列が影響を与えない問題のみ扱うので，出発する順列がどうであれ,「置換」としては同じとしてよい．従って，ひとつの「群」に置換 S と T があるなら，ST も確かにその群の置換である．

• **数学的な解説** 1： 上に挙げた，最初の主定理に関わって，ガロアが補足したいと考えたらしいいくつかの説明には，共通の言葉遣いが見られる．だから，まとめて書いてみたのだが，現代的な数学の視点から，もう少しつけ加え，総合的に理解する視点をもちたい．

言葉をバラバラに日本語に置き換えても意味が通じないだろうから.

ともかく，上に述べたように「順列」と「置換」について懇切丁寧に説明しようとしているガロアが，それらを混同すると考えるのは不自然であり，私の採るところではない.

さて，上に引いたガロアの言葉について，どこがポイントか．それらは，実際に書かれた時系列としては，定理が述べられた後のことになる．ところが，substitution の語の使用が，順列から順列への移行に**限る**と言う文言は，印刷公表された時に，Principes という，定理より前に配置される節に置かれる形になっている (ガロアの指示らしいが)．するとその適用について，字面上は微妙に齟齬が生じているようにも見える．定理の substitution は，実際は代入操作の側面が強いからである．もちろん，元の根の並びの代わりに V の共軛から作った根の順列に入れ替えて代入するのだから，それも順列の入れ替えと，言えば言える (が，自然かと言えば疑問だ).

一方，順列が仮の姿で置換が本質であるという認識は，定理を述べた時点から得られていたものではあっただろう．それは Scolie I にも現われている．そうではあっても「順列」自体は充分有効な役割を果たしており，論文自体を全面的・根本的に書き変える必要はない．但し，決闘前夜の読み直しで，論文に付け加える新たな構想にも言及し，記録しておきたい；コメントは簡潔に言うしかないので，似たような文言が繰り返される；時間があれば,「順列」でなく「置換」を主体にして書き直したかった；というのも，多分確かだろう.

そのあたりの揺らぎの中に，我々は群概念の成立過程を見ることができる．しかし，それを理由に「置換群」の概念に喜んで飛びつき，解釈を改変するのは間違いだ．最初の原稿で，混乱があったわけではないのだから.

以下，現代的な概念を交えて，上記のコメントについて，検討を述べる．問題は何かというと，有理域 (=体) のように演算を有している世界に於いて，値を入れ替えることをどう捉えるかということである.

文字式 (多項式，有理式) であれば，それは自由であるし，係数と根のそれぞれの有理式 (つまり既知量と未知量) を判別するのは，根の (あらゆる) 入れ替えで不変という性質であって，それが「対称式の基本定理」として知られていた．独立な文字は，入れ替えるのに，関係式のことを考慮しなくてよいから，気が楽だ．しかし，ガロアが扱っているのは，文字の世界ではなくて，数値的な方程式という，より一般で具体的なものが主要な対象である．その違いを強調したのが，前節の最初に引いた，定理の言明に対する注である．また，その両極端の二つの典型としてガロアは「一般方程式」(ガロアの用語では代数方程式

équations algebriques) と「円分方程式」を挙げて定理の補いとしている．

では，数値的な場合に「置換」(入れ替え) はどうするか．ガロアの論文でも，実は最初からそのようなことをやっているのが，補題 II の言明である．この場合は，fonction de racines という言い方で，根のあらゆる並べ替えで同じ値をとらない [une fonction V de racines, telle qu'aucue des valeurs que l'on obtient en permutant dans cette foncition les racines de toutes menières, ne soient égales à une autre] という表現である．これは，常識的に考えてもなんら疑問を抱かない箇所である．ここと，補題 III の証明中では，根の「並べ替え」の動詞は permute である (分詞の形 permutant で使われる)．

この場合でも，入れ替えるのは「根」(=数という範疇に入る) であって，文字=不定元ではないから，極めて厳格な言い方をするなら，(イ) 根 $a, b, c, \cdots$ に応じて文字 $x_a, x_b, x_c, \cdots$ を用意して，考える式の $a, b, c, \cdots$ をそれで置き換えたものを作り，その文字を入れ替えて新たな有理式を作り，そののちに $x_a = a$, $x_b = b$, $x_c = c, \cdots$ と代入する．このような操作を経てこそ入れ替えができるのではないか．実際，文字に数は代入はできるが，数に数は代入できないのだ．我々は，このような形で (無意識のうちに) 入れ替えの意味を与えているのではないだろうか．

いや，それは一つの解決の手段であるが，唯一のものではない．そのような反論もありうる．実際，補題 II, III では，(ロ) $V = \varphi(a, b, c, \cdots)$ と函数記号を持ち出している．そうすると，函数記号の中身の「位置」ならば入れ替えて，代入することはできる．代入すべき「器」がはっきりしていて，これなら入れ替えの意味は明瞭である．

但し，これは，$V = \varphi(a, b, c, \cdots)$ という**表式**によって表されている量 (数) に限っての話で，表示に依存している．その点は，文字 (独立な文字) の置換と数値の場合で大きく違う．

集合と写像という概念を有する現代ならば，幾分なりとも直接的にその操作を記述することが可能ではあろう．それでも我々は，代入だとか，置換だとか，或いは順列だとかの，諸事項と用語について，その意図を正しく理解するには，ガロアが感じたと同じように切実に，これらの言葉に内包する意味と問題を意識する必要がある．そのときに，上で言ったような (イ) とか (ロ) とかの手段を思い浮かべながら，コメントを読んではじめて何を言っているのかという真意に到達できる．

例えば，上で書いた (再録)

La permutation d'où l'on part pour indiquer les substitutions est toute arbitraire, quand il s'agit de fonctions; car il n'y a aucune raison pour que, dans une fonction de

plusieurs lettres, une lettre occupe un rang plutôt qu'un autre.

[有理式を扱うとき，変数の「置き換え」を指定する際に，最初の文字 (=変数) の「並べ方」は全く任意である．というのも，複数変数の有理式でひとつの文字がどこか特別の位置に置かれなくてはならないという理由は全くないから．]

は極めて意味が取りにくい．それに輪をかけて，既存の訳文 (私が見たのは二つ) では名詞の性という基本的なことにすら気をかけず (無視かもしれないが)，日本語にしたときになんとか意味が通じるようにしているが，不適切に思う．ただ，上のように訳したとしても，そのままで日本語からその意味を理解するのも難しい．しかし，先に述べたような (イ)(ロ) のような側面を思い浮かべると，内容に少しは迫れる．

まず，有理式 (変数は独立としても) を取ったとして，その表式に変数の順序はどこにも入り込まない：$x+y^2z$ と書こうが zy^2+x としようが同じもので，変数の入れ替えをするためには，変数の指定を，今なら $x \mapsto y$ 等々とか書くことになるが，ガロアの当時には，別の書き方をしないといけなかっただろう．しかし，函数記号を使って $f(x,y,z) = x+y^2z$ と書くなら，置き換えは $f(y,x,z)$ などと簡潔に書ける．ここで，f の中の変数の並びには，何の優先順位もない．今はアルファベットで書いているから，何か順序を思い浮かべるかもしれないし，文字に添字を数でつける場合でも同様だが，それは恣意的な順序である．上の一文はそのようなことを述べているのではないだろうか．函数記号には，それを書き入れる「位置」という特別な装置が，実は組み込まれている．つまり，この函数記号が (有理) 式を表わす際には，注目する箇所を，函数記号の中での「位置」で指示できることを特に指摘したい．我々は函数記号に慣れすぎているから，そのご利益と特殊性には気づかないが，ここで取り出して引用しているガロアの言明に対しては，重要なところである．

ついでに，今は文字は独立なものとしたが，数をそこに代入して $1+2^2\cdot 1$ のように書かれてしまっては，(イ) のようにすら書き換えられない．この式の中で，数 1 と 2 を入れ替えるなどと言っても何をしていいのか判らない．もちろん，大学初年度でならう (行列式のところでそのような訓練をする意味は少ないと思うが) 置換計算なら，出てくる「数」は本来の数ではなく「数字」と呼ばれるのが適切な「文字」である．住所の中の 1 丁目 2 番地と同じ役割だ．そのように使われる場所が限定されるなら，数でも入れ替えができる訳だが，ガロアが扱うのはそういうものではない．ガロアを理解するために，置換計算などを前提するのも，当然のように不適切である．[アーベルの論文の置換は，独立変数を扱っているのだと思うが，私は，充分読んでいないので，断定的なことが言えない．]

• **数学的な解説 2：** 上で述べたのは，順列と置換の関係の部分であるが，ガロアのコメントの，より重要で，おそらく最重要な部分と言えば，最後の「置換 S と T が「群=方程式の群」の中にあれば，ST もその「群」の中にあるというところだ．つまり，方程式の群である，V の共軛根からきまるもとの方程式の根の順列について，その順列の入れ替えである「群」の置換について，合成で閉じているという主張である．ここに，群概念の誕生のさまが描写されているのだ．

第一近似としてのアナロジーで，ここを説明するのに，アフィン空間とベクトル空間の違いを用いる．このアナロジーでは,「順列」は「アフィン空間の点」であり,「置換」は「ベクトル空間の元=ベクトル」になぞらえられる．アフィン空間の点の差を (束縛) ベクトルと捉えるなら，それが順列から順列へ移すものとしての置換に対応する (ガロアの最初の定義)．ここで，ベクトルとベクトルの和を考えるとき，束縛ベクトルでは，足すベクトルの始点と足されるベクトルの終点を一致させる状況でないと意味がわからず (ヤジルシをつなぐことによる位差の合成ができない)，一般には，束縛ベクトルを平行移動で移るものを同じと見做して，始点と終点を一致させる．これに当たることは「置換」で考えるなら，出発する順列をとりかえても置換として同じになるという実質を考えるということになる．ガロアが「方程式の群」で出発する順列の変更について言及するのは，それ故であり，それが可能なのは，V の代わりに V の共軛根を考えても構わないというところに根拠をもつ．

注意すべきなのは，アフィン空間とベクトル空間は，原点をひとつ決めると，すぐさま同一視されることで，それ故，順列と置換は，基準となる順列をひとつ**決める**と，容易に同一視されてしまう．しかし，ガロアは，そういうことはあからさまに述べていない [後世の解説では，そういう同一視をしたがるが，それは間違った解釈である]．

この第一近似を現代の群論の言葉で述べると,「順列の群」とは群の主等質空間 (このごろはトルソーという用語があるらしい) である．上のベクトル空間とアフィン空間の場合なら，群は可換なので，左右の区別はない．しかし，今考えている方程式に関わる場合には非可換群がでてくる．この段階では,「置換」を「順列」の比で書くとき，右から割るか，左から割るか，は全く選ぶ基準がない．どちらを取るかは記法の選択だけのことだ．だから第一近似と言っている．しかしながら，左右の区別がガロアに於いてはっきりする場面がでてくる．シュヴァリエへの遺書の最初に言及される「部分群」への分解に二様あるという説明である．ガロア論文の第 I 節の定理では，従って，そこまでの「置換」概念の必要性はない．第 II 節の定理とは，既知量を増やしたときに「方程式の群」がどのように縮

小するかという記述が主な内容だが，そこで,「群」と「部分群」の関係として置換の概念が表立ってくる．そこは例を出して述べるのがよりわかりやすいと思うので，あとに廻す．

• 数学的な解説 3： すぐ上では，順列と置換を，アフィン空間とベクトル空間のそれぞれの元に例えた．アフィン空間の点は，原点をどこかに設定してベクトルと見做さないかぎり，点と点を足すことはできない．方程式の群においても，順列と順列を「合成」することは，そのままではできない．しかし，本当にそうなのか．定理の証明を読むと，順列と順列が合成できそうな気がする．そこを検討しておく．

定理の証明では，根 $a, b, c, \cdots$ の有理式 $F(a, b, c, \cdots)$ があった時，V によってこれらの根を表わす有理式 $\varphi, \varphi_1, \varphi_2, \cdots, \varphi_{m-1}$ を以って，

$$\psi(x) = F(\varphi(x), \varphi_1(x), \cdots, \varphi_{m-1}(x))$$

という 1 変数の有理式 $\psi(x)$ を作り，ここに V の共軛根 $V^{(l)}$ を代入することで，(方程式の群に伴った) 根の入れ替えを合理的に実現する．結果としてそうなので，単純な「置換」かと思うかもしれないが，そうではない．注意すべき重要な点は,「代入操作」は四則演算を「保つ」ので，表式の不定性の問題が生じないというところである．現代用語では「環 (自己) 準同型」ということだが，デデキントがのちにガロア群を体の自己同型として定義したのは，この本質を抽象し得たからである．また，代入操作の場合は，合成演算は一般に非可換になっている点にも注意を向けたい．

ここで，ガロアは表立って書いてはいないが，F として特に $V = \varphi(a, b, c, \cdots)$ や，その共軛をとると，上のようにして作った ψ に V の共軛を代入することで，順列と順列の合成が可能となる．このように，のちにデデキントが，より実体的に体の同型として定義する「写像」としての群が，ガロアにも潜在的にあり，背後には，根の入れ替えという置換群的な表象 (symbol) があると捉えられる．しかし，それでは，アフィン空間の点と点は足せないと言ったことと矛盾する．どこに「原点」が隠れているのか．

じっくり考えるまでもなく，この場合に原点となるのは，最初にとった V であり，従って，必然的に V が単位元の役割を果たす．それは，V を他の共軛根で置き換えた状況を想定すると “原点”($\sim$ 単位元) が変更されることからも判る．

答えは判っているが，これをもう少し，現代数学の言語で説明しておこう．多変数 (m 変数) の有理式があったとき，そこに $\varphi, \varphi_1, \varphi_2, \cdots, \varphi_{m-1}$ を代入することを考えるわけだが，

出発点を V から，その共軛に変える時には，新たにこれら $\varphi, \varphi_1, \varphi_2, \cdots, \varphi_{m-1}$ たちの対応物を作る必要はなく，これらの順番を入れ替えるだけでよい．そのことが補題 IV の証明から読み取れるのであり，上に (補題 IV のあと) 書いたようなガロアの意図した「原理」の適用例なのだ．さらには，その順番の入れ替え方は，$V = \varphi(a, b, c, \cdots)$ が共軛にうつるときの φ の中の根の並びかたの入れ替えと同じになっている．その注意を独立して上で説明したが，現代用語で述べるために，根を $a, b, c, \cdots$ でなく，$a_0, a_1, \cdots, a_{m-1}$ と書き，$\sigma \in \mathfrak{S}_m$ を番号の入れ替えとして，

$$V^\sigma = \varphi(a_{0^\sigma}, a_{1^\sigma}, \cdots, a_{(m-1)^\sigma})$$

と右作用の形に書き，$a_i = \varphi_i V$ とするなら，まず $a_{i^\sigma} = \varphi_i V^\sigma$ であり，さらに．

$$a_{i^{\sigma\tau}} = \varphi_{i^\sigma} V^\tau$$

となっている．根の順列 (V^σ) とは $(\varphi_i V^\sigma)_{0 \le i \le m-1}$ のことだから，この φ_i の並びを σ で入れ替えたものを

$$(\varphi)_\sigma = (\varphi_{i^\sigma})_{0 \le i \le m-1}$$

と書くと，$(V^\sigma) = (\varphi) V^\sigma$ であり (ここで単位元は空 empty の記号で表わすことにする)，さらに，より一般に

$$(V^{\sigma\tau}) = (\varphi)_\sigma V^\tau$$

となる．つまり，二つの順列 $(V^{\sigma\tau})$ と (V^τ) の比 (ここの記号では右からの商) が代入する箇所を指定する φ_i の入れ替え (置換) として実現される．ここのところは，結果として，置換だけを取り出した形に集約されるが，話は (現代用語として) 「体の自己同型」を扱っているのだから，単なる「置換計算」という，数の世界 (有理域) から遊離したもの，ではない．明確に思想的区別がなされるべきものである．

話がくどくなっているが，現代的視点からもう一言付け加える．そもそも，順列とは，{ 位置 } から { 記号・文字 } への写像 (今の場合は双射) のことである．この写像 (=順列) の全体には,「位置の入れ替え」と「文字の入れ替え」の二種類の置換が考えられる．どのような (作用と合成の) 記号規約を使うかによって右と左は変わるが，上のような場合だと，位置の入れ替えが，二つの順列の右割り算として表された．そのとき，文字の入れ替えは左割り算となる．そして，単に二つの順列を入れ替えるだけなら，どちらを用いても同じ結果が得られる．この，右と左の区別がガロアに於いて，表立ってでてくるのは，シュ

ヴァリエへの手紙の中だが，その意味は今言った二種類の入れ替えに際し，既知量の拡大によって「方程式の群」が縮小するときに，左右の違いが顕著になるというのである．ここは，後で例を以って，説明する．

• 第 II 節 (Proposition II)：

ここで，既知量の拡大 (あらたな量を添加する) によって「方程式の群」が縮小するという様子を記述する．しかしまた，加筆訂正のなされた跡がさらにひどく，ガロアの意図を正確に読み取るのが難しい．いろいろな箇所を，表面的になぞると混乱する可能性が高くなる．ここでは，“意訳”を述べる．というのは，書き直し等の改訂と，それに伴って「正確な」定理の言明が何なのか等が揺れ動くからである．最初の定理とその周辺のような，原文の微妙な言い回しを検討する箇所ではなくなっている．シュヴァリエによる注などもあるし，テキスト自体が複数あるような状態である．

重要な注意をしておくと，論文中で，Principes を除くと，“順列の置換”という言葉が現れるのは，この定理 (の 2°) が最初である．つまり，書き加えられていないバージョンでは，これ以前に「順列の置換」はない．

定理 (大意)： 既知量に補助の既約方程式の根 r をつけくわえる．1° このとき，次のどちらかが起こる：「方程式の群」は全く変わらない；或いは，補助の方程式のそれぞれの一根を付け加えた既知量で考えた「順列の群」たちに分解する．

2° 補助の方程式の根を付け加えて (縮小した)「順列の群」二つをとると，同じ一つの置換 (une même substitution)[文字の置き換えは (部分)「群」に属する順列に共通の仕方で行う] で移りあう，という顕著 (remarquable) な性質をもつ．

ガロアの証明を文字どおりなぞると，まず，V の方程式が，同じ次数の因子に

$$f(V,r)\times f(V,r')\times f(V,r'')\times\cdots$$

と分解されるという [ここはガロアのとおり V と書いたが，我々の書き方では，文字を変えて v とすべきところである]．但し，$r,r',r'',\cdots$ は r の「他の値」(d'autre valeurs de r) とある．このあたりは，単純に読むと混乱する (解釈を誤ると正しくない式になる)．数行が消された跡もある．実際，タヌリの発表したガロアの草稿などのメモ (本稿の最初の方にネット上の引用をした) には，リウヴィルが書いたものも残されていて，そこでは苦労して

この式を導いているが，ちょっと見当はずれのように思える．一，二ヶ月そのことばかりを考えたリウヴィルですらそうなのだ．文字面に囚われるのは多分正しい読み方ではない．

ここで，この特別な場合と見做される，後の節 (Proposition IV) の定理の状況を参考にする．そこでは r が，根 $a, b, c, \cdots$ の有理式になっている場合が書かれていて，そのとき，第 I 節の主定理の直接の適用として，その根 r が動かない順列こそが，r の添加で (縮小する)「方程式の群」だということになる．おそらくは，そのように，r とその “共軛”である $r, r', r'', \cdots$ をイメージしている (ガロアが書いていないことを勝手に想像して断定するのは憚られるが) のだろう．つまり，最初の $a, b, c, \cdots$ に加えて r を含む未知量の総体を想定して，その中で最初の主定理を適用するということなのではないだろうか．話の流れとしては，それが自然だ．そうすると Scolie II で置換の「実体」は根の数にすらよらない，と注している内容や，ガロアが $a, b, c, \cdots$ の方程式を書かないという理由の説明が見える気がする (憶測だが).

以下，今までと同じ程度に書き綴る紙幅もないので，一つの例を使って,「方程式の群」の縮小と,「部分群」の分解の二通りの由来を説明する．

• **一つの例**　$x^3 - 2 = 0$

(0)　この 3 根は $a = \sqrt[3]{2}$, $b = \sqrt[3]{2}\,\omega$, $c = \sqrt[3]{2}\,\omega^2$ である．但し，ω は 1 の原始 3 乗根．ガロアの処方に従い V を作る：最も簡単に，$\varphi(a, b, c) = b - c$ とすると $V = \sqrt[3]{2}\,(\omega - \omega^2)$ であり，6 通りの根の入れ替えで値はすべて異なる (但し，一次独立ではない；関係して，正規底 [数学的にも数学史的にも興味深い] に触れたくなるが，今は措く)．ついでに $V^2 = -3\sqrt[3]{4}$ であり，従って $V^6 + 108 = 0$ である (これが V の満たす (有理数体上の) 既約方程式).

補題 III の処方どおり $F(v, a) = \big(v - \varphi(a, b, c)\big)\big(v - \varphi(a, c, b)\big)$ を作ると，

$$F(v, a) = v^2 + 3a^2$$

であり，$F(v, a) = 0$ と $a^3 - 2 = 0$ の共通根を求めると $av^2 + 6 = 0$ となる，つまり，a を V で表わす (有理) 式は $a = -6/V^2$．[この例から判るように，φ を素直な 1 次式に取っても，a を V で表わす式は有理式で出てくる．もちろん，多項式に書き直せるが．]

さらに

$$F(v, b) = \big(v - \varphi(b, a, c)\big)\big(v - \varphi(b, c, a)\big) = v^2 + 3b^2 \ (= v^2 + 3a^2\omega^2)$$
$$F(v, c) = \big(v - \varphi(c, a, b)\big)\big(v - \varphi(c, b, a)\big) = v^2 + 3c^2 \ (= v^2 + 3a^2\omega)$$

である．これらを用いて V の満たす方程式を求めるため，積を計算すると

$$F(v,a)F(v,b)F(v,c) = (v^2+3a^2)(v^2+3b^2)(v^2+3c^2) = v^6 + 2^2 3^3$$

となる．

これは $v-\varphi(a',b',c')$ で (a',b',c') をすべての (6 通りの) 入れ替えの積で，補題 IV の証明中に現われるもの．一般には V の満たす既約方程式は，その因子だが，ここではそれ自体になっている．従って，ガロア分解式は，この 6 次式である．

ついでに V で b を表わすために $F_1(v,b) = \big(v-\varphi(a,b,c)\big)\big(v-\varphi(c,b,a)\big)$ を作ると，

$$F_1(v,b) = \big(v-(b-c)\big)\big(v-(b-a)\big) = v^2 - 3bv + 3b^2$$

で，$b^3-2=0$ とから $b=(V^3+6)/2V^2$ となる．同様に $F_2(v,c) = v^2+3cv+3c^2$ で，$c=(-V^3+6)/2V^2$ となる．このようにして，

$$\varphi v = -\frac{6}{v^2}, \qquad \varphi_1 v = \frac{v^3+6}{2v^2}, \qquad \varphi_2 v = \frac{-v^3+6}{2v^2}$$

という具合に，$v=V$ と代入すると a,b,c を表わす有理式ができる．

さて，V の満たす既約方程式は上に見た通り $v^6+108=0$ で，根を $l=0,1,\cdots,5$ に対し

$$V^{(l)} = (-\omega^2)^l \cdot \sqrt[6]{-108} = (-\omega^2)^l \cdot 2^{\frac{1}{3}} \cdot 3^{\frac{1}{2}} \cdot \sqrt{-1}$$

と置く．対応する,「根の順列」を (実際に計算して) 書くと：

	φ	φ_1	φ_2
$V^{(0)}$	a	b	c
$V^{(1)}$	c	b	a
$V^{(2)}$	b	c	a
$V^{(3)}$	a	c	b
$V^{(4)}$	c	a	b
$V^{(5)}$	b	a	c

(1)　既知量に，新しい量 r の添加で，この順列の群がどうなるか (第 II 節の定理).

第一の例として $x^3-2=0$ を (もとの方程式だが) を考えて，一根ずつ添加するとどうなるか見る：$r=\sqrt[3]{2},\ \sqrt[3]{2}\,\omega,\ \sqrt[3]{2}\,\omega^2$ である．

V を根にもつ $\mathbb{Q}$ 上の既約多項式 v^6+108 は，3 根 a,b,c すべてを付け加えると，当然 1 次因子にまで分解する．しかし，a の一つだけを添加する場合は v^2+3a^2 は $\mathbb{Q}(a)$ 上既約であり ($\sqrt{-3}$ がいないから)，残りの $v^4+6a^2v^2+9a^4$ も既約となる．この場合の，a だけ添加した「順列の群」は $v^2+2a^2=(v-V^{(0)})(v-V^{(3)})$ から $V^{(0)}$ と $V^{(3)}$ の行を抜き出したもので，a は固定して，b,c を入れ替えたものである．これは $V=V^{(0)}=a(\omega-\omega^2)$ の $\mathbb{Q}(a)$ 上の既約多項式で，その体で群が縮小したということ．既知の量を増やすと V の満たす既約多項式が因数分解され，そのうちの V を含む因子をとった．

味をしめて，同じことを $\mathbb{Q}(b)$ で考えると，$\mathbb{Q}$ 上の既約多項式 v^6+108 は

$$v^6+108=(v^2+3b^2)(v^4+6b^2v^2+9b^4)$$

と既約多項式に分解される．ところが，

$$v^2+3b^2=(v-V^{(2)})(v-V^{(5)})$$

であって，根は V ではない．このあたりをどう定式化するのか (そもそも V は一回しか使えない)．リウヴィルは，苦労して，何やら証明を考えたようだが，スッキリしない．

上の v^6+108 を $F(v,a)F(v,b)F(v,c)$ と分解して，それぞれの因子が a や b や c を固定する順列に対応させるなら，

	φ	φ_1	φ_2
$V^{(0)}$	a	b	c
$V^{(3)}$	a	c	b

	φ	φ_1	φ_2
$V^{(2)}$	b	c	a
$V^{(5)}$	b	a	c

	φ	φ_1	φ_2
$V^{(1)}$	c	b	a
$V^{(4)}$	c	a	b

という 3 組の順列の群が，各々の因子の定義式に対応する分解になる．証明の式の書き方は，これだろう．

今は，V から出発した話だが，他の共軛根から出発することができるはずだ．例えば $V^{(1)}=\varphi(c,b,a)$ をとる．この時は $a=\varphi_2V^{(1)}$ である．それを不変にする順列の群は

	φ	φ_1	φ_2
$V^{(1)}$	c	b	a
$V^{(2)}$	b	c	a

同様に $V^{(4)}=\varphi(c,a,b)$ をとると $a=\varphi_1V^{(4)}$ で，それを不変にする順列の群は

	φ	φ_1	φ_2
$V^{(4)}$	c	a	b
$V^{(5)}$	b	a	c

この例は「位置」の入れ替えと「文字」の入れ替えの違いを示していて，二つの順列を持ってきて，その「比」をとる，というその比定の仕方にふた通りあることを示唆している．

ガロア分解式の根 V をひとつ固定して，補助の方程式の根 r を既知量に添加するとき，「順列の群」が「部分群」(ひとつ) に縮小する訳で，それは明確な事実だが，第 II 節の定理の 2° は，r の共軛に移ることで,「部分群」が「置換」で移されるということが観察されている．これは r の入れ替えだが，V の方を入れ替えて「部分群」が変わるということは，第一論文にはあからさまにないが，シュヴァリエへの手紙に言及されているのは，これも含めた二通りの分解の仕方である．

[**比較**]　二つの分解を並べて書いてみる：

	φ	φ_1	φ_2
$V^{(0)}$	a	b	c
$V^{(3)}$	a	c	b

	φ	φ_1	φ_2
$V^{(2)}$	b	c	a
$V^{(5)}$	b	a	c

	φ	φ_1	φ_2
$V^{(1)}$	c	b	a
$V^{(4)}$	c	a	b

	φ	φ_1	φ_2
$V^{(0)}$	a	b	c
$V^{(3)}$	a	c	b

	φ	φ_1	φ_2
$V^{(1)}$	c	b	a
$V^{(2)}$	b	c	a

	φ	φ_1	φ_2
$V^{(4)}$	c	a	b
$V^{(5)}$	b	a	c

上は文字の入れ替え，下は位置の入れ替えの形になっている．一つの順列を別の順列に移す時，それが文字の入れ替えか位置の入れ替えかの区別はできない．しかし，二つ (以上) の順列を同時に移すことを考えるなら，それが，文字か位置か，一般にはその違いが現われる．群が縮小に応じた “類別”は部分群に関わるが，文字と位置の入れ替えが等しい場合が生じて，それが正規部分群 (ガロアの用語で**固有分解**の場合) という概念の認識である．

(2)　この固有分解は，今の例で，既知量に ω を付け加えるときに現われる．もう紙幅がないので，一言だけ書いておく．

$$\omega = \frac{b}{a} = \frac{\varphi_1 V}{\varphi V} = -\frac{V^3+6}{12}$$

なので ω も ω^2 も V の “函数”であり，V をその共軛で入れ替えると「変わる」．ここに本質を見たデデキントは，それを「体の自己同型」と捉え直したのだろう．数は，絶対的に独立した「個」なのに「移る」．その「移り方」は何かの秩序を保って移るのだが，その秩序とは四則演算なのだ．

この ω が V の共軛でどのように変わるかは，$v^6=-108$ の根について $v^3=\pm 6\sqrt{-3}$ なので，符号のみを考慮すればよいが，上のように V の共軛に $V^{(l)}$ と名前をつけた時，V と同じ符号になるのは l が偶数の場合で，反対の符号は奇数の場合である．

これに注意すると v^6+108 は $\mathbb{Q}(\omega)$ 上

$$(v^3-6\sqrt{-3})(v^3+6\sqrt{-3})$$

が既約多項式への分解となって，根は $V^{(l)}$ で l の偶奇で分かれる．対応した順列の群は

	φ	φ_1	φ_2
$V^{(0)}$	a	b	c
$V^{(2)}$	b	c	a
$V^{(4)}$	c	a	b

	φ	φ_1	φ_2
$V^{(1)}$	c	b	a
$V^{(3)}$	a	c	b
$V^{(5)}$	b	a	c

に分かれる．これは，順列の「位置」の入れ替えと「文字」の入れ替えの二通りが一致する．

以上，すべてを完全に丁寧に説明するところまでは行かなかったが，相当詳しく考えを述べることができたと思う (くどい箇所もあったかもしれない)．関係する疑問や問題は当然尽きないが，更なる考察は，他日を期すこととしたい．

2025. 1. 29

[うめだ　とおる]
umeda.tooru.5x@kyoto-u.jp

追記：2025.2.3　原稿を読まれた佐藤文広氏から，補題 III に関わって，ガロアがコメントしたアーベルの遺稿についてご教示いただいた．その論文とは Précis d'une théorie des fonctions elliptiques で，Crelle 誌 (1829) に発表された (従ってガロアも読めた) ものだそうです．該当箇所は，全集第 I 巻 p.547 (アーベル全集もネット上で見ることができる)．

これを見ると，ガロアが書いた citée は「引用」と訳すのは適切でなく，単純に「言及」という程度の言葉．なお，このアーベルの論文の邦訳が『アーベル/ガロア 楕円関数論』(朝倉書店 高瀬正仁訳) にあり，対応する箇所は pp.204–205 だということです．

以上のご指摘と情報をいただいた佐藤氏に感謝いたします．