代數方程式論

代數方程式論

黃緣芳譯

Introduction To The Theory Of Algebraic Equations

by

L. E. Dickson

中華書局印行

原著者 L. E. Dickson
譯者 吳叔同
出版者 芳緣
印刷者 上海澳門路華華書局
發行者 中華書局 上海福州路
（339002）（一〇六四八）

著者略歷

狄克生 (L. E. Dickson) 美國人,曾得哲學博士學位,美國芝加谷 (Chicago) 大學算學教授,爲美國第一流代數學者.著作除本書外尙有

算術及其代數 (Arithmatics and Their Algebras),

近世代數理論 (Modern Algebraic Theories),

一次代數 (Linear Algebras),

代數不變式 (Algebraic Invariants),

數史 (History of the Numbers), 3 卷,

數論研究 (Studies in the Theory of Numbers),

數論初步 (Introd. to the Theory of Numbers),

初級方程式論 (First Course in the Th. of Equations),

方程式論初步 (Elementary Th. of Equations),

不變式及數論 (On Invariants and the Th. of Numbers) 刻於 Madison 算學講演集中

及與 Miller-Blichfeldt 合著之有限羣 (Finite Groups) 等書.

序

普通二次方程式解法,在第九世紀時卽已發見.至於普通三次及四次方程式解法,直至十六世紀始告發見.過此兩世紀間,多數學者致力於普通五次及高次方程式解法,而卒無成.1770 年, Lagrange 將前人解法加以解析,得將各種解法納於同一原理之下,利用豫解式以求方程式之根;並證明普通五次方程式不能藉有理豫解式之助而解之.繼此以後, Abel, Wantzel 及 Galois 諸氏遂證得普通 n (>4)次方程式不能藉有理或無理豫解式之助,而得代數解法.又由此等代數研究,遂產生代換論及羣論.法算學家 Cauchy 氏卽首先對代換作系統研究之人[參看 Journal de l'école Polytechnique, (工藝學校雜誌), 1815].

本書係按歷史上發展之程序而敍述.上篇論 Lagrange-Cauchy-Abel 諸氏之普通代數方程式論,下篇則論列 Galois 氏之代數方程式(其係數爲隨意或特殊皆可)論.敍述力求淺現,立言皆從初等代數出發,不牽連及算學上其他各門類.書中並有許多例解及初等習題,以資讀者學習.

著者草此書時,除引用雜誌上各門類論文外,並參考次列各書:

Lagrange: Réflexions sur la résolution algébrique des équations (方程式代數解法之評論);

Jordan: Traité des substitutions et des équations algébriques (代數方程式論及代換論);

Serret: Cours d'Algèbre supérieure (高等代數學);

Netto-Cole: Theory of substitutions and its Applications to Algebra (代換論及其在代數學上之應用);

Weber: Lehrbuch der Algebra (代數學);

Burnside: The Theory of Groups (羣論);

Pierpont: Galois' Theory of Algebraic Equations (代數方程式之 Galois 氏理論),刊於 Annals of Math. (算學年報) 第二輯第一、二兩卷中.

Bolza: On the Theory of Substitution-Groups and its Applications to Algebraic Equations (代換羣之理論及其在代數方程式上之應用),刊於 Amer. Journ. Math. (美國算學輯報) 之第13卷中.

Oscar Bolza 於 1894 年, E. H. Moore 於 1895 年, Sophie Lie 於 1896 年, Camille Jordan 於 1897 年皆講授羣論,著者均親承教澤;茲乘此機會,謹致其感謝之忱.

在上述各方面中,著者受 Bolza 教授之講演及著作之影響尤大;本書第65節內,方程式之羣之例,即係得教授之許可,由其講義中摘出者.

本書爲著者於1897年在 California 大學講演,於 1899 年在 Texas 大學講演,及 1902 年在 Chicago 大學講演兩次所得之收穫.

西曆1902年八月, L. E. Dickson 序於 Chicago.

譯者附言

1. 本書譯文力求忠實,務使原書內容毫無挂漏,除§§45, 46與原書次序互調外,其餘章節,無所改變;至此兩節互調之原因,全爲求讀者容易瞭解計耳.

2. 本書術語,多採用國立編譯館所暫定者;間有一名數譯或前後不一致處,則由譯者意見選用之.遇有未經擬定之名詞,則參酌日文著作而定之.

3. 原書祇有學名索引一項,譯者除將內容增補外,並添入人名索引一項.

4. 本書人名皆用原文,不用譯音,以免混淆及隔閡之病.

5. 譯者自維淺學,如有不當處,尙望海內人士不吝賜教!

中華民國二十四年元旦黃緣芳書於承瑞室.

目　錄

索引

代數方程式論

上篇

Lagrange-Abel-Cauchy
諸氏普通代數方程式論

第一章
普通二次三次及四次方程式之解法
關於根內無理數之 Lagrange 氏定理*

§1. 二次方程式 (Quadratic equation) 二次方程式 $x^2+px+q=0$ 之二根爲

$$x_1=\frac{1}{2}(-p+\sqrt{p^2-4q}),\qquad x_2=\frac{1}{2}(-p-\sqrt{p^2-4q}).$$

將此兩式相加、相減並相乘,得

$$x_1+x_2=-p,\quad x_1-x_2=\sqrt{p^2-4q},\quad x_1x_2=q.$$

由此知根式內之無理式 $\sqrt{p^2-4q}$ 可以根之有理函數表之,而等於 x_1-x_2. 至函數 x_1+x_2 及 x_1x_2 爲根之對稱函數,得以係數之有理函數表之.

---

*見於 Lagrange 論文集 (Œuvres de Lagrange, Paris, 1869) 第三卷中,標題爲 "Réflexions sur la résolution algébrique des équations" (方程式代數解法之評論);此文於 1770–71 年間,首由柏林學院刊行.

§2. 三次方程式 (Cubic equation) 普通三次方程式之形爲

$$x^3-c_1x^2+c_2x-c_3=0 \cdots\cdots (1)$$

令 $x=y+\frac{1}{3}c_1$, 方程式(1)可化簡爲

$$y^3+py+q=0 \cdots\cdots (2)$$

此處 $$p=c_2-\frac{1}{3}c_1^2,\quad q=-c_3+\frac{1}{3}c_1c_2-\frac{2}{27}c_1^3 \cdots\cdots (3)$$

此時,方程式(2)缺 y^2 項,稱爲**既約三次方程式** (Reduced cubic equation). 將來此式解後,(1)之諸根可由 $x=y+\frac{1}{3}c_1$ 求之.

在1505年以前,三次方程式(2)已爲 Scipio Ferreo 所解;後來 Tartaglia 復發現其解法,而以嚴守祕密爲條件,傳之於 Cardan, 但 Cardan 不遵信約,以1545年刊登其法於所著書 Ars Magna 中, 世所稱爲 Cardan 解法是也.次列之法,乃 Hudde 在1650年發表者. 其法,以變換式

$$y=z-\frac{p}{3z} \cdots\cdots (4)$$

代入方程式(2),得 $$z^3-\frac{p^3}{27z^3}+q=0,$$

即 $$z^6+qz^3-\frac{p^3}{27}=0 \cdots\cdots (5)$$

此式可作爲 z^3 之二次方程式解之,得

$$z^3=-\frac{1}{2}q\pm\sqrt{R},\qquad R\equiv\frac{1}{4}q^2+\frac{1}{27}p^3.$$

設以 $\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}$ 表 $-\frac{1}{2}q+\sqrt{R}$ 之立方根之一,則其餘兩根爲

$$\omega\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}\quad 及\quad \omega^2\sqrt[3]{-\frac{1}{2}q+\sqrt{R}};$$

此處 ω 表 1 之立方根內之一虛根,其求法如次:

1之三個立方根乃方程式

$$r^3-1=0,\text{或 }(r-1)(r^2+r+1)=0$$

之根.方程式 $r^2+r+1=0$ 之二根爲 $-\frac{1}{2}+\frac{1}{2}\sqrt{-3}\equiv\omega$ 及 $-\frac{1}{2}-\frac{1}{2}\sqrt{-3}=\omega^2$;故

$$\omega^2+\omega+1=0,\quad \omega^3=1 \cdots\cdots (6)$$

由 $\left(-\frac{1}{2}q+\sqrt{R}\right)\left(-\frac{1}{2}q-\sqrt{R}\right)=\frac{1}{4}q^2-R=-\frac{1}{27}p^3$

之關係,立方根 $\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$ 可選其能使

$$\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}\cdot\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}=-\frac{1}{3}p$$

者用之.

$$\therefore\ \omega\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}\cdot\omega^2\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}=-\frac{1}{3}p,$$

$$\omega^2\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}\cdot\omega\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}=-\frac{1}{3}p.$$

故方程式(5)之六根可分爲三對,各對之積皆等於 $-\frac{1}{3}p$;於是,與任一根 z 相配成對之根爲 $-\frac{p}{3z}$.由(4)知其和 $z-\frac{p}{3z}$ 爲三次方程式(2)之一根.又配成一對之二根均導出同一之 y 值,故(5)雖有六根,祇能導出方程式(2)之三根.更因(5)之任一對根之和皆得(2)之一根,於是,得(2)之三根 y_1, y_2, y_3 之 Cardan 氏公式爲

$$\left.\begin{aligned} y_1&=\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\frac{1}{2}q-\sqrt{R}},\\ y_2&=\omega\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\omega^2\sqrt[3]{-\frac{1}{2}q-\sqrt{R}},\\ y_3&=\omega^2\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\omega\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}. \end{aligned}\right\}\cdots\cdots (7)$$

以 $1, \omega^2, \omega$ 順序乘上列諸式而加之,並引用(6),得

$$\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}=\frac{1}{3}(y_1+\omega^2 y_2+\omega y_3);$$

次改用 $1, \omega, \omega^2$ 順序乘上列諸式而加之,得

$$\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}=\frac{1}{3}(y_1+\omega y_2+\omega^2 y_3).$$

如將此兩式之立方差分解爲因子,且引用全等式 $\omega-\omega^2\equiv\sqrt{-3}$, 得

$$\sqrt{R}=\frac{1}{54}\{(y_1+\omega^2 y_2+\omega y_3)^3-(y_1+\omega y_2+\omega^2 y_3)^3\}$$

$$=\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1).$$

故(7)之諸根內無理數,皆得以根之有理式表之,此爲 Lagrange 氏首先發見之結果也.

函數 $(y_1-y_2)^2(y_2-y_3)^2(y_3-y_1)^2=-27q^2-4p^3$

稱爲三次方程式(2)之**判別式**(Discriminant).

普通三次方程式(1)之根爲

$$x_1=y_1+\frac{1}{3}c_1,\quad x_2=y_2+\frac{1}{3}c_1,\quad x_3=y_3+\frac{1}{3}c_1;$$

故 $$x_1-x_2=y_1-y_2,\quad x_2-x_3=y_2-y_3,\quad x_3-x_1=y_3-y_1,$$

而 $$(x_1-x_2)(x_2-x_3)(x_3-x_1)=(y_1-y_2)(y_2-y_3)(y_3-y_1)$$

$$=\frac{18}{\sqrt{-3}}\sqrt{R}=-\sqrt{-3}\sqrt{\frac{1}{4}q^2+\frac{1}{27}p^3}\quad\cdots\cdots(8)$$

習 題

1. 求證 $x_1+\omega^2 x_2+\omega x_3=y_1+\omega^2 y_2+\omega y_3$, $x_1+\omega x_2+\omega^2 x_3=y_1+\omega y_2+\omega^2 y_3$.

2. 若 $R>0$, 則三次方程式(2)有一實根及二虛根;若 $R=0$, 有三實根,且有兩根相等;若 $R<0$, 即所謂不可約款(Irreducible case), 此時方程

式(2)之三根皆爲實根而不相等.

3. 求證三次方程式(1)之判別式 $(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2$ 等於 $c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2$.

提示:用(3)及(8)以求之.

4. $-\frac{1}{2}q+\sqrt{R}$ 之三立方根與 $-\frac{1}{2}q-\sqrt{R}$ 之三立方根次第相加 $\sqrt[3]{-\frac{1}{2}q+\sqrt{R}}+\sqrt[3]{-\frac{1}{2}q-\sqrt{R}}$,共得九式.求證:此九式乃次列三個三次方程式之根.

$$y^3+py+q=0,\quad y^3+\omega py+q=0,\quad y^3+\omega^2py+q=0.$$

5. 求證: $y_1+y_2+y_3=0$, $y_1y_2+y_2y_3+y_3y_1=p$, $y_1y_2y_3=-q$.

6. 用習題5,求證: $x_1+x_2+x_3=c_1$, $x_1x_2+x_2x_3+x_3x_1=c_2$, $x_1x_2x_3=c_3$. 倘欲由方程式(1)直接導出此等結果時,其方法如何?

§3. 六次方程式(Sextic)(5)之根,若除去因數$\frac{1}{3}$不計外,可列爲

$$\psi_1=x_1+\omega x_2+\omega^2x_3,\qquad \psi_4=x_1+\omega x_3+\omega^2x_2,$$
$$\psi_2=\omega^2\psi_1=x_2+\omega x_3+\omega^2x_1,\qquad \psi_5=\omega^2\psi_4=x_3+\omega x_2+\omega^2x_1,$$
$$\psi_3=\omega\psi_1=x_3+\omega x_1+\omega^2x_2,\qquad \psi_6=\omega\psi_4=x_2+\omega x_1+\omega^2x_3.$$

此等函數相異之點在 x_1, x_2, x_3 排列次序之不同;三文字共有六種排列,故將函數 ψ_1 內之 x_1, x_2, x_3 予以排列後,即得此等函數之全部;因此,ψ_1 稱爲**六值函數**(Six-valued function).

Lagrange 普通三次方程式(1)之演繹的解法,在直接決定六函數 $\psi_1,\cdots,\psi_6$. 此等函數乃六次方程式 $(t-\psi_1)\cdots(t-\psi_6)=0$ 之根,其係數爲 $\psi_1,\cdots,\psi_6$ 之對稱函數,故亦爲 x_1, x_2, x_3 之對稱函數;於是,可以 c_1, c_2, c_3 之有理函數表之.*次因 $\psi_2=\omega^2\psi_1, \psi_3=\omega\psi_1$,

*關於對稱函數基本定理之證明,見本書附錄內.

由(6),得

$$(t-\psi_1)(t-\psi_2)(t-\psi_3)=t^3-\psi_1{}^3,$$
$$(t-\psi_4)(t-\psi_5)(t-\psi_6)=t^3-\psi_4{}^3.$$

故六次豫解式(Resolvent)化爲

$$t^6-(\psi_1{}^3+\psi_4{}^3)t^3+\psi_1{}^3\psi_4{}^3=0 \quad \cdots\cdots(9)$$

但由§2後之習題6,

$$\psi_1\psi_4=x_1{}^2+x_2{}^2+x_3{}^2+(\omega+\omega^2)(x_1x_2+x_2x_3+x_3x_1)$$
$$=(x_1+x_2+x_3)^2-3(x_1x_2+x_2x_3+x_3x_1)$$
$$=c_1{}^2-3c_2,$$
$$\psi_1{}^3+\psi_4{}^3=2(x_1{}^3+x_2{}^3+x_3{}^3)-3(x_1{}^2x_2+x_1x_2{}^2+x_2{}^2x_3$$
$$+x_2x_3{}^2+x_3{}^2x_1+x_3x_1{}^2)+12x_1x_2x_3$$
$$=3(x_1{}^3+x_2{}^3+x_3{}^3)-(x_1+x_2+x_3)^3+18x_1x_2x_3$$
$$=2c_1{}^3-9c_1c_2+27c_3.$$

故方程式(9)化爲

$$t^6-(2c_1{}^3-9c_1c_2+27c_3)t^3+(c_1{}^2-3c_2)^3=0.$$

此式可當作t^3之二次方程式解之,得兩根θ及θ',因得

$$\psi_1=\sqrt[3]{\theta},$$
$$\psi_4=\sqrt[3]{\theta'}.$$

此處$\sqrt[3]{\theta}$可選取θ之任一立方根,而$\sqrt[3]{\theta'}$之選取則爲θ'之一定立方根,要使

$$\sqrt[3]{\theta}\cdot\sqrt[3]{\theta'}=c_1{}^2-3c_2 \quad \cdots\cdots(10)$$

者用之.遂得次之諸已知式:

$$x_1+\omega x_2+\omega^2x_3=\sqrt[3]{\theta},$$
$$x_1+\omega^2x_2+\omega x_3=\sqrt[3]{\theta'},$$
$$x_1+x_2+x_3=c_1.$$

順序以1, 1, 1乘此三式而加之,次以ω^2, ω, 1, 又次以ω, ω^2, 1

乘而加之,則得(1)之根

$$\left.\begin{aligned} x_1&=\frac{1}{3}(c_1+\sqrt[3]{\theta}+\sqrt[3]{\theta'}),\\ x_2&=\frac{1}{3}(c_1+\omega^2\sqrt[3]{\theta}+\omega\sqrt[3]{\theta'}),\\ x_3&=\frac{1}{3}(c_1+\omega\sqrt[3]{\theta}+\omega^2\sqrt[3]{\theta'}). \end{aligned}\right\}\quad\cdots\cdots(11)$$

§4. 四次方程式(Quartic equation)　普通四次方程式

$$x^4+ax^3+bx^2+cx+d=0\quad\cdots\cdots(12)$$

可化爲　$(x^2+\frac{1}{2}ax)^2=(\frac{1}{4}a^2-b)x^2-cx-d$

之形. Ferrari之解法,乃以 $(x^2+\frac{1}{2}ax)y+\frac{1}{4}y^2$ 加於上式之兩端,得

$$(x^2+\frac{1}{2}ax+\frac{1}{2}y)^2=(\frac{1}{4}a^2-b+y)x^2+(\frac{1}{2}ay-c)x+\frac{1}{4}y^2-d\quad\cdots(13)$$

再求 y 之值 y_1,使(13)之右端成完全平方.設令

$$a^2-4b+4y_1=t^2\quad\cdots\cdots(14)$$

則右端欲成完全平方,必須

$$\frac{1}{4}t^2x^2+(\frac{1}{2}ay_1-c)x+\frac{1}{4}y_1^2-d=\left(\frac{1}{2}tx+\frac{\frac{1}{2}ay_1-c}{t}\right)^2,$$

$$\therefore\quad \frac{1}{4}y_1^2-d=\left(\frac{\frac{1}{2}ay_1-c}{t}\right)^2=\frac{\left(\frac{1}{2}ay_1-c\right)^2}{a^2-4b+4y_1}\quad\cdots\cdots(15)$$

故 y_1 必爲三次方程式

$$y^3-by^2+(ac-4d)y-a^2d+4bd-c^2=0\quad\cdots\cdots(16)$$

之一根,此方程式稱爲四次方程式(12)之豫解式.

由(15),方程式(13)可析爲兩二次方程式

$$x^2+\left(\frac{1}{2}a-\frac{1}{2}t\right)x+\frac{1}{2}y_1-\left(\frac{1}{2}ay_1-c\right)\Big/t=0\quad\cdots\cdots(17)$$

$$x^2+\left(\frac{1}{2}a+\frac{1}{2}t\right)x+\frac{1}{2}y_1+\left(\frac{1}{2}ay_1-c\right)\Big/t=0\cdots\cdots\cdots\cdots(18)$$

設 x_1 及 x_2 爲(17)之根,x_3 及 x_4 爲(18)之根,則有

$$x_1+x_2=-\frac{1}{2}a+\frac{1}{2}t,\quad x_1x_2=\frac{1}{2}y_1-\left(\frac{1}{2}ay_1-c\right)\Big/t,$$

$$x_3+x_4=-\frac{1}{2}a-\frac{1}{2}t,\quad x_3x_4=\frac{1}{2}y_1+\left(\frac{1}{2}ay_1-c\right)\Big/t.$$

若加減之,得

$$x_1+x_2-x_3-x_4=t,\quad x_1x_2+x_3x_4=y_1\cdots\cdots\cdots\cdots\cdots(19)$$

解(17)及(18)兩式,得兩根數 (Radical),其一等於 x_1-x_2,他一等於 x_3-x_4 (參看§1). 故普通四次方程式根內所含之無理數,爲根之有理函數.

設不用 y_1,而以三次豫解式(16)之他根代之,則得與(17)、(18)不同之其他二次方程式,其四根仍爲 x_1, x_2, x_3, x_4,惟其各對配合,與前相異.故(16)之三根可推定其爲

$$y_1=x_1x_2+x_3x_4,\ y_2=x_1x_3+x_2x_4,\ y_3=x_1x_4+x_2x_3\cdots\cdots(20)$$

事實上,由次節之證明,知此種推測,確當無誤.

§5. 從有理函數 $x_1x_2+x_3x_4$ 及 $x_1+x_2-x_3-x_4=t$,亦可求得兩二次方程式,其根卽爲普通四次方程式(12)之四根,而不必借助於 Ferrari 之方法.蓋(20)內三量乃 $(y-y_1)(y-y_2)(y-y_3)=0$, 或

$$y^3-(y_1+y_2+y_3)y^2+(y_1y_2+y_2y_3+y_3y_1)y-y_1y_2y_3=0\cdots\cdots(21)$$

之三根,其係數可以 a, b, c, d 之有理函數表之:*

$$y_1+y_2+y_3=x_1x_2+x_3x_4+x_1x_3+x_2x_4+x_1x_4+x_2x_3=b,$$

$$y_1y_2+y_2y_3+y_3y_1=-4x_1x_2x_3x_4+(x_1+x_2+x_3+x_4)(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)=ac-4d,$$

*此因(見於§29之例2及§30) $1, 2, 3, 4$ 之任一排列,祇變換 y_1, y_2, y_3 之順序,故 y_1, y_2, y_3 之對稱函數,亦卽爲 $1, 2, 3, 4$ 之對稱函數,卽可以 a, b, c, d 之有理函數表之.

$$y_1y_2y_3=(x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)^2$$
$$+x_1x_2x_3x_4\{(x_1+x_2+x_3+x_4)^2$$
$$-4(x_1x_2+x_1x_3+\cdots+x_3x_4)\}$$
$$=c^2+d(a^2-4b).$$

故方程式(21)與豫解式(16)全同.又

$$t^2=(x_1+x_2+x_3+x_4)^2-4(x_1+x_2)(x_3+x_4)$$
$$=a^2-4(x_1x_2+x_1x_3+\cdots+x_3x_4)+4x_1x_2+4x_3x_4$$
$$=a^2-4b+4y_1,$$

而 $x_1+x_2+x_3+x_4=-a$, 故

$$x_1+x_2=\frac{1}{2}(t-a),\quad x_3+x_4=\frac{1}{2}(-t-a).$$

今欲求 x_1x_2 及 x_3x_4, 因 $x_1x_2+x_3x_4=y_1$, 而

$$-c=x_1x_2(x_3+x_4)+x_3x_4(x_1+x_2)$$
$$=x_1x_2\left(\frac{-t-a}{2}\right)+x_3x_4\left(\frac{t-a}{2}\right),$$

$$\therefore\quad x_1x_2=(c-\frac{1}{2}ay_1+\frac{1}{2}ty_1)/t,\quad x_3x_4=(-c+\frac{1}{2}ay_1+\frac{1}{2}ty_1)/t.$$

故 x_1 及 x_2 爲(17)之根, x_3 及 x_4 爲(18)之根.

§6. Lagrange 氏四次方程式(12)之演繹的解法,與上所述者殊相似.氏先求(16)之一根 $y_1=x_1x_2+x_3x_4$; 次因 $x_1x_2\equiv z_1$ 及 $x_3x_4\equiv z_2$ 爲

$$z^2-y_1z+d=0$$

之根,而 x_1+x_2 及 x_3+x_4 可由

$$(x_1+x_2)+(x_3+x_4)=-a,$$
$$z_2(x_1+x_2)+z_1(x_3+x_4)=x_3x_4x_1+x_3x_4x_2+x_1x_2x_3+x_1x_2x_4=-c$$

求之;解此兩方程式,得

$$x_1+x_2=(-az_1+c)/(z_1-z_2),\quad x_3+x_4=(az_2-c)/(z_1-z_2).$$

於是，x_1 及 x_2，同樣，x_3 及 x_4，皆可由解二次方程式求之.

§7. 解三次方程式(16)時，所遇之無理數(參看§2)爲

$$\Delta \equiv (y_1-y_2)(y_2-y_3)(y_1-y_3).$$

但，由(20)

$$y_1-y_2=(x_1-x_4)(x_2-x_3),$$
$$y_2-y_3=(x_1-x_2)(x_3-x_4),$$
$$y_1-y_3=(x_1-x_3)(x_2-x_4).$$

故 $$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4) \quad \cdots\cdots(22)$$

由§2，知(16)之既約式爲 $\eta^3+P\eta+Q=0$，此處，

$$\left.\begin{aligned} P&=ac-4d-\frac{1}{3}b^2, \\ Q&=-a^2d+\frac{1}{3}abc+\frac{8}{3}bd-c^2-\frac{2}{27}b^3 \end{aligned}\right\} \cdots\cdots(23)$$

由(8)，變其符號，得 $$\Delta=6\sqrt{-3}\sqrt{\frac{1}{4}Q^2+\frac{1}{27}P^3} \quad \cdots\cdots(24)$$

第二章
代換 有理函數

§8. 設 $\alpha, \beta, \cdots, \nu$ 爲 $1, 2, \cdots, n$ 排列之一種,則以 x_α 代 x_1, x_β 代 x_2, x_γ 代 x_3, $\cdots$, x_ν 代 x_n 之運算,稱爲就 $x_1, x_2, x_3, \cdots, x_n$ 之代換 (Substitution).通常以

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_\alpha & x_\beta & x_\gamma & \cdots & x_\nu \end{pmatrix}$$

表之.此種記法與列之次序無關,故此代換亦可記爲

$$\begin{pmatrix} x_2 & x_1 & x_3 & \cdots & x_n \\ x_\beta & x_\alpha & x_\gamma & \cdots & x_\nu \end{pmatrix}, \text{ 或} \begin{pmatrix} x_n & x_1 & x_2 & x_3 & \cdots \\ x_\nu & x_\alpha & x_\beta & x_\gamma & \cdots \end{pmatrix}, \cdots.$$

代換之使諸文字無改變者,

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_1 & x_2 & x_3 & \cdots & x_n \end{pmatrix},$$

稱爲么代換 (Identical substitution),以 $\boldsymbol{I}$ 表之.

§9. 定理 ***n* 文字所成不同代換之數爲 $n!=n(n-1)\cdots 3\cdot 2\cdot 1$.**

此因 n 文字之每一種排列,即有一種代換與之相應.

例 對於 $n=3$ 文字之 $3!=6$ 種代換爲

$$I=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix}, \quad a=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad b=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix},$$

$$c=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_3 & x_2 \end{pmatrix}, \quad d=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix}, \quad e=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}.$$

倘將此等代換施於 $\psi=x_1+\omega x_2+\omega^2 x_3$,則得六個不等函數(參看 §3.):

$\psi_I=x_1+\omega x_2+\omega^2 x_3\equiv\psi$, $\psi_a=x_2+\omega x_3+\omega^2 x_1=\omega^2\psi$, $\psi_b=x_3+\omega x_1+\omega^2 x_2=\omega\psi$,

$\psi_c=x_1+\omega x_3+\omega^2 x_2$, $\psi_d=x_3+\omega x_2+\omega^2 x_1=\omega^2\psi_c$, $\psi_e=x_2+\omega x_1+\omega^2 x_3=\omega\psi_c$.

若施於 $\phi\equiv(x_1-x_2)(x_2-x_3)(x_3-x_1)$，則得

$$\phi_I=\phi_a=\phi_b=\phi_c=\phi_d=\phi_e=-\phi.$$

故 ϕ 當施以代換 I, a, b 時不變，而施以代換 c, d, e 時則變.

§10. 積 令

$$s=\begin{pmatrix}x_1 & x_2 & \cdots & x_\eta\\ x_\alpha & x_\beta & \cdots & x_\nu\end{pmatrix},\qquad t=\begin{pmatrix}x_\alpha & x_\beta & \cdots & x_\nu\\ x_{\alpha'} & x_{\beta'} & \cdots & x_{\nu'}\end{pmatrix}.$$

設先用代換 s，次用代換 t，其終結排列 $x_{\alpha'}, x_{\beta'}, \cdots, x_{\nu'}$ 可直接由最初排列 $x_1, x_2, \cdots, x_n$ 施以如次代換

$$u=\begin{pmatrix}x_1 & x_2 & \cdots & x_\eta\\ x_{\alpha'} & x_{\beta'} & \cdots & x_{\nu'}\end{pmatrix}.$$

得來，吾人稱 u 爲以 t 乘 s 之積(Product)，以 $u=st$ 表之.

同樣，stv 表先用 s，次 t，又次 v 而得之代換 w，故

$$stv=uv=w.$$

此處施用因子之次序爲自左向右.*

例　就三文字之代換(§9)有

$$ab=ba=I,\quad ac=d,\quad ca=e,\quad ad=e,\quad da=c,$$

$$aa=b,\quad bb=a,\quad abc=Ic=c,\quad aca=da=c.$$

倘施代換 a 於函數 ψ，則得 ψ_a，施代換 c 於 ψ_a 得 ψ_d，故 $\psi_{ac}=\psi_d$. 同樣，$\psi_{ab}=\psi_I=\psi$, $\psi_{ba}=\psi$.

§11. 普通代換之乘法，其次序不可對易 (Non-commutative).

如上例內 $ac\neq ca$, $ad\neq da$. 但，$ab=ba$，故 a 及 b 稱爲對易代換.

§12. 代換之乘法適用締合律(Associative law):

$$st\cdot v=s\cdot tv.$$

---

*此爲近世所用之記法；以前，Cayley 及 Serret 二氏乃用其逆次序 ts, ots 表之.

令 s, t 及其積 $st=u$ 與 §10 之記法相同.設

$$v=\begin{pmatrix} x_\alpha' & x_\beta' & \cdots & x_\nu' \\ x_\alpha'' & x_\beta'' & \cdots & x_\nu'' \end{pmatrix},$$

則

$$tv=\begin{pmatrix} x_\alpha & x_\beta & \cdots & x_\nu \\ x_\alpha'' & x_\beta'' & \cdots & x_\nu'' \end{pmatrix}.$$

$$\therefore \quad st\cdot v=uv=\begin{pmatrix} x_1 & x_2 & \cdots & x_\eta \\ x_\alpha'' & x_\beta'' & \cdots & x_\nu'' \end{pmatrix}$$

$$=\begin{pmatrix} x_1 & x_2 & \cdots & x_\eta \\ x_\alpha & x_\beta & \cdots & x_\nu \end{pmatrix}\begin{pmatrix} x_\alpha & x_\beta & \cdots & x_\nu \\ x_\alpha'' & x_\beta'' & \cdots & x_\nu'' \end{pmatrix}$$

$$=s\cdot tv.$$

例　在三文字之例，$ac\cdot a=da=c$，$a\cdot ca=ab=c$.

§13. 冪 (Powers)　茲以 s^2 代 ss, s^3 代 sss, 餘仿此類推.故

$$s^m s^n=s^{m+n} \qquad (m \text{ 及 } n \text{ 爲正整數}) \cdots\cdots\cdots\cdots (25)$$

此乃由締合律得來,因 $s^m\cdot s^n=s^m\cdot ss^{n-1}=s^{m+1}s^{n-1}=\cdots$.

§14. 週期　因 n 文字之不同代換僅有 $n!$ 種,故 s 之各乘冪

$$s,\ s^2,\ s^3 \cdots \text{以至無窮}$$

中必有相等者,設 $s^m=s^{m+n}$, 此處 m, n 爲正整數.由 (25), $s^m=s^m s^n$; 故 s^n 使 n 文字無所改變;是以 $s^n=I$.

設 σ 爲**最小正整數能使** $s^\sigma=I$, 此 σ 稱爲 s **之週期** (Period). 於是,

$$s,\ s^2,\ s^3,\ \cdots,\ s^{\sigma-1},\ s^\sigma\equiv I \cdots\cdots\cdots\cdots (26)$$

爲不同之代換,而 $s^{\sigma+1}$, $s^{\sigma+2}$, $\cdots$ $s^{2\sigma}$, 則爲 (26) 內諸代換之重複; 如是類推,可知在 s, s^2, s^3, $\cdots$ 內,雖其數無窮,其實皆爲前 σ 個 s 之冪之循環重複.

例　由 §10 之例,得

$$a^2=b, \quad a^3=a^2a=ba=I, \quad \text{故 } a \text{ 之週期爲 3;}$$

$b^2=a$, $b^3=b^2b=ab=I$, 故 b 之週期爲 3;

c, d, e 之週期各爲 2; I 之週期爲 1.

§15. 逆代換 (Inverse substitution) 凡一代換 s, 必有一,且僅有一代換 s' 使 $ss'=I$. 設

$$s=\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_\alpha & x_\beta & \cdots & x_\nu \end{pmatrix}, \quad \text{則} \quad s'=\begin{pmatrix} x_\alpha & x_\beta & \cdots & x_\nu \\ x_1 & x_2 & \cdots & x_n \end{pmatrix},$$

而 $ss'=I$. 吾人稱 s' 爲代換 s 之**逆** (Inverse), 以 s^{-1} 表之.於是

$$ss^{-1}=s^{-1}s=I, \quad (s^{-1})^{-1}=s.$$

設 s 之週期爲 σ, 則 $s^{-1}=s^{\sigma-1}$. 因 s 使有理函數 $f\equiv f(x_1, x_2, \cdots, x_n)$ 換爲 $f_s\equiv f(x_\alpha, x_\beta, \cdots, x_\nu)$, 而 s^{-1} 則將 f_s 換爲 f.

例 對於三文字之代換 (§9) 爲

$$a=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad a^{-1}=\begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix}\equiv\begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}=b,$$

$$b^{-1}=a, \quad c^{-1}=c, \quad d^{-1}=d, \quad e^{-1}=e, \quad I^{-1}=I.$$

此等結果亦可由 §14 之例得來.其在 §9 之諸函數,則代換 a 將 ψ 換爲 ψ_a,而 $a^{-1}=b$,則將 ψ_a 換爲 ψ.

§16. 定理 設 $st=sr$, 則 $t=r$.

設以 s^{-1} 乘 st 及 r 之左側,得

$$s^{-1}st=t, \qquad s^{-1}sr=r.$$

故 $$t=r.$$

§17. 定理 設 $ts=rs$, 則 $t=r$.

§18. 代換之簡記法 代換之如

$$a=\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, b=\begin{pmatrix} x_1 & x_3 & x_2 \\ x_3 & x_2 & x_1 \end{pmatrix}, q=\begin{pmatrix} x_2 & x_3 & x_1 & x_4 \\ x_3 & x_1 & x_4 & x_2 \end{pmatrix}$$

者,乃將上行之第一文字以上行之第二文字換之,上行之第二文字以上行之第三文字換之,仿此,其上行之最後文字以上行

之第一文字換之.此種代換稱爲**循環代換**(Circular substitutions 或 Cycles).除以上複行記法(Double-row notation)以外,更有以單行記法(Single-row notation)表循環代換者.例如:

$$a=(x_1x_2x_3),\quad b=(x_1x_3x_2),\quad q=(x_2x_3x_1x_4).$$

因 $(x_1x_2x_3)$, $(x_2x_3x_1)$, $(x_3x_1x_2)$ 皆爲以 x_2 換 x_1, x_3 換 x_2, x_1 換 x_3,是以 $(x_1x_2x_3)=(x_2x_3x_1)=(x_3x_1x_2)$. 故**循環代換內各文字施以循環排列,結果皆同.**

任一代換可以取要替換之諸文字所成循環代換之積表之.例如:

$$\begin{pmatrix}x_1 & x_2 & x_3\\ x_1 & x_3 & x_2\end{pmatrix}=(x_1)(x_2x_3),$$

$$\begin{pmatrix}x_1 & x_2 & x_3 & x_4 & x_5 & x_6\\ x_3 & x_6 & x_5 & x_4 & x_1 & x_2\end{pmatrix}=(x_1x_3x_5)(x_2x_6)(x_4).$$

單文字之循環代換,常被省略,此時,吾人祇記取:不列出之文字在代換內皆爲不變者.例如, $(x_1)(x_2x_3)$ 僅須記爲 (x_2x_3).

兩文字之循環代換稱爲**易位**(Transposition), 如 (x_2x_3) 是.

§19. 當 $n=3,4,5$ 時之代換表.

當 $n=3$ 時,其 $3!=6$ 代換爲(與 §9 比較):

$$I=\text{么代換},\quad a=(x_1x_2x_3),\quad b=(x_1x_3x_2);$$

$$c=(x_2x_3),\quad d=(x_1x_3),\quad e=(x_1x_2).$$

當 $n=4$ 時,其 $4!=24$ 代換爲[下面祇將其下標(Subscript)列出]:

$I=$ 么代換;

6 易位: (12), (13), (14), (23), (24), (34);

8 個 3 文字循環代換: (123), (132), (124), (142), (134), (143), (234), (243);

6 個 4 文字循環代換: (1234), (1243), (1324), (1342), (1423),

(1432);

3 個兩易位之積: (12)(34), (13)(24), (14)(23).

當 $n=5$ 時,其 $5!=120$ 代換內,含

I = 么代換;

$\frac{5\cdot4}{2}=10$ 個如 (12) 形之易位;

$\frac{5\cdot4\cdot3}{3}=20$ 個如 (123) 形之循環代換;

$\frac{5\cdot4\cdot3\cdot2}{4}=30$ 個如 (1234) 形之循環代換;

$\frac{5\cdot4\cdot3\cdot2\cdot1}{5}=24$ 個如 (12345) 形之循環代換;

$5\cdot3=15$* 個如 (12)(34) 形之積;

20 † 個如 (123)(45) 形之積.

習 題

1. (123…n) 之週期爲 n,其逆代換爲 (n $n-1$ …321).

2. 任一代換之週期等於各循環代換週期之最小公倍數.例如: (123)(45) 之週期等於 $3\cdot2=6$.

3. 求六文字代換內每種形狀所含代換之數.

4. 求證施 I, (x_1x_2), (x_3x_4), $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$, $(x_1x_3x_2x_4)$, $(x_1x_4x_2x_3)$ 諸代換於函數 $x_1x_2+x_3x_4$ 其式不變.

5. 求證施 (x_2x_3), (x_1x_4), $(x_1x_3x_2)$, $(x_1x_2x_4)$, $(x_1x_4x_3)$, $(x_2x_3x_4)$, $(x_1x_2x_4x_3)$, $(x_1x_3x_4x_2)$ 諸代換於函數 $x_1x_2+x_3x_4$, 其式變爲 $x_1x_3+x_2x_4$.

---

*此因所刪去之文字,可爲五文字中之任一文字;而所餘四文字中之一字,可與其他三文字之任一文字締合而成一易位也.

† 因 (45)=(54), 故形狀爲 (123)(45) 之代換之數與 (123) 形代換之數同.

6. 求於習題 4, 5 內所列 4 文字代換外,將其他 8 種代換列出,並證此等代換將 $x_1y_2+x_3y_4$ 換爲 $x_1y_4+x_2y_3$.

第 三 章

代換羣 有理函數

§20. 在一組不同代換 $s_1, s_2, \cdots, s_m$ 內,任意二代換(或相等或不同) 之積倘亦爲此組內之一代換時,則此組代換構成一羣(Group). 如羣內含 m 個不同代換,則 m 爲此羣之**級**(Order). 諸代換所施之文字之數 n 爲此羣之**次**(Degree). 此羣以 $G_m^{(n)}$ 表之.

n 文字所成之 $n!$ 代換構成一羣,稱爲 ***n* 文字之對稱羣** (Symmetric group on n letters), 以 $G_{n!}^{(n)}$ 表之. 蓋 n 文字之任意兩代換之積,復爲 n 文字代換之一種,故成一羣;其稱爲對稱羣者,乃因施此羣內諸代換於任一有理對稱函數,其函數皆不生改變也.

例 1. 關於 §9 內 $n=3$ 文字之 6 代換,其乘積表 (Multiplication table) 如次:*

$G_6^{(3)}$

	I	a	b	c	d	e
I	I	a	b	c	d	e
a	a	b	I	d	e	c
b	b	I	a	e	c	d
c	c	e	d	I	b	a
d	d	c	e	a	I	b
e	e	d	c	b	a	I

例如, $ad=e$ 可由 a 行 d 列之交點求之.

例 2. 代換 I, a, b 亦成一羣,其乘積表爲

	I	a	b
I	I	a	b
a	a	b	I
b	b	I	a

*一部分已見於 §10 之例.

設 s 爲週期 m 之代換,則

$$I,\ s,\ s^2,\ \cdots,s^{m-1}$$

成一 m 級之羣,此羣稱爲**循環羣** (Cyclic group).

例 3.　$I,\ a=(123),\ b=a^2=(132)$ 成一循環羣(例 2).

例 4.　$I,\ s=(123)(45),\ s^2=(132),\ s^3=(45),\ s^4=(123),\ s^5=(132)(45)$ 成一 6 級 5 次之循環羣.

§21. 基本定理　凡就 $x_1, x_2, \cdots, x_n$ 之代換,施於有理函數 $\phi(x_1,x_2,\cdots,x_n)$,能使此函數不變時,此等代換全部成一羣 G.

命 ϕ_s 表施代換 s 於 ϕ 後之函數.設 a 及 b 爲使 ϕ 不改變之兩代換,即 $\phi_a\equiv\phi, \phi_b\equiv\phi$. 於是,

$$(\phi_a)_b=(\phi)_b=\phi_b=\phi,\ \text{或}\ \phi_{ab}=\phi.$$

故 ab 亦爲能使 ϕ 不改變之代換.以是知:使 ϕ 不改變之諸代換具羣之性質.

羣 G 稱爲**函數 ϕ 之羣** (Group of the function ϕ), 而函數 ϕ 稱爲**屬於羣 G** (To belong to the group G).

例 1.　3 文字之代換內,能使函數 $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 不變者:有(由 §9) $I,\ a=(x_1x_2x_3),\ b=(x_1x_3x_2)$ 三代換.此等代換成一羣(與 §20, 例 2 比較). 其他函數亦屬於此羣者爲 $(x_1+\omega x_2+\omega^2x_3)^3$, 此處 ω 表 1 之虛數立方根之一.

例 2.　3 文字代換能使 $x_1+\omega x_2+\omega^2x_3$ 不變而爲么代換 I (§9), 故單獨一么代換 I 成一級羣 G_1.

例 3.　在四次方程式解法 (§4) 內發生之諸有理函數,提供吾人以次列之四文字代換羣:

(a) 四文字諸代換所成之對稱羣 G_{24}.

(b) 函數 $y_1=x_1x_2+x_3x_4$ 所屬之羣 (第 16、17 頁,習題 4–6):

$$G_8=\{\ I,\ (12),\ (34),\ (12)(34),\ (13)(24),\ (14)(23),\ (1324),\ (1423)\ \}.$$

(c) 於函數 $y_1=x_1x_2+x_3x_4$ 內，將 x_2 及 x_3 互換，則得 $y_2=x_1x_3+x_2x_4$，故 y_1 之羣，可由 G_8 內諸代換將 x_2 及 x_3 互換得之．故 y_2 之羣爲

$$G_8'=\{I,\ (13),\ (24),\ (13)(24),\ (12)(34),\ (14)(32),\ (1234),\ (1432)\}.$$

(d) $y_3=x_1x_4+x_2x_3$ 可由 G_8 將 x_2 及 x_4 互換得來：

$$G_8''=\{I,\ (14),\ (32),\ (14)(32),\ (13)(42),\ (12)(43),\ (1342),\ (1243)\}.$$

(e) 函數 $x_1+x_2-x_3-x_4$ 屬於羣

$$H_4=\{I,\ (12),\ (34),\ (12)(34)\}.$$

因 H_4 之諸代換含於羣 G_8 內，H_4 稱爲 G_8 之**子羣**(Subgroup)．但 H_4 非 G_8' 之子羣．

(f) 使函數 $\psi\equiv y_1+\omega y_2+\omega^2y_3$，或

$$\psi\equiv x_1x_2+x_3x_4+\omega(x_1x_3+x_2x_4)+\omega^2(x_1x_4+x_2x_3),$$

不變之代換，必爲使 y_1，y_2 及 y_3 同時不改變之代換．舍此以外之其餘代換必不適用．故 ψ 之羣必爲三羣 G_8，G_8'，G_8'' 內公有代換所構成，卽必爲此三羣之**最大公子羣**(Greatest common subgroup)．

$$G_4=\{I,\ r=(12)(34),\ s=(13)(24),\ t=(14)(23)\}.$$

此四代換成爲一羣可如次直接驗之：

$$r^2=I,\quad s^2=I,\quad t^2=I,$$

$$rs=sr=t,\quad rt=tr=s,\quad st=ts=r.$$

由此知此羣內任意兩代換皆可對易．而此對易羣(Commutative group) G_4 爲 G_8，G_8'，G_8'' 之子羣．

§22. 定理　每一代換可用種種易位之積表之

任何一代換可取要替換諸文字所成循環代換之積表之(§18)，而含 n 文字之循環代換，又可以 $(n-1)$ 個易位之積表之：

$$(1234\cdots n)=(12)(13)(14)\cdots(1n),$$

故得定理之證．

例　$(123)(456)=(12)(13)(45)(46)$.

$$(132)=(13)(12)=(12)(23)=(12)(23)(45)(45).$$

§23. 定理　凡將所設代換 s 分解爲種種易位之積時,其分解之結果,非皆含偶數之易位,即皆含奇數之易位.屬於前種之代換稱爲偶代換(Even substitution);**屬於後者之代換稱爲奇代換**(Odd substitution).

施一次易位於**交錯函數**(Alternating function)*

$$\phi=(x_1-x_2)(x_1-x_3)(x_1-x_4)\cdots(x_1-x_n)$$
$$(x_2-x_3)(x_2-x_4)\cdots(x_2-x_n)$$
$$\cdots\cdots\quad\cdots\cdots\cdots\cdots$$
$$(x_{n-1}-x_n),$$

則變其符號.例如,(x_1x_2) 僅將積中之第一、二兩行各因子變爲

$$(x_2-x_1)(x_2-x_3)(x_2-x_4)\cdots(x_2-x_n)$$
$$(x_1-x_3)(x_1-x_4)\cdots(x_1-x_n).$$

故若 s 爲偶數易位之積時,則此代換使 ϕ 不變;若 s 爲奇數易位之積時,則此代換變 ϕ 爲 $-\phi$.

系　n 文字所成偶代換之全部構成一羣稱爲 n **文字之交錯羣**(Alternating group on n letters),因其使交錯函數不變也.

例 1.　3 文字之交錯羣爲(§§9, 19)

$$G_3^{(3)}=\{I,\ (123),\ (132)\}.$$

例 2.　4 文字之交錯羣爲(§19)

$$G_{12}^{(4)}=\{I,\ (12)(34),\ (13)(24),\ (14)(23),\ \text{及八個三文字之循環代換}\}.$$

*此函數可以行列式

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{vmatrix}$$

表之.

§24. 定理 n **文字交錯羣之級爲** $\frac{1}{2}n!$.

以 $$e_1, e_2, e_3, \cdots e_k \quad\cdots\cdots(e)$$

表不同偶代換.設 t 爲一易位,則

$$e_1t, e_2t, e_3t, \cdots, e_kt \quad\cdots\cdots(o)$$

各不相同(§17);又因其爲奇代換,故亦異於偶代換 (e).又各奇代換 s 皆含於 (o) 內,故 st 爲偶代換,必與 (e) 內一代換 e_i 相同.是以

$$s=e_it^{-1}=e_it.$$

故 (e) 及 (o) 共有 $2k$ 代換,合成 n 文字之全部 $n!$ 個代換.故

$$k=\frac{1}{2}n!.$$

§25. 由§21知:凡有理函數 $\phi(x_1, \cdots, x_n)$ 屬於文字爲 $x_1, x_2, \cdots, x_n$ 之某代換羣 G 時,則施 G 內各代換於此函數,必不變此函數;又施以 G 外其他代換時,必變此函數.反之,

與一 n **文字** $x_1, \cdots, x_n$ **之代換羣** G**,則吾人能作成屬於** G **之有理函數** $\phi(x_1, \cdots, x_n)$. 茲證之如次:

令 $G=\{a\equiv I, b, c, \cdots l\}$. 設

$$V=m_1x_1+m_2x_2+\cdots+m_nx_n,$$

其各係數 $m_1, m_2, \cdots, m_n$ 俱不相等,則 V 爲一 $n!$ 值函數.以 G 內之代換施於 V,得

$$V_a\equiv V,\ V_b,\ \cdots,\ V_l \quad\cdots\cdots(27)$$

亦不相等.次再以 G 之任意代換 c 施於(27),得

$$V_{ac},\ V_{bc},\ \cdots\ V_{lc} \quad\cdots\cdots(28)$$

因 $ac, bc, \cdots, lc$ 各不相同(§17),且全屬於羣 G,故(28)諸值爲(27)諸值之一種排列.於是,施 G 內各代換於 $V_a, V_b, \cdots, V_l$ 之任意對稱函數,則此函數必不變.試選定一參數(Parameter) ρ,則對稱函數

$$\phi\equiv(\rho-V)(\rho-V_b)(\rho-V_c)\cdots(\rho-V_l).$$

若施以 G 外各代換 s 必生改變.此因 V_s 與 $V, V_b, V_c, \cdots, V_t$ 不同,故

$$\phi_s \equiv (\rho - V_s)(\rho - V_{bs})(\rho - V_{cs})\cdots(\rho - V_{ts})$$

亦必與 ϕ 不同也.

例 1.　就 $G=\{I, a=(x_1x_2x_3), b=(x_1x_3x_2)\}$ 言之,吾人取

$$V=x_1+\omega x_2+\omega^2 x_3,$$

則 $V_a=\omega^2 V$, $V_b=\omega V$. 故

$$V+V_a+V_b=(1+\omega+\omega^2)V=0,$$

$$VV_a+VV_b+V_aV_b=0,$$

$$VV_aV_b=V^3.$$

函數 V^3 即爲屬於羣 G 之函數(參看 §21, 例 1).

例 2.　就 $G=\{I, c=(x_2x_3)\}$ 言之,吾人若即用前例之 V,則

$$VV_c=(x_1+\omega x_2+\omega^2 x_3)(x_1+\omega x_3+\omega^2 x_2)=\sigma_1^2-3\sigma_2.$$

若施以三文字之六個代換,不生變更.但,在 $\rho\neq c$ 時,函數

$$\phi=(\rho-V)(\rho-V_c)=\rho^2-(x_1+x_2+x_3)\rho+\sigma_1^2-3\sigma_2.$$

若施以 G 外之代換,皆生變更.故當 $\rho\neq 0$ 時,函數 ϕ 屬於 G.

習　題

1. 設 ω 爲 1 之第 μ 次質根 (Primitive μth root), 則

$$(x_1+\omega x_2+\omega^2 x_3+\cdots+\omega^{\mu-1}x_\mu)^\mu$$

屬於循環羣 $\{I, a, a^2, \cdots, a^{\mu-1}\}$, 此處 $a=(x_1x_2\cdots x_\mu)$.

2. 取 $V=x_1+ix_2-x_3-ix_4$ 及 $s=(x_1x_2)(x_3x_4)$,求證 $VV_s\equiv i(x_1-x_3)^2+i(x_2-x_4)^2$ 屬於 §21 之羣 G_8', 而 $V+V_s$ 則屬於 §21 之 H_4; 若 $\rho\neq 0$, 則 $(\rho-V)(\rho-V_s)$ 屬於羣 $\{I, s\}$.

3. 取 $V=x_1+ix_2-x_3-ix_4$ 及 $t=(x_1x_3)(x_2x_4)$, 求證 VV_t 屬於羣 $\{I, t\}$.

4. 設 $a_1, a_2, \cdots, a_n$ 爲不等數,則函數

$$\Gamma = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

爲 $n!$ 個函數,而 $V+V_b+V_c+\cdots+V_l$ 屬於 $\{I, h, c, \cdots l\}$.

5. 設 ϕ 屬於 G, 而 ϕ' 屬於 G', 則必有常數 a 及 a' 使函數 $a\phi+a'\phi'$ 屬於 G 及 G' 之最大公子羣.

§26. 定理 子羣之級必能整除原羣之級.

設羣 G 之級爲 N, 其子羣 H 所含之代換爲

$$h_1=I, h_2, h_3, \cdots h_P \cdots\cdots (29)$$

若 G 不含有(29)以外之代換,則 $N=P$, 而定理之爲眞也明甚.次設 G 含有 H 以外之代換 g_2,則 G 必含次之諸代換.

$$g_2, h_2g_2, h_3g_2, \cdots, h_Pg_2 \cdots\cdots (30)$$

此等代換間無相同者;卽與(29)諸代換亦不相同,此因 $h_\alpha g_2=h_\beta$, 則必須 $g_2=h_\alpha^{-1}h_\beta=H$ 內一代換,卽須與假設發生矛盾也.故由(29)及(30)得 G 之 $2P$ 個不同代換.若 G 之代換盡於此數, $N=2P$,則定理爲眞;倘或不止此數,則 G 必含一新代換 g_3; 於是, G 並含

$$g_3, h_2g_3, h_3g_3, \cdots h_Pg_3 \cdots\cdots (31)$$

與前同理,知(31)內各代換俱不相同,且與(29)諸代換亦不相同.又(31)亦與(30)內諸代換不同,此因 $h_\alpha g_3=h_\beta g_2$, 必須使 $g_3=h_\alpha^{-1}h_\beta g_2$ =(30)內一代換,卽須與假設發生矛盾也.故得 G 之 $3P$ 個不同代換.於是, $N=3P$, 或 G 更含有(29),(30),(31)以外之代換 g_4. 但如 G 含 g_4,則 G 必含

$$g_4, h_2g_4, h_3g_4, \cdots, h_Pg_4 \cdots\cdots (32)$$

等代換.此等代換絕不相同,且與(29),(30),(31)所列各代換亦異;於是,得 G 之 $4P$ 個不同代換.而 $N=4P$, 或不止此數.倣此類推.因 G 之級必爲有盡數(§9),故終必達到最後一組 P 個代換

$$g_\nu, h_2 g_\nu, h_3 g_\nu, \cdots, h_p g_\nu \cdots\cdots (33)$$

於是, $N=\nu P$.

定義　數值 $\nu=\frac{N}{P}$ 稱爲**子羣 H 在羣 G 下之指數** (Index of the subgroup H under G). 其關係以右圖表之.

$$\begin{matrix} G \\ | \\ \nu \\ | \\ H \end{matrix}$$

系　**n 文字之代換羣 H 之級必爲 $n!$ 之除數.**

蓋 H 爲 n 文字所成對稱羣 $G_{n!}^{(\nu)}$ 之子羣也.

§27. 定理　**設 G 爲 N 級羣,則其所含任一代換之週期必能除盡 N.**

設 G 含週期爲 P 之代換 s, 則 G 必含 P 級之循環子羣 H:

$$H=\{s, s^2, \cdots, s^{P-1}, s^P \equiv I\}.$$

故由 §26 知 P 爲 N 之一除數.

系*　**設羣 G 之級 N 爲一素數** (Prime number),**則 G 必爲循環羣,此羣乃週期等 N 之代換及其 $N-1$ 個羃之諸代換所湊成.**

§28. 由 §26 之證,知:羣 G 之 N 個代換,可排成長方整列(Rectangular array),其第一行爲任意子羣 H 內之代換:

$$\begin{matrix} h_1=I & h_2 & h_3 & \cdots & h_p \\ g_2 & h_2 g_2 & h_3 g_2 & \cdots & h_p g_2 \\ g_3 & h_2 g_3 & h_3 g_3 & \cdots & h_p g_3 \end{matrix}$$

---

*此爲次定理之特款 (Special case):

(i) 若一羣之級,可以一素數 p 除盡時,則此羣含有 p 級之子羣 (Cauchy 定理).

(ii) 若一羣之級,最多僅能以素數 p 之 t 羃除盡時,則此羣含有 p^t 級之子羣 (Sylow 定理).

其證明普通羣論中皆有之,茲不具錄.

.....

$$g_\nu \quad h_2 g_\nu \quad h_3 g_\nu \quad \cdots \quad h_p g_\nu$$

此處 $g_1=I, g_2, g_3, \cdots g_\nu$ 稱爲**右邊乘式** (Right-hand multipliers). 其選取之法有種種: g_2 乃 G 內任一代換不含於第一行者, g_3 乃 G 內任一代換, 不含於第一、二兩行者, g_4 乃 G 內任一代換不含於第一、二、三三行者, 其餘可倣此類推之.

同樣, G 之諸代換亦可用**左邊乘式** (Left-hand multipliers) 排成長方整列.

§29. **定理** 設 ψ 爲 $x_1, x_2, \cdots, x_n$ 之有理函數, 屬於子羣 H, 又此子羣 H 對於 G 之指數爲 ν, 則 ψ 對於 G 爲 ν 值函數.

假定 G 之 N 個代換排成如 §28 之長方整列. 倘將此等代換施於 ψ, 則凡在同行上諸代換施於 ψ 時, 必不變此函數之值. 蓋因

$$\psi_{h_i g_\alpha}=(\psi_{h_i})_{g_\alpha}=(\psi)_{g_\alpha}=\psi_{g_\alpha},$$

故此函數最多不過 ν 值. 又設

$$\psi_{g_\alpha}=\psi_{g_\beta},$$

則 $\psi_{g_\alpha g_\beta^{-1}}=\psi$. 於是, $g_\alpha g_\beta^{-1}$ 乃爲使 ψ 不變之一代換 h_i, 故 $g_\alpha=h_i g_\beta$, 此與長方整列之做法發生矛盾, 故 $\psi_{g_\alpha}\neq\psi_{g_\beta}$. 於是, ψ 爲 ν 值函數.

定義 此等 ν 個不等函數 $\psi, \psi_{g_2}, \psi_{g_3}, \cdots, \psi_{g_\nu}$ 稱爲**函數 ψ 在羣 G 下之相配值** (Conjugate values of the function ψ under the group G).

若 G 爲對稱羣 $G_{n!}$, 則得 **Lagrange 定理:**

n 文字之有理函數施以 $n!$ 個代換, 倘所得之值有若干種, 則其種數必可除盡 $n!$.

例 1.　對於 3 文字之對稱羣 G_6，試求函數

$$\Delta\equiv(x_1-x_2)(x_2-x_3)(x_3-x_1),\quad \theta\equiv(x_1+\omega x_2+\omega^2x_3)^3$$

之諸不等相配值.

由 §21 例 1 知，此兩函數屬於子羣 $G_3=\{I,\ a=(x_1x_2x_3),\ b=(x_1x_3x_2)\}$，此羣之長方整列及其相配值爲：

$$\begin{array}{ccc|cc} I, & a=(x_1x_2x_3), & b=(x_1x_3x_2) & \Delta & \theta \\ c=(x_2x_3), & ac=(x_3x_1) & bc=(x_1x_2) & -\Delta & \theta\omega \end{array}$$

例 2.　對於 4 文字之對稱羣 G_{24}，求 $x_1x_2+x_3x_4$ 之相配值.

將 §19 後面習題 4、5、6 之結果，改排爲以 G_8 排於第一行而得之 G_{24} 諸代換之一種長方整列爲：

$$\begin{array}{cccccccc|c} I, & (12), & (34), & (12)(34), & (13)(24), & (14)(23), & (1324), & (1423) & x_1x_2+x_3x_4 \\ (234), & (1342), & (23), & (132), & (143), & (124), & (14), & (1243) & x_1x_3+x_2x_4 \\ (243), & (1432), & (24), & (142), & (123), & (134), & (1234), & (13) & x_1x_4+x_2x_3 \end{array}$$

其右邊函數即爲 $x_1x_2+x_3x_4$ 之相配值.

§30. 定理　施全部 $n!$ 代換於一有理函數 $\phi(x_1,x_2,\cdots,x_n)$，倘得 ρ 個不等之值，則此諸值乃一 ρ 次方程式之根，其係數爲初等對稱函數

$$c_1=x_1+x_2+\cdots+x_n,\ c_2=x_1x_2+x_1x_3+\cdots+x_{n-1}x_n,\ \cdots,$$

$$c_n=x_1x_2\cdots x_n \qquad\cdots\cdots(34)$$

之有理函數.

設 $\phi(x_1,x_2,\cdots x_n)$ 之 ρ 個不等之值爲：

$$\phi_1\equiv\phi,\ \phi_2,\ \phi_3,\ \cdots,\ \phi_\rho \qquad\cdots\cdots(35)$$

則其方程式爲 $(y-\phi)(y-\phi_2)\cdots(y-\phi_\rho)=0$，其係數 $\phi_1+\phi_2+\cdots+\phi_\rho$，$\phi_1\phi_2+\phi_1\phi_3+\cdots+\phi_{\rho-1}\phi_\rho,\cdots,\pm\phi_1\phi_2\cdots\phi_\rho$ 爲 $\phi_1,\phi_2,\cdots,\phi_\rho$ 之對稱函數. 倘吾人能證出此等函數爲 $x_1,x_2,\cdots,x_n$ 之對稱函數，則由附錄

知此等函數亦爲(34)之有理函數矣.茲先證 n 文字 $x_1, x_2, \cdots, x_n$ 之任一代換 s 施於(35),祇互換(35)內之次序.設 s 將(35)內諸函數換爲

$$\phi_1', \phi_2', \phi_3', \cdots, \phi_\rho' \quad \cdots\cdots(36)$$

則:

(i) 各函數 ϕ' 必與(35)內一函數相同.此因在對稱羣內必有一代換 t 使 ϕ_1 變爲 ϕ_i,又代換 s 使 ϕ_i 變爲 ϕ_i'; 於是,代換 ts 使 ϕ_1 變爲 ϕ_i'.故羣中有一代換能使 ϕ_1 變爲 ϕ_i'; 於是, ϕ_i' 必見於(35)內.

(ii)(36)內諸函數不相等.蓋若 $\phi_i' \equiv \phi_j'$, 則當施以代換 s^{-1} 後,得 $\phi_i \equiv \phi_j$, 卽與假設發生矛盾矣.

由是知,對稱羣內任一代換不能使 $\phi_1, \phi_2, \cdots, \phi_\rho$ 之對稱函數改變,故 $\phi_1, \phi_2, \cdots, \phi_\rho$ 之對稱函數同時亦爲 $x_1, x_2, \cdots, x_n$ 之對稱函數.

定義 以(35)爲根之方程式稱爲 ϕ **之豫解式** (Resolvent equation for ϕ).

試與普通三次方程式(§3)及普通四次方程式(§5)之解法比較之.

§31. Lagrange氏定理 **設施於有理函數 $\psi(x_1, x_2, \cdots, x_n)$ 能使其不改變之一切代換,同時亦使有理函數 $\phi(x_1, x_2, \cdots, x_n)$ 不改變,則 ϕ 必爲 ψ 及 $c_1, c_2, \cdots, c_n$ 之有理函數**[§30,(34)].

設函數 ψ 屬於羣

$$H = \{h_1 \equiv I, h_2, h_3, \cdots, h_p\}.$$

又設 ν 爲在對稱羣 $G_{n!}$ 內 H 之指數.茲就以 H 之代換爲第一行而將 $G_{n!}$ 諸代換排爲一長方整列:

$$\begin{array}{c|c|c} I \quad h_2 \quad \cdots \quad h_p & \psi \equiv \psi_1 & \phi \equiv \phi_1 \\ g_2 \quad h_2 g_2 \quad \cdots \quad h_p g_2 & \psi_{g_2} \equiv \psi_2 & \phi_{g_2} \equiv \phi_2 \\ \cdots\cdots\cdots\cdots\cdots & \cdots\cdots & \cdots\cdots \\ g_\nu \quad h_2 g_\nu \quad \cdots \quad h_p g_\nu & \psi_{g_\nu} \equiv \psi_\nu & \phi_{g_\nu} \equiv \phi_\nu \end{array}$$

而考之函數$\psi_1, \psi_2, \cdots, \psi_\nu$之值必互不相同(§29), 但因$\phi$屬於另一羣$G$, 此羣可較$H$爲大, 故$\phi_1, \phi_2, \cdots, \phi_\nu$諸值未必全相異. 次因施$n$文字$x_1, x_2, \cdots, x_n$之任一代換$s$時, 僅變更函數$\psi_1, \psi_2, \cdots, \psi_\nu$之順序(§30). 又代換$s$將$\psi_i$變爲$\psi_j$時, 則亦將$\phi_i$變爲$\phi_j$. 命

$$g(t) \equiv (t-\psi_1)(t-\psi_2)\cdots(t-\psi_\nu),$$

$$\lambda(t) \equiv g(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\cdots+\frac{\phi_\nu}{t-\psi_\nu}\right),$$

則$\lambda(t)$爲t之$\nu-1$次整函數. 因$\lambda(t)$當施以各代換s時不生改變, 故其係數爲$x_1, x_2, \cdots, x_n$之有理對稱函數, 亦卽爲(34)各式之有理函數. 試以

$$\psi_1 \equiv \psi$$

代式中之t, 則得*

$$\lambda(\psi_1)=(\psi_1-\psi_2)(\psi_1-\psi_3)\cdots(\psi_1-\psi_\nu)\cdot\phi_1=g'(\psi_1)\cdot\phi_1,$$

$$\phi=\frac{\lambda(\psi)}{g'(\psi)} \qquad (37)$$

此定理可以便利之記號形式表之:

若 $\begin{matrix} G:\phi \\ | \\ H:\psi \end{matrix}$, 則$\phi=$ **Rat. Fune.** $(\psi; c_1, c_2, \cdots, c_n)$ $[=(\ ; c_1, c_2, \cdots, c_n)$

*(37) 當$c_1, c_2, \cdots, c_n$表不定量時, 能成立. 此因$\psi_1, \psi_2, \cdots, \psi_\nu$在代數上爲不相等, 於是, $g'(\psi)$亦不全等於零也. 但當與$c_1, c_2, \cdots, c_\nu$以特殊數值, 使函數$\psi_1, \psi_2, \cdots, \psi_\nu$之值眞有二個或多個變成相等時, 則$g'(\psi)=0$, 而$\phi$不能爲$\psi; c_1, c_2, \cdots, c_n$之有理函數矣. 在此等情狀之下, 可參看 Lagrange 論文集第3卷, 374—388頁. 又 Serret 代數學(Algèbre)第二卷, 434—441頁. 本書則於下篇論之.

之有理函數].

先令 $H=G$, 次令 $H=I$, 則得次之兩系:

系 1. 設兩有理函數同屬於一羣,則任一函數皆爲他一函數及 $c_1, c_2, \cdots, c_n$ 之有理函數.

系 2. 凡 $x_1, x_2, \cdots, x_n$ 之有理函數必爲任意一 $n!$ 值函數及 $c_1, c_2, \cdots, c_n$ 之有理函數.

例 1. §29, 例 1 內之函數 Δ 及 θ 同屬於羣 $G_3^{(3)}$, 故 Δ 可列爲 θ 之函數. 由 §§2, 3, 得

$$3\sqrt{-3}\,\Delta=(x_1+\omega^2x_2+\omega x_3)^3-(x_1+\omega x_2+\omega^2x_3)^3=\frac{(c_1^2-3c_2)^3}{\theta}-\theta.$$

至於 $\theta\equiv\psi_1^3$ 可列爲 Δ 之函數,可於 §34 見之.

例 2. 函數 $y_1=x_1x_2+x_3x_4$ 屬於羣 G_8, 又 $t\equiv x_1+x_2-x_3-x_4$ 屬於子羣 H_4 (§21), 故 y_1 爲 t 及以 x_1, x_2, x_3, x_4 爲根之方程式係數 a, b, c, d 之函數.由 §5, $y_1=\frac{1}{4}(t^2-a^2+4b)$.

例 3. 函數 $\psi_1\equiv x_1+\omega x_2+\omega^2x_3$ 乃 $3!=6$ 值函數,故每一個 x_1, x_2, x_3 之有理函數,必爲 ψ_1 及 c_1, c_2, c_3 之有理函數.由 §3 之 (11) 式可得 x_1, x_2, x_3 以 ψ_1 之有理函數表之之式.例如:

$$x_1=\frac{1}{3}\left(c_1+\psi_1+\frac{c_1^2-3c_2}{\psi_1}\right).$$

§32. 定理 設 $\nu\left|\begin{matrix}G:\phi\\H:\psi\end{matrix}\right.$, 則 ψ 必適合 (Satisfy) 一個 ν 次方程式, 其係數爲 $\phi, c_1, c_2, \cdots, c_n$ 之有理函數.

照 §29, 試在羣 G 內就 ψ 之 ν 個相配值:

$$\psi, \psi_{g_2}, \psi_{g_3}, \cdots, \psi_{g_\nu}$$

考之.羣 G 內任一代換祇變動此等值之次序,是以其對稱函數必不受影響.故由 Lagrange 定理,知必爲 $\phi, c_1, c_2, \cdots, c_n$ 之有理

函數.於是,方程式

$$(w-\phi)(w-\phi_{g_2})\cdots(w-\phi_{g_\nu})=0$$

之係數必爲 ϕ, $c_1, c_2, \cdots, c_n$ 之有理函數.

第 四 章

由羣之立場論普通方程式

§33. 按前定理,吾人再就既約三次方程式 $y^3+py+q=0$ 之 Cardan 氏解法(§2)而考之.依 Cardan 之法,根 y_1,y_2,y_3 之決定,全賴一組豫解式

$$\xi^2=\frac{q^2}{4}+\frac{p^3}{27},\quad \text{此處 } \xi\equiv\frac{\sqrt{-3}}{18}(y_1-y_2)(y_2-y_3)(y_3-y_1);$$

$$z^3=-\frac{q}{2}+\xi,\quad \text{此處 } z\equiv\frac{1}{3}(y_1+\omega y_2+\omega^2 y_3);$$

$$y_1=z-\frac{p}{3z},\quad y_2=\omega z-\frac{\omega^2 p}{3z},\quad y_3=\omega^2 z-\frac{\omega p}{3z}.$$

由所設方程式,首得屬於 y_1,y_2,y_3 之對稱羣 G_6 之初等對稱函數

$$y_1+y_2+y_3=0,\ y_1y_2+y_2y_3+y_3y_1=p,\ -y_1y_2y_3=q.$$

試解一個二次豫解式,則得屬於 G_6 之子羣 G_3(§21, 例 1)之二值函數(Two-valued function) ξ. 次又解一個三次豫解式,則得屬於 G_3 之子羣 G_1(§21, 例 2)之六值函數 z. 因 y_1,y_2,y_3 分別屬於次之各羣:

$$G_2'=\{I,(y_2y_3)\},\quad G_2''=\{I,(y_1y_3)\},\quad G_2'''=\{I,(y_1y_2)\},$$

而每羣皆含 G_1 亦可直接由§31, 系 2 得來),故 y_1,y_2,y_3 爲 z,p,q 之有理函數.更就羣之立場而言,與方程式之解法,可以次之圖式表之:

$$\begin{array}{cccc} G_6:p,q & & & \\ 2\big| & & & \\ G_3:\xi & G_2':y_1 & G_2'':y_2 & G_2''':y_3 \\ 3\big| & \big| & \big| & \big| \\ G_1:z & G_1:z & G_1:z & G_1:z. \end{array}$$

§34. 同法可得普通三次方程式

$$x^3-c_1x^2+c_2x-c_3=0$$

之解如次:吾人知函數

$$x_1+x_2+x_3=c_1,\ x_1x_2+x_2x_3+x_3x_1=c_2,\ x_1x_2x_3=c_3,$$

屬於文字爲 x_1, x_2, x_3 之對稱羣 G_6;而函數

$$\Delta=(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

則屬於子羣 $G_3=\{I,(x_1x_2x_3),(x_1x_3x_2)\}$. 又由§2, 習題 3, 知 Δ 爲二項豫解式

$$\Delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2$$

之一根.

由§3及§2,關於 $\psi_1=x_1+\omega x_2+\omega^2x_3$, $\psi_4=x_1+\omega^2x_2+\omega x_3$ 有

$$\psi_1^3+\psi_4^3=2c_1^3-9c_1c_2+27c_3,$$

$$\psi_1^3-\psi_4^3=-3\sqrt{-3}(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

$$=-3\sqrt{-3}\Delta.$$

$$\therefore\ \psi_1^3=\frac{1}{2}(2c_1^3-9c_1c_2+27c_3-3\sqrt{-3}\Delta),$$

$$\psi_4^3=\frac{1}{2}(2c_1^3-9c_1c_2+27c_3+3\sqrt{-3}\Delta).$$

故由開立方求得 ψ_1 後,* 得 ψ_4 之值爲(§3)

$$\psi_4=(c_1^2-3c_2)\div\psi_1.$$

又按§3, x_1, x_2, x_3 可以 ψ_1 之有理函數表之如次:

$$x_1=\frac{1}{3}(c_1+\psi_1+\psi_4),\quad x_2=\frac{1}{3}(c_1+\omega^2\psi_1+\omega\psi_4),$$

$$x_3=\frac{1}{3}(c_1+\omega\psi_1+\omega^2\psi_4).$$

§35. §5內所述之普通四次方程式

*別法可參看§48節後之習題4.

$$x^4+ax^3+bx^2+cx+d=0 \quad \cdots\cdots(12)$$

之解法,就羣之立場而言,可以次之圖式表之:

$$G_{24}:a,b,c,d$$
$$G_8: y_1=x_1x_2+x_3x_4,\ t^2=(x_1+x_2-x_3-x_4)^2$$
$$H_4: t, x_1+x_2, x_3+x_4, x_1x_2, x_3x_4$$
$$H_2:x_1-x_2 \qquad H_2':x_3-x_4$$

此處, $H_2=\{I,(x_3x_4)\}$, $H_2'=\{I,(x_1x_2)\}$, 而 G_8 與 H_4 則已見於 §21 中,茲不贅.

§36. 方程式(12)之 Lagrange 氏第二種解法,乃基於直接計算函數 $x_1+x_2-x_3-x_4$ 之值.此函數對於 G_{24} 之六個共軛值爲 $\pm t_1, \pm t_2, \pm t_3$, 此處

$$t_1=x_1+x_2-x_3-x_4,\ t_2=x_1+x_3-x_2-x_4,\ t_3=x_1+x_4-x_2-x_3.$$

故得六次豫解式 $(\tau^2-t_1^2)(\tau^2-t_2^2)(\tau^2-t_3^2)=0$.

由 §5 知 $t_1^2=a^2-4b+4y_1$, $t_2^2=a^2-4b+4y_2$, $t_3^2=a^2-4b+4y_3$.

即用該節之結果,得

$$t_1^2+t_2^2+t_3^2=3a^2-12b+4(y_1+y_2+y_3)=3a^2-8b,$$
$$t_1^2t_2^2+t_2^2t_3^2+t_3^2t_1^2=3(a^2-4b)^2+8(a^2-4b)(y_1+y_2+y_3)+16(y_1y_2+y_2y_3+y_3y_1)$$
$$=3a^4-16a^2b+16b^2+16ac-64d,$$
$$t_1^2t_2^2t_3^2=(a^2-4b)^3+4(a^2-4b)^2(y_1+y_2+y_3)+16(a^2-4b)(y_1y_2+y_2y_3+y_3y_1)+64y_1y_2y_3$$
$$=\{8c+a(a^2-4b)\}^2.$$

故六次豫解式之係數,即完全算出.* 設命 $\tau^2=\sigma$, 則豫解式化爲三次方程式,以 $\sigma_1=t_1^2$, $\sigma_2=t_2^2$, $\sigma_3=t_3^2$ 表其根,得

*試與 §48 後之習題 5 比較.

$$x_1+x_2-x_3-x_4=\sqrt{\sigma_1},\quad x_1+x_3-x_2-x_4=\sqrt{\sigma_2},$$
$$x_1+x_4-x_2-x_3=\sqrt{\sigma_3},\quad x_1+x_2+x_3+x_4=-a.$$

由此,遂得

$$\left.\begin{aligned} x_1&=\frac{1}{4}(-a+\sqrt{\sigma_1}+\sqrt{\sigma_2}+\sqrt{\sigma_3}),\ x_2=\frac{1}{4}(-a+\sqrt{\sigma_1}-\sqrt{\sigma_2}-\sqrt{\sigma_3})\\ x_3&=\frac{1}{4}(-a-\sqrt{\sigma_1}+\sqrt{\sigma_2}-\sqrt{\sigma_3}),\ x_4=\frac{1}{4}(-a-\sqrt{\sigma_1}-\sqrt{\sigma_2}+\sqrt{\sigma_3}) \end{aligned}\right\}\quad(38)$$

式內根數 $\sqrt{\sigma_1}$ 及 $\sqrt{\sigma_2}$ 前之符號可任意選定,至於 $\sqrt{\sigma_3}$ 之符號,則須取其能滿足

$$\sqrt{\sigma_1}\sqrt{\sigma_2}\sqrt{\sigma_3}=t_1t_2t_3=4ab-8c-a^3\quad\cdots\cdots\cdots\cdots\cdots\cdots(39)$$

之關係而後可.蓋因

$$t_1t_2t_3=\pm\{8c+a(a^2-4b)\}$$

之符號,可由假定 $x_1=1$, $x_2=x_3=x_4=0$, 從而 $a=-1$, $b=c=d=0$, $t_1t_2t_3=1$,而決定取負號也.

§37. 用下列方法解四次方程式,頗饒興味;因此解法直接引出一個 24- 值函數 V,且使方程式諸根皆能以 V 之有理函數列出也.

按§5方法,先解一三次方程式及一二次方程式,因得分別決定屬於 G_8 及 H_4 之函數 y_1 及 t 命

$$V=(x_1-x_2)+i(x_3-x_4),$$

則 V 屬於 G_1,而函數 $\psi=V^2$ 屬於 H_4 之子羣

$$G_2=\{I,\ (x_1x_2)(x_3x_4)\}.$$

在 H_4 下 ψ 之第二值 $\psi_1=\{(x_1-x_2)-i(x_3-x_4)\}^2$.故

$$z^2-(\psi+\psi_1)z+\psi\psi_1=0$$

爲 ψ 之豫解式.但

$$\psi\psi_1=\{(x_1-x_2)^2+(x_3-x_4)^2\}^2=\{a^2-2b-2y_1\}^2=\frac{1}{4}\{3a^2-8b-t^2\}^2,$$

$$\psi+\psi_1=2\{(x_1-x_2)^2-(x_3-x_4)^2\}=2(x_1-x_2+x_3-x_4)(x_1-x_2-x_3+x_4)$$
$$=2(4ab-8c-a^3)\div t \text{ [由 (39)]};$$

故當 ψ 及 ψ_1 之值已知時,得

$$V=\sqrt{\psi},\quad V_1=\sqrt{\psi_1}=(x_1-x_2)-i(x_3-x_4),$$
$$V_1=\frac{1}{2}(3a^2-8b-t^2)\div V \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(40)$$

又由函數 t, V, V_1 及 $x_1+x_2+x_3+x_4=-a$, 得

$$\left.\begin{aligned} x_1&=\frac{1}{4}(-a+t+V+V_1), & x_2&=\frac{1}{4}(-a+t-V-V_1),\\ x_3&=\frac{1}{4}(-a-t-iV+iV_1), & x_4&=\frac{1}{4}(-a-t+iV-iV_1). \end{aligned}\right\}\cdots(41)$$

§38. 普通三次方程式及普通四次方程式之解法 (§§34, 37), 其着眼點皆在決定一函數之值;此將要決定之函數,須對於根之每種代換均生改變者,即須屬於么羣 (Identity group) G_1 者. 仿此,對於普通 n 次方程式

$$x^n-c_1x^{n-1}+c_2x^{n-2}-\cdots+(-1)^nc_n=0 \cdots\cdots\cdots\cdots\cdots\cdots(42)$$

若能決定出一個屬於羣 G_1 之函數,例如

$$V=m_1x_1+m_2x_2+\cdots+m_nx_n \text{ (m 之值各不相同)}\cdots\cdots(43)$$

則此方程式即可完全解之,蓋由 §31, x_i 爲 $V, c_1, \cdots, c_n$ 之有理函數故也. 在解三次及四次方程式時,決定如 V 之函數值之圖式爲:

$$\begin{array}{l} G_6: c_1, c_2, c_3 \\ 2\,| \\ G_3: (x_1+\omega x_2+\omega^2 x_3)^3 \\ 3\,| \\ G_1: x_1+\omega x_2+\omega^2 x_3 \end{array} \qquad \begin{array}{l} G_{24}: a, b, c, d \\ 3\,| \\ G_8: x_1x_2+x_3x_4 \\ 2\,| \\ H_4: x_1+x_2-x_3-x_4 \\ 2\,| \\ G_2: (x_1-x_2+ix_3-ix_4)^2 \\ 2\,| \\ G_1: x_1-x_2+ix_3-ix_4. \end{array}$$

同樣,可推之於(42),其解法之圖式爲:

$$\begin{array}{ll} G_{n1}: c_1, c_2, \cdots, c_n & \\ \lambda\downarrow & \\ H: \xi, & \xi^{\lambda}+R_1(c_1, \cdots, c_n)\xi^{\lambda-1}+\cdots=0 \\ \mu\downarrow & \\ K: \eta, & \eta^{\mu}+R_2(\xi, c_1, \cdots, c_n)\eta^{\mu-1}+\cdots=0 \\ \vdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ M: \psi & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \rho\downarrow & \\ G_1: V, & V^{\rho}+R(\psi, c_1, \cdots, c_n)V^{\rho-1}+\cdots=0. \end{array}$$

由 §32 之定理,知此種豫解方程式必存在.但若此等豫解式全爲二項方程式時,則函數 V(於是$x_1, \cdots, x_n$)可由已知量之開方求之,而方程式卽可藉根數解出.惟豫解式如爲二項,則其次數可假定爲素數;蓋方程式之次數若爲非素數,如 $z^{pq}=A$, 則此方程式可以 $z^p=u$, $u^q=A$ 代換之也.到此,吾人要發次之問題:

設 $\nu\begin{matrix} G:\phi \\ \downarrow \\ H:\psi \end{matrix}$, 問如何始能使 ψ 之豫解式之形爲

$$\psi^{\nu}=\text{Rat. Func.}(\phi, c_1, \cdots, c_n) \cdots\cdots(44)$$

乎?吾人前固已說明,ν 可假定其爲素數矣.故 1 之第 ν 次質根 (Primitive root) 必存在,卽謂必有一數 ω 能適合次之性質者:

$$\omega^{\nu}=1, \quad \text{且當 } k<\nu, \text{則 } \omega^{k}\neq 1.$$

於是(44)之根,可書爲

$$\psi, \ \omega\psi, \ \omega^2\psi, \ \cdots, \ \omega^{\nu-1}\psi \cdots\cdots(45)$$

設以 $\phi_1\equiv\phi, \phi_2, \cdots, \phi_\nu$ 表 ϕ 在 G 下之相配函數(其數爲 ν, 參看 §29), 由假設知 ϕ 屬於羣 H,命 ϕ_2 屬於羣 H_2, ϕ_3 屬於 H_3, $\cdots$, ϕ_ν 屬於 H_ν 因(45)諸根相差僅一常數因子,諸根必同屬於一羣,故得所發問題之必需條件爲

$$H=H_2=H_3=\cdots=H_\nu.$$

§39. 設 ψ 屬於羣

$$H=\{h_1\equiv I, h_2, \cdots, h_p\},$$

而 ψ 施以代換 s 則變爲 ψ_s.試問函數 ψ_s 所屬之羣如何決定乎?設代換 σ 使 ψ_s 不變,則 $\psi_{s\sigma}=\psi_s$;於是

$$\psi_{s\sigma s^{-1}}=\psi_{ss^{-1}}=\psi.$$

命 $s\sigma s^{-1}=h$,而 h 表 H 內之一代換,則得

$$\sigma=s^{-1}hs.$$

反之,凡代換之形如 $s^{-1}hs$,皆使 ψ_s 不變;故知 ψ_s 屬於羣

$$\{s^{-1}h_1s=I,\ s^{-1}h_2s, \cdots,\ s^{-1}h_ps\},$$

以 $s^{-1}Hs$ 表之.於是,得次之定理:

設 ψ 屬於子羣 H,而 H 在羣 G 下之指數爲 ν,則 ψ 在 G 下之相配函數

$$\psi,\ \psi_{g_2},\ \cdots,\ \psi_{g_\nu}$$

分別屬於羣

$$H,\ g_2^{-1}Hg_2,\ \cdots,\ g_\nu^{-1}Hg_\nu.$$

定義 羣 $H,\ g_2^{-1}Hg_2,\ \cdots,\ g_\nu^{-1}Hg_\nu$ 稱爲**組成 G 之相配子羣組** (To form a set of conjugate subgroups of G). 若此等羣互相全等於 H,則 H 稱爲**G 之自配子羣** (Self-conjugate subgroup of G), 或稱爲**G 之不變子羣**(Invariant subgroup of G).

故普通 n 次方程式若欲按 §38 之設計,全以根數解之時,其必須條件,乃每次所得之羣須爲前羣之自配子羣,且其指數爲素數者.

因 $g^{-1}Ig=I$,故羣 $G_1=\{I\}$ 爲任何羣 G 之自配羣.

例 1. 設 G 爲 3 文字之對稱羣 G_6,而 H 爲 $G_3=\{I,(1\ 2\ 3),(1\ 3\ 2)\}$. $g_2=(x_2\ 3)$, 則

$$\psi=(x_1+\omega x_2+\omega^2 x_3)^3,\ \psi_{g_2}=(x_1+\omega^2 x_2+\omega x_3)^3$$

成爲在 G 下之相配函數組 (Set of conjugate functions under G). 因互換 x_2 與 x_3，即將 ψ 換爲 ψ_{g_2}，而羣 H 亦換爲 $\{I, (x_1x_3)(x_2x_4), (x_1x_2x_3)\}$，故 ψ_{g_2} 即屬於此羣，而 ψ 屬於 H. 但，按上述普通方法，則用

$$(x_2x_3)^{-1}(x_1x_2x_3)(x_2x_3)=(x_1x_3x_2),\quad (x_2x_3)^{-1}(x_1x_3x_2)(x_2x_3)=(x_1x_2x_3)$$

之運算，以得其結果. 然本例不論用何方法，所得之 ψ 及 ψ_{g_2} 之羣總是全同，故 G_3 在 G_6 下爲自配羣. 又 G_1 在 G_3 下亦爲自配羣，於是普通三次方程式能適合上述之必須條件，故可以根數解之.

例 2. 試在 G_6 下，就 x_1 之相配值 x_1, x_2, x_3 而考之.

$$\begin{array}{lll} & (x_2x_3) & \Big| x_1 \\ g_2=(x_1x_2), & (x_2x_3)g_2=(x_1x_2x_3) & \Big| x_2 \\ g_3=(x_1x_3), & (x_2x_3)g_3=(x_1x_3x_2) & \Big| x_3 \end{array}$$

因 $$g_2^{-1}Hg_2=\{I, (x_1x_3)\}\neq H,\quad g_3^{-1}Hg_3=\{I, (x_1x_2)\}\neq H,$$

故 $H=\{I, (x_2x_3)\}$ 在 G_6 下不爲自配羣.

§20. 定義 設 a 及 a' 爲羣 G 內之兩代換，若 G 內有一代換 g 能使 $g^{-1}ag=a'$ 時，則 a 及 a' 稱爲**在 G 下之相配代換**(Conjugate substitutions under G)；而 a' 稱爲 **a 就 g 之變換** (The transform of a by g).

茲今述一不必實施乘法以求代換 $g^{-1}ag$ 之簡法：先就 a 爲一循環代換，例如 $a=(\alpha\beta\gamma\delta)$，而言命 g 爲任意代換，如

$$g=\begin{pmatrix}\alpha & \beta & \gamma & \delta & \cdots & \lambda\\ \alpha' & \beta' & \gamma' & \delta' & \cdots & \lambda'\end{pmatrix}.$$

則有 $$g^{-1}=\begin{pmatrix}\alpha' & \beta' & \gamma' & \delta' & \cdots & \lambda'\\ \alpha & \beta & \gamma & \delta & \cdots & \lambda\end{pmatrix},\quad g^{-1}ag=\begin{pmatrix}\alpha' & \beta' & \gamma' & \delta' & \varepsilon' & \cdots & \lambda'\\ \beta' & \gamma' & \delta' & \alpha' & \varepsilon' & \cdots & \lambda'\end{pmatrix}.$$

故 $g^{-1}ag=(\alpha'\beta'\gamma'\delta')$，可從施代換 g 於循環代換 $a=(\alpha\beta\gamma\delta)$ 得之.

次設 $a=a_1a_2a_3\cdots$，此處 $a_1, a_2, a_3, \cdots$ 各表循環代換，則

$$g^{-1}ag=g^{-1}a_1g\cdot g^{-1}a_2g\cdot g^{-1}a_3g\cdots.$$

故 $g^{-1}ag$ 可於 a 之循環代換內施以 g 之代換得之.

例如 $(123)^{-1}\cdot(12)(34)\cdot(123)=(23)(14)$.

系 因任一代換皆將偶代換仍變爲偶代換,故交錯羣 $G_{\frac{1}{2}n!}$ 爲對稱羣 $G_{n!}$ 之自配子羣.

§41. 定理 次列各四文字之羣

$$G_{24},\ G_{12},\ G_4=\{I,\ (12)(34),\ (13)(24),\ (14)(23)\},$$

$$G_2=\{I,\ (12)(34)\},\quad G_1=\{I\}$$

中,每羣皆爲前一羣之自配子羣.

由 §40 之系,知在 G_{24} 下 G_{12} 爲其自配子羣.又因 G_4 含 $(\alpha\beta)(\gamma\delta)$ 形之一切代換;而四文字之任一代換,仍將此種形狀之代換變爲同形之代換 $(\alpha'\beta')(\gamma'\delta')$. 故在 G_{12} 下(又在 G_{24} 下), G_4 爲自配子羣.又以代換 $(12)(34),(13)(24),(14)(23)$ 仍將 $(12)(34)$ 變換爲 $(12)(34)$;* 故在 G_4 下, G_2 爲自配子羣.

§42. 由前定理知普通四次方程式

$$x^4+ax^3+bx^2+cx+d=0$$

可以根數解之,因其能適合 §39 所述之必須條件也.欲求 24- 值函數

$$V=x_1-x_2+ix_3-ix_4$$

之值,必須決定次數爲素數之一組二次豫解式之連索,俾使求得 V 後,而方程式之根 x_1,x_2,x_3,x_4 可以 V 之有理函數表之.仿 §4,設命

$$y_1=x_1x_2+x_3x_4,\ y_2=x_1x_3+x_2x_4,\ y_3=x_1x_4+x_2x_3\cdots\cdots(20)$$

則解法之圖式應爲

*此亦可由 §21 例(f)見之,因 $rs=sr$, 故得 $s^{-1}rs=r$ 也.

$$\begin{array}{l} G_{24}: a, b, c, d \\ 2\downarrow \\ G_{12}: \Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4) \\ 3\downarrow \\ G_4: \phi_1=y_1+\omega y_2+\omega^2 y_3 \\ 2\downarrow \\ G_2: \lambda=\phi_1\div(x_1+x_2-x_3-x_4) \\ 2\downarrow \\ G_1: V=x_1-x_2+ix_3-ix_4. \end{array}$$

引用 §7 之 (22), (23), (24) 諸公式,並命 $P=-4I, Q=16J$, 則得

$$\Delta=16\sqrt{I^3-27J^2},$$

$$I\equiv d-\frac{ac}{4}+\frac{b^2}{12},\quad J\equiv\frac{bd}{6}-\frac{c^2}{16}-\frac{a^2d}{16}+\frac{abc}{48}-\frac{b^3}{216}.$$

故 Δ 爲二項豫解式 $\Delta^2=256(I^3-27J^2)$ 之一根.至於 ϕ_1 之豫解式乃爲二項方程式

$$(\phi-\phi_1)(\phi-\omega\phi_1)(\phi-\omega^2\phi_1)\equiv\phi^3-\phi_1{}^3=0.$$

由 Lagrange 氏定理,知 $\phi_1{}^3$ 爲 Δ, a, b, c, d 之有理函數;故欲決定此函數,可令 $\phi_2=y_1+\omega^2y_2+\omega y_3$. 於是 (§§2, 7),

$$\phi_2{}^3-\phi_1{}^3=3\sqrt{-3}(y_1-y_2)(y_2-y_3)(y_3-y_1)=-3\sqrt{-3\Delta},$$

$$\phi_2{}^3+\phi_1{}^3=2(y_1{}^3+y_2{}^3+y_3{}^3)+12y_1y_2y_3+3(\omega+\omega^2)\delta,$$

此處 $\delta\equiv y_1{}^2y_2+y_1y_2{}^2+y_1{}^2y_3+y_1y_3{}^2+y_2{}^2y_3+y_2y_3{}^2$ 適合

$$(y_1+y_2+y_3)(y_1y_2+y_2y_3+y_3y_1)=\delta+3y_1y_2y_3,$$

$$(y_1+y_2+y_3)^3=3\delta+6y_1y_2y_3+y_1{}^3+y_2{}^3+y_3{}^3$$

之關係;故應用 §5,得

$$\begin{aligned}\phi_2{}^3+\phi_1{}^3&=2(y_1+y_2+y_3)^3-9(y_1+y_2+y_3)(y_1y_2+y_2y_3+y_3y_1)\\&\quad+27y_1y_2y_3\\&=2b^3-9b(ac-4d)+27(c^2+a^2d-4bd)=-432J.\end{aligned}$$

由此遂得 ϕ_1 之豫解式爲

$$\phi_1{}^3=\frac{1}{2}3\sqrt{-3\Delta}-216J.$$

又由 Lagrange 氏定理,知 y_1, y_2 及 y_3 爲 ϕ_1 之有理函數.且因

$$\begin{aligned}\phi_1\phi_2 &= y_1^2+y_2^2+y_3^2+(\omega+\omega^2)(y_1y_2+y_2y_3+y_3y_1)\\ &=(y_1+y_2+y_3)^2-3(y_1y_2+y_2y_3+y_3y_1)\\ &=b^2-3ac+12d\equiv H,\end{aligned}$$

及由

$$y_1+y_2+y_3=b,\ y_1+\omega y_2+\omega^2y_3=\phi_1,\ y_1+\omega^2y_2+\omega y_3=\frac{H}{\phi_1}$$

等關係,遂得

$$y_1=\frac{1}{3}\left(b+\phi_1+\frac{H}{\phi_1}\right),\ y_2=\frac{1}{3}\left(b+\omega^2\phi_1+\frac{\omega H}{\phi_1}\right),$$

$$y_3=\frac{1}{3}\left(b+\omega\phi_1+\frac{\omega^2H}{\phi_1}\right).$$

命 $t\equiv x_1+x_2-x_3-x_4$, 並引用§5內 t^2 之值,卽得 $\lambda=\phi_1/t$ 之二項豫解式

$$\lambda^2=\phi_1^2\div(a^2-4b+4y_1).$$

又以(§37)

$$\begin{aligned}V^2 &= (x_1-x_2)^2-(x_3-x_4)^2+2i(x_1-x_2)(x_3-x_4)\\ &=\frac{4ab-8c-a^3}{t}+2i(y_2-y_3)\\ &=\frac{\lambda}{\phi_1}(4ab-8c-a^3)+\frac{2}{3}\sqrt{3}\left(\phi_1-\frac{H}{\phi_1}\right),\end{aligned}$$

故 x_1, x_2, x_3, x_4 之值,可由(40)與(41)合而求之.

n 文字對稱羣之子羣系之討論

§43. 定義 設一羣 G 有一**最大自配子羣** (Maximal self-conjugate subgroup) H——H 爲 G 之最大自配子羣云者,卽謂 H 爲 G 之自配子羣之一,且 G 無有更大自配子羣能含 H 者——又設 H 有

一最大自配子羣 K. 仿此類推,便得一個羣系(Series of groups)

$$G,\ H,\ K,\ \cdots,\ M,\ G_1,$$

其中每羣皆爲前羣之最大自配子羣,而殿以么羣 G_1. 此羣系稱爲 **G之子羣系** (Series of composition of G). 數值如 λ (H在G下之指數), μ (K在H下之指數), $\cdots$, ρ (G_1在M下之指數) 稱爲 **G之子羣系因子** (Factors of composition of G).

若此系僅由 G 及 G_1 組成,則羣 G 稱爲**簡單羣** (Simple group). 故簡單羣乃除自身及么羣外,別無含其他自配子羣之羣也. 反之,若一羣不爲簡單羣,則此羣稱爲**合組羣** (Composite group).

例 1. 就 3 文字之對稱羣而言,其子羣系爲 G_6, G_3, G_1(參看§39, 例 1). 因指數 2, 3 爲素數,故此等自配子羣皆爲最大自配子羣(參看§26).

例 2. 就 4 文字之對稱羣而言,其子羣系爲 G_{24}, G_{12}, G_4, G_2, G_1 (§41),其指數皆爲素數.

例 3. 級數爲素數之循環羣必爲簡單羣 (§26).

§44. 引 (Lemma) **設一 n 文字之羣,含有由 n 文字內所成之一切 3 文字循環代換時,則此羣必爲對稱羣 G_n, 或交錯羣 $G_{\frac{1}{2}n!}$.**

欲證此引,即須證:凡偶代換 s 可以 3 文字之循環代換之積表之. 設

$$s=t_1t_2\cdots t_{2\nu-1}t_{2\nu},$$

而 $t_1, t_2, \cdots, t_{2\nu}$ 各爲一易位 (§§22, 23). 又設 $t_1\neq t_2$. 若 t_1 與 t_2 有一公共文字,則

$$t_1t_2=(\alpha\beta)(\alpha\gamma)=(\alpha\beta\gamma).$$

但若 t_1 及 t_2 無公共文字,則

$$t_1t_2=(\alpha\beta)(\gamma\delta)=(\alpha\beta)(\alpha\gamma)(\gamma\alpha)(\gamma\delta)=(\alpha\beta\gamma)(\gamma\alpha\delta)$$

同樣，t_3t_4 或爲么代換，或等於一個 3 文字循環代換，或等於兩個 3 文字循環代換之積.

故此羣含有一切 n 文字之偶代換，卽此羣必爲對稱羣或交錯羣.

§45. 定理 $n>4$ 文字之交錯羣，必爲簡單羣.

設 $G_{\frac{1}{2}n!}$ 有一較么羣 G_1 爲大之自配子羣 H，而在 H 內，除么代換 I 外之諸代換中，茲就其影響最少數文字之代換而考之. 此等每一代換內所含之各循環代換，其內之文字之數必相等；否則，此代換之某乘冪，既不爲 I，而其所影響文字之數，將較原代換爲少矣. 又此等代換內之任一循環代換所含文字，必無多於 3 者，此因 H 若含

$$s=(1234\lambda\cdots\rho)(\cdots)\cdots,$$

則 H 必含有就偶代換 $\sigma=(234)$ 之變換：

$$s_1=\sigma^{-1}s\sigma=(1342\lambda\cdots\rho)(\cdots)\cdots,$$

上兩式內之點乃表明全相同之文字也. 於是，H 必含有

$$ss_1^{-1}=(142)$$

之代換，其所影響之文字將較少於 s，而與假定發生抵觸矣. 故知一代換內之諸循環代換，無一含多於 3 文字者. 又上述之代換，每個僅由一循環代換構成. 蓋若 H 含 t 或 s，而

$$t=(12)(34)\cdots,\quad s=(123)(456)\cdots,$$

則 H 必含有 t 或 s 就偶代換 $\kappa=(125)$ 之變換，因而 H 必含代換 $t\cdot\kappa^{-1}t\kappa$ 或 $s^{-1}\cdot\kappa^{-1}s\kappa$. 但後者之代換使數字 4 不變，而其所含之字無有不含於 s 內者；而前者則使 3 及 4 不變，其所含之字，僅有一文字 5 不含於 t 內. 然此兩種變換，總是減少其所含之文字，與前設矛盾；故 H 所含之代換，每個非僅爲一循環代換不可.

凡代換除 I 外，含最少數文字者，其形不外爲 (ab) 或 (abc)

二種中之一但因 (ab) 爲奇代換,理當摒棄外,H 所含之代換必爲 (abc) 之形設 α,β,γ 爲 n 文字內之任意三文字,而 $\delta,\varepsilon,\cdots,\nu$ 爲其餘之文字,則 (abc) 可由代換

$$r=\begin{pmatrix} a & b & c & d & e & \cdots & n \\ \alpha & \beta & \gamma & \delta & \varepsilon & \cdots & \nu \end{pmatrix},\quad s=\begin{pmatrix} a & b & c & d & e & \cdots & n \\ \alpha & \beta & \gamma & \varepsilon & \delta & \cdots & \nu \end{pmatrix}$$

變換爲 $(\alpha\beta\gamma)$,此處在 r 內之點,與 s 內之點表同樣文字.因 $r=s(\delta\varepsilon)$,故代換 r 或 s 之一必爲偶代換而屬於 $G_{\frac{1}{2}n!}$.是以,在 $n>4$ 時,H 含 n 文字內一切 3 文字之循環代換;故 $H=G$.

§46. 定理　$n>4$ 文字之對稱羣,除自身,么羣 G_1 及交錯羣 $G_{\frac{1}{2}n!}$ 外,不含有其他自配子羣;故交錯羣爲 $G_{n!}$ $(n>4)$ 之唯一最大自配子羣.

交錯羣爲對稱羣之自配子羣,業於 §40 內證明矣.

今設 $G_{n!}$ 有一自配子羣 H,含有么代換 I 以外之一代換

先設 s 含有多於兩文字之循環代換如

$$s=(abc\cdots d)(ef\cdots)\cdots$$

者.令 α,β,δ 爲 n 文字內之任意三文字,而 $\gamma,\varepsilon,\cdots,\phi$ 爲其餘 $n-3$ 文字,則 H 必含有代換

$$s_1=(\alpha\beta\gamma\cdots\delta)(\varepsilon\phi\cdots)\cdots,\qquad s_2=(\beta\alpha\gamma\cdots\delta)(\varepsilon\phi\cdots)\cdots$$

(上式 s_1 內用點處與 s_2 內用點處所代之文字,完全同樣.) 此因

$$\sigma=\begin{pmatrix} a & b & c & \cdots & d & e & f & \cdots \\ \alpha & \beta & \gamma & \cdots & \delta & \varepsilon & \phi & \cdots \end{pmatrix}$$

爲一 n 文字之代換將 s 變換爲 s_1 者(§40).然 $G_{n!}$ 之任一代換 σ,將其自配子羣 H 內之一代換 s 仍變換爲該子羣之他一代換(§39),故 s_1 必屬於 H;同樣,s_2 亦屬於 H.今因 H 成一羣,故必含

有積 $s_2 s_1^{-1}=(\alpha\beta\delta)$. 於是, H 含有從 n 文字內任意選來 3 文字之循環代換;故 H 必爲 $G_{n!}$ 或 $G_{\frac{1}{2}n!}$ (§44).

次設 s 僅含易位,且至少亦含有兩個易位者.若

$$s=(ab)(ac)\cdots=(abc)\cdots,$$

則此場合已論列於前,此不復贅.故設

$$s=(ab)(cd)(ef)\cdots(lm).$$

命 $\alpha,\beta,\gamma,\delta$ 爲 n 文字內之任四個文字,而 $\varepsilon,\phi,\cdots,\lambda,\mu$ 爲其餘文字,則自配子羣 H 含有代換

$$s_1=(\alpha\beta)(\gamma\delta)(\varepsilon\phi)\cdots(\lambda\mu),\quad s_2=(\alpha\gamma)(\beta\delta)(\varepsilon\phi)\cdots(\lambda\mu);$$

於是,亦含代換 $s_2 s_1^{-1}=(\alpha\delta)(\beta\gamma)$. 因 $n>4$, 故在 $\alpha,\beta,\gamma,\delta$ 外,必更有他文字 ρ. 於是, H 含有代換 $(\alpha\rho)(\beta\gamma)$ 及積

$$(\alpha\delta)(\beta\gamma)\cdot(\alpha\rho)(\beta\gamma)=(\alpha\delta\rho).$$

由是,依前理知 H 必爲 $G_{n!}$ 或 $G_{\frac{1}{2}n!}$.

最後設 $s=(ab)$, 則自配子羣 H 含一切易位,故 $H=G_{n!}$.

綜上各段之研究,可知當 $n>4$ 時, $G_{\frac{1}{2}n!}$ 爲 $G_{n!}$ 之唯一自配子羣,故亦爲其最大自配子羣;又由前節知 $G_{\frac{1}{2}n!}$ 爲簡單羣,故本節定理完全證實.

§47. 由前兩定理知,**當 $n>4$ 時, n 文字之對稱羣僅能有一組子羣系 $G_{n!}, G_{\frac{1}{2}n!}, G_1$.** 但,此定理當 $n=3$ 時仍成立,此因 G_6 之第 3 級子羣只有 G_3 一個,而其他三個第 2 級子羣,皆非自配子羣也 (§39, 例 2). 至於 $n=4$, 則得例外場合;蓋因 G_{12} 含有自配子羣 G_4 也 (§41). 以上討論之結果,吾人可綜述之如次:

除 $n=4$ 外,凡 n 文字對稱羣之子羣系因子皆爲 2 及 $\left(\frac{1}{2}n\right)!$.

§48. 在 §38 內,曾提出:「欲以一組次數爲素數之二項豫解式

解普通 n 次方程式,其每個豫解式之根,且可由該普通方程式之根 $x_1, x_2, \cdots, x_n$ 之有理函數列出之」之計畫.又在 §§38—39 內證出實現此計畫之必需條件爲:$G_{n!}$ 所含之羣系

$$G_{n!},\ H, K, \cdots, M, G_1 \quad \cdots\cdots (46)$$

內之每一羣,要使其皆爲前一羣之自配子羣而指數爲素數者.倘按 §43 之說法而言,則此條件乃要 $G_{n!}$ 有一子羣系(46),其子羣系因子全爲素數者.但,按 §47,知 $n \geqq 5$ 時,$\left(\frac{1}{2}n\right)!$ 非爲素數,不能滿足上述之條件;而在 $n=3$ 或 $n=4$ 時則能適合(§39,例 1; §41).故按預定之計畫,知普通 $n > 4$ 次之方程式,不能以根數解之.但,普通三次方程式及普通四次方程式則不然,得以根數解之(§§34, 42).

欲得普通 $n>4$ 次方程式不能以根數解之之完全證明,除上面之證明外,更須證上之計畫爲要求以根數解方程式之唯一可能辦法.此項證明* 乃由 Abel 氏於 1826 年證次之定理而完成[Œuvres d' Abel (Abel 論文集)第一冊,第 66 頁]:

凡得用根數解之之方程式,必可化爲一組次數爲素數之二項方程式,且其根乃爲所設方程式之根之有理函數者.

以現在之立場,欲直接證明此定理,較爲繁長.茲因留於下篇(§94)就較廣汎之 Galois 氏理論立場而證之.

習　題

1. 證 $H=\{I, k_2, \cdots, k_p\}$ 爲 G 之子羣,且其指數爲 2 時,則 H 爲 G 之自配子羣.

*Wantzel 氏之簡單證法,可參看 Serret 氏代數學第二冊,其在第四版或第五版之頁數爲 512.

提示: G 之代換,其不含於 H 內者,可書爲 g, gh_2, ..., gh_p; 或 g, h_2g, ..., h_pg. 故凡每一個 $h_\beta g$ 必與某一個 gh_α 相同;於是,凡對於每一個 h_β,必有 h_α 與 g 與某一個 h_α 相同.

2. §21 之羣 G_8 有自配子羣 G_2, G_4, H_4, $C_4=\{I,(1324),(12)(34),(1423)\}$. 其餘之自配子羣祇有 G_8 及 G_1.

3. 設一羣含有 $m+2$ 文字之一切循環代換,則此羣亦必含 m 文字之一切循環代換.

提示: $(123\cdots m\ \overline{m+1}\ \overline{m+2})^2(m\ \overline{m-1}\cdots 23\ \overline{m+2}\ 1\ \overline{m+1})=(123\cdots\overline{m-1}\,m)$.

4. 求直接算出 §34 之函數 $\psi_1{}^3$.

提示: $\psi_1{}^3=x_1{}^3+x_2{}^3+x_3{}^3+6x_1x_2x_3+3\omega(x_1{}^2x_2+x_1x_2{}^2+x_2{}^2x_3+x_2x_3{}^2+x_3{}^2x_1+x_3x_1{}^2)$

$$+3\omega^2(x_1x_2{}^2+x_1{}^2x_3+x_2x_3{}^2+x_2{}^2x_1+x_3x_1{}^2+x_3{}^2x_2)$$

$$=x_1{}^3+x_2{}^3+x_3{}^3+6x_1x_2x_3-\frac{3}{2}(x_1{}^2x_2+x_1x_2{}^2+x_1{}^2x_3+x_1x_3{}^2+x_2{}^2x_3+x_2x_3{}^2)-\frac{3}{2}\sqrt{-3}\,\Delta$$

右邊之前兩節等於 $2c_1{}^3-9c_1c_2+27c_3$ 之半 (§3), 而後一部則係因

$$x_1{}^2x_2-x_1x_2{}^2+x_1x_3{}^2-x_1{}^2x_3+x_2{}^2x_3-x_2x_3{}^2=-(x_1-x_2)(x_2-x_3)(x_3-x_1)=-\Delta$$

得之.

5. 求直接算出 §36 內之係數.

提示: $t_1{}^2+t_2{}^2+t_3{}^2=3\Sigma x_i{}^2-2\Sigma x_ix_j=3a^2-8b$,

$$t_1t_2t_3=\Sigma x_1{}^3+2\Sigma x_1x_2x_3-\Sigma x_1(x_2{}^2+x_3{}^2+x_4{}^2)$$

$$=2\Sigma x_1{}^3+2\Sigma x_1x_2x_3-\Sigma x_i\Sigma x_i{}^2$$

$$=4ab-8c-a^3.$$

下 篇

Galois 氏代數方程式論

第 五 章

Galois 氏理論之代數的引言

§49. Lagrange 氏理論與 Galois 氏理論間之差異 以上各節,皆就 Lagrange 氏理論以討論普通 n 次方程式(其係數俱爲獨立變數,因之,其根 $x_1, x_2, \cdots, x_n$ 亦爲獨立量);在此種情況之下,兩個根之有理函數,祇有在 $x_1, x_2, \cdots, x_n$ 以一切值代入而皆全相等時,始得稱此兩函數爲相等.

但,對於根爲一定常數 (Definite constant) 之方程式則不然;兩個根之有理函數,祇要其數值相等,此兩函數卽可認爲相等.然,此時之兩函數其數值雖同,而形狀則不一致.

例如, $x^3+x^2+x+1=0$ 之根爲

$$x_1=-1,\ x_2=+i,\ x_3=-i\ (i\equiv\sqrt{-1}).$$

此時,函數 x_2^2, x_3^2 及 x_1 之形式雖相異,而其值則同.然因 $x_3^2\neq x_1^2$,故吾人此時不可施代換 $(x_1x_2x_3)$ 於方程式 $x_2^2=x_3^2$. 又根之代換能使函數 x_2^2 之值不變者爲 $I, (x_1x_3), (x_2x_3), (x_1x_2x_3)$,不能組成一羣.

再就 $x^4+1=0$ 而言,其根爲

$$x_1=\varepsilon,\ x_2=i\varepsilon,\ x_3=-\varepsilon,\ x_4=-i\varepsilon\ \left(\varepsilon\equiv\frac{1+i}{\sqrt{2}}\right).$$

故 $x_1^2=\varepsilon^2=i$, $x_2x_4=\varepsilon^2=i$. 函數 x_1^2 及 x_2x_4 形狀不相同,但其數

值相等.又x_1^2之值等於x_3^2,而不等於x_2^2及x_4^2.代換使x_1^2之數值不變者爲 I, (23), (24), (34), (234), (243), (13), (13)(24), (213), (413), (4213), (4132) 等12個,前6個保留x_1^2之形狀不變,後6個則將x_1^2換爲x_3^2.但,此等代換亦不能成一羣,此可由(13)及(23)兩代換之積(13)(23)不含於上列代換組內見之.

由是知從普通方程式之理論轉移爲特殊方程式之理論時,即發生重要困難,而打破之者,則爲 Galois 氏.*

欲改造已往之理論,對於方程式

$$x^n - c_1 x^{n-1} + c_2 x^{n-2} - \cdots + (-1)^n c_n = 0 \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

係數之性質,必須予以特殊之注意;此時,式內各係數 c_1, c_2, …, c_n 爲一定常數,或獨立變數,或其他變數之有理函數皆可.在 Galois 氏理論內,凡導入一新常數,則對此常數之性質即須特加注意.但在 Lagrange 氏理論則不然,1之方根與其他常數之使用,並無予以特殊考慮之必要.

§50. 有理性數統 欲精細說明所設問題之解 (Solution) 之意義,必須將此解內允許包含之諸量之性質述出.例如,吾人要實數或正數之解答;及在初等幾何作圖上,吾人容許任意正數之平方根,而不能容許高次根等.是.在研究一所設方程式,凡在係數內所含之各無理數,於解內自然容許其包含.例如,方程式 $x^2+(2-5\sqrt{3})x+2=0$ 內之 $\sqrt{3}$ 是.但,吾人於係數內原含之無

*Évariste Galois 於 1832 年因決鬥身死,年僅 21 歲耳.氏之主要論文,以缺乏嚴格證明,致遭法國學院之退回.當決鬥之前夕,氏將載有許多定理而不列證明之著作之詳細說明,交付與其友 Auguste Chevalier.後此 15 年,此包括 Galois 氏全部著作之 60 頁文字,始見於法國算學輯報 (Journal de mathématiques) (1846), 復見於 Galois 氏算學論文集 (Œuvres mathématiques D'ÉVARISTE GALOIS). 此書以 1897 年刊於巴黎,並有 Émile Picard 教授爲之序.

理數以外,預定參加他種之無理數,亦所許可.

在一所設問題內,有涉及某種常數或變數

$$R',\ R'',\ \cdots,\ R^{(\mu)} \qquad \cdots\cdots(2)$$

以及由此等數施以有限回之加,減,乘,除(除數假定不等零)等運算而得之一切量時,此等量之全系,稱爲$(R', R'', \cdots, R^{(\mu)})$之**有理性數統***(Domain of rationality).

例 1. 有理數之全體,成一數統.任一個數統R均含有此數統.蓋若ω爲R之任一不等零之元(Element),則$\omega \div \omega = 1$屬於R;又將1施以加減,即得一切整數;由此,倘再施以除法,則得一切分數.故一切有理數屬於R內.

例 2. 設$i = \sqrt{-1}$,而a及b可取一切有理值時,則$a+bi$形之數成一數統(i).但若a及b僅許取整數值,則$a+bi$形之數不能成一數統.

定義 設一方程式其係數可以量$R', R'', \cdots, R^{(\mu)}$之有理函數表之,且此函數各項係數俱爲整數者,又設此方程式之根,可由$R', R'', \cdots$諸量施以有限回之加,減,乘,除及某一個†任意次開方根導出者,此方程式稱爲**對於其數統可以代數解之**(To be algebraically solvable with respect to their domain),或謂**可以根數解之**(To be solvable by radicals).

§51. 在Galois氏理論上,**有理函數**(Rational function)一名詞僅能於與有理性數統R相關聯處用之.對於數統R而言,量$u, v, w, \cdots$之整有理函數,乃指如

---

*有理性數統一名,各家另有種種之稱謂; Kronecker氏呼之爲Rationalitätsbereich, Weber氏呼之爲Körper, Moore氏呼之爲Field(按前者亦'有理性數統'之義,後兩者乃'體'之義.——譯者).

†若吾人容納全部第p次開方根,則吾人必將容納全部1之第p次根之智識.然此在Galois氏理論上,固不見得容許也(參看§89之系).

$$\sum_{i,j,k,\cdots} C_{ijk\cdots} u^i v^j w^k \cdots \quad \cdots\cdots\cdots\cdots\cdots\cdots (3)$$

形之式,其內 $i, j, k, \cdots$ 表正整數,而係數 $C_{ijk\cdots}$ 爲屬於 R 之量. 兩個如(3)之函數之商,卽爲**就數統 R 之有理函數**(Rational function for domain R).

例如 $3u+\sqrt{2}$ 就數統$(\sqrt{2})$爲 u 之有理函數.但,就有理數數統(Domain of rational numbers)(1)而言,則非有理函數.

§52. 等式 (Equality) §49 內已述及兩個僅含常數之式,如其數值相等,則兩式卽謂爲**相等**(Equal).今試就兩個有理函數

$$\phi(u, v, w, \cdots), \quad \psi(u, v, w, \cdots).$$

[其係數爲數統 $R=(R', R'', \cdots, R^{(\nu)})$ 內之數]而考之.若 $R', R'', \cdots$ 全爲常數,且對於 $u, v, w, \cdots$ 所能取之各組數值 $u_1, v_1, w_1, \cdots$,函數 ϕ 及 ψ 之數值皆相等時,則吾人謂 ϕ **及** ψ **相等**.若 $R', R'', \cdots, R^{(\mu)}$ 又爲某獨立變數 $r', r'', \cdots, r^{(m)}$ 之函數,且對於 $u, v, w, \cdots, r', r'', \cdots, r^{(m)}$ 所能取之各組數值,函數 ϕ 及 ψ 之數值皆相等時,則吾人亦謂 ϕ **及** ψ **相等**.倘不能適合上述之相等意義,則謂 ϕ **及** ψ **不等**(Distinct 或 Different).

舉例言之,設 u 及 v 爲 $w^2+2\rho v+1=0$ 之根,則函數 $u+v$ 及 $-2\rho uv$ 對於數統 (ρ) 爲有理函數;而此兩函數,按上列定義,其值相等.

定義 設就 $x_1, x_2, \cdots, x_n$ 之代換 s,施於有理函數 $\phi(x_1, \cdots, x_n)$ 而得新函數 $\phi_s(x_1, \cdots, x_n)$. 若此函數與 ϕ(按本節所述相等定義)相等時,則吾人謂代換 s **使函數** ϕ **不變** (Unalter),亦常謂 s **使** ϕ **之數值上**(Numerically)依然不變.反之,按 Lagrange 氏理論,若 $x_1, x_2, \cdots, x_n$ 爲獨立變數,而函數 ϕ_s 與 ϕ 不論 $x_1, x_2, \cdots, x_n$ 之值如何,總是全相等時,則謂 s **使** ϕ **之形式上**(Formally)依然不變.其例可參看§49.

§53. 上之定義,乃將用於 Lagrange 氏理論內之定義,取而擴充之.從前之普通 n 次方程式 (General equation of degree n), 可視爲方程式(1)極端之例,其係數 $c_1, c_2, \cdots, c_n$ 在數統 $(R', R'', \cdots, R^{(\nu)})$ 內爲有理函數者.蓋因方程式之各係數爲屬於數統 $(R', R'', \cdots, R^{(\nu)})$ 內之獨立變數,故可取以代換數統內之 n 個元 $R', R'', \cdots$.於是,普通方程式化爲

$$x^n + R'x^{n-1} + R''x^{n-2} + \cdots + R^{(n)} = 0$$

之形;因其根亦爲獨立變數(參看附錄),是以根之兩個有理函數,祇有全相等時,才能互相等.

§54. 可約性及不可約性 (Reducibility and irreducibility) 設整有理函數 $F(x)$, 其係數屬於數統 R,且可分解爲低次之整有理因子,而其係數亦屬於 R 時,則吾人謂 $F(x)$ **爲在 R 內可約** (Reducible in R) 之函數.反之,若 $F(x)$ 不能如上分解時,則吾人謂 $F(x)$ **爲在 R 內不可約** (Irreducible in R) 之函數.*

例 1. 因 x^2+1 之因子 $x+i$ 及 $x-i$ 在 (i) 內爲有理函數;故 x^2+1 爲在數統 (i) 內可約之函數.又 x^2+1 自身,雖在有理數數統內爲有理函數,然在此數統內爲不可約之函數.

例 2. x^4+1 在數統 $(\sqrt{2})$、或 $(\sqrt{-2})$、或 (i)、或 $\left(\epsilon \equiv \frac{1+i}{\sqrt{2}}\right)$ 內,皆爲可約函數.但,在一切其他數統內,皆不可約.此因 x^4+1 之一次因子 (linear factor) 爲 $x \pm \epsilon$, $x \pm i\epsilon = x \pm \epsilon^3$; 而其二次因子爲 $x^2 \pm i$ 或 $x^2 + ax \pm 1 (a^2 = \pm 2)$ 也.

設 $F(x)$ 爲在 R 內可約,則吾人稱 $F(x)=0$ **爲在 R 內可約方程式** (Reducible equation in R). 但,若 $F(x)$ 在 R 內不可約,則稱 $F(x)=0$ **爲在 R 內不可約方程式** (Irreducible equation in R).

*以有限回有理運算,將所設整函數分解爲因子之法, Kronecker 氏曾經發見,見氏之論文集,第 2 册,第 256 頁.

§55. 定理 設方程式$F(x)=0$及$G(x)=0$之係數,爲數統R內之數.又設$F(x)=0$爲在R內不可約方程式.今若$F(x)=0$有一根能滿足$G(x)=0$,則$F(x)=0$之一切根皆能滿足$G(x)=0$,且在R內$F(x)$爲$G(x)$之一因子

先以x之最高次項係數除全式,然後令

$$F(x)=(x-\xi_1)(x-\xi_2)\cdots(x-\xi_n),\quad G(x)=(x-\eta_1)(x-\eta_2)\cdots(x-\eta_m).$$

由假設知ξ內至少有一個值與η相等.命$\xi_1=\eta_1,\cdots,\xi_r=\eta_r$,而其餘$\xi$之值與$\eta$之值不同,則函數

$$H(x)\equiv(x-\xi_1)\cdots(x-\xi_r)\equiv(x-\eta_1)\cdots(x-\eta_r)$$

爲$F(x)$及$G(x)$之最高公因子.但,Euclid 氏求最高公因子之法,僅應用除法運算;故$H(x)$之係數爲$F(x)$及$G(x)$之有理函數,亦屬於數統R.於是$F(x)=H(x)\cdot Q(x)$,此處$H(x)$及$Q(x)$皆爲整函數,其係數爲R內之數值.但,由假設,$F(x)$爲在R內不可約,故$Q(x)$必爲常數且等於1.故$F(x)=H(x)$,而在R內$F(x)$必爲$G(x)$之一因子.

系1. 設$G(x)$之次數$\geqq n-1$,則$G(x)\equiv 0$凡在R內不可約方程式之根,必不能滿足在R內之低次方程式.

若$G(x)=0$亦爲不可約,則不獨可證$F(x)$爲$G(x)$之一因子,同時亦可證$G(x)$爲$F(x)$之一因子.故得

系2. 設在R內,兩個不可約方程式有一公根,則此兩方程式必全相等.

第六章

方程式之羣

$n!$-值函數之存在 (Existence); Galois 氏豫解式

§56. 設 R 爲所設數統,而方程式爲

$$f(x)\equiv x^n-c_1x^{n-1}+c_2x^{n-2}-\cdots+(-1)^nc_n=0 \cdots\cdots\cdots\cdots\cdots(1)$$

其係數屬於 R, 並設根 $x_1, x_2, \cdots, x_n$ 互不相等.* 則吾人能作一個根之有理函數 V_1, 其係數爲 R 內之數,且對於 $x_1, x_2, \cdots, x_n$ 之 $n!$ 個代換, V_1 有 $n!$ 個不等值.若在 R 內適宜選擇 $m_1, m_2, \cdots, m_n$, 則此種函數之形可設爲

$$V_1\equiv m_1x_1+m_2x_2+\cdots+m_nx_n;$$

蓋因 $x_1, x_2, \cdots, x_m$ 全不相等,故對於 $m_1, m_2, \cdots, m_n$ 之一切值,函數 V_1 被施以兩不同代換 a, b, 其所得之兩值 V_a 及 V_b 必不相等也.故吾人可於 R 內選 $m_1, m_2, \cdots, m_n$ 之值,使其不能適合 $\frac{1}{2}n!$ $(n!-1)$ 個如 $V_a=V_b$ 形之關係式即可.

於是,由方程式 $V_{a'}=V_a$, 即得 $a'=a$ 之結果.

例如,就方程式 $x^3+x^2+x+1=0$ 而言,其根爲

$$x_1=-1, \quad x_2=+i\equiv\sqrt{-1}, \quad x_3=-i.$$

設 R 爲有理數數統,則由 x_1, x_2, x_3 之 $3!=6$ 種代換而得之六個函數

$$-m_1+im_2-im_3, \quad m_1-im_2+im_3, \quad im_1-m_2-im_3,$$

---

*因 $F(x)=0$ 之等根 (Equal roots) 亦能滿足方程式 $F'(x)=0$, 其係數亦屬於 R. 故 $F(x)=0$ 之等根亦能滿足 $H(x)=0$, 此處 $H(x)$ 表 $F(x)$ 及 $F'(x)$ 之最高公因子.設 $F(x)\div H(x)=Q(x)$, 則方程式 $Q(x)=0$ 之係數亦屬於 R, 且其根不相等.故當 $Q(x)=0$ 既解之後, $F(x)=0$ 之根即完全知道.

$$-im_1+im_2-m_3,\quad -im_1-m_2+im_3,\quad im_1-im_2-m_3,$$

當 m 之值不適合次列關係時,其值必不相等:

$$m_2-m_3=0,\quad m_1-m_2=0,\quad m_1-m_3=0,$$

$$(i+1)m_1-2im_2+(i-1)m_3=0,\quad (i-1)m_1+(i+1)m_2-2im_3=0,$$

$$(i-1)m_1-2im_2+(i+1)m_3=0,\quad (i+1)m_1+(i-1)m_2-2im_3=0,$$

$$-2im_1+(i-1)m_2+(i+1)m_3=0,\quad -2im_1+(i+1)m_2+(i-1)m_3=0.$$

但上面九式內,後六式間相異之點,僅在 m_1, m_2, m_3 排列次序之不同;故欲選 m 之值使不適合上之九式,可舉實例解釋之令 $m_3=0$, 而予 m_1 及 m_2 以不等零之任意有理值,且要 $m_1\neq\omega m_2$ [$\omega=1$, 或 $\pm i$, 或 $1\pm i$, 或 $\frac{1}{2}(1\pm i)$] 者而用之,故祇要 m_1 爲不等 0 及 1 之任意有理數,函數 $m_1x_1+x_2$ 即爲一個 6-值函數矣.

[例如,在數統(i)內,吾人若假定 $m_1\neq 0$, 1, $\pm i$, $1\pm i$, $\frac{1}{2}(1\pm i)$,則 $m_1x_1+x_2$ 即可選充爲所設函數.]

§57. 函數 V_1 之 $n!$ 個值,乃爲方程式

$$F(V)\equiv(V-V_1)(V-V_2)\cdots(V-V_{n!})=0 \quad\cdots\cdots(4)$$

之根,此方程式之係數乃 $m_1, m_2, \cdots, m_n, c_1, c_2, \cdots, c_n$ 之整有理函數而以整數爲其係數者,故(4)之係數屬於數統 R(§50). 若 $F(V)$ 爲在 R 內可約之函數,則命 $F_0(V)$ 爲其不可約因子中之能使 $F_0(V_1)=0$ 者;若 $F(V)$ 已爲在 R 內不可約之函數,則 $F_0(V)$ 即爲函數 $F(V)$ 之自身.此不可約方程式

$$F_0(V)=0 \quad\cdots\cdots(5)$$

稱爲方程式(1)之 **Galois 氏豫解式** (Galois resolvent).

再就前節之例言之,取

$$V_1=x_2-x_1,\quad V_2=x_2-x_3,\quad V_3=x_3-x_1.$$

則 V_1 之六值爲 $\pm V_1$, $\pm V_2$, $\pm V_3$, 此處

$$V_1=i+1,\quad V_2=2i,\quad V_3=-i+1.$$

方程式(4)此時爲

$$(V^2-V_1^2)(V^2-V_2^2)(V^2-V_3^2)=(V^2-2i)(V^2+4)(V^2+2i)$$
$$=V^6+4V^4+4V^2+16=0.$$

故 $F(V)$ 在有理數數統內之不可約因子爲

$$V^2+4=(V-V_2)(V+V_2),\quad V^2-2V+2\quad (V-V_1)(V-V_3),$$
$$V^2+2V+2=(V+V_1)(V+V_3).$$

故 Galois 氏數解式爲

$$F_0(V)\equiv V^2-2V+2=0.$$

[倘就數統(i)而言, Galois 氏豫解式爲 $V-V_1\equiv V-i-1=0$.]

§58. 定理 所設方程式(1)之根之任意有理函數(其係數在數統 R 內),必爲 V_1 之 $n!$-值函數(其係數亦在 R 內):

$$\phi(x_1,x_2,\cdots,x_n)=\Phi(V_1)\cdots\cdots\cdots\cdots\cdots\cdots(6)$$

先設方程式(1)內之係數 $c_1, c_2, \cdots, c_n$ 爲任意量,因而根 $x_1, x_2, \cdots, x_n$ 便爲獨立變數.於是,吾人可適用§31內 Lagrange 氏定理之證明,以僅對於 x 代換不變之函數 V_1 代§31之 ϕ,得

$$\phi=\lambda(V_1)+F'(V_1)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(6')$$

此處 $F'(V)$ 爲(4)之函數 $F(V)$ 之導微函數(Derivative). 次與 $c_1, c_2, \cdots, c_n$ 以特殊之 R 內之數,使 $x_1, x_2, \cdots, x_n$ 變爲所設方程式之根,則因 $F'(V_1)\neq 0$, 故關係(6')即化爲所求之關係式(6),將函數 ϕ 用 V_1 之有理函數(其係數在 R 內)表之.

系 設 s 爲就文字 $x_1, x_2, \cdots, x_n$ 之任意代換,則

$$\phi_s(x_1,x_2,\cdots,x_n)=\Phi(V_s)\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots(7)$$

此處假定吾人不得利用§57之方程式 $F_0(V_1)=0$ 將 $\Phi(V_1)$ 之形狀約簡.*

*若加約簡,即致結果失效;此可由§59之例見之.

試即就方程式 $x^3+x^2+x+1=0$ 爲例,而求將函數 $\phi\equiv x_2$ 以 $V_1\equiv x_2-x_1$ 之函數表之之式.因

$$F(V)=V^6+4V^4+4V^2+16,\quad F'(V)=6V^5+16V^3+8V,$$

$$\lambda(V)=F(V)\left\{\frac{x_2}{V-V_1}+\frac{x_1}{V+V_1}+\frac{x_2}{V-V_2}+\frac{x_3}{V-V_3}+\frac{x_3}{V+V_2}+\frac{x_1}{V+V_3}\right\}$$

$$=-2V^5-4V^4-12V^3-8V^2-16V-48,$$

此處最後一行乃由前一行以 $x_1=-1$, $x_2=i$, $x_3=-i$, $V_1=i+1$, $V_2=2i$, $V_3=-i+1$ 代入而得.故

$$x_2=\frac{\lambda(V_1)}{F'(V_1)}=\frac{-2V_1^5-4V_1^4-12V_1^3-8V_1^2-16V_1-48}{6V_1^5+16V_1^3+8V_1}\equiv\Phi(V_1).$$

欲驗所得結果之是否正確,試以 V_1 之值代各式,得

$$\lambda(V_1)=\lambda(i+1)=-48i-16,\quad F'(V_1)=16i-48,\quad \Phi(V_1)=i=x_2,$$

足徵其確實無誤.

由系得

$$x_1=\Phi(-V_1),\quad x_2=\Phi(V_2),\quad x_3=\Phi(V_3),\quad x_3=\Phi(-V_2),\quad x_1=\Phi(-V_3).$$

倘欲加檢驗,觀

$$\Phi(-V_1)=\frac{16i-48}{-16i+48}=-1,\quad \Phi(V_2)=\frac{-80}{80i}=i,\quad \Phi(-V_2)=\frac{-80}{-80i}=-i,$$

即知之,此處 $\Phi(V_3)$ 與 $\Phi(V_1)$, $\Phi(-V_3)$ 與 $\Phi(-V_1)$, x_3 與 x_2 皆爲相配複數 (Conjugate imaginaries), 惟 x_1 爲實數.

§59. 上述定理之特款 (Special case) 爲:

所設方程式之根乃 V_1 之有理函數:

$$x_1=\psi_1(V_1),\ x_2=\psi_2(V_1),\ \cdots,\ x_n=\psi_n(V_1)\quad\cdots\cdots(8)$$

其係數皆在 R 內.故吾人決定 V_1 之值,即同於解所設方程式.

因 V_s 爲 $x_1,x_2,\cdots,x_n$ 之有理函數,其係數在 R 內,故 **Galois 氏豫解式之一切根,皆爲任一根 V_1 之有理函數,其係數亦在 R 內.**

例 對於方程式 $x^3+x^2+x+1=0$ 及 $V_1=x_2-x_1$, 吾人得

$$\alpha_1=-1,\quad \alpha_2=V_1-1,\quad \alpha_3=-V_1+1,\quad V_2=2V_1-2,\quad V_3=-V_1+2.$$

雖 α_2 及 V_1-1 之數值相等,然施以代換$(\alpha_1\alpha_2)$而得之函數 α_1 及 $-V_1-1$ 則不相等;蓋 $\alpha_2=V_1-1$ 乃利用全等式 $V_1^2-2V_1+2=0$ 將 $\alpha_2=\Phi(V_1)$ 化簡而得之式,非 α_2 之原式也(§57). 其化簡之法爲:因

$$-2V_1^5-4V_1^4-12V_1^3-8V_1^2-16V_1-48=(V_1^2-2V_1+2)(-2V_1^3-8V_1^2-24V_1-40)$$
$$-48V_1+32$$
$$-48V_1+32,$$

$$6V_1^5+16V_1^3+8V_1=(V_1^2-2V_1+2)(6V_1^3+12V_1^2+28V_1+32)+16V_1-64$$
$$=16V_1-64$$

$$\therefore\quad \frac{-48V_1+32}{16V_1-64}=\frac{(-3V_1+2)(V_1+2)}{(V_1-4)(V_1+2)}=\frac{-3V_1^2-4V_1+4}{V_1^2-2V_1-8}=\frac{-10V_1+10}{-10}=V_1-1.$$

但,對於等式 $\alpha_2=V_2-1$,若施以代換$(\alpha_2\alpha_3)$,所得之 $\alpha_3=V_3-1=-V_1+1$ 仍爲等式;似此施 α_1, α_2, α_3 之么代換及$(\alpha_2\alpha_3)$而等式仍然成立,而施以其他代換,等式便不成立之理由,將於後面之普通定理解釋之.

方程式之羣

§60. 設 Galois 氏豫解式(5)之根,以

$$V_1,\ V_a,\ V_b,\ \cdots,\ V_l \quad\cdots\cdots(9)$$

表之.又設各根欲由 V_1 導出所用之代換爲

$$I,\ a,\ b,\ \cdots,\ l \quad\cdots\cdots(10)$$

此諸代換構成一羣稱爲對於有理性數統 R 之**所設方程式(1)之羣** (Group of the given equation).

欲證(10)內各代換構成一羣,祇須證:當 r 及 s 爲代換(10)之任二個代換時,則 rs 亦含於(10)內.今設 V_r 及 V_s 爲(5)之根,則

$$F_0(V_r)=0.$$

但, V_r 可按§58之法,列爲 V_1 之有理函數:

$$V_r=\theta(V_1) \quad \cdots\cdots (11)$$

其係數在R內,且其形狀不許化簡.若以之代入前式,得$F_0[\theta(V_1)]=0$;於是,在R內不可約方程式(5),有一根能滿足方程式

$$F_0[\theta(V)]=0 \quad \cdots\cdots (12)$$

(其係數在R內).由§55知:(5)之他根V_s必亦滿足(12),

$$\therefore \quad F_0[\theta(V_s)]=0.$$

又按§58之系,並由(11),得

$$(V_r)_s \equiv V_{rs}=\theta(V_s).$$

故得$F_0(V_{rs})=0$.於是,V_{rs}含於(9)內.

對於方程式$x^3+x^2+x+1=0$並就有理數數統R而言,其Galois氏豫解式,已於§57內證明其爲$V^2-2V+2=0$,而其根爲V_1及V_3.因V_3可從V_1施以代換(x_2x_3)得來;故對於R,方程式$x^3+x^2+x+1=0$之羣爲$\{I, (x_2x_3)\}$.

若就數統(i)而言,Galois氏豫解式業證得其爲$V-V_1=0$,故對於(i),所設方程式之羣爲么羣.

§61. 設方程式(1)之根爲$x_1, x_2, \cdots, x_n$,其羣G之級爲N,則此羣必有次之兩基本性質:

(A)**凡根之有理函數$\phi(x_1, x_2, \cdots, x_n)$,若施以$G$之一切代換皆保留不變時,則此函數必在數統$R$內.**

(B)**凡根之有理函數$\phi(x_1, x_2, \cdots, x_n)$,若等於$R$內之一量,則此函數必不爲$G$之一切代換所改變.**

所謂根之有理函數$\phi=\phi(x_1, x_2, \cdots, x_n)$云者,乃謂係數在$R$內之有理函數也.故由§58得

$$\phi=\Phi(V_1),\ \phi_a=\Phi(V_a),\ \phi_b=\Phi(V_b),\ \cdots,\ \phi_l=\Phi(V_l) \cdots\cdots (13)$$

此處Φ爲一有理函數,其係數在R內.

(*A*)之證明　設 $\phi=\phi_a=\phi_b=\cdots=\phi_l$，則由(13)得

$$\phi=\frac{1}{N}\{\Phi(V_1)+\Phi(V_a)+\Phi(V_b)+\cdots+\Phi(V_l)\}.$$

但，等式之右端爲 Galois 氏豫解式(5)之 N 個根(9)之對稱函數，故亦爲屬於 R 之各係數之有理函數；是以，ϕ 屬於 R 內.

(*B*)之證明　設 ϕ 等於 R 內之一量 r，則由(13)得等式

$$\Phi(V_1)-r=0.$$

是以，V_1 爲方程式

$$\Phi(V)-r=0 \quad \cdots\cdots(14)$$

(其係數在 R 內)之一根.然按§55，當不可約之 Galois 氏豫解式(5)之一根能適合(14)時，(5)之一切根 $V_1, V_a, \cdots, V_l$ 亦將適合(14)，而有

$$\Phi(V_1)-r=0,\ \Phi(V_a)-r=0,\ \cdots,\ \Phi(V_l)-r=0.$$

故由(13)，得 $\phi=\phi_a=\phi_b=\cdots=\phi_l$. 故 ϕ 對於 G 之一切代換，其值皆不變.

§62. 根 $x_1, x_2, \cdots, x_n$ 間之**有理關係**(Rational relation)云者，乃謂兩個有理函數 $\phi(x_1, x_2, \cdots, x_n)$ 及 $\psi(x_1, x_2, \cdots, x_n)$(其係數在 R 內)間，有一等式 $\phi(x_1, x_2, \cdots, x_n)=\psi(x_1, x_2, \cdots, x_n)$ 存在也.於是，$\phi-\psi$ 爲一有理函數等於零，亦爲 R 內之一量.故[由(*B*)]對於 G 之一切代換 s 不生變更.是以，$\phi_s-\psi_s=\phi-\psi=0$，而 $\phi_s=\psi_s$. 於是，得次之結論：

對於任一個根之有理關係，若於其等式兩端(Member)**俱施以羣 G 之任一代換，所得之結果仍爲眞.**

例　就有理數數統而言，前於§60內已指出方程式 $x^3+x^2+x+1=0$ 之羣爲 $\{I, (x_2x_3)\}$ 矣.有理關係(§59，例)

$$x_2=x_1-1\equiv x_2-x_1-1$$

施以代換 (x_2x_3)，仍得一正確關係：

$$x_3 = x_3 - x_1 - 1 \equiv V_3 - 1.$$

但,若施以代換$(\alpha_1\alpha_2)$,所得之關係$x_1 = x_1 - x_2 - 1$即不成立.

§63. 定理 性質(A)及(B)完全可以決定方程式之羣G.凡羣能有此兩性質者必與G全同.

先設對於羣

$$G' = \{I, a', b', \cdots, m'\}$$

之一切代換皆不變更之根$x_1, x_2, \cdots, x_n$之有理函數在R內.則方程式

$$F'(V) \equiv (V - V_I)(V - V_{a'})(V - V_{b'}) \cdots (V - V_{m'}) = 0$$

之係數,因其爲$V_I, V_{a'}, V_{b'}, \cdots, V_{m'}$之對稱函數,施以$G'$之代換不生變更,故必在$R$內.又因$F'(V)=0$能滿足不可約之 Galois 氏豫解式(5)之根$V_I$,故(5)之一切根$V_I, V_a, \cdots, V_l$亦必能滿足此方程式.於是,$I, a, \cdots, l$必見於$G'$之代換內,即$G$必爲$G'$之子羣.

次設在R內所有根$x_1, x_2, \cdots, x_n$之有理函數,對於一羣

$$G'' = \{I, a'', b'', \cdots, r''\}$$

之一切代換不生變更,則因有理函數$F_0(V_I)$之值等零,爲R內之數,故此函數對於$a'', b'', \cdots, r''$之代換不生變更,而得

$$0 = F_0(V_I) = F_0(V_{a''}) = F_0(V_{b''}) = \cdots = F_0(V_{r''}).$$

於是,$V_I, V_{a''}, \cdots, V_{r''}$必見於$F_0(V)=0$之根$V_I, V_a, \cdots, V_l$內,故$G''$必爲$G$之子羣.

若一羣同時具此兩種性質,則$G' \equiv G''$.於是,G'含G爲其子羣;同時,G'又爲G之子羣,故$G' \equiv G'' \equiv G$.

由是知:對於所設數統之所設方程式之羣祇有一個,其特例爲:方程式之羣與所選之特殊$n!$-值函數無關.

例 就方程式$x^3+x^2+x+1=0$及有理數數統R而言,§57內之函數$\pm V_1$, $\pm V_2$, $\pm V_3$皆爲6-值函數.倘吾人用V_I,則得 Galois 氏豫解式

$$(V-V_1)(V-V_3)=V^2-2V+2=0,$$

及其羣 $\{I, (x_2x_3)\}$. 若改用 V_3; 仍得同樣之結果.若吾人改用 $-V_1$ 或 $-V_3$, 則 Galois 氏豫解式爲

$$(V+V_1)(V+V_3)=V^2+2V+2=0,$$

其羣亦爲 $\{I, (x_2x_3)\}$. 若改用 V_2 或 $-V_2$ 得

$$(V-V_2)(V+V_2)=V^2+4=0.$$

因 $V_2=x_2-x_3$, 其使 V_2 變爲 $-V_2$ 之代換爲 (x_2x_3). 故羣亦爲 $\{I, (x_2x_3)\}$

所設方程式之羣 G 之實際決定法

§64. 普通 n 次方程式之羣　普通 n 次方程式,其係數 $c_1, c_2, \cdots, c_n$, 爲獨立變數,故其根亦爲獨立變數(參看附錄). 茲今證:**普通 n 次方程式對於數統 R(含有方程式之係數及任意指定常數於其內)之羣,必爲對稱羣 $G_{n!}$.** 欲證此定理,祇須證:凡 Galois 氏豫解式 $F_0(V)=0$ 必爲 $n!$ 次方程式.吾人於關係 $F_0(V_1)=0$ 內,將 V_1 及係數 $c_1, c_2, \cdots, c_n$ 等各以其用 $x_1, x_2, \cdots, x_n$ 所表之式代入,則因 $x_1, x_2, \cdots, x_n$ 爲獨立變數,故代入後所得之關係必爲全等式(參看附錄). 於是,此關係雖施以 $x_1, x_2, \cdots, x_n$ 之任意代換,結果仍然爲眞.然就他方面言之,若以各種適宜排列施於 V_1, 則 V_1 卽遞變爲 $V_2, \cdots, V_{n!}$, 又因 $c_1, c_2, \cdots, c_n$ 爲根之對稱函數,故施以排列,仍然不變.故得 $F_0(V_2)=0, \cdots, F_0(V_{n!})=0$, 卽 $F_0(V)=0$ 有 $n!$ 個不等根.

由 §63, 吾人可導出此定理之別證.設 $x_1, x_2, \cdots, x_n$ 爲獨立變數,則對於對稱羣 $G_{n!}$, (A) 及 (B) 兩性質皆能適用 —— 例如,(A) 謂根之每個對稱函數可以係數之有理函數表之 —— 故由前節定理,知方程式之羣卽爲 G_n 也.

§65. 欲決定一特殊方程式之羣,通常須另爲設法.從前所云,先作一$n!$-值函數,然後決定Galois 氏豫解式(5);或直接應用(A)及(B)兩性質之法,普通皆不切實用,因其牽涉及無窮數之根的有理函數也.至切於實用之法,可由假定已知一個有理函數及利用次之引而得之.

引 設有理函數$\phi(x_1, x_2, \cdots, x_n)$施以羣$G'$內各代換,其形式上均不生變,而施以其他代換則否,又設ϕ等於在數統R內之一量,而ϕ在$G_{n!}$下之相配函數各不相等時,則所設方程式對於數統R之羣,必爲G'之子羣.

由 §63 之前段,吾人欲證此引,祇須證:凡有理函數$\phi(x_1, \cdots, x_n)$施以羣G'之一切代換,而數值上不生變更時,則ϕ在R內.設G'之級爲P,則吾人可命

$$\phi=\frac{1}{P}(\phi_1+\phi_2+\cdots+\phi_P),$$

於是,可使ϕ成爲施以G'之一切代換而形式上不變之式.故由Lagrange 氏定理(§31),知ϕ必爲ψ之函數.故必等於R內之一量.

例 1. 就有理數數統R,試求方程式$x^3-1=0$之羣.

此方程式之根,爲

$$x_1=1, \quad x_2=\frac{1}{2}(-1+\sqrt{-3}), \quad x_3=\frac{1}{2}(-1-\sqrt{-3}).$$

命$\psi=x_1$,由引知G爲$G=\{I, (x_2\ x_3)\}$之子羣.因x_2不爲R內之數;故G必非么羣[性質(A)]. 於是,$G=G'$.

例 2. 就有理數數統R,試求方程式$y^3-7y+7=0$之羣G.

關於三次方程式$y^3+py+q=0$,得(§2)

$$D\equiv(y_1-y_2)^2(y_2-y_3)^2(y_3-y_1)^2=-27q^2-4p^3.$$

今$p=-7$, $q=7$, 故$D=7^3$. 於是,函數

$$\psi\equiv(y_1-y_2)(y_2-y_3)(y_3-y_1)$$

之值爲 ± 7，屬於 R 內之數；又在 G_6 下，其相配值 ψ 及 $-\psi$ 不同．故由引，知 G 必爲交錯羣 G_3 之子羣，即 G 必爲 G_3 自身，或爲么羣 G_1．但，若方程式之羣爲 G_1，則其根當在 R 內．然*如 $y^3-7y+7=0$ 形之方程式，其最高次項之係數爲 1，而其他係數皆爲整數，若此式有有理根時，則此根必爲整數．由試驗知 ± 1、± 7 皆不能爲此方程式之根，故其根必全爲無理數．於是，所設方程式之羣 G 必爲 G_3．

例 3. 就有理數數統 R，試求方程式 $x^4+1=0$ 之羣．

吾人先求一個含根 x_1，x_2，x_3，x_4 之有理函數，要其值能等於有理數者．試取函數 $y_1=x_1x_2+x_3x_4$ 考之．吾人於 §4 之普通四次方程式內，命 $a=b=c=0$，$d=1$，即得所設之方程式 $x^4+1=0$ 對於 y_1 之豫解式

$$y^3-4y=0.$$

今欲適當選定記法，以判別根 x_i，可命

$$y_1=-2,\quad y_2=0,\quad y_3=+2.$$

於是，y_1 等於有理數，而其在 G_{24} 下之相配值各不相同，故 G 必爲 G_8（即施於 $x_1x_2+x_3x_4$ 能保持其形式不變之羣）之子羣（§21）．同樣，由考相配函數 $y_2=x_1x_3+x_2x_4$ 及 $y_3=x_1x_4+x_2x_3$，吾人知 G 應爲 G_8' 及 G_8'' 之子羣．故 G 必爲 G_4 之子羣（§21）．於是，G 必爲 G_4，或 G_1，或

$$G_2=\{I,(x_1x_2)(x_3x_4)\},\quad G_2'=\{I,(x_1x_3)(x_2x_4)\},\quad G_2''=\{I,(x_1x_4)(x_2x_3)\}$$

中之一．

但，$G\neq G_1$，因 $x^4+1=0$ 無一根爲有理數也．

設爲 G_2．試就 $t_1\equiv x_1+x_2-x_3-x_4$ 考之．由 §5 知，就普通四次方程式 $x^4+ax^3+bx^2+cx+d=0$ 而言，$t_1^2=a^2-4b+4y_1$．故在 $x^4+1=0$ 時，$t_1^2=-8$．因此時 t_1 不爲有理數，故 $G\neq G_2$．

設爲 G_2''．試就 $t_3\equiv x_1+x_4-x_2-x_3$ 考之；普通 $t_3^2=a^2-4b+4y_3$，而在此

*參看 Dickson, College Algebra (John Wiley & Sons 公司出版)，第 198 頁．

處，則 $t_2^2=+8$. 然此時 t_2 不爲有理數，故 $G\neq G_2''$.

設爲 G_2'，試就 $t_2\equiv x_1+x_3-x_2-x_4$ 考之；普通 $t_2^2=a^2-4b+4y_2$，而在此處則 $t_2^2=0$. 但因此時 t_2 之相配值 $-t_2$ 亦等於 t_2，故用函數 t_2 並不能得出若何結果. 然 G_2' 施於 $\psi\equiv x_1x_3-x_2x_4$ 不生改變；而

$$\psi^2=(x_1x_3+x_2x_4)^2-4x_1x_2x_3x_4=y_2^2-4=-4;$$

是以 ψ 之值亦非有理數. 故 $G\neq G_2'$.

於是，就有理數數統而言，方程式 $x^4+1=0$ 之羣爲 G_4.

習 題

試就有理數數統，求次列各方程式之羣：

1. $x^3+x^2+x+1=0$ (用 §65 之引).

2. $(x-1)(x+1)(x-2)=0$.

3. $x^3-2=0$ [x_1, x_2, x_3 及 $(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 皆爲無理數].

4. $x^4+x^3+x^2+x+1=0$ 之根爲 $x_1=\epsilon$, $x_2=\epsilon^2$, $x_3=\epsilon^4$, $x^4=\epsilon^3$, 此處 ϵ 爲 1 之五次根中之一個虛根. 因 $x_1x_2+x_3x_4$ 之豫解式爲 $y^3-y^2-3y+2=0$, 其根爲 2, $\frac{1}{2}(-1\pm\sqrt{5})$, 故 G 爲 G_8' 之子羣. 但 G_8' 有一子羣爲 $G_4=\{I, (1234), (13)(24), (1432)\}$, 其所屬之函數爲 $\psi_1=x_1^2x_2+x_2^2x_3+x_3^2x_4+x_4^2x_1$. 在本例 $\psi_1=\epsilon^4+\epsilon^3+\epsilon+\epsilon^2=-1$ 爲一有理數. 又 ψ 在 G_{24} 下之六個相配函數各不相同，可由 ψ_1 施以 I, $(12)(34)$, (12), (14), (23), (34) 等代換得來，又其值爲 -1, 4, $1+2\epsilon+\epsilon^3$, $1+2\epsilon^3+\epsilon^4$, $1+2\epsilon^2+\epsilon$, $1+2\epsilon^4+\epsilon^2$. 故 G 亦爲 G_4 之一子羣. 次因

$$(x_1-x_3+ix_2-ix_4)^2=(1+2i)(\epsilon^2+\epsilon^3-\epsilon^4-\epsilon)=\pm\sqrt{5}(1+2i)$$

屬於 $G_2'=\{I, (13)(24)\}$，故 $G\neq G_2'$. 又 $G\neq G_1$，故 $G=G_4$.

5. 就數統 $(1, i)$ 求證 $x^4+1=0$ 之羣爲 G_2'.

6. 就數統 $(1, \omega)$ (此處 ω 爲 1 之立方根內之一虛根)，求證 $x^3-2=0$ 之羣爲 $G_3=\{I, (x_1x_2x_3), (x_1x_3x_2)\}$.

提示：$(x_1+\omega x_2+\omega^2 x_3)^3$ 及 $(x_1+\omega^2 x_2+\omega x_3)^3$ 有不同之有理值.

羣之協換性 (Transitivity) 方程式之不可約性

§66. 一個 n 文字之代換羣,若其中含有將一個任意所設文字,換爲其他任意所設文字之代換時,此羣稱爲**協換羣**(Transitive group);否則,稱爲**非協換羣**(Intransitive group).

例如, $G_4=\{I,\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)\}$ 爲協換羣,蓋 I 換 x_1 爲 x_1, $(x_1x_2)(x_3x_4)$ 換 x_1 爲 x_2, $(x_1x_3)(x_2x_4)$ 換 x_1 爲 x_3, $(x_1x_4)(x_2x_3)$ 換 x_1 爲 x_4.

凡羣內若有一代換 s 換 x_1 爲所設文字 x_i,及一代換 t 換 x_1 爲所設文字 x_j,則此羣必含有換 x_j 爲 x_j 之代換 $s^{-1}t$.

羣 $H_4=\{I,\ (x_1x_2),\ (x_3x_4),\ (x_1x_2)(x_3x_4)\}$ 爲非協換羣.

§67. 定理 ***n* 文字協換羣之級,必可以 *n* 除盡.**

在所設羣 G 之諸代換中,能使 x_1 不變之代換構成一子羣 $H=\{I,h_2,\cdots,h_r\}$.試就以 H 之代換排於第一行而得之 G 之諸代換之長方整列而考之(§28).取能將 x_1 換爲 x_2 之任一代換爲 g_2,將 x_1 換爲 x_3 之任一代換爲 g_3,餘仿此.則祇有第二行之代換將 x_1 換爲 x_2,第三行之代換將 x_1 換爲 x_3,餘仿此.因 G 爲協換羣,故共有 $\nu=n$ 行.然 G 之級可以 ν 除盡(§26),即 G 之級可以 n 除盡,如定理所云.

$G_3^{(3)}$, $G_6^{(3)}$, $G_{24}^{(4)}$, $G_{12}^{(4)}$, $G_8^{(4)}$, $G_4^{(4)}$ 皆爲協換羣之例.

由上知,n 文字協換羣之最小級數爲 n 級.

n 文字之協換羣,若其級爲 n,則此羣稱爲**有法羣**(Regular group).

例如, $G_3^{(3)}$ 及 $G_4^{(4)}$ 即爲有法羣.

§68. 定理　設一方程式在數統R內爲不可約,則對於R,此方程式之羣爲協換羣.倘此方程式在R內可約,則其羣爲非協換羣.

茲先證本定理之前部.設$f(x)=0$在R內不可約;倘對於R,此方程式之羣爲非協換羣,則吾人可假設G僅含將x_1換爲$x_1, x_2, \cdots, x_m$之代換,而不含換爲$x_{m+1}, \cdots, x_n$之代換.於是,G之每一代換祇予$x_1, x_2, \cdots, x_m$之次序以排列,故必不使$x_1, x_2, \cdots, x_m$之對稱函數更改;於是,函數$g(x)\equiv(x-x_1)(x-x_2)\cdots(x-x_m)$之係數皆爲$R$內之數,而$g(x)$遂爲$f(x)$之一有理因子.但,此與$f(x)$爲不可約之假設相矛盾,故方程式之羣必爲協換羣.

次設$f(x)$在R內爲可約,並設$g(x)\equiv(x-x_1)(x-x_2)\cdots(x-x_m)$爲$f(x)$之有理因子之一$(m<n)$.則有理關係$g(x_1)=0$當施以$G$之任意代換時,其結果仍爲眞(§62),故$G$必不含有將$x_1$換爲$x_{m+1}, \cdots, x_n$之代換.否則,$g(x)=0$將含有$x_{m+1}, \cdots, x_n$中之一,而與假設相矛盾矣.由是知$G$必爲非協換羣.

例 1.　方程式$x^3-1=0$在有理數數統R內爲可約.由§65 例 1,知其對於R之羣爲$\{I, (x_2\ x_3)\}$,乃一非協換羣.又就方程式$x^3+x^2+x+1=0$亦得同樣之結果(§60).

例 2.　方程式$y^3-7y+7=0$在有理數數統R內爲不可約,因其左端在R內不可分解爲一次因子也(§5, 例 2).故其在R內之羣爲協換羣;由§65, 知此羣爲$G_3^{(3)}$.

例 3.　方程式$x^4+1=0$在有理數數統R內爲不可約(§54, 例 2),故其在R內之羣爲協換羣,且其級至少爲 4.知此,吾人在§65 例 3 內決定羣G時,便可省許多手續.

例 4.　方程式在數統$(1, i)$內爲可約,其羣G_2'爲非協換羣(參看§5 後之習題 5).

屬於一羣之有理函數

§69. 定理　一個方程式之羣 G,其各代換中,能使根之有理函數 ϕ 不變者,必自成一羣.

設 $I, a, b, \cdots, k$ 爲 G 內之代換,能使 ϕ 不變者(此處不變乃就數值上而言,參看 §52). 設將羣 G 之代換 b 施於有理關係 $\phi=\phi_a$,則(§62) $\phi_b=\phi_{ab}$. 於是, $\phi_{ab}=\phi$; 而積 ab 遂亦含於使 ϕ 不變之代換中.故代換 $I, a, b, \cdots, k$ 成一羣 H.

不論 ϕ 形式上屬於何羣(§21),此後吾人將稱之爲 ϕ **屬於 G 之子羣 H**.

例　按 §65 例 3, 方程式 $x^4+1=0$ 就有理數數統 R 之羣爲

$$G_4=\{I,\ (x_1x_2)(x_3x_4),\ (x_1x_3)(x_2x_4),\ (x_1x_4)(x_2x_3)\}.$$

就 12 個代換而言,能使 x_1^2 數值上不變者(§49),僅爲見於 G_4 內之 I 及 $(x_1x_3)(x_2x_4)$. 故 $x^4+1=0$ 之根之函數 x_1^2 屬於羣 $\{I,\ (x_1x_3)(x_2x_4)\}$.

§70. 定理　設 H 爲所設方程式對於數統 R 之羣 G 內之任一子羣,則必有一個根之有理函數屬於 H,且其係數在 R 內.

設 V_1 爲根之任意 $n!$ 值函數,其係數在 R 內(§53). 設 $V_1, V_a, \cdots, V_k$ 爲由 V_1 施以 H 內之代換而得之函數,則

$$\phi\equiv(\rho-V_1)(\rho-V_a)\cdots(\rho-V_k).$$

(此處, ρ 爲在 R 內適宜選出之量)卽爲根之有理函數屬於 H 且其係數在 R 內(試與 §25 比較).

§71. 定理　設一方程式之根之有理函數 ϕ 屬於羣 H,而此羣在所設方程式對於數統 R 之羣 G 下之指數爲 ν,則 ϕ 若施以 G 之一切代換,可得 ν 個不等值,而此諸值乃豫解式

$$g(y)\equiv(y-\phi_1)(y-\phi_2)\cdots(y-\phi_\nu)=0 \qquad \cdots\cdots(15)$$

之根,其係數在 R 內.

關於函數 ψ 在 G 之諸代換下一切不相等數值祇有 ν 個之證法,與§29之證法相同;惟此處所謂不相等,乃就§52所述之意義而言.

羣 G 之任一代換,祇使函數 $\psi_1, \psi_2, \cdots, \psi_\nu$ 互相調換(試與§30比較);故其對稱函數若施以 G 之所有代換,必不改變.於是,此等函數必等於 R 內之量(§61定理A);故(15)之係數在 R 內.

注意 豫解式(15)在 R 內爲不可約.

設 $\gamma(y)$ 爲 $g(y)$ 之有理因子之一.若以 G 之各代換施於有理關係 $\gamma(\psi_1)=0$, 則得 $\gamma(\psi_2)=0, \cdots, \gamma(\psi_\nu)=0$. 於是, $g(y)=0$ 之一切根皆能適合方程式 $\gamma(y)=0$, 故 $\gamma(y)\equiv g(y)$.

例 1. 就有理數數統 R 而言,方程式 $x^3+x^2+x+1=0$ 之羣 G 爲 $\{I, (x_2x_3)\}$ (§60). 函數 x_2-x_1 (在 G 下之相配函數爲 $\psi_1=x_2-x_1$, 及 $\psi_2=x_3-x_1$) 爲

$$y^2-(\psi_1+\psi_2)y+\psi_1\psi_2=y^2-2y+2=0$$

之根.

例 2. 就數統 $(1, i)$ 而言, $x^4+1=0$ 之羣 G 爲 $\{I, (x_1x_3)(x_2x_4)\}$ (§65後之習題5),此處乃照§49之記法. x_1 在 G 下之相配函數爲 $\psi_1=x_1$, $\psi_2=x_3$, 爲

$$y^2-(\epsilon-\epsilon)y+\epsilon(-\epsilon)=y^2-i=0$$

之根.因 $\sqrt{i}=\frac{(1+i)}{\sqrt{2}}$, 故此方程式在 $(1, i)$ 內爲不可約.

§72.經 Galois 擴充後之 Lagrange 氏定理 設在方程式 $f(x)=0$ (其係數在數統 R 內)之羣 G 之代換內,能使其根之有理函數 $\psi(x_1, x_2, \cdots, x_n)$ 不變之一切代換,同時皆使有理函數 $\phi(x_1, x_2, \cdots, x_n)$ 不變時,則 ϕ 必爲 ψ 之有理函數,其係數在 R 內.

設函數 ψ 屬於 G 之一子羣 H, 命其指數爲 ν. 次將 G 之諸代換,依以 H 排在第一行而列成長方整列,則可得 ν 個不相等之相配函數 $\psi_1, \psi_2, \cdots, \psi_\nu$, 及函數值或有相等之一組函數 $\phi_1, \phi_2, \cdots, \phi_\nu$. 此兩者間,凡遇 G 之一代換能將 ψ_i 換爲 ψ_j 時,則亦將 ϕ_i 換爲 ϕ_j (試與 §31 比較). 設 $g(t)$ 即爲 (15) 之式,則

$$\lambda(t)\equiv g'(t)\left(\frac{\phi_1}{t-\psi_1}+\frac{\phi_2}{t-\psi_2}+\cdots+\frac{\phi_\nu}{t-\psi_\nu}\right)$$

爲 t 之一整函數,雖施以 G 之一切代換皆不改變,故其係數在 R 內 (§71). 以 $\psi_1\equiv x$ 代式中之 t, 則得 $\phi=\lambda(\psi)\div g'(\psi)$, 故如定理所云.

其例可參看 §53, 函數 V_1 僅能對於么代換不變,而此代換施於任一有理函數亦不生變.

羣之附益化簡法

(Reduction of the group by adjunction)

§73. 方程式 $x^3+x^2+x+1=0$ 對於有理數數統 $R=(1)$ 之羣爲 $G_2=\{I, (x_2x_3)\}$; 而對於數統 $R'=(1, i)$ 之羣爲么羣 G_1 (參看 §60). 倘用 Galois 及 Kronecker 二氏語法,則謂數統 $R'=(1, i)$ 乃由其所含數統 $R=(1)$ 上附益 (adjoin) 以量 i 而導出. 經此附益後, $x^3+x^2+x+1=0$ 之羣即化簡爲其子羣 G_1; 而所附益之 i, 乃根之有理函數, $i=x_2=-x_3$ (仍用 §49 之記法). 就數統 R 之 Galois 氏豫解式爲 $V^2-2V+2=0$; 此式若改就數統 R', 即變爲可約方程式 $(V-i-1)(V+i-1)=0$.

方程式 $x^4+1=0$ 就數統 $R=(1)$ 之羣爲 G_4; 若就數統 $(1, i)$ 而言,則其羣爲子羣 $G_2'=\{I, (x_1x_3)(x_2x_4)\}$ (§65). 故附益以 i 於數統 R, 則羣即化簡爲子羣 G_2'. 此處 $i=x_1^2=x_3^2=-x_2^2=-x_4^2=x_2x_4$ (用 §49 之記法). 函數 x_1^2 所屬之 G_2 之子羣爲 G_2', 設若吾人再附益以 $\sqrt{2}$, 則其根即全屬於擴

大數統 $(1, i, \sqrt{2})$;於是,其羣即化簡爲么羣.例如, $x_1=\frac{1+i}{\sqrt{2}}$ 是.

對於數統 $R=(1)$,方程式 $x^3-2=0$ 之羣爲 G_6;若對於數統 $(1, \omega)$——ω 表 1 之立方根中之一虛根——則其羣爲循環羣 C_3(§5 後之習題 3 及 6).命根

$$x_1=\sqrt[3]{2}, \quad x_2=\omega\sqrt[3]{2}\equiv\omega x_1, \quad x_3=\omega^2\sqrt[3]{2}\equiv\omega^2 x_1,$$

則 $\omega=x_2/x_1$ 爲屬於 C_3 之有理函數.蓋 $(x_1\ x_2\ x_3)$ 將 x_2/x_1 換爲 $x_3/x_2=\omega=x_2/x_1$,又 $(x_1\ x_3\ x_2)$ 將 x_2/x_1 換爲 $x_1/x_3=\omega^{-2}=\omega$;而此兩代換及么代換乃唯一使 x_2/x_1 不變之代換也.設若吾人附益以 $\sqrt[3]{2}$,則其根全屬於擴大數統 $(1, \omega, \sqrt[3]{2})$;於是,方程式之羣即化簡爲么羣.

§74. 普通對於所設數統 $R=(R', R'', \cdots)$ 及方程式 $f(x)=0$ (其係數在 R 內),命其羣爲 G,若附益以一量 ξ,則本來在 R 內爲不可約之 Galois 氏豫解式 $F_0(V)=0$,對此擴大數統 $R_1=(\xi; R', R'', \cdots)$,或能變爲可約.命 $\lambda(V, \xi)$ 爲 $F_0(V)$ 之因子,其在 R 內爲有理式且不可約者.又當 $V=V_1$ 時,其值等零.設 $V_1, V_a, \cdots, V_k$ 爲 $\lambda(V, \xi)=0$ 之根,則 $G'=\{I, a, \cdots, k\}$ 爲 $f(x)=0$ 就數統 R_1 之羣(§57).故 G' 必爲 G 之子羣,或 $G'=G$.此後者之場合,惟在附益 ξ 後,$F_0(V)$ 仍爲不可約,即 $\lambda(V, \xi)=F_0(V)$ 時,始能遇到.

定理　凡數統經附益後,羣 G 常被化簡爲子羣 G'.

§75. 仿 §73 之例,設附益於所設數統 R 之量爲根之有理函數 $\psi(x_1, x_2, \cdots, x_n)$,其係數在 R 內.

定理　設以屬於 G 之子羣 H 之有理函數 $\psi(x_1, \cdots, x_n)$ 附益於 R,則方程式之羣 G 恰能化簡爲子羣 H.

吾人祇要證明:羣 H 具有方程式就新數統 $R_1=(\psi; R', R'', \cdots)$ 之羣之兩種特性(§61).第一,任意有理函數 $\phi(x_1, \cdots, x_n)$ 施以 H 之一切代換不生變更時,則此函數爲 ψ 之有理函數,其係數在 R

內(§72),故亦在R_1內.第二,任意有理函數$\phi(x_1, \cdots, x_n)$,若其值等於R_1內之一量ρ,則當施以H之所有代換時,皆不生變,此因關係$\phi=\rho$可書爲在R內之有理關係也.故當施以G之任意代換時(§62),尤其在施以子羣H內之代換時,仍得合理之關係.但,後者使ϕ不生變更,故亦使ρ不生變更;於是,該關係之左邊雖施以H之一切代換,不生變更.

第 七 章

方程式利用豫解式之解法

§76. 在申述理論之前,先使讀者知道如何應用得將所設方程式 $f(x)=0$ 解出,實爲最妥善之辦法.設吾人能解豫解式(15),則其根之一必爲屬於方程式 $f(x)=0$ 之羣 G 之子羣 H 之有理函數 ψ.既知 ψ 後,即可將此數附益於所設有理性數統 $(R', R'', \cdots)$.就此擴大數統 $R_1=(\psi; R', R'', \cdots)$ 而言,$f(x)=0$ 之羣化簡爲 H.設 $\chi(x_1, \cdots, x_n)$ 爲一個屬於 H 之子羣 K 之有理函數,其係數在 R_1 內.更設吾人能將含 χ 爲一根之豫解式解出,則吾人又可取 χ 附益於數統 R_1,就此擴大數統 $R_2=(\chi, \psi; R', R'', \cdots)$ 而言,$f(x)=0$ 之羣爲 K.如此繼續做去,最後得一數統 R_k,就此數統而言,$f(x)=0$ 之羣乃爲么羣 G_1.於是,對此么羣不生改變之根 $x_1, x_2, \cdots, x_n$ 全屬於數統 R_k(§61,特性 A).故若各豫解式皆能解出時,則 $f(x)=0$ 之解法,即完全成功.用 Galois 氏方法以解各豫解式時,第一步乃求其對於相應有理性數統之羣.

§77. 同形 (Isomorphism) 設 G 爲所設方程式 $f(x)=0$ 就所設數統 R 之羣.設 $\psi(x_1, \cdots, x_n)$ 爲根之有理函數,其係數在 R 內.又設 ψ 屬於在 G 下指數爲 ν 之子羣 H.試就以 H 內代換排在首行之 G 內代換所排成之長方整列而考之,又就與 ψ 成相配之函數而考之:

$$\begin{array}{llll|l} h_1=I, & h_2 & \cdots & h_p & \psi_1=\psi \\ g_2 & h_2g_2 & \cdots & h_pg_2 & \psi_2=\psi_{g_2} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ g_\nu & h_2g_\nu & \cdots & h_pg_\nu & \psi_\nu=\psi_{g_\nu} \end{array}$$

若將羣 G 之任一代換 g 施於 v 個相配函數

$$\psi,\ \psi_{g_2},\ \psi_{g_3},\ \cdots,\ \psi_{g_v} \qquad (16)$$

其結果爲

$$\psi_g,\ \psi_{g_2 g},\ \psi_{g_3 g},\ \cdots\ \psi_{g_v g} \qquad (17)$$

不過將(16)內函數產生一種新排列,此於 §29 卽已證明矣.故關於文字爲 $x_1, \cdots, x_n$ 之羣 G 之任一代換 g,卽有一個關於文字爲 $\psi, \psi_{g_2}, \cdots, \psi_{g_v}$ 之一定代換

$$\gamma=\begin{pmatrix}\psi & \psi_{g_2} & \cdots & \psi_{g_v}\\ \psi_g & \psi_{g_2 g} & \cdots & \psi_{g_v g}\end{pmatrix}\equiv\begin{pmatrix}\psi_{g_i}\\ \psi_{g_i g}\end{pmatrix}$$

與之相應.於是,得* 如 γ 之一組代換 Γ,其中有時亦有相同者(參看下面例 1 及 2).

定理　**代換 γ 之全體 Γ 成一羣.**

此因與 g, g' 及 gg' 相應者爲

$$\gamma=\begin{pmatrix}\psi_{g_i}\\ \psi_{g_i g}\end{pmatrix},\quad \gamma'=\begin{pmatrix}\psi_{g_i}\\ \psi_{g_i g'}\end{pmatrix},\quad \gamma''=\begin{pmatrix}\psi_{g_i}\\ \psi_{g_i gg'}\end{pmatrix}.$$

欲計算積 $\gamma\gamma'$,先將 γ' 之第一行上文字之次序變動之,得

$$\gamma'=\begin{pmatrix}\psi_{g_i g}\\ \psi_{g_i gg'}\end{pmatrix},\quad \gamma\gamma'=\begin{pmatrix}\psi_{g_i}\\ \psi_{g_i gg'}\end{pmatrix}=\gamma''.$$

故若 Γ 含 γ 及 γ',則亦含積 $\gamma\gamma'$.

因 Γ 含換 ψ 爲 ψ_{g_i} $(i=1, 2, \cdots, v)$ 之代換,故羣 Γ 爲協換羣 (§66).

定義　因對於 G 內每一代換,在 Γ 內必有一代換 γ 與之相應.又對於 G 內任意兩代換之積 gg',在 Γ 內亦有兩相應代換之積 $\gamma\gamma'$ 與之相應.故羣 Γ 稱爲**與 G 同形** (To be isomorphic to G). 反之,設對於 Γ 之每一代換,亦僅與 G 之一代換相應時,則此兩羣稱爲成簡單同形 (Simply isomorphic 或 Holoedric); 否則稱爲

*不用函數 ψ 之 Γ 之定義,可參看 §104.

多歧同形(Multiply isomorphic 或 Meriedric).

例 1. 設 $G=G_6^{(3)}$, $H=G_1$, $\psi=x_1+\omega x_2+\omega^2 x_3$. 命(與 §9 相比較)

$$\psi_1=\psi,\ \psi_2=\psi_a,\ \psi_3=\psi_b,\ \psi_4=\psi_c,\ \psi_5=\psi_d,\ \psi_6=\psi_e.$$

則 $a=(x_1x_2x_3)$. 將 ψ_1 換爲 $\psi_2=\omega^2\psi_1$, 又將 ψ_4 換爲 $\psi_6=\omega\psi_4$ 故 a 將 ψ_2 換爲 $\omega^4\psi_1=\psi_3$, ψ_3 換爲 $\omega^6\psi_1=\psi_1$, ψ_6 換爲 $\omega^2\psi_4=\psi_5$, ψ_5 換爲 $\omega^3\psi_4=\psi_4$. 故與 a 成對應者爲 $\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$. 同樣,得與 $c=(x_2x_3)$ 成對應之 $\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$ 故與 $b=a^2$ 成對應者爲 $\beta=\alpha^2$, 與 $d=a^{-1}ca$ 成對應者爲 $\delta=\alpha^{-1}\gamma\alpha$, 與 $e=b^{-1}cb$ 成對應者爲 $\epsilon=\beta^{-1}\gamma\beta$. 於是,得次之 G 與 Γ 間之簡單同形:

I	I
$a=(x_1x_2x_3)$	$\alpha=(\psi_1\psi_2\psi_3)(\psi_4\psi_6\psi_5)$
$b=(x_1x_3x_2)$	$\beta=(\psi_1\psi_3\psi_2)(\psi_4\psi_5\psi_6)$
$c=(x_2x_3)$	$\gamma=(\psi_1\psi_4)(\psi_2\psi_5)(\psi_3\psi_6)$
$d=(x_1x_3)$	$\delta=(\psi_2\psi_6)(\psi_3\psi_4)(\psi_1\psi_5)$
$e=(x_1x_2)$	$\varepsilon=(\psi_3\psi_5)(\psi_1\psi_6)(\psi_2\psi_4)$

吾人並可直接證實與 b, d, e 成對應者爲 β, δ, ε.

因 I, α, β, γ, δ, ε 將 ψ_1 換爲 ψ_1, ψ_2, ψ_3, ψ_4, ψ_5, ψ_6; 故 Γ 爲協換羣.

例 2 設 $G=G_{12}^{(4)}$, $H=G_4$, $\psi=(x_1-x_2)(x_3-x_4)$. 命

$$\psi_1=\psi,\quad \psi_2=(x_1-x_3)(x_4-x_2),\quad \psi_3=(x_1-x_4)(x_2-x_3).$$

則得次之 G 與 Γ 間之多歧同形:

I,	$(x_1x_2)(x_3x_4)$,	$(x_1x_3)(x_2x_4)$,	$(x_1x_4)(x_2x_3)$	I
$(x_2x_3x_4)$,	$(x_1x_3x_2)$,	$(x_1x_4x_3)$,	$(x_1x_2x_4)$	$(\psi_1\psi_2\psi_3)$
$(x_2x_4x_3)$,	$(x_1x_4x_2)$,	$(x_1x_2x_3)$,	$(x_1x_3x_4)$	$(\psi_1\psi_3\psi_2)$

因羣 Γ 含換 ψ_1 爲 ψ_1, ψ_2 或 ψ_3 之代換;故 Γ 爲協換羣.

§78. 羣 Γ 之級 欲求 Γ 內不同代換之數,可先求在何種條件之下,Γ 之兩代換 γ 及 γ' 能全相同.試用 §77 之記法,則其條件爲

$$\psi_{g_i g}=\psi_{g_i g'}\quad (i=1,\ 2,\ \cdots,\ v)$$

命 $g_1=I$. 設以代換 $g^{-1}g_i^{-1}$ 施於上之等式,得

$$\psi=\psi_{g_ig'g^{-1}g_i^{-1}}$$

故 $g_ig'g^{-1}g_i^{-1}=h$, 而 h 乃爲使 ψ 不變之一代換,故必在羣 H 內. 於是,

$$g'g^{-1}=g_i^{-1}hg_i \quad (i=1, 2, \cdots, \nu).$$

但, $g_i^{-1}hg_i$ 屬於函數 ψ_{σ_i} 之羣 $H_i\equiv g_i^{-1}Hg_i$ (§39). 故 $g'g^{-1}$ 同時屬於 $H_1, H_2, \cdots, H_\nu$; 是以,亦屬於其最大公子羣 J.

反之,若 J 之任一代換 σ 使 $\psi_1, \psi_2, \cdots, \psi_\nu$ 不變,則必與 Γ 內之 α 代換成對應,故 g 及 $g'=\sigma g$ 卽與全相同之代換 γ 及 γ' 成對應.

設 G 之級爲 k, 又設 $H_1, H_2, \cdots, H_\nu$ 之最大公子羣 J 之級爲 j, 則 Γ 之級爲 k/j.

例 1. 若 $G=G_6$, $H=G_1$, 則 Γ 之級爲 6 (§77, 例 1).

例 2. 若 $G=G_{12}^{(4)}$, $H=G_4$ (§77, 例 2). 則因 G_4 在 G_{12} 下爲自配 (§41), 故得 $H_1=H_2=H_3$. 故 $k=12$, $j=4$. 於是, Γ 之級爲 3.

例 3. 若 $G=G_{24}^{(4)}$, $H_1=G_8$, $\psi=x_1x_2+x_3x_4$, 命 (參看 §29, 例 2)

$$\psi_1=x_1x_2+x_3x_4,\quad \psi_2=x_1x_3+x_2x_4,\quad \psi_3=x_1x_4+x_2x_3.$$

則 $H_1=G_8$, $H_2=G_8'$, $H_3=G_8''$, $J=G_4$ (§21). 故 Γ 之級爲 $\frac{24}{4}=6$. 此結果亦可直接予以解釋. 蓋因對於 3 文字 ψ_1, ψ_2, ψ_3 之不同代換共有 6 種. 但與 Γ 之么代換相應之 G 之代換,必使 ψ_1, ψ_2, ψ_3 皆不變,故必屬於 H_1, H_2, H_3 之最大公子羣 G_4. 故每 G 內四個代換,恰與 Γ 之每一代換相應;所以 Γ 之級爲 $\frac{24}{4}=6$. 若將 G_{24} 之子羣 G_4 內代換 I, $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$ 排於第一行,則任一組四個代換,皆排在 G_{24} 所成之長方整列之一行. 若用右邊乘式,則可取

$$g_1=I,\ g_2=(x_2x_3x_4),\ g_3=(x_2x_4x_3),\ g_4=(x_3x_4),\ g_5=(x_2x_4),\ g_6=(x_2x_3).$$

於是與第一行之四代換,第二行之四代換,…相應者爲

$$I,\ (\psi_1\psi_2\psi_3),\ (\psi_1\psi_3\psi_2),\ (\psi_2\psi_3),\ (\psi_1\psi_3),\ (\psi_1\psi_2).$$

§79. 在 $H_1, H_2, \cdots, H_\nu$ 全相同時,其結果尤爲重要;此時,**H 在 G 下爲自配羣**.於是,$J=H$,而 Γ 之級 k/j 等於 H 在 G 下之指數 ν.故 Γ 之不同代換之數,等於此等代換所施之文字 $\psi_1, \psi_2, \cdots, \psi_\nu$ 之數,即**羣 Γ 之級與次之數相等**.又因 Γ 爲一協換羣,故 Γ **必爲有法羣**(§67).

定義* 若 H 在 G 下爲自配羣,則羣 Γ 稱爲 G 對於 H 之商羣(Quotient-group),以 G/H 表之.其特例爲 G/H 之級等於 G 之級與 H 之級之商.

例 1. 由 §77 之例 1 及 2,商羣 G_6/G_1 爲對於六文字之有法羣.商羣 G_{12}/G_4 乃循環羣 $\{I, (\psi_1\psi_2\psi_3), (\psi_1\psi_3\psi_2)\}$,此羣亦爲一有法羣.

例 2. 因 G_6 在 G_{24} 下非爲自配羣,故吾人不可用記號 G_{24}/G_6(參看 §78,例 3).

例 3. 試就 3 文字之羣 G_6 及 G_3 而考之:函數 $\psi_1=(x_1-x_2)(x_2-x_3)(x_3-x_1)$ 屬於 G_3;而在 G_6 下,此函數並有第二值 $\psi_2=-\psi_1$(§9).故得次之 G_6 及 Γ 間之同形:

$$\begin{array}{lll|l} I, & (x_1x_2x_3), & (x_1x_3x_2) & I \\ (x_2x_3), & (x_1x_3), & (x_1x_2) & (\psi_1\psi_2) \end{array}$$

因 G_3 在 G_6 下爲自配,故 $\Gamma=G_6/G_3=\{I, (\psi_1\psi_2)\}$.

系 設 H 爲 G 之自配子羣,其指對爲素數 ν,則 Γ 爲 ν 級之循環羣(§27).

例 1 及 2 之羣 G_{12}/G_4 及 G_6/G_3,均可資爲說明之資料.

注意 任一代換羣 G 與一有法羣皆成簡單同形.欲證實

*參看 Hölder,算學年報 (Math. Ann.) 第 24 卷,第 31 頁.

此語,祇須隨意取一$n!$-值函數V_1爲ψ_1,於是,Γ之級卽等於G之級矣.

§80. 設H爲G之最大自配子羣(§43),則商羣$\Gamma=G/H$爲簡單羣(§43). 蓋若Γ有一自配子羣Δ,而此子羣非Γ自身亦非么羣G_1時,則因G與Γ間成對應之故,G亦有一自配子羣D,而此子羣與羣G及H不同,且必包含H爲其子羣但,因H爲最大子羣,故此結果與假設不合.

例如,設H爲G之自配子羣,其指數ν爲一素數時,則H必爲G之最大自配子羣.於是,Γ爲一ν級之循環羣(§79之系),故爲簡單羣.

§81. 以上皆研究文字爲$\psi_1, \psi_2, \cdots, \psi_\nu$之代換羣$\Gamma$,其所以爲重要者,乃因$\Gamma$在豫解式

$$g(y)\equiv(y-\psi_1)(y-\psi_2)\cdots(y-\psi_\nu)=0 \quad\cdots\cdots(15)$$

(其係數屬於所設數統R內)之研究上,甚有關係也.茲今證次之定理:

定理　就數統R,方程式(15)之羣爲Γ.

欲證此定理,卽須證Γ具有§61之A及B兩性質.吾人知道,任一有理函數$\rho(\psi_1, \psi_2, \cdots, \psi_\nu)$,其係數在$R$內者,可改書爲有理函數$r(x_1, x_2, \cdots, x_n)$,其係數亦在$R$內:

$$\rho(\psi_1, \psi_2, \cdots, \psi_\nu)=r(x_1, x_2, \cdots, x_n) \quad\cdots\cdots(18)$$

由此有理關係,則吾人施以文字爲$x_1, x_2, \cdots, x_n$之羣G內任一代換g時,仍得一眞實之關係.但,g能引起文字爲$\psi_1, \psi_2, \cdots, \psi_\nu$之羣$\Gamma$內一代換$\gamma$,故其結果所得之關係,乃爲

$$\rho_\gamma(\psi_1, \psi_2, \cdots, \psi_\nu)=r_g(x_1, x_2, \cdots, x_n) \quad\cdots\cdots(19)$$

今欲證A,設以Γ內一切代換施於$\rho(\psi_1, \psi_2, \cdots, \psi_\nu)$,均不生變更.於是,就$\Gamma$內任一代換$\gamma$,$\rho_\gamma=\rho$.故由(18)及(19)知,不論就$G$

內任一代換 $g, r_g=r$. 於是, r 在數統 R 內(此爲對於羣 G 之特性 A),故 ρ 亦在 R 內

次欲證 B, 設 ρ 在數統 R 內,則由 (18) 知 r 亦在 R 內;故就 G 內之任一代換 $g, r_g=r$ (此爲對於羣 G 之特性 B). 故由 (18) 及 (19), $\rho_\gamma=\rho$, 卽 ρ 雖施以 Γ 之一切代換 γ, 仍不生變也.

系 1. 因 Γ 爲協換羣 (§77), 故**方程式(15)在 R 內爲可約** (§68). 此系已別證於 §71 內.

系 2. 設 Γ 所屬之羣 H 在 G 下爲自配,則豫解式(15)之羣**必爲有法羣**(§79). 此時,豫解式稱爲**有法方程式** (Regular equation).

系 3. 設 H 爲 G 之自配子羣,其指數爲素數 ν, 則(15)之羣**爲循環羣**(§79之系). 此時,豫解式稱爲 ν(素數)次**循環方程式** (Cyclic equation).

系 4. 設 H 爲 G 之最大自配子羣,則 (15) 之羣爲簡單羣 (§80). 此時,豫解式稱爲**簡法方程式** (Regular and simple equation 或 Simple regular equation).

§82. 定理 任一所設方程式之解法,可化爲解一組簡法方程式之連索 (Chain) 而得之.

設 G 爲所設方程式對於數統 R 之羣,並設 G 之子羣系 (§43) 爲

$$G,\ H,\ K,\ \cdots,\ M,\ G_1,$$

其子羣系因子爲 λ(H 在 G 下之指數), μ(K 在 H 下之指數), …, ρ(G_1 在 M 下之指數). 設 $\phi, \psi, \cdots, \chi, V$ 順次爲屬於 $H, K, \cdots, M, G_1$ 之根之有理函數(§70). 則 ϕ 爲係數在 R 內之 λ 次豫解式之一根,而此豫解式乃爲簡法方程式(§81, 系4), 故以 ϕ 附益於數統 R 後,則方程式之羣 G 卽化簡爲 H(§75). 次則以 ψ 爲係數在擴

大數統(ϕ, R)內之μ次簡法方程式之一根,故附益以ψ後,而羣即化簡爲K.循此進行,直至羣化簡爲幺羣G_1時,方程式之各根$x_1, x_2, \cdots, x_n$即全在此最後所得之數統內矣(與§76相比較).

其特例爲:**當子羣系因子$\lambda, \mu, \cdots, \rho$全爲素數時,則各豫解式即全爲素數次數之有法循環方程式**(§81,系3).

§83. 定理　p(素數)次之循環方程式,可以根數解之.

設R爲所設數統,而根爲$x_0, x_1, \cdots, x_{p-1}$之所設方程式$f(x)=0$之係數皆屬於$R$中.又設對於此數統而言,$f(x)=0$之羣爲循環羣$G=\{I, s, s^2, \cdots, s^{p-1}\}$,而$s=(x_0x_1x_2\cdots x_{p-1})$.試以1之第$p$次虛根$\omega$*附益於$R$,並設就此擴大數統$R'$而言,$f(x)=0$之羣爲$G'$;於是,就次之有理函數(其係數在$R'$內)而考之:

$$\theta_i \equiv x_0 + \omega^i x_1 + \omega^{2i} x_2 + \cdots + \omega^{(p-1)i} x_{p-1} \quad\cdots\cdots\cdots(20)$$

此函數經施以代換s後,θ_i即變爲$\omega^{-i}\theta_i$.故函數$\theta_i{}^p \equiv \Theta_i$施以$s$不生變更;於是,施以$G$內之各代換,尤其是$G$之子羣$G'$內之代換,均不生變(§74),故$\Theta_i$屬於數統$R'$內(§61).若兩邊求$p$次根,得$\theta_i = \sqrt[p]{\Theta_i}$.因函數(20)屬於幺羣,故由Lagrange氏定理(§72)知,吾人能將根$x_0, x_1, \cdots, x_{p-1}$書爲$\theta_i$之有理函數.Lagrange氏曾以巧妙方法得其式,其法乃由(20)施以代換,遂得

$$\begin{aligned}
x_0 + x_1 \quad &+ \quad x_2 \quad + \cdots + \quad x_{p-1} &&= c,\\
x_0 + \omega x_1 \quad &+ \quad \omega^2 x_2 \quad + \cdots + \quad \omega^{(p-1)} x_{p-1} &&= \sqrt[p]{\Theta_1},\\
x_0 + \omega^2 x_1 \quad &+ \quad \omega^4 x_2 \quad + \cdots + \quad \omega^{2(p-1)} x_{p-1} &&= \sqrt[p]{\Theta_2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
x_0 + \omega^{p-1} x_1 &+ \omega^{2(p-1)} x_2 + \cdots + \omega^{(p-1)^2} x_{p-1} &&= \sqrt[p]{\Theta_{p-1}},
\end{aligned}$$

此處$c \equiv \sqrt[p]{\Theta_0}$等於$f(x)=0$內$x^{p-1}$之係數而變其符號者.以1,

---

*此在§89中證出ω可由一已知量每次取其開方之一根,連經有限回之運算得之.

ω^{-i}, ω^{-2i}, ···, $\omega^{-(p-1)i}$ 順次乘此等方程式而加之,並以 p 除兩邊,得*

$$x_i=\frac{1}{p}\{c+\omega^{-i}\sqrt[p]{\theta_1}+\omega^{-2i}\sqrt[p]{\theta_2}+\cdots+\omega^{-(p-1)i}\sqrt[p]{\theta_{p-1}}\},$$

$$(i=0,1,\cdots,p-1).$$

此等 $p-1$ 個根數中之一,設爲 $\sqrt[p]{\theta_1}$, 其值可隨意選定;但,此量經選定後,其他之量卽完全決定,皆可列爲此量之有理函數.實則,

$$\sqrt[p]{\theta_i}\div(\sqrt[p]{\theta_1})^i\equiv\theta_i\div\theta_1^i,$$

經施以代換 s 後,卽變爲 $\omega^{-i}\theta_i\div(\omega^{-1}\theta_1)^i$, 其值仍不變更,故屬於數統 R' 內.

§84. 由 §§82—83 之結果,得次之定理:

定理 設方程式之羣有一子羣系,且其子羣系因子全爲素數時,則此方程式可以根數解之,換言之,卽可以由已知量之方根解之.

如此所得羣之性質,成爲所設方程式可以代數解 (Algebraic solvability) 之充分條件;將來還要證明其亦爲可以代數解之必需條件 (§92).

*此因在 $t=1, 2, \cdots, p-1$ 時, $1+\omega^t+\omega^{2t}+\cdots+\omega^{(p-1)t}=0$ 也.

第八章

有法循環方程式　Abel氏方程式

§85. 設 $f(x)=0$ 對於數統 R 之羣,乃由一循環代換 $s=(x_1x_2\cdots x_n)$ 之各乘冪所構成:

$$G=\{I, s, s^2, \cdots, s^{n-1}\},$$

此處 n 爲任意整數.因循環羣 G 爲協換羣,又其羣之級與次相同,故爲有法羣(§67).反之,凡協換循環羣之母代換(Generator) s 必爲一就 n 文字之循環代換.*

此時,方程式 $f(x)=0$ 具次之性質:

(a)爲不可約,因其羣爲協換羣之故(§68).

(b)一切根皆爲任一根 x_1 之有理函數,其係數在 R 內.蓋因在 n 文字之協換羣內,僅有 n 個代換.故只有一個代換,卽么代換,使 x_1 不生改變.因 x_1 屬於么羣,故可由 Lagrange 氏定理得出結果(§72).設 $x_2=\theta(x_1)$,則吾人可將 G 之一切代換施於此有理關係(§62).於是,

$$x_2=\theta(x_1),\ x_3=\theta(x_2),\ \cdots,\ x_n=\theta(x_{n-1}),\ x_1=\theta(x_n)\cdots\cdots\cdots(21)$$

定義　設有一個就數統 R 不可約之方程式,其 n 根間有(21)形之關係,而 θ 爲一有理函數,其係數在 R 內時,此不可約方程式稱爲 **Abel氏方程式**(Abelian equation)†.

---

*從一個非循環代換,如 $t=(x_1x_2x_3)(x_4x_5)$,可產生一非協換羣,故 t 之各乘冪僅能以 x_1, x_2, 或 x_3 換 x_1.

†質言之,此爲簡單 Abel 氏方程式 (Uniserial Abelian),其在德語,Kronecker 氏則用 Einfache Abel'sche.其更一般之 Abel 氏方程式之形式,Abel 氏曾研究過,讀者可參看氏之論　　I, No. XI 第 114–140 頁.

§86. 定理 Abel 氏方程式之羣 G 乃一有法循環羣(Regular cyclic group).

設以

$$g=\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_\alpha & x_\beta & x_\gamma & \cdots & x_\nu \end{pmatrix}$$

表羣 G 之任一代換,將此代換施於有理關係 (21) 上,得 (§62)

$$x_\beta=\theta(x_\alpha),\ x_\gamma=\theta(x_\beta),\ \cdots,\ x_\alpha=\theta(x_\nu).$$

但,若吾人認定 $x_i=x_{i+n}=x_{i+2n}=\cdots$ 時,則由 (21), $\theta(x_\alpha)=x_{\alpha+1}$, 即在 $\alpha=n$ 時,仍然成立.於是,

$$x_\beta=x_{\alpha+1},\ x_\gamma=x_{\beta+1},\ \cdots,\ x_\alpha=x_{\nu+1}.$$

因方程式爲不可約,其根全不相同,故除去 n 之倍數外,

$$\beta=\alpha+1,\ \gamma=\beta+1=\alpha+2,\ \delta=\gamma+1=\alpha+3,\ \cdots,$$

$$\therefore\ g=\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_\alpha & x_{\alpha+1} & x_{\alpha+2} & \cdots & x_{\alpha+n-1} \end{pmatrix}.$$

因 g^k 將 x_i 換爲 $x_{i+\alpha-1}$, 故等於將 x_i 換爲 x_{i+1} 之循環代換 $s=(x_1x_2x_3\cdots x_n)$ 之 $\alpha-1$ 冪.所以 G 爲 $G'=\{I, s, s^2, \cdots, s^{n-1}\}$ 之子羣.但,因方程式爲不可約,故 G 爲協換羣,而 $G=G'$.

例 方程式 $x^4+x^3+x^2+x+1\equiv\frac{x^5-1}{x-1}=0$ 之根爲

$$x_1=\epsilon,\ x_2=\epsilon^2,\ x_3=\epsilon^4,\ x_4=\epsilon^3,$$

此處 ϵ 表 1 之五次根內之一虛根.故

$$x_2=x_1^2,\ x_3=x_2^2,\ x_4=x_3^2,\ x_1=x_4^2.$$

又此方程式在一切有理數數統 R 內爲不可約 (§88),此可由研究次之事實而直接了解之:蓋因一次因數爲 $x-\epsilon^i$, 故爲無理因數.然由

$$x^4+x^3+x^2+x+1\equiv(x^2+ax+r)(x^2+bx+r^{-1})$$

得 $a+b=1$, $ab+r+r^{-1}=1$, $ar^{-1}+br=1$, 故

$$a=\frac{1}{2}(1\pm\sqrt{5}),\quad b=\frac{1}{2}(1\mp\sqrt{5}),\quad r=1,$$

或
$$a=\frac{r}{r+1},\quad b=\frac{1}{r+1},\quad r^4+r^3+r^2+r+1=0.$$

故所設方程式對於 R 之羣爲一循環羣.此可與§75後之習題4比較.

§87. 設 p 爲素數,則關於 1 之 p 次根之**割圓方程式**(Cyclotomic equation)爲

$$x^{p-1}+x^{p-2}+\cdots+x+1=0 \quad\cdots\cdots(22)$$

設 ε 爲(22)之一根,而 $\varepsilon^p=1, \varepsilon\neq$ 時,則

$$\varepsilon,\ \varepsilon^2,\ \varepsilon^3,\ \cdots,\ \varepsilon^{p-1} \quad\cdots\cdots(23)$$

全爲(22)之根,且各不相等,故卽爲(22)之一切根.由數論知,對於每個素數 p,必有一整數 g,其 g^m-1 當 $m=p-1$ 時可以 p 除盡,而在 m 等於較小之正整數時,則不能除盡.*此整數 g,吾人稱爲 p 之**質根**(Primitive root).於是,一組整數

$$1,\ g,\ g^2,\ \cdots,\ g^{p-2}$$

當以 p 除之時,其餘數之值必爲

$$1,\ 2,\ 3,\ \cdots,\ p-1$$

(惟次序上與此相異).於是,根(23)可列爲

$$x_1=\varepsilon,\ x_2=\varepsilon^g,\ x_3=\varepsilon^{g^2},\ \cdots,\ x_{p-1}=\varepsilon^{g^{p-2}},$$

$$\therefore\quad x_2=x_1^g,\ x_3=x_2^g,\ \cdots,\ x_{p-1}=x_{p-2}^g,\ x_1=x_{p-1}^g.$$

上之關係,乃由 g 之定義得來,例如:

$$(\varepsilon^{g^{p-2}})^g=\varepsilon^{g^{p-1}}=\varepsilon^{1+qp}=\varepsilon$$

是.故割圓方程式之根,具(21)所述之性質.故由次節之見地而言,可得次之定理:

---

*例如,設 $p=5$,則可取 $g=2$,因

$$2^1-1=1,\quad 2^2-1=3,\quad 2^3-1=7,\quad 2^4-1=15.$$

當 $p=5$ 時,本節之結果,可於§86之例見之.

定理 當 p 爲素數時,關於 1 之第 p 次虛根之割圓方程式,就有理數數統而言,乃爲 Abel 氏方程式之一種.

§88. 在有理數數統 R 內,割圓方程式(22)之不可約性.* 設令

$$x^{p-1}+x^{p-2}+\cdots+x+1=\phi(x)\cdot\psi(x),$$

此處 ϕ 及 ψ 爲低於 $p-1$ 次之整函數,而其係數爲整數者.† 命 $x=1$,則得

$$p=\phi(1)\cdot\psi(1).$$

因 p 爲素數,故其整數因子之一,設爲 $\phi(1)$,必爲 ± 1. 但因 $\phi(x)=0$ 至少必含有(22)之一根,即含有(23)內之一根,故至少必有一式 $\phi(\varepsilon^t)$ 等零.於是,

$$\phi(\varepsilon)\cdot\phi(\varepsilon^2)\cdot\phi(\varepsilon^3)\cdots\phi(\varepsilon^{p-1})=0 \quad\cdots\cdots(24)$$

對於比 p 小之任意正整數 s 而言,此組

$$\varepsilon^s,\ \varepsilon^{2s},\ \varepsilon^{3s},\ \cdots,\ \varepsilon^{(p-1)s} \quad\cdots\cdots(25)$$

除次序不同外,其內容實與(23)全同;蓋因(25)內每一數皆與(23)內之一數相等,而(25)內之數全不相同故也.否則,命

$$\varepsilon^{rs}=\varepsilon^{ts}\ (0\leqq r<p,\ 0\leqq t<p),$$

則

$$\varepsilon^{(r-t)s}=1,$$

而 $(r-t)s$ 即可以 p 除盡;因之,$r-t$ 可以 p 除盡,將使 $r=t$ 矣.故當 ε 換爲 ε^s 時,(24)仍然爲眞.故

$$\phi(x)\cdot\phi(x^2)\cdots\phi(x^{p-1})=0$$

爲一方程式,其根包括有 (23) 內各數.故此式左端可以 $x^{p-1}+$

---

*此爲 Kronecker 氏之證法;參看 Crelle, 第 29 卷. Gauss, Eisenstein (Crelle, 第 39 卷,第 167 頁), Dedekind (見 Jordan, Traité des substitutions 書中第 413–414 節)等氏各有別證.

†若爲有理數,則必爲整數(參看 Weber 氏代數學第 1 卷, 1895 年版),第 27 頁).

$x^{p-2}+\cdots+x+1$ 除盡之,即

$$\phi(x)\cdot\phi(x^2)\cdots\phi(x^{p-1})=Q(x)\cdot(x^{p-1}+x^{p-2}+\cdots+x+1),$$

此處 $Q(x)$ 爲一整函數,其係數爲整數.命 $x=1$, 得

$$[\phi(\ )]^{p-1}=[\pm 1]^{p-1}=p\cdot Q(1).$$

因 ± 1 不能以 p 除盡,故 $x^{p-1}+x^{p-2}+\cdots+x+1$ 在 R 內爲可約之假設,會引起矛盾之結果.故此式爲不可約可知.

§89. 定理　任一Abel氏方程式可以根數解之.

設Abel氏方程式爲 n 次,由§86知其羣 G 爲一 n 級之有法循環羣 $\{I, s, s^2, \cdots s^{n-1}\}$. 命 $n=p\cdot n'$, 此處 p 爲素數,並命 $s^p=s'$, 則羣

$$H=\{I, s', s'^2, \cdots, s'^{\frac{n}{p}-1}\}$$

爲 G 之子羣,其指數爲素數 p. 由§13, 因

$$s^{-\beta}s'^{\alpha}s^{\beta}=s^{-\beta}s^{\alpha p}s^{\beta}=s^{\alpha p}=s'^{\alpha},$$

故知此羣爲自配羣.是以, H 可取爲 G 之子羣系內之第二羣.再從 H 照 G 之辦法繼續做去,最後卽達到結論:

第 n 級循環羣之子羣系因子皆爲 n 之素因子,其重複之回數,亦與 n 內各素因子重複之回數同.

由§82末段之注意而言,知**任一個 n 次 Abel 氏方程式可約簡爲一組 Abel 氏方程式之連索,其各方程式之次數皆爲 n 之素因子.**

茲用歸納法證明,每個次數爲素數 p 之 Abel 氏方程式可以根數解之之定理.先設次數爲素數而小於 p 時, Abel 氏方程式皆可用根數解之.則此等可用根數解之方程式內,必含有從求 1 之第 p 次虛根而用之 $p-1$ 次Abel氏方程式引出之次數爲素數之Abel氏方程式(§87).此後者既爲已知,則每個 p 次之 Abel 氏方程式卽可用根數解出矣(§83). 然吾人已知二次之

Abel 氏方程式可以用根數解之,故一般任意次 Abel 氏方程式可以用根數解之,而歸納法證明之手續卽告完全.

系 設 p 爲素數,則 1 之所有第 p 次根可由施以有限回之求一已知量之一個方根之演算而得之.其每個根數之指數乃爲 $p-1$ 之素數因子中之一.

§90. 引 設 p 爲素數,又設 A 爲數統 R 內之一量非爲 R 內他量之第 p 乘冪者,則 x^p-A 在 R 內爲不可約.

蓋若 x^p-A 在 R 內爲可約,

$$x^p-A=\phi_1(x)\cdot\phi_2(x)\cdots,$$

則各個因子欲其次數相同時,只有其次數皆爲 1 次,此因 1 爲 p 之唯一除數也.然在此種情狀之下,方程式各根將全爲 R 內之數矣.但,此與假設相矛盾,故不成立.次設 ϕ_1 之次數比 ϕ_2 高命

$$\phi_1(x)=(x-x'_1)\cdots(x-x'_{n_1}),\ \phi_2(x)=(x-x''_1)\cdots(x-x''_{n_2}),$$

而 $n_1-n_2>0$, 則因 $x^p-A=0$ 之根爲

$$x_1,\ \omega x_1,\ \omega^2x_1,\ \cdots,\ \omega^{p-1}x_1 \qquad (26)$$

此處 ω 爲 1 之第 p 次虛根,故上之乘積內,其最後係數必爲

$$\pm x'_1x'_2\cdots x'_{n_1}=\pm\omega^{\sigma_1}x_1^{n_1},\ \pm x''_1x''_2\cdots x''_{n_2}=\pm\omega^{\sigma_2}x_1^{n_2}.$$

但此最後係數及其商 $\pm\omega^{\sigma}x_1^{m}$(此處 $m=n_1-n_2>0$) 皆在 R 內.因 p 及 m 爲互素數,故能求得整數 μ 及 ν, 使

$$m\mu-p\nu=1,$$

$$\therefore\ (\omega^{\sigma}x_1^{m})^{\mu}=\omega^{\sigma\mu}x_1^{p\nu+1}=\omega^{\sigma\mu}A^{\nu}x_1=A^{\nu}x',$$

此處 x' 爲 (26) 內之一根.所以 $A_{\nu}x'$, 以至於 x' 自身,皆爲 R 內之數.故 A 等於 R 內一量 x' 之第 p 乘冪.此亦與假設相矛盾,故 x^p-A 必爲不可約.

§91. 定理 次數爲素數 p 之二項方程式(Binomial equation)

$$x^p-A=0$$

可以一組次數爲素數之Abel氏方程式之連索解之.

命R爲所設數統,A屬於其中.以ω附益之,命此擴大數統爲R'.則根(26)能滿足§85之(21)形狀之關係:

$$x_2=\omega x_1,\ x_3=\omega x_2,\ \cdots,\ x_p=\omega x_{p-1},\ x_1=\omega x_p,$$

此時$\theta(x)$爲有理函數ωx.由§90內之討論,知x^p-A非在此擴大數統R'內仍爲不可約,即其所有之根全屬R'內.就前者而言,$x^p-A=0$其就R'之羣乃一有法循環羣(§86).若就後者而言,則其就R'之羣乃爲幺羣.但,ω自身乃由一Abel氏方程式求來(§87),故不論屬於此兩情形中之何種情形,$x^p-A=0$皆賴一組Abel氏方程式之連索解之,而此組內各方程式之次數可假定其皆爲素數(§89).

第 九 章

判斷能用代數解之標準

§92. 茲今於此章將任意所設 n 次方程式

$$f(x)=0 \cdots\cdots (1)$$

代數解法之理論續完.在 §84 內,業用羣之性質,將(1)可用代數解之之充分條件證出矣.今若欲證明此性質同時亦爲(1)能用代數解之之必需條件,可從方程式(1)之討論出發,而假設(1)可以根數解之,卽假定(§50)(1)之根 $x_1, x_2, \cdots, x_n$ 可從原所設量 R', R'', …施以加減乘除及求任意次方根等運算而導出者.開方之根指數,可假定其爲素數.設 $\xi, \eta, \cdots, \psi$ 表示見於根 $x_1, x_2, \cdots, x_n$ 內之所有根數,則其解法可由一組次數爲素數之二項方程式之連索列出:

$$\xi^{\lambda}=L(R', R'', \cdots),$$
$$\eta^{\mu}=M(\xi, R', R'', \cdots),$$
$$\cdots\cdots,$$
$$\psi^{\rho}=P(\cdots, \eta, \xi, R', R'', \cdots),$$
$$x_i=R_i(\psi, \cdots, \eta, \xi, R', R'', \cdots) \quad (i=1, \cdots, n),$$

此處 $L, M, \cdots, P, R_i$ 乃係數爲整數之有理函數,而上面所書之 ξ, η, …,間可缺去一、二.由 §91, 知每一個此等二項方程式,以至全部連索內之方程式,皆可以一組次數爲素數之 Abel 氏方程式之連索替換之:

$\Phi(y; R', R'', \cdots)=0$, 對於數統 R 之 Abel 氏方程式;
$\Psi(Z; y, R', R'', \cdots)=0$, 對於 (y, R) 之 Abel 氏方程式;
……, ……;

$\Theta(w;\cdots,z,y,R',R'',\cdots)=0$ 對於$(\cdots,z,y,R)$之 Abel 氏方程式;

$x_i=\Omega_i(w,\cdots,z,y,R',R'',\cdots)\qquad(i=1,2,\cdots,n).$

茲由解第一個 Abel 氏方程式 $\Phi(y)=0$ 出發,而附益一根(命爲 y)於原數統 R;此時,(1)之羣 G 化簡爲某一子羣,茲以 H 表之 ($H=G$,自亦可能)(§74).然後,吾人解第二個 Abel 氏方程式. $\Psi(Z)=0$, 而附益其一根 (命爲 z) 於擴大數統 (y,R),而羣 H 亦化簡爲其某一子羣,茲以 J 表之 ($J=H$,亦屬可能). 照此進行,直至將最後方程式 $\Theta(w)=0$ 解出,並將其一根(命爲 w)附益於前得之擴大數統時,遂得一數統 $(w,\cdots,z,y,R)$. 此時,因一切根 x_i 在此數統內,故(1)對於此數統之羣爲么羣 G_1.

在此等陸續附益中,每施一次附益,則方程式(1)之羣或仍不能化簡,否則必化簡爲素數指數之自配子羣.此定理爲 Galois 氏所發見,卽爲次節之系.若以與 §75 相對照,可見出此定理所指之每附益量,並無假定其爲根之有理函數.以是,遂導出曾經 Abel 氏發見之關於可解方程式根式內所見之無理性性質上之緊要結論(§94),其重要可知矣.

由 Galois 氏此定理知,所設可解方程式化簡爲一組 Abel 氏方程式之連索時,吾人每次將組中各方程式之根陸續附益於數統,遂將方程式之羣次第約簡.此等約簡之羣,必造成所設方程式之羣 G 之子羣系,此子羣系因數必僅爲素數.蓋因此組以 G 始以么羣 G_1 終之子羣系內,每一羣皆爲前一羣之指數爲素數之自配子羣.故所設方程式能用代數解之之充分條件 (§84),同時亦爲其必需條件.因得 **Galois 氏判定能用代數解之標準** (Galois' criterion for algebraic solvability) 爲:

欲一個方程式可以根數解之之必需且充分條件 (Necessary and sufficient condition) **乃所設方程式之羣有一子羣系,其**

子羣系因子全爲素數者.

§93. 經 Hölder 氏*推廣並證明之 Jordan 氏定理† 設就一所設數統 R,附益以方程式 $F_2(x)=0$ 之一切根後,方程式 $F_1(x)=0$ 之羣 G_1 化簡爲 G_1'.又設 R 附益以方程式 $F_1(x)=0$ 之一切根後,方程式 $F_2(x)=0$ 之羣 G_2 化簡爲 G_2'.則 G_1' 及 G_2' 必各爲 G_1 及 G_2 之自配子羣,且商羣 G_1/G_1' 及 G_2/G_2' 必成簡單同形.

設 $\psi_1(\xi_1, \xi_2, \cdots, \xi_n)$ 乃方程式 $F_1(x)=0$ 之根之有理函數,其係數在 R 內,設此函數屬於 $F_1(x)=0$ 之羣 G_1 之子羣 G_1'(§70). 由假設,吾人將 $F_2(x)=0$ 之根 $\eta_1, \eta_2, \cdots, \eta_m$ 附益於 R 後,羣 G_1 即化簡爲 G_1' 故 ψ_1 在擴大數統內,而

$$\psi_1(\xi_1, \xi_2, \cdots, \xi_n)=\phi_1(\eta_1, \eta_2, \cdots, \eta_m) \cdots\cdots\cdots\cdots (27)$$

此處有理函數 ϕ_1 之係數乃在 R 內.

設以 $\psi_1, \psi_2, \cdots, \psi_k$ 表 ψ_1 在 G_1 之(對於文字爲 $\xi_1, \xi_2, \cdots, \xi_n$ 之)代換下所取一切絕對值不等之值,則 G_1' 乃在 G_1 下指數爲 k 之子羣(§71).又設 $\phi_1, \phi_2, \cdots, \phi_l$ 表 ϕ_1 在 G_2 之(對於文字爲 $\eta_1, \eta_2, \cdots, \eta_m$ 之)代換下所取絕對值不相等之一切值,則 ψ 之 k 個量乃爲一不可約方程式在 R 內之根(§71). 同樣,ϕ 之 l 個量亦爲一不可約方程式在 R 內之根.因此,兩不可約方程式有一公根 $\psi_1=\phi_1$,故此兩方程式必全相等 (§55, 系 2). 於是,$\psi_1, \psi_2, \cdots, \psi_k$ 必與 $\phi_1, \phi_2, \cdots, \phi_l$ 按某次序排列之結果全同.其特例爲 $k=l$.

設 s_i 爲 G_1 內之一個代換,將 ψ_1 換爲其相配函數 ψ_i 者.則 s_i 將 ψ_1 所屬之羣 G_1' 變爲與 G_1' 同級之 ψ_i 所屬之羣.但,ψ_i 等於 ϕ 之一個量,必在數統 $R'\equiv(R; \eta_1, \cdots, \eta_m)$ 內.故施以方程式 $F_1(x)=0$

---

*見 Math. Annalen (算學年報),第 34 卷.

†見 Traité des substitutions et des équations algébriques (代數方程式論及代換論),第 269, 270 兩頁.

就數統 R' 之羣 G_1' 內之代換,不生變更 (§61, 特性 B). 是以, ψ_i 之羣包括 G_1' 之一切代換;然又與 G_1' 之級相同,故 ψ_i 之羣與 G_1' 全相同.於是 G_1' 在 G 下爲自配子羣,而滿足 ψ_1 之不可約方程式之羣;故爲商羣 G_1/G_1' (§79).

設 H_2 爲 G_2 之子羣,而函數 $\phi_1(\eta_1, \eta_2, \cdots, \eta_m)$ 屬之.因 ϕ_1 爲在 R 內不可約之 $l=k$ 次方程式之根,故羣 H_2 爲在 G_2 下指數爲 k 之羣 (§71). 若附益以 ϕ_1 [由 (27), 吾人亦可以 ψ_1 附益之], 則方程式 $F_2(x)=0$ 對於 R 之羣 G_2 卽化簡爲 H_2 (§75). 設吾人不但附益以 $\psi_1(\xi_1, \xi_2, \cdots, \xi_n)$ 且將所有 $\xi_1, \xi_2, \cdots, \xi_n$ 附益於 R, 則羣 G_2 或不止化簡爲 H_2, 而可更化簡至 H_2 之子羣;故 G_2' 含於 H_2 內.於是,吾人得一初步結果:設 $F_1(x)=0$ 之羣,經附益以 $F_2(x)=0$ 之一切根後,化簡至指數爲 k 之子羣,則 $F_2(x)=0$ 之羣,經附益以 $F_1(x)=0$ 之一切根後,亦必化簡至指數爲 $k_1((k_1 \geqq k)$ 之一子羣.

將上面對於 F_1 及 F_2 之說法互換,則得其結果爲:設 $F_2(x)=0$ 之羣,經附益以 $F_1(x)=0$ 之一切根後,化簡至指數爲 k_1 之子羣;則 $F_1(x)=0$ 之羣,經附益以 $F_2(x)=0$ 之一切根後,化簡至指數爲 k_2 $(k_2 \geqq k_1)$ 之子羣.因對於後者說法之假設與前者說法之終結全同,故

$$k_2=k, \quad k_1 \geqq k, \quad k_2 \geqq k_1,$$

故 $k_1=k$. 於是,定理內之羣 G_2' 與使 ϕ_1 不變之 G_2 內一切代換之羣 H_2 全同.由是知 G_2' 在 G_2 下爲自配子羣(同理, G_1' 在 G_1 下亦爲自配子羣). 故在 R 內,滿足 ϕ_1 之不可約方程式之羣必爲商羣 G_2/G_2'.

然在 R 內,此兩個滿足 ϕ_1 及 ψ_1 之不可約方程式,業已證其爲全同.故羣 G_1/G_1' 及 G_2/G_2' 僅在其施運算之文字記法上之不同,故成簡單同形.

系 在特例,若 $F_2(x)=0$ 爲一素數 p 次之 Abel 氏方程式時,則方程式所有之根皆爲任一根在 R 內之有理函數.故附益以一根,即等於附益以一切根.於是:**吾人附益以素數 p 次之 Abel 氏方程式之任一根時,則所設方程式 $F_1(x)=0$ 之羣,非仍不化簡,即化簡至指數爲 p 之自配子羣.**

§94. 設 G_2 爲簡單羣,又設經附益後能使 G_2 化簡時,則 G_2 即化簡爲么羣.故 ϕ_1 所屬之羣 $G_2'=H_2$ 爲一么羣.故 $F_2(x)=0$ 之根 $\eta_1,\eta_2,\cdots,\eta_m$ 爲 ϕ_1 在 R 內之有理函數(§72).由(27)知其亦爲 $F_1(x)=0$ 之根 $\xi_1,\xi_2,\cdots,\xi_n$ 在 R 內之有理函數.

設一方程式 $F_1(x)=0$ 對於數統 R 之羣,經附益以方程式 $F_2(x)=0$ 之一切根而化簡,而 $F_2(x)=0$ 就 R 之羣爲簡單羣時,則 $F_2(x)=0$ 之一切根爲 $F_1(x)=0$ 之根(就數統 R)之有理函數.

因可解方程式 $f(x)=0$ 之羣有一子羣系,且其子羣系因子全爲素數,故方程式可以一組豫解式替換之,組內各式皆爲素數次數之 Abel 氏方程式(§82 之末段及§85).當吾人每次附益以每個豫解式之一根時,則方程式之羣即被化簡.但,豫解式之羣爲簡單羣,且爲一素數次數之循環羣.故每個 Abel 氏豫解式之根,全爲 $f(x)=0$ 之根之有理函數.但,見於素數次數之 Abel 氏方程式解法內之根數,可以方程式之根及 1 之第 p 次虛根之有理函數表之(§83).

$$\sqrt[p]{\theta_1}=x_0+\omega x_1+\omega^2 x_2+\cdots+\omega^{p-1}x_{p-1},\cdots,$$

故亦可以 $f(x)=0$ 之根及 1 之第 p 次根之有理函數表之.於是,得 Abel 氏定理如次:

一個代數可解方程式(Algebraically solvable equation)之解法,常可藉一組素數次數之二項方程式之連索而實現之,其根可列爲所設方程式之根及 1 之某次方根之有理函數.

故一個代數可解方程式之根之形狀,必其所含之一切根數可以列爲方程式之根及 1 之某次方根之有理函數.此結果在普通二次,三次及四次方程式之場合, Lagrange 氏曾首由經驗指出(參看第一章).

Abel 氏定理既經證明,則從前對於普通 $n>4$ 次方程式不能用代數解之證明(§48),到此完全成功.

§95. 欲解釋 Galois 氏理論,茲用 Abel 氏方程式之連索以列出普通三次及四次方程式之代數解法.

先就三次方程式 $x^3-c_1x^2+c_2x-c_3=0$ 言之.命有理性數統爲 $R=(c_1,c_2,c_3)$.則三次方程式就 R 之羣爲對稱羣 G_6 (§64).函數

$$\Delta=(x_1-x_2)(x_2-x_3)(x_3-x_1)$$

屬於子羣 G_3.由 §2 後之習題 3 知,Δ 爲方程式

$$\Delta^2=c_1^2c_2^2+18c_1c_2c_3-4c_2^3-4c_1^3c_3-27c_3^2 \quad \cdots\cdots (28)$$

之一根,其第二根 $-\Delta$ 乃爲第一根 Δ 之有理函數.且對於普通之 c_1,c_2,c_3 而 Δ 之值非在 R 內,故(28)爲不可約方程式.於是,爲一 Abel 氏方程式(§85).以 Δ 附益於 R,則羣卽化簡爲 G_3 (§75).試解 Abel 氏方程式 $\omega^2+\omega+1=0$ (§87) 而附益 ω 於數統 (Δ,R),則函數

$$\psi_1=x_1+\omega x_2+\omega^2x_3$$

之係數屬於擴大數統 $R'=(\omega,\Delta,c_1,c_2,c_3)$.由 §34, ψ_1^3 有一值在 R' 內,卽

$$\psi_1^3=\frac{1}{2}[2c_1^3-9c_1c_2+27c_3-3(\omega-\omega^2)\Delta].$$

此二項方程式爲一個就數統 R' 內之 Abel 氏方程式(§91).以 ψ_1 附益後,三次方程式之羣卽化簡爲幺羣.於是, x_1,x_2,x_3 在數統

$(\psi_1, \omega, \Delta, c_1, c_2, c_3)$ 內.由 §34, 得

$$x_1=\frac{1}{3}\left(c_1+\psi_1+\frac{{c_1}^2-3c_2}{\psi_1}\right),\quad x_2=\frac{1}{3}\left(c_1+\omega^2\psi_1+\omega\frac{({c_1}^2-3c_2)}{\psi_1}\right).$$

但,吾人亦可不用附益 ω 而解三次方程式.蓋在數統 (Δ, c_1, c_2, c_3) 內,因三次方程式之羣 G_3 爲循環羣 (§85), 故三次方程式自身爲一 Abel 氏方程式.將此 Abel 氏方程式之一根 x_1 附益之,則羣卽約簡爲么羣,而 x_2 及 x_3 必在此數統 $(x_1, \Delta, c_1, c_2, c_3)$ 內. Serret 氏於其所著高等代數學(Algèbre supérieure) 第 2 卷,第 511 節內,曾將此 x_2 及 x_3 之式求出,爲

$$x_2=\frac{1}{2\Delta}\{(6c_2-2{c_1}^2){x_1}^2+(9c_3-7c_1c_2+2{c_1}^3-\Delta)x_1$$
$$+4{c_2}^2-{c_1}^2c_2-3c_1c_3+c_1\Delta\},$$

及

$$x_3=\frac{1}{2\Delta}\{(6c_2-2{c_1}^2){x_1}^2+(9c_3-7c_1c_2+2{c_1}^3+\Delta)x_1$$
$$+4{c_2}^2-{c_1}^2c_2-3c_1c_3-c_1\Delta\}.$$

§96. 就普通四次方程式 $x^4+ax^3+bx^2+cx+d=0$ 而言,此方程式對於數統 $R=(a, b, c, d)$ 之羣爲 G_{24}. 函數

$$\Delta=(x_1-x_2)(x_1-x_3)(x_1-x_4)(x_2-x_3)(x_2-x_4)(x_3-x_4)$$

屬於子羣 G_{12}. 因 Δ^2 爲 a, b, c, d 之整函數,且其係數爲有理數 (§42),故可解一個(對於 R 爲 Abel 氏方程式之)方程式而得 Δ. 經附益以 Δ 後,方程式之羣化簡爲 G_{12}. 又函數 $y_1=x_1x_2+x_3x_4$ 屬於 G_{12} 之子羣 G_4,而此函數滿足一個三次豫解式(§4).

$$y^3-by^2+(ac-4d)y-a^2d+4bd-c^2=0 \quad\cdots\cdots(16)$$

此豫解式就數統 (Δ, a, b, c, d) 之羣爲一個第 3 級之循環羣(§79, 系).故此豫解式爲 Abel 氏方程式.若附益以 y_1,則四次方程式之羣化簡爲 G_4. 又函數 $t=x_1+x_2-x_3-x_4$ 屬於 G_4 之子羣 G_2,其值可由 Abel 氏方程式(§5)

$$t^2=a^2-4b+4y_1 \quad\cdots\cdots(23)$$

決定之.再附益以 t 後,方程式之羣卽化簡爲 G_2. 此時, x_1 卽屬於 G_2 之么子羣 G_1, 且爲 §4 之 (17).

$$x^2+\frac{1}{2}(a-t)x+\frac{1}{2}y_1-(\frac{1}{2}ay_1-c)/t=0$$

之一根.經附益以此 Abel 氏方程式之一根 x_1 後,羣卽化簡爲么羣 G_1. 於是(§72),一切根皆在數統 $(x_1, t, y_1, \Delta, a, b, c, d)$ 內.此可由 $x_1+x_2=-\frac{1}{2}(a-t)$, 及

$$x_3+x_4=x_1+x_2-t, \quad x_3-x_4=(y_2-y_3)\div(x_1-x_2)$$

知之,此處 y_2 及 y_3 (已證於 §85 之末段) 可以 y_1, Δ 及 (16) 之係數等之有理函數表之.實際上,由 §7,吾人知 $(y_1-y_2)(y_2-y_3)(y_1-y_3)$ 之值爲 Δ.

§97. 解普通四次方程式之別法已見於 §42. 設 ω 表 1 之虛立方根之一,則所設方程式對於數統 $R=(\omega, a, b, c, d)$ 之羣爲 G_{24} (§64). 經附益以 Δ 後,羣卽化簡爲 G_{12}. 命

$$y_1=x_1x_2+x_3x_4, \quad y_2=x_1x_3+x_2x_4, \quad y_3=x_1x_4+x_2x_3,$$

則函數 $\phi_1=y_1+\omega y_2+\omega^2 y_3$ 屬於自配子羣 G_4. 於是, ϕ_1 爲 x_1, x_2, x_3, x_4 之有理函數,其係數在 R 內.由 42,

$$\phi_1{}^3=\frac{3}{2}(\omega-\omega^2)\Delta-216J,$$

故 ϕ_1 乃由對於數統 $(\Delta, \omega, a, b, c, d)$ 成 Abel 氏方程式之方程式決定之.故,由 §42, y_1, y_2, y_3 屬於擴大數統 $(\phi_1, \Delta, \omega, a, b, c, d)$.

經附益以二項 Abel 氏方程式 (29) 之一根 t 後,羣卽化簡爲 G_2. 再經附益* 以 $i=\sqrt{-1}$ 及一個二項二次方程式 (§42) 之一根

*若不附益以 i 及 V, 吾人亦可由 $t_2{}^2=a^2-4b+4y_2$ 以決定 $t_2=x_1+x_3-x_2-x_4$. 因 $t_1t_2t_3=4ab-8c-a^3$ [§36之(39)], 此處 $t_1=t$, 故 $t_3=x_1+x_4-x_2-x_3$ 亦爲已知.於是

$$x_1=\frac{1}{4}(-a+t_1+t_2+t_3), \quad x_2=\frac{1}{4}(-a+t_1-t_2-t_3), \cdots.$$

$V=x_1-x_2+ix_3-ix_4$ 後,羣復化簡至么羣 G_1. 此時, x_1, x_2, x_3, x_4 列爲 t, V, i 及 a 之函數之式,卽爲§37 內之(41)及其附帶之關係(40).

第十章

準循環方程式　Galois 氏方程式

§98. 代換之解析表示　已知任意代換

$$s=\begin{pmatrix} x_0 & x_1 & x_2 & \cdots & x_{n-1} \\ x_a & x_b & x_c & \cdots & x_k \end{pmatrix},$$

此處 $a, b, c, \cdots, k$ 乃爲 $0, 1, 2, \cdots, (n-1)$ 之一種排列,則吾人能作一個 z 之函數 $\phi(z)$,滿足次之關係:

$$\phi(0)=a,\ \phi(1)=b,\ \phi(2)=c,\ \cdots,\ \phi(n-\ )=k.$$

此種函數可由 Lagrange 氏推值公式(Interpolatio -Formula)得之:

$$\phi(z)=\frac{aF(z)}{zF'(0)}+\frac{bF(z)}{(z-1)F'(1)}+\cdots+\frac{kF(z)}{(z-n+1)F'(n-1)},$$

式中 $F(z)\equiv z(z-1)(z-2)\cdots(z-n+1)$ 而 $F'(z)$ 表 $F(z)$ 之導微函數(Derivative). 於是,代換 s 可以解析表示之如次:

$$s=\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix}.$$

設吾人祇研究 n 爲素數 p 之場合.且命 $x_z=x_{z+p}=x_{z+2p}=\cdots$,則(如 §86)循環代換 $t=(x_0x_1x_2\cdots x_{p-1})$ 可以

$$t=\begin{pmatrix} x_z \\ x_{z+1} \end{pmatrix}$$

表之.

設 G 爲就 $x_0, x_1, \cdots, x_{p-1}$ 之最大代換羣,而循環羣 $H=\{I, t, t^2, \cdots, t^{p-1}\}$ 在 G 下爲自配子羣時,則 G 之普通代換 g 及 H 之普通代換 h 可以

$$g=\begin{pmatrix} x_z \\ x_{\phi(z)} \end{pmatrix},\qquad h=\begin{pmatrix} x_z \\ x_{z+a} \end{pmatrix}=t^a$$

表之.由假設,$g^{-1}tg$ 屬於 H,故其形爲 ^{a}

$$g^{-1}=\begin{pmatrix} x_{\phi(z)} \\ x_z \end{pmatrix},\quad g^{-1}t=\begin{pmatrix} x_{\phi(z)} \\ x_{z+1} \end{pmatrix},\quad g^{-1}tg=\begin{pmatrix} x_{\phi(z)} \\ x_{\phi(z+1)} \end{pmatrix}$$

但,t^{a} 將 $x_{\phi(z)}$ 換爲 $x_{\phi\phi(z)+a}$.故必

$$x_{\phi(z+1)}=x_{\phi(z)+a}.$$

陸續命 $z=0,1,2,\cdots$,並命 $\phi(0)=b$,則得

$$x_{\phi(1)}=x_{b+a},\quad x_{\phi(2)}=x_{\phi(1)+a}=x_{b+2a},\quad x_{\phi(3)}=x_{\phi(2)+a}=x_{b+3a},\cdots$$

由簡單歸納法知,凡 z 爲整數時,$x_{\phi(z)}=x_{b+za}$.故

$$g=\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix} \qquad \cdots(30)$$

此處 a 及 $b\equiv\phi(0)$ 皆表整數.因 $g^{-1}tg$ 非么代換,故 a 不能以 p 除盡.於是,g 之不同代換*可由命

$$a=1,2,\cdots,(p-1);\quad b=0,1,2,\cdots(p-1)$$

得之.如此之 $(p-1)$ 個代換構成一羣,稱爲**p次之準循環羣**†(Metacyclic group of degree p).此可由其來源或由

$$\begin{pmatrix} x_z \\ x_{az+b} \end{pmatrix}\begin{pmatrix} x_z \\ x_{cz+d} \end{pmatrix}=\begin{pmatrix} x_z \\ x_{a(cz+b)+d} \end{pmatrix}\equiv\begin{pmatrix} x_z \\ x_{ac\,z+(ba+\beta)} \end{pmatrix}$$

得之.

注意 準循環羣內週期爲 p 之唯一循環代換乃 t 之各乘冪.當 $a=1$,(30)變爲 t^{b};當 $a\neq1$,則(30)使一根不變,此根乃其指

---

*因 $b,a+b,a+b,\cdots(p-1)a+b$ 以 p 除之,其餘數之值乃 $0,1,2,\cdots(p-1)$ 按某次序排列者.故(30)決定出文字爲 $x_0,x_1,\cdots,x_{p-1}$ 之代換

$$\begin{pmatrix} x_0 & x_1 & x_2 & \cdots \\ x_b & x_{a+b} & x_{2a+b} & \cdots \end{pmatrix}.$$

欲加徵實,可證其餘數全不相同即可.

†此名詞乃 H. Weber 氏於其所著之代數學 (Lehrbuch der Algebra) 內創用之.參看此書之 1895 年版內之第 593 頁.—— 譯者.

數 z 能使 $az+b$ 及 z 相差爲 p 之倍數者.

§99. 設方程式之羣 G 對於數統 R 爲 p 次之準循環羣時,則此方程式稱爲 **p 次之準循環方程式**(Metacyclic equation of degree p). 因 G 爲協換羣(其循環子羣 H 爲協換羣),故其方程式爲不可約.又其一切根全爲其中二個根之有理函數(其係數在 R 內),此因經附益以兩根(設爲 x_u 及 x_v) 後,則方程式之羣化簡爲么羣故也.蓋若 g 使 x_u 及 x_v 不變時,則

$$(au+b)-u,\quad (av+b)-v$$

必爲 p 之倍數,於是其差 $(a-1)(u-v)$ 亦爲 p 之倍數.故 $a=1$,而 $b=0$. 故惟有么羣使 x_u 及 x_v 不變也.

定義　就數統 R,一個次數爲素數之不可約方程式,其根全爲其中二根之有理函數時,此方程式稱爲 **Galois 氏方程式** (Galoisian equation).

故一個準循環方程式爲一 Galois 氏方程式.

§100. 反之,設與吾人一個素數 p 次之 Galois 氏方程式,則吾人卽能決定其對於數統 R 之羣 G. 此方程式爲不可約,而其羣爲協換羣,故 G 之級可以 p 除盡(§67). 故 G 包含 p 級之循環子羣 H(參看 §27 之註). 命 x_0 及 x_1 爲方程式之二根,而各根可列爲此二根之有理函數者.則在週期爲 p 之任一循環代換之乘冪內,必有換 x_0 爲 x_1 之一代換,故將其餘諸根予以適當記法後,吾人可設 H 含有代換

$$t=(x_0x_1x_2\cdots x_{p-1}).$$

欲證 H 在 G 下爲自配子羣,可證含於 G 之任一循環代換

$$r=(x_{i_0}x_{i_1}x_{i_2}\cdots x_{i_{p-1}})$$

必等於 t 之某乘冪卽可.蓋如此則 t 施以 G 之代換後,仍得屬於 H 之代換也(§40). 因在 r 內每相隣兩文字均不相同,故 i_{z+1}

$-i_z$ 決不爲 p 之倍數,故從 $0,1,2,\cdots,p-1$ 內,至少必能選出 z 之兩個值 μ 及 ν,使以 p 除後所得之餘數相同.於是,

$$x_{i_{\mu+1}-i_\mu}=x_{i_{\nu+1}-i_\nu},\quad (\text{設令}=x_k).$$

因 r 等於將 x_0 換爲 x_1 之循環代換之某乘冪,故吾人可假定 $i_0=0$, $i_1=1$. 於是,由假設得

$$x_{i_\alpha}=\theta_\alpha(x_{i_0},\ x_{i_1})\ (\alpha=0,1,\cdots\ p-1),$$

此處 θ_α 爲一有理函數,其係數在 R 內.將羣 G 內之代換 $r^\mu t^{-i_\mu}$ 及 $r^\nu t^{-i_\nu}$ 施於此等有理關係,則由 §62 得

$$x_{i_{\alpha+\mu}-i_\mu}=\theta_\alpha(x_0,x_k),\qquad x_{i_{\alpha+\nu}-i_\nu}=\theta_\alpha(x_0,x_k).$$

故兩式左端之下標(Subscript)相等,而

$$i_{\alpha+\mu}-i_{\alpha+\nu}=i_\mu-i_\nu=c\quad(\alpha=0,\ 1,\ \cdots,\ p-1),$$

式中曾將 p 之倍數省去.故 r 內每個下標較在其前之第 $\mu-\nu$ 個下標多 c. 於是,r 等於 t 之某乘冪.

因 G 有一自配循環子羣 H, 故含於 p 次之準循環羣內 (§98).

一個素數 p 次子 Galois 氏方程式之羣乃 p 次準循環羣內之子羣.

§101. 一個準循環方程式可用兩個 Abel 氏方程式所成之連索解之.設 $\psi=R(x_0,x_1,\cdots,x_{p-1})$ 屬於 G 之子羣 H, 則

$$\psi_1=\psi,\quad \psi_2=R(x_0,x_2,x_4,\cdots,x_{2p-2}),\quad \cdots,$$

$$\psi_{p-1}=R(x_0,x_{p-1},x_{2p-2},\cdots,x_{(p-1)^2})$$

爲 ψ 在 G 下之 $p-1$ 個之值.但,ψ_i 經施以換 x_z 爲 x_{kz} 之代換後,即變爲 ψ_{ki}. 故 ψ 之 $p-1$ 個值,在 G 之 $p(p-1)$ 個代換之下,亦成循環排列.故豫解式

$$(w-\psi_1)(w-\psi_2)\cdots(w-\psi_{p-1})=0$$

之羣爲一個 $p-1$ 級之循環羣.故此豫解式爲一個 Abel 氏方程

式(§85).經以 ψ 附益後,原來方程式之羣化簡爲循環羣 H.於是,在擴大數統內亦爲 Abel 氏方程式.

此法亦可施於任一 Galois 氏方程式,其羣 G 爲準循環羣之子羣,且含 H 爲其子羣,故 G 之級爲 pd,此處 d 爲 $p-1$ 之一個除數.故此兩個輔助 Abel 氏方程式其次數爲 d 及 p.應用 §89,得次之結果.

一個 Galois 氏方程式可以一組素數次數之 Abel 氏方程式之連索解之.故此種方程式可以根數解之.

例 1. 設 A 爲所設數統 R 內之一量,但不等於 R 內之量之第 p 次乘羃.則

$$x^p-A=0$$

在 R 內爲不可約 (§90). 其根爲

$$x_0,\quad x_1=\omega x_0,\quad x_2=\omega^2 x_0,\quad \cdots,\quad x_{p-1}=\omega^{p-1}x_0.$$

此時一切根可列爲 x_0 及 x_1 之有理函數:

$$w_i=\left(\frac{x_1}{x_0}\right)^i x_0 \quad (i=0,\ 1,\ \cdots,\ p-1).$$

故此方程式爲一 Galois 氏方程式.因函數 ψ 屬於循環子羣 H, 故可取

$$\frac{x_1}{x_0}=\frac{x_2}{x_1}=\cdots\cdots=\frac{x_0}{x_{p-1}}=\omega.$$

豫解式 $\omega^{p-1}+\omega^{p-2}+\cdots+\omega+1=0$ 確爲一 Abel 氏方程式 (§87). 故經附益以 ω 後, $x^p-A=0$ 即變爲一個 Abel 氏方程式 (§91).

例 2. 求解五次方程式 (Quintic equation)*

$$y^5+py^3+\frac{1}{5}p^2y+r=0 \qquad (e)$$

命 $y=z-\frac{p}{5z}$, 則 (試與 §2 之三次方程式解法相比較)

$$z^5-\frac{p^5}{5^5z^5}+r=0.$$

*與 Dickson 氏 College Algebra 第 189 頁及第 193 頁相比較.

$$\therefore\ z^5=-\frac{r}{2}+\sqrt{Q},\qquad Q\equiv\frac{r^2}{4}+\left(\frac{p}{5}\right)^5.$$

設 ϵ 爲 1 之第 5 次虛根,則 (θ) 之根爲

$$y_1=A+B,\ y_2=\epsilon A+\epsilon^4 B,\ y_3=\epsilon^2 A+\epsilon^3 B,\ y_4=\epsilon^3 A+\epsilon^2 B,\ y_5=\epsilon^4 A+\epsilon B,$$

此處

$$A=\sqrt[5]{-\frac{r}{2}+\sqrt{Q}},\qquad B=\sqrt[5]{-\frac{r}{2}-\sqrt{Q}}.$$

此 A、B 兩式,吾人易知其可列爲 y_1 及 y_2 之一次函數.故 y_3, y_4, y_5 爲 y_1 及 y_2 之有理函數,其係在數數統 $R=(\epsilon, p, r)$ 內.因方程式 (θ) 之根無一個在 R 內,又因其在 R 內無二項因子(此可由根之形式知之),故對於普通 p 及 r 之值,方程式 (θ) 在 R 內爲不可約.故 (θ) 爲 Galois 氏方程式.

§102. 引 設 L 爲 K 之自配子羣之一,其指數爲素數 ν,又設 k 爲 K 之任意一代換不含於 L 內者,則 k^ν 屬於 L,且 k 別無比 ν 更低之乘冪能屬於 L 者;又 k 之週期可以 ν 除盡.

由 §79 之系,知商羣 K/L 爲一循環羣

$$\{I, \gamma, \gamma^2, \cdots, \gamma^{\nu-1}\}.$$

故 γ 必有一乘冪(命爲 γ^κ),與 k 相對應,此處 κ 不能以 ν 除盡.於是,$(\gamma^\kappa)^\nu=I$ 與 k^ν 成對應,故 k^ν 屬於 L.設 $0<m<\nu$,則因 $(\gamma^\kappa)^m=I$ 需要 κm 能用素數 ν 除盡,故 k^m 不屬於 L.

設 k 之週期 μ 可列爲

$$\mu=q\nu+\tau\quad(0\leqq\tau<\nu)$$

之形.因 $k^\nu=h$ 爲 L 之一代換,故得 $I=k^\mu=h^q k^\tau$.故 $k^\tau=h^{-q}$.由以前關於 k 之乘冪之結論,得 τ 如 $=0$.故 μ 可以 ν 除盡.

§103. Galois 氏定理 每個素數 p 次之不可約方程式可以根數解之者乃一 Galois 氏方程式.

設 G 爲方程式就數統 R 之羣,又設

$$G, H, \cdots, J, K, L, \cdots, G_1 \cdots\cdots\cdots\cdots\cdots\cdots (31)$$

爲 G 之子羣系.因方程式可以根數解之,故子羣系因子全爲素數(§92).因方程式在 R 內爲不可約,故 G 爲協換羣(§68).故其級可以 p 除盡(§67).故(§27 之註) G 含週期爲 p 之循環代換[命爲 $t=(x_0x_1\cdots x_{p-1})$].設 K 表在 (31) 內最後含有代換 t 之羣,則緊隨 K 後且在 K 下指數爲素數 ν 之羣 L 不復含 t.因 $t^p=I$ 屬於 L 而 t 之較低乘冪無屬於 L 者,故由 §102 知 $\nu=p$.

欲證 L 爲么羣 G_1,假設 L 含換 x_α 爲不同文字 x_β 之代換 s,則 $u\equiv st^{\alpha-\beta}$ 使 x_α 之值不變,故屬於 K.因 $\alpha-\beta$ 不能以 p 除盡,及因 t 不屬於 L,故 u 不屬於 L.由 §102 之引知,u 之週期可以 $\nu=p$ 除盡.但,因 u 爲 p 文字之代換,而又含一無替換之文字,故知其爲不可能.

因 $L=G_1$,及 L 在 K 下之指數爲 p,故羣 K 爲由 t 之乘冪所成之 p 級循環羣.因 (31) 內緊在 K 前之羣 J 含循環羣 K 爲其自配子羣,故 J 含於 p 次之準循環羣內.由 §98 末段所述之注意知,J 舍含 t 之乘冪外,不含其他週期爲 p 之循環代換.設 J' 爲 (31) 內緊在 J 前之羣,則 J 在 J' 下爲自配子羣,故 t 施以 J' 之任意代換,則得屬於 J 之代換,且爲週期等 p 之循環代換,故等於 t 之某乘冪.故循環羣 K 在 J' 下,亦如其在 J 下,皆爲自配子羣,故 J' 含於準循環羣內(§98).仿此推去,直至到達羣 G 時,吾人知 G 含於準循環羣內.故由 §101 知此定理爲眞.

第十一章

更專門結果之敍述

§104. 羣Γ(§77)之第二定義 欲證:「羣Γ可完全由所設羣G及H決定,且完全與用以決定此羣之函數ψ無關」之定理,茲先決定一個與屬於H之函數無關之羣Γ_1,並證明$\Gamma_1=\Gamma$.

試就以G之代換所排成之長方整列而考之,並設其子羣H內代換排於第一行,得

$$\begin{array}{c|cccc} r_1 & g_1=I & h_2 & \cdots & h_t \\ r_2 & g_2 & h_2g_2 & \cdots & h_tg_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_\nu & g_\nu & h_2g_\nu & \cdots & h_tg_\nu \end{array} \qquad \cdots\cdots(32)$$

此處r_j表整列之第j行.設g爲G之任一代換,因g_1g, ···, $g_\nu g$在整列(32)內,故可書爲

$$g_1g=h_{\alpha'}g_\alpha,\quad g_2g=h_{\beta'}g_\beta,\ \cdots,\ g_\nu g=h_{\kappa'}g_\kappa \qquad \cdots\cdots(33)$$

故整列(32)內之代換與g作右邊積時,其積可書爲(保持其同一次序):

$$\begin{array}{c|cccc} r_\alpha & h_{\alpha'}g_\alpha & (h_2h_{\alpha'})g_\alpha & \cdots & (h_th_{\alpha'})g_\alpha \\ r_\beta & h_{\beta'}g_\beta & (h_2h_{\beta'})g_\beta & \cdots & (h_th_{\beta'})g_\beta \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ r_\kappa & h_{\kappa'}g_\kappa & (h_2h_{\kappa'})g_\kappa & \cdots & (h_th_{\kappa'})g_\kappa \end{array} \qquad \cdots\cdots(34)$$

今$h_{\alpha'}$, $h_2h_{\alpha'}$, ···, $h_th_{\alpha'}$構成$h_1=I$, h_2, ···, h_t之一種排列,故(34)內第一行上之代換,各與(32)之第α行上之代換當全相同,惟其排列之次序各異.同樣,對於兩整列之他行亦具此性質.故(32)與g作右邊乘積時,兩整列之行上卽發生次之排列:

$$\gamma=\begin{pmatrix} r_1 & r_2 & \cdots & r_\nu \\ r_\alpha & r_\beta & \cdots & r_\kappa \end{pmatrix}.$$

欲將此等代換 γ 所成之羣 Γ_1 與上面所決定之羣 Γ 證爲同一，則因 $\psi_{g_1 g}=\psi_{h_\alpha g_\alpha}=\psi_{g_\alpha}$, ⋯⋯[由 (33)]，故

$$\begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \cdots & \psi_{g_\nu} \\ \psi_{g_1 g} & \psi_{g_2 g} & \cdots & \psi_{g_\nu g} \end{pmatrix}=\begin{pmatrix} \psi_{g_1} & \psi_{g_2} & \cdots & \psi_{g_\nu} \\ \psi_{g_\alpha} & \psi_{g_\beta} & \cdots & \psi_{g_\kappa} \end{pmatrix}$$

按上之定義爲與 g 成對應然此代換與 γ 所不同之點僅在其所用之記法，故知 $\Gamma_1=\Gamma$.

例 1.　設 G 爲循環羣 $\{I, c, c^2, c^3, c^4, c^5\}$，此處 $c^6=I$. 又設 H 爲子羣 $\{I, c^3\}$. 則整列爲

$$\begin{array}{c|cc} r_1 & I & c^3 \\ r_2 & c & c^4 \\ r_3 & c^2 & c^5 \end{array}$$

而 $(r_1r_2r_3)$ 與 c 對應.故 $\Gamma=\{I, (r_1r_2r_3), (r_1r_3r_2)\}$.

例 2.　設 G 爲交錯羣 $G_{12}^{(4)}$. 又設 H 爲對易子羣 (Commutative subgroup) G_4 (§21, 例 f)，則 G 之長方整列即爲 §77 例 2 內所列者.以 $(x_1x_2)(x_3x_4)$ 右邊乘所列之代換，得整列

$$\begin{array}{cccc} (x_1x_2)(x_3x_4), & I, & (x_1x_4)(x_2x_3), & (x_1x_3)(x_2x_4) \\ (x_1x_2x_4) & (\ 1\ 4\ 3), & (x_1x_3x_2), & (x_2x_3x_4) \\ (x_1x_2x_3), & (x_1x_3x_4), & (\ 2\ 4\ 3), & (x_1x_4x_2) \end{array}$$

於是整列之行仍然不變，而么代換與 (x_1x_2) (x_3x_4) 成對應.就代換 $(x_1x_3)(x_2x_4)$ 及此兩者之積 $(x_1x_4)(x_2x_3)$，亦得同樣之結果.但，將 $(x_2x_3x_4)$ 用作右邊乘式，則使各行間發生排列 $(r_1r_2r_3)$. 此可直接由施以右邊乘式 $(x_2x_3x_4)$ 及 $(\ 2\ 3\ 4)^2$ 而得之長方整列之構成得之.故 $\Gamma=\{I, (r_1r_2r_3), (r_1r_3r_2)\}$.

§105. 子羣系因子之固定性 (Constancy)　由 §92 之判斷標準，

知方程式欲能以根數解之者,必須且祇須方程式之羣 G 有一子羣系,且子羣系因子全爲素數.欲應用此判斷標準,必研究 G 之一切子羣系是否有一組其子羣系因子全爲素數者.此判斷標準在實用上之價值,藉次之 **C. Jordan 氏定理***而大宏:

設一羣有兩不同子羣系,則一組子羣系之因子必與他組子羣系之因子同,祇其排列次序各異.

例 1. 設 G_8, G_4, H_4 即如 §21 所表之羣,又 G_2, G_2', G_2'' 即如 §65 例 3 內所表之羣;並設

$$C_4=\{I,(x_1x_3y_2y_4),(x_1x_2)(y_3y_4),(x_1x_4y_2y_3)\},$$

$$H_2=\{I,(x_1x_2)\},\quad H_2'=\{I,(x_3y_4)\}.$$

則 G_8 有次之諸子羣系

$$G_8,\ G_4,\ G_2,\ G_1;\quad G_8,\ G_4,\ G_2',\ G_1;\quad G_8,\ G_4,\ G_2'',\ G_1;$$

$$G_8,\ C_4,\ G_2,\ G_1;\quad G_8,\ H_4,\ G_2,\ G_1;\quad G_8,\ H_4,\ H_2,\ G_1;\quad G_8,\ H_4,\ H_2',\ G_1.$$

其每組子羣系因子皆爲 2, 2, 2.

例 2. 設 C_{12} 爲由循環代換 $a=(x_1x_2x_3\cdots x_{12})$ 之乘羣造成之循環羣,其子羣爲

$$C_6=\{I,a^2,a^4,a^6,a^8,a^{10}\},\quad C_4=\{I,a^3,a^6,a^9\},$$

$$C_3=\{I,a^4,a^8\},\quad C_2=\{I,a^6\},\quad C_1=\{I\}.$$

則 C_{12} 之唯一子羣系爲†

$$C_{12},\ C_6,\ C_3,\ C_1;\quad C_{12},\ C_6,\ C_2,\ C_1;\quad C_{12},\ C_4,\ C_2,\ C_1.$$

其子羣系因子爲 2, 2, 3; 2, 3, 2; 3, 2, 2.

§103. 因子羣(Factor groups)之固定性 在 G 之子羣系 $G, G', G'', \cdots, G_1$

*見 Traité des substitutions 第 42 至 43 頁.其較短證則,可參看 Netto-Cole 氏所著之 Theory of Substitutions 第 99 至 100 頁.

†因 $a^{-i}a^ja^i=a^j$, 每個子羣皆爲自配子羣 (§13).

內,每羣俱爲前一羣之最大自配子羣(§43).由此作成之一鏈商羣

$$G/G',\ G'/G'',\ G''/G''',\ \cdots$$

構成 G 之因子羣系(Series of factor-groups of G).此時,每個因子羣皆爲簡單羣(§80).前節關於子羣系因子數值具有固定性之 Jordan 氏定理,包含於次之 Hölder 氏定理*之中:

若一羣有兩組子羣系時,則一組之因子羣必與他組之因子羣相同,祇其排列次序相異.

例如,在 §105 之例 1,其因子羣全爲第 2 級之循環羣,在例 2 則各組之因子羣爲

$$K_7,\ K_2,\ K_3;\quad K_2,\ K_3,\ K_2;\quad K_3,\ K_2,\ K_2.$$

此處 K_2 及 K_3 分別爲第 2 級及第 3 級之循環羣.至於 C_6/C_2 爲循環羣 K_3 可由令 $a^2=e$ 從 §104 例 1 導出之.又若 C_{12}/C_4 爲 K_3 則易由 §104 得出.

§107. Hölder 氏關於將任意方程式化爲一組輔助方程式(Auxiliary equations)之連索以求解之研究†,爲近代對於 Galois 氏理論之一大貢獻.從前限於代數可解方程式,現在此限制業已除去.本書於 §82 中卽已證出,所設方程式之解法,可由使用所設方程式根之有理函數,而化爲解一組簡法方程式之連索得之.輔助方程式之羣,卽爲所設方程式之簡單因子羣 G.倘使用**輔助無理數**(Accessory irrationalities)——卽使用非所設方程式根之有理函數之量——則此等簡單羣中,有能免去否?按

* Hölder, Math. Ann., 第 34 卷,第 37 頁.又 Burnside, The Theory of groups, 第 118 頁; Pierpont, Galois' Theory of Algebraic Equations, Annals of Math., 1900, 第 51 頁.

† Mathematische Annalen, 第 34 卷,第 26 頁;又 Pierpont 氏 Galois' Theory of Algebraic Equations, Annals of Math., 1900, 第 52 頁.

Hölder 氏之結果,不論輔助簡單方程式如何選擇,G之因子羣必見於此輔助簡單方程式之羣中.由是知上面疑問之答覆爲"不能".任一輔助方程式組可先以一組等值簡單方程式之連索替換之.於是,G之因子羣之數,卽爲所需輔助簡單方程式之最低限度.苟因子羣之數,不超過此最低度,則 Hölder 氏定理告吾人以一切輔助方程式所有之根,爲所設方程式之根及所設有理性數統內之量之有理函數.

上面結果,自然賴G之因子羣有固定性而成立,而 Hölder 氏之證明,則以§93之基本定理爲基礎.

因簡單羣與特殊重要之結果相關聯,遂引起對此種羣之許多研究.業發見有無數之簡單羣系,且曾將百萬以內之合組(Composite)級之簡單羣列成一表.*

關於 Galois 氏理論方面完備之參考書目及更進步之發展,讀者可檢閱算理科學全書 (Encyklopadie der Mathematischen Wissenschaften) 第一卷,第480—520頁.

*參看 Dickson, Linear Groups, 第 307 至 310 頁.本書於 1901 年刊於 Leipzig.

附　錄

方程式根與係數間之關係

設 $x_1, x_2, \cdots, x_n$ 表方程式 $f(x)=0$ 之根,並假定此方程式內 x^n 之係數,經施以除法後其值等 1 者.於是

$$f(x)\equiv(x-x_1)(x-x_2)\cdots(x-x_n),$$

此可由初等代數內因子定理證得之.若將 $f(x)$ 之式寫出,並將全等式之右端展開,得

$$\begin{aligned}x^n-c_1x^{n-1}+c_2x^{n-2}-\cdots+(-1)^nc_n\\ \equiv x^n-(x_1+x_2+\cdots+x_n)x^{n-1}\\ +(x_1x_2+x_1x_3+x_2x_3+\cdots+x_{n-1}x_n)x^{n-2}\\ -\cdots+(-1)^nx_1x_2x_3\cdots x_n.\end{aligned}$$

試比較兩端 x 同乘冪之係數,得

$$x_1+x_2+\cdots+x_n=c_1,\ x_1x_2+\cdots+x_{n-1}x_n=c_2,\ \cdots,\ x_1x_2\cdots x_n=c_n\cdots\cdots(i)$$

此等 $x_1, x_2, \cdots, x_n$ 之結合,稱爲**根之初等對稱函數** (Elementary symmetric functions of the roots). 試將此結果與§2後之習題 5 及 6 比較之.

對稱函數之基本定理*

$x_1, x_2, \cdots, x_n$ 之任意整對稱函數,必能以初等對稱函數 $c_1, c_2, \cdots, c_n$ 之整函數列出,且其列出之整函數祇有一種.

設對於兩項 $x_1^{m_1}x_2^{m_2}x_3^{m_3}\cdots$ 及 $x_1^{n_1}x_2^{n_2}x_3^{n_3}\cdots$,其指數之差 $m_1-n_1,\ m_2-n_2,\ m_3-n_3,\ \cdots$ 內,開始不等零之數爲正數時,則稱

*此處爲 Gauss 氏證明,見氏之論文集 (Gesammelte Werke) 第 III 卷,第 37,38 兩頁.

項 $x_1^{m_1}x_2^{m_2}\cdots$ 高於 (Higher than) $x_1^{n_1}x_2^{n_2}\cdots$. 於是 $c_1, c_2, \cdots, c_n$ 內, 其最高項 (Highest term) 分別爲 $x_1, x_1x_2, x_1x_2x_3, \cdots$. 就普通言之, 函數 $c_1^{\alpha}c_2^{\beta}c_3^{\gamma}\cdots$ 內之最高項爲

$$x_1^{\alpha+\beta+\gamma+\cdots}x_2^{\beta+\gamma+\cdots}x_3^{\gamma+\cdots}\cdots.$$

故此函數欲與 $c_1^{\alpha'}c_2^{\beta'}c_3^{\gamma'}\cdots$ 之最高項相同時, 必須且祇有假定

$$\alpha+\beta+\gamma+\cdots=\alpha'+\beta'+\gamma'+\cdots$$

$$\beta+\gamma+\cdots=\beta'+\gamma'+\cdots,$$

$$\gamma+\cdots=\gamma'+\cdots,$$

$$\cdots\cdots\cdots\cdots,$$

卽假定

$$\alpha=\alpha',\quad \beta=\beta',\quad \gamma=\gamma',\quad \cdots,$$

方能成立.

設 S 爲所設對稱函數, 其最高項爲

$$h\equiv ax_1^{\alpha}x_2^{\beta}x_3^{\gamma}x_4^{\delta}\cdots x_n^{\nu}\cdots\quad(\alpha\geqq\beta\geqq\gamma\geqq\delta\cdots\geqq\nu).$$

試作對稱函數

$$c\equiv ac_1^{\alpha-\beta}c_2^{\beta-\gamma}c_3^{\gamma-\delta}\cdots c_n^{\nu}.$$

若將此函數按公式 (i) 展開爲 $x_1, x_2, \cdots, x_n$ 之式時, 則其各項悉爲同次, 且其最高項卽爲 h. 於是, 差

$$S_1\equiv S-\sigma$$

仍爲對稱函數, 但較 S 爲簡單, 此因最高項 h 已消去也. 設令 S_1 之最高項爲

$$h_1\equiv a_1x_1^{\alpha_1}x_2^{\beta_1}x_3^{\gamma_1}x_4^{\delta_1}\cdots$$

則具有較低最高項之對稱函數爲

$$S_2\equiv S_1-a_1c_1^{\alpha_1-\beta_1}c_2^{\beta_1-\gamma_1}c_3^{\gamma_1-\delta_1}\cdots.$$

然因 S_1 及 S_2 之次數不大於 S 之次數, 又因對於所設次數, 其低於 h 之項 $x_1^{m_1}x_2^{m_2}x_3^{m_3}\cdots$ 之項數爲有限, 故經重複引用此法後,

最終必得對稱函數 0:

$$0 \equiv S_k - a_k c_1^{\alpha_k - \beta_k} c_2^{\beta_k - \gamma_k} c_3^{\gamma_k - \delta_k} \cdots .$$

於是,吾人達到所欲得之結果:

$$S = a_1 c_1^{\alpha - \beta} c_2^{\beta - \gamma} \cdots + a_2 c_1^{\alpha_1 - \beta_1} c_2^{\beta_1 - \gamma_1} \cdots + \cdots + a_k c_1^{\alpha_k - \beta_k} c_2^{\beta_k - \gamma_k} \cdots .$$

次欲證明對稱函數 S 以 $c_1, c_2, \cdots, c_n$ 表示之式,祇有一種,吾人可假定 S 能化爲 $\phi(c_1, c_2, \cdots, c_n)$ 及 $\psi(c_1, c_2, \cdots, c_n)$, 此處 ϕ 及 ψ 爲 $c_1, c_2, \cdots, c_n$ 之不同整函數.故 $\phi - \psi$ 若視爲 $c_1, c_2, \cdots, c_n$ 之函數而考之,必不全等於零.將 $\phi - \psi$ 內同類項加減約簡後,命 $bc_1^{\alpha} c_2^{\beta} c_3^{\gamma} \cdots$ 爲係數 $b \neq 0$ 之項.若換爲 $x_1, x_2, \cdots, x_n$ 之函數,則其最高項爲

$$b x_1^{\alpha+\beta+\gamma+\cdots} x_2^{\beta+\gamma+\cdots} x_3^{\gamma+\cdots} \cdots .$$

又與 $bc_1^{\alpha} c_2^{\beta} c_3^{\gamma} \cdots$ 相異之項 $b' c_1^{\alpha'} c_2^{\beta'} c_3^{\gamma'} \cdots$, 其最高項必與此最高項異,前既證之矣.故在此等最高項中,必有一項高於其餘諸項;因此項之係數不等零,於是函數 $\phi - \psi$ 以 $x_1, x_2, \cdots, x_n$ 表之時,亦不能全等於零.此與前假設[$S \equiv \phi, S \equiv \psi$ (就 $x_1, x_2, \cdots, x_n$ 之一切值)]相矛盾,故知 S 以 $c_1, c_2, \cdots, c_n$ 之式列出時,祇有一式.

系　係數爲整數之 $x_1, x_2, \cdots, x_n$ 之任意整對稱函數,可以係數爲整數之 $c_1, c_2, \cdots, c_n$ 之整函數表之.

在計算對稱函數時,此法之實用上價值,可參看 Serret 氏所著之高等代數學第 4 或第 5 版,第 1 卷,第 389—395 頁內之例.

關於普通方程式

設係數 $c_1, c_2, \cdots, c_n$ 爲不定量,兩根 $x_1, x_2, \cdots, x_n$ 爲 $c_1, c_2, \cdots, c_n$ 之函數;凡每組 $c_1, c_2, \cdots, c_n$ 之值一定時,則 $x_1, x_2, \cdots, x_n$ 亦爲一

定.茲今證次之定理:

設係數爲常數之 $x_1, x_2, \quad , x_n$ 之有理整函數等零時,則此函數必全等於零.

設 $\psi[x_1, x_2, \cdots, x_n]=0$. 命 $\xi_1, \xi_2, \cdots, \xi_n$ 表不定量,而 $\sigma_1, \sigma_2, \cdots, \sigma_n$ 表初等對稱函數 $\xi_1+\xi_2+\cdots+\xi_n, \cdots, \xi_1\xi_2\cdots\xi_n$. 則

$$\Pi\psi[\xi_{s_1}, \cdots, \xi_{s_n}]=\Psi[\sigma_1, \cdots, \sigma_n],$$

右邊之積展布及於 $1, 2, \cdots, n$ 之所有 $n!$ 個排列 $s_1, s_2, \cdots, s_n$,而 Ψ 表有理整函數.因積中含有因子 $\psi[x_1, x_2, \cdots, x_n]=0$,於是

$$\Pi\psi[x_{s_1}, \cdots, x_{s_n}]=\Psi[c_1, \cdots, c_n]=0.$$

但因 $c_1, \cdots, c_n$ 爲不定量;故 $\Psi[c_1, c_2, \cdots, c_n]$ 在用 $c_1, c_2, \cdots, c_n$ 表示之式必全等零.試就 $c_1, c_2, \cdots, c_n$ 爲新不定量 $y_1, y_2, \cdots, y_n$ 之函數考之,則就用 $y_1, y_2, \cdots, y_n$ 列出之式而言,

$$\Psi[c_1(y_1, y_2, \cdots, y_n), \cdots, c_n(y_1, y_2, \cdots, y_n)] \equiv 0.$$

故若變換其記法,則對於用 $\xi_1, \xi_2, \cdots, \xi_n$ 列出之式而言,得

$$\Psi[\sigma_1(\xi_1, \xi_2, \cdots, \xi_n), \cdots, \sigma_n(\xi_1, \xi_2, \cdots, \xi_n)] \equiv 0.$$

故必有一因子,其在用 $\xi_1, \xi_2, \cdots, \xi_n$ 表示之式言之,有

$$\psi[\xi_{s_1}, \cdots, \xi_{s_n}] \equiv 0.$$

若將記法略爲變動,可使上式變爲

$$\psi[\xi_1, \cdots, \xi_n] \equiv 0.$$

試舉其一種應用言之.吾人可決定普通方程式之羣,比 §64 之法更覺與 Galois 氏理論之精神貼切.設一有理函數 $\phi(x_1, x_2, \cdots, x_n)$,其係數在數統 $R=(c_1, c_2, \cdots, c_n)$ 內,此函數對於 R 之值,亦在 R 內.則當以 $x_1, x_2, \cdots, x_n$ 之初等對稱函數替換 $c_1, c_2, \cdots c_n$ 時,即得一關係

---

*此爲 Moore 氏證明,較 Weber 氏代數學(於 1900 年出版)內 §566 所載之證明,更爲明晰.

$$\phi[x_1, \cdots, x_n]=0,$$

按上之定理,知 $\phi[x_{s_1}, \cdots, x_{s_n}]=0$, 於是,

$$\phi(x_{s_1}, \cdots, x_{s_n})=\phi(x_1, \cdots, x_n).$$

索　引

學名索引

一　畫

四　畫

五　畫

六　畫

七　畫

十四畫

十五畫

十六畫

十八畫

二十三畫

人名索引