大學叢書

羣論

上冊

著造正園
譯絳君蕭

商務印書館發行

大學叢書

羣　論

園正造　著
蕭君絳　譯

商務印書館發行

節譯著者原序

本書由五篇而成:

第一篇,乃論羣一般通有之性質者也,卽所謂抽象羣論者是. 羣之抽象的討論,自 Frobenius 氏始. 本篇卽以氏之研究爲主而組織化者,然其間併非無著者之創意在.

第二篇所論,乃以置換爲羣之構成元素者,卽置換羣是. 此卽論由置換之一特殊元素而生之羣之性質者也. 置換羣分爲可遷的與非遷的兩種,而後者則由前者所構成. 著者當討論前者之際,乃以可遷羣得視爲羣之傍系置換表示之一點爲基礎而論究之;其本原性與非原性,亦由此見地而說明之;隨卽以是所得之結果而直用諸一般可遷羣焉.

第三篇,論母式之合同羣者也. 本來,在法母式之各項爲素數冪者之研究,雖由 Ranum 氏而始成,然著者乃使其一般化,並闡明母式之一意的合同乘法之條件而以定合同羣之義. 加以由 Dickson 氏著書 Linear groups 中所載一次變換羣之母元素得獲暗示,乃求得一般母式合同羣之母元素,及由是而克作羣者之母式所應有之條件,更將羣分解,以擴張關於一次變換羣之分解者之 Jordan 氏之定理. 最後就一次變換合同羣,作爲母式合同羣之特殊者

而論述之. 其中第 128 節所示之證明, 乃根據 Dickson 氏所與之方法者也. 此外關於母式合同羣, 雖尚有擴張之餘地, 然請以讓諸他日, 俟有機會, 再行詳論.

第四篇, 乃以特殊羣爲標題者, 其中關於 Abel 氏羣, 素數冪元羣之型以及分數變換羣皆在討論範圍之內.

第五篇, 乃論羣母式, 羣指標者. 此體爲 Frobenius 氏所創始, 顧在本篇, 乃從 Schur 氏之方法, 由羣之母式表示以導入羣指標, 然後再示其與 Frobenius 氏者一致也(第二十六, 第二十七章). 至第二十八章則示羣指標之應用焉.

本書所論, 僅及羣論大綱, 細微之處, 未暇詳及, 在使讀者理解其眞諦, 是爲區區之微意而亦所最努力者也.

一九二八年五月十日

著者識.

目　次

第一編　羣的概論

第一章　置換

第二章　羣之定義

第三章 約羣

第四章 共軛

第五章 合同, 商羣

第六章 重複同態

第七章 組成羣列

第十六章　自己同態，全形

第三篇　合同羣

第十七章　母式之合同乘法

第十八章　母式合同羣

第二十三章　母式之指標根

第二十四章　分數變換羣

第五篇　羣母式, 羣指標

第二十五章　母式之階級

第二十六章 羣母式

第二十七章 羣指標

第二十八章 羣指標之應用

第一篇

羣的概論

第一章 置換

1. 置換之定義.

今於此有五文字焉, a, b, c, d, e, 各置於一定之位置.次將各個位置變換,令 a 所在之處置以 b, b 之處置以 e, 順次 c, d, e 之處置以 a, d, c, 則此五文字間一置換生焉.

同樣,一般有 n 個相異之文字

(1) $\qquad a, a_1, a_2, \cdots\cdots, a_{n-1}$

時,若其兩相異之文字不以同一之文字置換之,則(1)之各文字而以屬於(1)之文字置換之舉,名曰在 n 個文字 $a, a_1, \cdots\cdots, a_{n-1}$ 上所施行之置換.

在 n 個文字 $a, a_1, \cdots\cdots, a_{n-1}$ 上所行之置換,若 a 爲 β 所置換, $a_1, a_2, \cdots\cdots, a_{n-1}$ 爲 $\beta_1, \beta_2, \cdots\cdots, \beta_{n-1}$ 所置換時,則此置換乃以記號

$$\begin{pmatrix} \alpha & \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{n-1} \\ \beta & \beta_1 & \beta_2 & \cdots\cdots & \beta_{n-1} \end{pmatrix}$$

表之.

例如

$$\begin{pmatrix} a & b & c & d & e \\ b & e & a & d & c \end{pmatrix}$$

者,乃示 a, b, c, d, e 以 b, e, a, d, c 置換所得之置換者也.

且就置換言,吾人所須注目者,僅在始初所與之各文字究以何文字去置換之一點,故其記號上,上列之文字任以何順序排列,儘可隨意. 如

$$\begin{pmatrix} a & b & c & d & e \\ b & e & a & d & c \end{pmatrix}, \quad \begin{pmatrix} b & e & a & d & c \\ e & c & b & d & a \end{pmatrix}$$

二者,上列文字配列之順序雖異,而以 b 換 a, e 換 b, a 換 c, d 換 d, c 換 e, 則全然一致.故兩者須視爲表示同一之置換者焉.

2. 置換之結合.

今 $$S=\begin{pmatrix} \alpha & \alpha_1 & \cdots & \alpha_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}, \quad T=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \gamma & \gamma_1 & \cdots\cdots & \gamma_{n-1} \end{pmatrix}$$

爲 n 個文字 α, α_1, α_2, $\cdots\cdots$, α_{n-1} 上所行之兩置換.由 T, 文字 β 爲 γ' 所置換, $\beta_1, \beta_2, \quad , \beta_{n-1}$ 爲 $\gamma'_1, \gamma'_2, \cdots\cdots \gamma'_{n-1}$ 所置換時,則 T 可換書如次:

$$T=\begin{pmatrix} \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \\ \gamma' & \gamma'_1 & \cdots\cdots & \gamma'_{n-1} \end{pmatrix}$$

茲 n 個文字

(1)　　$a, a_1, a_2, \cdots\cdots, a_{n-1}$

之上,若先施以置換 S, 則(1)之文字,其順序變而爲

$$\beta, \beta_1, \beta_2, \cdots\cdots, \beta_{n-1}$$

再於此施以置換 T,則其順序復變而爲

$$\gamma', \gamma'_1, \gamma'_2, \cdots\cdots, \gamma'_{n-1}.$$

由此觀之,(1)之上繼續施以兩置換 S 及 T,其結果與於(1)上施行唯一之置換

$$P=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \gamma' & \gamma'_1 & \cdots\cdots & \gamma'_{n-1} \end{pmatrix}$$

者相同.此最後之置換 P,名曰始初二置換 S 及 T 之積,而以 ST 表示之. 卽

$$P=ST$$

也.於是凡由兩置換以作其積者,名曰兩置換之**結合**或曰**乘法**.

如以

$$S=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, \quad T=\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, \quad U=\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$

則

$$ST=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}=\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}\begin{pmatrix} b & c & a \\ a & b & c \end{pmatrix}=\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix},$$

$$TS=\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}\begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}=\begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}\begin{pmatrix} c & a & b \\ a & b & c \end{pmatrix}=\begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix},$$

$$SU=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}\begin{pmatrix}b&c&a\\a&c&b\end{pmatrix}=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},$$

$$US=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}\begin{pmatrix}b&a&c\\c&b&a\end{pmatrix}=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}.$$

就此例而觀,當作兩置換之積時,如於S乘以T所得之積ST及於T乘以S所得之積TS雖則一致,然乘U於S之積SU與乘S於U之積US則互異.可見對置換之乘法言,其交換法則未見其必成立也.

雖然,置換之乘法上,交換法則固未見其必然成立,然組合法則實常成立焉. 例若

$$S=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix},\quad T=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix},\quad U=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}.$$

則

$$ST=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix},$$

$$\therefore\quad (ST)U=\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}=\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix}$$

又

$$TU=\begin{pmatrix}a&b&c\\c&b&a\end{pmatrix}\begin{pmatrix}a&b&c\\b&c&a\end{pmatrix}=\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix},$$

$$\therefore\quad S(TU)=\begin{pmatrix}a&b&c\\b&a&c\end{pmatrix}\begin{pmatrix}a&b&c\\a&c&b\end{pmatrix}=\begin{pmatrix}a&b&c\\c&a&b\end{pmatrix}.$$

因之

$$(ST)U=S(TU).$$

注意. 當有一置換S,而取他置換T以作積ST,名曰T右乘於S;而作積TS,則名曰T左乘於S.

3. 不動置換,逆置換.

於 n 個文字 $\alpha, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$ 上所得施行置換之總數爲

$$n(n-1)\cdots\cdots 3\cdot 2\cdot 1=n!$$

明矣.然此 $n!$ 個之中,彼 n 個文字之任何個皆不動者,亦以之爲一置換而包含在內.此種置換名曰**不動置換**,而以 1 表之,卽

$$\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}=1$$

是也.今取任意一置換

$$S=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}.$$

此時

$$1\cdot S=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=S$$

又

$$S\cdot 1=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}$$

$$=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}\begin{pmatrix}\beta & \beta_1 & \cdots\cdots & \beta_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=S.$$

故不動置換,對於任意之置換 S,無論左乘右乘,皆不能變化 S 者也.

其次,若有一置換

$$S=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}.$$

茲顛倒其上下列而作成一置換

$$\begin{pmatrix}\beta & \beta_1 & \cdots\cdots & \beta_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}$$

時,則此名曰 S 之逆置換,而以 S^{-1} 表之.

於是

$$SS^{-1}=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}\begin{pmatrix}\beta & \beta_1 & \cdots\cdots & \beta_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}=1,$$

$$S^{-1}S=\begin{pmatrix}\beta & \beta_1 & \cdots\cdots & \beta_{n-1}\\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\end{pmatrix}\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=\begin{pmatrix}\beta & \beta_1 & \cdots\cdots & \beta_{n-1}\\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1}\end{pmatrix}=1.$$

是卽一置換與其逆置換之積,乃一不動置換也.

如 $$S=\begin{pmatrix}a & b & c & d\\ c & d & b & a\end{pmatrix},$$

則 $$S^{-1}=\begin{pmatrix}c & d & b & a\\ a & b & c & d\end{pmatrix}=\begin{pmatrix}a & b & c & d\\ d & c & a & b\end{pmatrix},$$

而 $$SS^{-1}=\begin{pmatrix}a & b & c & d\\ c & d & b & a\end{pmatrix}\begin{pmatrix}a & b & c & d\\ d & c & a & b\end{pmatrix}=1.$$

復次,於 n 個文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 上所行之兩置換 S 及 T,

若 $$ST=1 \qquad (\text{或} \quad TS=1),$$

則 T 爲 S 之逆置換.

蓋於上式之兩邊,以 S^{-1} 左乘(或右乘),則

$$S^{-1}(ST)=S^{-1}\cdot 1 \qquad (\text{或} \quad (TS)S^{-1}=1\cdot S^{-1}),$$

適用組合法則於此式左邊,得

$$(S^{-1}S)T=S^{-1}\cdot 1 \qquad (\text{或} \quad T(SS^{-1})=1\cdot S^{-1}),$$

$$\therefore \quad 1\cdot T=S^{-1} \qquad (\text{或} \quad T\cdot 1=S^{-1}),$$

$$\therefore \quad T=S^{-1}$$

注意. 本來,由置換以說置換羣,更進以論一般抽象羣時,不動置換之定義,以對於任意之置換 S 而能滿足

$$S1=S$$

之置換 1 充之,及一置換 S 之逆置換,以能滿足

$$S\hat{X}=1$$

之置換 X 充之,自爲妥當;惟吾人於此爲使容易了解起見,遂與以上之定義焉. (參照第15,18節)

4. 置換之連乘積,羣及其逆.

在三個置換之積中,組合法則原已成立,故於四個置換 A, B, C, D 之積間,得次之關係:

$$[(AB)C]D=[A(BC)]D=A[(BC)D]$$
$$=A[B(CD)]=(AB)(CD).$$

爲說明此理起見,先於此四個置換之列 A, B, C, D 中,任取相隣兩置換,而將此二者以其積置換之,如 A,(BC), D 是.更於此中取相隣之二者,再施以前法,遂得唯一之置換焉.如是所得最後之置換,有如上列關係所示,無論隣接置換之選擇方法如何,常爲同一者也.

不僅此也,對於四以上置換之積,亦能得同樣之結果,此則用數學的歸納法得以證明者也.於是若干個之置換 A, B, C, D, …… 順次相乘所得之積,乃以 ABCD …… 表示之焉.

是中,以同一置換 S 之 m 個相乘之積,以 S^m 表示,名之曰 S 之 m 乘冪.於是準上所述,則

$$S^mS^n=S^{m+n},\qquad (S^m)^n=S^{mn}$$

明矣.

復次,若 S 之逆置換之 m 乘冪 $(S^{-1})^m$,以 S^{-m} 表示之,則 S^{-m} 者,遂成爲 S^m 之逆置換矣.即

$$S^mS^{-m}=1,$$

蓋因

$$S^2S^{-2}=S^2(S^{-1})^2=SSS^{-1}S^{-1}=S(SS^{-1})S^{-1}$$

$$=S\cdot 1\cdot S^{-1}=S\ S^{-1}=1,$$

同樣

$$S^mS^{-m}=S^m(S^{-1})^m=S^{m-1}(SS^{-1})(S^{-1})^{m-1}$$

$$=S^{m-1}S^{-(m-1)},$$

故由數學的歸納法,

$$S^mS^{-m}=1.$$

5. 巡回置換.

茲就一特別的置換

$$\begin{pmatrix}\alpha & \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{n-2} & \alpha_{n-1}\\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots\cdots & \alpha_{n-1} & \alpha\end{pmatrix}$$

而觀,則見 α 爲 α_1, α_1 爲 α_2, ……, α_{n-2} 爲 α_{n-1} 所置換,而最後 α_{n-1} 爲 α 所置換者也.此置換名曰在 n 個文字.

$$\alpha,\ \alpha_1,\ \alpha_2,\ \cdots\cdots,\ \alpha_{n-1}$$

上所施行之**巡回置換**,而以

$$(\alpha\ \alpha_1\ \alpha_2 \cdots\cdots\ \alpha_{n-1})$$

表示之焉.

巡回置換

$$\begin{pmatrix} \alpha & \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{n-2} & \alpha_{n-1} \\ \alpha_1 & \alpha_2 & \alpha_3 & \cdots\cdots & \alpha_{n-1} & \alpha \end{pmatrix}$$

又可換書之如

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_{n-1} & \alpha \\ \alpha_2 & \alpha_3 & \cdots\cdots & \alpha & \alpha_1 \end{pmatrix},\ \cdots\cdots,\ \begin{pmatrix} \alpha_{n-1} & \alpha & \cdots\cdots & \alpha_{n-3} & \alpha_{n-2} \\ \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-2} & \alpha_{n-1} \end{pmatrix}$$

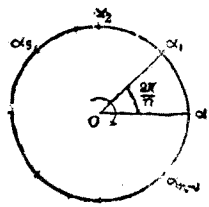
也,故依上之記法,則

$$(\alpha\ \alpha_1 \cdots\cdots\ \alpha_{n-2}\ \alpha_{n-1}),\ (\alpha_1\ \alpha_2 \cdots\cdots\ \alpha_{n-1}\ \alpha),\ \cdots\cdots,$$

$$(\alpha_{n-1}\ \alpha \cdots\cdots\ \alpha_{n-3}\ \alpha_{n-2})$$

皆爲表示同一之巡回置換者焉.

注意. 將圓 O 分成 n 等分而將各分點,順次以 α, α_1, α_2, $\cdots\cdots$ α_{n-1} 表之. 是圓也,若於中心 O 之周圍,依矢之方向迴轉 $\frac{2\pi}{n}$,則 α_1, α_2, $\cdots\cdots$, α_{n-1}, α, 各自來到 α, α_1, $\cdots\cdots$, α_{n-2}, α_{n-1} 始初所占之位置,發產生一巡回置換$(\alpha\ \alpha_1 \cdots\cdots\ \alpha_{n-2}\ \alpha_{n-1})$焉.



6. 巡回置換之積.

茲有兩個巡回置換

$$(\alpha\ \alpha_1 \cdots\cdots\ \alpha_{n-2}\ \alpha_{n-1}),\ (\alpha'\ \alpha'_1\ \cdots\cdots\ \alpha'_{m-2}\ \alpha'_{m-1}),$$

若二者係由同文字而成時,則其積,由第 2 節之定義,直可以求得也.蓋將兩者換書之爲

$$(\alpha\ \alpha_1\ \cdots\cdots\ \alpha_{n-1})=\begin{pmatrix}\alpha & \alpha_1 & \cdots & \alpha_{n-1}\\ \alpha_1 & \alpha_2 & \cdots & \alpha\end{pmatrix},$$

$$(\alpha'\ \alpha'_1\ \cdots\cdots\ \alpha'_{n-1})=\begin{pmatrix}\alpha' & \alpha'_1 & \cdots & \alpha'_{n-1}\\ \alpha'_1 & \alpha'_2 & \cdots & \alpha'\end{pmatrix},$$

而依同定義將二者乘之可也.如

$$(a\,b\,c\,d)(b\,a\,c\,d)=\begin{pmatrix}a & b & c & d\\ b & c & d & a\end{pmatrix}\begin{pmatrix}b & a & c & d\\ a & c & d & b\end{pmatrix}=\begin{pmatrix}a & b & c & d\\ a & d & b & c\end{pmatrix}.$$

反之,若兩巡回置換,非以同文字而成立時,如欲作$(a\,b\,c)$, $(a\,b\,d\,e)$之積,則次所示之方法足取焉.

兩巡回置換中所含之文字,其全體乃

$$a,\ b,\ c,\ d,\ e$$

之五個也.$(a\,b\,c)$者,固爲其中 a,b,c 三文字上所施行之置換,然將觀點變換,以其爲上列五文字上所行之置換而 $d,\ e$ 爲不動者,亦無不可,即可視爲

$$(a\,b\,c)=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}=\begin{pmatrix}a & b & c & d & e\\ b & c & a & d & e\end{pmatrix}$$

者也.又$(a\,b\,d\,e)$亦同樣的可視爲

$$(a\,b\,d\,e)=\begin{pmatrix}a & b & d & e\\ b & d & e & a\end{pmatrix}=\begin{pmatrix}a & b & c & d & e\\ b & d & c & e & a\end{pmatrix}.$$

作其積

$$\begin{pmatrix}a & b & c & d & e\\ b & c & a & d & e\end{pmatrix}\begin{pmatrix}a & b & c & d & e\\ b & d & c & e & a\end{pmatrix}=\begin{pmatrix}a & b & c & d & e\\ d & c & b & e & a\end{pmatrix}$$

即以是定兩巡回置換(abc), $(abde)$之積之義.至論到一般之

情態,厥理全同.

此外尙有特別者,卽巡回置換

$$(p\,q\,r\,\cdots\cdots\,s),\quad (p'\,q'\,r'\,\cdots\cdots\,s'),\ \cdots\cdots$$

不含有共通文字時,其積可極簡單而得.卽

$$(p\,q\,r\,\cdots\cdots\,s)(p'\,q'\,r'\,\cdots\cdots\,s')\ \cdots\cdots$$

$$=\begin{pmatrix} p\,q & \cdots & s\,p'\,q' & \cdots\cdots & s' & \cdots\cdots \\ q\,r & \cdots\cdots & p\,q'\,r' & \cdots\cdots & p' & \cdots\cdots \end{pmatrix}$$

例.

$$(pq)(pr)=(pqr),$$

$$(pq)(pr)(ps)=(pqr)(ps)=(pqrs),$$

$$(pq)(pr)(ps)\ \cdots\cdots\ (pu)=(pqr\ \cdots\cdots\ u).$$

7. 巡回表示法.

茲有一置換

$$S=\begin{pmatrix} \alpha & \alpha_1 & \cdots & \alpha_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix},$$

請表示之爲巡回置換之積,而示其方法焉.今於 $\alpha,\ \alpha_1,\ \cdots\cdots,\ \alpha_{n-1}$ 中取其任意一文字 p.依 S,則 p 爲 q 所置換,卽在上之記法中,來到上列文字 p 之正下者爲 q 也.次以在 q 正下之文字爲 r,更取在 r 正下之文字而再施前法.然文字之數爲有限,故 p 非來到某文字之正下不可,茲以之爲 s.

若以 $p,\ q,\ r,\ \cdots\cdots,\ s$ 而所與之 n 個文字 $\alpha,\ \alpha_1,\ \cdots\cdots,\ \alpha_{n-1}$ 爲能盡時,則

$$S=\begin{pmatrix} p & q & \cdots & s \\ q & r & \cdots\cdots & p \end{pmatrix},$$

因之

$$S=(p\ q\ r\cdots\cdots s).$$

反之,$p, q, r, \cdots\cdots, s$ 不能盡彼所與之 n 個文字之全般時,則於 $p, q, r, \cdots, s$ 以外,任取一文字 p'.在 S 中,來到 p' 正下之文字以爲 q',以下準前法,而 p' 爲來到 s' 之正下.若以

$$p, q, r, \cdots\cdots, s,$$

$$p', q', r', \cdots\cdots, s'$$

而能盡 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之全,則

$$S=\begin{pmatrix} p & q & \cdots & s & p' & q' & \cdots\cdots & s' \\ q & r & \cdots\cdots & p & q' & r' & \cdots\cdots & p' \end{pmatrix},$$

故由第 6 節末所述,

$$S=(p\ q\ r\cdots\cdots s)(p'\ q'\ r'\cdots\cdots s').$$

若以 $p, q, r, \cdots, s, p', q', \cdots\cdots, s'$ 尙不能盡所與之 n 個文字之全般時,則更可於此外,取任意一文字 p'', 而將上述方法重施之.但始初所與文字之數爲有限,故此方法施行有限回數之後,不得不告終也.因之

$$S=\begin{pmatrix} p & q & \cdots & s & p' & q' & \cdots\cdots & s' & p'' & q'' & \cdots\cdots & s'' & \cdots\cdots \\ q & r & \cdots\cdots & p & q' & r' & \cdots\cdots & p' & q'' & r'' & \cdots\cdots & p'' & \cdots\cdots \end{pmatrix}$$

$$=(p\,q\,r\cdots\cdots s)(p'\,q'\,r'\cdots\cdots s')(p''\,q''\,r''\cdots\cdots s'')\cdots\cdots.$$

且由上之說明,可知巡回置換

$$(p\,q\cdots\cdots s),(p'\,q'\cdots s'),(p''\,q''\cdots\cdots s''),\cdots\cdots,$$

其中任取二者,決不含有共通之文字也甚明.

以故任如何之置換,皆能以相互不含共通文字之巡回

置換之積而表示之也.此種表法,名曰置換之**巡回表示法**,而構成此置換之各個巡回置換

$$(p\,q\cdots\ s),\ (p'\,q'\cdots\cdots s'),\ (p''\,q''\cdots\cdots s''),\cdots\cdots$$

則名曰**巡回因子**云.

如

$$\mathrm{P}=\begin{pmatrix}a&b&c&d&e&f\\c&e&d&a&b&f\end{pmatrix}=\begin{pmatrix}a&c&d&&b&e&&f\\c&d&a&&e&b&&f\end{pmatrix}=(a\,c\,d)(b\,e)(f).$$

在此例中,巡回因子(f)者,乃示文字f依置換P而不動者也.若施行置換之文字全體無有明示之必要時,有如(f)僅以唯一文字而成之因子,可以省去,如

$$\mathrm{P}=(acd)(be)(f)=(acd)(be)$$

是.

例.　置換之積用巡回表示者.

$$(abc)(abde)=(ade)(bc)\qquad[\text{參照第 6 節}].$$

$$(12345)(2431)=(1452)(3)=(1452).$$

$$(12345)(14)(23)=(13)(2)(45)=(13)(45).$$

注意.　如$\begin{pmatrix}a&b&c&d&e&f\\b&c&a&e&f&d\end{pmatrix}=(abc)(def)$者然,一置換之巡回表示,若其巡回因子皆以同數之文字而成時,則此置換名曰**正置換**.

8.　轉換,轉換表示法.

巡回置換之中,其僅以二文字而成者,如$(a\,b)$然,則名曰**轉換**.

且由第 6 節第三例所示,則巡回置換$(p\,q\,r\cdots\cdots s)$,可如

$$(p\,q\,r\cdots\cdots s)=(p\,q)(p\,r)\cdots(p\,s),$$

得以轉換之積而表示者也.然一般,凡置換皆得表之爲巡回置換之積,故凡置換皆足以之爲轉換之積而表之焉.是名曰**置換之轉換表示法**.如

$$\mathrm{P}=\begin{pmatrix} a & b & c & d & e & f \\ c & e & d & a & b & f \end{pmatrix}=(a\,c\,d)(b\,e)=(a\,c)(a\,d)(b\,c)$$

如此例所示,在轉換表示法中,其作因子者之兩轉換,含有共通之文字者有之,是此表示法與巡回表示法相異之點也.

不寧惟是,轉換表示法,其作因子者之轉換之數,亦不一定.如

$$(be)=(ab)(ae)(ab),$$

故上例之置換 P 得書之如次:

$$\begin{aligned}\mathrm{P}&=(ac)(ad)(be)\\&=(ac)(ad)(ab)(ae)(ab);\end{aligned}$$

且

$$(ac)=(fa)(fc)(fa),$$

再代入之,又得

$$\mathrm{P}=(fa)(fc)(fa)(ad)(ab)(ae)(ab)$$

也.雖然,誠如所示,P 之轉換表示法中因子之數固不一定,然其間卻有一定不變之關係在,有如次節之所證,乃謂:

在所設置換 S 之轉換表示法中,其因子之數,若一度爲

偶數,則無論用何方法以表S爲轉換之積,其因子之數常爲偶數也.反之,若其因子之數一度爲奇則常爲奇云.

置換之能以偶數個轉換之積表示者曰**偶數置換**,其以奇數個轉換之積表示者曰**奇數置換**.

9. 1°. 茲取 n 個文字 a, a_1, a_2, ……, a_{n-1} 之整式

$$\Delta=(a-a_1)(a-a_2)\cdots\cdots(a-a_{n-1})$$
$$(a_1-a_2)\cdots\cdots(a_1-a_{n-1})$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(a_{n-2}-a_{n-1})$$

而覘其由轉換$(a_r a_s)$得生如何之變化.但 a_r,a_s 乃此 n 文字中任意之兩個,而 $r<s$.

Δ之因數中蒙轉換$(a_r\ a_s)$之影響者,爲含有a_r, a_s之兩個,或僅含其一者也,以故此類因數,得別爲次之四組:

(1)　(a_r-a_s),

(2)　(a_i-a_r), (a_i-a_s), $i=0,\ 1,\ 2,\cdots\cdots,\ r-1$, $[a_0=a]$,

(3)　(a_r-a_j), (a_s-a_j), $j=s+1,\ s+2,\ \cdots\cdots,\ n-1$,

(4)　(a_i-a_k), (a_k-a_s), $k=r+1,\ r+2,\ \cdots\cdots,\ s-1$.

元來,由轉換$(a_r\ a_s)$,因數(a_r-a_s)遂變爲

$$a_s-a_r=-(a_r-a_s),$$

是則僅變其符號也.

其次,(a_i-a_r), (a_i-a_s),由此轉換,乃各別變爲(a_i-a_s), (a_i-a_r),因之是二者之積,由轉換$(a_r\ a_s)$,僅變其因數之順序.以故凡

屬於(2)因數之積,雖對之施行轉換 $(a_r\ a_s)$,仍可得與原來相等之式也.

同理,屬於(3)之因數之相乘積,亦由此轉換而不變.

最後,(a_r-a_k), (a_k-a_s),由轉換 $(a_r\ a_s)$ 各別變爲

$$a_s-a_k=-(a_k-a_s),\ a_k-a_r=-(a_r-a_k),$$

因之兩者之積不變也.故凡屬於(4)因數之積,亦由轉換 $(a_r\ a_s)$ 而不變.

由是,凡屬於(1),(2),(3),(4)因數之相乘積,換言之,卽謂 Δ 之因數內,凡含有 a_r, a_s 之兩個或僅含其一者之積,由轉換 $(a_r\ a_s)$,只變其符號已也.至若 Δ 中不含 a_r, a_s 之任何者之因數之積,則本不蒙此轉換之影響.故 Δ 者,由轉換 $(a_r\ a_s)$,變而爲 $-\Delta$ 也.

2°. 由 1° 以觀,若於 Δ 行轉換一回,則變爲 $-\Delta$,更於 $-\Delta$ 上行轉換一回,則復成 Δ. 故當於 Δ 上繼續行轉換若干回時,使回數爲奇,爲 $-\Delta$ 也;若爲偶數則不變.

3°. 今以 S 爲一所與之置換,而以

$$S=(ab)(a'b')\cdots\cdots$$

$$S=(cd)(c'd')\ \cdots$$

爲其兩轉換表示.茲由得施置換之文字

$$a,\ b,\ a',\ b',\cdots\cdots$$

$$c,\ d,\ c',\ d',\cdots\cdots$$

中,將其互異者全行取出,而以

$$a,\ a_1,\ a_2,\ \cdots\cdots,\ a_{n-1}$$

表之.

再於此 n 個文字之整式

$$\Delta=(a-a_1)(a-a_2)\cdots\cdots(a-a_{n-1})$$
$$(a_1-a_2)\cdots\cdots(a_1-a_{n-1})$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$(a_{n-2}-a_{n-1})$$

上行以 S,則以

$$S=(ab)(a'b')\cdots\cdots,$$

故其結果,與於 Δ 上陸續行以轉換 (ab), $(a'b')$,……者同一也. 因之,此轉換之數若爲偶數,則 Δ 不變;而若爲奇數,則成爲 $-\Delta$ 焉.更取其第二表示

$$S=(cd)(c'd')\cdots\cdots,$$

亦同樣的依轉換數之爲偶爲奇,而 Δ 不變或成爲 $-\Delta$ 也.

上兩表示中轉換之數,若其一爲偶,而其他爲奇,則 Δ 上雖行以同一置換 S,而其結果,竟生 Δ 與 $-\Delta$ 兩種之不同,豈非不合理乎?故兩表示中轉換之數,非得共爲偶或共爲奇不可也.於是,置換者,信如前節所述,得別之爲偶數置換與奇數置換二種云.

注意. 因 $(ab)(ab)=1$, 故不動置換,得置諸偶數置換中也.

例 1. 置換及其積用轉換表示者.

(i) $\begin{pmatrix}123456\\254361\end{pmatrix}=(1256)(34)=(12)(15)(16)(34).$

(ii) $(abcd)(acd)=(ab)(ac)(ad)(ac)(ad).$

或 $(abcd)(acd)=(abdc)=(ab)(ad)(ac).$

例 2. 將轉換表示改爲巡回表示者.

(i) $(ac)(bd)(ab)=(acbd).$

(ii) $(12)(34)(15)(23)(45)=(135)(24).$

第二章 羣之定義

10. 置換羣.

今就三文字 a, a_1, a_2 上所行之三置換

$$(a\ a_1\ a_2),\quad (a\ a_2\ a_1),\quad 1$$

而觀之,則知其中二者之積,有如次所示,仍與此三置換之中某一個等也.

$$(a\ a_1\ a_2)(a\ a_2\ a_1)=1,\ (a\ a_2\ a_1)(a\ a_1\ a_2)=1,$$

$$(a\ a_1\ a_2)^2=(a\ a_2\ a_1),\quad (a\ a_2\ a_1)^2=(a\ a_1\ a_2),$$

$$(a\ a_1\ a_2)\cdot 1=1\cdot(a\ a_1\ a_2)=(a\ a_1\ a_2),$$

$$(a\ a_2\ a_1)\cdot 1=1\cdot(a\ a_2\ a_1)=(a\ a_2\ a_1),$$

$$1^2=1.$$

一般,若於 n 文字 a, a_1, ……, a_{n-1} 上所施行之 g 個相異置換

$$S_0,\ S_1,\ S_2,\ \cdots\cdots,\ S_{g-1}$$

中,使其中任意兩個之積(包含一置換之二乘冪在內)復與此 g 個置換之某一個等時,則此等置換之集合,名曰**置換羣**,而作此羣之置換(互異的)之數 g,名曰其羣之**元數**.而屬於羣之得行置換之文字數 n,名曰置換羣之**次數**焉.如次之三置換

$$(a\ a_1\ a_2),\quad (a\ a_2\ a_1),\quad 1,$$

成羣者也,其元數爲 3,次數亦爲 3 焉.

注意. 三置換

$$\begin{pmatrix} a & a_1 & a_2 & a_3 \\ a_1 & a_2 & a & a_3 \end{pmatrix},\quad \begin{pmatrix} a & a_1 & a_2 & a_3 \\ a_2 & a & a_1 & a_3 \end{pmatrix},\quad 1,$$

亦成羣者也,但其中所含文字 a, a_1, a_2, a_3, 內之 a_3, 任由其間之何置換而全無所動.故當定羣之次數時,如此 a_3 之以屬於羣之任何置換而不動之文字者,不能算入次數之內,故上例之羣,其次數非 4,乃 3 也.

11. 對稱羣.

在 n 個文字 a, a_1, ……, a_{n-1} 上所行之置換中,其一之平方(二乘冪)以及其兩置換之積,仍爲此 n 文字上所行之置換也.故若將 n 個文字 a, a_1, ……, a_{n-1} 上所行置換之全體而悉取之,則其相集遂成羣也,是羣也,稱曰 n **次之對稱羣**焉.其元數爲 $n!$,因 n 文字上所行之置換,其總數爲 $n!$ 故.

例 1　三次對稱羣(元數 $3!=6$).

$$1;\quad (abc),\quad (acb),\quad (ab),\quad (ac),\quad (bc)$$

例 2. 四次對稱羣(元數 $4!=24$).

$$1,\quad (bcd),\quad (cad),\quad (dab),\quad (acb),$$
$$(bdc),\quad (cda),\quad (dba),\quad (abc),$$
$$(ab)(cd),\quad (ac)(bd),\quad (ad)(bc),$$
$$(ab),\quad (abcd),\quad (adcb),\quad (bd),\quad (ac),$$
$$(abdc),\quad (acdb),\quad (ad),\quad (bc),$$
$$(cd),\quad (acbd),\quad (adbc).$$

注意. 所設 n 個文字上得以施行之置換,其總數爲 $n!$,故 n 次置換羣之元數,不得超過 $n!$,因之常爲有限也.

12. 交代羣.

偶數置換之積,仍爲偶數置換也.故若將 n 文字上所施行偶數置換之全數而盡取之,其集合之成一羣,明已.爰名之曰 n 次之**交代羣**焉.而其元數,則如次所證,爲 $\frac{n!}{2}$.

今就 n 個文字 $a,\ a_1,\ \cdots\cdots,\ a_{n-1}$ 上所施行置換全體之集合即對稱羣者而思之,取其中偶數置換之全數,而表之爲

$$(1)\qquad S_0,\ S_1,\ S_2,\ \cdots\cdots,\ S_{g-1}.$$

此時集合(1),n 次之交代羣也.今於(1)之各置換乘以轉換 $(a\ a_1)$,則得

$$(2)\qquad S_0(aa_1),\quad S_1(aa_1),\ \cdots\cdots,\ S_{g-1}(aa_1).$$

此諸置換之爲奇數置換也明甚.且彼此互異.蓋若(2)中,$S_i(aa_1)=S_j(aa_1)$,則兩邊以 (aa_1) 右乘之,遂得 $S_i=S_j$ 故耳.

復次,若以 T 爲任意之奇數置換,則 $T(aa_1)$ 乃偶數置換

也,因之必與(1)中某一個等.即

$$T(a\ a_1)=S_i.$$

此兩邊以$(a\ a_1)$右乘之,則

$$T(aa_1)^2=S_i(aa_1),\qquad \therefore\quad T=S_i(aa_1).$$

是則 T 屬於集合(2)也.

是種屬於(2)之 g 個之置換,任何一個皆奇數置換,且彼此互異.不僅此也,凡奇數置換皆屬於(2).故由(1)與(2),可知 n 次對稱羣之全置換悉盡於斯.因之

$$g+g=n!,$$

$$\therefore\qquad g=\frac{n!}{2}.$$

即謂 n 次交代羣之元數爲 $\frac{n!}{2}$ 也.

例 1. 三次交代羣(元數 3).

$$1,\quad (abc),\quad (acb)$$

例 2. 四次交代羣(元數 12).

$$1,\quad (bcd),\quad (cad),\quad (dab),\quad (acb),$$
$$(bdc),\quad (cda),\quad (dba),\quad (abc),$$
$$(ab)(cd),\quad (ac)(bd),\quad (ad)(bc).$$

13　羣之基本性質.

今以 $\mathfrak{G}$ 爲一置換羣,則 $\mathfrak{G}$ 乃有次之四性質:

(i)　屬於 $\mathfrak{G}$ 之任意兩置換之積仍屬於 $\mathfrak{G}$

(ii)　屬於 $\mathfrak{G}$ 之三置換之積間,組合法則常成立.

(iii) $\mathfrak{G}$ 含有不動置換.

(iv) 對於屬於$\mathfrak{G}$之任意之置換,其逆置換必存在於$\mathfrak{G}$中.

證明. 今以$\mathfrak{G}$爲一置換羣.

(i) 全然置換羣之定義者也.

(ii) 由置換之積之性質自明.(參照第 2 節)

(iii) 以 S 爲屬於$\mathfrak{G}$之一置換,若 S 爲不動置換,則無復問題已.反之,若 S 非不動置換時,爰作 S 之乘冪

$$S,\ S^2,\ S^3,\ \cdots,\ S^p,\ \cdots,\ S^q,\ \cdots,$$

則由(i)知其皆屬於$\mathfrak{G}$也.然置換羣之元數常爲有限(第11節注意),故上乘冪中非有相等者不可.茲以

$$S^p=S^q \qquad (q>p).$$

S^p乃一置換,故由第3節所述,其逆置換S^{-p}必存在也.(雖S^{-p}屬於$\mathfrak{G}$與否尙不可知).今以此乘上式之兩邊,則

$$S^q\ S^{-p}=S^p\ S^{-p},$$

$$\therefore \qquad S^{q-p}=1 \qquad (q-p>0).$$

然 S 之乘冪S^{q-p}屬於$\mathfrak{G}$,故$\mathfrak{G}$中有不動置換 1 存在也.

(iv) 以 S 爲$\mathfrak{G}$之任意一置換.若 S 爲不動置換,則

$$S\cdot S=1\cdot 1=1,$$

$$\therefore \qquad S=S^{-1} \qquad \text{(參照第 3 節)}$$

若 S 非不動置換,則如證明(iii)中者然,

$$S^{q-p}=1 \qquad (q-p>0).$$

但 $S\neq 1$ 故 $q-p>1$. 因之由第 4 節所述,

$$S^{q-p}=S\cdot S^{q-p-1}.$$

$$\therefore \quad S\cdot S^{q-p-1}=1,$$

$$\therefore \quad S^{q-p-1}=S^{-1} \qquad (\text{參照第 3 節}).$$

如是,對於任意之置換 S, 其逆置換 S^{-1} 必存在於$\mathfrak{G}$中也.

14. 元素與其結合.

吾人在數學上所討論各個之物,如代數學上之數,幾何學上之點,線等,總稱之概曰**元素**.置換亦一種元素也.若有多數之元素,試將其概括而思之,則此曰元素之集合.更嚴格以言:今於此有由若干元素而成之一團體焉,若對於任意取來之一元素,能判定其含於此團體之中與否,或假定得以判定之之時,則此團體稱曰**集合**.作一集合之元素,其數有限者有之,無限者亦有之.至有限無限之分,可先將無限者定其義然後其不適合此者,卽有限也.茲有甲乙兩集合,若對甲之各元素,可每使乙元素之一與之對應,反之,對乙之各元素,可每使甲元素之一與之對應時,則此兩集合,名曰具有同一之濃度,或曰同等.今取 1, 2, 3 等正整數之全體爲甲集合,2, 4, 6 等正偶數之全體爲乙集合,若對甲之 1, 使乙之 2, 甲之 2, 使乙之 4, 一般,對甲之 h, 使乙之 $2h$ 相對應時,則此兩集合之元素間,其一一對應,已告成立,可知此兩集合正具有同一之濃度也.且就此例而觀,甲集合乃正整數之全體,故彼僅由偶數而成之乙集合,是不過其一部分而包含厥中,而卻兩成同等也.

如是者之一集合與由其元素之一部分所成之集合同等時，此集合曰含有無限多之元素云.於是其非無限者卽係有限，由有限個元素而成之兩集合,若具有同一之濃度,則兩者中所含元素之數,以常語言,是曰同一也.

且當欲論理的組成數學時,非先將集合之元素間相等,或不等之定義與之不可.此定義之立,其法固可隨吾人意,但僅次之三條件,則無論如何,非滿足不可者也.

(i) 各元素,以之作定義之結果言,乃等於其自身也;又A等於B時,B亦等於A.

(ii) 兩元素,或等或不等,二者必居其一,且以此爲限.

(iii) A等於B,而B等於C時,則A等於C.

除此三條以外,再無有他制限,而今日之數學上,其相等之定義,咸適合此條件焉.

復次,請論元素之結合.如於置換(bcd),乘以(ab),則成爲$(abcd)$,此由形式上觀,乃由(bcd)與(ab)兩置換而想定$(abcd)$之置換者也.一般,對於兩元素A,B,且對其順序,而想定第三之元素C時,此名曰A與B之結合,而C則曰結合之結果.就上例言,乘(ab)於(bcd)者,兩者之結合也;其積$(abcd)$者,此結合之結果也.且兩元素結合之方法,依時依地,原有種種,而不可以一概論,第吾人之所論者,乃其所謂一意的,卽若元素A等於A',B等於B'時,則A與B結合之結果,與A'與B'者等者是也.又結合之種類亦不限於唯一,如就算術觀,加法爲

一結合,乘法亦一結合而與是異也.若就一集合言,當僅論其一種類之結合時,則兩元素A,B之結合(且就A,B之順序),仍與置換者同樣,通常皆以A·B或AB表之,而其結果爲C,則以

$$AB=C$$

示之也.用此記法時,A與B之結合,名曰A以B乘,而其結合之結果,名曰其積焉.

關於結合之須特別留意者,乃被結合元素之順序是.在普通之算術上,2與3之積,3與2之積,雖係同一,然一般討論結合時,如就置換所見,在A,B之順序所行者,與在BA,之順序所行者,其結果未見其必一致也.若兩結果一致,卽AB=BA時,則對此兩元素之結合(乘法),名曰**交換法則**成立;而A,B兩元素,則曰**交換可能**云.

又就三元素A,B,C之結合(乘法)言,(AB)C與A(BC),其結果不限其必一致也.但苟一致,卽

$$(AB)C=A(BC)$$

時,則對此三元素之結合,曰**組合法則**成立云.

元素之結合,如

$$2\cdot3=6,\qquad (b\,c\,d)(a\,b)=(a\,b\,c\,d)$$

然,由兩元素,在某法則之下,以導出其結合之結果而與以定義者,固有之矣;反是,於此有一集合,其屬於此集合之兩元素,僅假定其結合爲可能,而再進而推理者,亦或有焉.斯時也,關於元素之結合,若不設立若干之公理,而欲推理演繹者,未之

或能也.此公理之設立,依其方法如何,而構成羣,環,體等諸對象,隨之產生此諸種之理論.次節所示,乃關於羣之公理也,卽所以示羣之一般的定義焉.

15. 羣之一般的定義.

若構成羣之元素爲置換時,則以作羣之定義者,如前所述,只需第13節之性質(i)爲已足也.但所論者若出乎置換以外,且不問元素之種類如何而求其一般皆可通用,則除上(i)外,再加該節所舉之其他三性質而定其義如次焉可.

由有限或無限個元素而成之集合 $\mathfrak{G}$,若滿足次之四條件時,則 $\mathfrak{G}$ 曰羣

(i) $\mathfrak{G}$ 之任意兩元素(相等者或不等者)之積仍屬於 $\mathfrak{G}$

(ii) $\mathfrak{G}$ 之任意三元素 A, B, C 之結合上,組合法則常告成立.

$$(AB)C=A(BC).$$

(iii) 任選 $\mathfrak{G}$ 之何元素以爲元素 A,而常有

$$AE=A$$

之關係之元素E, $\mathfrak{G}$ 之中至少有一個.

(iv) 對於 $\mathfrak{G}$ 之一元素A而滿足

$$AX=E$$

之元素 X,存在於 $\mathfrak{G}$.但式中 E,卽(iii)中所述元素E之意.

上定義中 (iii) 之E者,非對各個之元素而分別定之之物,乃爲號稱E之一特殊元素,無論選 $\mathfrak{G}$ 之任何元素以爲A,

而常成AE=A者也.此特殊元素E,名曰羣之**主元素**或**單一元素**.主元素之數,雖有如後之所證,乃係唯一的(第18節),但尚未決定之先,則視爲有若干個主元素而演繹之可也.今若取此中任意一個E,則與此主元素相應,且對$\mathfrak{G}$之任意元素A而滿足AX=E之X,存在於$\mathfrak{G}$,是卽(iv)之意義也.此X名曰A之**逆元素**,或單曰**逆**,此逆元素,亦如後所證,對於一元素,只唯一個存在焉(第18節).

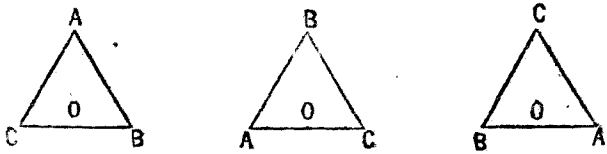
若干元素相集以成羣,若其互異元素之數爲有限,則此名曰**有限羣**,若其數爲無限,則曰**無限羣**,有限羣中,其互異元素之總數,名曰羣之**元數**,而元數g之羣,則曰g元之羣或g元羣焉.

16.　羣之例(I)　三角羣.

茲取一正三角形ABC,且以使其運動之前後占有同一空間之方法而將此三角形運動.如令其在中心O之周圍迴轉120°(與時鐘之指針成反對方向),則其結果,頂點A,B,C便分別來到C,A,B始初所占之位置,而三角形自身,仍與原來者占同一之空間也.因之,此迴轉,卽爲吾人所論運動之一焉.又於中心O之周,依同方向雖迴轉480°,然其結果,仍與前同,亦爲頂點A,B,C來到C,A,B所占之位置而已.是種產生同一結果之兩運動,卽視之爲相等者.於是吾人於此所論之運動,究不外次之六者之或一焉.

(i)　於三角形之中心O之周圍,作120°及240°之迴轉

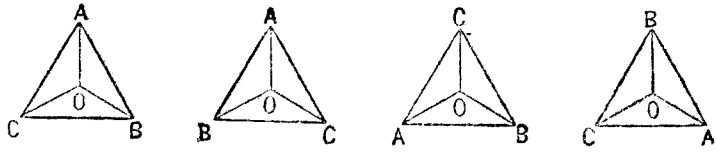
者(與時鐘之指針成反對方向行之).



此運動之結果,頂點 A, B, C 原來所占之位置,今則 B, C, A 及 C, A, B 分別來居其地.因之此兩運動,遂各別以 $\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$ 及 $\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$ 表之也.

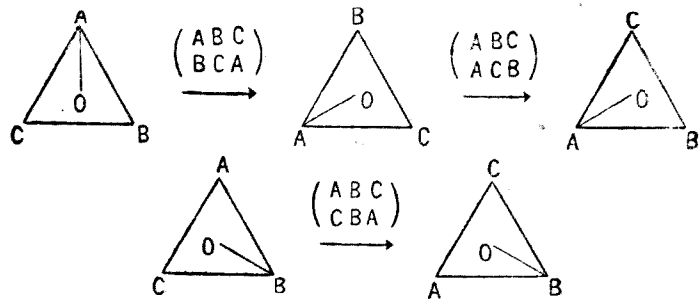
(ii) 在固定於三角形之三軸 OA, OB, OC 之周,作 180° 之迴轉者.

以 OA 爲軸作 180° 之迴轉,即頂點 B, C 將其位置轉倒,而 A 則保留原位置不變,以故此運動乃以 $\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$ 表之.同樣以 OB, OC 爲軸之迴轉,分別記以 $\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$, $\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$.



(iii) 三角形全然不使動者.此以 $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ 表之.

復次,如將 ΔABC, 於 O 之周圍迴轉 120° (以與時鐘之指針之反對方向行之),更續以此於軸 OA 之周迴轉 180°,則其結果,於最初頂點 A, B, C 所占之位置, C, B, A 分別來居其處,是則兩運動續行之結果,與將三角形於軸 OB 之周迴轉 180° 者等也.



如是者之先行運動甲,繼於此續行運動乙,名曰以乙乘甲,若兩運動續行之結果與行運動丙者一致時,則丙名曰甲乙之積云.如

$$\begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}=\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}.$$

運動之相等以及其積,若如上定義時,則上記之六運動

$$\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix},\ \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix},\ \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},$$

$$\begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix},\ \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix},\ \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix};$$

如次所示,滿足前節之四條件,因而成一羣也.

(i)　兩運動雖繼續施行,然 ΔABC 之與原來者共占同一之空間明已.但於運動之前後,ΔABC 得占同一空間之運動,乃與上記六運動之一等.故兩運動之積,等於此六運動之或一也.

(ii)　今取三運動甲,乙,丙.

$$甲=\begin{pmatrix} A & B & C \\ A' & B' & C' \end{pmatrix},\ 乙=\begin{pmatrix} A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix},\ 丙=\begin{pmatrix} A'' & B'' & C'' \\ A''' & B''' & C''' \end{pmatrix}$$

式中 A′, B′, C′; A″, B″, C″; A‴, B‴, C‴ 者,皆係將 A, B, C 書於某次序者也, $\begin{pmatrix} A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix}$, 乃以示頂點 A′, B′, C′ 之位置, A″, B″, C″ 分別來到之意.丙式準此.

於是

$$(甲\cdot乙)丙=\left\{\begin{pmatrix} A & B & C \\ A' & B' & C' \end{pmatrix}\begin{pmatrix} A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix}\right\}\begin{pmatrix} A'' & B'' & C'' \\ A''' & B''' & C''' \end{pmatrix}$$

$$=\begin{pmatrix} A & B & C \\ A'' & B'' & C'' \end{pmatrix}\begin{pmatrix} A'' & B'' & C'' \\ A''' & B''' & C''' \end{pmatrix}=\begin{pmatrix} A & B & C \\ A''' & B''' & C''' \end{pmatrix};$$

$$甲(乙\cdot丙)=\begin{pmatrix} A & B & C \\ A' & B' & C' \end{pmatrix}\left\{\begin{pmatrix} A' & B' & C' \\ A'' & B'' & C'' \end{pmatrix}\begin{pmatrix} A'' & B'' & C'' \\ A''' & B''' & C''' \end{pmatrix}\right\}$$

$$=\begin{pmatrix} A & B & C \\ A' & B' & C' \end{pmatrix}\begin{pmatrix} A' & B' & C' \\ A''' & B''' & C''' \end{pmatrix}=\begin{pmatrix} A & B & C \\ A''' & B''' & C''' \end{pmatrix}.$$

$$\therefore \quad (甲\cdot乙)丙=甲(乙\cdot丙).$$

(iii) 運動 $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$,乃不變更頂點之位置者.故雖行一運動甲,繼續再行 $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$,其結果與單行甲者同一.因之運動 $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ 具有主元素之性質也.

(iv) 今以由甲運動,頂點 A, B, C 爲達到某位置.此時使此三角形之頂點回復原來位置之運動,必定存在.茲以之爲丁,則運動甲及丁續行之結果,其與頂點全然不動之運動同一,明甚.是卽甲丁之積,與主元素 $\begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$ 等,因之對甲言,其逆元素丁爲存在也.

注意. 由上之運動,頂點 A, B, C 乃爲他之頂點所置換.故此運動者,正以示三文字 A, B, C 間之置換;而運動之記

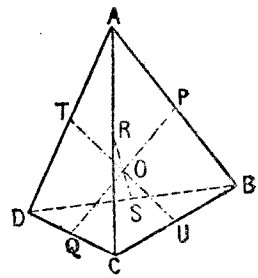
號如$\begin{pmatrix}A&B&C\\B&C&A\end{pmatrix}$，亦得以視爲表A,B,C之置換者也.誠如所論，則上記之運動羣,卽爲由A,B,C上所行之置換而成之對稱羣耳.實則運動之積爲與其相當之置換之積一致,亦容易證明故也.

此外,正n邊形之運動亦成羣,其元數爲$2n$,是蓋與本節所示,同一論之可也.

17. 羣之例(II). 四面體羣.

試以前例之思想,再就正四面體ABCD一論之.今將在運動前後此四面體仍占同一空間之運動思之,而其中產生同一結果之運動,則視爲相等者.於是此四面體之運動,乃與次之十二運動之或一者等焉.

茲以O爲四面體之中心,OA,OB,OC,OD爲固定於四面體之四軸,PQ,RS,TU爲過對稜(AB,CD),(AC,BD),(AD,BC)之中點之三軸.(此等軸可視爲固定於四面體者.)



(i) 於四軸OA,OB,OC,OD之周之120°及240°之八迴轉.(將目置於O點而觀時,將四面體,以ΔBCD依時鐘之指針之反對方向而迴轉之方向,令其在OA之周圍迴轉.至對他軸之迴轉方向,皆準此類推.)

用前例同樣之記法,此八運動表之如次:

$$\begin{pmatrix}A&B&C&D\\A&C&D&B\end{pmatrix},\ \begin{pmatrix}A&B&C&D\\D&B&A&C\end{pmatrix},\ \begin{pmatrix}A&B&C&D\\B&D&C&A\end{pmatrix},\ \begin{pmatrix}A&B&C&D\\C&A&B&D\end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & B & D & A \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & A & C & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ B & C & A & D \end{pmatrix}.$$

(ii) 以 PQ, RS, TU 爲軸之 180° 之三迴轉:

$$\begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix}, \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix}.$$

(iii) 四面體之全然不動者,卽

$$\begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix}.$$

復次,與前例同樣,將甲乙兩運動繼續施行之舉,定義曰乘乙於甲,則上之十二運動,乃成羣也.其證明全然與前節同樣.此羣卽名曰**四面體羣**焉.

此外,由正八面體及正二十面體之運動,尙得構成爲羣.前者之元數24,曰**八面體羣**;後者之元數60,曰**二十面體羣**.

注意 1. 由立方體及正十二面體,雖同樣得以成羣,然其與八面體羣及二十面體羣乃爲同型也.(**同型之意義**,述在後第21節.)

注意 2. 如於前節之注意,若將正四面體 ABCD 之運動,視爲 A, B, C, D 四文字間之置換,則上記之十二運動[(i), (ii), (iii)],乃構成一四次之交代羣焉.

18 主元素與逆元素.

當論羣時,關於其主元素與逆元素間須注意之事項,試列舉二三如次:

(I)　羣之主元素者,乃於任意一元素,無論以之右乘或左乘,皆不變其元素者也.今以E爲羣𝔊之主元素之一,而A爲任意一元素,則

$$AE=A, \qquad EA=A.$$

前者固卽主元素之定義自身,今試就後者之證明而述之.先令

$$EA=B. \tag{1}$$

由第15節羣之成立條件(iv),則滿足

$$AX=E \tag{2}$$

之元素X確乎存在.以之右乘於(1)之兩邊,

$$(EA)X=BX.$$

由組合法則,得

$$E(AX)=BX.$$

$$\therefore \qquad EE=BX. \qquad (\because AX=E.)$$

但E乃主元素,故由羣之成立條件(iii),

$$EE=E.$$

故

$$BX=E.$$

以此與(2)比較,

$$BX=AX. \tag{3}$$

次以如$XY=E$者之元素Y,右乘於(3)之兩邊,得

$$(BX)Y=(AX)Y,$$

由之, $$B(XY)=A(XY),$$

$$\therefore \quad BE=AE. \qquad (\because XY=E.)$$

然E係主元素.故

$$B=A$$

因之由(1), $$EA=A.$$

(II) 羣之主元素,僅唯一個.嚴格言之,則謂凡主元素皆相等也.

證明. 設以E爲一主元素, E′ 爲他一主元素.由(1),則對任意之元素A,

$$AE=A=EA$$

也.今代A而置以E′,則

$$E'E=EE'.$$

但E, E′皆主元素,故

$$E'E=E', \quad EE'=E,$$

故 $$E'=E$$

注意. 如(I) (II)之所示,羣之主元素只唯一個,而對乘法,具有與1同樣之性質,故通常皆以1表之.

(III) 一元素乃其逆元素之逆也.卽若A爲一元素,

$$AX=E \quad (E=1),$$

則又有

$$XA=E$$

也.換言之,卽謂一元素之逆元素者,以之右乘或左乘於A,其

積皆與主元素等者也.

證明. 令 $AX=E$. 先以

$$XA=B$$

此兩邊皆以 X 右乘之,則

$$(XA)X=BX,$$

即

$$X(AX)=BX.$$

$$\therefore \quad XE=BX,$$

$$\therefore \quad X=BX.$$

次之,於此兩邊,以 X 之逆元素 Y 右乘之,再適用組合法則.

則

$$XY=B(XY).$$

$$\therefore \quad E=BE.$$

但

$$BE=B,$$

故

$$B=E.$$

因之

$$XA=E.$$

(IV) 一元素之逆只唯一個(證如下),而元素 A 之逆,即以 A^{-1} 表之.

證明. 以 A 爲一元素,及

$$AX=E, \quad AX'=E \quad (E=1),$$

則

$$X(AX')=XE,$$

即

$$(XA)X'=XE.$$

但由(III),

$$XA=E,$$

故

$$EX'=XE.$$

$$\therefore \quad X' = X.$$

(V) 關於羣之元素之連乘積,冪以及其逆,第4節中就置換所述之各事項,在此均同樣成立,至其證明亦全無二致,而冪與其逆之記號亦同樣採用.如羣之元素之冪 A^m 之逆,以 A^{-m} 表之,而對之又有

$$(A^{-1})^m = A^{-m}$$

者是也.

例 1. $(AB)^{-1} = B^{-1}A^{-1}$.

例 2. 一羣之三元素 A, B, C, 若 AC = BC, 則 A = B. CA = CB 時,亦 A = B. (試以 C 之逆右乘或左乘於其兩邊,再適用組合法則便得.)

19. 有限羣.

定理. 第15節羣之成立條件中(iii)及(iv),若在有限羣時,則得以次之條件代替之,卽:

若 AC = BC 或 CA = CB, 則 A = B.

[此條件暫記曰(v).]

證明. 由羣之成立四條件得以導出條件 (v), 則已於前節述之矣.因之於有限個元素,如互異之 g 個元素

$$A, A_1, A_2, \cdots\cdots, A_{g-1} \text{(此集團暫以 } \mathfrak{G} \text{ 示之.)}$$

之間,若第15節之條件 (i), (ii) 及本節之條件(v)得成立時,則只須示由此而自滿足條件(iii)及(iv)爲已足也.

今取 $\mathfrak{G}$ 之一元素 A, 而無限的作其冪

$$A, A^2, A^3, \cdots\cdots.$$

於是由(i),知此等皆屬於$\mathfrak{G}$也.但屬於$\mathfrak{G}$者之數爲有限,故上所作諸冪之中非有相等者不可.今以之爲

$$A^{r+s}=A^r.$$

再於此應用條件(ii)卽組合法則,則

$$A^{s+1}A^{r-1}=AA^{r-1}.$$

更應用條件(v),則

$$A^{s+1}=A.$$

於此兩邊以$\mathfrak{G}$之任意元素A_i左乘之,

$$A_iA^{s+1}=A_iA.$$

由是　　$A_iA^s\cdot A=A_i.A$　　(組合法則)

故由條件(v),

$$A_iA^s=A_i.$$

是卽A^s者,具有第15節條件(iii)中E之職能也.由是,主元素之存在可知.

復次,以$\mathfrak{G}$之任意元素A_i左乘$\mathfrak{G}$之各元素,乃有

$A_iA, A_iA_1, A_iA_2, \cdots\cdots, A_iA_{g-1}$ (此集團以$\mathfrak{H}$示之,).

然此諸積皆互異,蓋由條件(v),若$A_iA_h=A_iA_k$,則有$A_h=A_k$故也.且此g個積,由條件(i),悉屬於$\mathfrak{G}$.故以屬於$\mathfrak{H}$之積能盡$\mathfrak{G}$中元素之全數.因之$\mathfrak{H}$中,與$\mathfrak{G}$之主元素E相等者非存在不可.是卽謂對於$\mathfrak{G}$之任意一元素A_i,而能有$A_iA_j=E$者之元素A_j,必存在於$\mathfrak{G}$中也.此無外乎第15節之條件(iv)耳.故云云

注意. 本節之定理,僅對有限羣而言,若對無限羣,則不得成立也.如就正整數之全體

$$1, 2, 3, 4, \cdots\cdots$$

思之,若取數之乘法以爲元素之結合,則條件(i), (ii) 及 (v)之能滿足明矣;又與主元素相當之數 1 亦存在,然對 1 以外之數,其逆元素不存在也.故此時正整數之集團不能成羣焉.

就元素之無限集合言,條件(i), (ii)及(v)雖成立,而(iv)不成立時,則此集合呼曰**半羣**者有之.

20. Abel 氏羣.

兩元素 A, B 之乘法中,若交換法則(AB=BA)成立時,則 A 與 B 曰**交換可能**.就一羣言,若其任意兩元素爲交換可能時,則此羣曰**交換可能羣**,或曰 Abel 氏羣.

如取一置換羣

$$\begin{array}{ccc} 1 & (abc) & (acb) \\ (de) & (abc)(de) & (acb)(de), \end{array}$$

由實際計算,即可知其任意兩元素之乘法間,交換法則實成立也.故此爲 Abel 氏羣焉.

在 Abel 氏羣,交換法則固成立已,而由羣之定義,則組合法則亦當然適用.故如下所證明,其有限個元素之連乘積,不論因子之順序如何,常一定也.因之 Abel 氏羣之元素之乘法,可以與普通之數同樣駕御焉.

且置換原可以轉換之積表示者已.故欲證明上所言,則

僅示若干元素之連乘積,與將其任意二因子相互交換者等可也.

今以 $A_1, A_2, \cdots\cdots, A_m$ 爲 Abel 氏羣之元素, A_i 及 A_{i+j} 爲其中任意之兩個.於是由組合法則之適用(參照第 4 節及第 18 節),乃有

$$\begin{aligned}
&A_1\cdots\cdots A_{i-1}A_iA_{i+1}A_{i+2}\cdots\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}(A_iA_{i+1})A_{i+2}\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}(A_{i+1}A_i)A_{i+2}\cdots A_m \qquad (\because\ A_iA_{i+1}=A_{i+1}A_i)\\
=&A_1\cdots\cdots A_{i-1}A_{i+1}A_iA_{i+2}\cdots\cdots A_m \qquad (\text{參照第 4, 18 節}).
\end{aligned}$$

同樣

$$\begin{aligned}
&A_1\cdots\cdots A_{i-1}A_{i+1}A_iA_{i+2}A_{i+3}\cdots\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}A_{i+1}A_{i+2}A_iA_{i+3}\cdots\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}A_iA_{i+1}A_{i+2}A_{i+3}\cdots\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}A_{i+1}A_{i+2}A_iA_{i+3}\cdots\cdots A_m
\end{aligned}$$

將此反覆 j 回,

$$\begin{aligned}
&A_1\cdots\cdots A_{i-1}A_iA_{i+1}\cdots\cdots A_{i+j-1}A_{i+j}A_{i+j+1}\cdots\cdots A_m\\
=&A_1\cdots\cdots A_{i-1}A_{i+1}\cdots\cdots A_{i+j-1}A_{i+j}A_iA_{i+j+1}\cdots\cdots A_m
\end{aligned}$$

更同樣行之,則此最後者便等於

$$A_1\cdots\cdots A_{i-1}A_{i+j}A_{i+1}\cdots\cdots A_{i+j-1}A_iA_{i+j+1}\cdots A_m.$$

因之

$$\begin{aligned}
&A_1\cdots\cdots A_{i-1}A_iA_{i+1}\cdots A_{i+j-1}A_{i+j}A_{i+j+1}\cdots\cdots A_m.\\
=&A_1\cdots\cdots A_{i-1}A_{i+j}A_{i+1}\cdots\cdots A_{i+j-1}A_iA_{i+j+1}\cdots\cdots A_m.
\end{aligned}$$

此卽前所欲示者也.

21. 羣之同態.

兩羣$\mathfrak{G}$與$\mathfrak{G}'$,若其元素間,得有適合次之條件之對應時,則兩羣名曰同態或同型焉.

(i) 對於$\mathfrak{G}$之一元素,$\mathfrak{G}'$之一而且唯一之元素與之對應.

(ii) 對於$\mathfrak{G}'$之一元素,$\mathfrak{G}$之一而且唯一之元素與之對應.

(iii) 對於$\mathfrak{G}$之兩元素A, B,若$\mathfrak{G}'$之二元素A', B'與之對應時,則積A'B'與積AB相對應.

若羣$\mathfrak{G}$之元素無有相等者,而若$\mathfrak{G}'$中亦然,則上之定義無復疑問;苟不如是,則尚需一言之說明.卽其所謂對於$\mathfrak{G}$之元素A,$\mathfrak{G}'$中之唯一元素A'與之對應者,乃係謂與A對應之$\mathfrak{G}'$中元素,僅與A'等者之意云耳.

例. 下列左右兩欄,乃六次及八次之置換羣.

$$\begin{pmatrix} A & B & C & D & E & F \\ A & C & D & E & B & F \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & c & d & a & f & g & h & e \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ A & D & E & B & C & F \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ c & d & a & b & g & h & e & f \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ A & E & B & C & D & F \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & a & b & c & h & e & f & g \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ C & B & F & D & A & E \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ e & f & b & a & h & g & c & d \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ F & b & E & D & C & A \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & g & f & e & d & c & b & a \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ E & B & A & D & F & C \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & c & g & h & a & b & f & e \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ B & F & C & A & E & D \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ e & a & d & h & f & b & c & g \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ F & D & C & B & E & A \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ f & e & h & g & b & a & d & c \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ D & A & C & F & E & B \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & f & g & c & a & e & h & d \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ B & C & A & E & F & D \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & d & h & e & b & c & g & f \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ C & A & B & F & D & E \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & e & f & b & d & h & g & c \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ C & F & D & A & B & E \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ f & b & a & e & g & c & d & h \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ D & E & A & C & F & B \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ c & b & f & g & d & a & e & h \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ D & C & F & E & A & B \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ f & g & c & b & e & h & d & a \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ E & F & B & A & D & C \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & d & c & g & e & a & b & f \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ E & A & D & F & B & C \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ c & g & h & d & b & f & e & a \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ B & E & F & C & A & D \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & e & a & d & g & f & b & c \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ B & A & E & F & C & D \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & h & e & a & c & g & f & b \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ C & D & A & B & F & E \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & a & e & f & c & d & h & g \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ D & F & E & A & C & B \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & c & b & f & h & d & a & e \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ E & D & F & B & A & C \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & h & d & c & f & e & a & b \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ F & C & B & E & D & A \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ e & h & g & f & a & d & c & b \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ F & E & D & C & B & A \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & f & e & h & c & b & a & d \end{pmatrix}$$

$$\begin{pmatrix} A & B & C & D & E & F \\ A & B & C & D & E & F \end{pmatrix} \qquad \begin{pmatrix} a & b & c & d & e & f & g & h \\ a & b & c & d & e & f & g & h \end{pmatrix}$$

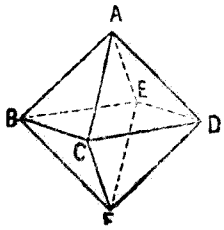
今於此而令左右對立之置換相對應,則對於左欄兩置換之積,右欄相應兩置換之積便與之對應也.如

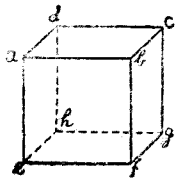
$$\begin{pmatrix} A & B & C & D & E & F \\ A & C & D & E & B & F \end{pmatrix}\begin{pmatrix} A & B & C & D & E & F \\ B & C & A & E & F & D \end{pmatrix} = \begin{pmatrix} A & B & C & D & E & F \\ B & A & E & F & C & D \end{pmatrix},$$

$$\begin{pmatrix} a & b & c & d & e & f & g & h \\ b & c & d & a & f & g & h & e \end{pmatrix}\begin{pmatrix} a & b & c & d & e & f & g & h \\ a & d & h & e & b & c & g & f \end{pmatrix} = \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & h & e & a & c & g & f & b \end{pmatrix}.$$

故此兩羣爲同態.

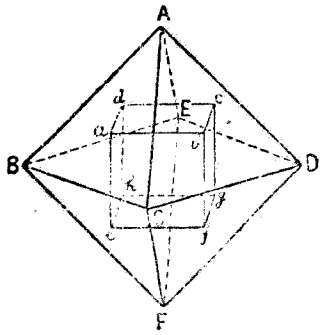
又關於此兩羣,尙欲一言.今取正八面體 ABCDEF 而就其在運動之前後仍占同一空間之運動討論之,若其相等不等以及結合之定義,與論正四面體者同樣,則是等運動相集乃成羣也.且各運動之表示,若仍照第17節之方法,是卽以左欄中所記之置換而克示;而右欄則同樣視爲表示立方體 $abcd-efgh$ 之運動羣者可.





但如上所述,左右兩欄之羣,同態者也.故由正多面體之運動所成之羣中,其由正八面體與由正六面體所成者乃係同態.

今爲使此兩羣之對應關係更爲明瞭起見,乃以正八面體 ABCDEF 中聯結其隣接兩面之中心所得之立方體爲 $abcd-efgh$. 於是八面體運動時,立方體亦伴之運動,反之立方體運動時,八面體亦伴之運動.故上述之對應者,乃使此相伴之運動對立者也.



又在正二十面體中,若連結其隣接面之中心,則得一正十二面體,故由正二十面體及正十二面體之運動所成之羣,亦同態也.

且吾人若抽象的討論羣時,則同態之羣,得視爲全然同一者也.固然,當其論諸種羣之性質時,羣或其元素之表示法,一般原係必要;但若僅考察與之無關係之性質,換言之,即僅論其由元素之結合法則之性質時,則便宜上,一個羣雖以其

同態之羣代用之無妨也.本篇中則卽以論述與羣之表示方法無關係之諸性質爲主焉.

第三章 約 羣

22. 約羣.

今就四文字 a, b, c, d 之交代羣(第12節例2)及對稱羣(第11節例2)而觀,則前者之置換,皆屬於後者中也.如斯一羣 $\mathfrak{H}$ 之元素,全屬於羣 $\mathfrak{G}$ 時,則 $\mathfrak{H}$ 名曰 $\mathfrak{G}$ 之約羣焉.

主元素者,乃以其自身而成羣也.此名曰主元素羣.但任何羣皆含主元素,故凡羣皆以主元素羣爲約羣而包含之也.

定理. 在有限羣 $\mathfrak{G}$ 之若干元素之集合 $\mathfrak{H}$ 中,若其任意兩元素(相等或互異)之積,仍屬於 $\mathfrak{H}$ 時,則 $\mathfrak{H}$ 爲一羣,因之卽爲 $\mathfrak{G}$ 之約羣.

證明. 今取 $\mathfrak{H}$ 之一元素 H,而無限的作其冪

$$H,\ H^2,\ H^3,\ \cdots\cdots$$

於是由假設,凡此種種皆屬於 $\mathfrak{H}$ 也.但屬於 $\mathfrak{H}$ 中元素之數爲有限,故此諸冪中,非有相等者存在不可.茲以之爲

$$H^{r+s}=H^s.$$

然 $\mathfrak{G}$ 乃一羣,故其元素 H^s 之逆 H^{-s} 存在於 $\mathfrak{G}$ 內.將此乘上式之兩邊,得

$$H^r=E \quad (E\text{爲}\mathfrak{G}\text{之主元素}).$$

但由假設,H 之冪,原屬於 $\mathfrak{H}$.故主元素 E 屬於 $\mathfrak{H}$.

次之,若$r=1$,則$H=E$,因之$H\cdot H=E$.即H乃其自身之逆元素也.反之,若$r>1$,則

$$H\cdot H^{r-1}=E,$$

是即H^{r-1}者H之逆元素之謂也.

以故$\mathfrak{H}$中,主元素及其各元素之逆,皆包含在內.且$\mathfrak{H}$之元素本屬於$\mathfrak{G}$,故對其三元素之乘法,組合法則之成立蓋當然也.故$\mathfrak{H}$爲羣焉.

系. 兩個有限羣中共通元素之全體亦成羣. (此約羣名曰兩羣之最大公約羣.)

蓋若A及B爲有限羣$\mathfrak{G}$及$\mathfrak{G}'$共通之二元素,則其積AB,一方屬於$\mathfrak{G}$,他方亦屬於$\mathfrak{G}'$.因之積AB亦兩羣共通者也.

注意. 此定理,當$\mathfrak{G}$爲有限羣,或$\mathfrak{H}$爲由有限個之元素而成時,固爾成立,但若$\mathfrak{H}$含有無限多之元素時,則未見其必成立也.如以正有理數爲元素,而以乘法爲元素之結合,則正有理數之全體成羣也.但由此中取出正整數之全體,雖二整數之積仍爲整數,然僅以此卻不能成羣焉.(參照第19節.)

23. 傍系.

設$\mathfrak{H}$爲羣$\mathfrak{G}$之約羣(元數h),而以其元素爲

(1)　　$H_0, H_1, H_2, \cdots\cdots, H_{h-1}.$

乃於此之各個以$\mathfrak{G}$之元素A右乘之,則其所得h個之積

(2)　　$H_0A, H_1A, H_2A, \cdots\cdots, H_{h-1}A$

皆屬於$\mathfrak{G}$而彼此互異.蓋因$\mathfrak{G}$原爲羣,故(2)之積之屬於$\mathfrak{G}$,明

已;又若 $H_iA=H_jA$, 則 $H_i=H_j$ 故也.

以$\mathfrak{G}$之元素 A, 右乘於約羣$\mathfrak{H}$之各元素而作成一組之積(2)時,此名曰於$\mathfrak{H}$之**右乘以** A;或曰**右乘** A 於$\mathfrak{H}$,而積之一組(2),則以$\mathfrak{H}A$表之.

定理. 元素 A 屬於$\mathfrak{H}$時,則$\mathfrak{H}A$與$\mathfrak{H}$一致;反之, A 不屬於$\mathfrak{H}$時,則$\mathfrak{H}A$與$\mathfrak{H}$無共通之元素.

證明. A 爲$\mathfrak{H}$之元素時,則(2)之元素皆屬於$\mathfrak{H}$也.但(2)乃由與$\mathfrak{H}$同數個之互異元素而成.故(2)者,不過將(1)之元素置換爲某順序者已耳.是卽在此時$\mathfrak{H}A$與$\mathfrak{H}$一致.

復次,若(2)之元素 H_iA 與$\mathfrak{H}$之元素 H_j 等,卽

$$H_iA=H_j$$

時,將此兩邊以 H_i 之逆元素 H_i^{-1} 左乘之,則得

$$A=H_i^{-1}H_j.$$

但$\mathfrak{H}$爲羣,故 H_i^{-1} 屬於$\mathfrak{H}$, 隨之積 $H_i^{-1}H_j$ 亦屬於$\mathfrak{H}$. 故 A 不得不爲$\mathfrak{H}$之元素也.於是, A 若不屬於$\mathfrak{H}$,則(2)中與$\mathfrak{H}$之元素相等者不得存在.故云云.

定理. 若元素 B 屬於$\mathfrak{H}A$,則$\mathfrak{H}B$與$\mathfrak{H}A$一致;否則$\mathfrak{H}B$與$\mathfrak{H}A$無共通之元素.

證明. 若 B 屬於$\mathfrak{H}A$,則

$$B=HA \quad (H \text{ 爲 } \mathfrak{H} \text{ 之一元素}).$$

故由組合法則,$\mathfrak{H}B$得表示如次:

(3)　　$(H_0H)A,\ (H_1H)A,\ \cdots\cdots,\ (H_{h-1}H)A.$

但 H 爲 $\mathfrak{H}$ 之元素,故由前定理,可知

$$H_0H,\quad H_1H,\ \cdots\cdots,\ H_{h-1}H$$

不過爲(1)中元素之順序更換者而已.因之(3)卽 $\mathfrak{H}B$ 乃與(2)卽 $\mathfrak{H}A$ 一致.

復次,$\mathfrak{H}B$ 與 $\mathfrak{H}A$ 若有共通之元素如

$$H_iB=H_jA,$$

則於此兩邊以 H_i^{-1} 左乘之,得

$$B=H_i^{-1}H_jA.$$

但 $H_i^{-1}H_j$ 屬於 $\mathfrak{H}$.故 B 不得不爲 $\mathfrak{H}A$ 之元素也.如是,若 B 不屬於 $\mathfrak{H}A$ 時,則 $\mathfrak{H}B$ 與 $\mathfrak{H}A$ 無共通元素.

定義. 羣 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$ 與不屬於 $\mathfrak{H}$ 但係 $\mathfrak{G}$ 之元素 A 之積 $\mathfrak{H}A$,名曰屬於 $\mathfrak{H}$ 之傍系.

注意. 在記述之便宜上,不問 A 之屬於 $\mathfrak{H}$ 與否,然積 $\mathfrak{H}A$ 輒名曰 $\mathfrak{H}$ 之傍系者亦有之.

24. 定理. 有限羣 $\mathfrak{G}$ 之約羣之元數,乃 $\mathfrak{G}$ 之元數之約數.

證明. 試以 $\mathfrak{H}$(元數 h)爲 $\mathfrak{G}$(元數 g)之約羣.若除屬於 $\mathfrak{H}$ 之元素之外,$\mathfrak{G}$ 之元素便不存在時,則有 $g=h$,是本定理爲自明也.

若 $\mathfrak{G}$ 中尙有不屬於 $\mathfrak{H}$ 之元素時,乃取其一如 P_1.以之右乘於 $\mathfrak{H}$ 而作傍系 $\mathfrak{H}P_1$,則 $\mathfrak{H}P_1$,由前節之定理,爲由 h 個互異

之元素而成,且與$\mathfrak{H}$無共通之元素.故若以$\mathfrak{H}$及$\mathfrak{H}P_1$而能盡$\mathfrak{G}$之元素全數時,則$\mathfrak{G}$之元數,爲$g=2h$也.

反之,$\mathfrak{G}$之元素,除$\mathfrak{H}$及$\mathfrak{H}P_1$外,尙有存在時,取其一如P_2.由是作傍系$\mathfrak{H}P_2$,則此不但由h個互異之元素而成,且與$\mathfrak{H}$以及$\mathfrak{H}P_1$皆無共通之元素也.故若$\mathfrak{G}$之元素能以$\mathfrak{H}$,$\mathfrak{H}P_1$及$\mathfrak{H}P_2$而盡時,$g=3h$.反之,以此三傍系尙不能盡$\mathfrak{G}$之元素,則更以同一之手段反覆施之可.然$\mathfrak{G}$之元數爲有限,故有限回之後,$\mathfrak{G}$之元素,非得以有限個之傍系

$$\begin{aligned}
\mathfrak{H}&: \quad H_0,\ H_1,\ H_2,\ \cdots\cdots,\ H_{h-1}\\
\mathfrak{H}P_1&: \quad H_0P_1,\ H_1P_1,\ \cdots\cdots,\ H_{h-1}P_1\\
\mathfrak{H}P_2&: \quad H_0P_2,\ H_1P_2,\ \cdots\cdots,\ H_{h-1}P_2\\
&\cdots\cdots \quad \cdots\cdots\cdots\cdots\cdots\cdots\\
\mathfrak{H}P_{\nu-1}&: \quad H_0P_{\nu-1},\ H_1P_{\nu-1},\ \cdots\cdots,\ H_{h-1}P_{\nu-1}
\end{aligned}$$

盡之不可.因之

$$g=\nu h.$$

如是,$\mathfrak{H}$之元數乃$\mathfrak{G}$之元數之約數也.

系. n次之置換羣之元數爲$n!$之約數.

蓋因n次之置換羣,皆n次之對稱羣之約羣故也.(參照第11節注意.)

定義. 若g爲羣$\mathfrak{G}$之元數,h爲其約羣$\mathfrak{H}$之元數,則g/h爲整數.此數g/h名曰$\mathfrak{G}$之約羣$\mathfrak{H}$之指數.

表示羣$\mathfrak{G}$之由ν個傍系

$$\mathfrak{H},\ \mathfrak{H}P_1,\ \mathfrak{H}P_2,\ \cdots\cdots,\ \mathfrak{H}P_{\nu-1}$$

而成,乃記之如

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1+\mathfrak{H}P_2+\cdots\cdots+\mathfrak{H}P_{\nu-1}.$$

以$\mathfrak{G}$表於此形,爰名曰就$\mathfrak{H}$分$\mathfrak{G}$爲傍系云.但此處記號+,非加$\mathfrak{G}$之元素之意,不過示$\mathfrak{G}$由上之ν個傍系所成立而已.

例. 若$\mathfrak{S}$爲四次之對稱羣(第11節例2),$\mathfrak{A}$爲四次之交代羣(第12節例2)則

$$\mathfrak{A}:\begin{cases}1 & (bcd) & (cad) & (dab) & (acb)\\ & (bdc) & (cda) & (dba) & (abc)\\ (ab)(cd) & & (ac)(bd) & & (ad)(bc),\end{cases}$$

$$\mathfrak{A}(ab):\begin{cases}(ab) & (abcd) & (adcb) & (bd) & (ac)\\ & (abdc) & (acdb) & (ad) & (bc)\\ (cd) & & (acbd) & & (adbc).\end{cases}$$

而

$$\mathfrak{S}=\mathfrak{A}+\mathfrak{A}(ab).$$

又四置換

$$1\qquad (ab)(cd),\qquad (ac)(bd),\qquad (ad)(bc)$$

爲$\mathfrak{A}$之約羣.以之名$\mathfrak{B}$,則$\mathfrak{A}$就$\mathfrak{B}$而分爲傍系,則

$$\mathfrak{A}=\mathfrak{B}+\mathfrak{B}(bcd)+\mathfrak{B}(bdc).$$

注意 1. 此後專討論有限羣,故若單言羣,則係指有限羣者也,請留意焉.

注意 2. 本來構成羣之元素,不限其僅爲互異的;但論

元素之數時,則相等者只算作一個,而以互異者之數爲其數也.又當取羣之部分時,亦以與此部分之一元素相等者悉屬於此部分也.如傍系 $\mathfrak{H}P_1$, 則凡與其一元素 HP_1 相等者概包含在內是.因之便宜上,以羣爲由互異之元素而成,從而討論之,亦無不可.卽就本節定理之證明言,亦準此而述之者也.

25. 元素之巡回率,巡回羣.

如第19節定理之證明中所述,在有限羣 $\mathfrak{G}$ 中,對其一元素 A 而滿足

$$A^s=1$$

之正整數 s 必定存在也.如斯之正整數 s 之中,其最小者,名曰元素 A 之**巡回率**.如彼四次之交代羣(第12節例 2),因

$$(abc),\qquad (abc)^2=(acb),\qquad (abc)^3=1,$$

故 (abc) 之巡回率爲 3 也

今若 a 爲元素 A 之巡回率,則 a 個之元素

$$1,\ A,\ A^2,\ \cdots\cdots,\ A^{a-1}$$

彼此互異,且形成一羣,明已.此羣也,稱曰 $\mathfrak{G}$ 之巡回約羣,而以 $\{A\}$ 表之焉.

若 $a=g$, 則 $\mathfrak{G}=\{A\}$. 一般,僅以同一元素之冪而成之羣,名曰**巡回羣**. $a=g$ 時,則 $\mathfrak{G}$ 爲巡回羣也.

定理. 若元素 A 之巡回率爲 a, 則 a 爲 $\mathfrak{G}$ 之元數 g 之約數.

蓋因 a 爲 $\mathfrak{G}$ 之約羣 $\{A\}$ 之元數故也.

次之,若 $\mathfrak{H}$ 爲羣 $\mathfrak{G}$ 之約羣,而 A 爲 $\mathfrak{G}$ 之元素,則 A 之乘冪

列　　$$A,\ A^2,\ A^3,\ \cdots\cdots$$

中,屬於 $\mathfrak{H}$ 者必定存在.蓋若 A 之巡回率爲 a,則 $A^a=1$,而 A^a 確含於 $\mathfrak{H}$ 故也.在此諸冪中,其屬於 $\mathfrak{H}$ 者內之最低冪爲 A^b 時,換言之,卽 A 須 b 乘然後始與 $\mathfrak{H}$ 之一元素等時,則此指數 b 名曰關於 $\mathfrak{H}$ 之 A 之**相對巡回率**.

今 A 之巡回率 a,以 b 除之,得

$$a=qb+r \qquad (0\leqq r<b)$$

則　　$$A^r=A^{a-qb}=A^aA^{-qb}=(A^b)^{-q}.$$

而 A^b 乃 $\mathfrak{H}$ 之元素,故 A^r 亦非屬於 $\mathfrak{H}$ 不可也.由是,若 $r\neq 0$,則違反 b 爲關於 $\mathfrak{H}$ 之 A 之相對巡回率之假定,以故 r 不得不爲零也.爰得次之

定理. 相對巡回率,乃巡回率之約數.

25. 部分及其結合.

一集合,若由屬於羣 $\mathfrak{G}$ 之若干元素而成,則名曰 $\mathfrak{G}$ 之**部分**.* 今以 $\mathfrak{A}$ 及 $\mathfrak{B}$ 爲 $\mathfrak{G}$ 之二部分,而其元素分別爲

$$\mathfrak{A}:\ A_0,\ A_1,\ \cdots\cdots,\ A_{a-1},$$

$$\mathfrak{B}:\ B_0,\ B_1,\ \cdots\cdots,\ B_{b-1},$$

由此兩部分之元素作次之積:

---

* 於兩個部分 $\mathfrak{A},\mathfrak{B}$ 中,若與 $\mathfrak{A}$ 之元素相等者含於 $\mathfrak{B}$ 內,而與 $\mathfrak{B}$ 之元素相等者亦存在于 $\mathfrak{A}$ 中時,則此兩部分名曰相等,而以 $\mathfrak{A}=\mathfrak{B}$ 表之.(參照第 24 節注意 2)

$$A_iB_j \quad \begin{cases} i=0,\ 1,\ 2,\ \cdots\cdots,\ a-1 \\ j=0,\ 1,\ 2,\ \cdots\cdots,\ b-1. \end{cases}$$

如是所得之ab個之積,其中相等者容或有之,雖不得而知,然終係$\mathfrak{G}$之元素也.故此等積相集,亦形成一個部分,乃以$\mathfrak{AB}$表之,而名之曰$\mathfrak{A}$與$\mathfrak{B}$之積焉.於是由二部分以作其積$\mathfrak{AB}$,名之曰$\mathfrak{A}$與$\mathfrak{B}$之結合,或曰$\mathfrak{A}$與$\mathfrak{B}$相乘云.

原來羣之三元素之結合間,組合法則本適用已,故對於三部分$\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$之結合,組合法則

$$(\mathfrak{AB})\mathfrak{C}=\mathfrak{A}(\mathfrak{BC})$$

亦告成立.但交換法則,則未必成立也.故若對於$\mathfrak{A}$, $\mathfrak{B}$之結合,交換法則

$$\mathfrak{AB}=\mathfrak{BA}$$

得成立時,則此兩部分名曰**交換可能**云.

特別,苟部分$\mathfrak{B}$爲由一個元素而成時,則有

$$\mathfrak{A}B: \quad A_0B,\ A_1B,\ \cdots\cdots,\ A_{a-1}B,$$

$$B\mathfrak{A}: \quad BA_0,\ BA_1,\ \cdots\cdots,\ BA_{a-1};$$

而$\mathfrak{A}B$中互異元素之數乃與$\mathfrak{A}$中互異元素之數等.又關於$B\mathfrak{A}$亦然.蓋$\mathfrak{A}$中,若$A_i=A_j$,則於此兩邊以B右乘(或左乘),得$A_iB=A_jB$(或$BA_i=BA_j$);反之於$\mathfrak{A}B$(或$B\mathfrak{A}$)中,若$A_iB=A_jB$(或$BA_i=BA_j$),則兩邊以B^{-1}右乘(或左乘),得$A_i=A_j$故也.

又兩積$\mathfrak{A}B$, $B\mathfrak{A}$相等時,則名曰$\mathfrak{A}$與元素B交換可能.若$\mathfrak{A}$與B爲交換可能,則

$$B^{-1}\mathfrak{A}B=\mathfrak{A}$$

明矣;反之若 $B^{-1}\mathfrak{A}B=\mathfrak{A}$, 則 $\mathfrak{A}B=B\mathfrak{A}$. 又 $\mathfrak{A}$ 若與 B 交換可能,則對於 $\mathfrak{A}$ 之任意一元素 A_i 而能滿足

$$A_iB=BA' \quad (\text{或}BA_i=A''B)$$

之元素 A′ (或 A″),定存在於 $\mathfrak{A}$ 也.即 $B^{-1}A_iB$ 及 BA_iB^{-1} 皆屬於 $\mathfrak{A}$ 焉.

27. 定理. 令 $\mathfrak{H}$ 爲羣 $\mathfrak{G}$ 之部分.若 $\mathfrak{H}$ 爲約羣,則 $\mathfrak{H}^2=\mathfrak{H}$;反之,若 $\mathfrak{H}^2=\mathfrak{H}$, 則 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之約羣.

證明. 以 $\mathfrak{H}$ 之元素爲

$$(1) \qquad H_0,\ H_1,\ H_2,\ \cdots\cdots,\ H_{h-1}$$

於是 $\mathfrak{H}^2$ 之元素,得以積

$$(2) \qquad H_iH_j \quad (i,j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1)$$

與之.

$\mathfrak{H}$ 若爲約羣,則 $\mathfrak{H}$ 不得不含主元素.以之爲 H_0, 則

$$H_iH_0=H_i \qquad (i=0,1,2,\cdots\cdots,h-1)$$

因之(2)中,(1) 之元素悉包含在內也.然 $\mathfrak{H}$ 爲羣,故(2)之元素 H_iH_j 屬於 $\mathfrak{H}$,故 $\mathfrak{H}^2=\mathfrak{H}$.

反之,若 $\mathfrak{H}^2=\mathfrak{H}$, 則 $\mathfrak{H}$ 之二元素之積 H_iH_j 屬於 $\mathfrak{H}$. 因之 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之約羣(第22節定理).

定理. 若 $\mathfrak{H}$ 及 $\mathfrak{K}$ 爲一羣之約羣,則於兩者之積 $\mathfrak{H}\mathfrak{K}$, 其互異元素之數,乃與以兩者之最大公約羣之元數除此兩約羣元數之積之商等.

證明. 爲容易理解起見,以 $\mathfrak{H}$ 爲由互異之 h 個元素而成 $\mathfrak{R}$ 爲由 k 個互異之元素而成者,而兩羣之最大公約羣 $\mathfrak{L}$ 之元數爲 l,其元素爲

$$(1) \qquad L_0,\ L_1,\ \cdots\cdots,\ L_{l-1}.$$

先將 $\mathfrak{R}$ 就 $\mathfrak{L}$ 分爲傍系:

$$\mathfrak{R}=\mathfrak{L}S_0+\mathfrak{L}S_1+\cdots\cdots+\mathfrak{L}S_{\sigma-1} \qquad (S_0=1).$$

如是,$\mathfrak{H}\mathfrak{R}$ 爲由下記之 σl 個之積而成,明已. 卽:

$$\mathfrak{H}1\ {}_0S_0,\ \mathfrak{H}L_1S_0,\ \cdots\cdots,\ \mathfrak{H}L_{l-1}S_0$$

$$\mathfrak{H}L_0S_1,\ \mathfrak{H}L_1S_1,\ \cdots\cdots,\ \mathfrak{H}L_{l-1}S_1$$

$$\cdots\cdots\cdots\cdots \qquad \cdots\cdots\cdots\cdots$$

$$\mathfrak{H}L_0S_{\sigma-1},\ \mathfrak{H}L_1S_{\sigma-1},\cdots\ \mathfrak{H}L_{l-1}S_{\sigma-1}.$$

然 L_i 爲 $\mathfrak{L}$ 之元素,隨之亦卽爲 $\mathfrak{H}$ 之元素.故由第23節定理,

$$\mathfrak{H}L_i=\mathfrak{H}, \qquad \mathfrak{H}L_iS_j=\mathfrak{H}S_j$$

故 $\mathfrak{H}\mathfrak{R}$ 中互異之元素,悉含於 σ 個傍系

$$(2) \qquad \mathfrak{H}S_0,\ \mathfrak{H}S_1,\cdots\ ,\mathfrak{H}S_{\sigma-1}$$

中也.

但 $\mathfrak{H}$ 乃由 h 個互異之元素而成.故由前節所述,$\mathfrak{H}S_j$ 亦含有 h 個互異之元素也.且屬於(2)之傍系無有共通之元素. 蓋若假定 $\mathfrak{H}S_t$ 與 $\mathfrak{H}S_u$ 含有共通之元素,則

$$S_t=HS_u \quad (H \text{ 爲 } \mathfrak{H} \text{ 之一元素}),$$

因之

$$S_tS_u^{-1}=H.$$

是卽 $S_tS_u^{-1}$ 屬於 $\mathfrak{H}$ 也. 但 S_t, S_u^{-1} 乃 $\mathfrak{R}$ 之元素,因之積 $S_tS_u^{-1}$ 亦屬

於 $\mathfrak{R}$. 故 $S_tS_u^{-1}$ 乃爲 $\mathfrak{H}$ 及 $\mathfrak{R}$ 所公共.故

$$S_tS_u^{-1}=L \quad (L\text{爲}\mathfrak{L}\text{之元素})$$

$$\therefore \quad S_t=LS_u.$$

是卽示 S_t 屬於傍系 $\mathfrak{L}S_u$. 但若 $S_t\neq S_u$, 則此爲不可能.故 $S_t\neq S_u$ 時,則 $\mathfrak{H}S_t$ 與 $\mathfrak{H}S_u$ 不得有公共之元素.

如是,(2)之傍系,皆由互異之 h 元素而成,且二者無有共通之元素者也.故含於(2)之元素之總數爲 $h\sigma$. 是卽 $\mathfrak{H}\mathfrak{R}$ 中互異元素之數也.故

$$h\sigma=\frac{hk}{l}.$$

故定理爲眞

定理. 設 $\mathfrak{H}$ 及 $\mathfrak{R}$ 爲羣 $\mathfrak{G}$ 之約羣.若兩者之積 $\mathfrak{H}\mathfrak{R}$ 爲羣時,則 $\mathfrak{H}$ 與 $\mathfrak{R}$ 爲交換可能;反之若兩者爲交換可能,則其積 $\mathfrak{H}\mathfrak{R}$ 爲羣.

證明. 以 H 爲 $\mathfrak{H}$ 之任意之元素, K 爲 $\mathfrak{R}$ 之任意之元素. 若 $\mathfrak{H}$ 之主元素表以 H_0, $\mathfrak{R}$ 之主元素表以 K_0 時,則 H_0 及 K_0,共爲 $\mathfrak{G}$ 之主元素,故

$$KH=H_0K\cdot HK_0.$$

若 $\mathfrak{H}\mathfrak{R}$ 爲羣,則

$$H_0K\cdot HK_0=H'K',$$

但 H', K' 分別爲 $\mathfrak{H}$ 及 $\mathfrak{R}$ 之元素.故

$$KH=H'K'.$$

由是,與 $\mathfrak{R}\mathfrak{H}$ 之元素相等者,皆存在於 $\mathfrak{H}\mathfrak{R}$ 也.然由前定理, $\mathfrak{H}\mathfrak{R}$ 及

$\mathfrak{H}\mathfrak{K}$ 中互異元素之數爲同一的.故得

$$\mathfrak{H}\mathfrak{K}=\mathfrak{K}\mathfrak{H}.$$

反之,若 $\mathfrak{H}\mathfrak{K}=\mathfrak{K}\mathfrak{H}$, 則

$$(\mathfrak{H}\mathfrak{K})^2=\mathfrak{H}\cdot\mathfrak{K}\mathfrak{H}\cdot\mathfrak{K}=\mathfrak{H}\cdot\mathfrak{H}\mathfrak{K}\cdot\mathfrak{K}=\mathfrak{H}^2\cdot\mathfrak{K}^2.$$

然 $\mathfrak{H}$ 與 $\mathfrak{K}$ 共爲 $\mathfrak{G}$ 之約羣.故由本節第一定理,

$$\mathfrak{H}^2=\mathfrak{H},\qquad \mathfrak{K}^2=\mathfrak{K}.$$

故

$$(\mathfrak{H}\mathfrak{K})^2=\mathfrak{H}\mathfrak{K}.$$

故由本節第一定理,知 $\mathfrak{G}$ 之部分 $\mathfrak{H}\mathfrak{K}$ 者,羣也.故云云.

系. 設 $\mathfrak{H}$ 及 $\mathfrak{K}$ 爲一羣之約羣.若 $\mathfrak{H}$ 之各元素與 $\mathfrak{K}$ 爲交換可能時,則兩約羣之積 $\mathfrak{H}\mathfrak{K}$ 形成一羣,而其元數則與 $\frac{hk}{l}$ 等. 但 h 爲 $\mathfrak{H}$ 之元數, k 爲 $\mathfrak{K}$ 之元數,而 l 則爲 $\mathfrak{H}$ 及 $\mathfrak{K}$ 之最大公約羣之元數.

證明. 若 $\mathfrak{H}$ 之各元素與 $\mathfrak{K}$ 爲交換可能,則 $\mathfrak{H}$ 與 $\mathfrak{K}$ 之交換可能,明已.故 $\mathfrak{H}\mathfrak{K}$ 者,羣也.而其元數,則由本節第二定理爲 $\frac{hk}{l}$.

定理. 於一羣之二約羣 $\mathfrak{H}$ 及 $\mathfrak{K}$, 若 $\mathfrak{H}$ 與 $\mathfrak{K}$ 之各元素爲交換可能,而 $\mathfrak{K}$ 與 $\mathfrak{H}$ 之各元素亦交換可能,且兩約羣除主元素外,無共通之元素時,則 $\mathfrak{H}$ 之各元素,與 $\mathfrak{K}$ 之各元素爲交換可能.

證明. 茲以 H 爲 $\mathfrak{H}$ 之任意之元素, K 爲 $\mathfrak{K}$ 之任意之元素,而討論積 $H^{-1}K^{-1}HK$, 則因 K 與 $\mathfrak{H}$ 爲交換可能,故由前節所述, $K^{-1}HK$ 屬於 $\mathfrak{H}$, 隨之 $H^{-1}K^{-1}HK$ 亦非屬於 $\mathfrak{H}$ 不可也.又

自他面觀之，H 與 $\mathfrak{R}$ 爲交換可能，故 $H^{-1}K^{-1}H$ 屬於 $\mathfrak{R}$，因之 $H^{-1}K^{-1}H\cdot K$ 亦屬於 K，由是，$H^{-1}K^{-1}HK$ 乃爲 $\mathfrak{H}$ 及 $\mathfrak{R}$ 之所公共.但兩約羣之共通元素僅主元素.故

$$H^{-1}K^{-1}HK=1.$$

此兩邊以 KH 左乘之，得

$$HK=KH.$$

即 $\mathfrak{H}$ 之各元素與 $\mathfrak{R}$ 之各元素爲交換可能也.故云云.

於兩約羣 $\mathfrak{H}$ 及 $\mathfrak{R}$，其一之各元素與其他之各元素爲交換可能，且除主元素以外無有共通之元素時，則積 $\mathfrak{H}\mathfrak{R}$ 名曰 $\mathfrak{H}$ 及 $\mathfrak{R}$ 之直乘積.直乘積之元數，由第二定理，乃與兩約羣之元數之積等.

第四章　共　軛

28. 共軛元素.

令 A，G 爲羣 $\mathfrak{G}$ 之二元素.由 A 以作 $G^{-1}AG$，則此名曰 A 以 G 變形.如於第 12 節之四次交代羣，若以 $(ab)(cd)$ 將 (bcd) 變形，則

$$[(ab)(cd)]^{-1}(bcd)[(ab)(cd)]=(adc).$$

若元素 B 爲由他元素 A 變形而成者時，換言之，即適合於

$$B=G^{-1}AG$$

之元素 G 存在於 $\mathfrak{G}$ 時，則 B 名曰與 A 共軛.如於上所示之四

次交代羣,(adc)者,乃共軛於(bcd)者也.

元素B若共軛於A,則A亦共軛於B也.蓋因

$$G^{-1}AG=B,$$

故

$$G\cdot G^{-1}AG\cdot G^{-1}=GBG^{-1}$$

即

$$A=(G^{-1})^{-1}B(G^{-1}),$$

而G^{-1}又屬於$\mathfrak{G}$故也.

又元素B若共軛於A,C共軛於B,則C共軛於A.蓋若

$$B=G^{-1}AG,\qquad C=H^{-1}BH,$$

則

$$C=H^{-1}\cdot G^{-1}AG\cdot H=(GH)^{-1}A(GH)$$

故也.

特別,若羣$\mathfrak{G}$之元素S,雖以$\mathfrak{G}$之任何元素而使之變形,其結果仍等於S自身時,則S名曰$\mathfrak{G}$之**自己共軛元素**,或曰**孤立元素**.

如就置換羣

$$1,\qquad (abcd),\qquad (ac)(bd),\qquad (adcb)$$
$$(ab)(cd),\qquad (bd),\qquad (ad)(bc),\qquad (ac)$$

之置換$(ac)(bd)$而觀,則

$$(abcd)^{-1}(ac)(bd)(abcd)=(bd)(ca)=(ac)(bd),$$
$$[(ab)(cd)]^{-1}(ac)(bd)[(ab(cd)]=(bd)(ca)=(ac)(bd),$$
$$(bd)^{-1}(ac)(bd)(bd)=(ac)(bd).$$

此外雖以他之置換而使變形,而結果仍同爲(ac) (bd)也.故$(ac)(bd)$於上羣中爲自己共軛

又自己共軛元素與羣之各元素爲交換可能.蓋若S爲羣$\mathfrak{G}$之自己共軛元素,則對於$\mathfrak{G}$之元素G, $G^{-1}SG=S$,因之$SG=GS$故也.反之,與羣之各元素爲交換可能之元素,乃係自己共軛.

又主元素,雖以屬於羣之任何元素而使之變形,仍不能得1以外之物也.故主元素常自己共軛焉.

定理. 共軛元素,乃有同一之巡回率.

證明. $(G^{-1}AG)^2=G^{-1}AG\cdot G^{-1}AG=G^{-1}A^2G,$

$(G^{-1}AG)^3=(G^{-1}AG)^2(G^{-1}AG)=G^{-1}A^2G\cdot G^{-1}AG=G^{-}A^3G,$

.....

$(G^{-1}AG)^a=(G^{-1}AG)^{a-1}(G^{-1}AG)=G^{-1}A^{a-1}G\cdot G^{-1}AG=G^{-1}A^aG.$

故若$A^a=1$,則

$$(G^{-1}AG)^a=G^{-1}A^aG=G^{-1}\cdot 1\cdot G=G^{-1}G=1$$

反之,若 $$(G^{-1}AG)^a=1,$$

則 $$G^{-}A^aG=1,$$

$$\therefore\quad G\cdot G^{-1}A^aG\cdot G^{-1}=G\cdot 1\cdot G^{-1}.$$

$$\therefore\quad A^a=1.$$

因之A及$G^{-1}AG$之巡回率相等也.

系 二元素之積AB及BA爲共軛,因之其巡回率同一.

蓋因 $AB=B^{-1}(BA)B$故.

注意. 若$B^{-1}AB=A$,則$AB=BA$,而其逆亦眞.

29. 定理. 與羣$\mathfrak{G}$之元素A爲交換可能之元素($\mathfrak{G}$的)相集,乃形成一羣.若以此羣爲$\mathfrak{H}$,則$\mathfrak{H}$於$\mathfrak{G}$之指數,乃等於與

A 共軛元素之數(A 亦含在內).

證明. 若二元素 K_1, K_2 與 A 爲交換可能,即

$$AK_1=K_1A, \qquad AK_2=K_2A$$

則
$$A(K_1K_2)=(AK_1)K_2=(K_1A)K_2$$
$$=K_1(AK_2)=K_1(K_2A)=(K_1K_2)A.$$

如是,則與 A 交換可能之元素之積,又與 A 交換可能也.

因之,此類元素之總體(屬於 $\mathfrak{G}$)作一羣焉.試以此羣爲 $\mathfrak{K}$.

茲以 $\mathfrak{K}$ 之元數爲 k, 而其元素爲

$$(1) \qquad K_0, K_1, K_2, \cdots, K_{k-1}.$$

再就 $\mathfrak{K}$ 而將 $\mathfrak{G}$ 分爲傍系:

$$\mathfrak{G}=\mathfrak{K}P_0+\mathfrak{K}P_1+\mathfrak{K}P_2+\cdots\cdots+\mathfrak{K}P_{\nu-1} \qquad (P_0=1)$$

乃以傍系 $\mathfrak{K}P_i$ 之任意元素 K_sP_i (K_s 爲 $\mathfrak{K}$ 之元素)將 A 變形,則有

$$(K_sP_i)^{-1}A(K_sP_i)=(P_i^{-1}K_s^{-1})A(K_sP_i) \quad [\because (K_sP_i)^{-1}=P_i^{-1}K_s^{-1}]$$
$$=P_i^{-1}(K_s^{-1}AK_s)P_i=P_i^{-1}AP_i.$$

故傍系 $\mathfrak{K}P_i$ 之各元素,乃將 A 變形爲同一元素 $P_i^{-1}AP_i$ 也.因之,以 $\mathfrak{G}$ 所有之元素而將 A 變形,其可得之結果爲

$$(2) \qquad A, P_1^{-1}AP_1, P_2^{-1}AP_2, \cdots\cdots, P_{\nu-1}^{-1}AP_{\nu-1}.$$

且此各個皆互異.蓋若假定

$$P_i^{-1}AP_i=P_j^{-1}AP_j \qquad (i\neq j)$$

則有
$$P_i\cdot P_i^{-1}AP_i\cdot P_j^{-1}=P_i\cdot P_j^{-1}AP_j\cdot P_j^{-1}.$$

或
$$A(P_iP_j^{-1})=(P_iP_j^{-1})A,$$

隨之 $P_iP_j^{-1}$ 不得不屬於 $\mathfrak{R}$ 也.茲令

$$P_i P_j^{-1}=K \qquad (K \text{ 爲 } \mathfrak{R} \text{ 之一元素}),$$

則

$$P_i=KP_j,$$

此卽謂 P_i 得屬於傍系 $\mathfrak{R}P_j$ 也,是不合理.由是知(2)之中,相等之元素不得存在也.

故與 A 共軛且互異之元素,以(2)之 ν 個足以盡其全數但 ν 乃 $\mathfrak{R}$ 於 $\mathfrak{G}$ 之指數.故與 A 共軛元素之數乃與 $\mathfrak{R}$ 之對於 $\mathfrak{G}$ 之指數等也.

30. 共軛元素系.

在一羣中,其所有與同一元素共軛之元素之集合,名曰**共軛元素系.**

茲取羣 $\mathfrak{G}$ 之元素 A,而以 $\mathfrak{G}$ 之各元素將其變形.如斯所得之元素,若命爲

$$(1) \qquad A, A_1, A_2, \cdots\cdots,$$

則此等元素,由上之定義,乃作成一共軛元素系也.如以屬於此系之元素(互異的)之數爲 m,則 m 由前定理乃 $\mathfrak{G}$ 之元數 g 之約數.

且系(1)之一元素 A_i,原與 A 共軛,故共軛於 A_i 之元素,亦與 A 共軛,因之非屬於(1)不可.又系(1)之元素,皆共軛於 A,故亦共軛於 A_i.以故任取(1)中任何元素以作共軛元素系,其所得全與(1)同一也.

次之,以 B 爲不屬於共軛系(1)之 $\mathfrak{G}$ 之元素,則與 B 共軛

之元素,其不屬於(1),明已.因之,$\mathfrak{G}$之元素,以之分爲若干共軛元素系,而使各元素屬於一而且唯一系,爲可能.換言之,卽將$\mathfrak{G}$之元素分爲若干組,令互爲共軛之元素屬於同一組,不共軛之二元素屬於異組;且各元素,無論何組,皆有所隸屬,爲可能也.此則名曰以$\mathfrak{G}$之元素**分爲共軛系焉**.

今以$\mathfrak{G}$中互異之共軛元素系爲

$$(2) \qquad \mathfrak{C}_0, \mathfrak{C}_1, \cdots\cdots, \mathfrak{C}_{r-1}$$

而以屬於各個之元素(互異的)之數,分別爲

$$(3) \qquad m_0, m_1, \cdots\cdots, m_{r-1},$$

則因以此諸系,可盡$\mathfrak{G}$之所有之元素,故得

$$g=m_0+m_1+\cdots\cdots+m_{r-1}$$

式中g,爲表$\mathfrak{G}$之元數者.

尙須注意者,此式中$m_0, m_1, \cdots\cdots, m_{r-1}$,皆係$g$之約數是也.

例. 將四次交代羣(第12節例2,或第24節$\mathfrak{A}$)之置換分爲共軛元素系,則如次之四者:

$$1,$$

$$(bcd), \quad (acb), \quad (cad), \quad (dab)$$

$$(bdc), \quad (dba), \quad (abc), \quad (cda)$$

$$(ab)(cd), \quad (ac)(bd), \quad (ad)(bc)$$

而

$$12=1+4+4+3.$$

31. 自已共軛元素,雖以羣中任何元素變其形,仍不能

產生與之相異之元素,故自己共軛元素,單獨形成共軛元素系.反之,單獨形成共軛系之元素,卽自己共軛焉.

又主元素乃自己共軛者也.故於前節(3),卽

$$m_0,\ m_1,\ \cdots\cdots,\ m_{r-1}$$

中,等於1者必存在.今以之爲m_0,則得

$$g=1+m_1+m_2+\cdots\cdots+m_{r-1}.$$

若主元素以外,尙有自己共軛元素時則於$m_1,\ m_2,\ \cdots\cdots,\ m_{r-1}$之中,仍得有等於1者在也.

定理. 元數爲素數冪之羣,除主元素外,必含有自己共軛元素.

證明. 以p爲素數,而以$g=p^m$.於是如前節所述因$m_1,\ m_2,\ \cdots\cdots\ m_{r-1}$之任何個皆爲$g$之約數,故是等非通爲$p$之冪不可也.茲以之分別爲$p^{\alpha_1},\ p^{\alpha_2},\ \cdots\cdots,\ p^{\alpha_{r-1}}$,則得

$$p^m=1+p^{\alpha_1}+p^{\alpha_2}+\cdots\cdots+p^{\alpha_{r-1}}.$$

此式左邊,乃素數p之冪也.故右邊必得以p整除.爲此之故,指數$\alpha_1,\ \alpha_2,\ \cdots\cdots,\ \alpha_{r-1}$中,定需有等於零者在,因之$p^{\alpha_1},\ p^{\alpha_2},\ \cdots\cdots,\ p^{\alpha_{r-1}}$之中,定有等於1者也.以故此羣,除主元素外,乃含有自己共軛元素.故云云.

例. 將第28節中所示之置換羣.

$$1,\qquad (abcd),\qquad (ac)(bd),\qquad (adcb),$$
$$(ab)(cd),\qquad (bd),\qquad (ad)(bc),\qquad (ac)$$

分爲共軛元素系,則得次之五組,$(ac)(bd)$爲自己共軛:

1;

$(ac)(bd)$;

$(ab)(cd)$, $(ad)(bc)$;

$(abcd)$, $(adcb)$;

(bd), (ac);

而 $8=2^3=1+1+2+2+2$.

定理. 元數等於素數之自乘之羣,爲 Abel 氏羣.

證明. 以 p 爲素數,而以羣 $\mathfrak{G}$ 之元數爲 p^2. 因羣之元素之巡回率乃元數之約數,故 $\mathfrak{G}$ 中主元素以外之元素之巡回率,非爲 p^2 或 p 不可也.

巡回率 p^2 之元素存在時,以其一爲 S, 則 $\mathfrak{G}$ 之元素,得以

$$1, S, S^2, \cdots\cdots, S^{p^2-1}$$

與之,因之 $\mathfrak{G}$ 爲巡回羣也.是則當然爲 Abel 氏羣矣.

巡回率 p^2 之元素不存在時,乃取 $\mathfrak{G}$ 中自己共軛元素(主元素以外者)之一(本節定理),而以之爲 P, 則其巡回率又爲 p 也.次以 Q 爲不屬於巡回約羣{P}之 $\mathfrak{G}$ 之元素之一,則其巡回率亦不得不爲 p. 今就約羣{P}, {Q}而觀之,兩者之元數,共爲 p 也,且 Q 不屬於{P}.故兩者之共通元素,僅主元素.因之,其積{P}{Q}含有 p^2 個互異之元素也(第27節定理).然 $\mathfrak{G}$ 之元數爲 p^2. 故

$$\mathfrak{G}=\{P\}\{Q\}.$$

更就{P}{Q}之二元素 P^iQ^j 及 P^kQ^l 之積而觀,因 P 乃自己共軛

元素,故

$$P^iQ^j\cdot P^sQ^t=P^iP^sQ^jQ^t=P^sP^iQ^tQ^j=P^sQ^t\cdot P^iQ^j.$$

因之$\{P\}\{Q\}$卽$\mathfrak{G}$爲 Abel 氏羣也.

32. 共軛約羣.

茲以$\mathfrak{H}$爲羣$\mathfrak{G}$之約羣(元數 h),而以

(1)　　$H_0, H_1, \cdots\cdots, H_{h-1}$

爲其元素.以$\mathfrak{G}$之元素 G 將$\mathfrak{H}$之各元素變形,乃有

(2)　　$G^{-1}H_0G, G^{-1}H_1G, \cdots\cdots, G^{-1}H_{h-1}G.$

而此各個皆互異.蓋若

$$G^{-1}H_iG=G^{-1}H_jG,$$

則於其兩邊以 G 左乘之,以G^{-1}右乘之,便得$H_i=H_j$故也.

且(2)之元素又成羣.因其二元素之積爲

$$G^{-1}H_iG\cdot G^{-1}H_jG=G^{-1}(H_iH_j)G,$$

而H_iH_j屬於約羣$\mathfrak{H}$故也.

如是考之由$\mathfrak{G}$之約羣$\mathfrak{H}$,而以$\mathfrak{G}$之元素 G 作羣(2),名曰以 G 將$\mathfrak{H}$變形云.如將四次交代羣(第24節$\mathfrak{A}$)之約羣

$$1, \quad (bcd), \quad (bdc),$$

以$\mathfrak{A}$之置換$(ab)(cd)$而變形,則成爲

$$1, \quad (cad), \quad (cda).$$

以元素 G 而將約羣$\mathfrak{H}$變形所得之羣,用第26節之記法,乃以$G^{-1}\mathfrak{H}G$表之焉.

於羣$\mathfrak{G}$之二約羣$\mathfrak{H}$及$\mathfrak{H}'$,若$\mathfrak{H}'$爲將$\mathfrak{H}$變形所得者時,

即謂適合 $$\mathfrak{H}'=G^{-1}\mathfrak{H}G$$

之元素 G, 存在於 $\mathfrak{G}$ 中時,則 $\mathfrak{H}'$ 名曰與 $\mathfrak{H}$ 共軛云.若 $\mathfrak{H}'$ 與 $\mathfrak{H}$ 共軛,則與元素之共軛者同樣,$\mathfrak{H}$ 亦共軛於 $\mathfrak{H}'$ 也.如於四次交代羣,上記之二約羣互爲共軛者是.

又約羣 $\mathfrak{H}''$ 共軛於 $\mathfrak{H}'$, 而 $\mathfrak{H}'$ 共軛於 $\mathfrak{H}$ 時,則 $\mathfrak{H}''$ 亦共軛於 $\mathfrak{H}$ 也.

定理. 共軛約羣爲同態.

證明. 試取上記之約羣 $\mathfrak{H}$ 及 $G^{-1}\mathfrak{H}G$. 因(2)之元素彼此互異,故兩羣之元數同一.於是對於 $\mathfrak{H}$ 之元素

$$H_0,\ H_1,\ \cdots\cdots,\ H_{h-1},$$

分別以

$$G^{-1}H_0G,\ G^{-1}H_1G,\ \cdots\cdots,\ G^{-1}H_{h-1}G$$

對應之.是兩羣之元素之間,得成立其一一對應矣.更以 $\mathfrak{H}$ 之二元素 H_i, H_j 之積爲 H_k 則與之對應之 $G^{-1}\mathfrak{H}G$ 之元素,爲 $G^{-1}H_kG$ 也.然

$$G^{-1}H_kG=G^{-1}(H_iH_j)G=G^{-1}H_iG\cdot G^{-1}H_jG,$$

故於 H_i 及 H_j 之積,乃相應而有與是各個對應之元素 $G^{-1}H_iG$ 及 $G^{-1}H_jG$ 之積也.因之兩羣爲同態焉.

注意. 因約羣 $\mathfrak{H}$ 與其共軛羣 $G^{-1}\mathfrak{H}G$ 有同一之元數,故若 $G^{-1}\mathfrak{H}G$ 之元素皆屬於 $\mathfrak{H}$ 時,則得

$$G^{-1}\mathfrak{H}G=\mathfrak{H}.$$

且此時傍系 $\mathfrak{H}G$ 之元素與 H 爲交換可能.蓋因對於 $\mathfrak{H}$ 之任意元素 H, 乃有

$$(HG)^{-1}\mathfrak{H}(HG)=G^{-1}H^{-1}\mathfrak{H}HG=G^{-1}\mathfrak{H}G=\mathfrak{H}$$

故也.反之,若傍系 $\mathfrak{H}G$ 之一元素與 $\mathfrak{H}$ 爲交換可能,則 G 亦復如是

33. 共軛約羣系.

令 $\mathfrak{H}$ 爲羣 $\mathfrak{G}$ 之約羣.以 $\mathfrak{G}$ 之元素而使 $\mathfrak{H}$ 變形所得之所有一切約羣之集合,換言之卽與 $\mathfrak{H}$ 共軛之一切約羣之集合($\mathfrak{H}$ 自身亦包含在內),則名曰**共軛約羣系**.

定理. 若 $\mathfrak{H}$ 爲羣 $\mathfrak{G}$ 之約羣時,則 $\mathfrak{G}$ 之元素中,與 $\mathfrak{H}$ 交換可能者相集,乃形成一羣.以此羣爲 $\mathfrak{N}$,則 $\mathfrak{N}$ 於 $\mathfrak{G}$ 之指數,乃與與 $\mathfrak{H}$ 共軛之 $\mathfrak{G}$ 之約羣($\mathfrak{H}$ 亦包含在內)之數等.

此定理之證明,與論共軛元素者,雖全然同樣,然爲讀者之便宜計,仍約略述之如次:

以 K_1, K_2 爲與 $\mathfrak{H}$ 交換可能者之 $\mathfrak{G}$ 中二元素,則

$$\mathfrak{H}(K_1K_2)=(\mathfrak{H}K_1)K_2=(K_1\mathfrak{H})K_2=K_1(\mathfrak{H}K_2)=K_1(K_2\mathfrak{H})=(K_1K_2)\mathfrak{H}.$$

故與 $\mathfrak{H}$ 交換可能者之 $\mathfrak{G}$ 之元素形成羣也.以此羣爲 $\mathfrak{N}$,而就 $\mathfrak{N}$ 將 $\mathfrak{G}$ 分爲傍系

$$\mathfrak{G}=\mathfrak{N}P_0+\mathfrak{N}P_1+\mathfrak{N}P_2+\cdots\cdots+\mathfrak{N}P_{\nu-1}\quad(P_0=1).$$

以傍系 $\mathfrak{N}P_i$ 之任意之元素 K_sP_i (K_s 爲 $\mathfrak{N}$ 之元素)將 $\mathfrak{H}$ 變形,則有

$$(K_sP_i)^{-1}\mathfrak{H}(K_sP_i)=P_i^{-1}K_s^{-1}\mathfrak{H}K_sP_i$$

$$=P_i^{-1}\mathfrak{H}P_i\quad[\because \mathfrak{H}K_s=K_s\mathfrak{H}\text{ 卽 }K_s^{-1}\mathfrak{H}K_s=\mathfrak{H}]$$

故以 $\mathfrak{G}$ 之元素將 $\mathfrak{H}$ 變形所可得之約羣爲

(1) $\mathfrak{H}$, $P_1^{-1}\mathfrak{H}P_1$, $P_2^{-1}\mathfrak{H}P_2$, ……, $P_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1}$.

然此諸約羣皆互異.蓋若假定

$$P_i^{-1}\mathfrak{H}P_i = P_j^{-1}\mathfrak{H}P_j,$$

則於此兩邊以 P_i 左乘,以 P_j^{-1} 右乘,得

$$\mathfrak{H}(P_iP_j^{-1}) = (P_iP_j^{-1})\mathfrak{H}.$$

$$\therefore \quad P_iP_j^{-1} = K \qquad (K \text{ 爲 } \mathfrak{N} \text{ 之一元素}).$$

故

$$P_i = KP_j.$$

是卽示 P_i 屬於傍系 $\mathfrak{N}P_j$ 也.然使 $i \neq j$, 則此爲不可能.故(1)之約羣互異.由是,則本定理後半之爲眞可知.

本定理中之羣 $\mathfrak{N}$, 卽爲與約羣 $\mathfrak{H}$ 交換可能之元素($\mathfrak{G}$的)所作之羣,名曰 $\mathfrak{G}$ 中 $\mathfrak{H}$ 之正常化羣.求之之法,可先將 $\mathfrak{G}$ 就 $\mathfrak{H}$ 分成傍系:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}Q_1 + \cdots\cdots + \mathfrak{H}Q_{\lambda-1},$$

於 $Q_1, Q_2, \cdots\cdots, Q_{\lambda-1}$ 中,選其與 $\mathfrak{H}$ 交換可能者,而以之爲 $Q_1, Q_2, \cdots\cdots, Q_{\mu-1}$, 則

$$\mathfrak{N} = \mathfrak{H} + \mathfrak{H}Q_1 + \cdots\cdots + \mathfrak{H}Q_{\mu-1}.$$

此之理由,由前節之注意自明.

例 1 試取四次交代羣(第24節 $\mathfrak{A}$)之約羣

$$1, \qquad (bcd), \qquad (bdc),$$

而以之名曰 $\mathfrak{H}$. 就 $\mathfrak{H}$ 而將 $\mathfrak{A}$ 分成傍系,則有

$$\mathfrak{A} = \mathfrak{H} + \mathfrak{H}(ab)(cd) + \mathfrak{H}(ac)(bd) + \mathfrak{H}(ad)(bc).$$

三置換 $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$, 無論何一,皆非與 $\mathfrak{H}$ 爲交

換可能者.故 $\mathfrak{H}$ 之正常化羣爲 $\mathfrak{H}$ 自身.故與 $\mathfrak{H}$ 共軛之約羣,乃下記之4 (=12÷3)個:

$$\mathfrak{H}: \quad 1,\ (bcd),\ (bdc);$$

$$[(ab)(cd)]^{-1}\mathfrak{H}[(ab)(cd)]: \quad 1,\ (cad),\ (cda);$$

$$[(ac)(bd)]^{-1}\mathfrak{H}[(ac)(bd)]: \quad 1,\ (dab),\ (dba);$$

$$[(ad)(bc)]^{-1}\mathfrak{H}[(ad)(bc)]: \quad 1,\ (acb),\ (abc).$$

關於此例,尙有一言:正四面體 ABCD 之運動(第17節),如前所述,得視爲四文字 A, B, C, D 之置換也,夫若是,則此運動羣爲四次交代羣.而軸 OA 之周之運動所作之約羣

$$1,\ \begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix},\ \begin{pmatrix} A & B & C & D \\ A & D & B & C \end{pmatrix},$$

則相當於上記交代羣之約羣 $\mathfrak{H}$,此外對他軸之三者,則與上之三約羣相當.故於四面體,其對各軸之約羣,互爲共軛也.

例 2. 於四次對稱羣 $\mathfrak{S}$ (第24節例),試取與前例同一之約羣 $\mathfrak{H}$.於是,則得

$$\mathfrak{S}=\mathfrak{H}+\mathfrak{H}(ab)(cd)+\mathfrak{H}(ac)(bd)+\mathfrak{H}(ad)(bc)$$
$$+\mathfrak{H}(cd)+\mathfrak{H}(ab)+\mathfrak{H}(adbc)+\mathfrak{H}(acbd).$$

(參照第24節例),而 $\mathfrak{H}$ 之正常化羣爲

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}(cd),$$

卽 $\quad 1,\ (bcd),\ (bdc),\ (cd),\ (db),\ (bc)$

就 $\mathfrak{N}$ 而將 $\mathfrak{S}$ 分成傍系,則有

$$\mathfrak{S}=\mathfrak{N}+\mathfrak{N}(ab)(cd)+\mathfrak{N}(ac)(bd)+\mathfrak{N}(ad)(bc),$$

而 $\mathfrak{S}$ 之共軛約羣,則與前例同一.

次之,取 $\mathfrak{S}$ 之 8 元約羣

$$\mathfrak{T}:\begin{cases} 1, & (ab)(cd), & (ac)(bd), & (ad)(bc), \\ (cd), & (ab), & (adbc), & (acbd) \end{cases}$$

則

$$\mathfrak{S}=\mathfrak{T}+\mathfrak{T}(ac)+\mathfrak{T}(ad),$$

而 $\mathfrak{T}$ 之正常化羣爲 $\mathfrak{T}$ 之自身.故 $\mathfrak{T}$ 之共軛約羣,除 $\mathfrak{T}$ 外,乃爲下記之二:

$$(ac)^{-1}\mathfrak{T}(ac):\begin{cases} 1, & (ad)(bc), & (ac)(bd), & (ab)(cd), \\ (ad), & (bc), & (acdb), & (abdc); \end{cases}$$

$$(ad)^{-1}\mathfrak{T}(ad):\begin{cases} 1, & (ac)(bd), & (ab)(cd), & (ad)(bc), \\ (ac), & (bd), & (abcd), & (adcb). \end{cases}$$

注意. 與本節全然同樣,得證明次之定理:

設 $\mathfrak{H}$ 及 $\mathfrak{A}$ 爲羣 $\mathfrak{G}$ 之二約羣.$\mathfrak{A}$ 之元素之中,與 $\mathfrak{H}$ 交換可能者,相集成羣.若以之爲 $\mathfrak{B}$,則 $\mathfrak{B}$ 於 $\mathfrak{A}$ 之指數,與以 $\mathfrak{A}$ 之元素將 $\mathfrak{H}$ 變形所可得之羣(互異者)之數等.

34. 自己共軛約羣.

再取四次交代羣 $\mathfrak{A}$ (前節例 1),而就其約羣

$$\mathfrak{B}: \quad 1, \quad (ab)(cd), \quad (ac)(bd), \quad (ad)(bc)$$

而觀,則 1 乃自己共軛元素,故雖以 $\mathfrak{A}$ 之任何元素而變其形,其結果不過 1 也.又他之三元素相集,乃作成 $\mathfrak{A}$ 中一共軛元素系(第30節例).故將此三元素之一,以 $\mathfrak{A}$ 之元素而變形,其結果仍與此三元素之一等.如是,$\mathfrak{B}$ 者,爲雖以 $\mathfrak{A}$ 之任何元

素而將其元素變形,其所得仍屬於$\mathfrak{B}$之一物也.故對於$\mathfrak{A}$之任意元素A,得

$$A^{-1}\mathfrak{B}A=\mathfrak{B}. \qquad \text{(參照第32節注意)}$$

於是,一羣$\mathfrak{G}$之約羣$\mathfrak{N}$,若對於$\mathfrak{G}$之任意元素G,滿足

$$G^{-1}\mathfrak{N}G=\mathfrak{N} \quad 或 \quad \mathfrak{N}G=G\mathfrak{N}$$

之條件,換言之,$\mathfrak{N}$與$\mathfrak{G}$所有之元素爲交換可能*時,則$\mathfrak{N}$於$\mathfrak{G}$曰自己共軛,或正常云.如$\mathfrak{B}$之爲$\mathfrak{A}$之自己共軛約羣是.

羣$\mathfrak{G}$之約羣$\mathfrak{N}$爲自己共軛時,則由定義,對於$\mathfrak{G}$之任意元素G,而有$\mathfrak{N}G=G\mathfrak{N}$也.故若N爲$\mathfrak{N}$之元素,則得

$$NG=GN',\ GN=N''G,$$

式中N', N''爲$\mathfrak{N}$之元素.此雖一極其簡單之事,但因常遇,是特須留意者耳.

此外則由定義,可知自己共軛約羣,單獨形成共軛約羣系也.

定理, 羣$\mathfrak{G}$之兩個自己共軛約羣之最大公約羣,於$\mathfrak{G}$爲自己共軛.

證明. 以$\mathfrak{N}_1$, $\mathfrak{N}_2$爲$\mathfrak{G}$之自己共軛約羣,而$\mathfrak{D}$爲兩約羣之最大公約羣.取$\mathfrak{D}$之元素D,而以$\mathfrak{G}$之任意元素G將其變形.於是,因$\mathfrak{N}_1$, $\mathfrak{N}_2$爲自己共軛,故$G^{-1}DG$者,若視D屬於$\mathfrak{N}_1$,則屬於$\mathfrak{N}_1$;而以D爲屬於$\mathfrak{N}_2$,則屬於$\mathfrak{N}_2$.故$G^{-1}DG$乃爲$\mathfrak{N}_1$及$\mathfrak{N}_2$所公

* $\mathfrak{N}$與元素G交換可能者,非$\mathfrak{N}$之各元素與G交換可能之意,乃以G將$\mathfrak{N}$之元素變形,其所得結果,仍屬於$\mathfrak{N}$之意云爾也.(參照第26節)

共,因之卽爲$\mathfrak{D}$之元素也.如是,$\mathfrak{D}$之元素者,雖以$\mathfrak{G}$之任何元素而將其變形,其結果仍屬於$\mathfrak{D}$者也.故$\mathfrak{D}$於$\mathfrak{G}$爲自己共軛.

例. 於前節例2中之羣$\mathfrak{T}$,其二約羣

$$\{1,(ab)(cd),(ac)(bd),(ad)(bc)\},\{1,(ab)(cd),(ab),(cd)\},$$

卽於$\mathfrak{T}$爲自己共軛者也.故由本定理,知兩者之最大公約羣$\{1,(ab)(cd)\}$亦需同樣.此則以$\mathfrak{T}$之各置換將$(ab)(cd)$變形,卽可知之.

定理. 與羣$\mathfrak{G}$之約羣$\mathfrak{H}$共軛之約羣全體中之共通元素相集,卽作成$\mathfrak{G}$之自己共軛約羣.

證明. 以約羣$\mathfrak{H}$所屬之共軛約羣系爲

$$(1)\qquad \mathfrak{H},\quad P_1^{-1}\mathfrak{H}P_1,\quad P_2^{-1}\mathfrak{H}P_2,\cdots\cdots,\quad P_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1},$$

而以其全體所共通之一切元素之集合爲$\mathfrak{D}$.

$\mathfrak{D}$之爲羣,明已.(第22節系)

次以G爲$\mathfrak{G}$之元素,而以其逆G^{-1}將(1)之各個變形,得

$$(2)\quad G\mathfrak{H}G^{-1},\ GP_1^{-1}\mathfrak{H}P_1G^{-1},\ GP_2^{-1}\mathfrak{H}P_2G^{-1},\cdots\cdots,GP_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1}G^{-1}$$

如是,此諸羣當然與$\mathfrak{H}$共軛* 也.然由假設,與$\mathfrak{H}$共軛之約羣,皆共有$\mathfrak{D}$者.故(2)之約羣乃共有$\mathfrak{D}$.於是以$\mathfrak{D}$視爲$G\mathfrak{H}G^{-1}$之約羣,則$G^{-1}\mathfrak{D}G$含於

$$G^{-1}\cdot G\mathfrak{H}G^{-1}\cdot G=\mathfrak{H},$$

若以$\mathfrak{D}$視爲$GP_i^{-1}\mathfrak{H}P_iG^{-1}(i=1,2,\cdots\cdots,\nu-1)$之約羣,則$G^{-1}\mathfrak{D}G$含於

---

* (2)之約羣皆互異,因之(2)與(1)乃同一之共軛約羣系,此則容易證明者也,但共軛約羣之排列順序則未顧及.

$$G^{-1}\cdot GP_i^{-1}\mathfrak{S}P_iG^{-1}\cdot G=P_i^{-1}\mathfrak{S}P_i \quad (i=1, 2, \cdots\cdots, \nu-1).$$

故 $G^{-1}\mathfrak{T}G$ 含於(1)之所有之羣中,因之即含於 $\mathfrak{T}$ 也.故對於 $\mathfrak{D}$ 之任意元素 G

$$G^{-1}\mathfrak{T}G=\mathfrak{D},$$

即 $\mathfrak{T}$ 爲自己共軛也.(參照第32節注意).

例　前節例 2 中共軛約羣

$$\mathfrak{T},\ (ac)\mathfrak{T}(ac),\ (ad)\mathfrak{T}(ad)$$

之最大公約羣

$$\mathfrak{V}:\ 1,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc),$$

由本定理,知於四次對稱羣 $\mathfrak{S}$ 爲自己共軛.

35.　單羣,複羣

羣,大別之有二種.凡除羣自身及主元素羣以外,無有正常約羣者,曰單純羣或單羣;不然者,即除羣自身及主元素羣以外,有正常約羣者,曰**複合羣**,或**複羣**.

元數不爲素數之 Abel 氏羣,常爲複合的.蓋若以 $\mathfrak{A}$ 爲 Abel 氏羣,S 爲其一元素(不爲主元素者),則 S 之巡回率 s 較 $\mathfrak{A}$ 之元數 a 小時,巡回羣 $\{S\}$ 爲 $\mathfrak{A}$ 之眞約羣.*然 Abel 氏羣之元素皆自己共軛,故此約羣之爲正常,明已.故 $s<a$ 時,$\{S\}$ 者,$\mathfrak{A}$ 之正常眞約羣(≠1)也.反之,$s=a$ 時,取 s 之一約數 $d(<s)$,而作巡回約羣 $\{S^d\}$,則其元數爲 $\frac{s}{d}$,因之 $\{S^d\}$ 爲 $\mathfrak{A}$ 之正常眞約羣(≠1)

* 設 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之約羣.若不含於 $\mathfrak{H}$ 之元素而存在於 $\mathfrak{G}$ 時,則 $\mathfrak{H}$ 名曰 $\mathfrak{G}$ 之眞約羣.

由是以觀,無論如何,$\mathfrak{A}$除其自身及主元素羣外必有正常約羣也.因之,元數不爲素數之 Abel 氏羣爲複合的.

又凡一羣中自己共軛元素之集合,乃爲正常約羣.蓋若 S_1, S_2 爲羣 $\mathfrak{G}$ 之自己共軛元素,則對於 $\mathfrak{G}$ 之任意元素 G,

$$S_1G=GS_1, \quad S_2G=GS_2,$$

故

$$S_1S_2\cdot G=S_1GS_2=G\cdot S_1S_2,$$

S_1, S_2 之積,既與 $\mathfrak{G}$ 之各元素爲交換可能,因之亦自己共軛也.故自己共軛元素之集合成羣焉.且自己共軛元素,雖以 $\mathfrak{G}$ 之任何元素變其形,其結果仍不外乎其自身,故自己共軛元素所作之羣之爲正常的,明也.

一羣中自己共軛元素所作之正常約羣,曰羣之**中核**.中核者在 Abel 氏羣,則與羣自身一致,否則爲其眞約羣也.故主元素以外,尙有自己共軛元素,而元數不爲素數之羣,如元數等於素數之羃者(第 31 節定理),常爲複合的也.

36. 重傍系.

設 $\mathfrak{H}$ 及 $\mathfrak{K}$ 爲羣 $\mathfrak{G}$ 之約羣,而 S 爲 $\mathfrak{G}$ 之一元素時,則積 $\mathfrak{H}S\mathfrak{K}$ 名曰屬於 $\mathfrak{H}$ 及 $\mathfrak{K}$ 之重傍系.

定理. 於重傍系 $\mathfrak{H}S\mathfrak{K}$,其互異元素之數,等於以二約羣 $S^{-1}\mathfrak{H}S$ 及 $\mathfrak{K}$ 之最大公約羣之元數除 $\mathfrak{H}$ 之元數與 $\mathfrak{K}$ 之元數之積所得之商.

證明.

$$\mathfrak{H}S\mathfrak{K}=S(S^{-1}\mathfrak{H}S\cdot\mathfrak{K}),$$

故於 $\mathfrak{H}S\mathfrak{K}$ 中互異元素之數,乃與 $S^{-1}\mathfrak{H}S\cdot\mathfrak{K}$ 中者等(第 26 節). 但

兩約羣 $S^{-1}\mathfrak{H}S$ 及 $\mathfrak{G}$ 之積中互異元素之數,等於以其最大公約羣之元數除兩者之元數之積所得之商(第27節).而 $S^{-1}\mathfrak{H}S$ 之元數與 $\mathfrak{H}$ 之元數一致.故定理云云.

定理. 元素 T 若屬於重傍系 $\mathfrak{H}S\mathfrak{K}$, 則重傍系 $\mathfrak{H}T\mathfrak{K}$ 與 $\mathfrak{H}S\mathfrak{K}$ 一致,否則 $\mathfrak{H}T\mathfrak{K}$ 與 $\mathfrak{H}S\mathfrak{K}$ 無有共通之元素.

證明. 若 T 屬於 $\mathfrak{H}S\mathfrak{K}$, 則

$$T=HSK \quad (H, K \text{分別爲} \mathfrak{H}, \mathfrak{K} \text{之元素})$$

$$\therefore \quad \mathfrak{H}T\mathfrak{K}=\mathfrak{H}HSK\mathfrak{K}.$$

但

$$\mathfrak{H}H=\mathfrak{H}, \quad K\mathfrak{K}=\mathfrak{K} \quad (\text{第23節定理})$$

$$\therefore \quad \mathfrak{H}T\mathfrak{K}=\mathfrak{H}S\mathfrak{K}.$$

次之,若兩重傍系有共通之元素,如

$H'TK'=H''SK''$ (H', H'' 爲 $\mathfrak{H}$ 之元素; K', K'' 爲 $\mathfrak{K}$ 之元素),

則兩邊以 H'^{-1} 左乘,以 K'^{-1} 右乘,得

$$T=(H'^{-1}H'')\,S\,(K''K'^{-1})$$

然 $H'^{-1}H''$ 屬於 $\mathfrak{H}$, $K''K'^{-1}$ 屬於 $\mathfrak{K}$, 故 T 不得不爲 $\mathfrak{H}S\mathfrak{K}$ 之元素也. 因之 T 若不屬於 $\mathfrak{H}S\mathfrak{K}$ 時,則 $\mathfrak{H}T\mathfrak{K}$ 與 $\mathfrak{H}S\mathfrak{K}$ 無有共通之元素.故云云.

且羣 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$, $\mathfrak{K}$ 之積,有與 $\mathfrak{G}$ 一致及不一致者.以後者論,乃取不屬於 $\mathfrak{H}\mathfrak{K}$ 之 $\mathfrak{G}$ 之元素 S_1 而作重傍系 $\mathfrak{H}S_1\mathfrak{K}$, 則 $\mathfrak{H}\mathfrak{K}$ 與 $\mathfrak{H}S_1\mathfrak{K}$ 無共有之元素.故若以兩傍系而能盡 $\mathfrak{G}$ 之元素之全部,則有

$$\mathfrak{G}=\mathfrak{H}\mathfrak{R}+\mathfrak{H}S_1\mathfrak{R}.*$$

反之,不屬於兩傍系之元素尙存在於$\mathfrak{G}$時,取其一如S_2,作重傍系$\mathfrak{H}S_2\mathfrak{R}$,則此與前之兩重傍系無公共元素也.故若以此三個重傍系而$\mathfrak{G}$之所有元素得盡時,則

$$\mathfrak{G}=\mathfrak{H}\mathfrak{R}+\mathfrak{H}S_1\mathfrak{R}+\mathfrak{H}S_2\mathfrak{R}.$$

若以此三重傍系尙不能盡$\mathfrak{G}$之元素,則取不屬於此三者之元素而將同樣之手續反覆行之.然$\mathfrak{G}$之元數乃有限,故有限回之後,$\mathfrak{G}$之所有元素必盡,而得

$$\mathfrak{G}=\mathfrak{H}\mathfrak{R}+\mathfrak{H}S_1\mathfrak{R}+\mathfrak{H}S_2\mathfrak{R}+\cdots\cdots.$$

如是,$\mathfrak{G}$之元素,乃於屬於$\mathfrak{H}$及$\mathfrak{R}$之若干重傍系而得分類也.此之謂將$\mathfrak{G}$就$\mathfrak{H}$及$\mathfrak{R}$分爲重傍系云:

第五章 合同,商羣

37. 合同之元理.

數學中研究之對象,元素之集合也,數論代數學尤然.其間關於元素之相等不等,結合及結合之法則,乃有若干之公理以爲其規定.而結合則一般爲一意的者也.卽若A等於A′,B等於B′,則A與B結合之結果,與A′與B′結合之結果等而定厥義者是.又就元素之相等不等言,有如第14節所述,只需其能滿足三個條件,則其他任如何定之,均無所不可也.此相

* 參照第21節及同節注意2.

等不等之關係,如論運動羣者然(第16,17節),最初卽揭以規約而明示之者,固有之矣,然不若是者亦有焉.雖然,無論如何,當其討論一對象如羣時,元素間之相等不等,既以其爲能由某規約而定者,而在此豫想之下,進行其推理可也.

今也吾人假定有對象焉,爲由相等之定義及關於結合之公理所規定者,茲公理方面,不稍變更,一仍舊貫;只於其相等定義,欲事更張,能乎?否乎?是卽使始初相等之元素,定義變更後,亦仍相等;且在此變更後,各元素仍能滿足始初所與之公理;於若是條件之下以企圖變更,究竟能否之謂也.如云可能,則須以何方法而爲之乎?

欲獲此問題之解決,必先求變更時之必要條件.換言之,則須討論由相等定義變更之結果,其相等之元素,究可作如何組類是也.次之,須決定者,此必要條件,使適合矣,然果能卽成就吾人所欲之變更否?卽謂必要條件同時復爲充分條件否之問題也.此如得知,則變更之方法亦自明白.第變更之可能條件,隨之,其方法,以規定對象之公理之種類之不同而自異,故欲概括於一言之下爲不可能耳.此相等定義之變更,乃構成數學上合同之根本觀念者.在從來數論代數學中所與之合同之定義,雖由對象異而隨異而不一定,然皆僅採取於相等定義變更方法之表面上所顯現者,因定義之變更,則對於相等兩元素稱爲兩者合同已耳.又他之部門中,有廣義的解釋之得視爲合同者之諸事項亦復同樣.於是由相等定義

變更之見地,可將在種種情形下所表現於各種形狀之合同定義,得以統一之焉.

38. 羣之合同.

本節中乃以前之立場而就羣之合同一述.特爲避術語及記號之混淆,而又求言辭之簡單起見,乃於定義變更後之相等不等自始卽用合同非合同之語,而分別以記號≡,≢表示.吾人之所得而論,乃在使適合次之條件,而將此相等定義之變更,對於羣而述之焉.

(I)(i) 若 A 等於 B,則於定義變更之後,A 爲合同於 B;又若 A 與 B 合同,則 B 亦與 A 合同.

(ii) 兩元素,或合同,或非合同,二者必居其一,且以一爲限.

(iii) 若 A≡B, B≡C, 則 A≡C.

(II) 若 A≡B, A′≡B′, 則 AA′≡BB′.

(III) 羣之四條件.

今請就其結果述之,爰有次之

定理. 對於羣之相等定義之變更,其合同關係,必定之如次:

(i) 於與羣𝔊之元素中,其與主元素合同者之全體,作成𝔊之正常約羣𝔑.

(ii) 就𝔑言,其屬於同一傍系之元素,互爲合同.

(iii) 互爲合同之元素,就𝔑言,屬於同一之傍系.

反之,此三條件皆爲充分的.

證明. 1°. 於羣 $\mathfrak{G}$, 假定其相等定義之變更爲已成就者;其結果,與主元素相等之元素之集合,以爲 $\mathfrak{N}$.

(i) 以 N, N′ 爲 $\mathfrak{N}$ 之任意二元素,則

$$N\equiv 1, \qquad N'\equiv 1.$$

故由變更條件(II),

$$NN'\equiv 1\cdot 1.$$

但 $$1\cdot 1=1,$$

因之由(I, i), $$1\cdot 1\equiv 1.$$

故由(I, iii), $$N\cdot N'\equiv 1$$

卽 $\mathfrak{N}$ 之二元素之積 NN′ 屬於 $\mathfrak{N}$.故 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之約羣.

次之,取 $\mathfrak{G}$ 之任意元素 G,而以此將 $\mathfrak{N}$ 之元素 N(≡1)變形,則由(I, i),

$$G^{-1}\equiv G^{-1}, \qquad G\equiv G,$$

故由(II), $$G^{-1}NG\equiv G^{-1}\cdot 1\cdot G.$$

但 $$G^{-1}\cdot 1\cdot G=1,$$

因之由(I, i), $$G^{-1}\cdot 1\cdot G\equiv 1.$$

故由(I, iii), $$G^{-1}NG\equiv 1.$$

是卽 $\mathfrak{N}$ 之元素者,雖以 $\mathfrak{G}$ 之任何元素變其形,其結果仍屬於 $\mathfrak{N}$ 者也.故 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之正常約羣.

(ii) 由傍系 $\mathfrak{N}$A, 任意取二元素 NA, N′A(N, N′爲 $\mathfrak{N}$ 之元素),

因 $N\equiv 1,\quad N'\equiv 1,\quad A\equiv A,$

故由(II), $NA\equiv 1\cdot A,\qquad N'A\equiv 1\cdot A.$

再由(I, iii), $NA\equiv N'A$

如是,同一傍系之元素,互爲合同也.

(iii) 由定義之變更,若元素B已等於A,卽 $B\equiv A$,則由(I, i),因 $A^{-1}\equiv A^{-1}$,故由(II),

$$BA^{-1}\equiv AA^{-1}.$$

然 $AA^{-1}=1,$

因之由(I, i), $AA^{-1}\equiv 1.$

故由(I, iii), $BA^{-1}\equiv 1.$

因之 BA^{-1} 非屬於 $\mathfrak{N}$ 不可也.今以

$$BA^{-1}=N\quad (N\text{爲}\mathfrak{N}\text{之元素}),$$

則得 $B=NA.$

因之B屬於A之所屬之同一傍系 $\mathfrak{N}A$ 也.

2°. 逆之證明.

以 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之正常約羣,而相等之定義,則以之爲已適合上記之條件(i),(ii)及(iii)而曾變更者.

(a) 其結果,對於相等之條件(I, i),(I, ii),及(I, iii)之得滿足,明已.

(b) 以A, B爲 $\mathfrak{G}$ 之任意的元素,則由(ii)及(iii),與A合同之元素,形成傍系 $\mathfrak{N}A$ 也;與B合同之元素,形成傍系 $\mathfrak{N}B$ 也.再就由兩傍系各取一個之元素 NA, N'B 之積而觀,因 $\mathfrak{N}$ 爲正

常的,故

$$NA\cdot N'B=N''(AB)\quad (N''\text{ 乃 }\mathfrak{N}\text{ 之元素}).\ (\text{參照第34節})$$

但右邊乃屬於傍系 $\mathfrak{N}(AB)$ 之元素,因之由條件 (ii),

$$N''(AB)\equiv AB.$$

故由(a),

$$NA\cdot N'B\equiv AB.$$

如是,與 A 合同之元素及與 B 合同之元素之積常與 A 及 B 之積合同也.因之,其結合爲一意的.

(c)　因 $\mathfrak{G}$ 爲羣,故其二元素之積與 $\mathfrak{G}$ 之一元素等,因之由(a),亦卽與之合同.

次之,因對於 $\mathfrak{G}$ 之三元素 A, B, C,

$$(AB)C=A(BC),$$

故由(a),

$$(AB)C\equiv A(BC).$$

又因對 $\mathfrak{G}$ 之元素 A,

$$A\cdot 1=A,\quad AA^{-1}=1,$$

故由(a),

$$A\cdot 1\equiv A,\quad AA^{-1}\equiv 1.$$

故雖在相等定義之變更後,$\mathfrak{G}$ 之元素亦成羣也.故云云.

39. 羣之相等定義之變更,如前節之所示,乃由將正常約羣之元素,使與主元素等而完全行使者,且只由是而後始可能.於是再定義之曰:於羣 $\mathfrak{G}$,使其正常約羣 $\mathfrak{N}$ 之元素與主元素等而變更其相等定義時,則此名曰對於法 $\mathfrak{N}$ 而取 $\mathfrak{G}$ 云.由是而兩元素相等者,稱曰對於法 $\mathfrak{N}$ 爲相互合同;其不相等者,曰對於法 $\mathfrak{N}$ 爲非合同.兩元素 A, B, 對於法 $\mathfrak{N}$ 合同者,以

$$A\equiv B(\mathrm{mod.}\ \mathfrak{N})$$

表之;其爲非合同者,以

$$A\not\equiv B(\mathrm{mod.}\ \mathfrak{N})$$

表之焉.

特別當N爲$\mathfrak{N}$之元素時,則有

$$N\equiv 1(\mathrm{mod.}\ \mathfrak{N}).$$

就合同而言,使不溯其根本觀念,而僅就處理上之便利以立論,則釋之如次,亦爲得也.於羣$\mathfrak{G}$,其二元素A, B,對正常約羣$\mathfrak{N}$,爲屬於同一傍系時,則此兩元素曰對法$\mathfrak{N}$爲合同,而以$A\equiv B(\mathrm{mod.}\ \mathfrak{N})$表之.反之,兩者屬於異傍系時,則此兩元素曰對法$\mathfrak{N}$爲非合同,而以$A\not\equiv B(\mathrm{mod.}\ \mathfrak{N})$表之焉.

今將$\mathfrak{G}$就其正常約羣$\mathfrak{N}$而分爲傍系,則有

$$(1)\qquad \mathfrak{G}=\mathfrak{N}+\mathfrak{N}Q_1+\cdots\cdots+\mathfrak{N}Q_{\mu-1}.$$

茲由各傍系而各取出一元素,若以之爲

$$(2)\qquad Q_0',\ Q_1',\cdots\cdots,Q'_{\mu-1},$$

則此各元素,由合同之定義,乃有次之性質:

(a) 此諸元素,對於法$\mathfrak{N}$互爲非合同;

(b) $\mathfrak{G}$之元素,對於法$\mathfrak{N}$,與此之或一爲合同.

一般,$\mathfrak{G}$之若干元素之集合,若有與(2)同樣之性質(a)及(b)時,則此集合名曰$\mathfrak{G}$之**非合同(法$\mathfrak{N}$)元素系**.

對於非合同(法$\mathfrak{N}$)元素系,如(2),則

$$\mathfrak{G}=\mathfrak{N}Q_0'+\mathfrak{N}Q_1'+\cdots\cdots+\mathfrak{N}Q'_{\mu-1}$$

甚明.

注意. 設$\mathfrak{M}, \mathfrak{N}$爲$\mathfrak{G}$之正常約羣,而$\mathfrak{N}$又爲$\mathfrak{M}$之約羣.於是,對於$\mathfrak{G}$之二元素,若$A \equiv B \pmod{\mathfrak{N}}$,則$A \equiv B \pmod{\mathfrak{M}}$.此則注目於$\mathfrak{M}A$含有$\mathfrak{N}A$以爲其部分之一點自明也.

40. 商羣.

將羣$\mathfrak{G}$,就其正常約羣$\mathfrak{N}$而取之之時,其所生之羣,名曰對於$\mathfrak{N}$之$\mathfrak{G}$之商羣,或簡曰商,而以$\frac{\mathfrak{G}}{\mathfrak{N}}$表之.*

商羣乃羣論上重要要素之一,故爲助讀者之理解及研究之便利計,不厭重複,再申述如次.用前節之記號,而以

$$(2) \qquad Q_0', Q_1', \cdots\cdots, Q'_{\mu-1}$$

爲羣$\mathfrak{G}$之非合同(法$\mathfrak{N}$)元素系.於是此諸元素,就其對於法$\mathfrak{N}$之結合言,實具備下記之四性質,因之成羣也.是卽商羣$\frac{\mathfrak{G}}{\mathfrak{N}}$焉.而其元數,則與$\mathfrak{N}$對於$\mathfrak{G}$之指數等明甚.

(i) 非合同元素系(2)之二元素之積,對於法$\mathfrak{N}$,乃與(2)之一合同.

蓋因$\mathfrak{G}$爲羣,故(2)之二元素之積$Q_i'Q_j'$屬於$\mathfrak{G}$.但(2)乃非合同(法$\mathfrak{N}$)元素系,故積$Q_i'Q_j'$與(2)之一元素合同(法$\mathfrak{N}$).

(ii) 三元素之積間,組合法則常成立.

蓋因
$$(Q_i'Q_j')Q_k' = Q_i'(Q_j'Q_k'),$$
$$(Q_i'Q_j')Q_k' \equiv Q_i'(Q_j'Q_k') \pmod{\mathfrak{N}}.$$

(iii) 因Q_0'爲屬於$\mathfrak{N}$之元素,故

---

*商羣$\mathfrak{G}/\mathfrak{N}$亦有稱之曰關於$\mathfrak{G}$之$\mathfrak{N}$之補羣者.

$$Q_0' \equiv 1 \pmod{\mathfrak{N}}.$$

故對於(2)之任意元素 Q_i'

$$Q_i' Q_0' \equiv Q_i' \pmod{\mathfrak{N}}$$

是卽 Q_0' 不啻爲主元素矣.

(iv) $\mathfrak{G}$ 之元素既與(2)之一合同(法 $\mathfrak{N}$),故與(2)之一元素 Q_i' 之逆 $Q_i'^{-1}$ 合同(法 $\mathfrak{N}$)之元素,必存在於(2)內.以之爲 Q_k',則

$$Q_i' Q_k' \equiv Q_i Q_i'^{-1} \pmod{\mathfrak{N}}.$$

$$\therefore \quad Q_i' Q_k' \equiv 1 \pmod{\mathfrak{N}}.$$

但

$$Q_0' \equiv 1 \pmod{\mathfrak{N}},$$

$$\therefore \quad Q_i' Q_k' \equiv Q_0' \pmod{\mathfrak{N}}.$$

是卽 Q_k' 爲 Q_i' 之逆也.

41. 定理. 若羣 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$ 之各元素與他之約羣 $\mathfrak{N}$ 爲交換可能時,則兩商羣 $\frac{\mathfrak{H}\mathfrak{N}}{\mathfrak{N}}$ 及 $\frac{\mathfrak{H}}{\mathfrak{Q}}$ 爲同態.但 $\mathfrak{Q}$ 爲 $\mathfrak{H}$ 與 $\mathfrak{N}$ 之最大公約羣.

證明. 由第27節之定理,則知積 $\mathfrak{H}\mathfrak{N}$ 者羣也.但 $\mathfrak{N}$ 既與 $\mathfrak{H}$ 之各元素爲交換可能,故卽 $\mathfrak{H}\mathfrak{N}$ 之正常約羣焉.此何故歟?蓋若 H 及 K 分別爲 $\mathfrak{H}$ 及 $\mathfrak{N}$ 之任意元素,則以積 HK 而使 $\mathfrak{N}$ 變形,便有

$$(HK)^{-1}\mathfrak{N}(HK) = K^{-1}H^{-1}\mathfrak{N}HK$$

$$= K^{-1}\mathfrak{N}K \quad (\because \text{由假設 } H^{-1}\mathfrak{N}H = \mathfrak{N} \text{ 故})$$

$$= \mathfrak{N}$$

故耳.

次之，$\mathfrak{L}$ 卽爲 $\mathfrak{H}$ 之正常約羣.蓋若 L 爲 $\mathfrak{L}$ 之任意元素，而以 $\mathfrak{H}$ 之任意元素 H 將其變形，則如以 L 爲 $\mathfrak{L}$ 之元素，乃由假設而知 $H^{-1}LH$ 屬於 $\mathfrak{K}$；若以 L 爲 $\mathfrak{H}$ 之元素，則是 $H^{-1}LH$ 之屬於 $\mathfrak{H}$ 爲當然也.故 $H^{-1}LH$ 爲 $\mathfrak{H}$ 及 $\mathfrak{K}$ 之所公共，因之屬於 $\mathfrak{L}$ 以故曰 $\mathfrak{L}$ 者 $\mathfrak{H}$ 之正常約羣也.

茲請證商羣 $\frac{\mathfrak{H}\mathfrak{K}}{\mathfrak{K}}$, $\frac{\mathfrak{H}}{\mathfrak{L}}$ 之爲同態.試以

$$(1) \qquad A, B, C, \cdots\cdots$$

爲對 $\mathfrak{L}$ 之 $\mathfrak{H}$ 之非合同元素系.此諸元素之屬於羣 $\mathfrak{H}\mathfrak{K}$，明已.且其對於法 $\mathfrak{K}$ 爲非合同的.蓋若假定 $A \equiv B \pmod{\mathfrak{K}}$，

則 $$AB^{-1} \equiv 1 \pmod{\mathfrak{K}},$$

是卽謂 AB^{-1} 非屬於 $\mathfrak{K}$ 不可也.但 A, B 皆爲 $\mathfrak{H}$ 之元素，故積 AB^{-1} 當然屬於 $\mathfrak{H}$.故 AB^{-1} 乃 $\mathfrak{H}$, $\mathfrak{K}$ 之所共通，因之卽必屬於 $\mathfrak{L}$，卽

$$AB^{-1} \equiv 1 \pmod{\mathfrak{L}}.$$

$$\therefore \qquad A \equiv B \pmod{\mathfrak{L}}.$$

是則與(1)爲非合同(法 $\mathfrak{L}$)元素系之假定相反.故(1)之元素對於 $\mathfrak{K}$ 爲非合同.

次之，試取羣 $\mathfrak{H}\mathfrak{K}$ 之任意元素 HK，(H, K 分別爲 $\mathfrak{H}$, $\mathfrak{K}$ 之元素)，因 $K \equiv 1 \pmod{\mathfrak{K}}$，故

$$(2) \qquad HK \equiv H \pmod{\mathfrak{K}}$$

然 $\mathfrak{H}$ 之元素 H，對於法 $\mathfrak{L}$，乃與(1)之一元素合同，而 $\mathfrak{L}$ 又係 $\mathfrak{K}$ 之約羣，故若以 H 爲屬於 $\mathfrak{H}\mathfrak{K}$，則 H 便與(1)之一元素合同(法 $\mathfrak{K}$).因之由(2)，HK 乃與(1)之一元素合同(法 $\mathfrak{K}$).

如是,(1)之元素屬於$\mathfrak{H}\mathfrak{R}$,而互爲非合同(法$\mathfrak{R}$),且$\mathfrak{H}\mathfrak{R}$之元素與(1)之一元素合同(法$\mathfrak{R}$).故(1)爲$\mathfrak{H}\mathfrak{R}$之非合同元素系(法$\mathfrak{R}$).

於是,(1),若就法$\mathfrak{L}$而取之,則爲商$\frac{\mathfrak{H}}{\mathfrak{L}}$,若就法$\mathfrak{R}$而取之,則爲商$\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}$. 即

$$\frac{\mathfrak{H}}{\mathfrak{L}}: \quad A, B, C, \cdots\cdots\cdots \pmod{\mathfrak{L}}$$

$$\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}: \quad A, B, C, \cdots\cdots\cdots \pmod{\mathfrak{R}}$$

更使兩羣之元素對應,對於$\frac{\mathfrak{H}}{\mathfrak{L}}$之A, B, C, ……,分別以$\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}$之A, B, C,…對應之,若$AB\equiv C \pmod{\mathfrak{L}}$,則$AB\equiv C \pmod{\mathfrak{R}}$(第39節注意).故對於$\frac{\mathfrak{H}}{\mathfrak{L}}$之二元素之積,乃有與是相應之$\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}$之二元素之積對應也.因之$\frac{\mathfrak{H}}{\mathfrak{L}}$與$\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}$爲同態.

42. 換位羣.

設A及B爲$\mathfrak{G}$之二元素,若令

$$A^{-1}B^{-1}AB = T, \tag{1}$$

則得

$$AB = BAT.$$

是卽於積BA以T右乘之,則因子之順序交換而成AB也.於是,此之T名曰A, B之**換位元素**云.

於(1)取其兩邊之逆,則有

$$B^{-1}A^{-1}BA = T^{-1}$$

故T爲A, B之換位元素時,則T^{-1}爲B, A之換位元素也.

於羣$\mathfrak{G}$,一元素爲其二元素之換位元素時,則此單稱曰

$\mathfrak{G}$之換位元素.主元素,常爲換位元素也.蓋若於(1)令B=A則得T=1故.特別在Abel氏羣時,**則只主元素爲換位元素.**因對其任意兩元素A, B,則有

$$A^{-1}B^{-1}AB=B^{-1}A^{-1}AB=1$$

故.反之,非Abel氏羣,於主元素外,常含有若干之換位元素焉.

一羣之換位元素之數,比在共軛元素系中含有最多數元素者之元素之數不爲少.蓋若於(1)之兩邊,以A左乘之,則得

$$B^{-1}AB=AT.$$

故換位元素者,乃以之右乘於一元素而克得其共軛元素者也.今以A之所屬共軛系爲含有最多數之元素,而以此數爲m,則欲得A之共軛元素,至少m個之換位元素爲必要.故換位元素之數不少於m.

茲於羣$\mathfrak{G}$,以其主元素以外所有之換位元素爲

(1)　　$T_1, T_2, \cdots\cdots\cdots, T_{\mathfrak{R}}$

含此$\mathfrak{R}$個元素之約羣中,元數之最小者只一個.* 名之曰$\mathfrak{G}$之換位羣.* 是羣也,乃以下記之方法,由換位元素而生成者也.

先由$T_1, T_2, \cdots\cdots\cdots, T_{\mathfrak{R}}$,盡量作其二因子之積(自乘者在

* 蓋若有二個,則其最大公約羣,便含有所有之換位元素,而與假定違反故也.

* 羣$\mathfrak{G}$之換位羣與$\mathfrak{G}$一致時,則$\mathfrak{G}$名曰完全羣.

內)乃將由此所得之新元素* 全體附加於$\mathfrak{R}$個之換位元素(卽(1)),此集合名曰(2). 次由$T_1, T_2, \cdots\cdots, T_{\mathfrak{R}}$,盡量作其三因子之積(同一因子有二以上亦可). 若由此不能得到不屬於(2)之元素,則(2)之爲羣,明已. 反之,如能得不屬於(2)之元素時,則以其全數附加於(2),而名其集合爲(3),更作其四因子之積. 苟由是再可得新元素,則再作其五因子之積. 反覆行之,因羣$\mathfrak{G}$之元數有限,故於有限回之後可無新元素復出現也. 如斯所得元素之集合,明成一羣. 是卽換位羣是已. 一般,由若干元素用上記之方法而作羣時,此卽名曰由所與元素以**生成**一羣,而所與元素曰**母元**素. 用此術語,則換位羣者,乃由換位元素所生成之羣者也.

定理. 一個羣之換位羣爲正常的(自己共軛).

證明. 以T爲羣$\mathfrak{G}$之二元素 A, B 之換位元素,乃以$\mathfrak{G}$之任意元素 G 而變其形,則有

$$G^{-1}TG = G^{-1}(A^{-1}B^{-1}AB)G$$
$$= G^{-1}A^{-1}G\cdot G^{-1}B^{-1}G\cdot G^{-1}AG\cdot G^{-1}BG$$
$$= (G^{-1}AG)^{-1}(G^{-1}BG)^{-1}(G^{-1}AG)(G^{-1}BG).$$

故換位元素 T 之共軛 $G^{-1}TG$ 爲二元素$(G^{-1}AG), (G^{-1}BG)$之換位元素. 但換位羣乃由換位元素所生成,今取換位羣之任意元素.

---

* (1)因不含主元素,故決不成羣. 於是作其二元素之積,倾產生不屬於(1)之元素爲必然也.

$S=TT'\cdots\cdots T^{(\lambda)}$ $(T, T', \cdots\cdots, T^{(\lambda)}$ 皆換位元素),而以 $\mathfrak{G}$ 之任意元素變其形,則得

$$G^{-1}SG=(G^{-1}TG)(G^{-1}T'G)\cdots\cdots(G^{-1}T^{(\lambda)}G).$$

而由上所示,其各因子,任何一皆換位元素.故 $G^{-1}SG$ 屬於換位羣.因之換位羣爲正常的.

定理. 設 $\mathfrak{N}$ 爲羣 $\mathfrak{G}$ 之正常約羣.若 $\mathfrak{G}$ 之換位羣爲 $\mathfrak{N}$ 之約羣時,則商 $\mathfrak{G}/\mathfrak{N}$ 爲 Abel 氏羣.反之,若 $\mathfrak{G}/\mathfrak{N}$ 爲 Abel 氏羣,則換位羣爲 $\mathfrak{N}$ 之約羣.

證明. 茲首以換位羣爲 $\mathfrak{N}$ 之約羣.若 A, B 爲 $\mathfrak{G}$ 之二元素,則

$$AB=BAT,$$

但 T 爲 A, B 之換位元素.今就法 $\mathfrak{N}$ 而取 $\mathfrak{G}$,則因 $\mathfrak{N}$ 含有所有換位元素之故,

$$T\equiv 1 \pmod{\mathfrak{N}}.$$

$$\therefore \quad AB\equiv BA \pmod{\mathfrak{N}}.$$

如斯對於法 $\mathfrak{N}$ 而取 $\mathfrak{G}$ 時,其所生之羣即商 $\mathfrak{G}/\mathfrak{N}$ 中,交換法則實成立也,故 $\mathfrak{G}/\mathfrak{N}$ 爲 Abel 氏羣.

次之,命 $\mathfrak{G}/\mathfrak{N}$ 爲 Abel 氏羣.於是對於 $\mathfrak{G}$ 之任意二元素 A, B, 乃有

$$AB\equiv BA \pmod{\mathfrak{N}}.$$

$$\therefore \quad A^{-1}B^{-1}AB\equiv 1 \pmod{\mathfrak{N}}.$$

但 $(A^{-1}B^{-1}AB)$ 乃 A, B 之換位元素.故 $\mathfrak{G}$ 之換位元素,任何一

皆屬於$\mathfrak{N}$,因之換位羣爲$\mathfrak{N}$之約羣.

系. 若$\mathfrak{N}$爲羣$\mathfrak{G}$之換位羣,則商$\mathfrak{G}/\mathfrak{N}$爲Abel氏羣.(此商名曰**換位商羣**,或單曰**換位商**).

例1. 第31節例中所示之羣之換位元素爲

$$1, \quad (ac)(bd),$$

而此兩元素卽作成一換位羣.

例2. 四次交代羣(第12節例2,或第24節$\mathfrak{N}$)之換位元素,爲 $1, \quad (ab)(cd), (ac)(bd), (ad)(bc)$

此時,此四元素亦卽形成一換位羣也.(參照第30節例)

例3. 於四次對稱羣(第11節例2),其四次交代羣之元素,皆爲換位元素.因之,交代羣乃對稱羣之換位羣.

注意. 於某共軛元素系,若屬於此之一元素爲換位元素,則他之元素亦同然.(參照第一定理證明).

第六章 重複同態

43. 重複同態.

於兩羣$\mathfrak{G}$,$\mathfrak{G}'$,若兩者之元素間得有適合下之條件之對應時,則兩羣曰同態.

(i) 對於$\mathfrak{G}$之各元素,乃有$\mathfrak{G}'$之若干元素與之對應,反之,於$\mathfrak{G}'$之各元素,乃有$\mathfrak{G}$之若干元素與之對應.

(ii) 若$\mathfrak{G}$之元素A與$\mathfrak{G}'$之元素A′對應,又$\mathfrak{G}$之元素B

與$\mathfrak{G}'$之元素B'對應時,則AB與A'B'亦對應.*

特別,對於一羣之元素,其各個皆有他羣之一元素與之對應時,則此同態曰單純的,否則其同態曰重複的.第21節之定義,乃就前者而言者也.

定理. 若兩羣$\mathfrak{G}$,$\mathfrak{G}'$爲同態時,以與$\mathfrak{G}$之主元素對應之$\mathfrak{G}'$之元素之集合爲$\mathfrak{N}'$,與$\mathfrak{G}'$之主元素對應之$\mathfrak{G}$之元素之集合爲$\mathfrak{N}$,則

(i) $\mathfrak{N}$爲$\mathfrak{G}$之正常約羣;$\mathfrak{N}'$爲$\mathfrak{G}'$之正常約羣.

(ii) 與$\mathfrak{G}$之同一元素對應之$\mathfrak{G}'$之元素,形成屬於$\mathfrak{N}'$之一傍系;而與$\mathfrak{G}'$之同一元素對應之$\mathfrak{G}$之元素,形成屬於$\mathfrak{N}$之一傍系.

(iii) 對於就$\mathfrak{N}$(又$\mathfrak{N}'$)爲同一之傍系中所屬之元素,乃有就$\mathfrak{N}'$(又$\mathfrak{N}$)爲同一之傍系中所屬之元素與之對應.

證明. 爲敍述之簡明起見,乃以A, B, C, ……表$\mathfrak{G}$之元素,而$\mathfrak{G}'$之元素,遂將其附以 ' 而以A' B' C'……表之;至與A對應之元素之一爲A'(因之A乃與A'對應之元素之一)之表示,卽以A～A'記之焉.

(i) 若N_1, N_2爲$\mathfrak{N}$之任意二元素,則由假設,

$$N_1 \sim 1, \quad N_2 \sim 1,$$

---

* 就對應言,當A爲對應於A'之一元素時,則A'乃視爲與A對應元素之一者也.又A, A'二者,其各個爲與其他個相對應之元素之一時,爲語句之簡潔起見,便記爲A與A'對應云.

故由同態之條件(ii),

$$N_1N_2\sim 1\cdot 1\ (=1).$$

因之積 N_1N_2 亦屬於 $\mathfrak{N}$,故 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之約羣.

次以 G 爲 $\mathfrak{G}$ 之任意元素,G′ 爲與之對應之 $\mathfrak{G}'$ 之元素之一,則有

$$G^{-1}\sim G'^{-1}.$$

蓋若取 m 爲與 G 及 G′ 之巡回率之公倍數(>1)等時,則

$$G^m=1,\qquad G'^m=1.$$

因之

$$G^{m-1}=G^{-1},\quad G'^{m-1}=G'^{-1}.$$

但由同態之條件(ii),

$$G^{m-1}\sim G'^{m-1},$$

$$\therefore\quad G^{-1}\sim G'^{-1}$$

今以 N 爲 $\mathfrak{N}$ 之任意元素,則與之對應者,爲 $\mathfrak{G}'$ 之主元素.

故

$$G^{-1}NG\sim G'^{-1}\cdot 1\cdot G'\ (=1).$$

因之 $G^{-1}NG$ 屬於 $\mathfrak{N}$. 如是,$\mathfrak{N}$ 之元素,雖以 $\mathfrak{G}$ 之任何元素變其形,其結果仍爲 $\mathfrak{N}$ 之元素.故 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之正常約羣也.

同樣,$\mathfrak{N}'$ 爲 $\mathfrak{G}'$ 之正常約羣.

(ii) 以 A,B 爲與 $\mathfrak{G}'$ 之元素 A′ 對應之 $\mathfrak{G}$ 之元素之二,即

$$A\sim A',\qquad B\sim A'$$

然由上所示,

$$A^{-1}\sim A'^{-1},$$

故由同態之條件(ii),

$$BA^{-1}\sim A'A'^{-1}\ (=1).$$

故 BA^{-1} 必屬於 $\mathfrak{N}$. 卽

$$BA^{-1}=N \quad (N \text{ 爲 } \mathfrak{N} \text{ 之元素}).$$

$$\therefore \qquad B=NA.$$

此卽示 B 屬於傍系 $\mathfrak{N}A$ 者也.

次取屬於傍系 $\mathfrak{N}A$ 之任意元素 N_1A,則因 $N_1\sim 1$, $A\sim A'$,故

$$N_1A\sim 1\cdot A' \quad (=A').$$

卽謂傍系 $\mathfrak{N}A$ 之元素皆與 A' 對應也.

因之,若 $A\sim A'$,則由上述之兩項,知與 A' 對應之 $\mathfrak{G}$ 之元素,形成傍系 $\mathfrak{N}A$.

同樣, $A\sim A'$ 時,則與 A 對應之 $\mathfrak{G}'$ 之元素,形成傍系 $\mathfrak{N}'A'$.

(iii) 以 N' 爲 $\mathfrak{N}'$ 之任意元素,而 $A\sim A'$,則因 $1\sim N'$,故由同態之條件(ii),

$$1\cdot A\sim N'A'.$$

$$\therefore \qquad A\sim N'A'.$$

故與 $N'A'$ 對應之 $\mathfrak{G}$ 之元素,由本定理(ii),乃形成傍系 $\mathfrak{N}A$. 但與 A' 對應之 $\mathfrak{G}$ 之傍系,亦爲 $\mathfrak{N}A$. 故與傍系 $\mathfrak{N}'A'$ 之任意元素 $N'A'$ 對應之傍系,乃與與 A' 對應者同一也.

系. $\mathfrak{G}$ 及 $\mathfrak{G}'$ 爲同態時,則與屬於就 $\mathfrak{N}$ 爲相異之傍系之元素相對應之 $\mathfrak{G}'$ 之傍系(對於 $\mathfrak{N}'$ 者)亦互異.但 $\mathfrak{N}$, $\mathfrak{N}'$ 之意義,與在本定理中者同.

證明. 若與 $\mathfrak{G}$ 之一元素 A 對應之 $\mathfrak{G}'$ 之傍系,以及與他之元素 B 對應者同爲 $\mathfrak{N}'A'$,則得

$$A\sim A',\quad B\sim A'.$$

由本定理,則B非屬於$\mathfrak{N}A$不可.故若B不屬於$\mathfrak{N}A$,則與A對應之$\mathfrak{G}'$之傍系以及與B對應者,不得不互異也.

44. 定理. $\mathfrak{G}$及$\mathfrak{G}'$爲同態時,則二商$\mathfrak{G}/\mathfrak{N}$及$\mathfrak{G}'/\mathfrak{N}'$爲單純同態.但$\mathfrak{N}$爲與$\mathfrak{G}'$之主元素相對應之$\mathfrak{G}$之正常約羣,$\mathfrak{N}'$爲與$\mathfrak{G}$之主元素相對應之$\mathfrak{G}'$之正常約羣.

證明. 今將$\mathfrak{G}$就$\mathfrak{N}$分爲傍系:

$$(1)\qquad \mathfrak{G}=\mathfrak{N}Q_0+\mathfrak{N}Q_1+\cdots\cdots+\mathfrak{N}Q_{\mu-1},$$

若Q_0'爲與Q_0對應之$\mathfrak{G}'$之元素之一,Q_1'爲與Q_1對應之元素之一,……,以之作傍系

$$(2)\qquad \mathfrak{N}'Q_0',\ \mathfrak{N}'Q_1',\cdots\cdots\mathfrak{N}'Q'_{\mu-1},$$

則得

$$(3)\qquad \mathfrak{G}'=\mathfrak{N}'Q_0'+\mathfrak{N}'Q_1'+\cdots\cdots+\mathfrak{N}'Q'_{\mu-1}$$

蓋由前節定理之系,則(2)之傍系互異.次之,以G'爲$\mathfrak{G}'$之任意元素,而以與是對應之$\mathfrak{G}$之傍系爲$\mathfrak{N}Q_i$,則$G'\sim Q_i$.但$Q_i'\sim Q_i$.故由前定理,G'不得不屬於傍系$\mathfrak{N}'Q_i'$.因之$\mathfrak{G}'$得以(3)表之也.

且於$\mathfrak{G}$及$\mathfrak{G}'$,

$$Q_i\sim Q_i',\quad Q_j\sim Q_j',\quad Q_iQ_j\sim Q_i'Q_j'$$

故由前節之定理,若Q_iQ_j屬於$\mathfrak{N}Q_k$,則$Q_i'Q_j'$不得不爲$\mathfrak{N}'Q_k'$之元素.卽若$Q_iQ_j\equiv Q_k\pmod{\mathfrak{N}}$,則$Q_i'Q_j'\equiv Q_k\pmod{\mathfrak{N}'}$也.因之於二商羣

$$\frac{\mathfrak{G}}{\mathfrak{N}} : Q_0, Q_1, \cdots\cdots, Q_{\mu-1} \pmod{\mathfrak{N}};$$

$$\frac{\mathfrak{G}'}{\mathfrak{N}'} : Q_0', Q_1', \cdots\cdots, Q'_{\mu-1} \pmod{\mathfrak{N}'},$$

對於 $Q_0, Q_1, \cdots\cdots, Q_{\mu-1}$ 而分別使 $Q_0'\ Q_1', \cdots\cdots, Q'_{\mu-1}$ 對應,則兩商之元素間,一一對應成立,且由上述, Q_iQ_j 與 $Q_i'Q_j'$ 對應. 故 $\frac{\mathfrak{G}}{\mathfrak{N}}$ 與 $\frac{\mathfrak{G}'}{\mathfrak{N}'}$ 爲單純同態也.

定理. 令 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之正常約羣, $\mathfrak{N}'$ 爲 $\mathfrak{G}'$ 之正常約羣. 若商 $\mathfrak{G}/\mathfrak{N}$ 及 $\mathfrak{G}'/\mathfrak{N}'$ 爲單純同態,則 $\mathfrak{G}$ 與 $\mathfrak{G}'$ 爲重複同態.

證明. 以

$$\frac{\mathfrak{G}}{\mathfrak{N}} : Q_0, Q_1, \cdots\cdots, Q_{\mu-1} \pmod{\mathfrak{N}},$$

$$\frac{\mathfrak{G}'}{\mathfrak{N}'} : Q_0', Q_1', \cdots\cdots, Q'_{\mu-1} \pmod{\mathfrak{N}'},$$

則

$$\mathfrak{G} = \mathfrak{N}Q_0 + \mathfrak{N}Q_1 + \cdots\cdots + \mathfrak{N}Q_{\mu-1},$$

$$\mathfrak{G}' = \mathfrak{N}'Q_0' + \mathfrak{N}'Q_1' + \cdots\cdots + \mathfrak{N}'Q'_{\mu-1}$$

若由使 Q_i 與 Q_i' 相對應而 $\frac{\mathfrak{G}}{\mathfrak{N}}$ 與 $\frac{\mathfrak{G}'}{\mathfrak{N}'}$ 之同態關係便得成立,則於 $\mathfrak{G}$ 及 $\mathfrak{G}'$, 對於傍系 $\mathfrak{N}Q_i$ 之各元素,使 $\mathfrak{N}'Q_i'$ 之全部元素與之對應; 又對於傍系 $\mathfrak{N}'Q_i'$ 之各元素,使 $\mathfrak{N}Q_i$ 之全部元素與之對應,由是而 $\mathfrak{G}$ 與 $\mathfrak{G}'$ 之重複同態關係亦成立也.

例. 若 $\mathfrak{H}, \mathfrak{K}$ 爲一個羣之約羣,而 $\mathfrak{K}$ 與 $\mathfrak{H}$ 之各元素爲交換可能,則商 $\frac{\mathfrak{H}\mathfrak{K}}{\mathfrak{K}}$ 與 $\frac{\mathfrak{H}}{\mathfrak{Q}}$ 爲單純同態(第41節定理). 故 $\mathfrak{H}\mathfrak{K}$ 與 $\mathfrak{H}$ 爲重複同態.

45. 設兩羣$\mathfrak{G}$, $\mathfrak{G}'$爲同態,而與$\mathfrak{G}$之主元素相對應之$\mathfrak{G}'$之正常約羣爲$\mathfrak{N}'$,與$\mathfrak{G}'$之主元素相對應之$\mathfrak{G}$之正常約羣爲$\mathfrak{N}$. $\mathfrak{N}$, $\mathfrak{N}'$之元數,分別爲n, n'. 於是,由前節之定理,對於$\mathfrak{G}$之元素之各個,乃有$\mathfrak{G}'$之n'個元素(屬於同一傍系者)相對應,而於$\mathfrak{G}'$之元素之各個,則有$\mathfrak{G}$之n個元素與之對應. 此時,此同態名曰 **n−n′ 同態**. 於前節第二定理,若$\mathfrak{N}$, $\mathfrak{N}'$之元數分別爲n, n',則如其證所示,$\mathfrak{G}$與$\mathfrak{G}'$之爲$n-n'$同態明已.

特別當$n'=1$時,即對於$\mathfrak{G}$之各元素,只有$\mathfrak{G}'$之唯一元素與之對應,而對於$\mathfrak{G}'$之元素,其各個皆有$\mathfrak{G}$之n個元素與之對應時,則名曰$\mathfrak{G}$與$\mathfrak{G}'$爲 **n 重同態** 焉.

定理. 若$\mathfrak{G}$與$\mathfrak{G}'$爲n重同態時,而與$\mathfrak{G}'$之主元素對應之$\mathfrak{G}$之正常約羣(元數n)爲$\mathfrak{N}$,則$\mathfrak{G}/\mathfrak{N}$與$\mathfrak{G}'$爲單純同態.

證明. 此乃前節之第一定理中$\mathfrak{N}'$爲主元素羣者而已. 故由同定理則此自明.

定理. 以$\mathfrak{N}$爲$\mathfrak{G}$之正常約羣,而以其元數爲n,若商$\mathfrak{G}/\mathfrak{N}$與羣$\mathfrak{G}'$爲單純同態,則$\mathfrak{G}$與$\mathfrak{G}'$爲$n$重同態.

證明. 於前節第二定理,令$\mathfrak{N}'=1$自明.

系. 若$\mathfrak{N}$爲$\mathfrak{G}$之n元正常約羣* 時,則$\mathfrak{G}$與$\mathfrak{G}/\mathfrak{N}$爲$n$重同態.

定理. 若$\mathfrak{G}$與Γ爲n重同態,$\mathfrak{G}'$又與Γ爲n'重同態時,則$\mathfrak{G}$與$\mathfrak{G}'$爲$n-n'$重同態.

* 元數h之約羣,呼曰h元約羣(第15節).

證明. 以與Γ之主元素相對應之$\mathfrak{G}$之正常約羣爲$\mathfrak{N}$(元數n),而$\mathfrak{G}'$之正常約羣爲$\mathfrak{N}'$(元數n'),則由前二個定理,商$\frac{\mathfrak{G}}{\mathfrak{N}}$及$\frac{\mathfrak{G}'}{\mathfrak{N}'}$皆與$\Gamma$爲單純同態.故兩商爲單純同態.因之由前節第二定理,$\mathfrak{G}$與$\mathfrak{G}'$爲$n-n'$同態.

注意. 兩羣爲同態時,表示其同態關係之對應方法,並不限於一種.如於兩羣$\mathfrak{G}$及$\mathfrak{G}'$,對於$\mathfrak{G}$之元素

$$A, B, C, \cdots\cdots,$$

分別使$\mathfrak{G}$之元素

$$A', B', C', \cdots\cdots$$

與之對應,由是同態之條件(ii)得以滿足;然對於$\mathfrak{G}$之元素$A, B, C, \cdots\cdots$,分別使$\mathfrak{G}'$之元素

$$G'^{-1}A'G',\quad G'^{-1}B'G',\quad G'^{-1}C'G', \cdots\cdots$$

與之對應,其條件(ii)亦得以滿足也.但G'爲$\mathfrak{G}'$之一元素.

次於兩羣

$$\mathfrak{G}:\begin{cases} 1,\ (abc),\ (acb), \\ (bc),\ (ca),\ (ab), \\ (de),\ (abc)(de),\ (acb)(de), \\ (bc)(de),\ (ca)(de),\ (ab)(de), \end{cases};$$

$$\mathfrak{G}':\begin{cases} 1,\ (ABC),\ (ACB), \\ (BC),\ (CA)\ \ (AB) \end{cases}$$

對於$\mathfrak{G}'$之主元素,以$\mathfrak{G}$之正常約羣

$$\mathfrak{N}:\ 1,\ (de)$$

之元素與之對應,而於

$$(ABC),\ (ACB),\ (BC),\ (CA),\ (AB)$$

則分別以傍系

$$\mathfrak{N}(abc),\ \mathfrak{N}(acb),\ \mathfrak{N}(bc),\ \mathfrak{N}(ca),\ \mathfrak{N}(ab)$$

之元素與之對應,則同態之條件(ii)得以滿足,因之$\mathfrak{G}$與$\mathfrak{G}'$爲二重同態也.

又於此兩羣,對於$\mathfrak{G}'$之正常約羣

$$\mathfrak{H}':\quad 1,\quad (ABC),\quad (ACB)$$

之元素,以$\mathfrak{G}$之正常約羣

$$\mathfrak{H}:\begin{cases}1, & (abc), & (acb)\\ (de), & (abc)(de), & (acb)(de)\end{cases}$$

之元素使與對應,而於$\mathfrak{G}'$之傍系$\mathfrak{H}'(AB)$之元素,以$\mathfrak{G}$之傍系$\mathfrak{H}(ab)$之元素對應之,則同態條件(ii)仍能滿足也.故$\mathfrak{G}$與$\mathfrak{G}'$爲6−3同態.

如是,同態之種類,亦未必一定也.

46. 約羣之對應.

定理. 設二羣$\mathfrak{G},\mathfrak{G}'$爲$n-n'$同態,而與$\mathfrak{G}'$之主元素對應之$\mathfrak{G}$之正常約羣爲$\mathfrak{N}$,與$\mathfrak{G}$之主元素對應之$\mathfrak{G}'$之正常約羣爲$\mathfrak{N}'$.於是與含有$\mathfrak{N}$之$\mathfrak{G}$之約羣$\mathfrak{H}$之元素相對應之$\mathfrak{G}'$之元素,形成一含$\mathfrak{N}'$之$\mathfrak{G}'$之約羣$\mathfrak{H}'$.而此$\mathfrak{H}$與$\mathfrak{H}'$爲$n-n'$同態.(此$\mathfrak{H}'$名曰與$\mathfrak{H}$對應之$\mathfrak{G}'$之約羣).

證明 將$\mathfrak{H}$就$\mathfrak{N}$分爲傍系:

$$\mathfrak{H}=\mathfrak{N}S_0+\mathfrak{N}S_1+\cdots\cdots+\mathfrak{N}S_{e-1}.$$

茲以 S_0' 爲對應於 S_0 之 $\mathfrak{G}'$ 之元素之一，S_1' 爲對應於 S_1 之 $\mathfrak{G}'$ 元素之一，……，乃以之作傍系

$$\mathfrak{N}'S_0',\ \mathfrak{N}'S_1',\ \cdots\cdots,\ \mathfrak{N}'S_{e-1}'.$$

於是 $\mathfrak{N}S_i$ 之元素與 $\mathfrak{N}'S_i'$ 之元素對應(第 43 節定理)，且此等傍系，因於 $\mathfrak{G}$ 及 $\mathfrak{G}'$ 爲 $S_i\sim S_i'$，由是與第 44 節第一定理之證明同樣得知其爲互異也.故

$$\mathfrak{H}'=\mathfrak{N}'S_0'+\mathfrak{N}'S_1'+\cdots\cdots+\mathfrak{N}'S_{e-1}'.$$

今取 $\mathfrak{H}'$ 之任意二元素 $N_1'S_i',\ N_2'S_j'$ ($N_1',\ N_2'$ 爲 $\mathfrak{N}'$ 之元素)

$$N_1'S_i'\sim S_i,\ N_2'S_j'\sim S_j,$$

$$\therefore\qquad N_1'S_i'\cdot N_2'S_j'\sim S_iS_j.$$

然 $\mathfrak{H}$ 爲羣.故 S_iS_j 屬於 $\mathfrak{H}$. 故 $N_1'S_i'\cdot N_2'S_j'$ 亦不得不屬於 $\mathfrak{H}'$. 因之 $\mathfrak{H}'$ 爲羣.而其含有 $\mathfrak{N}'$，則甚明也.

次之，於 $\mathfrak{G}$ 及 $\mathfrak{G}'$，以 $N_1,\ N_2$ 爲 $\mathfrak{N}$ 之二元素，$N_1',\ N_2'$ 爲 $\mathfrak{N}'$ 之二元素，則由 $\mathfrak{N}S_i$ 之元素與 $\mathfrak{N}'S_i'$ 之元素對應，乃有

$$N_1S_i\sim N_1'S_i',\ N_2S_j\sim N_2'S_j'.$$

又由同態之條件(ii)，則得

$$N_1S_i\cdot N_2S_j\sim N_1'S_i'\cdot N_2'S_j'.$$

故雖於 $\mathfrak{H}$ 及 $\mathfrak{H}'$，若對於 $\mathfrak{N}S_i$ 之各元素，以 $\mathfrak{N}'S_i'$ 之元素全部與之對應，於 $\mathfrak{N}'S_i'$ 之各元素，以 $\mathfrak{N}S_i$ 之全部元素使與對應之，則同態之條件(ii)亦能滿足也.而於 $\mathfrak{H}$ 之主元素，則 $\mathfrak{H}'$ 之約羣 $\mathfrak{N}'$ 與之對應，於 $\mathfrak{H}'$ 之主元素則 $\mathfrak{H}$ 之約羣 $\mathfrak{N}$ 與之對應.但 $\mathfrak{N},\ \mathfrak{N}'$ 之元

數分別爲 n, n'. 故 $\mathfrak{H}$ 與 $\mathfrak{H}'$ 爲 $n-n'$ 同態.

系 1. 本定理中之 $\mathfrak{H}/\mathfrak{N}$ 與 $\mathfrak{H}'/\mathfrak{N}'$ 爲單純同態.

證明與第 44 節第一定理同樣.

系 2. 在同態之二羣 $\mathfrak{G}$ 及 $\mathfrak{G}'$ 中,若 $\mathfrak{H}'$ 爲與 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$ (含有 $\mathfrak{N}$)對應之 $\mathfrak{G}'$ 之約羣,則 $\mathfrak{H}$ 爲與 $\mathfrak{H}'$ 對應之 $\mathfrak{G}$ 之約羣.因之與相異約羣對應之約羣亦互異.

此則由本定理之證明之內容容易得知.

系 3. 設 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之 n 元正常約羣.則於以 $\mathfrak{G}$ 之約羣 $\mathfrak{N}$ 使與商 $\mathfrak{G}/\mathfrak{N}$ 之主元素對應所生之 $\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{N}$ 之 n 重同態中,對於 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$,乃有 $\mathfrak{G}/\mathfrak{N}$ 之約羣 $\mathfrak{H}/\mathfrak{N}$ 與之對應.

定理. 於前定理,若 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之正常約羣,則 $\mathfrak{H}$ 亦爲 $\mathfrak{G}'$ 之正常約羣而 $\mathfrak{G}/\mathfrak{H}$ 與 $\mathfrak{G}'/\mathfrak{H}'$ 爲單純同態.

證明. 若 G' 爲 $\mathfrak{G}'$ 之任意元素, H' 爲 $\mathfrak{H}'$ 之任意元素, G 爲與 G' 相對應之 $\mathfrak{G}$ 之元素之一, H 爲與 H' 對應之元素之一,則

$$G'^{-1}H'G' \sim G^{-1}HG.$$

但由假設,

$$G^{-1}HG = H_1 \quad (H_1 \text{ 爲 } \mathfrak{H} \text{ 之元素})$$

$$\therefore \quad G'^{-1}H'G' \sim H_1.$$

然與 $\mathfrak{H}$ 之元素對應之 $\mathfrak{G}'$ 之元素乃屬於 $\mathfrak{H}'$. 故 $G'^{-1}H'G'$, 即將 $\mathfrak{H}'$ 之元素以 $\mathfrak{G}'$ 之元素變其形之結果,爲屬於 $\mathfrak{H}'$ 者也.故 $\mathfrak{H}'$ 於 $\mathfrak{G}'$ 爲正常的.

復次,用前定理中之記號,以

(1)　$\mathfrak{S}=\mathfrak{N}S_0+\mathfrak{N}S_1+\cdots\cdots\quad\cdots+\mathfrak{N}S_{e-1}$,

(2)　$\mathfrak{S}'=\mathfrak{N}'S_0'+\mathfrak{N}'S_1'+\cdots\cdots\cdots+\mathfrak{N}'S_{e'-1}$,

而　(3)　$\mathfrak{G}=\mathfrak{S}P_0+\mathfrak{S}P_1+\cdots\cdots\cdots+\mathfrak{S}P_{\nu-1}$,

則

(4)
$$\begin{aligned}\mathfrak{G}=&\mathfrak{N}S_0P_0+\mathfrak{N}S_1P_0+\cdots\cdots+\mathfrak{N}S_{e-1}P_0\\&+\mathfrak{N}S_0P_1+\mathfrak{N}S_1P_1+\cdots\cdots+\mathfrak{N}S_{e-1}P_1\\&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&+\mathfrak{N}S_0P_{\nu-1}+\mathfrak{N}S_1P_{\nu-1}+\cdots\cdots+\mathfrak{N}S_{e-1}P_{\nu-1}.\end{aligned}$$

再以P_0'爲與P_0對應之$\mathfrak{G}'$之元素之一，P_1'爲與P_1對應之$\mathfrak{G}'$之元素之一，……，且以之作傍系

$$\mathfrak{N}'S_0'P_0',\ \mathfrak{N}'S_1'P_0',\cdots\cdots,\mathfrak{N}'S'_{e-1}P'_0,$$
$$\mathfrak{N}'_0S'P_1',\ \mathfrak{N}'S_1'P_1',\cdots\cdots,\mathfrak{N}'S'_{e-1}P'_1,$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{N}'S_0'P'_{\nu-1},\ \mathfrak{N}'S_1'P'_{\nu-1}\cdots\cdots,\mathfrak{N}'S'_{e-1},P'_{\nu-1},$$

則由第43節定理，$\mathfrak{N}'S_i'P_j'$爲與$\mathfrak{N}S_iP_j$之元素對應之傍系，且由同節定理之系，知此諸傍系互異也．故得

(5)
$$\begin{aligned}\mathfrak{G}'=&\mathfrak{N}'S_0'P_0'+\mathfrak{N}'S_1'P_0'+\cdots\cdots+\mathfrak{N}'S'_{e-1}P_0'\\&+\mathfrak{N}'S_0'P_1'+\mathfrak{N}'S_1'P_1'+\cdots\cdots+\mathfrak{N}'S'_{e-1}P_1'\\&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&+\mathfrak{N}'S_0'P'_{\nu-1}+\mathfrak{N}'S_1'P'_{\nu-1}+\cdots+\mathfrak{N}'S'_{e-1}P'_{\nu-1}\end{aligned}$$

因之由(2)，得

(6)　$\mathfrak{G}'=\mathfrak{S}'P_0'+\mathfrak{S}'P_1'+\cdots\cdots+\mathfrak{S}'P'_{\nu-1}$,

今就法$\mathfrak{H}$而取$\mathfrak{G}$,就法$\mathfrak{H}'$而取$\mathfrak{G}'$,則由(3)及(6),得

$$\frac{\mathfrak{G}}{\mathfrak{H}}: \quad P_0, P_1, \cdots\cdots, P_{\nu-1} \pmod{\mathfrak{H}},$$

$$\frac{\mathfrak{G}'}{\mathfrak{H}'}: \quad P_0', P_1', \cdots\cdots, P'_{\nu-1} \pmod{\mathfrak{H}'}.$$

於是,對於$P_0, P_1, \cdots\cdots, P_{\nu-1}$分別使$P_0', P_1', \cdots\cdots, P'_{\nu-1}$與之對應,則兩商之元素之間,便成立一一一對應.而於$\frac{\mathfrak{G}}{\mathfrak{H}}$之二元素之積$P_sP_t$,則有與是各別相應之元素($\frac{\mathfrak{G}'}{\mathfrak{H}'}$的)之積$P_s'P_t'$與之對應,因之兩商爲單純同態.

蓋於兩羣$\mathfrak{G}, \mathfrak{G}'$中,因

$$S_i \sim S_i', \quad P_s \sim P_s', \quad S_iP_s \sim S_i'P_s',$$

故傍系$\mathfrak{N}S_iP_s$之元素與傍系$\mathfrak{N}'S_i'P_s'$之元素對應.以故若

$$P_sP_t = NS_j \cdot P_u' \quad (N \text{ 爲 } \mathfrak{N} \text{ 之元素}),$$

則由同態之條件(ii),

$$P_s'P_t' = N'S_j'P_u \quad (N' \text{ 爲 } \mathfrak{N}' \text{ 之元素}).$$

但
$$NS_j \equiv 1, \pmod{\mathfrak{H}}, \quad N'S_j' \equiv 1 \pmod{\mathfrak{H}'}$$

故若$P_sP_t \equiv P_u \pmod{\mathfrak{H}}$,則$P_s'P_t' \equiv P_u' \pmod{\mathfrak{H}'}$因之於兩商$\frac{\mathfrak{G}}{\mathfrak{H}}$, $\frac{\mathfrak{G}'}{\mathfrak{H}'}$中,$P_sP_t$與$P_s'P_t'$相對應也.

系1. 二羣$\mathfrak{G}$及$\mathfrak{G}'$爲單純同態時,若其一爲單羣,則其他亦然.

系2. 設$\mathfrak{H}, \mathfrak{N}$爲羣$\mathfrak{G}$之正常約羣,而$\mathfrak{H}$則包含$\mathfrak{N}$.於是$\frac{\mathfrak{G}/\mathfrak{N}}{\mathfrak{H}/\mathfrak{N}}$與$\mathfrak{G}/\mathfrak{H}$爲單純同態.

證明. 以$\mathfrak{N}$之元數爲n, 且以$\mathfrak{G}$之約羣$\mathfrak{N}$使與$\frac{\mathfrak{G}}{\mathfrak{N}}$之主元素相對應,則$\mathfrak{G}$與$\frac{\mathfrak{G}}{\mathfrak{N}}$爲$n$重同態,而於$\mathfrak{G}$之約羣$\mathfrak{H}$, 則有$\frac{\mathfrak{G}}{\mathfrak{N}}$之約羣$\frac{\mathfrak{H}}{\mathfrak{N}}$與之對應(第一定理系).然$\mathfrak{H}$於$\mathfrak{G}$爲正常,故由本定理,$\frac{\mathfrak{G}}{\mathfrak{H}}$與$\frac{\frac{\mathfrak{G}}{\mathfrak{N}}}{\frac{\mathfrak{H}}{\mathfrak{N}}}$爲單純同態也.

此系若如次思之,則更爲明瞭.

於羣$\mathfrak{G}$, 將屬於$\mathfrak{N}$之元素置之與主元素等,其所生之羣爲$\frac{\mathfrak{G}}{\mathfrak{N}}$;而於此諸元素中,屬於$\mathfrak{H}$者之集合爲$\frac{\mathfrak{H}}{\mathfrak{N}}$.再將相等定義變更,將$\frac{\mathfrak{H}}{\mathfrak{N}}$之元素令等於主元素,則其結果,最初屬於$\mathfrak{H}$之元素,皆與主素等也.故二回變更之結果,$\mathfrak{H}$之元素,與直置之與主元素等者同一.故

$$\frac{\frac{\mathfrak{G}}{\mathfrak{N}}}{\frac{\mathfrak{H}}{\mathfrak{N}}}=\frac{\mathfrak{G}}{\mathfrak{H}}.$$

本節之事項,可約言之如次:

二羣$\mathfrak{G}$及$\mathfrak{G}'$爲$n-n'$同態時,若以與$\mathfrak{G}$之主元素相對應之$\mathfrak{G}'$之正常約羣爲$\mathfrak{N}'$(元數n'), 與$\mathfrak{G}'$之主元素對應之$\mathfrak{G}$之正常約羣爲$\mathfrak{N}$(元數n),則含$\mathfrak{N}$之$\mathfrak{G}$之約羣與含$\mathfrak{N}'$之$\mathfrak{G}'$之約羣間,便成立一一一對應,而對應約羣爲$n-n'$同態也.於是$\mathfrak{N}$與$\mathfrak{N}'$之相對應明已.又若$\mathfrak{G}$之約羣$\mathfrak{H}$爲正常,則其對應約

羣 $\mathfrak{H}'$ 亦爲正常,且 $\frac{\mathfrak{G}}{\mathfrak{H}}$ 與 $\frac{\mathfrak{G}'}{\mathfrak{H}'}$ 爲單純同態.

此外,則於本節及前節之定理,若令 $\mathfrak{N}'$ 爲主元素羣,卽 $n'=1$,則得 $\mathfrak{G}$ 與 $\mathfrak{G}'$ 爲 n 重同態時之定理焉.此時 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$ 之元數,爲其對應約羣 $\mathfrak{H}'$ 之元數之 n 倍.

注意. 於第二定理,若以 $\mathfrak{H}$ 及 $\mathfrak{H}'$ 之元數分別爲 h 及 h',則由 $\frac{\mathfrak{G}}{\mathfrak{H}}$ 與 $\frac{\mathfrak{G}'}{\mathfrak{H}'}$ 之爲單純同態,$\mathfrak{G}$ 與 $\mathfrak{G}'$ 又爲 $h-h'$ 同態也.(參照第45節注意)

47. 關於素數冪元數羣之定理

定理. 以素數冪 p^m 爲元數之羣,乃有元數 $p^s\ (s<m)$ 之正常約羣.

證明. 以 $\mathfrak{G}$ 爲 p^m 元羣.由第31節之定理,則 $\mathfrak{G}$ 除主元素以外,含有自己共軛元素.今以其一爲A,則 A 之巡回率爲 p^α $(0<\alpha\leqq m)$.便宜上令 $P=A^{p^{\alpha-1}}$,則巡回羣$\{P\}$之爲 p 元正常約羣明已.

復次作商 $\frac{\mathfrak{G}}{\{P\}}$,則其元數爲 p^{m-1}. 故與前同樣,知其含有 p 元正常約羣.以其一爲 Γ. 又他方面言,$\mathfrak{G}$ 與 $\frac{\mathfrak{G}}{\{P\}}$ 爲 p 重同態(第45節第二定理系). 故與 $\frac{\mathfrak{G}}{\{P\}}$ 之正常約羣 Γ 相對應之正常約羣 $\mathfrak{N}$ 存在於 $\mathfrak{G}$ 之內,而 $\mathfrak{N}$ 之元數爲 p^2 也(前節)

更作商 $\frac{\mathfrak{G}}{\mathfrak{N}}$,乃取與此之 p 元正常約羣相對應之 $\mathfrak{G}$ 之正常約羣 $\mathfrak{N}'$,則此之元數爲 p^3 也.再作商 $\frac{\mathfrak{G}}{\mathfrak{N}'}$,以同樣之法反覆之,

遂得到 p^s 元之正常約羣($\mathfrak{G}$的)焉.

定理. 令 $\mathfrak{H}$ 爲 p^m 元羣 $\mathfrak{G}$ 之約羣,而以 p^s 爲其元數. 於是以此 $\mathfrak{H}$ 爲正常約羣,而元數爲 p^{s+t} $(t\geqq 1)$ 之羣,定存在於 $\mathfrak{G}$ 之約羣中.

證明. 以 $\mathfrak{L}_1$ 爲 $\mathfrak{G}$ 之自己共軛元素(所有的)所作之羣,而以其元數爲 p^{n_1}. $\mathfrak{L}_1$ 與 $\mathfrak{G}$ 不一致時,取其商 $\mathfrak{G}/\mathfrak{L}_1$,而以此之自己共軛元素所作之羣爲 Γ_2. 因 $\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{L}_1$ 爲 p^{n_1} 重同態之故,則與 $\mathfrak{G}/\mathfrak{L}_1$ 之正常約羣 Γ_2 相對應之正常約羣 $\mathfrak{L}_2$ 定存在於 $\mathfrak{G}$.* 以 $\mathfrak{L}_2$ 之元數爲 p^{n_2}. 若 $\mathfrak{L}_2$ 與 $\mathfrak{G}$ 復不一致,再取商 $\mathfrak{G}/\mathfrak{L}_2$,而以與此之自己共軛元數所作之羣 Γ_3 相對應之 $\mathfrak{G}$ 之約羣爲 $\mathfrak{L}_3$,而以 $\mathfrak{L}_3$ 之元數爲 p^{n_3}. 若 $\mathfrak{L}_3$ 仍不與 $\mathfrak{G}$ 一致,更取商 $\mathfrak{G}/\mathfrak{L}_3$ 而以同法反覆行之,則得 $\mathfrak{G}$ 之正常約羣列

$$(1) \qquad \mathfrak{L}_1,\ \mathfrak{L}_2,\ \cdots\cdots,\ \mathfrak{L}_r,\ \mathfrak{G}.$$

於是 $\mathfrak{L}_{i+1}/\mathfrak{L}_i$ 者,乃 $\mathfrak{G}/\mathfrak{L}_i$ 中自己共軛元素所作之羣也.

且於羣列(1)將其項自左至右順次而檢點之,觀其有含於約羣 $\mathfrak{H}$ 者與否,若 $\mathfrak{L}_{i+1}$ 爲不含於 $\mathfrak{H}$ 者之最初一個,乃作其積 $\mathfrak{H}\mathfrak{L}_{i+1}$. 於是以 $\mathfrak{L}_{i+1}$ 於 $\mathfrak{G}$ 爲正常之故,$\mathfrak{H}\mathfrak{L}_{i+1}$ 遂成羣焉,而其元數則爲 p^{s+t} $(t\geqq 1)$.

---

* 由第46節第一定理系3, $\Gamma_2=\mathfrak{L}_2/\mathfrak{L}_1$.

自他面言，$\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{Q}_i$ 爲 p^{n_i} 重同態，而於 $\mathfrak{G}$ 之約羣 $\mathfrak{H}$，$\mathfrak{Q}_{i+l}$，分別有 $\mathfrak{G}/\mathfrak{Q}_i$ 之約羣 $\mathfrak{H}/\mathfrak{Q}_i$，$\mathfrak{Q}_{i+l}/\mathfrak{Q}_i$ 與之對應(第 46 節第一定理系 3). 因之 $\frac{\mathfrak{H}}{\mathfrak{Q}_i}\cdot\frac{\mathfrak{Q}_{i+l}}{\mathfrak{Q}_i}$ 與 $\mathfrak{H}\mathfrak{Q}_{i+l}$ 對應也. 但 $\frac{\mathfrak{Q}_{i+l}}{\mathfrak{Q}_i}$ 乃由 $\frac{\mathfrak{G}}{\mathfrak{Q}_i}$ 中自己共軛元素而成. 故 $\frac{\mathfrak{Q}_{i+l}}{\mathfrak{Q}_i}$ 之各元素與 $\frac{\mathfrak{H}}{\mathfrak{Q}_i}$ 爲交換可能，因之 $\frac{\mathfrak{H}}{\mathfrak{Q}_i}$ 於 $\frac{\mathfrak{H}}{\mathfrak{Q}_i}\cdot\frac{\mathfrak{Q}_{i+1}}{\mathfrak{Q}_i}$ 爲正常也. 故 $\mathfrak{H}$ 於 $\mathfrak{H}\mathfrak{Q}_{i+l}$ 爲正常. 而後者之元數，如上所記，爲 p^{s+t} $(t\geqq 1)$.

系 1. 於 p^m 元羣中，其 p^{m-1} 元約羣皆正常的.

系 2. 於 p^m 元羣中，其 p^s 元約羣，含於 p^{s+1} 元約羣之內.

證明. 以 $\mathfrak{H}$ 爲 p^s 元約羣，以 $\mathfrak{N}$ 爲 $\mathfrak{H}$ 之正常化羣(參照第 33 節). 於是由上定理，$\mathfrak{N}$ 之元數爲 p^{s+u} $(u\geqq 1)$. 於 $\mathfrak{N}$，以其不屬於 $\mathfrak{H}$ 之元素之一爲 K，以 K 之關於 $\mathfrak{H}$ 之相對巡回率爲 p^κ. $\kappa=1$ 時，令 $\mathrm{T}=\mathrm{K}$，$\kappa>1$ 時，令 $\mathrm{T}=\mathrm{K}^{p^{\kappa-1}}$，則 T 關於 $\mathfrak{H}$，乃有相對巡回率 p. 但 T 屬於 $\mathfrak{N}$，故與 $\mathfrak{H}$ 爲交換可能. 因之

$$\mathfrak{H}+\mathfrak{H}\,\mathrm{T}+\mathfrak{H}\,\mathrm{T}^2+\cdots\cdots+\mathfrak{H}\,\mathrm{T}^{p-1},$$

作成一元數 p^{s+1} 之羣也.

定理. 於 p^m 元羣，其 p 元正常約羣乃由自己共軛元素而成.

證明. 以 $\mathfrak{G}$ 爲 p^m 元羣，$\mathfrak{P}$ 爲其 p 元正常約羣. 又 A 爲

$\mathfrak{G}$之任意元素，p^{α}爲其巡回率，乃作巡回羣$\{A\}$. $\mathfrak{P}$若含於$\{A\}$，則$\mathfrak{P}$之各元素與A爲交換可能，明已.

反之，$\mathfrak{P}$若不含於$\{A\}$，則兩羣除主元素外，不得有共通之元素. 但由假設，$\mathfrak{P}$於$\mathfrak{G}$爲正常. 故兩羣之積$\mathfrak{P}\{A\}$爲羣，而其元數爲$p^{\alpha+1}$也(第27節第三定理系). 然由前定理系，$\{A\}$乃此羣之正常約羣. 故$\{A\}$與$\mathfrak{P}$之各元素爲交換可能. 如是，於$\mathfrak{P}$及$\{A\}$，其各個乃與其他之各元素爲交換可能，且其共通元素僅爲主元素. 故$\mathfrak{P}$之各元素與A爲交換可能也(第27節第四定理).

第七章　組成羣列

48. 極大正常約羣.

設$\mathfrak{M}$爲羣$\mathfrak{G}$之正常約羣. 若除$\mathfrak{M}$及$\mathfrak{G}$以外，含$\mathfrak{M}$之正常約羣不存在於$\mathfrak{G}$時，則$\mathfrak{M}$曰$\mathfrak{G}$之**極大正常約羣**. 特別若主元素羣爲極大，則此羣之爲單純的明已.

於此有須注意者，此之所謂極大者，非正常約羣中元數最大者之謂，因之一羣中得有二以上之極大正常約羣存在，且其元數不一致者，常有之焉.

如於羣

$$\mathfrak{G}:\begin{cases} 1, & (abc), & (acb), \\ (bc), & (ca), & (ab), \\ (def), & (abc)(def), & (acb)(def), \\ (bc)(def), & (ca)(def), & (ab)(def), \\ (dfe), & (abc)(dfe), & (acb)(dfe), \\ (bc)(dfe), & (ca)(dfe), & (ab)(dfe), \end{cases}$$

下記之兩正常約羣共爲極大，其元數，一爲 6 一爲 9 也

$$\mathfrak{H}:\begin{cases} 1, & (abc), & (acb), \\ (bc), & (ca), & (ab), \end{cases}$$

$$\mathfrak{K}:\begin{cases} 1, & (abc), & (acb), \\ (def), & (abc)(def), & (acb)(def), \\ (dfe), & (abc)(dfe), & (acb)(dfe). \end{cases}$$

定理. 設$\mathfrak{M}$爲羣$\mathfrak{G}$之正常約羣. 若$\mathfrak{M}$爲極大，則$\mathfrak{G}/\mathfrak{M}$爲單羣；反之，若$\mathfrak{G}/\mathfrak{M}$爲單羣，則$\mathfrak{M}$爲極大.

證明. 若$\mathfrak{M}$之元數爲m，則$\mathfrak{G}$與$\mathfrak{G}/\mathfrak{M}$爲$m$重同態(第45節定理系). 若$\mathfrak{G}/\mathfrak{M}$除主元素羣外，含有正常眞約羣$\Gamma$，則與$\Gamma$對應之$\mathfrak{G}$之約羣，乃含$\mathfrak{M}$而爲與$\mathfrak{M}$及$\mathfrak{G}$異之正常約羣也(第46節). 因之$\mathfrak{M}$便不爲極大. 故若$\mathfrak{M}$爲極大，則$\mathfrak{G}/\mathfrak{M}$爲單羣

其次$\mathfrak{M}$若不爲極大時，則由極大正常約羣之定義，其含此且與$\mathfrak{G}$及$\mathfrak{M}$異之正常約羣$\mathfrak{H}$定存在於$\mathfrak{G}$. 而與是對

應之 $\mathfrak{G}/\mathfrak{M}$ 之約羣，則與前同樣，知爲異於 1 之正常眞約羣也．因之 $\mathfrak{G}/\mathfrak{M}$ 爲複合的．故 $\mathfrak{G}/\mathfrak{M}$ 如爲單羣，則 $\mathfrak{M}$ 爲極大．

注意．上之證明，乃使對於 $\mathfrak{G}/\mathfrak{M}$ 之主元素，以 $\mathfrak{G}$ 中 $\mathfrak{M}$ 之元素與之對應而行之者也．

定理．若 $\mathfrak{H}$，$\mathfrak{K}$ 爲羣 $\mathfrak{G}$ 之兩個極大正常約羣，$\mathfrak{L}$ 爲 $\mathfrak{H}$，$\mathfrak{K}$ 之最大公約羣，則

(i) $\mathfrak{H}\,\mathfrak{K}=\mathfrak{G}$.

(ii) $\mathfrak{H}/\mathfrak{L}$ 與 $\mathfrak{G}/\mathfrak{K}$，以及 $\mathfrak{K}/\mathfrak{L}$ 與 $\mathfrak{G}/\mathfrak{H}$ 皆爲單純同態．

(iii) $\mathfrak{L}$ 爲 $\mathfrak{H}$ 之極大正常約羣，又爲 $\mathfrak{K}$ 之極大正常約羣．

證明 (i) 令 $\mathfrak{H}$，$\mathfrak{K}$，$\mathfrak{L}$ 之元數分別爲 h，k，l，因 $\mathfrak{K}$ 爲 $\mathfrak{G}$ 之正常約羣，故 $\mathfrak{K}$ 與 $\mathfrak{H}$ 之各元素爲交換可能，明已．故 $\mathfrak{H}\,\mathfrak{K}$ 爲 $\mathfrak{G}$ 之約羣，其元數爲 $\frac{h\,k}{l}$ $(>h,\ k)$ (第 27 節第三定理系)．而 $\mathfrak{H}$，$\mathfrak{K}$ 共爲正常，故其積 $\mathfrak{H}\,\mathfrak{K}$ 亦於 $\mathfrak{G}$ 爲正常也．然 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之極大正常約羣，故羣 $\mathfrak{H}\,\mathfrak{K}$ 不得不與 $\mathfrak{G}$ 一致．

(ii) 因 $\mathfrak{K}$ 與 $\mathfrak{H}$ 之各元素爲交換可能，故 $\mathfrak{L}$ 爲 $\mathfrak{H}$ 之正常約羣，且 $\mathfrak{H}/\mathfrak{L}$ 與 $\mathfrak{H}\mathfrak{K}/\mathfrak{K}$ $(=\mathfrak{G}/\mathfrak{K})$ 爲單純同態 (第 41 節定理)．

同樣，$\mathfrak{K}/\mathfrak{L}$ 與 $\mathfrak{G}/\mathfrak{H}$ 亦單純同態．

(iii) $\mathfrak{K}$ 既爲 $\mathfrak{G}$ 之極大正常約羣，故由前定理，$\mathfrak{G}/\mathfrak{K}$ 爲單羣也．因之與是同態之 $\mathfrak{H}/\mathfrak{L}$ 亦爲單純 (第 46 節第二定理系)．於是由前定理 $\mathfrak{L}$ 爲 $\mathfrak{H}$ 之極大正常約羣．

同樣，$\mathfrak{L}$ 又於 $\mathfrak{R}$ 亦極大正常.

例. 本節開端所揭之羣中，$\mathfrak{H}$ 及 $\mathfrak{R}$ 之共通置換爲 1, (abc), (acb), 此諸置換卽造成 $\mathfrak{H}$ 及 $\mathfrak{R}$ 之極大正常約羣. 若以 $\mathfrak{L}$ 表之，則得

$$\mathfrak{R}=\mathfrak{L}+\mathfrak{L}(def)+\mathfrak{L}(dfe)$$

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}(def)+\mathfrak{H}(dfe).$$

由是則有

$$\mathfrak{R}/\mathfrak{L}:\quad 1,\quad (def),\quad (dfe)\quad (\mathrm{mod}.\ \mathfrak{L}),$$

$$\mathfrak{G}/\mathfrak{H}:\quad 1,\quad (def),\quad (dfe)\quad (\mathrm{mod}.\ \mathfrak{H}).$$

此兩商之爲單純同態，明也.

49. 組成列.

$\mathfrak{G}$ 爲一羣. $\mathfrak{G}$ 之極大正常約羣之一爲 $\mathfrak{G}_1$, $\mathfrak{G}_1$ 之極大正常約羣之一爲 $\mathfrak{G}_2$, 順次如斯以進之，以 $\mathfrak{G}$ 之元數爲有限之故，遂達到單羣 $\mathfrak{G}_{\nu-1}$, 此之極大正常約羣卽主元素羣 1 也. 如是所得之羣列

$$(1)\qquad \mathfrak{G},\quad \mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_{\nu-1},\quad 1,$$

名曰 $\mathfrak{G}$ 之**組成羣列**，或曰**組成列**. 而由此所得之商羣之列.

$$(2)\qquad \frac{\mathfrak{G}}{\mathfrak{G}_1},\ \frac{\mathfrak{G}_1}{\mathfrak{G}_2};\ \cdots\cdots,\ \frac{\mathfrak{G}_{\nu-1}}{1}\quad \left(\frac{\mathfrak{G}_{\nu-1}}{1}=\mathfrak{G}_{\nu-1}\right)$$

名曰由組成列 (1) 所導出之**商羣列**. 此中 $\mathfrak{G}_i$ 既爲 $\mathfrak{G}_{i-1}$ 之極大正常約羣，故商 $\mathfrak{G}_{i-1}/\mathfrak{G}_i$ 爲單羣 (第 48 節定理). 因之商羣列之各項，皆單羣也.

次以(1)之各羣之元數分別爲

$$g,\quad g_1,\quad g_2,\quad \cdots\cdots\quad g_{\nu-1},\quad 1,$$

則商羣列(2)之各項之元數分別爲

$$(3)\qquad \frac{g}{g_1},\quad \frac{g_1}{g_2},\quad \cdots\cdots,\quad \frac{g_{\nu-1}}{1}.$$

而 $\frac{g_{i-1}}{g_i}$ 則爲 $\mathfrak{G}_i$ 於 $\mathfrak{G}_{i-1}$ 中之指數. 此之(3)名曰 $\mathfrak{G}$ 之指數列.

特別, 指數列爲僅由素數而成者時, 則羣 $\mathfrak{G}$ 曰可解的. 此時商羣列之項, 皆爲素數元數之巡回羣也. 如元數爲素數之冪之羣, 則由第47節第一定理易知其爲可解的是.

例 1. 四次對稱羣之組成列.

以 $\mathfrak{S}$ 爲四次對稱羣(第11節例2), $\mathfrak{A}$ 爲四次交代羣(第12節例2), $\mathfrak{B}$ 爲第34節所示之 $\mathfrak{A}$ 之正常約羣

$$1,\quad (ab)(cd),\quad (ac)(bd),\quad (ad)(bc),$$

$\mathfrak{W}$ 爲 $\mathfrak{B}$ 之正常約羣

$$1,\quad (ab)(cd).$$

於是

$$\mathfrak{S},\quad \mathfrak{A},\quad \mathfrak{B},\quad \mathfrak{W},\quad 1$$

爲對稱羣 $\mathfrak{S}$ 之組成列. 而其商羣列爲

$$\frac{\mathfrak{S}}{\mathfrak{A}},\quad \frac{\mathfrak{A}}{\mathfrak{B}},\quad \frac{\mathfrak{B}}{\mathfrak{W}},\quad \frac{\mathfrak{W}}{1},$$

但

$$\frac{\mathfrak{S}}{\mathfrak{A}}:\quad 1,\quad (ab)\quad (\mathrm{mod.}\ \mathfrak{A}),$$

$$\frac{\mathfrak{A}}{\mathfrak{B}}:\quad 1,\quad (bcd),\quad (bdc)\quad (\mathrm{mod}\ \mathfrak{B}),$$

$$\frac{\mathfrak{B}}{\mathfrak{W}}: \quad 1, \ (ac)(bd) \pmod{\mathfrak{W}},$$

$$\frac{\mathfrak{W}}{1}: \quad 1, \ (ab)(cd), \qquad \text{(參照第 24 節例)}.$$

而指數列則爲

$$2, \ 3, \ 2, \ 2.$$

此指數列既僅由素數而成，故四次對稱羣爲可解的. 至於商羣列各項之爲素數元數巡回羣，亦如上得知之，明也.

例 2. 試取前節例中所示之羣 $\mathfrak{G}$，則如此所述，$\mathfrak{H}$ 爲其極大正常約羣也. 今以 $\mathfrak{L}$ 爲

$$1, \ (abc), \ (acb),$$

則此爲 $\mathfrak{H}$ 之極大正常約羣，且爲單羣. 故

$$\mathfrak{G}, \ \mathfrak{H}, \ \mathfrak{L}, \ 1$$

爲 $\mathfrak{G}$ 之組成羣列. 而其指數列則爲

$$3, \ 2, \ 3.$$

又取 $\mathfrak{G}$ 之極大正常約羣 $\mathfrak{K}$，則 $\mathfrak{L}$ 復爲此之極大正常約羣. 故

$$\mathfrak{G}, \ \mathfrak{K}, \ \mathfrak{L}, \ 1$$

亦 $\mathfrak{G}$ 之組成列也. 又或代 $\mathfrak{L}$ 而取

$$\mathfrak{K}': \ 1, \ (def), \ (dfe),$$

以此爲 $\mathfrak{K}$ 之極大正常約羣，故

$$\mathfrak{G},\quad \mathfrak{R},\quad \mathfrak{R}',\quad 1$$

亦爲$\mathfrak{G}$之組成列. 而對後二者, 指數列皆爲

$$2,\quad 3,\quad 3.$$

故此羣亦與前例同爲可解的也.

如本例之所示, 一羣之組成列不限於唯一也. 當組成列有二以上時, 其間有不變之關係在. 次節之定理, 所以示此者也.

50. Hölder 氏定理. 一羣之商羣列, 不問其組成列之選擇方法如何, 常爲一定. 但商羣列中各項之順序, 則在所不論.

證明之先, 請將定理之意義說明之. 今以$\mathfrak{G}$爲一羣, 以

$$(1)\qquad \mathfrak{G},\quad \mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_{\nu-1},\quad 1,$$

$$(2)\qquad \mathfrak{G}',\quad \mathfrak{G}_1',\quad \mathfrak{G}_2',\quad \cdots\cdots,\quad \mathfrak{G}'_{\mu-1},\quad 1$$

爲其任意二個組成列, 則由各個中所導出之商羣列

$$(3)\qquad \frac{\mathfrak{G}}{\mathfrak{G}_1},\quad \frac{\mathfrak{G}_1}{\mathfrak{G}_2},\quad \cdots\cdots,\quad \frac{\mathfrak{G}_{\nu-1}}{1},$$

$$(4)\qquad \frac{\mathfrak{G}}{\mathfrak{G}_1'},\quad \frac{\mathfrak{G}_1'}{\mathfrak{G}_2'},\quad \cdots\cdots,\quad \frac{\mathfrak{G}'_{\mu-1}}{1}$$

之爲一致, 乃定理之所主張者也. 此之所謂一致者, 乃謂與(3)之一項爲單純同態者, 必存在於(4)之中; 反之, 與(4)之一項爲單純同態者, 亦必存在於(3)之內; 且於(3)與其一項爲單純同態者之個數(該項亦包含在內), 與於(4)與之單純同態者之個數相等之意. 換言之, 兩商羣列之項數

相等而復互爲單純同態者，得以使之成一一對應，是卽定理之所主張也.

證明.* 以數學的歸納法行之.

1°. 以(1),(2)爲羣$\mathfrak{G}$之任意二組成列，而$\mu \geqq \nu$. 在此兩組成列中，一方之項數不超過ν時，則假定由此所導出之兩商羣列爲一致；再於此假定下，以示由其一方爲$\nu+1$項所成之兩組成列(1)及(2)所導出之商羣列(3)及(4)亦爲一致也.

(i) $\mathfrak{G}_1' = \mathfrak{G}_1$ 時.

(1),(2)中各省去$\mathfrak{G}$而得之二羣列

$$\mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_{\nu-1},\quad 1$$

$$\mathfrak{G}_1',\quad \mathfrak{G}_2',\quad \cdots\cdots,\quad \mathfrak{G}'_{\mu-1},\quad 1 \qquad (\mathfrak{G}_1' = \mathfrak{G}_1),$$

共爲$\mathfrak{G}_1$之組成列，而前者之項數爲ν. 故依假定，其由此所導出之二商羣列

$$\frac{\mathfrak{G}_1}{\mathfrak{G}_2},\quad \frac{\mathfrak{G}_2}{\mathfrak{G}_3},\quad \cdots\cdots,\quad \frac{\mathfrak{G}_{\nu-1}}{1},$$

$$\frac{\mathfrak{G}_1'}{\mathfrak{G}_2'},\quad \frac{\mathfrak{G}_2'}{\mathfrak{G}_3'},\quad \cdots\cdots,\quad \frac{\mathfrak{G}'_{\mu-1}}{1}$$

爲一致. 因之，兩者之前分別附加一相等之$\mathfrak{G}/\mathfrak{G}_1$及$\mathfrak{G}/\mathfrak{G}_1'$所得之(3)及(4)當然一致也.

---

*此證明與 Hölder 氏之方法異，乃在雖對無限羣以及其他皆得應用之方針之下所爲者也.

(ii)　$\mathfrak{G}_1 \neq \mathfrak{G}_1'$ 時.

$\mathfrak{G}_1$, $\mathfrak{G}_1'$ 之最大公約羣若爲 $\mathfrak{L}$, 則 $\mathfrak{L}$ 爲 $\mathfrak{G}_1$ 及 $\mathfrak{G}_1'$ 之極大正常約羣(第48節第二定理). 於是取 $\mathfrak{L}$ 之組成列

$$\mathfrak{L},\ \mathfrak{M},\ \mathfrak{N},\ \cdots\cdots,$$

則二羣列

(5)　$\mathfrak{G},\ \mathfrak{G}_1,\ \mathfrak{L},\ \mathfrak{M},\ \mathfrak{N},\ \cdots\cdots,$

(6)　$\mathfrak{G},\ \mathfrak{G}_1',\ \mathfrak{L},\ \mathfrak{M},\ \mathfrak{N},\ \cdots\cdots$

皆爲 $\mathfrak{G}$ 之組成列甚明. 由之以導出商羣列, 則得

(7)　$\dfrac{\mathfrak{G}}{\mathfrak{G}_1},\ \dfrac{\mathfrak{G}_1}{\mathfrak{L}},\ \dfrac{\mathfrak{L}}{\mathfrak{M}},\ \dfrac{\mathfrak{M}}{\mathfrak{N}},\ \cdots\cdots,$

(8)　$\dfrac{\mathfrak{G}}{\mathfrak{G}_1'},\ \dfrac{\mathfrak{G}_1'}{\mathfrak{L}},\ \dfrac{\mathfrak{L}}{\mathfrak{M}},\ \dfrac{\mathfrak{M}}{\mathfrak{N}},\ \cdots\cdots.$

且就 $\mathfrak{G}$ 之二組成列(1)及(5)而觀, 其第二項共爲 $\mathfrak{G}_1$ 也. 故與於(i)中者同樣, 由各個所導出之商羣列(3)及(7)爲一致. 因之羣列(5)及(6)皆由 $\nu+1$ 項而成. 又於(2)及(6), 其第二項爲同一, 而(6)之項數爲 $\nu+1$. 故由此各個所導出之商羣列(4)及(8), 亦與前同樣爲一致也.

復次, 試取(7), (8)而比較之, 因 $\mathfrak{L}$ 爲 $\mathfrak{G}$ 之兩極大正常約羣 $\mathfrak{G}_1$ 及 $\mathfrak{G}_1'$ 之最大公約羣, 故由第48節第二定理, $\mathfrak{G}/\mathfrak{G}_1$ 與 $\mathfrak{G}_1'/\mathfrak{L}$ 以及 $\mathfrak{G}/\mathfrak{G}_1'$ 與 $\mathfrak{G}_1/\mathfrak{L}$ 皆單純同態. 而第三項以下復同一. 故商羣列(7)及(8)一致也.

但如上所述. 商羣列(3)與(7)一致, (4)與(8)一致矣. 故由組成列(1)及(2)所導出之商羣列(3)及(4)爲一致也.

2'. 組成列,當其項數爲2時,爲

$$\mathfrak{G},\quad 1,$$

是只能得唯一個.故若兩組成列之一由三項而成時,使能示本定理爲眞,則由此而歸納法可完成,定理之一般得成立可知也. 今以

(9) $\mathfrak{G},\quad \mathfrak{G}_1,\quad 1,$

(10) $\mathfrak{G},\quad \mathfrak{G}_1',\quad \mathfrak{G}_2',\quad \cdots\cdots$

爲二組成列.若 $\mathfrak{G}_1$ 與 $\mathfrak{G}_1'$ 爲同一,則以 $\mathfrak{G}_1$ 爲單純之故,(10)與(9)不得不同一也.

若 $\mathfrak{G}_1$ 與 $\mathfrak{G}_1'$ 互異,則兩者之最大公約羣 $\mathfrak{L}$ 爲 $\mathfrak{G}_1$ 之極大正常約羣(第48節第二定理).但 $\mathfrak{G}_1$ 爲單羣.故 $\mathfrak{L}=1$ 爲必要也.又自他面言,$\mathfrak{L}$ 乃 $\mathfrak{G}_1'$ 之極大正常約羣.而 $\mathfrak{L}=1$. 故 $\mathfrak{G}_1'$ 亦非爲單羣不可.因之組成列(10)遂爲

(11) $\mathfrak{G},\quad \mathfrak{G}_1',\quad 1,$

而由(9)及(11)以作商羣列,則得

(12) $\dfrac{\mathfrak{G}}{\mathfrak{G}_1},\quad \dfrac{\mathfrak{G}_1}{1},$

(13) $\dfrac{\mathfrak{G}}{\mathfrak{G}_1'},\quad \dfrac{\mathfrak{G}_1'}{1}.$

然 $\mathfrak{G}$, 及 $\mathfrak{G}_1'$ 之最大公約羣爲1,故由第48節第二定理,$\mathfrak{G}/\mathfrak{G}_1$ 與 $\mathfrak{G}_1'/1$,以及 $\mathfrak{G}/\mathfrak{G}_1'$ 與 $\mathfrak{G}_1/1$ 爲單純同態. 於是在兩組成列中,若一方由三項而成時,則由兩者所導出之商羣列一致也.

系. 一羣之指數列,不問組成列之選擇方法如何,常爲一定. (Jordan 氏之定理.)

證明. 指數列者,不外在商羣列中,僅將其各項之元數而討論之者而已. 但商羣列一定,故指數列亦一定也.

51. 主組成列.

羣 $\mathfrak{G}$ 之正常約羣列

$$(1)\qquad \mathfrak{G},\ \mathfrak{H}_1,\ \mathfrak{H}_2,\ \cdots\cdots,\ \mathfrak{H}_{\mu-1},\ 1,$$

若適合次之二條件時,則名曰 $\mathfrak{G}$ 之**主組成羣列**,或曰**主組成列**.

(i) 各羣均含於其先一羣內.

(ii) 含於一項 $\mathfrak{H}_{i-1}$ 而又含其次項 $\mathfrak{H}_i$ 之正常約羣 ($\mathfrak{G}$ 的),除 $\mathfrak{H}_{i-1}$ 及 $\mathfrak{H}_i$ 以外不復存在.

因羣 $\mathfrak{G}$ 之主組成列之各項皆爲 $\mathfrak{G}$ 之正常約羣,故其爲其先一項之正常約羣乃當然也. 於是得作一商羣列

$$(2)\qquad \frac{\mathfrak{G}}{\mathfrak{H}_1},\ \frac{\mathfrak{H}_1}{\mathfrak{H}_2},\ \cdots\cdots,\ \frac{\mathfrak{H}_{\mu-1}}{1}\quad\left(\frac{\mathfrak{H}_{\mu-1}}{1}=\mathfrak{H}_{\mu-1}\right).$$

爰名此曰由主組成列 (1) 所導出之**商羣列**.

定理. 商羣列(由主組成列所導出者),不問主組成列之選擇方法如何,常爲一定. 但商羣列中各項之順序則在所不論.

本定理中'一定'之意義,與關於由組成列所導出之商羣列之定理(第50節)中者全然同一. 故此之證明,用下

記之二項,便得與該定理同樣行之也.

(i) 設 $\mathfrak{H}_1, \mathfrak{H}_1'$ 爲 $\mathfrak{G}$ 中兩互異之極大正常約羣,而 $\mathfrak{L}$ 爲此二者之最大公約羣,則 $\mathfrak{L}$ 乃 $\mathfrak{G}$ 之正常約羣也(第34節第一定理). 又 $\mathfrak{L}$ 爲 $\mathfrak{H}_1$ 之極大正常約羣(第48節第二定理). 故 $\mathfrak{H}_1$ 無有含 $\mathfrak{L}$ 而卻與 $\mathfrak{H}_1$ 及 $\mathfrak{L}$ 異之正常約羣. 因之 $\mathfrak{G}$ 亦當然不得有此. 同樣,含 $\mathfrak{L}$ 而又含於 $\mathfrak{H}_1'$ 之正常約羣($\mathfrak{G}$ 的)亦不存在.

(ii) 令

(a) $\mathfrak{G}, \quad \mathfrak{H}_1, \quad 1$

(b) $\mathfrak{G}, \quad \mathfrak{H}_1', \quad \mathfrak{H}_2', \cdots\cdots$

爲 $\mathfrak{G}$ 之二主組成列,而 $\mathfrak{H}_1 \neq \mathfrak{H}_1'$. 於是若 $\mathfrak{L}$ 爲 $\mathfrak{H}_1$ 及 $\mathfrak{H}_1'$ 之最大公約羣,則有如上述,$\mathfrak{L}$ 於 $\mathfrak{G}$ 爲正常也. 故(a)既爲主組成列,則須 $\mathfrak{L}=1$. 但 $\mathfrak{H}_1'/\mathfrak{L}\ (=\mathfrak{H}_1')$ 乃與 $\mathfrak{G}/\mathfrak{H}_1$ 爲單純同態,因之即爲單羣. 故 $\mathfrak{H}_1'$ 之正常約羣 $\mathfrak{H}_2'$ 不得不爲主元素羣. 因之(b)乃成爲

(c) $\mathfrak{G}, \quad \mathfrak{H}_1', \quad 1.$

$\mathfrak{H}_1$ 及 $\mathfrak{H}_1'$ 之最大公約羣既爲主元素羣,於是適用第48節之定理,則由(a)及(c)所導出之商羣列之一致可知也.

52. 極小正常約羣.

設 $\mathfrak{N}$ 爲羣 $\mathfrak{G}$ 之正常約羣. 若 $\mathfrak{G}$ 除 $\mathfrak{N}$ 及主元素羣以外,無有含於 $\mathfrak{N}$ 之正常約羣時,則 $\mathfrak{N}$ 名曰 $\mathfrak{G}$ 之**極小正常約羣**.

極小之意義,與極大同,非所以示元數爲最小之正常

約羣者也. 以故一個羣中,元數相異之若干個極小正常約羣存在者亦有之焉.

如於羣

$$\left\{\begin{array}{lll} 1 & (abc) & (acb) \\ (bc) & (ca) & (ab) \\ (de) & (abc)(de) & (acb)(de) \\ (bc)(de) & (ca)(de) & (ab)(de), \end{array}\right.$$

其二正常約羣

$$1 \qquad (abc) \qquad (acb)$$

及

$$1 \qquad (de)$$

共爲極小,而其元數則一爲3一爲2者是也.

定理. 若$\mathfrak{N}$爲羣$\mathfrak{G}$之極小正常約羣,則$\mathfrak{G}$之正常約羣$\mathfrak{M}$,或含$\mathfrak{N}$,或僅與$\mathfrak{N}$有主元素公共. 而以後者論,則此時$\mathfrak{M}$之各元素與$\mathfrak{N}$之各元素爲交換可能.

證明. $\mathfrak{G}$之二正常約羣$\mathfrak{N}$及$\mathfrak{M}$之最大公約羣,在$\mathfrak{G}$中乃正常也. 但$\mathfrak{N}$爲極小. 故$\mathfrak{N}$及$\mathfrak{M}$之公約羣,或爲$\mathfrak{N}$自身,或則爲主元素羣,是爲必要.

復次,既$\mathfrak{N}$,$\mathfrak{M}$共於$\mathfrak{G}$爲正常,故各個之與他個各元素爲交換可能,明矣. 故共通元素僅爲主元素時,則由第27節第四定理,兩羣之元素爲交換可能也.

定理. 一羣之極小正常約羣或爲單純羣,或則得以互爲單純同態之單羣之直乘積表之.

證明. 令$\mathfrak{N}$爲$\mathfrak{G}$之極小正常約羣.$\mathfrak{N}$不爲單羣時,則以$\mathfrak{Q}$爲$\mathfrak{N}$之極小正常約羣之一,而以

$$(1) \qquad \mathfrak{Q}, \mathfrak{Q}_1, \cdots\cdots, \mathfrak{Q}_{s-1}$$

爲於$\mathfrak{G}$之共軛約羣系.* 於是此各個皆單純同態(第32節定理),且同爲$\mathfrak{N}$之極小正常約羣.蓋若

$$Q_i^{-1}\mathfrak{Q}Q_i=\mathfrak{Q}_i \quad (Q_i \text{爲} \mathfrak{G} \text{之元素}),$$

則於兩羣$\mathfrak{N}$及$Q_i^{-1}\mathfrak{N}Q_i$,以$Q_i^{-1}\mathfrak{N}Q_i$之元素$Q_i^{-1}KQ_i$使與$\mathfrak{N}$之元素K對應,於是兩羣之單純同態關係便告成立,而$\mathfrak{N}$之約羣$\mathfrak{Q}$與$Q_i^{-1}\mathfrak{N}Q_i$之約羣$Q_i^{-1}\mathfrak{Q}Q_i$對應.但$\mathfrak{Q}$爲$\mathfrak{N}$之極小正常約羣.故$Q_i^{-1}\mathfrak{Q}Q_i$於$Q_i^{-1}\mathfrak{N}Q_i$不得不爲極小正常也.然由假設,$\mathfrak{N}$於$\mathfrak{G}$爲正常,因之$Q_i^{-1}\mathfrak{N}Q_i=\mathfrak{N}$.故$Q_i^{-1}\mathfrak{Q}Q_i$即$\mathfrak{Q}_i$乃$\mathfrak{N}$之極小正常約羣也.

次之,因(1)之各羣既均於$\mathfrak{N}$爲極小正常,故其任意一個之各元素與其他羣之各元素爲交換可能也(前定理).

今作$\mathfrak{Q}$及$\mathfrak{Q}_1$之直乘積$\mathfrak{Q}\mathfrak{Q}_1$,而以$\mathfrak{G}$之任意元素G變其形,乃有

$$G^{-1}\mathfrak{Q}\mathfrak{Q}_1G=G^{-1}\mathfrak{Q}G\cdot G^{-1}\mathfrak{Q}_1G$$

即與$\mathfrak{Q}$之共軛約羣之積等也.於是若積$\mathfrak{Q}\mathfrak{Q}_1$含有與$\mathfrak{Q}$共軛之所有之約羣時,則$G^{-1}\mathfrak{Q}\mathfrak{Q}_1G$非含於$\mathfrak{Q}\mathfrak{Q}_1$不可,因之$\mathfrak{Q}\mathfrak{Q}_1$爲

---

*因$\mathfrak{N}$爲$\mathfrak{G}$之極小正常約羣,故$\mathfrak{Q}$於$\mathfrak{G}$非正常.因之$\mathfrak{Q}$所屬之共軛約羣系,由二或二以上之共軛約羣而成也.

$\mathfrak{G}$之正常約羣.然$\mathfrak{Q}\mathfrak{Q}_1$之含於$\mathfrak{R}$甚明而$\mathfrak{R}$於$\mathfrak{G}$又爲極小正常.故$\mathfrak{Q}\mathfrak{Q}_1$含有屬於共軛系(1)之所有之約羣時,則

$$\mathfrak{R}=\mathfrak{Q}\mathfrak{Q}_1.$$

反之,若(1)中有不含於$\mathfrak{Q}\mathfrak{Q}_1$者存在時,則以其一爲$\mathfrak{Q}_2$而作此與$\mathfrak{Q}\mathfrak{Q}_1$之直乘積$\mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2$焉(前定理參照).若積$\mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2$含有屬於(1)之所有之約羣時,則與前同樣

$$\mathfrak{R}=\mathfrak{Q}\mathfrak{Q}_1\mathfrak{Q}_2$$

也.如若不然,則將同樣之手段反覆施之.第$\mathfrak{R}$之元數有限,故$\mathfrak{R}$者,定能以屬於(1)之若干約羣之直乘積如$\mathfrak{Q}\mathfrak{Q}_1\cdots\cdots\mathfrak{Q}_{r-1}$者表之也.

終之,屬於(1)1之約羣皆單羣也.此何故歟?蓋若假定$\mathfrak{Q}$非單純,而以$\mathfrak{H}$爲$\mathfrak{Q}$之正常眞約羣(≠),則以$\mathfrak{Q}$之各元素與$\mathfrak{Q}_1,\mathfrak{Q}_2,\cdots\cdots,\mathfrak{Q}_{r-1}$之各元素交換可能之故,$\mathfrak{H}$遂爲$\mathfrak{Q}\mathfrak{Q}_1\cdots\mathfrak{Q}_{r-1}$(=$\mathfrak{R}$)之正常約羣,而與$\mathfrak{Q}$於$\mathfrak{R}$爲極小正常之假設反也.故$\mathfrak{Q}$不得不爲單羣.

綜上所述,概括言之,乃謂$\mathfrak{G}$之極小正常約羣$\mathfrak{R}$如不爲單純時,如以$\mathfrak{Q}$爲$\mathfrak{R}$之極小正常約羣之一,則$\mathfrak{Q}$爲單羣,而$\mathfrak{R}$遂得以$\mathfrak{G}$中與$\mathfrak{Q}$共軛之若干約羣之直乘積表之者也.

系. 可解羣之極小正常約羣,乃元數爲素數冪之Abel氏羣.

53. 設$\mathfrak{R}$爲羣$\mathfrak{G}$之極小正常約羣.苟非單羣時,則$\mathfrak{R}$得表之爲其極小正常約羣之直乘積而以之爲

$$\mathfrak{R} = \mathfrak{Q}\mathfrak{Q}_1 \cdots \mathfrak{Q}_{r-1}$$

此之因子 $\mathfrak{Q}\mathfrak{Q}_1 \cdots \mathfrak{Q}_{s-1}$ 與 $\mathfrak{Q}_s$ 之各元素交換可能，且與 $\mathfrak{Q}_s$ 所共有者僅一主元素．故商 $\dfrac{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_s}{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{s-1}}$ 與 $\dfrac{\mathfrak{Q}_s}{1}\left(=\mathfrak{Q}_s\right)$ 爲單純同態．然 $\mathfrak{Q}_s$ 乃單羣．故 $\dfrac{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_s}{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{s-1}}$ 亦不得不爲單羣也．因之 $\mathfrak{R}$ 之約羣列

(1) $\quad \mathfrak{R},\ \mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{r-2},\ \mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{r-3},\ \cdots\cdots,\ \mathfrak{Q},\ 1$

爰作成 $\mathfrak{R}$ 之組成列甚明(第48節第一定理參照)．而以 $\mathfrak{Q}_s$ 與 $\mathfrak{Q}$ 爲單純同態之故，由(1)所導出之商羣列各項，皆與 $\mathfrak{Q}$ 爲單純同態焉．

將此所得之結果應用於羣 $\mathfrak{G}$ 之主組成列

(2) $\quad \mathfrak{G},\ \mathfrak{H}_1,\ \mathfrak{H}_2,\cdots\cdots,\ \mathfrak{H}_{\mu-1},\ 1,$

若其一項 $\mathfrak{H}_i$ 之元數爲 h_i，則對 $\mathfrak{G}/\mathfrak{H}_i$ 之主元素，使 $\mathfrak{G}$ 之正常約羣 $\mathfrak{H}_i$ 與之對應時，$\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{H}_i$ 遂爲 h_i 重同態也，而於 $\mathfrak{G}$ 之約羣如 $\mathfrak{H}'$ 者，$\mathfrak{G}/\mathfrak{H}_i$ 之約羣 $\mathfrak{H}'/\mathfrak{H}_i$ 與對應焉．(第46節第一定理系3)．然 $\mathfrak{G}$ 中，含於 $\mathfrak{H}_{i-1}$ 又含 $\mathfrak{H}_i$ 之正常約羣不存在也(指 $\mathfrak{H}_{i-1}$ 及 $\mathfrak{H}_i$ 以外言)．故於 $\mathfrak{G}/\mathfrak{H}_i$ 中，含於 $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ 之正常約羣亦不存在(指 $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ 及1以外言)．故 $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ 爲 $\mathfrak{G}/\mathfrak{H}_i$ 之極小正常約羣．

今以 $\mathfrak{G}_{i-1,1}$ 爲含 $\mathfrak{H}_i$ 之 $\mathfrak{H}_{i-1}$ 之極大正常約羣，$\mathfrak{G}_{i-1,2}$ 爲含 $\mathfrak{H}_i$ 之 $\mathfrak{G}_{i-1,1}$ 之極大正常約羣，以下準此．於是由如斯所得之羣列

(3)　$\mathfrak{H}_{i-1}$, $\mathfrak{G}_{i-1,1}$, $\mathfrak{G}_{i-1,2}$, ……, $\mathfrak{G}_{i-1,s}$, $\mathfrak{H}_i$

以作商羣列

(4)　$\frac{\mathfrak{H}_{i-1}}{\mathfrak{H}_i}$, $\frac{\mathfrak{G}_{i-1,1}}{\mathfrak{H}_i}$, $\frac{\mathfrak{G}_{i-1,2}}{\mathfrak{H}_i}$, ……, $\frac{\mathfrak{G}_{i-1,s}}{\mathfrak{H}_i}$, 1

則此卽爲$\mathfrak{H}_{i-1}/\mathfrak{H}_i$之組成列明甚. (蓋對$\mathfrak{G}$之約羣$\mathfrak{H}'$, $\mathfrak{G}/\mathfrak{H}_i$之約羣$\mathfrak{H}'/\mathfrak{H}_i$與之對應故.) 而由此所導出之商羣列, 則由第46節第二定理系2, 爲

(5)　$\frac{\mathfrak{H}_{i-1}}{\mathfrak{G}_{i-1,1}}$, $\frac{\mathfrak{G}_{i-1,1}}{\mathfrak{G}_{i-1,2}}$, ……, $\frac{\mathfrak{G}_{i-1,s}}{\mathfrak{H}_i}$.

然由上所述, $\mathfrak{H}_{i-1}/\mathfrak{H}_i$於$\mathfrak{G}/\mathfrak{H}_i$爲極小正常. 故(5)之各商與$\mathfrak{G}_{i-1,s}/\mathfrak{H}_i$爲單純同態. 因之得有次之

定理. 設$\mathfrak{H}_{i-1}$, $\mathfrak{H}_i$爲一羣之主組成列中之相隣兩項, $\mathfrak{G}_{i-1,1}$爲含$\mathfrak{H}_i$之$\mathfrak{H}_{i-1}$之極大正常約羣, $\mathfrak{G}_{i-1,2}$爲含$\mathfrak{H}_i$之$\mathfrak{G}_{i-1,1}$之極大正常約羣, ……. 於是由若是所得之羣列

$$\mathfrak{H}_{i-1},\ \mathfrak{G}_{i-1,1},\ \mathfrak{G}_{i-1,2},\ \cdots\cdots,\ \mathfrak{G}_{i-1,s},\ \mathfrak{H}_i$$

所導出之商羣列

$$\frac{\mathfrak{H}_{i-1}}{\mathfrak{G}_{i-1,1}},\ \frac{\mathfrak{G}_{i-1,1}}{\mathfrak{G}_{i-1,2}},\ \frac{\mathfrak{G}_{i-1,2}}{\mathfrak{G}_{i-1,3}},\ \cdots\cdots\cdots,\ \frac{\mathfrak{G}_{i-1,s}}{\mathfrak{H}_i}$$

之各項互爲單純同態. 而$\mathfrak{H}_{i-1}/\mathfrak{H}_i$得以與$\mathfrak{G}_{i-1,s}/\mathfrak{H}_i$爲單純同態之單羣之直乘積表之.

第八章 Sylow 及 Frobenius 兩氏之定理.

54. Sylow 氏定理. 令 p^α 爲整除羣 $\mathfrak{G}$ 之元數 g 之素數 p 之最高冪. 卽 $g=p^\alpha m$ $(m\not\equiv 0 \pmod{p})$. 於是

(I) $\mathfrak{G}$ 乃有元數 p^α 之約羣. (此名曰與素因數 p 相應之 Sylow 氏約羣.)

(II) 元數 p^α 之約羣, 形成一共軛系. 而此約羣之數, 得以 $1+\lambda p$ 之形表之.

(I) 之證明. 1°. 茲先證'元數爲素數 p 之倍數之 Abel 氏羣含有巡回率 p 之元素'以資補助.

令 $\mathfrak{A}$ 爲元數 a 之 Abel 氏羣,

$$A_1,\quad A_2,\quad \cdots\cdots,\quad A_\alpha$$

爲其元素, 則由此各個所作之巡回羣之積 $\{A_1\}\{A_2\}\{A_3\}\cdots\cdots$ 含有 $\mathfrak{A}$ 所有之元素明已. 故

$$\mathfrak{A}=\{A_1\}\{A_2\}\cdots\cdots\{A_\alpha\}.$$

今以 $a_1, a_2, a_3, \cdots\cdots$, 分別爲 $A_1, A_2, A_3, \cdots\cdots$ 之巡回率. 則由第 27 節第三定理系, $\{A_1\}\{A_2\}$ 之元數乃 $a_1\,a_2$ 之約數, 因之 $\{A_1\}\{A_2\}\cdot\{A_3\}$ 之元數乃 $a_1\,a_2\,a_3$ 之約數, $\cdots\cdots$. 故 $\mathfrak{A}$ 之元數 a 乃 $a_1a_2a_3\cdots\cdots$ 之約數也. 於是若 a 爲素數 p 之倍數, 則 $a_1, a_2, a_3, \cdots\cdots$ 之中, p 之倍數定然存在. 茲以其一爲 a_1, 則 A_1 之 $\frac{a_1}{p}$

乘冪之巡回率爲 p 也.

2°. 茲假定羣之元數中素因數之個數少於 ν 時定理 (I) 爲眞, 而羣 $\mathfrak{G}$ 之元數含有 ν 個之素因數. 於是雖對於 $\mathfrak{G}$, 定理 (I) 亦成立也, 請示之焉.

(i) $\mathfrak{G}$ 含有巡回率 p 之自己共軛元素時.

設 P 爲巡回率 p 之自己共軛元素, 則巡回羣 $\{P\}$ 乃 $\mathfrak{G}$ 之正常約羣, 而其元數爲 p. 故商 $\mathfrak{G}/\{P\}$ 之元數爲

$$\frac{g}{p}=p^{\alpha-1}m.$$

而 $p^{\alpha-1}m$ 中素因數之數爲 $\nu-1$ 個. 故由假定, $\frac{\mathfrak{G}}{\{P\}}$ 含有元數 $p^{\alpha-1}$ 之約羣, 而以其一爲 Γ. 茲對於 $\frac{\mathfrak{G}}{\{P\}}$ 之主元素, 以 $\mathfrak{G}$ 之約羣 $\{P\}$ 使與對應, 由是, $\mathfrak{G}$ 與 $\frac{\mathfrak{G}}{\{P\}}$ 成 p 重同態, 而與 $\frac{\mathfrak{G}}{\{P\}}$ 之約羣 Γ (元數 $p^{\alpha-1}$) 對應約羣 ($\mathfrak{G}$ 的) 之元數爲 p^{α} 也. 蓋因對 $\mathfrak{G}/\{P\}$ 之一元素, $\mathfrak{G}$ 之 p 元素與之對應故. 以故 $\mathfrak{G}$ 非含元數 p^{α} 之約羣不可.

(ii) $\mathfrak{G}$ 不含巡回率 p 之自己共軛元素時.

此時 $\mathfrak{G}$ 之非 Abel 氏羣, 明已. 蓋若爲 Abel 氏羣, 則以 g 爲 p 之倍數故, 由 1°, $\mathfrak{G}$ 不得不含巡回率 p 之元素故也.

茲以 $\mathfrak{G}$ 中自己共軛元素所作之約羣爲 $\mathfrak{L}$, 其元數爲 l. 乃將非自己共軛之元素分成共軛系, 而以之爲

$$\mathfrak{C},\ \mathfrak{C}_1,\ \cdots\cdots,\ \mathfrak{C}_{t-1},$$

其各個所屬元素之數分別爲

$$c,\quad c_1,\quad \cdots\cdots,\quad c_{t-1}.$$

於是得

$$(1)\qquad \mathfrak{G}=\mathfrak{L}+\mathfrak{C}+\mathfrak{C}_1+\cdots\cdots+\mathfrak{C}_{t-1},$$

$$(2)\qquad g=l+c+c_1+\cdots\cdots+c_{t-1}.$$

且$\mathfrak{L}$既爲自己共軛元素之集合,故爲Abel氏羣.然$\mathfrak{G}$不含有巡回率p之自己共軛元素.故$\mathfrak{L}$之元數l卽(2)之右邊之第一項,不爲p之倍數(由1°).但(2)之左邊g爲p之倍數.故欲(2)之成立,$c, c_1, \cdots\cdots c_{t-1}$之中,其不爲$p$之倍數者非存在不可也.以其一爲$c$,而以屬於$\mathfrak{C}$之元素之一爲T,則因與T共軛元素之數爲$c$之故,其與T交換可能元素所作之羣(名之曰$\mathfrak{R}$)之元數遂爲$\frac{p^\alpha m}{c}$(第29節定理).但$\frac{p^\alpha m}{c}$得以$p^\alpha$整除($c$不爲$p$之倍數故),且其素因數少於$\nu$個.故由假定,$\mathfrak{R}$不得不含元數$p^\alpha$之約羣也.而此約羣當然屬於$\mathfrak{G}$.

夫如是,無論(i)或(ii)$\mathfrak{G}$皆有元數p^α之約羣焉.

3°. 茲再就羣$\mathfrak{G}$之元數中素因數有二個時定理(I)亦得成立者而示之.

此時元數或爲p^2或爲pq $(q\neq p)$,但爲p^2時,乃自明也.故僅後者而證明之,斯足已.

$\mathfrak{G}$爲Abel氏羣時,則由1°,$\mathfrak{G}$者含有p元約羣者也.而在非Abel氏羣時,乃以自己共軛元素所作之約羣爲$\mathfrak{L}'$,則其元數l'爲p或1抑或q. $l'=p$,則$\mathfrak{G}$便含有p元約羣;而l'爲

1或q時，則有如2°然，將非自己共軛元素分爲共軛系，而以之爲$\mathfrak{C}'$, $\mathfrak{C}_1'$, ……，其各個所屬元素之數，分別以爲c', c_1', ……，則

$$\mathfrak{G}=\mathfrak{L}'+\mathfrak{C}'+\mathfrak{C}_1'+\cdots\cdots \tag{3}$$

$$g=l'+c'+c_1'+\cdots\cdots \tag{4}$$

然g雖爲p之倍數，而l'卻非p之倍數．故c', c_1', …… 之中，其不爲p之倍數者非存在不可也．今以之爲c'，而以與$\mathfrak{C}'$中元素之一爲交換可能之元素所作之羣爲$\mathfrak{R}'$，則$\mathfrak{R}'$之元數爲$\frac{pq}{c'}$，但c'非p之倍數．故$c'=q$．因之

$$\frac{pq}{c'}=p.$$

是則$\mathfrak{G}$含有p元約羣$\mathfrak{R}'$也．

如是，元數pq之羣，常有元數p之約羣焉．

由2°及3°，可知羣常有Sylow氏約羣也．

(II) **之證明**．1°．以$\mathfrak{H}$及$\mathfrak{H}'$爲任意兩Sylow氏約羣(元數p^α)，而就此分$\mathfrak{G}$爲重傍系：

$$\mathfrak{G}=\mathfrak{H}\,S_0\,\mathfrak{H}'+\mathfrak{H}\,S_1\,\mathfrak{H}'+\mathfrak{H}\,S_2\,\mathfrak{H}'+\cdots\cdots \quad (S_0=1). \tag{5}$$

因$\mathfrak{H}$之元數爲p^α，故兩羣$S_i^{-1}\,\mathfrak{H}\,S_i$及$\mathfrak{H}'$之最大公約羣(以$[S_i^{-1}\,\mathfrak{H}\,S_i, \mathfrak{H}']$表之)之元數爲$p^{\gamma_i}$($\gamma_i\leqq\alpha$)．於是由第36節第一定理，重傍系$\mathfrak{H}\,S_i\,\mathfrak{H}'$乃含有互異之$p^{2\alpha-\gamma_i}$個元素．且(5)之右邊之重傍系無有共通之元素．因之由(5)

$$g=p^{2\alpha-\gamma_0}+p^{2\alpha-\gamma_1}+p^{2\alpha-\gamma_2}+\cdots\cdots$$

此兩邊各以 p^α 除之,得

$$m=p^{\alpha-\gamma_0}+p^{\alpha-\gamma_1}+p^{\alpha-\gamma_2}+\cdots\cdots \tag{6}$$

但左邊 m 對 p 爲互素. 故右邊諸項中,不能以 p 整除者定存在也. 以之爲 $p^{\alpha-\gamma_1}$, 則

$$\alpha-\gamma_1=0.$$

因之 $[S_1^{-1}\mathfrak{H}S_1, \mathfrak{H}']$ 之元數爲 p^α. 然 $S_1^{-1}\mathfrak{H}S_1$ 及 $\mathfrak{H}'$ 之元數共爲 p^α. 故須得

$$S_1^{-1}\mathfrak{H}S_1=\mathfrak{H}'$$

也. 卽 $\mathfrak{H}'$ 與 $\mathfrak{H}$ 共軛.

如上,元數 p^α 之約羣互爲共軛. 故是等約羣形成一共軛系也.

2. 茲以 p^α 元約羣之一,與前同樣爲 $\mathfrak{H}$,其與 $\mathfrak{H}$ 交換可能之元素($\mathfrak{G}$ 的)所作之羣爲 $\mathfrak{N}$, 而其元數爲 $p^\alpha m'$ (參照第 33 節).

$m'=m$ 時,則 $\mathfrak{N}=\mathfrak{G}$, 而 $\mathfrak{H}$ 於 $\mathfrak{G}$ 爲正常. 此時若假定 $\mathfrak{G}$ 除 $\mathfrak{H}$ 外含有 p^α 元約羣 $\mathfrak{H}'$, 則因 $\mathfrak{H}$ 於 $\mathfrak{G}$ 爲正常, $\mathfrak{H}'$ 之各元素遂與 $\mathfrak{H}$ 爲交換可能,而積 $\mathfrak{H}\mathfrak{H}'$ 之元數乃較 p^α 爲高冪也(第 27 節第三定理系). 但積 $\mathfrak{H}\mathfrak{H}'$ 非屬於 $\mathfrak{G}$ 不可甚明. 是此爲不合理. 故若 $\mathfrak{H}$ 於 $\mathfrak{G}$ 爲正常時, p^α 元約羣僅 $\mathfrak{H}$ 已也.

$m'<m$ 時,乃將 $\mathfrak{G}$ 就 $\mathfrak{H}$ 及 $\mathfrak{N}$ 分爲重傍系:

$$\mathfrak{G}=\mathfrak{N}T_0\mathfrak{H}+\mathfrak{N}T_1\mathfrak{H}+\mathfrak{N}T_2\mathfrak{H}+\cdots\cdots \quad (T_0=1). \tag{7}$$

因 $\mathfrak{H}$ 之元數爲 p^α, 故 $T_i^{-1}\mathfrak{N}T_i$ 與 $\mathfrak{H}$ 之最大公約羣(以

$[T_i^{-1}\mathfrak{R}T_i, \mathfrak{H}]$ 表之) 之元數爲 p^{δ_i} ($\delta_i \leqq \alpha$). 以故由第 36 節第一定理, 重傍系 $\mathfrak{R}T_i\mathfrak{H}$ 乃由互異之 $m'p^{2\alpha-\delta_i}$ 個元素而成. 且 (7) 之右邊之重傍系無有共通之元素(第 36 節). 故由 (7),

$$g = p^{\alpha}m'(p^{\alpha-\delta_0}+p^{\alpha-\delta_1}+p^{\alpha-\delta_2}+\cdots\cdots).$$

但 $\mathfrak{R}$ 之元數爲 $p^{\alpha}m'$. 故 $\mathfrak{R}$ 於 $\mathfrak{G}$ 之指數, 乃爲

$$(8) \qquad \frac{g}{p^{\alpha}m'} = p^{\alpha-\delta_0}+p^{\alpha-\delta_1}+p^{\alpha-\delta_2}+\cdots\cdots$$

也. 今就此式右邊諸項而觀, 乃知 $\delta_0 = \alpha$. 蓋因 $T_0 = 1$, 而 $\mathfrak{R}$ 又含 $\mathfrak{H}$, 則

$$[T_0^{-1}\mathfrak{R}T_0, \mathfrak{H}] = [\mathfrak{R}, \mathfrak{H}] = \mathfrak{H}$$

故.

次之, $\delta_i < \alpha$ ($i = 1, 2, \cdots$) 爲必要. 蓋若 $\delta_i = \alpha$, 則 $[T_i^{-1}\mathfrak{R}T_i, \mathfrak{H}]$ 之元數爲 p^{α}, 因之

$$[T_i^{-1}\mathfrak{R}T_i, \mathfrak{H}] = \mathfrak{H},$$

卽 $T_i^{-1}\mathfrak{R}T_i$ 含有 $\mathfrak{H}$ 也. 然 $\mathfrak{R}$ 含 $\mathfrak{H}$, 且 $\mathfrak{R}$ 之元素與 $\mathfrak{H}$ 爲交換可能. 故 $T_i^{-1}\mathfrak{R}T_i$ 包含 $T_i^{-1}\mathfrak{H}T_i$, 而其元素則與 $T_i^{-1}\mathfrak{H}T_i$ 爲交換可能. 因之 $T_i^{-1}\mathfrak{R}T_i$ 之約羣 $\mathfrak{H}$ 之元素與 $T_i^{-1}\mathfrak{H}T_i$ 爲交換可能, 隨之其積之元數須爲 p 之冪也. 然 $i \neq 0$ 時, 則 $T_i^{-1}\mathfrak{H}T_i \neq \mathfrak{H}$, 故 $\mathfrak{H}\cdot T_i^{-1}\mathfrak{H}T_i$ 之元數乃較 p^{α} 爲高冪. 是則元數 $p^{\alpha}m$ 之羣 $\mathfrak{G}$ 竟含較 p^{α} 爲高冪之元數之約羣也, 豈非不合理乎? 以故 $i \neq 0$ 時, 不得不 $\delta_i < \alpha$ 也.

由是, (8) 之右邊第一項等於 1, 第二項以下則皆爲 p 之倍數. 故 $\mathfrak{R}$ 之指數得以 $1+\lambda p$ 形表之焉. 然與 $\mathfrak{H}$ 共軛之

約羣之數與 $\mathfrak{R}$ 之指數等(第33節定理). 故其數爲 $1+\lambda p$.

系 1. 令 $p^\alpha m'$ 爲與 $\mathfrak{G}$ 之Sylow氏約羣(元數 p^α)皮交換可能之元素所作之羣之元數,則 $\mathfrak{G}$ 之元數定爲

$$p^\alpha m'(1+\lambda p)$$

之形. 而屬於 p 之Sylow氏約羣之數爲 $1+\lambda p$.

由此系,則於羣 $\mathfrak{G}$ 之元數 $p^\alpha m$, 若 $m<p$, 則必 $\lambda=0$. 故此時Sylow氏約羣僅一個,隨之爲正常也.

例. 就第24節所示之四次對稱羣(元數 $2^3\cdot 3$)而觀,其3元約羣乃爲

$$\{1,(bcd),(bdc)\},\quad \{1,(cad),(cda)\},$$
$$\{1,(dab),(dba)\},\quad \{1,(acb),(abc)\}$$

之4個 $(4=1+3)$, 此各個如第33節例2所示互爲共軛也. 又8元約羣亦不過 $\mathfrak{T}$, $(ac)\,\mathfrak{T}\,(ac)$, $(ad)\,\mathfrak{T}\,(ad)$ 之三個. 而 $3\equiv 1 \pmod 2$

系 2. 羣 $\mathfrak{G}$ 之元數得以素數之冪 p^β 整除時,則 $\mathfrak{G}$ 乃有元數 p^β 之約羣. 而此約羣乃含於Sylow氏約羣(與 p 相應者)之某一個之內.

證明. 與本節之定理中者同樣,以 $\mathfrak{G}$ 之元數爲 $p^\alpha m$, 則 $\mathfrak{G}$ 乃含 p^α 元約羣卽Sylow氏約羣. 以其一爲 $\mathfrak{H}$, 則 $\mathfrak{H}$ 由第47節第一定理,含有 p^β 元約羣. 而此羣當然屬於 $\mathfrak{G}$.

次之以 $\mathfrak{L}$ 爲任意之 p^β 元約羣 $(\beta<\alpha)$, 乃以 $\mathfrak{G}$ 就 $\mathfrak{H}$, $\mathfrak{L}$ 分爲重傍系:

$$\mathfrak{G}=\mathfrak{H}\,S_0\,\mathfrak{L}+\mathfrak{H}\,S_1\,\mathfrak{L}+\mathfrak{H}\,S_2\,\mathfrak{L}+\cdots\cdots;$$

而 $S_i^{-1}\mathfrak{H}\,S_i$ 與 $\mathfrak{L}$ 之最大公約羣，則以 $[S_i^{-1}\mathfrak{H}S_i,\mathfrak{L}]$ 表示，其元數以爲 p^{δ_i} $(\delta_i\leqq\beta)$. 於是由上之關係.

$$p^{\alpha}m=p^{\alpha+\beta-\delta_0}+p^{\alpha+\beta-\delta_1}+p^{\alpha+\beta-\delta_2}+\cdots\cdots \quad (\text{參照第 36 節}).$$

兩邊以 p^{α} 除之，得

$$m=p^{\beta-\delta_0}+p^{\beta-\delta_1}+p^{\beta-\delta_2}+\cdots\cdots.$$

但左邊 m 對素數 p 爲互素. 故爲本式成立計，右邊諸項中其不能以 p 整除者非存在不可也. 以之爲 $p^{\beta-\delta_1}$，則 $\beta-\delta_1=0$. 因之

$$[S_1^{-1}\mathfrak{H}\,S_1,\ \mathfrak{L}]=\mathfrak{L},$$

即謂 $\mathfrak{L}$ 者含於 Sylow 氏約羣 $S_1^{-1}\,\mathfrak{H}\,S_1$ 者也.

注意. 在本定理中，將 $\mathfrak{G}$ 就 $\mathfrak{R}$ 分爲傍系，而以之爲

$$\mathfrak{G}=\mathfrak{R}\,Q_0+\mathfrak{R}\,Q_1+\cdots\cdots+\mathfrak{R}\,Q_{\lambda p}\quad (Q_0=1).$$

於是 $\mathfrak{R}$ 之共軛約羣 $Q_i^{-1}\,\mathfrak{R}\,Q_i$ 乃以 $Q_i^{-1}\,\mathfrak{H}\,Q_i$ 爲正常約羣而含之也. 但由 Sylow 氏定理 (II)，$Q_i^{-1}\,\mathfrak{R}\,Q_i$ 除此外再不含 p^{α} 元約羣. 因之

$$\mathfrak{R},\quad Q_1^{-1}\,\mathfrak{R}\,Q_1,\ \cdots\cdots,\ Q^{-1}{}_{\lambda p}\,\mathfrak{R}\,Q_{\lambda p}$$

互異，而由此，$\mathfrak{R}$ 所屬之共軛系得以作之焉.

55. Frobenius 氏之擴張.

定理. 素數之冪 p^{β}，整除一羣之元數時，則其羣中 p^{β} 元約羣之數與 $1+\mu p$ 等. 但 μ 爲零或正整數.

證明. 分六段論之.

1°. p^2 元羣中 p 元約羣之數爲 1 或 $1+p$.

如第 31 節所述, 元數 p^2 之羣乃 Abel 氏羣也. 在巡回羣時, 則此得以

$$(1) \qquad 1,\ A,\ A^2,\ \cdots\cdots,\ A^{p^2-1}$$

與之. 此中 p 元約羣以爲 $\{A^t\}$, 則

$$A^{tp}=1.$$

故 t 不得不爲 p 之倍數. 卽

$$t=pt'.$$

若 t' 更爲 p 之倍數, 則以 $A^{tp}=1$ 之故, t' 對於 p 須互素也. 因此選擇一正整數 x 得滿足

$$t'x\equiv 1 \pmod{p}$$

者爲可能. 對此 x, 乃有

$$(A^t)^x=A^{pt'x}=A^p.$$

故 $\{A^t\}$ 含於 $\{A^p\}$. 然兩羣之元數同. 故

$$\{A^t\}=\{A^p\}.$$

因之於 p^2 元巡回羣 (1), 其 p 元約羣僅 $\{A^p\}$ 一個.

其次, 在不爲巡回羣時, p^2 元 Abel 氏羣得以兩個互異之 p 元羣 $\{A\}$ 及 $\{B\}$ 之積表之. 卽

$$(2) \qquad A^iB^j \ (i, j=0, 1, 2, \cdots\cdots, p-1).$$

今取其一元素 A^tB^u. 若 $t\neq 0$, 則對於適合 $tx\equiv 1 \pmod{p}$ 之正整數 x, 乃有

$$(A^tB^u)^x=AB^{ux}.$$

故與前同樣

$$\{A^tB^u\}=\{AB^{ux}\}.$$

$t=0$, $u\neq 0$ 時，乃取如 $uy\equiv 1 \pmod{p}$ 者之正整數 y，則

$$(B^u)^y=B.$$

$$\therefore \quad \{B^u\}=\{B\}.$$

因之羣(2)中之 p 元羣不得不爲下記 $p+1$ 個中之一也：

(3)　$\{A\}$, $\{AB\}$, $\{AB^2\}$, ……, $\{AB^{p-1}\}$, $\{B\}$.

且此各個皆互異．蓋若 $\{AB^i\}=\{AB^j\}$，則

$$(AB^j)^z=AB^i \quad (z \text{ 爲 } 1, 2, \cdots\cdots, p-1 \text{ 之一數})$$

因之　$A^zB^{jz}=AB^i$.

但(2)之元素互異．故欲上之等式成立，必得

$$z=1, \quad j=i$$

也．故若 $i\neq j$，則 $\{AB^i\}\neq\{AB^j\}$.

其他準此．因是，(3)中 $p+1$ 個之羣彼此互異，而羣(2)含有 $p+1$ 個之 p 元約羣焉．

2°．以下概以 $\mathfrak{H}$ 爲 p^α 元約羣，而其 p^β 元約羣之數，則以 r_β 表之．試先證

$$r_{\alpha-1}\equiv 1 \pmod{p}.$$

設 $\mathfrak{H}$ 含有兩個 $p^{\alpha-1}$ 元約羣 $\mathfrak{A}$ 及 $\mathfrak{A}'$，而其最大公約羣爲 $\mathfrak{D}$．由第47節第二定理系1，此兩約羣皆於 $\mathfrak{H}$ 爲極大正常．故 $\mathfrak{D}$ 爲 $\mathfrak{H}$ 之正常約羣也(第34節第一定理)．而兩約羣之積 $\mathfrak{A}\mathfrak{A}'$ 等於 $\mathfrak{H}$，且 $\mathfrak{A}/\mathfrak{D}$ 與 $\mathfrak{H}/\mathfrak{A}'$ 爲單純同態(第48節

第二定理). 因之 $\mathfrak{D}$ 之元數爲 $p^{\alpha-2}$.

由 $\mathfrak{H}=\mathfrak{A}\mathfrak{A}'$ 及 $\mathfrak{H}$ 與 $\mathfrak{H}/\mathfrak{D}$ 成 $p^{\alpha-2}$ 重同態之故, 乃有

$$\mathfrak{H}/\mathfrak{D}=\mathfrak{A}/\mathfrak{D}\cdot\mathfrak{A}'/\mathfrak{D} \qquad (\text{第 46 節第一定理系 3}).$$

但 $\mathfrak{A}/\mathfrak{D}$, $\mathfrak{A}'/\mathfrak{D}$ 之元數皆爲 p. 故 $\mathfrak{H}/\mathfrak{D}$ 與兩個 p 元羣之積等. 以故由 1° 所述, $\mathfrak{H}/\mathfrak{D}$ 乃含有 $p+1$ 個之 p 元約羣. 因之 $\mathfrak{H}$ 乃含 $p+1$ 個之共有 $\mathfrak{D}$ 者之 $p^{\alpha-1}$ 元約羣也(參照第 46 節). 是卽 $\mathfrak{A}$ 之外, 其共有 $\mathfrak{D}$ 者之 $p^{\alpha-1}$ 元約羣, 得有 p 個存在焉. 若由此其 $p^{\alpha-1}$ 元約羣之全數得盡時, 則 $r_{\alpha-1}=p+1\equiv 1 \pmod{p}$, 定理之爲眞, 明矣. 反之, 除此外尙有 $p^{\alpha-1}$ 元約羣存在時, 乃以其一爲 $\mathfrak{A}''$, 而此與 $\mathfrak{A}$ 之最大公約羣以爲 $\mathfrak{D}'$. 於是與前同樣, 知 $\mathfrak{H}$ 於 $\mathfrak{A}$ 外尙含有 p 個之共有 $\mathfrak{D}'$ 者之 $p^{\alpha-1}$ 元約羣也. 第此之 p 個卻與前此之 p 個者異. 蓋若以其有相等者如 $\mathfrak{A}_1$, 則 $\mathfrak{A}_1$ 非含 $\mathfrak{D}$ 及 $\mathfrak{D}'$ 之兩羣不可. 然積 $\mathfrak{D}\mathfrak{D}'$ 之元數, 較之 $p^{\alpha-2}$ 爲高冪, 因之 $\mathfrak{D}\mathfrak{D}'=\mathfrak{A}$. 故 $\mathfrak{A}_1=\mathfrak{A}$, 是與假定反耳.

由 $\mathfrak{A}$ 及前後所得者之 $2p$ 個得以盡 $p^{\alpha-1}$ 元約羣之全數時, 則 $r_{\alpha-1}=2p+1\equiv 1 \pmod{p}$, 定理告成立也. 若除此之外, $p^{\alpha-1}$ 元約羣尙有存在時, 乃取其一而施以與前同樣之方法, 終可得到 $r_{\alpha-1}=1+xp\equiv 1 \pmod{p}$.

3°. $$r_1\equiv 1 \pmod{p}.$$

主元素以及巡回率 p 之自己共軛元素之集合, 其形成一羣, 明矣; 而其元數則爲 p 之冪(因 $\mathfrak{H}$ 之元數爲 p^{α} 故).

以此元數爲p^γ, 則$\mathfrak{S}$中巡回率p之自己共軛元素之數爲$p^\gamma-1$.

自他面言, 巡回率p之自己共軛元素, 其任何一個皆生成p元正常約羣; 反之$\mathfrak{S}$中之p元正常約羣, 皆由此類元素而成也(第47節第三定理). 且互異之p元羣除主元素外, 無共有之元素. 故p元正常約羣之數, 若以n_1表之, 則巡回率p之自己共軛元素之數與$n_1(p-1)$等. 因之

$$n_1(p-1)=p^\gamma-1.$$

$$\therefore \quad n_1=\frac{p^\gamma-1}{p-1}\equiv 1 \pmod{p}.$$

次之, 若非正常之p元約羣存在於$\mathfrak{S}$時, 乃將其分爲共軛約羣系. 於是屬於各共軛系之約羣之數, 乃爲p之冪焉(第33節定理). 故若以此諸數分別爲$p^\tau, p^{\tau'}, \cdots\cdots$, 則彼非正常之$p$元約羣之數爲

$$p^\tau+p^{\tau'}+\cdots\cdots \quad (\tau, \tau', \cdots\cdots \geqq 1).$$

因之$\mathfrak{S}$中p元約羣之總數爲

$$n_1=n_1+p^\tau+p^{\tau'}+\cdots\cdots\equiv 1 \pmod{p}.$$

4°. $\mathfrak{Q}$爲p^β元約羣$(\beta<\alpha-1)$時, 則含$\mathfrak{Q}$之$p^{\beta+1}$元約羣之數, 對法p乃與1合同.

茲以含$\mathfrak{Q}$之$p^{\beta+1}$元約羣之任意一個爲$\mathfrak{M}$以與$\mathfrak{Q}$成交換可能之$\mathfrak{S}$之元素所作之羣爲$\mathfrak{C}$. 因$\mathfrak{Q}$於$\mathfrak{M}$爲正常(第47節第二定理系1), 故$\mathfrak{M}$非含於$\mathfrak{C}$不可. 因之共有$\mathfrak{Q}$者之$p^{\beta+1}$元約羣皆含於$\mathfrak{C}$.

自他方面觀, $\mathfrak{G}$ 之元數爲 $p^{\beta+\delta}(\delta\geqq 1)$ (第47節第二定理). 因之商 $\mathfrak{G}/\mathfrak{Q}$ 之元數爲 p^{β}. 故由3°, $\mathfrak{G}/\mathfrak{Q}$ 乃含有 $1+xp$ 個之 p 元約羣在. 然 $\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{Q}$ 爲 p^{β} 重同態. 故 $\mathfrak{G}$ 乃包含共有 $\mathfrak{Q}$ 者之 $1+xp$ 個之 $p^{\beta+1}$ 元約羣也.

因之 $\mathfrak{Q}$ 含於 $1+xp$ 個之 $p^{\beta+1}$ 元約羣焉.

5°. $$r_{\beta}\equiv 1\ (\mathrm{mod.}\ p).\quad (\beta\leqq\alpha-1).$$

茲以

(4) $$\mathfrak{Q}_1, \mathfrak{Q}_2, \cdots\cdots, \mathfrak{Q}_{r_\beta}$$

爲 $\mathfrak{G}$ 中 p^{β} 元約羣之全數 $(\beta<\alpha-1)$;

(5) $$\mathfrak{M}_1, \mathfrak{M}_2, \cdots\cdots, \mathfrak{M}_{r_{\beta+1}}$$

爲 $\mathfrak{G}$ 中 $p^{\beta+1}$ 元約羣之全數. 於是(4)之各羣乃含於(5)之或一個之中(第47節第二定理系2). 今以 $\mathfrak{Q}_i$ 爲含於(5)中 l_i 個之羣者, 又以 $\mathfrak{M}_j$ 爲含有(4)之羣 m_j 個者, 如是.

(6) $$l_1+l_2+\cdots\cdots+lr_{\beta}=m_1+m_2+mr_{\beta+1}$$

明已. 然由2°及4°,

$$l_i\equiv 1\ (\mathrm{mod.}\ p),\quad m_j\equiv 1\ (\mathrm{mod.}\ p).$$

故由(6)

$$r_{\beta}\equiv r_{\beta+1}\ (\mathrm{mod.}\ p).$$

$$\therefore\quad r_1\equiv r_2\equiv\cdots\cdots\equiv r_{\alpha-1}\ (\mathrm{mod.}\ p).$$

但由3°, $r_1\equiv 1\ (\mathrm{mod.}\ p)$. 故

$$r_{\beta}\equiv 1\ (\mathrm{mod.}\ p).$$

6°. 茲則漸達於本定理之證明矣. 乃以羣 $\mathfrak{G}$ 之元數

爲 $p^{\alpha}m$, $(m \not\equiv o \pmod{p})$; 以

(7)　　$\mathfrak{H}, \mathfrak{H}_1, \cdots\cdots, \mathfrak{H}_{\lambda p}$

爲 $\mathfrak{G}$ 之 Sylow 氏約羣(元數 p^{α}); 以

(8)　　$\mathfrak{Q}, \mathfrak{Q}_1, \cdots\cdots, \mathfrak{Q}_{n-1}$

爲 p^{β} 元約羣($\beta<\alpha$)之全數.

由 Sylow 氏定理系 2, 則 $\mathfrak{Q}$ 含於 Sylow 氏約羣(7)之某一個之中. 於是將 Sylow 氏約羣分爲二組, 以含 $\mathfrak{Q}$ 者入於第一組, 不含者入於第二組. 乃以 $\mathfrak{H}_t$ 爲屬於後者之一, 而以其與 $\mathfrak{Q}$ 之最大公約羣爲 $\mathfrak{D}$, 及其元數爲 p^{δ} $(\delta<\beta)$. 由是, $\mathfrak{Q}$ 之元素中得與 $\mathfrak{H}_t$ 交換可能者惟含於 $\mathfrak{D}$ 中者爲能. 蓋若 $\mathfrak{Q}$ 之元素 L 與 $\mathfrak{H}_t$ 交換可能, 然卻不屬於 $\mathfrak{D}$; 則積 $\mathfrak{H}_t\{L\}$ 爲元數較 p^{α} 爲高羃之羣, 而 $p^{\alpha}m$ 元羣竟至含若是之約羣也, 豈非不合理耶?

以故若以 $\mathfrak{Q}$ 之各元素將 $\mathfrak{H}_t$ 變形, 則可得 $p^{\beta-\delta}$ 個之 Sylow 氏約羣(第 33 節注意參照). 且此各個皆屬於第二組. 蓋若其一, $L^{-1}\mathfrak{H}_tL$, (L 乃 $\mathfrak{Q}$ 之元素) 屬於第一組, 卽含有 $\mathfrak{Q}$, 則 $L(L^{-1}\mathfrak{H}_tL)L^{-1}=\mathfrak{H}_t$ 亦含 $\mathfrak{Q}$, 是與假定反故也. 若此之 $p^{\beta-\delta}$ 個不能盡第二組之 Sylow 氏約羣之全數時, 則取此外之一, $\mathfrak{H}_u$, 而以 $\mathfrak{Q}$ 之各元素將其變形, 則與前同樣, 可得屬於第二組之 $p^{\beta-\delta'}$ 個 $(\delta'<\beta)$ Sylow 氏約羣也. 而此所得之 $p^{\beta-\delta'}$ 個與先之 $p^{\beta-\delta}$ 個彼此互異, 容易證明. 故以前後所得之約羣而得盡第二組之全數時, 則屬於是之羣之數爲 $p^{\beta-\delta}+p^{\beta-\delta'}$. 反之

除此二者外,屬於第二組者尚存在時,更取其一而以與前同樣之手段反覆,終之第二組之Sylow氏約羣克以取盡,隨之其數之爲

$$p^{\beta-\delta}+p^{\beta-\delta'}+\cdots\cdots \quad (\delta,\delta',\cdots\cdots<\beta)$$

可知也.

又自他面觀,Sylow氏約羣之數爲$1+\lambda p$也. 故屬於第一組者卽含$\mathfrak{Q}$之Sylow氏約羣之數爲

$$1+\lambda p-p^{\beta-\delta}-p^{\beta-\delta'}-\cdots\cdots.$$

此數爰以$1+\nu_0 p$表之.

同樣,含$\mathfrak{Q}_i$之Sylow氏約羣之數爲$1+\nu_i p$.

復次,p^β元約羣(8)之中,含於$\mathfrak{H}$者之個數若以r_β表之,則由Sylow氏定理,因(7)之羣互相共軛,故(7)之各個,皆含屬於(8)之羣之r_β個. 因之

$$\sum_{i=0}^{n-1}(1+\nu_i p)=(1+\lambda p)\,r_\beta.$$

然由5^0, $r_\beta\equiv 1 \pmod{p}$. 故

$$n\equiv 1 \pmod{p}$$

卽謂$\mathfrak{G}$中p^β元約羣之數等於$1+\mu p$也.

例. 試取四次對稱羣,其4元約羣爲次之7個($7=1+3\cdot 2$):

$$1,\quad (ab)(cd),\quad (ac)(bd),\quad (ad)(bc);$$

$$1,\quad (abcd),\quad (ac)(bd),\quad (adcb);$$

1,　(abdc),　(ad)(bc),　(acdb);

1,　(acbd),　(ab)(cd),　(adbc);

1,　(ab),　(cd),　(ab)(cd);

1,　(ac),　(bd),　(ac)(bd);

1,　(ad),　(bc),　(ad)(bc).

而第一之約羣爲自己共軛;其他每三個皆作共軛系.

如本例之所示,其p^β元約羣($\beta<\alpha$)乃與Sylow氏約羣異,未見其必作一共軛系也.

第九章. 羣之單複,可解性

56. 在元數爲已知之羣中,欲考究其單羣之存在與否,且欲決定其型,此爲羣論上一重要而富有興趣之問題也. 對於前者,姑就由Sylow氏定理之應用比較的得容易解決者而論,併將關乎此之Frobenius氏定理一舉之焉.

定理. p, q爲互異之素數時,則元數$p^\alpha q$($\alpha\geqq 1$)之羣爲複合的.

證明. 設$\mathfrak{G}$爲元數$p^\alpha q$之羣.

1°. $\alpha=1$時. 由Sylow氏定理系1,若$p>q$,則p元約羣爲正常;又若$p<q$,則q元約羣爲正常.

2°. $\alpha>1, p>q$時. 由上所引用之系,則p^α元約羣爲正常.

3'. $\alpha>1$, $p<q$ 時.

因 q 爲素數, 故 p^α 元約羣 $\mathfrak{H}$ 之正常化羣 $\mathfrak{R}$ 之元數爲 $p^\alpha q$ 或 p^α. 以前者論, 則 $\mathfrak{R}=\mathfrak{G}$, 而 $\mathfrak{H}$ 爲正常; 以後者論, 則 $\mathfrak{R}=\mathfrak{H}$, 而 p^α 元約羣之數爲 q 個. 以下專就此而論之.

茲以

(1) $\qquad \mathfrak{H},\ \mathfrak{H}_1,\ \cdots\cdots,\ \mathfrak{H}_{q-1}$

爲屬於 p 之 Sylow 氏約羣, 以 $\mathfrak{D}$ 爲此等約羣每兩個之最大公約羣中元數之最大者之一, 而以 $\mathfrak{H}$ 與 $\mathfrak{H}_1$ 則爲共有此 $\mathfrak{D}$ 者.

$\mathfrak{D}$ 爲主元素羣時, 則主元素以外之元素, 於 (1) 之二羣中皆非共通. 故含於 (1) 之羣中元素 (互異的) 之總數, 除主元素外爲

$$(p^\alpha-1)q.$$

又自他面觀, 巡回率不爲 p 之冪之元素, 則不含於此 $(p^\alpha-1)q$ 個之內. 故將屬於 $\mathfrak{G}$ 之 q 元約羣之 q 個元素加於此中, 則其和爲

$$(p^\alpha-1)q+q=p^\alpha q,$$

而與 $\mathfrak{G}$ 之元數等也. 因之 q 元約羣只唯一個存在. 卽 $\mathfrak{D}$ 爲主元素羣時, q 元約羣爲正常也.

若 $\mathfrak{D}$ 非主元素羣時, 乃以 $\mathfrak{L}$ 及 $\mathfrak{L}_1$ 分別爲 $\mathfrak{H}$ 及 $\mathfrak{H}_1$ 中之 $\mathfrak{D}$ 之正常化羣.* 於是由第 47 節第二定理, $\mathfrak{L}$ 及 $\mathfrak{L}_1$ 之元數,

*$\mathfrak{L}$ 乃 $\mathfrak{H}$ 之元素中與 $\mathfrak{D}$ 交換可能者所作之羣; $\mathfrak{L}_1$ 爲 $\mathfrak{H}_1$ 中同樣之約羣.

共較 $\mathfrak{D}$ 之元數爲高冪. 因之 $\mathfrak{Q}_1$ 不含於 $\mathfrak{H}$. 今就由 $\mathfrak{Q}$ 及 $\mathfrak{Q}_1$ 之元素所生成之羣* (以 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 表之) 而觀, 則 $\mathfrak{D}$ 在此羣中之爲正常明已. 且 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 之元數, 決不爲 p 之冪. 蓋若爲 p 之冪, 則由 Sylow 氏定理系 2, Sylow 氏約羣 (1) 之中, 含有 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 者必存在無疑. 茲以之爲 $\mathfrak{H}'$, 則因 $\mathfrak{H}$ 不含 $\mathfrak{Q}_1$ 之故, $\mathfrak{H}'$ 與 $\mathfrak{H}$ 異也. 而 $\mathfrak{H}'$ 與 $\mathfrak{H}$ 之最大公約羣含有 $\mathfrak{Q}$, 因之其元數較 $\mathfrak{D}$ 之元數爲大. 是則與對於 $\mathfrak{D}$ 之假定相反, 爲不合理. 故 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 之元數, 決非 p 之冪, 隨之非有

$$p^{\gamma}n \quad (1<n\not\equiv 0 \pmod{p})$$

之形不可. 然 $\mathfrak{G}$ 之元數爲 $p^{\alpha}q$. 故 $n=q$ 爲必要. 今於此取 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 之 q 元約羣, 而以之爲

$$1, \quad Q, \quad Q^2, \cdots\cdots, \quad Q^{q-1}.$$

乃以此各元素將 $\mathfrak{H}$ 變形, 則因 $\mathfrak{H}$ 之正常化羣爲 $\mathfrak{H}$ 自身故, 遂得 q 個之共軛約羣

$$(2) \qquad \mathfrak{H}, \quad Q^{-1}\mathfrak{H}Q, \cdots\cdots, \quad Q^{-q+1}\mathfrak{H}Q^{q-1}.$$

但如前所述, $\mathfrak{D}$ 於 $\{\mathfrak{Q}, \mathfrak{Q}_1\}$ 爲正常. 故 $\mathfrak{D}$ 含於 (2) 之全部中也. 然自他面觀, (2) 與 (1) 不得不一致, 甚明. 故 $\mathfrak{D}$ 乃爲 (1) 全部所共有. 又由假定, 則 $\mathfrak{D}$ 原爲在 (1) 之兩羣之最大公約羣中元數之最大者. 因之 $\mathfrak{D}$ 乃爲 (1) 中 q 個羣之最大公約羣. 但由 Sylow 氏定理, (1) 之羣形成一共軛系. 故由

---

*生成之義意, 請參照第 42 節.

第34節定理, $\mathfrak{D}$ 爲 $\mathfrak{G}$ 之正常約羣焉.

由是以觀, 可知無論如何, $\mathfrak{G}$ 除主元素羣以外皆有正常約羣也. 故云云.

系. 元數 $p^\alpha q$ 之羣爲可解的. 但 p, q 爲互異之素數.

證明. 吾人只須求 $p^\alpha q$ 元羣 $\mathfrak{G}$ 之極大正常約羣, 其指數爲素數便足.

茲以 $\mathfrak{N}$ 爲 $\mathfrak{G}$ 之正常約羣, 則商 $\mathfrak{G}/\mathfrak{N}$ 之元數爲 $p^{\alpha-\beta}\ (\beta<\alpha)$ 或 $p^{\alpha-\gamma}q\ (\gamma\leqq\alpha)$. 此元數若非素數時, 則由第47節第一定理及本節之定理, $\mathfrak{G}/\mathfrak{N}$ 除主元素羣以外, 尙有正常約羣. 以之爲 Γ. 然 $\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{N}$ 爲重複同態. 故 $\mathfrak{G}$ 含有與 Γ 對應之正常約羣. 而此之元數較 $\mathfrak{N}$ 之元數當然爲大. 故 $\mathfrak{N}$ 之指數不爲素數時, $\mathfrak{N}$ 則非極大. 如是, 極大正常約羣之指數不得不爲素數也.

例 1. 試就第33, 34節例中所示之四次對稱羣一論之.

例 2. 令 $\mathrm{P}=(abcdef)$, $\mathrm{Q}=(bf)(ce)$, 則

$$\mathrm{Q}^{-1}\mathrm{PQ}=(afedcb)=\mathrm{P}^5.$$

$$\therefore\qquad \mathrm{Q}^{-1}\{\mathrm{P}\}\mathrm{Q}=\{\mathrm{P}\}.$$

故兩巡回羣 $\{\mathrm{P}\}$, $\{\mathrm{Q}\}$ 之積

$$1,\ \mathrm{P},\ \mathrm{P}^2,\ \mathrm{P}^3,\ \mathrm{P}^4,\ \mathrm{P}^5,\ \mathrm{Q},\ \mathrm{PQ},\ \mathrm{P}^2\mathrm{Q},\ \mathrm{P}^3\mathrm{Q},\ \mathrm{P}^4\mathrm{Q},\ \mathrm{P}^5\mathrm{Q}$$

形成一 12 元羣. 以之名曰 $\mathfrak{G}$. 其中之 4 元約羣爲次之三個:

$$\mathfrak{H}: \quad 1, \quad (ad)(be)(cf), \quad (bf)(ce), \quad (ad)(bc)(ef);$$

$$P^{-1}\mathfrak{H}P: \quad 1, \quad (ad)(be)(cf), \quad (ca)(df), \quad (be)(cd)(fa);$$

$$P^{-2}\mathfrak{H}P^2: \quad 1, \quad (ad)(be)(cf), \quad (db)(ea), \quad (cf)(de)(ab).$$

斯三者含有公約羣

$$1, \quad (ad)(be)(cf),$$

而此公約羣於$\mathfrak{G}$爲正常焉.

注意. 上兩例之羣,其3元約羣,在第二例爲正常,而於第一例則否. 若$p^\alpha > q$, 則$p^\alpha q$元羣,無論q元約羣爲正常與否,常有p^β元($\beta < \alpha$)之正常約羣. 關於此點;若以$p^\alpha q$元羣$\mathfrak{G}$爲無有p^β元正常約羣者,則於上定理之證明中,q元約羣之得爲正常,殆甚明也;若$\mathfrak{G}$含有q個之p^α元約羣時,則$\mathfrak{G}$得表之爲q次可遷羣(第77節);而含有q元正常約羣之q次可遷羣乃爲亞巡回羣或其約羣(第100節);由是種種,是不難得知焉.

57. **Frobenius氏定理**. 設整數a之素因數爲互異,而其最大素因數,則較他之整數b之各素因數爲小.如是,元數ab之羣,巡回率爲b之約數之元素,恰含有b個.

證明. 分五段論之.

1°. 以$\mathfrak{G}$爲元數爲ab之羣,以p爲a之素因數,則由Sylow氏定理$\mathfrak{G}$含有p元約羣焉.以其一爲$\mathfrak{P}=\{P\}$. $\mathfrak{P}$之正常化羣爲$\mathfrak{N}$,而其元數爲$a'pb'$. 但$a'p$爲a之約數,b'爲b之約數.卽$a=a'a''p$, $b=b'b''$.

次之將$\mathfrak{G}$就$\mathfrak{N}$分成傍系而以之爲

$$\mathfrak{G}=\mathfrak{N}Q_0+\mathfrak{N}Q_1+\cdots\cdots+\mathfrak{N}Q_{a''b''-1}\quad Q_0=1),$$

則$\mathfrak{P}$所屬之共軛約羣系爲

$$(1)\quad Q_0^{-1}\mathfrak{P}Q_0(=\mathfrak{P}),\quad Q_1^{-1}\mathfrak{P}Q_1,\cdots\cdots,\quad Q_{a''b''-1}^{-1}\mathfrak{P}Q_{a''b''-1}.$$

因ab不含p之自乘.故由Sylow氏定理,$\mathfrak{G}$除(1)之$a''b''$個以外,無有p元約羣.且由同節之注意.

$$(2)\quad Q_0^{-1}\mathfrak{N}Q_0(=\mathfrak{N}),\quad Q_1^{-1}\mathfrak{N}Q_1,\cdots\cdots,\quad Q_{a''b''-1}^{-1}\mathfrak{N}Q_{a''b''-1}$$

形成$\mathfrak{N}$所屬之共軛系,而其一羣$Q_i^{-1}\mathfrak{N}Q_i$雖含$Q_i^{-1}\mathfrak{P}Q_i$,然除此外則無有p元約羣也.

2°. $\mathfrak{G}$之元素中,其巡回率爲p之倍數者定含於(2)之某一個而且唯一個之內.

蓋若$\mathfrak{G}$之一元素R之巡回率爲p^r,則其冪R^r之巡回率爲p.故$\{R^r\}$非屬於(1)之某一個不可.以之爲

$$\{R^r\}=Q_i^{-1}\mathfrak{P}Q_i,$$

則
$$R\cdot Q_i^{-1}\mathfrak{P}Q_i=R\{R^r\}=\{R^r\}R=Q_i^{-1}\mathfrak{P}Q_i\cdot R.$$

是卽R與$Q_i^{-1}\mathfrak{P}Q_i$爲交換可能也.故R不得不屬於$Q_i^{-1}\mathfrak{N}Q_i$.

次之,若假定此元素R爲含於(2)中二羣如$Q_i^{-1}\mathfrak{N}Q_i$,$Q_j^{-1}\mathfrak{N}Q_j$中,則生p元羣$\{R^r\}$爲含於此二羣內之一結果,是與1°之所述違反乃不合理.故云云.

3°. 於$\mathfrak{N}$,其巡回率爲pb'之約數之元素,與P爲交換可能.

茲以$\mathfrak{N}$之元素S之巡回率s爲pb'之約數.s爲p之倍

故 ps' 時，則巡回羣 $\{S^{s'}\}$，其元數爲 p，因之由 1°，不得不與 $\mathfrak{P}$ 一致也．即

$$\mathfrak{P}=\{S^{s'}\}.$$

$$\therefore \quad P=S^{s'\mu} \quad (0<\mu\leqq p-1)$$

$$\therefore \quad SP=SS^{s'\mu}=S^{s'\mu}S=PS.$$

是即 S 與 P 爲交換可能．

s 不爲 p 之倍數時，乃以 S 將 P 變形，則以 S 與 $\mathfrak{P}$ 爲交換可能故，遂得

$$S^{-1}PS=P^{\lambda} \quad (0<\lambda\leqq p-1).$$

故

$$S^{-s}PS^{s}=P^{\lambda^{s}}.$$

但

$$S^{s}=1.$$

$$\therefore \quad P^{\lambda^{s}}=P.$$

$$\therefore \quad \lambda^{s}\equiv 1 \pmod{p}.$$

然 s 乃 pb' 之約數；而 pb' 之素因數，則由假設，其任何個皆比 $p-1$ 大．故 s 與 $p-1$ 互素．因之欲 $\lambda^{s}\equiv 1 \pmod{p}$，則 $\lambda\equiv 1 \pmod{p}$，隨而 $\lambda=1$ 爲必要也．故

$$S^{-1}PS=P,$$

即 S 與 P 爲交換可能．

4°．$\mathfrak{R}$ 之元素 S 之巡回率 s 爲 pb' 之約數時，傍系 $\mathfrak{P}$ S 之元素

$$(3) \qquad S,\ PS,\ P^{2}S,\ \cdots\cdots,\ P^{p-1}S,$$

無論何個，其巡回率皆爲 pb' 之約數．且此中有 $p-1$ 個其

巡回率爲p之倍數,而其餘一個之巡回率則不爲p之倍數.

蓋由3°, S與P爲交換可能,故

$$(P^tS)^{pb'}=P^{pb't}S^{pb'}$$

但S之巡回率乃pb'之約數,而P之巡回率爲p. 故

$$(P^tS)^{pb'}=1.$$

因之$\mathfrak{P}S$之元素之巡回率爲pb'之約數也.

次之,$\mathfrak{P}S$之元素中,其巡回率不爲p之倍數者,則其巡回率之必爲b'之約數,所當然也. 茲先論S之巡回率不爲p之倍數,因之爲b'之約數者. 此時, P^tS $(0<t\leqq p-1)$之巡回率乃爲p之倍數. 蓋因

$$(P^tS)^{b'}=P^{b't}S^{b'}=P^{b't}\neq 1$$

故. 次之,S之巡回率爲p之倍數ps'時,則因$\{S^{s'}\}$之元數爲p,故由1°,

$$\mathfrak{P}=\{S^{s'}\}.$$

$$\therefore \quad P=S^{s'\mu} \qquad (0<\mu\leqq p-1).$$

故$\mathfrak{P}S$之元素爲

$$(4) \qquad S,\ S^{s'\mu+1},\ S^{2s'\mu+1},\ \cdots\cdots,\ S^{(p-1)s'\mu+1}.$$

是中若$S^{is'\mu+1}$之巡回率不爲p之倍數,則

$$(S^{is'\mu+1})^{b'}=1.$$

$$\therefore \quad b'(is'\mu+1)\equiv 0 \pmod{ps'}.$$

然b'與p爲互素. 故

$$is'\mu+1\equiv 0 \pmod{p}.$$

以 s', μ 皆與 p 互素之故，則滿足此關係之 i 之值，於

$$0,\ 1,\ 2,\ \cdots\cdots,\ p-1$$

之中僅有一個存在也. 故 (4) 卽 (3) 中巡回率不爲 p 之倍數者只一個在. 因之於此時，$\mathfrak{P}S$ 之元素中巡回率爲 p 之倍數者有 $p-1$ 個.

5°. 利用上來諸事項，用歸納法以證明本定理.

$a=1$ 時，卽 a 之素因數之數爲零時，本定理爲自明也.

茲假定 a 之素因數之個數爲 ν，而 a 之素因數之個數少於 ν 個時定理爲眞者.

乃以 p 爲 a 中最大之素因數，則元數爲 $\frac{a}{p}\cdot pb$ 之羣 $\mathfrak{G}$，由假定，其巡回率爲 pb 之約數之元素恰含 pb 個. 此 pb 個中巡回率爲 p 之倍數者，由 2°，各含於 (2) 之一而且唯一之羣中. 故若巡回率爲 pb 之約數又爲 p 之倍數之元素 (2) 之各羣究各含其幾個爲得知時，則此等之總和，乃成爲上述之 pb 元素中其巡回率等於 p 之倍數者之個數也.

於 (2) 之一羣 $\mathfrak{H}$，若對其一元素，巡回率爲 pb 之約數，則必爲 pb' 之約數甚明. (蓋 $\mathfrak{H}$ 之元數爲 $a'pb'$ 而 $a'pb'$ 與 pb 之最大公約數爲 pb' 故). 今以 S 爲如斯之元素，則由 4°，傍系 $\mathfrak{P}S$ 之各元素，其巡回率亦 pb' 之約數也. 故是種之元素，得分爲就 $\mathfrak{P}$ 而分者之傍系.* 然由假定，$\mathfrak{H}$ 之元素中，其巡

* 證明與論羣者全然同樣.

回率爲pb'之約數者，有pb'個(因$\mathfrak{N}$之元數爲$a'\cdot pb'$，而a'爲$\frac{a}{p}$之約數故). 故此等元素就$\mathfrak{H}$而分爲傍系時，則由此所生之傍系之數爲b'個. 但由4°，各傍系所含之巡回率爲p之倍數之元素皆$p-1$個. 故$\mathfrak{N}$中，巡回率爲pb之約數，因之爲pb'之約數而又爲p之倍數之元素，乃有$(p-1)b'$個存在. (2)之他羣，亦全然同樣. (因(2)之各羣與$\mathfrak{N}$爲共軛故.) 因之$\mathfrak{G}$中是類元素之總數爲

$$a''(p-1)b'b''=a''(p-1)b.$$

又自他面觀，在巡回率爲pb之約數之pb個元素中，其巡回率不爲p之倍數者必定存在. (蓋主元素卽其一也.) 故巡回率爲p之倍數者其數少於pb個. 因之

$$a''(p-1)b<pb.$$

$$\therefore\quad (a''-1)(p-1)<1.$$

然a''，p共爲整數. 故

$$a''=1.$$

故於$\mathfrak{G}$，在巡回率爲pb之約數之元素中，其巡回率爲p之倍數者之個數爲$(p-1)b$，因之其不爲p之倍數者之個數爲

$$pb-(p-1)b=b.$$

又巡回率，雖爲pb之約數，然不爲p之倍數時，是不得不爲b之約數也明甚. 故$\mathfrak{G}$含巡回率爲b之約數之元素其b個. 是則a中素因數之個數雖爲ν時，定理亦成立也. 於是歸納法告完結焉.

53. 定理. 若 $p_1, p_2, \cdots\cdots, p_n, p$ 爲互異的 $n+1$ 個素數，而 $p_1<p_2<p_n<p$，則在元數等於 $p_1p_2\cdots\cdots p_np^\alpha$ 之羣 $\mathfrak{G}$ 中，元數爲 $p_{\lambda+1}p_{\lambda+2}\cdots\cdots p_np^\alpha$ 之約羣存在，且其數爲唯一個. 因之此約羣於 $\mathfrak{G}$ 爲正常的. (Frobenius.)

證明. 由 Sylow 氏定理，則 $\mathfrak{G}$ 含有 p^α 元約羣 $\mathfrak{G}_n$. 但由前節之定理，$\mathfrak{G}$ 之元素中，其巡回率爲 p^α 之約數者有 p^α 個. 故 $\mathfrak{G}$ 除 $\mathfrak{G}_n$ 外，不得含 p^α 元羣. 因之 $\mathfrak{G}_n$ 於 $\mathfrak{G}$ 之爲正常，蓋當然也.

次之，試取商 $\mathfrak{G}/\mathfrak{G}_n$，其元數爲 $p_1p_2\cdots\cdots p_n$. 故與前同樣，此商乃含有元數 p_n 之約羣 Γ_n. 然 $\mathfrak{G}$ 與 $\mathfrak{G}/\mathfrak{G}_n$ 爲 p^α 重同態. 故 $\mathfrak{G}$ 必含 p_np^α 元之約羣(與 Γ_n 對應者). 以之爲 $\mathfrak{G}_{n-1}$. p_np^α 元約羣 $\mathfrak{G}_{n-1}$ 之元素，其巡回率爲 p_np^α 之約數；而有若是之巡回率之元素，由前定理，知 $\mathfrak{G}$ 中僅有 p_np^α 個. 故 $\mathfrak{G}$ 除 $\mathfrak{G}_{n-1}$ 以外，無有 p_np^α 元約羣也. 因之 $\mathfrak{G}_{n-1}$ 於 $\mathfrak{G}$ 爲正常.

更取商 $\mathfrak{G}/\mathfrak{G}_{n-1}$，而將前同樣之手續反覆之，便得定理焉.

系. 元數 $p_1p_2\cdots\cdots p_np^\alpha$ 之羣爲可解的. 但 $p_1, p_2, \cdots\cdots, p_n, p$ 爲如定理中之素數.

用定理之證明中之記號，則 $\alpha=1$ 時，

$$\mathfrak{G},\quad \mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_n,\quad 1$$

乃 $\mathfrak{G}$ 之組成列甚明；而其指數列則爲

$$p_1,\quad p_2,\quad \cdots\cdots,\quad p_n,\quad p.$$

次之, $a>1$ 時, $\mathfrak{G}_n$ 中元數爲

$$p^{\alpha-1},\quad p^{\alpha-2},\quad \cdots\cdots,\quad p$$

之正常約羣分別以之爲

$$\mathfrak{G}_{n+1},\quad \mathfrak{G}_{n+2},\quad \cdots\cdots,\quad \mathfrak{G}_{n+a-1},$$

則(參照第47節第一定理)

$$\mathfrak{G},\quad \mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_n,\quad \mathfrak{G}_{n+1},\quad \cdots\cdots,\quad \mathfrak{G}_{n+a-1},\quad 1$$

爲 $\mathfrak{G}$ 之組成列,而其指數列則爲

$$p_1,\quad p_2,\quad \cdots\cdots,\quad p_n,\quad p,\quad p,\quad \cdots\cdots,\quad p.$$

59. 元數不超過 100 之羣之單複.

若 p, q, p_1, p_2, …… 爲素數時,則元數等於

$$p^{\alpha},\quad p^{\alpha}q,\quad p_1p_2\ \cdots\cdots,\quad p_np^{\alpha}\quad (p_1<p_2<\cdots\cdots<p_n<p)$$

之羣,已如第 49, 56, 58 諸節所述,皆爲可解的也. 故對於元數不超過100之羣之單複,僅就下之六種論之爲已足:

$$36=2^2\cdot 3^2,\qquad 60=2^2\cdot 3\cdot 5,\qquad 72=2^3\cdot 3^2,$$

$$84=2^2\cdot 3\cdot 7,\quad 90=2\cdot 3^2\cdot 5,\quad 100=2^2\cdot 5^2.$$

(i) 由 Sylow 氏定理系 1, 則 84 元羣中之 7 元約羣,以及 100 元羣中之 25 元約羣爲正常也.

(ii) 36 元, 72 元羣.

對此兩羣,其 9 元約羣以 $\mathfrak{H}$ 表之. $\mathfrak{H}$ 若非正常,則其共軛約羣之數($\mathfrak{H}$ 亦包含在內),由 Sylow 氏定理,不得不爲 4. 然如第 78 節所述,此時之羣與四次置換羣爲同態,因之爲複合的. 此之證明,以讓於該節,今於此僅記其結果,

謂元數36, 72之羣決非單純的一言而已.

(iii)　90元羣.

設 $\mathfrak{G}$ 爲90元羣, 而 $\{P\}$ 爲其5元羣之一. 若 $\{P\}$ 非正常, 則由Sylow氏定理, $\mathfrak{G}$ 乃有6個之5元約羣, 而 $\{P\}$ 之正常化羣 $\mathfrak{N}$ 之元數爲15. 今就此論之. 乃以 $\mathfrak{N}$ 中3元約羣之一爲 $\{Q\}$, 而以Q將 $\{P\}$ 變形, 則因 $\{P\}$ 於 $\mathfrak{N}$ 爲正常, 故

$$Q^{-1}\{P\}Q=\{P\}.$$

$$\therefore \quad Q^{-1}PQ=P^{x} \qquad (0<x<5).$$

$$\therefore \quad Q^{-3}PQ^{3}=P^{x^3}.$$

然

$$Q^{3}=1.$$

$$\therefore \quad x^{3}\equiv 1 \pmod 5.$$

$$\therefore \quad x\equiv 1 \pmod 5.$$

$$\therefore \quad Q^{-1}PQ=P.$$

即P與Q爲交換可能也. 因之 $\mathfrak{G}$ 中 $\{Q\}$ 之正常化羣不得不含P, 隨而其元數不得不爲P之巡回率5所整除也.

又自他面觀, 含 $\{Q\}$ 之9元約羣 $\mathfrak{L}$ 存在於 $\mathfrak{G}$ (Sylow氏定理系2), 而 $\{Q\}$ 於 $\mathfrak{L}$ 爲正常(第47節第二定理). 故 $\{Q\}$ 之正常化羣, 又不得不爲 $\mathfrak{L}$ 之元數9所整除也. 因之 $\{Q\}$ 之正常化羣之元數爲 $3^2\cdot 5$ 或爲 $2\cdot 3^2\cdot 5$. 以後者論, 則 $\{Q\}$ 爲 $\mathfrak{G}$ 之正常約羣; 以前者論, 則 $\{Q\}$ 之共軛約羣之數($\{Q\}$ 包含在內)爲

$$\frac{2\cdot 3^2\cdot 5}{3^2\cdot 5}=2$$

(第33節定理). 而由第77節所述,則$\mathfrak{G}$與二次置換羣爲同態,而$\{Q\}$之正常化羣爲$\mathfrak{G}$之正常約羣也. 但證明則讓諸該節焉.

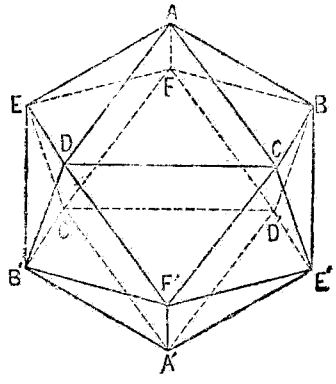
(iv) 60元羣.

此中,其由正二十面體之運動所生者,卽二十面體羣(第17節),如次節所述,乃單純的. 而60元羣,皆與之同態,後自明也. 換言之,若成單純同態之二羣稱爲同型,則60元單羣只有唯一之型焉(參照第79節).

由是以觀,彼元數不超過100之羣,除60元者外,皆複合的也. 故60元羣以外之任何個皆爲可解的.

60. 二十面體羣.

以正二十面體,作與第17節所述者同樣之運動,其所生之羣,乃由次之六十迴轉而成.



(i) 在連結相對之頂點之六個軸AA', BB', CC', DD', EE', FF'之各個周圍之72°, 144°, 216°, 288°之迴轉. 此等運動之總數爲$4\times6=24$.

(ii) 連結對面之中心之十個軸之各個周圍之120°, 240°之迴轉. 此類運動之總數爲$2\times10=20$.

(iii) 連結對稜之中點之十五個軸之各個周圍之 180° 之迴轉. 此等運動之數爲15.

(iv) 全然不動者(此以1表之)

在上之運動中, 軸 AA′ 周圍之 72° 之迴轉* (BCDEF)(B′C′D′E′F′) 以 ((A)) 表之, 則同軸周圍之他三個迴轉得以 $((A))^2$, $((A))^3$, $((A))^4$ 表之也. 而

$$1,\quad ((A)),\quad ((A))^2,\quad ((A))^3,\quad ((A))^4$$

形成二十面體羣(以 $\mathfrak{G}$ 呼之)之5元約羣甚明. 此約羣名曰屬於頂點A或A′之約羣焉. 至對他軸(連結相對頂點者)周圍之迴轉, 其名稱記號均準此推. 於是知((A))與((B))卽 (AFD′E′C)(A′F′DEC′) 共軛也. 此何故歟? 蓋若連結對稜AB, A′B′之中點之軸之周圍之 180° 之迴轉

$$(AB)(CF)(DD')(EE')(C'F')(A'B')$$

以 ((AB)) 表之, 則得

$$((AB))((A))((AB))^{-1}=((B))$$

故也. 由是,

$$((AB))((A))^m((AB))^{-1}=((B))^m \quad (m=2,\ 3,\ 4).$$

因之屬於A之約羣 $\{((A))\}$, 與屬於B之約羣 $\{((B))\}$ 共軛. 同樣對於屬於他之頂點C, D, E, F之約羣, 亦與之共軛. 如是, 屬於各頂點之5元巡回約羣互爲共軛也.

---

*與第17節中同樣, 以運動視爲頂點間之置換, 再以巡回表示示之焉.

其次，在連結對面ABC, A′B′C′之中心之軸之周圍之120°迴轉(ABC)(DFE′)(D′F′E)(A′B′C′)若以((ABC))表之，則在同軸周圍之他之迴轉得以$((ABC))^2$示之也．而

$$1,\quad ((ABC)),\quad ((ABC))^2$$

形成$\mathfrak{G}$之3元巡回約羣甚明．此約羣名曰屬於面ABC或A′B′C′之約羣．至對他面之名稱記號亦復同樣．如是，則((ABC))與((AFB))即(AFB)(CED′)(C′E′D)(A′F′B′)共軛也．蓋因

$$((AB))((ABC))((AB))^{-1}=((AFB))$$

故．由是，

$$((AB))((ABC))^2((AB))^{-1}=((AFB))^2.$$

因之屬於ABC之約羣{((ABC))}與屬於AFB之約羣{((AFB))}共軛．夫如是，屬於相隣二面之約羣互爲共軛也．因之順次取其隣接之面，其屬於各面之約羣之互爲共軛可知也已．

又

$$((A))((AB))((A))^{-1}=((AF)),$$

式之右邊，乃示連結對稜AF, A′F′之中點之軸之周圍之180°之迴轉(AF)(BE)(CC′)(DD′)(A′F′)(B′E′)者也．故若用上同樣之名稱則屬於相隣之稜之二元約羣互爲共軛．因之，順次取其隣接之稜，其屬於各稜之約羣，遂互爲共軛也．

總上所述，$\mathfrak{G}$之元素，由(i), (ii), (iii)，其巡回率之爲5，

3及2，明已．而此約羣之中，5元者任何個皆屬於頂點，因之形成一共軛系．3元者屬於面，亦形成一共軛系．2元者屬於稜，復形成一共軛系也．

今欲證二十面體羣之爲單羣，乃先假定$\mathfrak{N}$爲其正常約羣，其元數爲n．若n爲5之倍數，則$\mathfrak{N}$不得不含5元約羣．但由上所述，$\mathfrak{G}$中之5元約羣形成一共軛系也．故正常約羣$\mathfrak{N}$得含$\mathfrak{G}$中5元約羣之全部．以故n爲5所整除時，則$\mathfrak{N}$遂含(i)中全部之運動．反之，n不爲5之倍數時，則屬於(i)之運動，竟全然不含．(蓋因(i)中各個其巡回率皆爲5故)．因之含於$\mathfrak{N}$之(i)之運動之數，得以$24x$示之也，但x爲1或0焉．

又3元約羣既作一共軛系，故與前同樣，則$\mathfrak{N}$或含(ii)之運動之全部，或竟全然不含也．因之含於$\mathfrak{N}$之(ii)之運動之數爲$20y$ ($y=1$或0)．又2元約羣亦作一共軛系，故含於$\mathfrak{N}$中(iii)之運動之數爲$15z$ ($z=1$或0)．而$\mathfrak{N}$又必含主元素(iv)．故$\mathfrak{N}$之元數如次：

$$n=24x+20y+15z+1.$$

但自他面言，$\mathfrak{G}$之約羣$\mathfrak{N}$之元數n，乃60之約數．爲適合此起見，則上式中x, y, z可取之值，僅

$$x=y=z=1,$$

或

$$x=y=z=0.$$

以前者言，則$n=60$，是則$\mathfrak{N}$與$\mathfrak{G}$一致也．以後者論，則$n=1$，

而 $\mathfrak{P}$ 遂爲主元素羣焉. 於是, 二十面體羣 $\mathfrak{G}$, 除其自身及主元素羣以外, 無有正常約羣, 是卽爲單羣也.

注意. 連結對稜中點之軸, 得分爲由每三個互爲直角交之軸而成之五組. 如過稜 AB, DE, CF′ 之中點者, 卽爲其一組也. 而與之對應之迴轉 ((AB)), ((DE)), ((CF′)), 乃與主元素共作 $\mathfrak{G}$ 中之 4 元約羣焉. 他之組準此. 因之 $\mathfrak{G}$ 含有五個 4 元約羣, 而此諸羣互爲共軛也.

61. 由前二節之所述, 單羣之最小元數爲 60 也. 其次則爲 168. 而迄於 1000 爲正, 其間單羣之元數, 不過

$$60,\ 168,\ 360,\ 504,\ 660$$

之五焉. 而於此各個, 其存在者, 又僅唯一型之單羣已也.

Dickson 氏, 在其著書 Linear Groups 中, 曾揭有元數不超過百萬之羣中其既知之單羣共 53 個之一表. 幷曾示此中元數同而型互異者爲得存在.

表中之單羣, 其元數皆偶數. 於是奇數元單羣之存否, 雖則爲一問題, 第尙未得解決耳.

此外若軼乎本章之範圍, 更思進而論羣之單複, 或討論其可解性, 則 Frobenius 氏所導入之羣指標之應用爲必要, 且甚便宜. 關乎此, 俟第五篇詳之.

第二篇

置換羣

第十章 可遷羣

62. 設 $\mathfrak{G}$ 爲由 n 個文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 上所行之置換而成之羣. 若將某文字如 α, 分別置換於他之文字 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_{n-1}$ 者之置換存在於 $\mathfrak{G}$ 中時, 則 $\mathfrak{G}$ 便含有將任意之文字 α_i 置換於他之任意文字 α_j 者之置換. 蓋若以 α 置換於 α_i 之置換之一爲 S, α 置換於 α_j 之置換之一爲 T, 則積 $S^{-1}T$ 乃置換 α_i 於 α_j 者甚明, 而由羣之定義, 此又屬於 $\mathfrak{G}$ 故也.

如是者之置換羣, 含有將任意選擇之一文字置換於他任意文字之置換時, 名曰**可遷置換羣**, 或單曰**可遷羣**.

如 4 次置換羣

$$1, \quad (ab)(cd), \quad (ac)(bd), \quad (ad)(bc),$$

含有將 a 分別置換於 b, c, d 者之置換. 故爲可遷的.

其次, 若取 4 次置換羣

$$1, \quad (ab), \quad (cd), \quad (ab)(cd),$$

則由此置換，a 決不能置換於 c 或 d 也. 若斯之非可遷的置換羣，乃名曰**非遷的**.

爲語句之簡潔計，乃以由 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 上所行之置換而成之羣，單呼曰 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 之置換羣，而此爲可遷的(或非遷的)時，則稱曰 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 之可遷(或非遷)羣焉.

53. 定理. 設 $\mathfrak{G}$ 爲 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 之可遷羣. 於是

(i) $\mathfrak{G}$ 中一個定文字不動之置換相集而成羣.

(ii) 以 a 不動之置換所作之羣爲 $\mathfrak{H}$，則以 a 置換於 a_i 之置換相集乃作一傍系 $\mathfrak{H}S_i$. 但 S_i 爲以 a 置換於 a_i 之置換之一.

證明. 設 H, H′ 爲 a 不動之兩置換.

(i) 積 HH′ 不能使 a 動甚明. 故不使 a 動之置換之集合，形成 $\mathfrak{G}$ 之約羣* 焉.

(ii) 積 HS_i 之置換 a 於 a_i 明已. 故傍系 $\mathfrak{H}S_i$ 之置換，皆置換 a 於 a_i 者也. 反之，若 T_i 爲將 a 置換於 a_i 之任意的置換 ($\mathfrak{G}$ 的)，則因 S_i^{-1} 置換 a_i 於 a 之故，積 $T_iS_i^{-1}$ 不能使 a 動，因之屬於 $\mathfrak{H}$ 也. 卽

$$T_iS_i^{-1}=H'' \quad (H'' \text{ 爲 } \mathfrak{H} \text{ 之置換}).$$

---

*便宜上遂呼此曰 a 不動之約羣. 而其次數至多不過 $n-1$ 也.

$$\therefore \qquad T_i = H'' S_i.$$

是卽 T_i 屬於 $\mathfrak{H}S_i$ 故云云.

定理. 用前定理之記號, 則

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}S_1 + \cdots\cdots + \mathfrak{H}S_{n-1}.$$

因之可遷羣之元數爲其次數之倍數. 卽

$$g = nh.$$

但 g, h 爲 $\mathfrak{G}$, $\mathfrak{H}$ 之元數.

證明. $\mathfrak{G}$ 之置換, 乃以 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之任何個皆得置換 α 者也. 故由前定理, 是非屬於

$$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{n-1}$$

之或一個不可. 但自他方言, 若 $i \neq j$, 則 $\mathfrak{H}S_i$ 之置換, 乃置換 α 於 α_i, $\mathfrak{H}S_j$ 之置換, 則置換 α 於 α_j, 故兩傍系 $\mathfrak{H}S_i$ 及 $\mathfrak{H}S_j$ 互異. 於是遂得定理中之關係矣.

定理. 於前記之可遷羣 $\mathfrak{G}$, 以其 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 各別不動之置換所作之約羣爲

$$\mathfrak{H}, \mathfrak{H}_1, \cdots\cdots, \mathfrak{H}_{n-1}.$$

於是

(i) 此諸羣皆與 $\mathfrak{H}$ 共軛.

(ii) 凡與 $\mathfrak{H}$ 共軛者, 皆爲此中之某一個.

(iii) 若依 $\mathfrak{H}$ 之任何置換皆不動之文字之數爲 m 個時, 則 $\mathfrak{H}$ 之正常化羣之元數爲 mh, 因之與 $\mathfrak{H}$ 共軛之約羣之

數等於 $\frac{n}{m}$.

證明. (i) 如上所記,若H爲屬於$\mathfrak{H}$之一置換,S_i爲置換 α 於 α_i 者. 則 $S_i^{-1}HS_i$ 不能使 α_i 動甚明,因之屬於$\mathfrak{H}_i$也. 反之,若 H_i 爲屬於$\mathfrak{H}_i$之任意置換,則 $S_iH_iS_i^{-1}$ 不能動 α. 故

$$S_iH_iS_i^{-1}=H' \quad (H' \text{ 爲 } \mathfrak{H} \text{ 之元素}).$$

$$\therefore \quad H_i=S_i^{-1}H'S_i.$$

是卽$\mathfrak{H}_i$之置換屬於$S_i^{-1}\mathfrak{H}S_i$也. 因之

$$\mathfrak{H}_i=S_i^{-1}\mathfrak{H}S_i.$$

(ii) 茲取$\mathfrak{G}$之任意之置換S,則S者,將α置換於$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$之某一個者也. 若在以$\alpha_i$置換之之時,則$S^{-1}\mathfrak{H}S$之置換,皆不足以動$\alpha_i$. 故此乃含於$\mathfrak{H}_i$. 但$\mathfrak{H}_i$與$\mathfrak{H}$,因之與$S^{-1}\mathfrak{H}S$同元數. 故$S^{-1}\mathfrak{H}S$與$\mathfrak{H}_i$一致.

(iii) 今令m個文字

(1) $$\alpha, \ \alpha_1, \ \cdots\cdots, \ \alpha_{m-1}$$

爲雖由$\mathfrak{H}$全部之置換而全然不動者. (但他之文字,則以之爲由$\mathfrak{H}$之某一置換而動者.) 於是$\mathfrak{H}$之置換皆含於$\mathfrak{H}_1$. 但此兩羣爲同元數. 故$\mathfrak{H}_1$不得不與$\mathfrak{H}$一致也. 其他準此. 故得

$$\mathfrak{H}=\mathfrak{H}_1=\cdots\cdots=\mathfrak{H}_{m-1}.$$

今試取將α置換於α_i $(i<m)$之任意置換S,則

$$S^{-1}\mathfrak{H}S=\mathfrak{H}_i=\mathfrak{H},$$

即S與$\mathfrak{H}$爲交換可能也. 反之,以T爲與$\mathfrak{H}$交換可能者,而由此,α得爲α_j($\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$之一)所置換,則

$$\mathfrak{H}_j = \mathrm{T}^{-1}\mathfrak{H}\mathrm{T} = \mathfrak{H}.$$

故α_j不以$\mathfrak{H}$之置換而動. 於是α_j不得不爲(1)之一也. 即與$\mathfrak{H}$交換可能之置換,乃將α置換於(1)之一焉.

要之,與$\mathfrak{H}$交換可能之置換者,乃置換α於(1)之某一個且僅限於此一個者也. 故如斯置換所作之羣即$\mathfrak{H}$之正常化羣,由第一定理爲

$$\mathfrak{H} + \mathfrak{H}\mathrm{S}_1 + \cdots\cdots + \mathfrak{H}\mathrm{S}_{m-1}.$$

但$\mathrm{S}_1, \mathrm{S}_2, \cdots, \mathrm{S}_{m-1}$乃示將$\alpha$分別置換於$\alpha_1, \alpha_2, \cdots\cdots, \alpha_{m-1}$之置換者. 而此羣之元數之爲$mh$則甚明焉.

定理 n次置換羣$\mathfrak{G}$含有n次可遷約羣$\mathfrak{R}$時,若$\mathfrak{G}$中一個定文字不動之約羣爲$\mathfrak{H}$,則

$$\mathfrak{G} = \mathfrak{H}\mathfrak{R}.$$

證明. 命$\mathfrak{G}$之施行置換之文字爲

$$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}.$$

因$\mathfrak{G}$之約羣$\mathfrak{R}$,對此之文字爲可遷的,故$\mathfrak{G}$當然爲可遷的. 今於此以其一定文字α不動之約羣爲$\mathfrak{H}$. 但自他面言,因$\mathfrak{R}$爲可遷的,故$\mathfrak{R}$乃含置換α於文字α_i($i=1, 2, \cdots\cdots, n-1$)之置換. 以其一爲$\mathrm{S}_i$,則積$\mathfrak{H}\mathfrak{R}$乃含傍系$\mathfrak{H}\mathrm{S}_i$($i=1, 2, \cdots\cdots, n-1$). 然由本節第二定理,

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}\mathrm{S}_1 + \cdots\cdots + \mathfrak{H}\mathrm{S}_{n-1}.$$

故 $\mathfrak{H}\mathfrak{K}$ 含有 $\mathfrak{G}$. 反之,以 $\mathfrak{H}$, $\mathfrak{K}$ 共爲 $\mathfrak{G}$ 之約羣之故,積 $\mathfrak{H}\mathfrak{K}$ 之元素皆含於 $\mathfrak{G}$. 因之

$$\mathfrak{H}\mathfrak{K}=\mathfrak{G}.$$

例 1. 在三次對稱羣

$$1,\quad (aa_1a_2),\quad (aa_2a_1),$$
$$(a_1a_2),\quad (aa_2),\quad (aa_1)$$

中,一個定文字不動之約羣爲

$$\mathfrak{H}\ :\ 1,\quad (a_1a_2);$$
$$\mathfrak{H}_1\ :\ 1,\quad (aa_2);$$
$$\mathfrak{H}_2\ :\ 1,\quad (aa_1).$$

又若令 $S_1=(aa_1)$, $S_2=(aa_2)$, 則

$$\mathfrak{H}S_1:\quad (aa_1),\quad (aa_1a_2);$$
$$\mathfrak{H}S_2:\quad (aa_2),\quad (aa_2a_1).$$

例 2. 於六次可遷羣

$$1,\qquad (a_1a_5)(a_2a_4),$$
$$(aa_1a_2a_3a_4a_5),\qquad (aa_5)(a_1a_4)(a_2a_3),$$
$$(aa_2a_4)(a_1a_3a_5),\qquad (aa_4)(a_1a_3),$$
$$(aa_3)(a_1a_4)(a_2a_5),\qquad (aa_3)(a_1a_2)(a_4a_5),$$
$$(aa_4a_2)(a_1a_5a_3),\qquad (aa_2)(a_3a_5),$$
$$(aa_5a_4a_3a_2a_1),\qquad (aa_1)(a_2a_5)(a_3a_4),$$

$$\mathfrak{H}\ :\ 1,\quad (a_1a_5)(a_2a_4);$$
$$\mathfrak{H}_1\ :\ 1,\quad (aa_2)(a_3a_5);$$

$$\mathfrak{H}_2 : 1,\quad (aa_4)a_1a_3);$$

$$\mathfrak{H}_2 : 1,\quad (a_1a_5)(a_2a_4);$$

$$\mathfrak{H}_4 : 1,\quad (aa_2)(a_3a_5);$$

$$\mathfrak{H}_5 : 1,\quad (aa_4)(a_1a_3).$$

64. 多重可遷羣.

設 $\mathfrak{G}$ 爲 n 個文字 $a, a_1, \cdots\cdots, a_{n-1}$ 之置換羣.若此之文字中某 m 個

$$a, a_1, \cdots\cdots, a_{m-1},$$

得以任意之 m 個(n 文字中者)置換元之置換存在於 $\mathfrak{G}$ 中時,則 $\mathfrak{G}$ 乃含有將任意 m 個文字

$$a', a_1', \cdots\cdots, a'_{m-1}$$

以任意之 m 個文字

$$a'', a_1'', \cdots\cdots, a''_{m-1}$$

置換之之置換.蓋若

$$S=\begin{pmatrix} a & a_1, & \cdots\cdots & a_{m-1} & \cdots\cdots \\ a' & a_1' & \cdots\cdots & a'_{m-1} & \cdots\cdots \end{pmatrix},\quad T=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{m-1} & \cdots\cdots \\ a'' & a_1'' & \cdots\cdots & a''_{m-1} & \cdots\cdots \end{pmatrix},$$

則得

$$S^{-1}T=\begin{pmatrix} a' & a_1' & \cdots\cdots & a'_{m-1} & \cdots\cdots \\ a'' & a_1'' & \cdots\cdots & a''_{m-1} & \cdots\cdots \end{pmatrix}$$

故也.

如是,一 n 次置換羣,若含有將任意所選擇之 m 文字得以任意之 m 文字置換之之置換時,則此羣稱曰 m **重可遷**的.如四次交代羣,乃二重可遷的者是也.

定理. 在 n 次 m 重可遷羣中,其一個定文字不動之置換作一 $(n-1)$ 次 $(m-1)$ 重可遷羣.

證明. 設 $\mathfrak{G}$ 爲 n 文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之 m 重可遷羣. α 不動之置換由前節第一定理乃作羣 $\mathfrak{H}$. 今以 $\alpha_1', \alpha_2', \cdots\cdots, \alpha'_{m-1}$ 爲

$$(1) \qquad \alpha_1, \quad \alpha_2, \cdots\cdots, \alpha_{n-1}$$

中任意之 $m-1$ 個,則以 $\mathfrak{G}$ 由假設爲 m 重可遷的之故, $\mathfrak{G}$ 遂含有將 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 置換於 $\alpha, \alpha_1', \cdots\cdots, \alpha'_{m-1}$ 者之置換也. 然此乃 α 不動者,故屬於 $\mathfrak{H}$. 因之 $\mathfrak{H}$ 含有將 $n-1$ 個文字 (1) 中之 $m-1$ 個 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_{m-1}$ 以任意之 $m-1$ 個 ((1) 中者) 置換之之置換. 故 $\mathfrak{H}$ 爲 $(n-1)$ 次 $(m-1)$ 重之可遷的焉.

系. 於 n 次 m 重可遷羣,其特定之 r 文字 $(r<m)$ 不動之置換,形成 $(n-r)$ 次 $(m-r)$ 重之可遷羣.

證明. 於上記之羣 $\mathfrak{G}$, 其二文字 α, α_1 不動之置換,明屬於 $\mathfrak{H}$. 故如斯置換之集合 $\mathfrak{H}_{01}$, 不外乎於 $\mathfrak{H}$ 中其 α_1 不動之置換之集合也. 然 $\mathfrak{H}$ 爲 $(n-1)$ 次 $(m-1)$ 重可遷羣. 故由定理, $\mathfrak{H}_{01}$ 者, $(n-2)$ 次 $(m-2)$ 重可遷者也. 以下準此,爰得本系焉.

定理. n 次 m 重可遷羣之元數爲

$$n(n-1)\cdots\cdots(n-m+1)$$

之倍數.

證明. 於上記之羣 $\mathfrak{G}$, 以文字 α 不動之置換所作約

羣 $\mathfrak{H}$ 之元數爲 h，則 $\mathfrak{G}$ 之元數 g 等於 nh. 然 $\mathfrak{H}$ 由上系爲 $(n-1)$ 次 $(m-1)$ 重可遷. 故於 $\mathfrak{H}$，若 α_1 不動之置換所作約羣 $\mathfrak{H}_{01}$ 之元數爲 h_{01}，則

$$h=(n-1)h_{01}.$$

因之

$$g=n(n-1)h_{01}.$$

但 $\mathfrak{H}_{01}$ 由上系爲 $(n-2)$ 次 $(m-2)$ 重可遷. 故將上同樣方法反覆，遂得

$$g=n(n-1)\cdots\cdots(n-m+1)k.$$

但 k 爲 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 不動之置換 ($\mathfrak{G}$ 的) 所作約羣之元數.

定理. 設 $\mathfrak{G}$ 爲由文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 上所行置換而成之 m 重可遷羣，而 $\alpha', \alpha_1', \cdots\cdots, \alpha'_{m-1}$ 爲此 n 個中之任意 m 個文字. 於是 $\alpha', \alpha_1', \cdots\cdots, \alpha'_{m-1}$ 不動之置換所作之約羣，乃與 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 不動之置換所作之約羣共軛.

證明. 與第 63 節第三定理者同樣.

定理. 於 n 次可遷羣 $\mathfrak{G}$，其一個定文字不動之約羣若爲 $m-1$ 重可遷的，則 $\mathfrak{G}$ 爲 m 重可遷的.

證明. 於 n 文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之可遷羣 $\mathfrak{G}$，其一文字 α 不動之置換之約羣爲 $\mathfrak{H}$，且以之爲 $m-1$ 重可遷的. 而 $\alpha', \alpha_1', \cdots\cdots, \alpha'_{m-1}$ 則爲 n 文字中之任意的 m 個.

因 $\mathfrak{G}$ 爲可遷的，故其含有置換 α' 於 α 者之置換. 以其一爲

$$S=\begin{pmatrix} a\,a'_1\cdots\cdots a'_{m-1}\cdots\cdots \\ a a_1''\cdots\cdots a''_{m-1}\cdots\cdots \end{pmatrix},$$

次之因S爲$m-1$重可遷,故其含有將$a_1'', a_2'', \cdots\cdots, a''_{m-1}$置換於$a_1, a_2, \cdots\cdots, a_{m-1}$之置換. 以其一爲

$$T=\begin{pmatrix} a a_1''\, a_2''\cdots\cdots a''_{m-1}\cdots\cdots \\ a a_1\ \ a_2\ \ \cdots\cdots a_{m-1}\ \ \cdots\cdots \end{pmatrix},$$

則

$$ST=\begin{pmatrix} a\,a_1'\,a_2'\cdots\cdots a'_{m-1}\cdots\cdots \\ a\ a_1\ a_2\ \cdots\cdots a_{m-1}\ \cdots\cdots \end{pmatrix},$$

因之

$$(ST)^{-1}=\begin{pmatrix} a\ a_1\ a_2\ \cdots\cdots a_{m-1}\cdots\cdots \\ a'a_1'\,a_2'\cdots\cdots a'_{m-1}\cdots\cdots \end{pmatrix}.$$

是卽$\mathfrak{G}$含有以任意之m文字得置換$a, a_1, \cdots\cdots, a_{m-1}$者之置換也. 故$\mathfrak{G}$爲$m$重可遷的.

系. 於n次可遷羣,某特定之一文字不動之約羣若爲$m-1$重可遷的,則他之一文字不動之約羣亦復同樣.

證明. 於n文字$a, a_1, \cdots\cdots, a_{n-1}$之可遷羣$\mathfrak{G}$,若$a$不動之約羣$\mathfrak{H}$爲$m-1$重可遷;則由定理,$\mathfrak{G}$爲$m$重可遷. 故由本節第一定理,$a_i$不動之約羣爲$m-1$重可遷.

65. 對稱羣與交代羣.

置換者一般得以表之爲轉換之積者也. 然

$$(a_r a_s)=(a a_r)(a a_s)(a a_r).$$

故n文字

(1) $$a, a_1, \cdots\cdots, a_{n-1}$$

上所行之置換,與將$n-1$個轉換

(2)　　$(\alpha\alpha_1),\ (\alpha\alpha_2),\ \cdots\cdots,\ (\alpha\alpha_{n-1})$

適宜乘之所得之積等. 因之,於由n文字上所行置換而成之羣,若含有(2)中$n-1$個之轉換,卽共有一文字之$n-1$個轉換時,則此羣遂含n文字(1)上所行置換之全數,因之爲對稱的也.

n次對稱羣,以其由n文字上所行全部之置換而成之故,其可遷重複度*之爲n明已. 又n次置換羣,若爲$n-1$重可遷的,則此羣爲n重可遷的,因而爲對稱的. 蓋若將n文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$就任意之順序而取之,而以之爲$\alpha', \alpha_1', \cdots\cdots, \alpha'_{n-1}$,則$n-1$文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-2}$分別爲$\alpha', \alpha_1', \cdots\cdots, \alpha'_{n-2}$所置換者之置換,不得不以$\alpha'_{n-1}$置換$\alpha_{n-1}$也. 卽成爲$\begin{pmatrix}\alpha & \alpha_1, & \cdots\cdots\alpha_{n-1}\\ \alpha' & \alpha_1', & \cdots\cdots\alpha'_{n-1}\end{pmatrix}$. 故云.

復次　　$(\alpha\alpha_r)(\alpha\alpha_s)=(\alpha\alpha_r\alpha_s),$

$$(\alpha\alpha_r\alpha_s)=(\alpha\alpha_1\alpha_s)(\alpha\alpha_1\alpha_r)(\alpha\alpha_1\alpha_s)^2.$$

故n文字(1)上所行之偶數置換卽(2)中轉換之偶數個之積(相等因子之存在亦所容許),乃與$n-2$個之三項巡回置換†

(3)　　$(\alpha\alpha_1\alpha_2),\ (\alpha\alpha_1\alpha_3),\ \cdots\cdots,\ (\alpha\alpha_1\alpha_{n-1})$

適宜乘得之積等. 故於n文字(1)之置換羣,若其共有二

---

*於m重可遷羣,其m名曰其可遷重複度.

†由m個文字而成之巡回置換名曰m項巡回置換.

文字之$n-2$個之三項巡回置換(3)含於其中時,則此羣非含n次交代羣不可也。因之爲交代的或爲對稱的.(n次置換羣皆n次對稱羣之約羣也. 故此羣若含n次交代羣時,則其元數爲$\frac{n!}{2}$或$n!$爲必要. 爲$\frac{n!}{2}$則爲交代的,爲$n!$則爲對稱的.)

定理. n次交代羣爲$n-2$重可遷的. 反之,n次$n-2$重可遷羣爲交代的.

證明. 令$\mathfrak{A}_n$爲由文字$a, a_1, \cdots\cdots, a_{n-1}$上所行置換而成之交代羣. 因

$$(aa_1)(aa_2)=(aa_1a_2).$$

$$(aa_i)(aa_1)=(aa_ia_1) \qquad i=2, 3, \cdots\cdots, n-1,$$

而是等又皆含於$\mathfrak{A}_n$. 故$\mathfrak{A}_n$爲可遷的.

次以a_{n-1}不動之$\mathfrak{A}_n$之約羣爲$\mathfrak{A}_{n-1}$,則$\mathfrak{A}_{n-1}$之爲由$n-1$文字$a, a_1, \cdots\cdots, a_{n-2}$上所行之偶數置換而成甚明. 而由第63節第二定理,此之元數爲

$$\frac{n!}{2}\div n=\frac{(n-1)!}{2}.$$

然$(n-1)$文字上所行之偶數置換之總數爲$\frac{(n-1)!}{2}$. 故$\mathfrak{A}_{n-1}$爲$n-1$次交代羣.

同樣,於$\mathfrak{A}_{n-1}$中其a_{n-2}不動之置換所作之約羣$\mathfrak{A}_{n-2}$,爲$n-2$次交代羣. 以下同樣行之,則$\mathfrak{A}_3$爲三次交代羣

$$1, \quad (aa_1a_2), \quad (aa_2a_1).$$

然$\mathfrak{A}_3$明爲一重可遷. 故由前節第四定理, 則$\mathfrak{A}_4$爲二重可遷, 因而$\mathfrak{A}_5$爲三重可遷, 順次如斯, 遂得$\mathfrak{A}_n$爲$n-2$重可遷也.

反之, 設$\mathfrak{A}$爲由n文字$a, a_1, \cdots\cdots, a_{n-1}$上所行之置換而成之$n-2$重可遷羣. 但不爲$n-1$重可遷者. 於是$\mathfrak{A}$之爲交代的, 得以歸納法而證明之焉.

今假定$n-1$次$n-3$重之可遷羣爲交代的. 於n次$n-2$重可遷羣$\mathfrak{A}$, 其文字a_{n-1}不動之約羣$\mathfrak{B}$, 由前節第一定理, 爲$n-1$文字$a, a_1, \cdots\cdots, a_{n-2}$之$n-3$重可遷羣. 因之由假定爲交代的. 故$\mathfrak{B}$含有$n-3$個之三項巡回置換

$$(aa_1a_2),\quad (aa_1a_3),\quad \cdots\cdots,\quad (aa_1a_{n-2}).$$

同樣, 於$\mathfrak{A}$, 其a_{n-2}不動之約羣乃$n-1$文字$a, a_1, \cdots\cdots, a_{n-3}, a_{n-1}$之$n-3$重可遷羣, 因之含有三項巡回置換

$$(aa_1a_2),\quad \cdots\cdots,\quad (aa_1a_{n-3}),\quad (aa_1a_{n-1}).$$

此之結果, 遂爲$\mathfrak{A}$含有$n-2$個之三項巡回置換

$$(aa_1a_i),\ i=2, 3, \cdots\cdots, n-1,$$

因而由既述, 爲交代的或對稱的也. 若爲對稱羣, 則其可遷重複度爲n, 是與假定反. 故$\mathfrak{A}$不得不爲交代羣也.

自他方言, 次數爲3時, 則$\mathfrak{A}$爲交代的. 蓋此時, $\mathfrak{A}$乃三次一重可遷羣, 因之其置換爲

$$1,\quad (aa_1a_2),\quad (aa_2a_1)$$

爲必要故也. 由是歸納法遂告完結云.

66. 交代羣之單純性.

定理. 5次或5次以上之交代羣爲單純的.

證明. 設$\mathfrak{A}$爲由n文字

$$1, 2, 3, \cdots\cdots, n$$

上所行置換而成之交代羣, 而$\mathfrak{N}$爲$\mathfrak{A}$之正常約羣. 證明之方針, 在首示若$\mathfrak{N}$含有三項巡回置換, 則其與$\mathfrak{A}$得一致, 次則明$\mathfrak{N}$非含三項巡回置換不可. 由是而$\mathfrak{A}$之爲單純得知焉.

1°. 設$\mathfrak{N}$爲含三項巡回置換(123)者. 由前節定理, $\mathfrak{A}$之可遷重複度爲

$$n-2 \geqq 5-2=3,$$

故$\mathfrak{A}$含有以1, 2, i ($i=3, 4, \cdots\cdots, n$)置換1, 2, 3之置換

$$A_i=\begin{pmatrix}123\cdots\cdots\\12i\cdots\cdots\end{pmatrix}.$$

以是變(123)之形, 則有

$$A_i^{-1}(123)A_i=(12i),$$

而由假設$\mathfrak{N}$爲正常, 故此屬於$\mathfrak{N}$. 於是$\mathfrak{N}$含有$(n-2)$個之三項巡回置換

$$(123), (124), \cdots\cdots, (12n),$$

因之由前節所述, 乃與交代羣$\mathfrak{A}$一致也.

2°. 以N爲$\mathfrak{N}$之置換, A爲$\mathfrak{A}$之置換, 而令

$$L=N^{-1}A^{-1}NA.$$

於是因$\mathfrak{N}$爲正常，故$A^{-1}NA$屬於$\mathfrak{N}$，隨之L亦屬於$\mathfrak{N}$.

今將$\mathfrak{N}$之置換，統以巡回表示之，則由此而得起之情況，有次之五種：

(i) 含有四項以上之巡回因子者之置換

$$N=(123\cdots\cdots m)(\cdots)\cdots\cdots \quad (m\geqq 4)$$

爲存在時. 此時取

$$A=(123),$$

則
$$\begin{aligned} L&=[(123\cdots\cdots m)\cdots]^{-1}(123)^{-1}[(123\cdots\cdots m)\cdots](123)\\ &=[(123\cdots\cdots m)\cdots]^{-1}(132)[(123\cdots\cdots m)\cdots](123)\\ &=(243)(123)=(123). \end{aligned}$$

故$\mathfrak{N}$含有三項巡回置換也.

(ii) 含有三項巡回因子兩個者之置換

$$N=(123)(456)\cdots\cdots$$

之存在時. 此時取

$$A=(134),$$

則
$$\begin{aligned} L&=[(123)(456)\cdots\cdots]^{-1}(134)^{-1}[(123)456)\cdots\cdots]\cdot(134)\\ &=[(123)(456)\cdots\cdots]^{-1}(143)[(123)(456)\cdots\cdots]\cdot(134)\\ &=(251)(134)=(12534), \end{aligned}$$

歸於(i)也.

(iii) 含有三項及二項巡回因子者之置換

$$N=(123)(45)\cdots\cdots$$

存在時. 此時取

$$A=(124),$$

則 $$L=[(123)(45)\cdots\cdots]^{-1}(124)^{-1}[(123)(45)\cdots\cdots](124)$$
$$=(253)(124)=(12534),$$

是與前同樣亦歸於(i)也.

(iv) 含有二項巡回因子三個者之置換

$$N=(12)(34)(56)\cdots\cdots$$

之存在時. 此時取

$$A=(135),$$

則 $$L=[(12)(34)(56)\cdots\cdots]^{-1}(135)^{-1}[(12)(34)(56)\cdots\cdots](135)$$
$$=(264)(135),$$

此則歸於(ii)隨之歸於(i)也.

(v) 如 $N=(12)(34)(5)$ 者之置換存在時, 取

$$A=(125),$$

則 $$L=(251)(125)=(152).$$

總上以觀, 可見無論在何情況之下, $\mathfrak{N}$ 非常含三項巡回置換不可也. 故由 1°, $\mathfrak{N}$ 與 $\mathfrak{A}$ 一致.

定理. 對稱羣, 若其次數 n 不小於 5 時, 則除 n 次交代羣及主元素羣以外, 不得有正常眞約羣.

證明. 設 $\mathfrak{S}$ 爲 n 次對稱羣, $\mathfrak{A}$ 爲 $\mathfrak{S}$ 中 n 次交代羣. 若假定 $\mathfrak{S}$ 有異於 $\mathfrak{A}$ 及 1 之正常約羣 $\mathfrak{N}$, 則因 $\mathfrak{A}$ 於 $\mathfrak{S}$ 爲極大正常, 故積 $\mathfrak{N}\mathfrak{A}$ 與 $\mathfrak{S}$ 一致, 而商 $\mathfrak{S}/\mathfrak{A}$ 與 $\mathfrak{N}/\mathfrak{D}$ 爲單純同態也, 但 $\mathfrak{D}$ 爲 $\mathfrak{A}$ 與 $\mathfrak{N}$ 之最大公約羣.

自他面言，$\mathfrak{N}$ 者單純羣也．故 $\mathfrak{D}$ 爲 $\mathfrak{N}$ 或爲 1，是所必要．若 $\mathfrak{D}=\mathfrak{N}$，則 $\mathfrak{N}$ 不得不與 $\mathfrak{S}$ 一致；若 $\mathfrak{D}=1$，則以 $\mathfrak{N}/\mathfrak{D}$ $(=\mathfrak{N})$ 與 $\mathfrak{S}/\mathfrak{N}$ 爲單純同態之故，$\mathfrak{N}$ 之元數不得不爲 2 也．即

$$\mathfrak{N}:\quad 1,\quad N.$$

於是 N 之巡回率既爲 2，故若以巡回表示示之，則如

$$N=(12)(34)\cdots\cdots,$$

其巡回因子皆二項也．此 N 以 $\mathfrak{S}$ 之置換 (23) 變其形，則得

$$(23)N(23)=(13)(24)\cdots\cdots,$$

是與 N 異者也．但 $\mathfrak{N}$ 於 $\mathfrak{S}$ 爲正常．故 $(23)N(23)$ 亦應屬於 $\mathfrak{N}$，因之 $\mathfrak{N}$ 之元數乃較 2 爲大，是爲矛盾．故不能有 $\mathfrak{D}=1$ 者．以故曰 $\mathfrak{S}$ 除自身以外不得有與 $\mathfrak{N}$ 及 1 異之正常約羣也．

注意．含轉換者之二重可遷羣爲對稱的．而含三項巡回置換者之三重可遷羣，則爲交代的或對稱的．

蓋 n 文字 $1, 2, \cdots\cdots, n$ 之置換羣 $\mathfrak{G}$，若爲三重可遷，則含將三文字 r, s, t 分別置換於 $1, 2, i$ $(i=3, 4, \cdots\cdots, n)$ 之置換

$$T_i=\begin{pmatrix} rst\cdots\cdots \\ 12i\cdots\cdots \end{pmatrix}\qquad i=3, 4, \cdots\cdots, n.$$

故此時若 $\mathfrak{G}$ 含有三項巡回置換 (rst)，則以 T_i 變其形，乃有

$$T_i^{-1}(rst)T_i=(12i),\quad i=3, 4, \cdots\cdots, n,$$

而 $\mathfrak{G}$ 遂含 $n-2$ 個之三項巡回置換

$$(123),\quad (124),\quad \cdots\cdots,\quad (12n).$$

故 $\mathfrak{G}$ 須爲交代羣或對稱羣也.

二重可遷羣之含轉換者,其證明全然同樣.

67. 可遷置複度之限界.

定理. 若 n 次可遷羣不含 n 次交代羣時,則其可遷重複度不得超過 $\frac{n+3}{3}$.

證明. 設 $\mathfrak{G}$ 爲 n 文字 $1, 2, 3, \cdots\cdots, n$ 之 m 重可遷羣,而 $m \geqq 3$.

試於 $\mathfrak{G}$ 之置換中,取其移動最少數之文字者(但非不動置換)之一,S. 設由S,有 c 個文字移動,而其巡回表示爲

$$S=(12\cdots\cdots)\cdots\cdots(j+1,\ \cdots\cdots,\ c-1,\ c).$$

今假定 $c \leqq m$,則 $\mathfrak{G}$ 因係 m 重可遷的之故,不得不含將 c 個文字

$$1, 2, 3, \cdots\cdots, c-1, c$$

分別以 $\qquad 1, 2, 3, \cdots\cdots, c-1, d$ (d 與 c 異)

置換之之置換也. 以其一爲

$$T=\begin{pmatrix}1, 2, \cdots\cdots, c-1, c, \cdots\cdots\\ 1, 2, \cdots\cdots, c-1, d, \cdots\cdots\end{pmatrix},$$

則以此變 S 之形,遂得

$$T^{-1}ST=(12\cdots\cdots)\cdots\cdots(j+1,\ \cdots\cdots,\ c-1,\ d),$$

因而

$$S^{-1}T^{-1}ST=(j+1,\ c,\ d).$$

是即$\mathfrak{G}$含有三項之巡回置換也. 但$\mathfrak{G}$之可遷重複度m爲3或較3爲大. 故$\mathfrak{G}$不得不含n次交代羣(參照前節注意). 因之若$\mathfrak{G}$不含此時, 則$c>m$爲必要也.

$c>m$時, 置換S乃有次形之某一個焉. 即

$$S=(12\cdots)\cdots(\cdots, i-1, i)(i+1, \cdots, m-1, m, \cdots)\cdots,$$

$$S=(12\cdots)\cdots(\cdots, m-2)(m-1, m, \cdots)\cdots,$$

或

$$S=(12\cdots)\cdots(\cdots, m-2, m-1)(m, m+1, \cdots)\cdots.$$

茲於$\mathfrak{G}$試取次之一置換U, 即其中有$m-1$文字1, 2, 3, ……, $m-1$不使之動, 而文字m則置換於文字c者:

$$U=\begin{pmatrix}1, 2, \cdots\cdots, m-1, m, \cdots\cdots\\ 1, 2, \cdots\cdots, m-1, c, \cdots\cdots\end{pmatrix},$$

乃以之變S之形, 則對於上三者, 分別有

$$U^{-1}SU=(12\cdots)\cdots(\cdots, i-1, i)(i+1, \cdots, m-1, c, \cdots)\cdots,$$

$$U^{-1}SU=(12\cdots)\cdots(\cdots, m-2)(m-1, c, m+1, \cdots)\cdots,$$

$$U^{-1}SU=(12\cdots)\cdots(\cdots, m-2, m-1)(c, m+1, \cdots)\cdots,$$

而此每一個皆與S不一致. 故於此以S^{-1}左乘之, 其所得之積$S^{-1}U^{-1}SU$決非不動的, 而對於各個, 分別有次之文字

$$1, 2, \cdots\cdots, i, i+2, \cdots\cdots, m-1 \quad (m-2\text{ 個});$$

$$1, 2, \cdots\cdots, m-2 \quad (m-2\text{ 個});$$

及

$$1, 2, \cdots\cdots, m-1 \quad (m-1\text{ 個})$$

之不動者也. 然在出現於兩置換S及$S^{-1}U^{-1}SU$之文字中, 其互異者之總數不得超過$2c-m$(因至少有m個文字1, 2,

……, $m-1$, c 爲兩置換所共通故). 而 $S^{-1}U^{-1}SU$ 則於此諸文字中至少有 $m-2$ 個不使之動. 故由 $S^{-1}U^{-1}SU$, 至多不過有 $2c-2m+2$ 個之文字移動也. 然由假設, ⑤ 爲不含有移動文字少於 c 個之置換(非不動的)者. 故

$$c \leqq 2c-2m+2.$$

由是,

(1) $$c \geqq 2m-2.$$

自他方言, 由置換 U 而移動之文字不多於 $n-m+1$ 個. 故

(2) $$n-m+1 \geqq c.$$

由此與(1), 遂得

(3) $$m \leqq \frac{n+3}{3}.$$

又 $n \geqq 3$ 時, 因

$$\frac{n+3}{3} \geqq 2,$$

故(3)式雖在 m 爲2時亦適合也. 因之可遷重複度 m 與次數 n 之關係式(3), 對於 m 之值, 無例外而告成立焉.

第十一章 非遷羣

68. 由可遷羣以作非遷羣

設 $\mathfrak{G}_a$ 爲 a 文字

(1) $$a, a_1, \cdots\cdots, a_{a-1}$$

之可遷羣，而其元素爲

$$,S_0, S_1, \cdots\cdots, S_{g_\alpha-1}.$$

次以 $\mathfrak{G}_\beta$ 爲 b 文字

$$(2)\qquad \beta, \beta_1, \cdots\cdots, \beta_{b-1}$$

之可遷羣，其元素爲

$$T_0, T_1, \cdots\cdots, T_{g_\beta-1}.$$

且以(2)之文字爲異於(1)者.

今作兩羣之積

$$\mathfrak{G}_\alpha\,\mathfrak{G}_\beta:\quad S_iT_j \begin{cases} i=0, 1, 2, \cdots\cdots, g_\alpha-1, \\ j=0, 1, 2, \cdots\cdots, g_\beta-1, \end{cases}$$

則此明爲由 $(a+b)$ 個之文字(1)及(2)上所行之置換而成之非遷羣，而其元數爲 $g_\alpha g_\beta$ 也.

其次，$\mathfrak{G}_\alpha$ 與 $\mathfrak{G}_\beta$ 爲單純同態時，其相互對應之元素(以之爲 S_i, T_j)相乘而得之 g_α 個積:

$$(3\qquad S_0T_0, S_1T_1, \cdots\cdots, S_{g_\alpha-1}T_{g_\alpha-1}\quad (g_\beta=g_\alpha),$$

乃形成一羣也. 蓋若 $S_iS_j=S_k$，則由同態之定義，乃有 $T_iT_j=T_k$，因之

$$(S_iT_i)(S_jT_j)=S_iS_j\cdot T_iT_j=S_kT_k$$

故耳. 而此羣之爲 $(a+b)$ 次非遷的則甚明焉.

終之，若 $\mathfrak{G}_\alpha$ 與 $\mathfrak{G}_\beta$ 爲重複同態，而於 $\mathfrak{G}_\alpha$ 之主元素，則有 $\mathfrak{G}_\beta$ 之正常約羣 $\mathfrak{H}_\beta$ 相對應，於 $\mathfrak{G}_\beta$ 之主元素，則 $\mathfrak{G}_\alpha$ 之正常約羣 $\mathfrak{H}_\alpha$ 與之對應時，乃先將兩羣分爲傍系:

$$\mathfrak{G}_\alpha=\mathfrak{H}_\alpha+\mathfrak{H}_\alpha P_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\mu-1},$$

$$\mathfrak{G}_\beta=\mathfrak{H}_\beta+\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\beta Q_{\nu-1},$$

而更作其積

$$(4)\qquad \mathfrak{H}_\alpha\mathfrak{H}_\beta,\ \ \mathfrak{H}_\alpha P_1\mathfrak{H}_\beta Q_1,\ \cdots\cdots,\ \mathfrak{H}_\alpha P_{\nu-1}\mathfrak{H}_\beta Q_{\nu-1},$$

但 $\mathfrak{H}_\alpha P_i$ 與 $\mathfrak{H}_\beta Q_i$ 爲相互對應之傍系(參照第 43-45 節). 茲以 $\mathfrak{H}_\alpha$, $\mathfrak{H}_\beta$ 之元數分別爲 h_α, h_β 則 (4) 之各項含有 $h_\alpha h_\beta$ 個之置換,而相異之項則無共通之置換也. 故於(4)其互異置換之總數爲 $\nu h_\alpha h_\beta$. 且此諸置換實乃作羣. 蓋若以 $H_\alpha P_i$, $H_\alpha' P_j$, $H_\beta Q_i$, $H_\beta' Q_j$ 分別爲傍系 $\mathfrak{H}_\alpha P_i$, $\mathfrak{H}_\alpha P_j$, $\mathfrak{H}_\beta Q_i$, $\mathfrak{H}_\beta Q_j$ 中任意之置換,則

$$(H_\alpha P_i H_\beta Q_i)(H_\alpha' P_j H_\beta' Q_j)=(H_\alpha P_i\cdot H_\alpha' P_j)(H_\beta Q_i\cdot H_\beta' Q_j).$$

然

$$H_\alpha P_i\cdot H_\alpha' P_j=H_\alpha'' P_k\quad (H_\alpha''\text{ 爲 }\mathfrak{H}_\alpha\text{ 之元素}),$$

由是且依同態之定理,遂得

$$H_\beta Q_i\cdot H_\beta' Q_j=H_\beta'' Q_k\quad (H_\beta''\text{ 爲 }\mathfrak{H}_\beta\text{ 之元素}).$$

因之

$$(H_\alpha P_i H_\beta Q_i)(H_\alpha' P_j H_\beta' Q_j)=H_\alpha'' P_k H_\beta'' Q_k.$$

故(4)之置換作羣也. 而此亦 $(a+b)$ 次之非遜羣焉.

例 1 $\mathfrak{G}_\alpha$: $1,\quad (\alpha\alpha_1\alpha_2),\quad (\alpha\alpha_2\alpha_1)$;

$\mathfrak{G}_\beta$: $1,\quad (\beta\beta_1)$;

$\mathfrak{G}_\alpha\mathfrak{G}_\beta$:
$$\begin{cases} 1, & (\alpha\alpha_1\alpha_2), & (\alpha\alpha_2\alpha_1) \\ (\beta\beta_1), & (\alpha\alpha_1\alpha_2)(\beta\beta_1), & (\alpha\alpha_2\alpha_1)(\beta\beta_1). \end{cases}$$

例 2.　$\mathfrak{G}_\alpha$: 1, $(a a_1 a_2)$, $(a a_2 a_1)$;

$\mathfrak{G}_\beta$: 1, $(\beta\beta_1\beta_2)$, $(\beta\beta_2\beta_1)$

時, 則

$$1,\quad (a a_1 a_2)(\beta\beta_1\beta_2),\quad (a a_2 a_1)(\beta\beta_2\beta_1)$$

作成六次非遷羣.

例 3. 第 21 節所示之兩羣, 若以之分別視爲 A, B, C, D, E, F 之置換羣及 a, b, c, d, e, f, g, h 之置換羣, 則共爲可遷的. 而如同節所述, 兩者爲同態也. 故其互相對應之置換相乘而得之 24 個之積, 乃作一 14 次 24 元非遷羣焉.

例 4.

$$\mathfrak{G}_\alpha : \begin{cases} 1, & (a a_1 a_2), & (a a_2 a_1), \\ (a a_1), & (a_1 a_2), & (a a_2); \end{cases}$$

$$\mathfrak{H}_\alpha : \quad 1, \quad (a a_1 a_2), \quad (a a_2 a_1);$$

$$\mathfrak{H}_\alpha(a a_1) : \quad (a a_1), \quad (a_1 a_2), \quad (a a_2);$$

$$\mathfrak{G}_\alpha = \mathfrak{H}_\alpha + \mathfrak{H}_\alpha(a a_1).$$

$$\mathfrak{G}_\beta : \quad 1, \quad (\beta\beta_2)(\beta_1\beta_3), \quad (\beta\beta_1\beta_2\beta_3), \quad (\beta\beta_3\beta_2\beta_1);$$

$$\mathfrak{H}_\beta : \quad 1, \quad (\beta\beta_2)(\beta_1\beta_3);$$

$$\mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3) : \quad (\beta\beta_1\beta_2\beta_3), \quad (\beta\beta_3\beta_2\beta_1);$$

$$\mathfrak{G}_\beta = \mathfrak{H}_\beta + \mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3).$$

於兩個可遷羣 $\mathfrak{G}_\alpha$, $\mathfrak{G}_\beta$, 對前者之正常約羣 $\mathfrak{H}_\alpha$ 乃使後者之正常約羣 $\mathfrak{H}_\beta$ 與之對應, 則兩羣之同態明已, 而於傍系 $\mathfrak{H}_\alpha(a a_1)$, 乃有傍系 $\mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3)$ 相對應焉.

於是依上述之方法以作次之積:

$$\mathfrak{H}_\alpha\mathfrak{H}_\beta:\begin{cases}1, & (\alpha\alpha_1\alpha_2), & (\alpha\alpha_2\alpha_1)\\ (\beta\beta_2)(\beta_1\beta_3), & (\alpha\alpha_1\alpha_2)(\beta\beta_2)(\beta_1\beta_3), & (\alpha\alpha_2\alpha_1)(\beta\beta_2)(\beta_1\beta_3);\end{cases}$$

$$\mathfrak{H}_\alpha(\alpha\alpha_1)\mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3):\begin{cases}(\alpha\alpha_1)(\beta\beta_1\beta_2\beta_3), & (\alpha_1\alpha_2)(\beta\beta_1\beta_2\beta_3),\\ (\alpha\alpha_2)(\beta\beta_1\beta_2\beta_3)\\ (\alpha\alpha_1)(\beta\beta_3\beta_2\beta_1) & (\alpha_1\alpha_2)(\beta\beta_2\beta_3\beta_1),\\ (\alpha\alpha_2)(\beta\beta_3\beta_2\beta_1),\end{cases}$$

則此所得之12個置換作一七次非遷羣也.

由 a 次可遷羣 $\mathfrak{H}_\alpha$ 與 b 次可遷羣 $\mathfrak{H}_\beta$, 以上記方法所構成之 $(a+b)$ 次非遷羣, 名曰 $\mathfrak{G}$; 更取 c 次可遷羣 $\mathfrak{H}_\gamma$. 於是由 $\mathfrak{G}$ 以及 $\mathfrak{H}_\gamma$, 依上記之方法得作 $(a+b+c)$ 次非遷羣也. 凡非遷羣皆得由此方法構成, 於第70節自明.

69. 可遷系.

設 $\mathfrak{G}$ 爲 n 次非遷羣, 其施行置換之文字爲

(1) $\qquad a, a_1, \cdots\cdots, a_{n-1}.$

而由 $\mathfrak{G}$ 之置換, 一文字 a 雖得分別置換爲

(2) $\qquad a, a_1, \cdots\cdots, a_{\alpha-1} \qquad (\alpha<n),$

但若以之置換爲他之文字 $a_\alpha, a_{\alpha+1}, \cdots\cdots, a_{n-1}$, 則以爲不可得者. 於是由 $\mathfrak{G}$ 之置換, (2) 之文字, 只能在此等間移動也. 蓋若由 $\mathfrak{G}$ 之置換 G, (2) 之文字 a_i $(i<\alpha)$ 爲置換於 a' 者, 則 $\mathfrak{G}$ 乃含以 a 置換於 a_i 之置換 H, 而因 HG 置換 a 於 a', 故由假設, 則 a' 不得不屬於 (2) 故耳.

又由 $\mathfrak{G}$ 之置換, (2) 之文字得置換於其中之任意一個.

蓋試取(2)之二文字 α_i, α_j, ⑤乃含 α 置換於 α_i 以及 α 置換於 α_j 之兩置換. 以之分別爲 G_1, G_2, 則 $G_1^{-1}G_2$ 乃置換 α_i 於 α_j 故也.

如是, (2) 之文字對於⑤, 於其間得可遷的施行置換. 此一組之文字, 爰呼曰**可遷系**焉.

復次, 試取不屬於(2)之文字 α_a, 由是與前同樣作一可遷系, 則此不得與(2)有共通之文字也. 以之爲

(3)　　$\alpha_a, \alpha_{a+1}, \cdots\cdots, \alpha_{a+b-1}$　$(a+b\leqq n)$.

若以(2)及(3)尙不能盡(1)之全數, 則更取不屬於此兩系之文字而作可遷系. 以同樣方法反覆行之, 則必至將非遷羣⑤之施行置換之文字(1)分爲若干可遷系也.

例. 前節例4之七次非遷羣之可遷系乃爲次之二者:

$$\alpha, \alpha_1, \alpha_2;\quad \beta, \beta_1, \beta_2, \beta_3.$$

70. 非遷羣之構造.

設⑤爲非遷羣. 今將其中施行置換之文字分爲二組: 其一爲可遷系

(1)　　$\alpha, \alpha_1, \cdots\cdots, \alpha_{a-1}$,

其他則爲由剩餘之文字

(2)　　$\beta, \beta_1, \cdots\cdots, \beta_{b-1}$

而成者. 於是取⑤之置換 G, 則

$$G=\begin{pmatrix} \alpha\ \alpha_1\cdots\cdots\alpha_{a-1}\ \beta\ \beta_1\cdots\cdots\beta_{b-1} \\ \alpha'\alpha_1'\cdots\cdots\alpha'_{a-1}\beta'\beta_1'\cdots\cdots\beta'_{b-1} \end{pmatrix},$$

但 α_i' 屬於(1), β_i' 屬於(2). 故若令

$$(3)\qquad S=\begin{pmatrix}\alpha\ \alpha_1\cdots\cdots\alpha_{a-1}\\ \alpha'\alpha_1'\cdots\cdots\alpha'_{a-1}\end{pmatrix},\quad T=\begin{pmatrix}\beta\ \beta_1\beta_2\cdots\cdots\beta_{b-1}\\ \beta'\beta_1'\beta_2'\cdots\cdots\beta'_{b-1}\end{pmatrix},$$

則

$$(4)\qquad G=\begin{pmatrix}\alpha\ \alpha_1\cdots\cdots\alpha_{a-1}\\ \alpha'\alpha_1'\cdots\cdots\alpha'_{a-1}\end{pmatrix}\begin{pmatrix}\beta\ \beta_1\cdots\cdots\beta_{b-1}\\ \beta'\beta_1'\cdots\cdots\beta'_{b-1}\end{pmatrix}=ST.$$

夫如是, $\mathfrak{G}$ 之置換, 乃得以分別於(1)及(2)上所行置換之積而表之者也. 且於 $\mathfrak{G}$ 之置換, 若僅着眼於(1)之文字之移動而以(2)之文字付諸不問, 則上之置換 G 歸於 S; 又若僅注目於(2)之文字之移動, 則 G 歸於 T 焉.

今以 $\mathfrak{G}$ 之置換爲

$$(5)\qquad G_0,\ G_1,\ \cdots\cdots,\ G_{g-1}\quad (G_0=1),$$

而依上記, 將各個分解, 以之爲

$$G_i=S_iT_i\quad (i=0,\ 1,\ 2,\ \cdots\cdots,\ g-1)$$

時, 則

$$(6)\qquad S_0,\ S_1,\ \cdots\cdots,\ S_{g-1}$$

成羣, 而

$$(7)\qquad T_0,\ T_1,\ \cdots\cdots,\ T_{g-1}$$

亦成羣也. 蓋試取(6)之任意之置換 S_i, S_j, 因

$$G_i=S_iT_i,\quad G_j=S_jT_j,$$

故

$$G_iG_j=S_iT_iS_jT_j=S_iS_j\cdot T_iT_j.$$

然 G_iG_j 屬於 $\mathfrak{G}$. 以之爲 G_k, 則

$$G_iG_j=G_k=S_kT_k.$$

故　　$S_iS_j=S_k.$

因之(6)成羣耳. (7)準此. 於是(6)及(7)乃分別以$\mathfrak{G}_\alpha$及G_β表示之焉.

且(1)既爲可遷系,故G_α之爲可遷的甚明. 若$\mathfrak{G}$之可遷系僅有兩個,則$\mathfrak{G}_\beta$雖亦爲可遷的,不如是,則$\mathfrak{G}_\beta$爲非遷的也.

復次,$\mathfrak{G}$與$\mathfrak{G}_\alpha$及$\mathfrak{G}_\beta$爲同態. 蓋於$\mathfrak{G}$之置換G_i,使$\mathfrak{G}_\alpha$之置換S_i對應,則因

$$G_iG_j=S_iS_j\cdot T_iT_j$$

之故,對於積G_iG_j,有對應置換之積S_iS_j相應也. 因之$\mathfrak{G}$與$\mathfrak{G}_\alpha$同態. 就$\mathfrak{G}_\beta$言,亦復同樣. 故云

但此同態卻不限於單純. 卽(6)或(7)之中,相等置換存在時,同態遂爲重複也.

上記之對應成立時,以與$\mathfrak{G}_\alpha$之主元素對應之$\mathfrak{G}$之正常約羣爲$\mathfrak{H}_\beta$,則$\mathfrak{H}_\beta$之元素,乃得表之爲$1\cdot T$之形,但T爲示(2)之文字上所行之置換者. 因之$\mathfrak{H}_\beta$爲$\mathfrak{G}_\beta$之約羣. 又以對應於$\mathfrak{G}_\beta$之主元素之$\mathfrak{G}$之正常約羣爲$\mathfrak{H}_\alpha$,則$\mathfrak{H}_\alpha$爲$\mathfrak{G}_\alpha$之約羣.

次乘$\mathfrak{H}_\alpha$與$\mathfrak{H}_\beta$,若兩者之元數分別爲h_α, h_β,則積之元數爲$h_\alpha h_\beta$. (蓋兩者共於$\mathfrak{G}$爲正常,且無有共通之元素故.)茲於$\mathfrak{H}_\alpha\mathfrak{H}_\beta$,若僅注目於文字(1)間之移動,則此之爲$\mathfrak{H}_\alpha$甚明.

故於 $\mathfrak{G}$ 與 $\mathfrak{G}_\alpha$ 之同態關係，對於前者之正常約羣 $\mathfrak{H}_\alpha\mathfrak{H}_\beta$，則後者之正常約羣 $\mathfrak{H}_\alpha$ 相與對應也．因之 $\mathfrak{G}/\mathfrak{H}_\alpha\mathfrak{H}_\beta$ 與 $\mathfrak{G}_\alpha/\mathfrak{H}_\alpha$ 爲單純同態．同樣，對於 $\mathfrak{G}$ 之約羣 $\mathfrak{H}_\alpha\mathfrak{H}_\beta$，乃有 $\mathfrak{G}_\beta$ 之約羣 $\mathfrak{H}_\beta$ 相對應，隨而 $\mathfrak{G}/\mathfrak{H}_\alpha\mathfrak{H}_\beta$ 與 $\mathfrak{G}_\beta/\mathfrak{H}_\beta$ 爲單純同態焉．

(i) $\mathfrak{G}=\mathfrak{H}_\alpha\mathfrak{H}_\beta$ 時．此時若僅注目於文字(1)間之移動，則以 $\mathfrak{G}$ 成爲 $\mathfrak{H}_\alpha$ 之故，

$$\mathfrak{G}_\alpha=\mathfrak{H}_\alpha.$$

同樣，

$$\mathfrak{G}_\beta=\mathfrak{H}_\beta.$$

因之 $\mathfrak{G}$ 乃與分別於文字(1)及(2)上所行之兩個可遷羣之直乘積等．

(ii) $\mathfrak{H}_\alpha\mathfrak{H}_\beta$ 爲 $\mathfrak{G}$ 之眞約羣時．以 $\mathfrak{G}$ 分爲傍系，命爲

$$\mathfrak{G}=\mathfrak{H}_\alpha\mathfrak{H}_\beta+\mathfrak{H}_\alpha\mathfrak{H}_\beta K_1+\cdots\cdots+\mathfrak{H}_\alpha\mathfrak{H}_\beta K_{\nu-1}.$$

然

$$K_i=P_iQ_i \quad (i=1, 2, \cdots\cdots, \nu-1),$$

但 P_i, Q_i 乃示分別於文字(1)及(2)上所行之置換者．故

$$(8)\quad \mathfrak{G}=\mathfrak{H}_\alpha\mathfrak{H}_\beta+\mathfrak{H}_\alpha P_1\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\nu-1}\mathfrak{H}_\beta Q_{\nu-1}.$$

今於 $\mathfrak{G}$ 之置換，若僅注目於文字(1)之移動，則於上式，$\mathfrak{G}$ 遂爲 $\mathfrak{G}_\alpha$，而右邊之各傍系分別成爲

$$(9)\quad \mathfrak{H}_\alpha, \mathfrak{H}_\alpha P_1, \cdots\cdots, \mathfrak{H}_\alpha P_{\nu-1}.$$

而於 $\mathfrak{G}$ 與 $\mathfrak{G}_\alpha$ 之同態關係，對於 $\mathfrak{G}$ 之傍系 $\mathfrak{H}_\alpha P_i\mathfrak{H}_\beta Q_i$ 乃有 $\mathfrak{G}_\alpha$ 之傍系 $\mathfrak{H}_\alpha P_i$ 相與對應．但以重複同態言，與互異傍系對應者爲互異傍系．故(9)之傍系互異也．因之得

$$(10)\quad \mathfrak{G}_\alpha=\mathfrak{H}_\alpha+\mathfrak{H}_\alpha P_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\nu-1}.$$

同樣

$$(11)\qquad \mathfrak{G}_\beta=\mathfrak{H}_\beta+\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\beta Q_{\nu-1}.$$

而於$\mathfrak{G}$之傍系$\mathfrak{H}_\alpha P_i\mathfrak{H}_\beta Q_k$, $\mathfrak{G}_\beta$之傍系$\mathfrak{H}_\beta Q_i$相與對應. 於是$\mathfrak{G}_\alpha$與$\mathfrak{G}_\beta$爲重複同態, 傍系$\mathfrak{H}_\alpha P_i$與傍系$\mathfrak{H}_\beta Q_i$相對應也.

就上三式(8), (10), (11)而觀, 可知非遷羣$\mathfrak{G}$, 乃與在彼成$h_\alpha-h_\beta$同態之二羣$\mathfrak{G}_\alpha$, $\mathfrak{G}_\beta$中乘其相互對應之傍系所得者等也.

特別當$\mathfrak{H}_\alpha$, $\mathfrak{H}_\beta$共爲主元素羣時, $\mathfrak{G}_\alpha$, $\mathfrak{G}_\beta$乃互成單純同態, 而$\mathfrak{G}$遂由兩者之對應元素之積而成. 總合上述, 爰得

定理. 非遷羣, 或爲置換羣之直乘積, 或爲在同態的置換羣中乘其對應傍系所得之積之集合.

系1. 在非遷羣中施行置換之文字得分爲兩個可遷系時, 則此羣爲兩個可遷羣之直乘積, 或爲同態可遷羣之對應傍系相乘所得之積之集合.

又上記之$\mathfrak{G}_\beta$爲非遷的時, 則將本節中對$\mathfrak{G}$所施之考察, 同樣以施諸$\mathfrak{G}_\beta$乃得次系.

系2. 非遷羣之有l個可遷系者, 得由l個可遷羣而構成之.

一般, 構成一個非遷羣之可遷羣, 名曰此非遷羣之可遷構成羣.*

*由僅注目於一個可遷系中文字之移動, 而自非遷羣所得之可遷羣, 卽可遷構成羣者也.

例 1. 在六次非遷羣

$$\mathfrak{G}:\begin{cases} 1, & (ab), \quad (cd), \quad (ef), \quad (ab)(cd)(ef), \\ (ab)(cd), & (ab)(ef), \quad (cd)(ef) \end{cases}$$

中之文字得分爲三個可遷系:

$$a, b; \quad c, d; \quad e, f.$$

若僅注目於二文字 a, b 之移動, 則 $\mathfrak{G}$ 遂成

$$\mathfrak{G}_\alpha : \quad 1, \quad (ab);$$

而僅着眼於他文字之移動, 則爲

$$\mathfrak{G}_\beta : \quad 1, \quad (cd), \quad (ef), \quad (cd)(ef);$$

而

$$\mathfrak{G} = \mathfrak{G}_\alpha \mathfrak{G}_\beta.$$

又 $\mathfrak{G}_\beta$ 等於兩個可遷羣 $\{1, (cd)\}$, $\{1, (ef)\}$ 之直乘積. 因之 $\mathfrak{G}$ 由三個可遷羣

$$\{1, (ab)\}, \quad \{1, (cd)\}, \quad \{1, (ef)\}$$

所構成.

例 2. 在八次非遷羣

$$\mathfrak{G}:\begin{cases} 1, \quad (12)(34), \quad (56), \quad (12)(34)(56), \\ (13)(24)(78), \quad (13)(24)(56)(78), \\ (14)(23)(78), \quad (14)(23)(56)(78) \end{cases}$$

中文字

$$(\alpha) \qquad 1, 2, 3, 4$$

作一可遷系. 將文字分爲此與他之組

$$(\beta) \qquad 5, 6, 7, 8,$$

而$\mathfrak{G}$之置換，依本節之方法分解之，則得

$$1\cdot 1,\quad (12)(34)\cdot 1,\quad 1\cdot(56),\quad (12)(34)\cdot(56),$$
$$(13)(24)\cdot(78),\quad (13)(24)\cdot(56)(78),$$
$$(14)(23)\cdot(78),\quad (14)(23)\cdot(56)(78).$$

今於此僅注目於(α)之文字之移動，則$\mathfrak{G}$爲

$$\mathfrak{G}_\alpha:\quad 1,\quad (12)(34),\quad (13)(24),\quad (14)(23);$$

若僅視(β)之文字之移動，則爲

$$\mathfrak{G}_\beta:\quad 1,\quad (56),\quad (78),\quad (56)(78).$$

而與$\mathfrak{G}_\beta$之主元素對應之$\mathfrak{G}$之正常約羣，則由上之分解得知爲

$$\mathfrak{H}_\alpha:\quad 1,\quad (12)(34);$$

而對應於$\mathfrak{G}_\alpha$之主元素者爲

$$\mathfrak{H}_\beta:\quad 1,\quad (56)$$

也．將$\mathfrak{G}_\alpha$及$\mathfrak{G}_\beta$分別就$\mathfrak{H}_\alpha,\mathfrak{H}_\beta$分爲傍系，則得

$$\mathfrak{G}_\alpha=\mathfrak{H}_\alpha+\mathfrak{H}_\alpha(13)(24),\quad \mathfrak{G}_\beta=\mathfrak{H}_\beta+\mathfrak{H}_\beta(78).$$

而
$$\mathfrak{H}_\alpha\mathfrak{H}_\beta:\quad 1,\quad (12)(34),\quad (56),\quad (12)(34)(56);$$

$$\mathfrak{H}_\alpha(13)(24)\cdot\mathfrak{H}_\beta(78):\begin{cases}(13)(24)(78), & (13)(24)(56)(78),\\ (14)(23)(78), & (14)(23)(56)(78);\end{cases}$$

兩積之集合形成$\mathfrak{G}$．若更將$\mathfrak{G}_\beta$分解，則$\mathfrak{G}$之可遷構成羣，知爲次之三也：

$$\{1,\quad (12)(34),\quad (13)(24),\quad (14)(23)\},$$
$$\{1,(56)\},\quad \{1,(78)\}.$$

注意. 本節中非遷羣$\mathfrak{G}$之置換G, 分解爲

$$G=ST\ (S, T\text{分別爲}\mathfrak{G}_\alpha, \mathfrak{G}_\beta\text{之元素})$$

時, 則如上述已明, 無論於(i)或(ii), 若$S=1$, 則T屬於$\mathfrak{H}_\beta$也. 故對$S=1$, 若$T=1$, 則$\mathfrak{H}_\beta=1$. 又$T=1$時, 若$S=1$, 則對(i), 乃有$\mathfrak{G}=\mathfrak{H}_\alpha\mathfrak{H}_\beta=1$; 而於(ii), 二羣$\mathfrak{G}_\alpha\mathfrak{G}_\beta$爲單純同態, 而其對應元素之積乃作$\mathfrak{G}$. 故$\mathfrak{G}$之置換, 表示爲其可遷構成羣中之置換之積時, 一因子若爲不動的, 則在他亦爲不動的之際, 構成羣遂互爲單純同態, 而其對應元素之相乘積形成$\mathfrak{G}$也. 因之$\mathfrak{G}$之元數與構成羣之元數一致.

71. 不動文字之數.

定理. 於g元n次置換羣, 若其不動文字恰爲r個者之置換之數以ν_r表之, 則

$$\nu_1+2\nu_2+\cdots\cdots+n\nu_n=lg.$$

但l, 若羣爲可遷的, 則等於1; 若爲非遷的, 則表示可遷系之數.

此如換言之, 卽謂在g元n次置換羣中, 其由置換而不動之文字之總數等於lg也. 但文字對於各置換, 分別逐回計算焉. 是卽以對於羣之全部置換, 爲總計有ng個文字在, 而其中之不動者, 乃如上述者也.

證明. 設$\mathfrak{G}$爲由文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$上所行之置換而成之$g$元羣.

1°. 可遷者時.

令$\mathfrak{H}$爲文字α不動之$\mathfrak{G}$之約羣，而就之分$\mathfrak{G}$爲傍系：

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1},$$

但S_i爲表置換α於α_i之置換者．於是$\mathfrak{G}$中其至少一個文字不動之置換，非含於

(1)　　$\mathfrak{H}, S_1^{-1}\mathfrak{H}S_1, \cdots\cdots, S_{n-1}^{-1}\mathfrak{H}S_{n-1}$

中之一個不可也(參照第63節)．今於$\mathfrak{H}$，其r個文字不動之置換之數爲ν_r'，* 則就(1)之各個皆爲同樣．故在屬於(1)中各羣之全部置換之中，其r個文字不動之置換之總數爲$n\nu_r'$也．然(1)之置換中，r個文字不動者，乃(1)中r個羣之所共通．故(1)之置換中，r個文字不動，且互異者，其數爲$\frac{n\nu_r'}{r}$個．是卽$\mathfrak{G}$中此類置換之數也．故

$$\frac{n\nu_r'}{r}=\nu_r.$$

自他方言，因$\mathfrak{H}$之元數爲$\frac{g}{n}$，故

$$\nu_1'+\nu_2'+\cdots\cdots+\nu_n'=\frac{g}{n}$$

甚明．茲於此代入前式，遂得

$$\nu_1+2\nu_2+\cdots\cdots+n\nu_n=g.$$

2°．非遷者時．

將施行置換之文字，與前節同樣，分爲可遷系

---

*$\mathfrak{H}$之置換，皆視爲在n文字上所施行者，乃以其r個文字不動之置換之數爲ν_r'焉．

(1) $$\alpha, \alpha_1, \cdots\cdots, \alpha_{a-1}$$

及剩餘之文字

(2) $$\beta, \beta_1, \cdots\cdots, \beta_{b-1} \quad (a+b=n)$$

兩組，而以屬於可遷系(1)之可遷構成羣爲$\mathfrak{G}_\alpha$，以僅注目於(2)之文字之移動時由$\mathfrak{G}$所生之羣爲$\mathfrak{G}_\beta$. 於是由前節，或爲

(3) $$\mathfrak{G}=\mathfrak{G}_\alpha\mathfrak{G}_\beta,$$

或爲

(4) $$\mathfrak{G}=\mathfrak{H}_\alpha\mathfrak{H}_\beta+\mathfrak{H}_\alpha P_1\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\mu-1}\mathfrak{H}_\beta Q_{\mu-1},$$

但

(5) $$\begin{cases}\mathfrak{G}_\alpha=\mathfrak{H}_\alpha+\mathfrak{H}_\alpha P_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\mu-1}\\ \mathfrak{G}_\beta=\mathfrak{H}_\beta+\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\beta Q_{\mu-1}\end{cases}$$

茲請先就後者而將定理證明之. 令$\mathfrak{H}_\alpha$, $\mathfrak{H}_\beta$之元素分別爲

$$\mathfrak{H}_\alpha: \quad A_0, A_1, \cdots\cdots, A_{h_\alpha-1},$$

$$\mathfrak{H}_\beta: \quad B_0, B_1, \cdots\cdots, B_{h_\beta-1},$$

則由(5)其構成羣之置換，分別得以

$$\mathfrak{G}_\alpha: \quad A_iP_s \begin{cases} i=0, 1, 2, \cdots\cdots, h_\alpha-1 \quad [\mu h_\alpha=g_\alpha] \\ s=0, 1, 2, \cdots\cdots, \mu-1 \quad [P_0=1]\end{cases}$$

$$\mathfrak{G}_\beta: \quad B_jQ_s \begin{cases} j=0, 1, 2, \cdots\cdots, h_\beta-1 \quad [\mu h_\beta=g_\beta] \\ s=0, 1, 2, \cdots\cdots, \mu-1 \quad [Q_0=1]\end{cases}$$

與之，而$\mathfrak{G}$之置換則爲

$$A_iP_s\cdot B_jQ_s \quad [\mu h_\alpha h_\beta=g].$$

由是以觀，$\mathfrak{G}_\alpha$ 中同一之置換乃作 $\mathfrak{G}$ 之置換之因子而出現 h_β 回也. 但可遷羣 $\mathfrak{G}_\alpha$，其不動文字之數，由 1°，知總計爲 g_α. 故當計算 $\mathfrak{G}$ 中不動文字之數時，先將置換分爲屬於 $\mathfrak{G}_\alpha$ 之置換與屬於 $\mathfrak{G}_\beta$ 之置換之積，而僅就屬於 $\mathfrak{G}_\alpha$ 之因子而計算之，則不動文字之數爲 $g_\alpha h_\beta$ 也. 將此數換書之，則得

$$g_\alpha h_\beta = \mu h_\alpha h_\beta = g,$$

是卽屬於可遷系 (1) 之文字，由 $\mathfrak{G}$ 之置換而不動者，其回數總計爲 g 也. 他之可遷系準此. 因之若 $\mathfrak{G}$ 中可遷系之數爲 l，則由此置換而不動之文字，其總數爲 lg 焉.

$\mathfrak{G}=\mathfrak{G}_\alpha\mathfrak{G}_\beta$ 時，亦同樣得證明之.

例 1. 於四次交代羣

$$1,\ (bcd),\ (cad),\ (dab),\ (acb),$$
$$(bdc),\ (cda),\ (dba),\ (abc),$$
$$(ab)(cd),\ (ac)(bd),\ (ad)(bc),$$

$$\nu_0=3,\quad \nu_1=8,\quad \nu_2=0,\quad \nu_3=0,\quad \nu_4=1,$$

$$\therefore\quad \nu_1+2\nu_2+3\nu_3+4\nu_4=8+4\cdot 1=12.$$

例 2. 於十二元七次非遷羣(第 68 節例 4 參照)

$$\begin{array}{ccc} 1 & (xyz) & (xzy) \\ (ae)(bd) & (xyz)(ac)(bd) & (xzy)(ac)(bd) \\ (xy)(abcd) & (yz)(abcd) & (zx)(abcd) \\ (xy)(adcb) & (yz)(adcb) & (zx)(adcb), \end{array}$$

$$\nu_0=2,\ \nu_1=6,\ \nu_2=0,\ \nu_3=1,\ \nu_4=2,\ \nu_5=0,\ \nu_6=0,\ \nu_7=1.$$

$$\therefore\quad \nu_1+2\nu_2+\cdots\cdots+7\nu_7=6+3\cdot1+4\cdot2+7\cdot1=2\cdot12.$$

是卽不動文字之數與乘可遷系之數2於元數者等也.

72. 由正置換而成之羣.

在一個置換之巡回表示中,其巡回因子皆由同數之文字而成時,則此置換曰正置換(第7節). 而其巡回率,則等於各巡回因子中文字之數也. 今後正置換所施行之文字之數,名曰其次數焉.

如四次置換羣

$$1,\qquad (ab)(cd),$$
$$(ac)(bd),\qquad (ad)(bc)$$

然,若n次可遷羣僅由n次正置換而成時,則稱之曰**正置換羣**. 此時由羣之置換(非不動者),所有文字皆動. 卽一文字不動之約羣,乃主元素羣. 故由第63節第二定理,正置換羣之元數與次數一致也.

反之,元數與次數相等之可遷羣爲正置換羣. 蓋試取此羣之一置換$G(\neq1)$,其巡回表示以之爲

$$G=(\alpha\alpha_1\cdots\cdots\alpha_{a-1})(\beta\beta_1\cdots\beta_{b-1})\cdots\cdots.$$

a不等於b時,若$a<b$,則得

$$G^a=(\beta\beta_1\cdots\cdots\beta_{b-1})^a\cdots\cdots$$

而此乃α不動且非不動置換. 故在此可遷羣中,文字α不動之約羣之元數大於1,因之羣之元數遂大於其次數(第63節第二定理). 以故在次數與元數一致時,則其不得不

爲正置換羣也.

復次,羣之僅由正置換而成者,如

$$1,\quad (abc)(xyz),\quad (acb)(xzy)$$

然之非遷的時,乃有次之

定理. *n次非遷羣$\mathfrak{G}$,僅由n次正置換而成時,則其可遷構成羣,皆爲次數等於$\mathfrak{G}$之元數之正置換羣,且互爲單純同態. 而$\mathfrak{G}$則由可遷構成羣中互相對應之元素相乘而得之積而成.*

證明. 以$\mathfrak{G}$之可遷構成羣爲$\mathfrak{G}_\alpha, \mathfrak{G}_\beta, \cdots\cdots$,其各個之次數分別爲$a, b, \cdots\cdots$. 於是$\mathfrak{G}$之元素G,得分解爲

$$G = ST\cdots\cdots$$

之形. 但S, T, ……分別爲屬於$\mathfrak{G}_\alpha, \mathfrak{G}_\beta, \cdots\cdots$之置換.

今$\mathfrak{G}_\alpha$乃a次之正置換羣也. 蓋若S爲非a次之正置換,則與上示者同樣,以之高至於適當之冪,則於a文字之中,由S而不動者生焉,此文字者,由G之同冪而不動者也. 是則與G爲n文字之正置換之假設矛盾. 故云.

他之構成羣亦同樣爲正置換羣.

次之,$\mathfrak{G}$之元素G既爲n次正置換,故若其一因子S爲不動置換,則他之因子T, …… 亦不得不爲不動的明也. 又他之一因子爲不動的時,亦復同樣. 故有如第70節之所注意,構成羣$\mathfrak{G}_\alpha, \mathfrak{G}_\beta \cdots\cdots$爲單純同態,而其對應元素之相乘積則形成$\mathfrak{G}$也. 因之構成羣之元數與$\mathfrak{G}$之元數一致.

又構成羣既爲正置換羣，則如前所述，其次數與元數一致也．故定理云云．

系．僅由n次正置換而成之n次置換羣之元數，乃n之約數．（此系由前節之定理亦易導出之．）

第十二章 羣之置換表示

73. 表爲正置換羣者．

設$\mathfrak{G}$爲g元羣，

$$(1)\qquad G_0,\ G_1,\ \cdots\cdots,\ G_{g-1}\quad (G_0=1)$$

爲其元素．於此各個，以$\mathfrak{G}$之任意一元素G_i右乘之，其所得之g個元素

$$(2)\qquad G_0G_i,\ G_1G_i,\ \cdots\cdots,\ G_{g-1}G_i,$$

不外乎將(1)置換於某順序者而已也．故對元素G_i乃得元素間之置換：

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}.$$

便宜上以$\begin{pmatrix} G \\ GG_i \end{pmatrix}$表之，則對$\mathfrak{G}$之$g$元素乃得$g$個之置換：

$$(3)\qquad \begin{pmatrix} G \\ GG_0 \end{pmatrix},\ \begin{pmatrix} G \\ GG_1 \end{pmatrix},\ \cdots\cdots,\ \begin{pmatrix} G \\ GG_{g-1} \end{pmatrix};$$

且彼此互異．蓋若

$$\begin{pmatrix} G \\ GG_i \end{pmatrix}=\begin{pmatrix} G \\ GG_j \end{pmatrix},$$

即 $\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix} = \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_j & G_1G_j & \cdots\cdots & G_{g-1}G_j \end{pmatrix}$,

則 $$G_0G_i = G_0G_j \quad (G_0 = 1)$$

即 $$G_i = G_j$$

爲必要故也.

其次(3)之置換乃成羣. 蓋若作(3)之二置換 $\begin{pmatrix} G \\ GG_i \end{pmatrix}$ 及 $\begin{pmatrix} G \\ GG_j \end{pmatrix}$ 之積,則以

$$(4) \qquad \begin{pmatrix} G \\ GG_j \end{pmatrix} = \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_j & G_1G_j & \cdots\cdots & G_{g-1}G_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \\ G_0G_i \cdot G_j & G_1G_i \cdot G_j & \cdots\cdots & G_{g-1}G_i \cdot G_j \end{pmatrix}$$

之故,* 遂得

$$(5) \qquad \begin{pmatrix} G \\ GG_i \end{pmatrix}\begin{pmatrix} G \\ GG_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}\begin{pmatrix} G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \\ G_0G_i \cdot G_j & G_1G_i \cdot G_j & \cdots\cdots & G_{g-1}G_iG_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0 \cdot G_iG_j & G_1 \cdot G_iG_j & \cdots\cdots & G_{g-1} \cdot G_iG_j \end{pmatrix} = \begin{pmatrix} G \\ G \cdot G_iG_j \end{pmatrix}.$$

而積 G_iG_j 屬於 $\mathfrak{G}$. 故(3)成羣焉.

就羣(3)而觀,因 $G_0G_i = G_i$,故此羣乃含將 G_0 置換於他之任意的 G_i 之置換,是爲可遷的. 且其次數與元數 g 等.

---

*置換 $\begin{pmatrix} G \\ GG_j \end{pmatrix}$,乃示 $\mathfrak{G}$ 之各元素,得以右乘 G_j 於此元素所得之積而置換之者也. 故得(4)式焉.

於是由前節所述,(3)爲正置換羣也.

終之,(3)與 $\mathfrak{G}$ 同態. 蓋若對 $\mathfrak{G}$ 之元素 G_i, 使(3)之置換 $\begin{pmatrix} G \\ GG_i \end{pmatrix}$ 與之對應時,若

$$G_iG_j=G_k,$$

則對 G_k 乃有置換 $\begin{pmatrix} G \\ GG_k \end{pmatrix}$ 即 $\begin{pmatrix} G \\ G\cdot G_iG_j \end{pmatrix}$ 相對應. 然由(5),

$$\begin{pmatrix} G \\ G\cdot G_iG_j \end{pmatrix}=\begin{pmatrix} G \\ GG_i \end{pmatrix}\begin{pmatrix} G \\ GG_j \end{pmatrix},$$

故對積 G_iG_j 乃有分別對應之置換之積相對應. 故 $\mathfrak{G}$ 與(3)同態. 而兩羣之元數共爲 g, 故此同態爲單純也.

總上所述,乃得次

定理. 對於一個 g 元羣,得作與之單純同態之 g 次正置換羣. 即 g 元羣得表之爲 g 次正置換羣也.

一般,對於一個羣,得作與之同態(單純或重複)之置換羣者,名曰以置換羣表示一羣也,而此置換羣則稱曰羣之表示. 特別在正置換羣時,則呼之曰**正置換表示**焉.

例. 爲將三次對稱羣

$$1,\ (abc),\ (acb),\ (ab),\ (bc),\ (ca)$$

表示爲六次正置換羣起見,乃以此諸元素分別示以

$$G_0,\ G_1,\ G_2,\ G_3,\ G_4,\ G_5,$$

則有

$$\begin{pmatrix} G_r \\ G_rG_0 \end{pmatrix}=\begin{pmatrix} 012345 \\ 012345 \end{pmatrix}=1,$$

$$\begin{pmatrix} G_r \\ G_rG_1 \end{pmatrix} = \begin{pmatrix} 012345 \\ 120534 \end{pmatrix} = (012)(354),$$

$$\begin{pmatrix} G_r \\ G_rG_2 \end{pmatrix} = \begin{pmatrix} 012345 \\ 201453 \end{pmatrix} = (021)(345),$$

$$\begin{pmatrix} G_r \\ G_rG_3 \end{pmatrix} = \begin{pmatrix} 012345 \\ 345012 \end{pmatrix} = (03)(14)(25),$$

$$\begin{pmatrix} G_r \\ G_rG_4 \end{pmatrix} = \begin{pmatrix} 012345 \\ 453201 \end{pmatrix} = (04)(15)(23),$$

$$\begin{pmatrix} G_r \\ G_rG_5 \end{pmatrix} = \begin{pmatrix} 012345 \\ 534120 \end{pmatrix} = (05)(13)(24),$$

但右邊係僅記 G 之添數者.

74. 正置換羣爲羣之置換表示者.

設 $\mathfrak{G}$ 爲 n 次正置換羣,而施行置換之文字則爲

(1)　　$\alpha,\ \alpha_1,\ \cdots\cdots,\ \alpha_{n-1}.$

先取一文字 α. 因 $\mathfrak{G}$ 爲正置換羣,故將 α 置換爲 (1) 之文字 α_i 之置換乃唯一個. 以之爲

$$S_i = \begin{pmatrix} \alpha\ \alpha_1 & \cdots\cdots \alpha_{n-1} \\ \alpha_i \alpha_1^{(i)} & \cdots\cdots \alpha_{n-1}^{(i)} \end{pmatrix},$$

則置換 $\alpha_1, \alpha_2, \cdots\cdots, \alpha_{n-1}$ 之文字 $\alpha_1^{(i)}, \alpha_2^{(i)}, \cdots\cdots, \alpha^{(i)}{}_{n-1}$, 乃由置換 α 爲 α_i 之置換,一意的得以決定者也. 於是利用 S_i, 由次之規約,得定 (1) 之文字與 α_i 之結合之義. 即

(2)　　$\alpha\alpha_i = \alpha_i, \quad \alpha_s\alpha_i = \alpha_s^{(i)} \quad (s = 1,\ 2,\ \cdots\cdots,\ n-1).$

換言之,乃於 S_i, 以得置換 α_s 之文字 $\alpha_s^{(i)}$, 而定右乘 α_i 於 α_s 所得之積者也. 夫如是,則 (1) 之文字間之結合由是得以

定義焉. 蓋因 $\mathfrak{G}$, 含有將 α 分別置換爲 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之置換故耳.

文字間之結合, 果若是而定義, 則 $\mathfrak{G}$ 之置換得換書如次:

$$(3)\qquad S_i=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha\alpha_i & \alpha_1\alpha_i & \cdots\cdots & \alpha_{n-1}\alpha_i \end{pmatrix} \quad i=0, 1, 2, \cdots\cdots, n-1,$$

或

$$(3')\qquad S_i=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i & \alpha_1\alpha_i & \cdots\cdots & \alpha_{n-1}\alpha_i \end{pmatrix} \quad i=0, 1, 2, \cdots\cdots, n-1,$$

但 $\alpha_0=\alpha$. 於 $\mathfrak{G}$, 其使 α 不動之置換僅爲主元素, 故得

$$(4)\qquad \alpha_i\alpha=\alpha_i, \quad i=0, 1, 2, \cdots\cdots, n-1,$$

因之

$$S_0=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha\alpha & \alpha_1\alpha & \cdots\cdots & \alpha_{n-1}\alpha \end{pmatrix}=1.$$

又文字(1), 關乎所定之結合復具備次之四條件, 因而成羣也.

(i) 任意二文字之積屬於(1).

(ii)
$$S_iS_j=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha\alpha_i & \alpha_1\alpha_i & \cdots\cdots & \alpha_{n-1}\alpha_i \end{pmatrix}\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha\alpha_j & \alpha_1\alpha_j & \cdots\cdots & \alpha_{n-1}\alpha_j \end{pmatrix}$$

$$=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i & \alpha_1\alpha_i & \cdots\cdots & \alpha_{n-1}\alpha_i \end{pmatrix}\begin{pmatrix} \alpha_i & \alpha_1\alpha_j & \cdots\cdots & \alpha_{n-1}\alpha_i \\ \alpha_i\cdot\alpha_j & \alpha_1\alpha_i\cdot\alpha_j & \cdots\cdots & \alpha_{n-1}\alpha_i\cdot\alpha_j \end{pmatrix}$$

$$=\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i\alpha_j & \alpha_1\alpha_i\cdot\alpha_j & \cdots\cdots & \alpha_{n-1}\alpha_i\cdot\alpha_j \end{pmatrix}.$$

而 $\mathfrak{G}$ 爲羣, 故此積當然非屬於 $\mathfrak{G}$ 卽 (3') 不可也. 然於 (3'), 置換 α 於 $\alpha_i\alpha_j$ 之置換, 乃唯一之

$$\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i\alpha_j & \alpha_1\cdot\alpha_i\alpha_j & \cdots\cdots & \alpha_{n-1}\cdot\alpha_i\alpha_j \end{pmatrix}.^{*}$$

故 $$\begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i\alpha_j & \alpha_1\alpha_i\cdot\alpha_j & \cdots\cdots & \alpha_{n-1}\alpha_i\cdot\alpha_j \end{pmatrix} = \begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i\alpha_j & \alpha_1\cdot\alpha_i\alpha_j & \cdots\cdots & \alpha_{n-1}\cdot\alpha_i\alpha_j \end{pmatrix}.$$

$$\therefore \qquad \alpha_s\alpha_i\cdot\alpha_j = \alpha_s\cdot\alpha_i\alpha_j.$$

即文字之結合，服從組合法則也.

(iii) $\alpha_i\,\alpha = \alpha_i$ [由 (4)]. 故 α 即司主元素之務者.

(iv) 以 $$S_i = \begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i & \alpha_1\alpha_i & \cdots\cdots & \alpha_{n-1}\alpha_i \end{pmatrix}$$

之逆置換爲

$$S_i^{-1} = \begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha\alpha_i' & \alpha_1\alpha_i' & \cdots\cdots & \alpha_{n-1}\alpha_i' \end{pmatrix},$$

則應用組合法則 (ii)，遂得

$$S_iS_i^{-1} = \begin{pmatrix} \alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1} \\ \alpha_i\alpha_i' & \alpha_1\alpha_i\alpha_i' & \cdots\cdots & \alpha_{n-1}\alpha_i\alpha_i' \end{pmatrix}.$$

然 $S_iS_i^{-1} = 1$. 故

$$\alpha_i\alpha_i' = \alpha$$

爲必要. 即 α_i 之逆元素 α_i' 存在也.

又對此文字所作之羣，置換羣 $\mathfrak{G}$. 即 (3) 爲其置換表示，由前節自明.

總上所述，乃謂 n 次正置換羣爲已知時，則利用其置換，n 文字間之結合遂得以定義，而關於此結合，此諸文字成羣也. 而元來所與之羣，乃爲此諸文字所作羣之正置換表示云. 爰有次之

---

* 於 (3′) 以 $\alpha_i\alpha_j$ 代 α_i 遂得此置換.

定理. 凡正置換羣，皆得視爲羣之表示.

當討論正置換羣時，若應用此定理，可得不少之便利. 又前司主元素之役者之文字 α，任選何文字充之皆無妨礙；此而定，則文字間之結合法則亦自定也.

例. 試取四次正置換羣

$$\mathfrak{G}:\quad 1,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc),$$

即

$$\begin{pmatrix} abcd \\ abcd \end{pmatrix},\ \begin{pmatrix} abcd \\ badc \end{pmatrix},\ \begin{pmatrix} abcd \\ cdab \end{pmatrix},\ \begin{pmatrix} abcd \\ dcba \end{pmatrix}.$$

由上記，換書之爲

$$\begin{pmatrix} abcd \\ abcd \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ aa & ba & ca & da \end{pmatrix},$$

$$\begin{pmatrix} abcd \\ badc \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ ab & bb & cb & db \end{pmatrix},$$

$$\begin{pmatrix} abcd \\ cdab \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ ac & bc & cc & dc \end{pmatrix},$$

$$\begin{pmatrix} abcd \\ dcba \end{pmatrix} = \begin{pmatrix} a & b & c & d \\ ad & bd & cd & dd \end{pmatrix},$$

則由此，於諸文字之間，得如次定其結合之義：

$$aa=a,\quad ba=b,\quad ca=c,\quad da=d,$$

$$ab=b,\quad bb=a,\quad cb=d,\quad db=c,$$

$$ac=c,\quad bc=d,\quad cc=a,\quad dc=b,$$

$$ad=d,\quad bd=c,\quad cd=b,\quad dd=a.$$

由此結合，則 a, b, c, d 乃作與 $\mathfrak{G}$ 單純同態之羣焉.

75. 表示爲傍系之置換羣者.

設 $\mathfrak{G}$ 爲一 g 元羣，其元素爲

(1)　　$G_0, G_1, \cdots\cdots, G_{g-1}$,

而其就約羣$\mathfrak{H}$分成之傍系爲

(2)　　$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1+\cdots\cdots+\mathfrak{H}P_{\nu-1}$.

茲於各傍系以$\mathfrak{G}$之一元素G_i右乘之，則其所得之積

$$\mathfrak{H}G_i,\ \mathfrak{H}P_1G_i,\cdots\cdots,\ \mathfrak{H}P_{\nu-1}G_i,$$

無論何個皆爲屬於$\mathfrak{H}$之傍系，且彼此互異(參照第23節). 故此各個，不外乎將傍系

(3)　　$\mathfrak{H}, \mathfrak{H}P_1, \cdots\cdots, \mathfrak{H}P_{\nu-1}$

換列於某個順序者已也. 因之，對於$\mathfrak{G}$之元素G_i，乃得傍系間之置換

(4)　　$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{\nu-1}\\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{\nu-1}G_i\end{pmatrix}$$

焉. 便宜上將此以$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}$記之，則相應於$\mathfrak{G}$之$g$元素，遂生$g$個之置換

(5)　　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_0\end{pmatrix},\ \begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_1\end{pmatrix},\cdots\cdots\cdots\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_{g-1}\end{pmatrix}.$$

作此任意二者之積，則得

(6)　　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_j\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_rG_i\\ \mathfrak{H}P_rG_i\cdot G_j\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\cdot G_j\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_r\cdot G_iG_j\end{pmatrix}.^*$$

---

*置換$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_j\end{pmatrix}$者，所以示置換(3)之各項時，右乘$G_j$於其各個之所得者也. 依此遂得(6)式焉.

而積 G_iG_j 屬於 $\mathfrak{G}$. 故 (5) 成羣. 且於 (4), 取 $P_1, P_2, \cdots\cdots, P_{\nu-1}$ 以爲 G_i, 因之羣 (5) 之爲可遷的可知也.

其次, 對 $\mathfrak{G}$ 之元素 G_i 使置換 $\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}$ 與之對應, 則由 (6) 式之關係, $\mathfrak{G}$ 與 (5) 之爲同態, 明已. 故 (5) 者 $\mathfrak{G}$ 之置換表示之一也. 但此時之同態, 不限其必爲單純的焉.

欲察此同態關係之單複, 可先於 (5) 求其不動置換, 乃以

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{\nu-1}\\ \mathfrak{H}G_t & \mathfrak{H}P_1G_t & \cdots\cdots & \mathfrak{H}P_{\nu-1}G_t\end{pmatrix}=1,$$

則 $$\mathfrak{H}P_rG_t=\mathfrak{H}P_r \quad (r=0, 1, \cdots\cdots, \nu-1;\ P_0=1)$$

爲必要, 於是

$$P_rG_t=HP_r \quad (H \text{ 爲 } \mathfrak{H} \text{ 之一元素})$$

或 $$G_t=P_r^{-1}HP_r \quad (r=0, 1, \cdots\cdots, \nu-1).$$

故 G_t 非屬於

(7) $$\mathfrak{H},\ P_1^{-1}\mathfrak{H}P_1, \cdots\cdots, P_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1}$$

之全部不可也. 反之若 G_t 爲此等共軛約羣之所共通, 則

$$\mathfrak{H}P_rG_t=\mathfrak{H}P_r,$$

而置換 $\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_t\end{pmatrix}$ 之爲不動的, 明已. 因之 (5) 中之不動置換, 乃與 (7) 之羣之共通元素對應者也.

今以 (7) 之羣之最大公約羣* 爲 $\mathfrak{D}$, 而就之分 $\mathfrak{G}$ 爲傍系:

*此最大公約羣於 $\mathfrak{G}$ 爲正常的 (參照第 34 節).

$$(8)\qquad \mathfrak{G}=\mathfrak{D}Q_0+\mathfrak{D}Q_1+\cdots\cdots+\mathfrak{D}Q_{\mu-1}\quad (Q_0=1)$$

於是對$\mathfrak{D}$之任意一元素D，乃有

$$(9)\qquad \left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rDQ_i\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rD\end{matrix}\right)\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right).$$

故由$\mathfrak{G}$之元素所得之置換，不過次之μ個：

$$(10)\qquad \left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_0\end{matrix}\right),\ \left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_1\end{matrix}\right),\ \cdots\cdots,\ \left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_{\mu-1}\end{matrix}\right).$$

且此各個皆互異。蓋若

$$\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{matrix}\right),$$

則

$$(11)\qquad \left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right)\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{matrix}\right)^{-1}=1.$$

然

$$\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_rQ_j^{-1}\\ \mathfrak{H}P_rQ_j^{-1}\cdot Q_j\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_rP_j^{-1}\\ \mathfrak{H}P_r\end{matrix}\right),$$

因之

$$\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right)\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{matrix}\right)^{-1}=\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{matrix}\right)\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j^{-1}\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_iQ_j^{-1}\end{matrix}\right).$$

故由(11)，
$$\left(\begin{matrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_iQ_j^{-1}\end{matrix}\right)=1.$$

爲此之故，由上述，$Q_iQ_j^{-1}$之屬於$\mathfrak{D}$爲必要也；因之Q_i與Q_j乃成爲對於$\mathfrak{H}$而屬於同一之傍系者焉．是則(10)中之置換互異也．

夫如是，(10)之μ個乃表示(5)中互異之置換者，因之

羣(5)之元數爲μ. 而如(9)式之所示, 對$\mathfrak{G}$之傍系$\mathfrak{D}Q_i$, (10)之置換$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}$相與對應.

於是, $\mathfrak{D}$若爲主元素羣, 則$\mu=g$, 而同態爲單純的. 反之, $\mathfrak{D}$之元數d若大於1, 則同態爲d重. 要約上言, 得次

定理. 設$\mathfrak{G}$爲一羣, 其元素爲$G_0, G_1, \cdots\cdots, G_{g-1}$, 而其就約羣$\mathfrak{H}$分成之傍系爲

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1+\cdots\cdots+\mathfrak{H}P_{\nu-1}.$$

於是, $\mathfrak{G}$與傍系之置換羣

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{\nu-1}\\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{\nu-1}G_i\end{pmatrix}\quad (i=0, 1, 2, \cdots\cdots, g-1)$$

爲同態. 又$\mathfrak{H}$之共軛約羣

$$\mathfrak{H},\quad P_1^{-1}\mathfrak{H}P_1,\ \cdots\cdots,\ P_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1}$$

之最大公約羣以爲$\mathfrak{D}$, 則此置換羣與商$\mathfrak{G}/\mathfrak{D}$爲單純同態.

爲言辭簡潔起見, 其由本定理之羣之表示, 單呼之曰**傍系置換表示**. 當同時討論兩個以上之傍系置換表示, 或一表示有特別指定之必要時, 則明示其傍系所屬之約羣, 有如上記, 呼之曰關於約羣$\mathfrak{H}$之傍系置換表示以與他區別可.

特別當$\mathfrak{H}$於$\mathfrak{G}$爲正常時, $\mathfrak{D}$與$\mathfrak{H}$一致也. 故傍系置換表示由定理乃與$\mathfrak{G}/\mathfrak{H}$爲單純同態. 而此時(8)式與(2)式一致, 因之(10)中之Q置以P, 所得之ν個置換

(12) $\begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{\nu-1} \\ \mathfrak{H}P_i & \mathfrak{H}P_1P_i & \cdots\cdots & \mathfrak{H}P_{\nu-1}P_i \end{pmatrix}$, $i=0, 1, 2, \cdots, \nu-1$; $P_0=1$,

乃示傍系置換表示中互異之置換者也. 且此各個皆正置換. (但不動置換除外). 蓋若對 r 之特別值,

$$\mathfrak{H}P_rP_i=\mathfrak{H}P_r,$$

則
$$P_r^{-1}\mathfrak{H}P_rP_i=P_r^{-1}\mathfrak{H}P_r.$$

$$\therefore\quad \mathfrak{H}P_i=\mathfrak{H}\quad [\mathfrak{H}\text{爲正常故}].$$

$$\therefore\quad P_i=P_0.$$

故(12)中不使傍系之一動者,僅不動置換已也.

如是,$\mathfrak{H}$ 於 $\mathfrak{G}$ 爲正常時,則關於 $\mathfrak{H}$ 之傍系置換表示,乃與 $\mathfrak{G}/\mathfrak{H}$ 成單純同態之正置換羣也.

例. 將四次交代羣 $\mathfrak{A}$ (第12節例2又第71節例1)就其約羣

$$\mathfrak{B}:\quad 1,\quad (ab)(cd),\quad (ac)(bd),\quad (ad(bc)$$

分爲傍系,則得

$$\mathfrak{A}=\mathfrak{B}+\mathfrak{B}(bcd)+\mathfrak{B}(bdc)$$

(參照第24節例). 故 $\mathfrak{A}$ 得表之爲三次可遷羣. 然 $\mathfrak{B}$ 爲正常,故表示羣與 $\mathfrak{A}/\mathfrak{B}$ 即

$$1,\quad (bcd),\quad (bdc)\quad (\text{mod. }\mathfrak{B})$$

爲單純同態也,示之如次:

$\mathfrak{A}$ 之置換 G 屬於 $\mathfrak{B}$ 時,

$$\begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}G & \mathfrak{B}(bcd)G & \mathfrak{B}(bdc)G \end{pmatrix}=1;$$

G 屬於傍系 $\mathfrak{B}(bcd)$ 時,

$$\begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}G & \mathfrak{B}(bcd)G & \mathfrak{B}(bdc)G \end{pmatrix} = \begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}(bcd) & \mathfrak{B}(bdc) & \mathfrak{B} \end{pmatrix};$$

G 爲傍系 $\mathfrak{B}(bdc)$ 之置換時,

$$\begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}G & \mathfrak{B}(bcd)G & \mathfrak{B}(bdc)G \end{pmatrix} = \begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}(bdc) & \mathfrak{B} & \mathfrak{B}(bcl) \end{pmatrix}.$$

爲記號之簡單計,將各傍系分別表之爲 P, Q, R, 則表示羣遂成爲

$$1, \quad \begin{pmatrix} PQR \\ QRP \end{pmatrix}, \quad \begin{pmatrix} PQR \\ RPQ \end{pmatrix}$$

卽

$$1, \quad (PQR), \quad (PRQ)$$

也,其與 $\mathfrak{A}/\mathfrak{B}$ 之爲單純同態明矣.

76. 可遷羣之爲羣之傍系置換表示者.

設 $\mathfrak{G}$ 爲由 n 文字

(1) $$a, a_1, \cdots\cdots, a_{n-1}$$

上所行置換而成之 g 元可遷羣,其置換爲

(2) $$G_0, G_1, \cdots\cdots, G_{g-1} \quad (G_0=1).$$

次以文字 a 不動之約羣爲 $\mathfrak{H}$, 而就之分 $\mathfrak{G}$ 爲傍系:

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1},$$

但 S_i 爲示將 a 置換於 a_i 之置換之一者. 於是,傍系上所行 g 個之置換

(3) $$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix} (i=0, 1, 2, \cdots\cdots, g-1),$$

由前節定理，乃作與$\mathfrak{G}$同態之羣焉．且此同態爲單純的．蓋因共軛約羣

$$\mathfrak{H},\quad S_1^{-1}\mathfrak{H}S_1,\quad \cdots\cdots,\quad S_{n-1}^{-1}\mathfrak{H}S_{n-1},$$

乃分別爲$a, a_1, \cdots\cdots, a_{n-1}$之不動者；因而此各個之共通元素，乃使$n$文字皆不動，是卽不動置換（主元素）爲必要故也．

今取$\mathfrak{G}$之任意置換

$$G_i=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a^{(i)} & a_1^{(i)} & \cdots\cdots & a_{n-1}^{(i)} \end{pmatrix},$$

以之右乘於S_r（$r=0, 1, 2, \cdots\cdots, n-1$; $S_0=1$），則其積S_rG_i乃置換a爲$a_r^{(i)}$也．因之$\mathfrak{H}S_rG_i$卽爲在$\mathfrak{G}$中將a置換爲$a_r^{(i)}$者之置換之集合（第63節定理）．故在與G_i對應之置換

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix}$$

中其a置換爲a_r者之傍系$\mathfrak{H}S_r$，得以a置換爲$a_r^{(i)}$者之傍系$\mathfrak{H}S_rG_i$而置換之者也．以故於n文字

(1)　　$a, a_1, \cdots\cdots, a_{n-1},$

分別使傍系

(4)　　$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{n-1}$

與之對應，*則G_i中n文字之移動與置換$\begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}S_rG_i \end{pmatrix}$中傍系之移動全然同一．換言之，卽於置換$G_i$將$n$文字$a, a_1, \cdots\cdots,$

---

*對於文字a_i使a置換爲a_j者之傍系與之對應．

a_{n-1} 代以傍系 $\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{n-1}$，則得傍系之置換 $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}$ 也. 若更自反對方面觀之，則羣 $\mathfrak{G}$ 不過在傍系之置換羣 (3) 中將傍系 (4) 分別代以 (1) 之文字者已也. 爰得次

定理. 可遷羣得視爲一個羣之傍系置換表示.

本定理亦與第74節者同樣，匪特關於可遷羣之考察得以廣爲應用，而於可遷羣與一般羣之關係，使之更爲密接之點，是甚爲重要者也.

例. 試取四次可遷羣

$$\mathfrak{G}: \begin{cases} 1 & (abcd) & (ac)(bd) & (adcb) \\ (bd) & (ad)(bc) & (ac) & (ab)(cd). \end{cases}$$

其文字 a 不動之約羣爲

$$\mathfrak{H}: \quad 1, \quad (bd),$$

而

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}\,(abcd)+\mathfrak{H}\,(ac)(bd)+\mathfrak{H}\,(adcb).$$

至將 $\mathfrak{G}$ 之各元素右乘於各傍系之結果，則載在次頁之表中. 由此表以作 $\mathfrak{G}$ 之傍系置換表示，則得

$$\begin{matrix}\begin{pmatrix}\mathrm{ABCD}\\ \mathrm{ABCD}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{BCDA}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{CDAB}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{DABC}\end{pmatrix},\\ \| & \| & \| & \|\\ 1 & (\mathrm{ABCD}) & (\mathrm{AC})(\mathrm{BD}) & (\mathrm{ADCB})\end{matrix}$$

$$\begin{matrix}\begin{pmatrix}\mathrm{ABCD}\\ \mathrm{ADCB}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{DCBA}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{CBAD}\end{pmatrix}, & \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{BADC}\end{pmatrix}.\\ \| & \| & \| & \|\\ (\mathrm{BD}) & (\mathrm{AD})(\mathrm{BC}) & (\mathrm{AC}) & (\mathrm{AB})(\mathrm{CD})\end{matrix}$$

於是若將 A, B, C, D 代以 a, b, c, d，遂得 $\mathfrak{G}$ 焉.

傍系 / 右乘之置換	$\mathfrak{H}$ ‖ A	$\mathfrak{H}\,(abcd)$ ‖ B	$\mathfrak{H}\,(ac)(bd)$ ‖ C	$\mathfrak{H}\,(adcb)$ ‖ D
1	$\mathfrak{H}$ ‖ A	$\mathfrak{H}\,(abcd)$ ‖ B	$\mathfrak{H}\,(ac)(bd)$ ‖ C	$\mathfrak{H}\,(adcb)$ ‖ D
$(abcd)$	$\mathfrak{H}\,(abcd)$ ‖ B	$\mathfrak{H}\,(ac)(bd)$ ‖ C	$\mathfrak{H}\,(adcb)$ ‖ D	$\mathfrak{H}$ ‖ A
$(ac)(bd)$	$\mathfrak{H}\,(ac)(bd)$ ‖ C	$\mathfrak{H}\,(adcb)$ ‖ D	$\mathfrak{H}$ ‖ A	$\mathfrak{H}\,(abcd)$ ‖ B
$(adcb)$	$\mathfrak{H}\,(adcb)$ ‖ D	$\mathfrak{H}$ ‖ A	$\mathfrak{H}\,(abcd)$ ‖ B	$\mathfrak{H}\,(ac)(bd)$ ‖ C
(bd)	$\mathfrak{H}\,(bd)$ ‖ A	$\mathfrak{H}\,(ad)(bc)$ ‖ D	$\mathfrak{H}\,(ac)$ ‖ C	$\mathfrak{H}\,(ab)(cd)$ ‖ B
$(ad)(bc)$	$\mathfrak{H}\,(ad)(bc)$ ‖ D	$\mathfrak{H}\,(ac)$ ‖ C	$\mathfrak{H}\,(ab)(cd)$ ‖ B	$\mathfrak{H}\,(bd)$ ‖ A
(ac)	$\mathfrak{H}\,(ac)$ ‖ C	$\mathfrak{H}\,(ab)(cd)$ ‖ B	$\mathfrak{H}\,(bd)$ ‖ A	$\mathfrak{H}\,(ad)(bc)$ ‖ D
$(ab)(cd)$	$\mathfrak{H}\,(ab)(cd)$ ‖ B	$\mathfrak{H}\,(bd)$ ‖ A	$\mathfrak{H}\,(ad)(bc)$ ‖ D	$\mathfrak{H}\,(ac)$ ‖ C

有如本例之傍系置換表示，其傍系 A, B, C, D 代以文字 a, b, c, d 遂得羣 $\mathfrak{G}$ 者然，一般，置換羣 $\mathfrak{P}$，其施行置換之文字 α_1

$\alpha_1, \cdots\cdots, \alpha_{n-1}$, 代以他之文字 $\beta, \beta_1, \cdots\cdots, \beta_{n-1}$ 時所生之置換羣, 名曰與 $\mathfrak{R}$ 同值. 用此術語, 則上之定理, 得換書如次. 卽:

對於一個可遷羣, 其與之同值之傍系置換表示, 必定存在.

至若一個羣之置換表示(不互爲同值者)之數, 則於第108節述之.

注意. 置換羣之共軛約羣, 同值者也. 蓋於約羣 $\mathfrak{T}$, 若其施行置換之文字爲 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$, 而

$$\begin{pmatrix} \alpha & \alpha_1 \cdots\cdots & \alpha_{m-1} \cdots\cdots \\ \beta & \beta_1 \cdots\cdots & \beta_{m-1} \cdots\cdots \end{pmatrix}^{-1} \mathfrak{T} \begin{pmatrix} \alpha & \alpha_1 \cdots\cdots & \alpha_{m-1} \cdots\cdots \\ \beta & \beta_1 \cdots\cdots & \beta_{m-1} \cdots\cdots \end{pmatrix} = \mathfrak{T}',$$

則 $\mathfrak{T}'$ 乃將文字 $\alpha, \alpha_1, \cdots\cdots \alpha_{m-1}$, 代以 $\beta, \beta_1, \cdots\cdots, \beta_{m-1}$ 而由 $\mathfrak{T}$ 而得者, 以故 $\mathfrak{T}$ 與 $\mathfrak{T}'$ 同值. 但同值之二約羣不必爲共軛焉.

77. 表示爲共軛約羣(或元素)之置換羣者.

設 $\mathfrak{G}$ 爲一羣,

$$(1) \qquad G_0, G_1, \cdots\cdots, G_{\nu-1}$$

爲其元素,

$$(2) \qquad \mathfrak{H}, \mathfrak{H}_1, \cdots\cdots, \mathfrak{H}_{\nu-1}$$

爲 $\mathfrak{G}$ 之約羣(或元素) $\mathfrak{H}$ 所屬之共軛系.

以 $\mathfrak{G}$ 之一元素 G_i 將(2)之各項變形, 其所得之

$$G_i^{-1} \mathfrak{H} G_i, \; G_i^{-1} \mathfrak{H}_1 G_i, \cdots\cdots, G_i^{-1} \mathfrak{H}_{\nu-1} G_i$$

互異, 且與 $\mathfrak{H}$ 共軛. 故此各個, 不外(2)之置於某順序者已也(參照第34節). 以故與 $\mathfrak{G}$ 之元素 G_i 相應, 遂得共軛約羣

(或共軛元素)間之置換

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}_1 & \cdots\cdots & \mathfrak{H}_{\nu-1} \\ G_i^{-1}\mathfrak{H}G_i & G_i^{-1}\mathfrak{H}_1 G_i & \cdots\cdots & G_i^{-1}\mathfrak{H}_{\nu-1}G_i \end{pmatrix}.$$

便宜上以 $\begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_r G_i \end{pmatrix}$ 記之，則對 $\mathfrak{G}$ 之 g 元素，g 個之置換

$$(3)\quad \begin{pmatrix} \mathfrak{H}_r \\ G_0^{-1}\mathfrak{H}_r G_0 \end{pmatrix}, \begin{pmatrix} \mathfrak{H}_r \\ G_1^{-1}\mathfrak{H}_r G_1 \end{pmatrix}, \cdots\cdots, \begin{pmatrix} \mathfrak{H}_r \\ G_{g-1}^{-1}\mathfrak{H}_r G_{g-1} \end{pmatrix}$$

生焉．且其成羣也．蓋因作其任意二者之積，乃成爲次之(4):

$$(4)\quad \begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_r G_i \end{pmatrix}\begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}\mathfrak{H}_r G_j \end{pmatrix} = \begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_r G_i \end{pmatrix}\begin{pmatrix} G_i^{-1}\mathfrak{H}_r G_i \\ G_j^{-1}\cdot G_i^{-1}\mathfrak{H}_r G_i \cdot G_j \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}G_i^{-1}\mathfrak{H}_r G_i G_j \end{pmatrix} = \begin{pmatrix} \mathfrak{H}_r \\ (G_iG_j)^{-1}\mathfrak{H}_r (G_iG_j) \end{pmatrix},^{*}$$

而積 G_iG_j 又屬於 $\mathfrak{G}$ 故．而(2)爲一共軛系，故羣(3)當然爲可遷的．

其次，若對 $\mathfrak{G}$ 之元素 G_i，使置換 $\begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_r G_i \end{pmatrix}$ 與之對應，則由(4)式，$\mathfrak{G}$ 之與(3)同態可知也．故(3)爲 $\mathfrak{G}$ 之置換表示之一種．但此時之同態亦不必定爲單純的．

欲察此同態關係之單複，乃先求(3)中之不動置換．以

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}_1 & \cdots\cdots & \mathfrak{H}_{\nu-1} \\ G_t^{-1}\mathfrak{H}G_t & G_t^{-1}\mathfrak{H}_1 G_t & \cdots\cdots & G_t^{-1}\mathfrak{H}_{\nu-1}G_t \end{pmatrix} = 1,$$

---

*置換 $\begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}\mathfrak{H}_r G_j \end{pmatrix}$，乃示當置換(2)之各項時，以 G_j 變其形之所得者也．故得(4)式．

則 $$G_t^{-1}\mathfrak{H}_rG_t=\mathfrak{H}_r \quad (r=0,\ 1,\ \cdots\cdots,\ \nu-1;\ \mathfrak{H}_0=\mathfrak{H}).$$

故 G_t 與(2)之所有各項皆交換可能爲必要也. 反之,若 G_t 與(2)之各項皆交換可能,則與是相應之置換之爲不動的甚明. 故羣(3)中之不動置換,乃與 $\mathfrak{H},\mathfrak{H}_1,\cdots\cdots,\mathfrak{H}_{\nu-1}$ 之正常化羣

$$(5)\qquad \mathfrak{K},\mathfrak{K}_1,\cdots\cdots,\mathfrak{K}_{\nu-1}$$

之全部所共通之元素相對應者也. 茲以此諸正常化羣之最大公約羣爲 $\mathfrak{D}$,而就之分 $\mathfrak{G}$ 爲傍系:

$$\mathfrak{G}=\mathfrak{D}Q_0+\mathfrak{D}Q_1+\cdots\cdots+\mathfrak{D}Q_{\mu-1}\quad (Q_0=1).$$

於是對於 $\mathfrak{D}$ 之任意元素 D,則有

$$\left((DQ_i)^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}(DQ_i)\right)=\left(Q_i^{-1}D^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}DQ_i\right)=\left(Q_i^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_i\right).$$

故由 $\mathfrak{G}$ 之元素所得之置換不過次之 μ 個:

$$(6)\quad \left(Q_0^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_0\right),\ \left(Q_1^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_1\right),\ \cdots\cdots,\ \left(Q_{\mu-1}^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_{\mu-1}\right).$$

而此各個之爲互異,則易得而證明. 故此之 μ 個,乃表示(3)中相異之置換,因而羣(3)之元數爲 μ 也. 而對 $\mathfrak{G}$ 中傍系 $\mathfrak{D}Q_i$,則(6)之置換 $\left(Q_i^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_i\right)$ 相對應焉.

於是,若 $\mathfrak{D}$ 爲主元素羣,則 $\mu=g$,其同態遂爲單純的. 反之,若 $\mathfrak{D}$ 之元數 d 大於1,則同態爲 d 重的. 爰有次

定理. 一個羣,其一共軛系(約羣的或元素的)由 ν 項而成時,則此羣得表之爲 ν 次可遷羣.

例. 將第63節例2所示之六次可遷羣

$$1, \qquad Q=(a_1a_5)(a_2a_4)$$

$$P_1=(aa_1a_2a_3a_4a_5) \qquad Q_1=(aa_5)(a_1a_4)(a_2a_3)$$

$$P_2=(aa_2a_4)(a_1a_3a_5) \qquad Q_2=(aa_4)(a_1a_3)$$

$$P_3=(aa_3)(a_1a_4)(a_2a_5) \qquad Q_3=(aa_3)(a_1a_2)(a_4a_5)$$

$$P_4=(aa_4a_2)(a_1a_5a_3) \qquad Q_4=(aa_2)(a_3a_5)$$

$$P_5=(aa_5a_4a_3a_2a_1) \qquad Q_5=(aa_1)(a_2a_5)(a_3a_4)$$

名爲$\mathfrak{G}$, 其約羣

$$1, P_3, Q, Q_3$$

則以$\mathfrak{H}$表之. 於是$\mathfrak{H}$之正常化羣乃$\mathfrak{H}$自身, 而與$\mathfrak{H}$共軛之約羣, 除$\mathfrak{H}$自身外, 爲

$$\mathfrak{H}_1=P_1^{-1}\mathfrak{H}P_1: \quad 1, P_3, Q_4, Q_1;$$

$$\mathfrak{H}_2=P_2^{-1}\mathfrak{H}P_2: \quad 1, P_3, Q_2, Q_5.$$

而此等之最大公約羣爲

$$1, \quad P_3.$$

將其表以$\mathfrak{D}$, 則得

$$\mathfrak{G}=\mathfrak{D}+\mathfrak{D}P_1+\mathfrak{D}P_2+\mathfrak{D}Q+\mathfrak{D}Q_4+\mathfrak{D}Q_2.$$

於是依本節之方法, 將$\mathfrak{G}$表之爲由三共軛約羣之置換而成之可遷羣, 則表示羣與$\mathfrak{G}/\mathfrak{D}$爲單純同態也. 因之爲六元焉. 示之如次:

$\mathfrak{G}$之置換G若

屬於$\mathfrak{D}$時, $\left(\begin{matrix}\mathfrak{H}_r\\ G^{-1}\mathfrak{H}_rG\end{matrix}\right)=\left(\begin{matrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\end{matrix}\right)=1;$

屬於 $\mathfrak{D}P_1$ 時, $\begin{pmatrix} \mathfrak{H}_r \\ G^{-1}\mathfrak{H}_r G \end{pmatrix} = \begin{pmatrix} \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2 \\ \mathfrak{H}_1\mathfrak{H}_2\mathfrak{H} \end{pmatrix} = (\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2);$

屬於 $\mathfrak{D}P_2$ 時, $\begin{pmatrix} \mathfrak{H}_r \\ G^{-1}\mathfrak{H}_r G \end{pmatrix} = \begin{pmatrix} \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2 \\ \mathfrak{H}_2\mathfrak{H}\mathfrak{H}_1 \end{pmatrix} = (\mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1);$

屬於 $\mathfrak{D}Q$ 時, $\begin{pmatrix} \mathfrak{H}_r \\ G^{-1}\mathfrak{H}_r G \end{pmatrix} = \begin{pmatrix} \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2 \\ \mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1 \end{pmatrix} = (\mathfrak{H}_1\mathfrak{H}_2);$

屬於 $\mathfrak{D}Q_4$ 時, $\begin{pmatrix} \mathfrak{H}_r \\ G^{-1}\mathfrak{H}_r G \end{pmatrix} = \begin{pmatrix} \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2 \\ \mathfrak{H}_2\mathfrak{H}_1\mathfrak{H} \end{pmatrix} = (\mathfrak{H}_2\mathfrak{H});$

屬於 $\mathfrak{D}Q_2$ 時, $\begin{pmatrix} \mathfrak{H}_r \\ G^{-1}\mathfrak{H}_r G \end{pmatrix} = \begin{pmatrix} \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2 \\ \mathfrak{H}_1\mathfrak{H}\mathfrak{H}_2 \end{pmatrix} = (\mathfrak{H}\mathfrak{H}_1).$

故表示羣如次:

$$1,\quad (\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2),\ (\mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1),\ (\mathfrak{H}_1\mathfrak{H}_2),\ (\mathfrak{H}_2\mathfrak{H}),\ (\mathfrak{H}\mathfrak{H}_1).$$

78. 元數 36, 72, 80 者之羣之複合性.

(i) 元數 36, 72 者.

因 $$36=2^2\cdot 3^2,\quad 72=2^3\cdot 3^2,$$

故 3^2 元約羣之數, 得以 $1+3\lambda$ 形表之, 且對前者須爲 2^2 之約數, 對後者須爲 2^3 之約數 (第 54 節 Sylow 氏定理). 故此數不得不爲 1 或 4 也. 3^2 元約羣之數爲 1 時, 則此約羣爲正常; 反之爲四個時, 則此諸約羣作一共軛系 (Sylow 氏定理). 故由前節定理, 此羣得表之爲四次可遷羣. 然四次置換羣之元數不得超過 24. 故此表示中之同態須爲重複的; 因之與表示羣之主元素相對應者, 其羣之正常約羣 (非主元素羣) 定存在也. 是則無論如何, 36 元, 72 元羣之爲複合的可知已.

(ii) 元數 90 者. $(90=2\cdot3^2\cdot5)$

由 Sylow 氏定理, 5 元約羣之數, 得以 $1+5\lambda$ 形表之, 且爲 $2\cdot3^2$ 之約數. 故此數不得不爲 1 或 6 也. 以前者言, 則 5 元約羣爲正常, 因而其羣爲複合.

其次, 請就該羣(名曰 $\mathfrak{G}$)之有六個 5 元約羣者論之. 此時此諸約羣互爲共軛, 故若以其一爲

$$\{P\} \qquad (P^5=1),$$

則 $\{P\}$ 之正常化羣, 15 元也, 以 $\mathfrak{H}$ 表之. $\mathfrak{H}$ 中 3 元約羣(以 $\{Q\}$ 表之), 由 Sylow 氏定理, 於 $\mathfrak{H}$ 爲正常. 故 $\{Q\}$ 與 P 爲交換可能. 又 $\{P\}$ 於 $\mathfrak{H}$ 亦正常, 故與 Q 爲交換可能. 且兩羣 $\{P\}$ $\{Q\}$, 除主元素外, 無共通之元素. 故由第 27 節第四定理, P 與 Q 爲交換可能. 因之

$$(PQ)^5=P^5Q^5=Q^2\neq1,$$

$$(PQ)^3=P^3Q^3=P^3\neq1.$$

然積 PQ 屬於 $\mathfrak{H}$, 故其巡回率爲 15 之約數. 以故由上式, 則 PQ 之巡回率須爲 15 也.

自他面言, 因 $\mathfrak{G}$ 中與 $\{P\}$ 共軛約羣之數爲六個, 故由前節定理, $\mathfrak{G}$ 得以六次可遷羣(以之爲 $\mathfrak{G}'$)表之也. 若 $\mathfrak{G}$ 爲單羣, 則 $\mathfrak{G}'$ 與 $\mathfrak{G}$ 爲單純同態, 因之與 $\mathfrak{G}$ 之元素 PQ 相對應之 $\mathfrak{G}'$ 之元素, 其巡回率不得不爲 15. 然六次置換羣, 不含巡回率爲 15 者之置換. (因由六個之文字不能作巡回率 15 之置換故.) 故 $\mathfrak{G}$ 爲單羣之假定乃不合理. 是卽 $\mathfrak{G}$ 爲

複合也.

90元羣之爲複合,其證明由第59節所示之方針亦可能. 卽{P}不爲正常時,乃利用上記P與Q之爲交換可能,及3元約羣{Q}於9元約羣之一中爲正常等等,則如同節之所示,{Q}之正常化羣$\mathfrak{N}$爲90元或45元也. 以前者言,則$\mathfrak{N}$與$\mathfrak{G}$一致,因而{Q}於$\mathfrak{G}$爲正常. 以後者論,因$\mathfrak{N}$之指數爲2,故$\mathfrak{G}$就$\mathfrak{N}$分爲傍系,則爲

$$\mathfrak{G}=\mathfrak{N}+\mathfrak{N}S.$$

因之{Q}所屬之共軛系,由

$$\{Q\},\quad S^{-1}\{Q\}S$$

二羣而成,其各個之正常化羣爲

$$\mathfrak{N},\quad S^{-1}\mathfrak{N}S$$

也. 故由前節定理,$\mathfrak{G}$得以二次可遷羣$\mathfrak{G}'$表示,而於$\mathfrak{G}'$之主元素,則兩正常化羣$\mathfrak{N}$, $S^{-1}\mathfrak{N}S$之最大公約羣$\mathfrak{D}$相對應焉. 然$\mathfrak{G}'$, 2元; $\mathfrak{G}$, 90元. 故$\mathfrak{D}$之元數須爲45, 因之$\mathfrak{D}$與$\mathfrak{N}$一致($\mathfrak{N}$亦45元故). 是則$\mathfrak{N}$於$\mathfrak{G}$爲正常也.

79. 60元單羣.

設$\mathfrak{G}$爲60元單羣. 由Sylow氏定理,$\mathfrak{G}$中5元約羣之數爲六個. 然此中二羣,除主元素外,無有共通元素(元數爲素數故). 故巡回率5之元素,$\mathfrak{G}$之中有

$$(5-1)\times 6=24$$

個存在. 以5元約羣爲

$$\{A_1\},\ \{A_2\},\ \cdots\cdots,\ \{A_6\},$$

其各個之正常化羣，則分別以

$$\mathfrak{A}_1,\ \mathfrak{A}_2,\ \cdots\cdots,\ \mathfrak{A}_6$$

表之．此正常化羣之元數，當然爲 10 也．

又 3 元約羣之數爲 4 或 10．若爲四個，則與前節同樣，$\mathfrak{G}$ 得以四次可遷羣(名曰 $\mathfrak{G}'$)表之．然 $\mathfrak{G}'$ 之元數不得超過 24．故 $\mathfrak{G}$ 與 $\mathfrak{G}'$ 爲重複同態，因之 $\mathfrak{G}$ 爲複合的，是與假定反．故 3 元約羣之數須爲 10，隨而巡回率爲 5 之元素之數爲

$$(3-1)\times 10=20.$$

茲以 3 元約羣爲

$$\{B_1\},\ \{B_2\},\ \cdots\cdots,\ \{B_{10}\},$$

其各個之正常化羣，分別以

$$\mathfrak{B}_1,\ \mathfrak{B}_2,\ \cdots\cdots,\ \mathfrak{B}_{10}$$

示之．後者之元數，無論何個皆 6 也．

復次，巡回率 2 之元素，決不與巡回率 5 之元素交換可能．蓋若假定巡回率 2 之元素 C 與巡回率 5 之元素，如 A_1，爲交換可能，則兩巡回率約羣 $\{A_1\}$ 及 $\{C\}$ 之積形成一 10 元約羣，因之積 A_1C 之巡回率須爲 10 之約數．然 A_1 與 C 爲交換可能，故

$$(A_1C)^2=A_1{}^2C^2=A_1{}^2\neq 1,$$

$$(A_1C)^5=A_1{}^5C^5=C\neq 1.$$

是則 A_1C 之巡回率不得不爲 10 也．以故

$$\{A_1\}\{C\}=\{A_1C\}.$$

但自他面觀，$\{A_1\}$ 之正常化羣 $\mathfrak{A}_1$ 之元數亦爲 10. 故

$$\mathfrak{A}_1=\{A_1C\}.$$

卽 $\mathfrak{A}_1$ 乃成 10 元之巡回約羣，因而含有巡回率 10 之元素 4 個也. 若 $\mathfrak{A}_1$ 爲巡回羣，則他之正常化羣 $\mathfrak{A}_2, \mathfrak{A}_3, \mathfrak{A}_4, \mathfrak{A}_5, \mathfrak{A}_6$ 亦復同樣(因此各個皆與 $\mathfrak{A}_1$ 共軛故). 故此時 $\mathfrak{G}$ 非含巡回率 10 之元素 $4\times6(=24)$ 個不可也. 將此與巡回率 5, 3 之元素及主元素總計之，其數爲

$$24+24+20+1=69,$$

是超過 $\mathfrak{G}$ 之元數 60. 故若假定巡回率 2 之元素 C 與巡回率 5 之元素 A_1 爲交換可能，則 $\mathfrak{A}_1$ 乃成爲 10 元巡回約羣而生上之不合理之結果. 因之 C 決不能與巡回率 5 之元素交換可能也.

又巡回率 2 之元素與巡回率 3 之元素亦非交換可能. 蓋若假定巡回率 2 之元素 C 與巡回率 3 之元素如 B_1 爲交換可能，則與前同樣，兩元素之積 B_1C 之巡回率爲 6，而

$$\mathfrak{B}_1=\{B_1C\},$$

卽 $\mathfrak{B}_1$ 乃成 6 元之巡回約羣，因而含巡回率 6 之元素兩個. 又他之正常化羣 $\mathfrak{B}_2, \mathfrak{B}_3, \cdots\cdots, \mathfrak{B}_{10}$ 亦復同然，於是 $\mathfrak{G}$ 遂不得不含如是者之元素 $2\times10(=20)$ 個也. 將此與巡回率 5, 3 之元素及主元素總計之，其數爲

$$20+24+20+1=65,$$

是又超過$\mathfrak{G}$之元數而不合理也. 以故曰巡回率2之元素決不與巡回率3之元素爲交換可能云.

再取巡回率2之一元素C, 其正常化羣(與C交換可能之元素之集合)之元數, 由上述, 不得有5及3爲其因數也. 故此之元數須爲2或4. 然2元約羣{C}, 由Sylow氏定理系, 乃含於4元約羣; 而4元約羣, 依第31節第二定理, 又爲Abel氏羣. 故C之正常化羣之元數, 不得不爲4也. 因之與C共軛元素之數爲$\frac{60}{4}(=15)$. 將巡回率5及3之元素以及主元素加於此15元素, 則其總數爲

$$15+24+20+1=60,$$

是以此而$\mathfrak{G}$之元素可盡也. 因之巡回率2之元數有15個存在, 且互爲共軛. 而$\mathfrak{G}$遂不含巡回率爲5, 3及2以外者之元素也(主元素在外).

更就4元約羣而觀, 則此中兩羣除主元素外無有共通元素. 蓋若假定二4元約羣$\mathfrak{C}$, $\mathfrak{C}'$共有巡回率2之元素C', 則因4元約羣爲Abel氏羣故, C'遂與$\mathfrak{C}$之元素以及$\mathfrak{C}'$之元素爲交換可能. 故C'之正常化羣不得不含$\mathfrak{C}$及$\mathfrak{C}'$, 因之其元數較4大也. 是與以2爲巡回率之元素之正常化羣爲4元之事實相反, 是不合理. 故互異之4元約羣不得有共通元素(非主元素).

且4元約羣之數, 由Sylow氏定理, 爲3, 5或15. 如爲3個或15個, 則以2爲巡回率之元素之數爲

$$(4-1)\times 3=9<15,\ (4-1)\times 15=45>15,$$

二者皆所不可. 故$\mathfrak{G}$中4元約羣之數不得不爲5個也. 此5個約羣, 由Sylow氏定理, 乃作一共軛系. 因之, 由第77節定理, $\mathfrak{G}$得表之爲5次可遷羣. 此表示羣茲以$(\mathfrak{G})$記之. 由假設, $\mathfrak{G}$乃單羣, 故此之表示$(\mathfrak{G})$當然須與$\mathfrak{G}$爲單純同態. 因之其元數爲60也. 若假定$(\mathfrak{G})$含有奇數置換, 則$(\mathfrak{G})$中之偶數置換, 作$(\mathfrak{G})$之正常約羣, 是與$\mathfrak{G}$爲單羣之假設反. 故$\mathfrak{G}$之置換, 非全數爲偶數的不可也. 然5次對稱羣中偶數置換之總數爲$\frac{5!}{2}(=60)$, 此數與$(\mathfrak{G})$之元數一致. 故$(\mathfrak{G})$爲5次交代羣. 如是, 60元單羣常與5次交代羣同態. 因之得次

定理. 60元單羣只有唯一個型.

注意. 如第60節所示, 二十面體羣爲單純的. 因之由本定理之證明, 乃與5次交代羣同態也. 以故5次交代羣之單純性, 雖不由第66節之定理, 亦自明焉.

第十三章 可遷羣之本原性及非原性

80. 非原羣.

在第63節例2所示之六次可遷羣

$$P_1=(\alpha\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5) \qquad Q=(\alpha_1\alpha_5)(\alpha_2\alpha_4)$$

$$1 \qquad Q_1=(\alpha\alpha_5)(\alpha_1\alpha_4)(\alpha_2\alpha_3)$$

$$P_2=(aa_2a_4)(a_1a_3a_5) \qquad Q_2=(aa_4)(a_1a_3)$$

$$P_3=(aa_3)(a_1a_4)(a_2a_5) \qquad Q_3=(aa_3)(a_1a_2)(a_4a_5)$$

$$P_4=(aa_4a_2)(a_1a_5a_3) \qquad Q_4=(aa_2)(a_3a_5)$$

$$P_5=(aa_5a_4a_3a_2a_1) \qquad Q_5=(aa_1)(a_2a_5)(a_3a_4)$$

中，將施行置換之文字分爲三組：

$$a,\ a_3;\ a_1,\ a_4;\ a_2,\ a_5.$$

於是，由置換 P_3，各組之文字皆於其組內移動；而由 P_1，則第一，第二，第三組之文字，分別爲第二，第三，第一之文字所置換．又由 Q，則第一組之文字不動，第二組之文字與第三組之文字相互交換；而由 Q_3，則第一組之文字於其組內移動，他組之文字，則組全體互換也．又就他之置換而觀，由羣中之置換，各組之文字，或於其組內移動，或一組全體爲他組所置換．於是在可遷羣中，其施行置換之文字得如上分成若干組時，則其羣曰**非原的**，而此等文字之組稱曰**非原系**．反之，施行置換之文字不得分成非原系時，則曰可遷羣爲**本原的**，而此羣遂呼爲**本原羣**或單曰**原羣**．

在非原羣中，其非原系之取法，幷不限於唯一的．如於上例之羣，將文字分爲

$$a,\ a_2,\ a_4;\ a_1,\ a_3,\ a_5$$

之二組，亦作成非原系也．

但在一個已定之取法中，則各非原系，乃由同數之文

字而成焉. 蓋於非原羣 $\mathfrak{G}$, 以

$$(1) \qquad \alpha,\ \alpha_1,\ \cdots\cdots,\ \alpha_{a-1}$$

$$(2) \qquad \beta,\ \beta_1,\ \cdots\cdots,\ \beta_{b-1}$$

爲非原系之二, 則 $\mathfrak{G}$ 因爲可遷的, 故含將 α 置換爲 β 者之置換也. 以此爲 S, 則因 (1), (2) 爲非原系, 故由 S, (1) 之文字不得不全部爲 (2) 之文字所置換; 而由 S^{-1}, (2) 之文字又不得不全數爲 (1) 之文字所置換. 是則兩非原系有同數之文字也.

其次, 非原羣乃一重可遷, 決不爲二重可遷的也. 蓋若假定上記之非原羣 $\mathfrak{G}$ 爲二重可遷, 則 α 不動而 α_1 置換爲 β 者之置換存在, 因而與 (1), (2) 爲非原系之假設矛盾故耳.

81. 傍系置換表示之本原性及非原性

設 $\mathfrak{G}$ 爲 g 元羣,

$$(1) \qquad G_0,\ G_1,\ \cdots\cdots,\ G_{g-1} \quad (G_0=1)$$

爲其元素. 又以 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之約羣, 而就之分 $\mathfrak{G}$ 爲傍系, 如

$$(2) \qquad \mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1}.$$

於是傍系上所行之 g 個置換

$$(3) \quad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix} \quad (i=0,1,2,\cdots\cdots,g-1),$$

乃作一與 $\mathfrak{G}$ 同態之羣焉. 此表示以 $(\mathfrak{G})$ 示之.

茲先假定 $(\mathfrak{G})$ 爲非原的, 而其非原系中含有 $\mathfrak{H}$ 者以爲

$$(4)\qquad \mathfrak{H},\ \mathfrak{H}S_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}\quad (1<m<n).$$

今取屬於此諸傍系中任意一個 $\mathfrak{H}S_t$ 之任意元素 HS_t (H 爲 $\mathfrak{H}$ 之任意元素)，則與此元素對應之 $(\mathfrak{G})$ 之置換，由 (3) 爲

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1} & \mathfrak{H}T_1 & \cdots\cdots \\ \mathfrak{H}HS_t & \mathfrak{H}S_1HS_t & \cdots\cdots & \mathfrak{H}S_{m-1}HS_t & \mathfrak{H}T_1HS_t & \cdots\cdots \end{pmatrix}$$

也．然

$$\mathfrak{H}HS_t=\mathfrak{H}S_t\quad (0\leqq t\leqq m-1).$$

故由此置換，$\mathfrak{H}$ 乃爲非原系 (4) 之一項 $\mathfrak{H}S_t$ 所置換．因之由非原系之定義，(4) 中之他項，亦不得不爲 (4) 之項所置換也．是卽

$$\mathfrak{H}HS_t,\ \mathfrak{H}S_1HS_t\ \cdots\cdots,\ \mathfrak{H}S_{m-1}HS_t,$$

在某順序言，乃與 (4) 一致耳．因之由此傍系之任意一個，取任意之元素 $H'S_rHS_t$ (H' 爲 $\mathfrak{H}$ 之元素)，則此元素定必屬於 (4) 之某一個．卽

$$H'S_rHS_t=H''S_u\ (0\leqq u\leqq m-1),$$

但 H'' 爲 $\mathfrak{H}$ 之一元素．由此式以觀，含於傍系 (4) 中任意二元素之積又仍含於 (4) 可知也．故屬於傍系 (4) 中所有之元素成羣焉．換言之，若令

$$(5)\qquad \mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1},$$

則 $\mathfrak{K}$ 爲含 $\mathfrak{H}$ 者之 $\mathfrak{G}$ 之約羣也．以故 $(\mathfrak{G})$ 若爲非原的，則非原系中之含有 $\mathfrak{H}$ 者，乃作 $\mathfrak{G}$ 之約羣焉．

反之，若屬於 (4) 之傍系之元素相集而成羣時，卽 (5) 中

之$\mathfrak{R}$爲$\mathfrak{G}$之眞約羣時,請就此一論之.

$\mathfrak{G}$就$\mathfrak{R}$分爲傍系,若爲

$$\mathfrak{G}=\mathfrak{R}+\mathfrak{R}T_1+\cdots\cdots+\mathfrak{R}T_{l-1}\quad (l>1), \tag{6}$$

則(2)式得換書之爲

$$\begin{aligned}\mathfrak{G}=&\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}\\&+\mathfrak{H}T_1+\mathfrak{H}S_1T_1+\cdots\cdots+\mathfrak{H}S_{m-1}T_1\\&+\cdots\cdots\cdots\cdots\cdots\cdots\\&+\mathfrak{H}T_{l-1}+\mathfrak{H}S_1T_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}T_{l-1},\end{aligned} \tag{7}$$

而($\mathfrak{G}$)之置換(3)乃得表示如次:

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots & \mathfrak{H}S_{m-1} & \mathfrak{H}T_1 & \cdots & \mathfrak{H}S_{m-1}T_1 & \cdots & \mathfrak{H}T_{l-1} & \cdots & \mathfrak{H}S_{m-1}T_{l-1}\\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots & \mathfrak{H}S_{m-1}G_i & \mathfrak{H}T_1G_i & \cdots & \mathfrak{H}S_{m-1}T_1G_i & \cdots & \mathfrak{H}T_{l-1}G_i & \cdots & \mathfrak{H}S_{m-1}T_{l-1}G_i\end{pmatrix}. \tag{8}$$

由此置換,則含於傍系* $\mathfrak{R}T_r$之傍系(關於$\mathfrak{H}$者)

$$\mathfrak{H}T_r,\ \mathfrak{H}S_1T_r,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_r \tag{9}$$

分別爲

$$\mathfrak{H}T_rG_i,\ \mathfrak{H}S_1T_rG_i,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_rG_i \tag{10}$$

所置換. 然此等相集而作傍系$\mathfrak{R}T_rG_i$, 卽

$$\mathfrak{R}T_rG_i=\mathfrak{H}T_rG_i+S\mathfrak{H}_1T_rG_i+\cdots\cdots+\mathfrak{H}S_{m-1}T_rG_i.$$

故若$\mathfrak{R}T_rG_i=\mathfrak{R}T_r$, 則(10)與(9)一致, 因之由置換(8),(9)之傍系僅於其自身間移動已也. 反之, 若$\mathfrak{R}T_rG_i\neq\mathfrak{R}T_r$, 則含於$\mathfrak{R}T_r$之傍系(9), 全體爲含於$\mathfrak{R}T_rG_i$之傍系(10)所置換. 因之若將屬於$\mathfrak{H}$之傍系分爲次之$l$個組:

---

* 以$T_0=1$, 卽$\mathfrak{R}T_0=\mathfrak{R}$.

$$(11)\quad \begin{cases} \mathfrak{H},\ \mathfrak{H}S_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1} \\ \mathfrak{H}T_1,\ \mathfrak{H}S_1T_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{H}T_{l-1},\ \mathfrak{H}S_1T_{l-1},\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_{l-1}, \end{cases}$$

則各組之傍系，由$(\mathfrak{G})$之置換，或於其組內移動，或一組全體爲他組所置換也．卽上之各組，形成一非原系焉．如是，含$\mathfrak{H}$之眞約羣$\mathfrak{K}$存在於$\mathfrak{G}$時，則$(\mathfrak{G})$爲非原的．綜合上述，得次

定理．在一個羣中，其關於約羣$\mathfrak{H}$之傍系置換表示，或爲本原的，或爲非原的，由$\mathfrak{H}$之爲極大或不爲極大而定．如含$\mathfrak{H}$之眞約羣$\mathfrak{K}$存在，且爲

$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}$$

時，則傍系$\mathfrak{H}$，$\mathfrak{H}S_1$，……，$\mathfrak{H}S_{m-1}$，乃在關於$\mathfrak{H}$之傍系置換表示中，形成一非原系．反之，此等傍系成一非原系時，則$\mathfrak{K}$爲$\mathfrak{G}$之眞約羣．

如本定理之所示，含$\mathfrak{H}$之約羣與$(\mathfrak{G})$中之非原系成爲一一對應．以故上記之約羣$\mathfrak{K}$，呼曰與非原系$\mathfrak{H}$，$\mathfrak{H}S_1$，……，$\mathfrak{H}S_{m-1}$對應之約羣焉．

注意．極大之意義，乃與正常約羣中者(第48節)同樣．卽$\mathfrak{H}$爲$\mathfrak{G}$之約羣，而$\mathfrak{G}$及$\mathfrak{M}$以外，含$\mathfrak{M}$之約羣不存在時，$\mathfrak{M}$曰極大云．

82. 非原系之置換羣．

在前節之傍系置換表示(𝔊)中,傍系

$$(4)\qquad \mathfrak{H},\ \mathfrak{H}S_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}\quad (1<m<n)$$

作一非原系時,則如前節之所述,

$$(5)\qquad \mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}$$

乃羣也,而非原系之全部,由前節(11)而盡得之焉. 於是非原系分別作成關於$\mathfrak{K}$之傍系

$$(12)\quad \begin{cases} \mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1} \\ \mathfrak{K}T_1=\mathfrak{H}T_1+\mathfrak{H}S_1T_1+\cdots\cdots+\mathfrak{H}S_{m-1}T_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{K}T_{l-1}=\mathfrak{H}T_{l-1}-\mathfrak{H}S_1T_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}T_{l-1} \end{cases}$$

因之關於$\mathfrak{K}$之傍系,直視之爲非原系可.

且由𝔊之置換(8),傍系

$$(9)\qquad \mathfrak{H}T_r,\ \mathfrak{H}S_1T_r,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_r,$$

分別爲

$$(10)\qquad \mathfrak{H}T_rG_i,\ \mathfrak{H}S_1T_rG_i,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_rG_i$$

所置換. 然(9)與(10)共於(𝔊)爲非原系,而

$$\mathfrak{H}T_r+\mathfrak{H}S_1T_r+\cdots\cdots+\mathfrak{H}S_{m-1}T_r=\mathfrak{K}T_\gamma,$$

$$\mathfrak{H}T_rG_i+\mathfrak{H}S_1T_rG_i+\cdots\cdots+\mathfrak{H}S_{m-1}T_rG_i=\mathfrak{K}T_rG_i,$$

故若置非原系內傍系(關於$\mathfrak{H}$者)之移動於不顧,而僅注目於其非原系全體之移動,則由置換(8),$\mathfrak{K}T_r$遂爲$\mathfrak{K}T_rG_i$所置換. 卽伴乎(𝔊)之置換(8),非原系之間乃生次之置換也(非原系卽視爲關於$\mathfrak{K}$之傍系者):

(13)　$$\begin{pmatrix} \mathfrak{R} & \mathfrak{R}T_1 & \cdots\cdots & \mathfrak{R}T_{l-1} \\ \mathfrak{R}G_i & \mathfrak{R}T_1G_i & \cdots\cdots & \mathfrak{R}T_{l-1}G_i \end{pmatrix}.$$

於此而令 $i=0, 1, 2, \cdots\cdots, g-1$, 則得伴 $(\mathfrak{G})$ 之各置換而生之非原系之置換之全部. 而此又不外乎關於 $\mathfrak{R}$ 之傍系置換表示已也. 因之得次之結論:

$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{m-1}$ 若於 $(\mathfrak{G})$ 作非原系時, 則伴 $(\mathfrak{G})$ 之置換而生之非原系之置換成羣也; 而此羣乃與關於 $\mathfrak{R}(=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1})$ 之傍系置換表示一致. 此羣爰名曰非原羣 $(\mathfrak{G})$ 中之**非原系之置換羣**焉.

次以共軛約羣

$$\mathfrak{R}, T_1^{-1}\mathfrak{R}T_1, \cdots\cdots, T_{l-1}^{-1}\mathfrak{R}T_{l-1}$$

之最大公約羣* 爲 $\mathfrak{C}$, 其元素爲

$$C_0, C_1, \cdots\cdots, C_{c-1},$$

則在非原系之置換羣卽關於 $\mathfrak{R}$ 之傍系置換表示 [以 $((\mathfrak{G}))$ 記之] 中, 與 $\mathfrak{C}$ 之元素對應之置換

(14)　$$\begin{pmatrix} \mathfrak{R} & \mathfrak{R}T_1 & \cdots\cdots & \mathfrak{R}T_{l-1} \\ \mathfrak{R}C_j & \mathfrak{R}T_1C_j & \cdots\cdots & \mathfrak{G}T_{l-1}C_j \end{pmatrix} \quad (j=0, 1, 2; \cdots\cdots, c-1)$$

皆爲不動的也 (參照第 75 節). 故 $(\mathfrak{G})$ 中 c 個之置換

(15)　$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1} & \mathfrak{H}T_1 & \mathfrak{H}S_1T_1 & \cdots\cdots \\ \mathfrak{H}C_j & \mathfrak{H}S_1C_j & \cdots\cdots & \mathfrak{H}S_{m-1}C_j & \mathfrak{H}T_1C_j & \mathfrak{H}S_1T_1C_j & \cdots\cdots \end{pmatrix}$$

$$j=0, 1, \cdots\cdots, c-1$$

---

* 此羣於 $\mathfrak{G}$ 爲正常的 (第 34 節).

乃將各傍系(關於$\mathfrak{H}$者)於其所屬非原系內移動. 反之,($(\mathfrak{G})$)之置換中之不動置換僅上記之(14)(參照第75節). 因之於($\mathfrak{G}$)中使各傍系於其所屬非原系內移動之置換僅上記之(15). 又他方就($\mathfrak{G}$)與$\mathfrak{G}$之同態關係言,置換(15)乃與$\mathfrak{G}$之正常約羣$\mathfrak{C}$之元素對應者. 以故此諸置換於($\mathfrak{G}$)作正常約羣[以($\mathfrak{C}$)示之]焉. 卽:

於($\mathfrak{G}$),使各傍系於其所屬非原系內移動之置換,形成正常約羣($\mathfrak{C}$). 而($\mathfrak{C}$)若含有不動置換以外之置換時,則此羣明爲非遷的.

更就($(\mathfrak{G})$)與($\mathfrak{G}$)之同態關係言,對於($(\mathfrak{G})$)之置換 $\begin{pmatrix}\mathfrak{R} & \mathfrak{R}T_1 & \cdots\cdots\\ \mathfrak{R}G_i & \mathfrak{R}T_1G_i & \cdots\cdots\end{pmatrix}$,使($\mathfrak{G}$)之置換 $\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots\\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots\end{pmatrix}$與之對應,由是兩羣爲同態,而對($(\mathfrak{G})$)之不動置換卽(14),($\mathfrak{G}$)之正常約羣($\mathfrak{C}$)相與對應. 故與第75節中者同樣,非原系之置換羣($(\mathfrak{G})$)與($\mathfrak{G}$)/($\mathfrak{C}$)爲單純同態可知也. 特別當($\mathfrak{C}$)爲主元素羣時,($(\mathfrak{G})$)與($\mathfrak{G}$)之同態關係雖爲單純的,否則爲重複的焉.

83. 今請將前二節所得之結果,應用於由文字上所行置換而成之一般可遷羣.

茲取n文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$之可遷羣爲前節中之羣$\mathfrak{G}$,而以文字$\alpha$不動之約羣爲其$\mathfrak{H}$. 又以$S_i$表示以$\alpha$置換爲$\alpha_i$之置換之一,則由第76節所述,($\mathfrak{G}$)與$\mathfrak{G}$爲同值. 卽($\mathfrak{G}$)者,乃以傍系$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{n-1}$代替文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$而由$\mathfrak{G}$所得者也. 因之由第81節定理,直得次之定理焉.

定理. 於可遷羣$\mathfrak{G}$, 若其特定一文字不動之約羣$\mathfrak{H}$不爲極大時, 則$\mathfrak{G}$爲非原的. 反之, $\mathfrak{G}$若爲非原的, 則$\mathfrak{H}$不爲極大. 又$a, a_1, \cdots\cdots, a_{m-1}$作非原系時, 若令

$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1} \quad (1<m<n),$$

則$\mathfrak{K}$爲$\mathfrak{G}$之約羣, 但$\mathfrak{H}$爲a不動之約羣, 而S_i爲將a置換爲a_i之置換之一. 反之, 若$\mathfrak{K}$爲$\mathfrak{G}$之約羣時, 則$a, a_1, \cdots\cdots, a_{m-1}$作非原系.

如本定理之所示, 其含$\mathfrak{H}$之眞約羣與$\mathfrak{G}$中之非原系乃成一一對應也. 於是與第81節同樣, 上記之約羣$\mathfrak{K}$, 呼曰與非原系$a, a_1, \cdots\cdots, a_{m-1}$對應之約羣焉.

例. 令 $P=(012345678)$, $Q=(18)(27)(36)(45)$,

則 $$Q^{-1}PQ=P^{-1},$$

因之 $$Q^{-1}\{P\}Q=\{P\}.$$

故9元巡回羣$\{P\}$與2元羣$\{Q\}$之積作一18元羣(參照第27節第三定理之系). 以之名曰$\mathfrak{G}$, 則$\mathfrak{G}$之爲9次可遷羣甚明, 而其中文字0不動之約羣乃$\{Q\}$也. 但約羣$\{Q\}$非極大. 蓋由最初之式, 乃有

$$Q^{-1}P^3Q=P^{-3}=P^6,$$

故 $$Q^{-1}\{P^3\}Q=\{P^3\}.$$

於是與前同樣, 兩羣$\{P^3\}, \{Q\}$之積作一6元羣. 之羣也, 當然爲$\mathfrak{G}$之約羣. 故$\{Q\}$於$\mathfrak{G}$非極大也.

次之, 將此6元約羣就$\{Q\}$而分爲傍系, 則得

$$\{Q\}\{P^3\}=\{Q\}+\{Q\}P^3+\{Q\}P^6.$$

而 P^3, P^6 乃將文字 0 分別置換爲 3 與 6. 故由本節定理,

$$0,\quad 3,\quad 6$$

作一非原系. 而他之非原系, 分別爲

$$1,\quad 4,\quad 7$$

及

$$2,\quad 5,\quad 8$$

焉. 今爲此更求明瞭起見, 乃將 $\mathfrak{G}$ 之置換全部書之於下:

1	(18)(27)(36)(45)
(012345678)	(08)(17)(26)(35)
(024681357)	(07)(16)(25)(34)
(036)(147)(258)	(06)(15)(24)(78)
(048372615)	(05)(14)(23)(68)
(051627384)	(04)(13)(58)(67)
(063)(174)(285)	(03)(12)(48)(57)
(075318642)	(02)(38)(47)(56)
(087654321)	(01)(28)(37)(46)

系 1. 可遷羣, 其施行置換之文字中特定一個不動之置換, 若其中之任何個皆使二或二以上之文字不動時, 則此羣爲非原的.

證明. 設 $\mathfrak{G}$ 爲由文字 $a, a_1, \cdots\cdots, a_{n-1}$ 上所行置換而成之可遷羣. $\mathfrak{G}$ 中 a 不動之置換所作之約羣爲 $\mathfrak{H}$, 而由 $\mathfrak{H}$ 全部之置換全然不動之文字爲次之 m 個:

(1)　　$a, a_1, \cdots\cdots, a_{m-1}$　$(1<m<n)$.

(但他之文字,皆以之爲由 $\mathfrak{H}$ 之任何置換而均移動者.) 於是 $\mathfrak{H}$ 之正常化羣,由第 63 節第三定理爲

$$\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1},$$

但 $S_1, S_2, \cdots\cdots, S_{m-1}$ 爲將 a 分別置換爲 $a_1, a_2, \cdots\cdots, a_{m-1}$ 之置換. 因之由定理,(1) 遂作 $\mathfrak{G}$ 中之非原系焉.

例. 試就第 63 節例 2 中 6 次可遷羣而觀,其 a 不動之約羣 $\mathfrak{H}$ 之置換,又不使 a_3 動也. 故 a, a_3 作非原系而此羣爲非原的. 第 80 節所揭之例卽此.

注意. 如本節定理之例所示,此系之逆命題不成立也.

系 2. 可遷羣,若由其施行置換之文字中,得選擇適合次之條件一組之文字時,則此等文字作一非原系,隨之其羣爲非原的. 卽:將屬於該組之某一文字,以同組之文字置換之之各置換,乃使其組之文字於其自身間移動者.

證明. 於第 81 節之傍系置換表示 ($\mathfrak{G}$) 中,以其將 $\mathfrak{H}$ 置換爲

(4)　　$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{m-1}$

之一之置換爲使此等傍系於其自身間移動者. 於是對於此諸傍系中任意之元素 HS_t (H 爲 $\mathfrak{H}$ 之元素),乃有

$$\mathfrak{H}HS_t=\mathfrak{H}S_t,$$

故 ($\mathfrak{G}$) 之置換

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1} & \cdots\cdots \\ \mathfrak{H}HS_t & \mathfrak{H}S_1HS_t & \cdots\cdots & \mathfrak{H}S_{m-1}HS_t & \cdots\cdots \end{pmatrix} \quad (0 \leqq t \leqq m-1),$$

不得不使傍系(4)於其自身間移動也. 以故傍系

$$\mathfrak{H}HS_t,\ \mathfrak{H}S_1HS_t,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}HS_t$$

與(4)一致. 因之與該節中者同樣,知屬於傍系(4)之元素成羣,而由同節定理,(4)之傍系於(𝔊)中作非原系也.

於此所得之結果,與導出本節定理者同樣,若將傍系(4)以文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 置換之,則得本系焉.

例. 於第80節中所示之羣,取其三文字

$$\alpha,\quad \alpha_2,\quad \alpha_4,$$

其將 α 置換爲 α, α_2 或 α_4 之置換爲

$$1,\ Q,\ P_2,\ Q_4,\ P_4,\ Q_2,$$

而對此各置換上之三文字,乃於其自身間移動. 故 $\alpha, \alpha_2, \alpha_4$ 作非原系.

其次,爲將前節之結果適用於一般非原羣計,乃以 $\mathfrak{G}$, $\mathfrak{H}$, S_i 爲具有本節開始所示之同一意義者,而 m 文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 則於 $\mathfrak{G}$ 中作非原系. 於是因(𝔊)與 $\mathfrak{G}$ 同值,故 m 傍系 $\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{m-1}$ 亦於(𝔊)作非原系. 故伴 $\mathfrak{G}$ 之置換而生之非原系之置換,乃作(𝔊)中非原系之置換羣,即與關於 $\mathfrak{R}\ (=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1})$ 之傍系置換表示((𝔊))同值之羣也,因之得次

定理. 於可遷羣 $\mathfrak{G}$,其施行置換之文字得分爲若干個

非原系時，則伴 $\mathfrak{G}$ 之置換而生之非原系之置換成羣；而此羣則與關於一約羣之對應一非原系者之傍系置換表示 $(\mathfrak{G}$ 的$)$ 同值.

系. 設對應於一非原系之約羣爲 $\mathfrak{N}$，而與 $\mathfrak{N}$ 共軛之全部約羣之最大公約羣爲 $\mathfrak{C}$，則非原系之置換羣與 $\mathfrak{G}/\mathfrak{C}$ 爲單純同態.

證明. 由本定理及第75節定理即得.

又因關於 $\mathfrak{H}$ 之傍系置換表示 $(\mathfrak{G})$ 中之使各傍系於其所屬非原系內移動之置換，如前節所示，作正常約羣 $(\mathfrak{C})$；以及 $\mathfrak{G}$ 與 $(\mathfrak{G})$ 同值之二者遂得次

定理. 於一非原羣，其使施行置換之文字於各所屬非原系內移動之置換，形成一正常約羣. 而此正常約羣，乃爲約羣之對應於一非原系者之共軛羣全部之最大公約羣.

例. 於第80節所示之六次非原羣 $\mathfrak{G}$，其非原系

$$\alpha,\ \alpha_3;\ \alpha_1,\ \alpha_4;\ \alpha_2,\ \alpha_5,$$

分別以 A, B, Γ 示之. $\mathfrak{G}$ 中 α 不動之約羣爲

$$\mathfrak{H}:\ 1,\ Q,$$

而與非原系 α, α_3 對應之約羣爲

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}P_3.$$

因之

$$\mathfrak{G}=\mathfrak{N}+\mathfrak{N}P_1+\mathfrak{N}P_2.$$

復次作$\mathfrak{R}$之共軛約羣,則有

$$\mathfrak{R}: 1, Q, P_3, Q_3 (=QP_3);$$

$$P_1^{-1}\mathfrak{R}P_1: 1, Q_4, P_3, Q_1;$$

$$P_2^{-1}\mathfrak{R}P_2: 1, Q_2, P_3, Q_5;$$

而其最大公約羣,則爲

$$\mathfrak{C}: 1, P_3.$$

就$\mathfrak{G}$之各置換而觀,其使各文字於其所屬非原系內移動之置換,僅此二者而已. 是與上第三定理之主張一致也.

次之將$\mathfrak{G}$就$\mathfrak{C}$分爲傍系,則有

$$\mathfrak{G}=\mathfrak{C}+\mathfrak{C}P_1+\mathfrak{C}P_2+\mathfrak{C}Q+\mathfrak{C}Q_4+\mathfrak{C}Q_2,$$

因之關於$\mathfrak{R}$之傍系置換表示中之互異之置換爲次之六個(參照第75節).

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\end{pmatrix}=1,$$

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_1 & \mathfrak{R}P_1P_1 & \mathfrak{R}P_2P_1\end{pmatrix}=\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_1 & \mathfrak{R}P_2 & \mathfrak{R}\end{pmatrix}=(\mathfrak{R}, \mathfrak{R}P_1, \mathfrak{R}P_2),$$

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_2 & \mathfrak{R}P_1P_2 & \mathfrak{R}P_2P_2\end{pmatrix}=\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_2 & \mathfrak{R} & \mathfrak{R}P_1\end{pmatrix}=(\mathfrak{R}, \mathfrak{R}P_2, \mathfrak{R}P_1),$$

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}Q & \mathfrak{R}P_1Q & \mathfrak{R}P_2Q\end{pmatrix}=\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R} & \mathfrak{R}P_2 & \mathfrak{R}P_1\end{pmatrix}=(\mathfrak{R}P_1, \mathfrak{R}P_2),$$

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}Q_4 & \mathfrak{R}P_1Q_4 & \mathfrak{R}P_2Q_4\end{pmatrix}=\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_2 & \mathfrak{R}P_1 & \mathfrak{R}\end{pmatrix}=(\mathfrak{R}P_2, \mathfrak{R}),$$

$$\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}Q_2 & \mathfrak{R}P_1Q_2 & \mathfrak{R}P_2Q_2\end{pmatrix}=\begin{pmatrix}\mathfrak{R} & \mathfrak{R}P_1 & \mathfrak{R}P_2\\ \mathfrak{R}P_1 & \mathfrak{R} & \mathfrak{R}P_2\end{pmatrix}=(\mathfrak{R}, \mathfrak{R}P_1).$$

終之，就$\mathfrak{G}$之各置換，而察與是相伴之非原系 A, B, Γ 之置換，再將此結果與上之傍系置換表示共記之，則得次表：

羣之置換	非原系之置換	關於$\mathfrak{R}$之傍系之置換
$1,\ P_3$	1	1
$P_1, P_4\ (=P_3P_1)$	(ABΓ)	$(\mathfrak{R}, \mathfrak{R}P_1, \mathfrak{R}P_2)$
$P_2, P_5\ (=P_3P_2)$	(AΓB)	$(\mathfrak{R}, \mathfrak{R}P_2, \mathfrak{R}P_1)$
$Q_1, Q_3\ (=P_3Q)$	(BΓ)	$(\mathfrak{R}P_1, \mathfrak{R}P_2)$
$Q_4, Q_1\ (=P_3Q_4)$	(ΓA)	$(\mathfrak{R}P_2, \mathfrak{R})$
$Q_2, Q_5\ (=P_3Q_2)$	(AB)	$(\mathfrak{R}, \mathfrak{R}P_1)$

此表乃將羣之某置換，其相伴之非原系之置換，以及與之對應之傍系之置換記於同一列者也.

再就此表而觀，可知非原系之置換羣乃與關於約羣$\mathfrak{R}$之對應於非原系α, α_3者之傍系置換表示爲同值.

84. 非遷正常約羣.

如前節第三定理之所示，在非原羣中，使各文字於其所屬非原系內移動之置換，除主元素外尙存在時，則此等置換，作此羣之非遷正常約羣也. 此定理之逆亦成立. 卽：

定理. 可遷羣$\mathfrak{G}$若有非遷正常約羣$\mathfrak{N}$時，則$\mathfrak{G}$爲非原的. 而$\mathfrak{N}$中之可遷系作$\mathfrak{G}$中之非原系.

證明. 令$\mathfrak{N}$中可遷系之一爲

$$A: \quad \alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}.$$

而以α爲系A之文字α_i所置換之任意置換爲S; 且由是而系A之文字α_j得爲x所置換者. 卽

$$S=\begin{pmatrix}\alpha \cdots\cdots \alpha_j \cdots\cdots\\ \alpha_i \cdots\cdots x \cdots\cdots\end{pmatrix},$$

但x爲$\mathfrak{G}$中得以施行置換之文字之一. 此x若表示爲屬於系A者, 則由前節第一定理系2, $\mathfrak{G}$爲非原的, 而系A卽爲其非原系.

元來系A在$\mathfrak{N}$中爲可遷系, 故$\mathfrak{N}$含有將α置換爲α_j之置換. 以其一爲

$$N=\begin{pmatrix}\alpha \cdots\cdots\\ \alpha_j \cdots\cdots\end{pmatrix};$$

而以S變其形, 則得

$$S^{-1}NS=\begin{pmatrix}\alpha_i \cdots\cdots\\ x \cdots\cdots\end{pmatrix},$$

卽$S^{-1}NS$者乃以x置換α_i者也. 然$\mathfrak{N}$爲正常, 故此置換屬於$\mathfrak{N}$. 是則x非與α_i屬於同一可遷系不可, 卽系A之文字也.

系. 原羣之正常約羣爲可遷的.

例. 第80節所示之可遷羣(名之曰$\mathfrak{G}$), 其三置換1, P_2, P_4, 作非遷正常約羣甚明. 而其可遷系α, α_2, α_4以及α_1, α_3, α_5, 則如該節之所示, 作$\mathfrak{G}$之非原系焉.

注意. 在本例之羣$\mathfrak{G}$中, 其使兩非原系α, α_2, α_4及α_1,

a_3, a_5之文字於其所屬系內移動之置換，除上之三置換外，爲 Q, Q_2 Q_4 之三也.

85. 非原系之選法.

設 $\mathfrak{H}$ 爲羣 $\mathfrak{G}$ 之約羣，而

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1}.$$

至 $\mathfrak{G}$ 之傍系置換表示(關於 $\mathfrak{H}$ 者)，則與第 81 節同樣，以 $(\mathfrak{G})$ 示之.

若含 $\mathfrak{H}$ 之 $\mathfrak{G}$ 之眞約羣 $\mathfrak{K}$ 存在，而

$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}$$

時，則傍系

$$\mathfrak{H},\ \mathfrak{H}S_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}$$

於 $(\mathfrak{G})$ 作非原系；反之此諸傍系作非原系時，則 $\mathfrak{K}$ 爲羣(第 81 節定理). 故 $\mathfrak{G}$ 爲非原羣時，則含 $\mathfrak{H}$ 之眞約羣與 $(\mathfrak{G})$ 中之非原系成一一對應. 因之 $(\mathfrak{G})$ 中非原系之選法有幾，由 $\mathfrak{G}$ 中含 $\mathfrak{H}$ 之眞約羣有幾而定. 卽兩者之數一致也.

此結果，由第 83 節開始所述之方法，直可適用之於可遷羣. 如第 80 節所示之羣(名曰 $\mathfrak{G}'$)，其文字 α 不動之約羣若爲 $\mathfrak{H}'$，則爲

$$\mathfrak{H}':\ 1,\ Q,$$

而
$$\mathfrak{G}'=\mathfrak{H}'+\mathfrak{H}'P_1+\mathfrak{H}'P_2+\mathfrak{H}'P_3+\mathfrak{H}'P_4+\mathfrak{H}'P_5.$$

於是含 $\mathfrak{H}'$ 之約羣爲次之二：

$$\mathfrak{K}_1'=\mathfrak{H}'+\mathfrak{H}'P_3,$$

$$\mathfrak{R}_2' = \mathfrak{H}' + \mathfrak{H}'P_2 + \mathfrak{H}'P_4.$$

故 $\mathfrak{G}$ 中非原系之選法有次之二種:

$$a, a_3 \text{ (因之其他爲 } a_1, a_4; a_2, a_5);$$

$$a, a_2, a_4 \text{ (因之其他爲 } a_1, a_3, a_5).$$

再於表示 $(\mathfrak{G})$ 就其中之非原系得以二種方法選擇之者一言. 兩非原系(含有 $\mathfrak{H}$)除 $\mathfrak{H}$ 外有共通之傍系時,則此等共通傍系($\mathfrak{H}$ 亦包含在內)復於 $(\mathfrak{G})$ 作非原系也. 何以故? 因此之共通傍系,作對應於兩非原系之約羣之最大公約羣故. 又因約羣之元數爲羣之元數之約數,故此時共通傍系之個數爲兩非原系中傍系之個數之公約數甚明. 此結果,以應用於可遷羣,則得次之定理:

在非原羣中,其施行置換之文字得以二種方法分爲非原系,而一方之某系與他方之某系含有二個以上之公共文字時,則此等公共文字又作一非原系. 而公共文字之數,則爲上兩非原系中文字之數之公約數.

例. 令 $P=(012345)(0'1'2'3'4'5'),$

$$Q=(15)(24)(1'5')(2'4'),$$

$$R=(00')(11')(22')(33')(44')(55').$$

於是因

$$Q^{-1}PQ=P^{-1}, \quad \text{隨之} \quad Q^{-1}\{P\}Q=\{P\}$$

之故, $\{P\}$, $\{Q\}$ 之積乃作一 12 元羣,而以 $\mathfrak{C}$ 表之. 次則 R 與 $\mathfrak{C}$ 之各元素爲交換可能甚明. 故 $\mathfrak{C}$ 與 $\{R\}$ 之積作如下之

24 元羣:

$$1$$

$$P=(012345)(0'1'2'3'4'5')$$

$$P^2=(024)(135)(0'2'4')(1'3'5')$$

$$P^3=(03)(14)(25)(0'3')(1'4')(2'5')$$

$$P^4=(042)(153)(0'4'2')(1'5'3')$$

$$P^5=(054321)(0'5'4'3'2'1')$$

$$Q=(15)(24)(1'5')(2'4')$$

$$PQ=(05)(14)(23)(0'5')(1'4')(2'3')$$

$$P^2Q=(04)(13)(0'4')(1'3')$$

$$P^3Q=(03)(12)(45)(0'3')(1'2')(4'5')$$

$$P^4Q=(02)(35)(0'2')(3'5')$$

$$P^5Q=(01)(25)(34)(0'1')(2'5')(3'4')$$

$$R=(00')(11')(22')(33')(44')(55')$$

$$PR=(01'23'45')(0'12'34'5)$$

$$P^2R=(02'40'24')(13'51'35')$$

$$P^3R=(03')(14')(25')(0'3)(1'4)(2'5)$$

$$P^4R=(04'20'42')(15'31'53')$$

$$P^5R=(05'43'21')(0'54'32'1)$$

$$QR=(00')(15')(24')(1'5)(2'4)$$

$$PQR=(05')(14')(23')(0'5)(1'4)(2'3)$$

$$P^2QR=(04')(13')(0'4)(1'3)(22')(55')$$

$$P^3QR=(03')(12')(45')(0'3)(1'2)(4'5)$$

$$P^4QR=(02')(35')(0'2)(3'5)(11')(44')$$

$$P^5QR=(01')(25')(34')(0'1)(2'5)(3'4).$$

是中文字0不動之約羣爲

$$\mathfrak{H}:\ 1,\ Q,$$

而就之分$\mathfrak{G}$爲傍系，則爲

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P+\mathfrak{H}P^2+\mathfrak{H}P^3+\mathfrak{H}P^4+\mathfrak{H}P^5$$
$$+\mathfrak{H}R+\mathfrak{H}PR+\mathfrak{H}P^2R+\mathfrak{H}P^3R+\mathfrak{H}P^4R+\mathfrak{H}P^5R.$$

其含$\mathfrak{H}$之約羣則爲次之六個：

$$\mathfrak{K}_1=\mathfrak{H}+\mathfrak{H}P^3,$$

$$\mathfrak{K}_2=\mathfrak{H}+\mathfrak{H}P^2+\mathfrak{H}P^4,$$

$$\mathfrak{K}_3=\mathfrak{H}+\mathfrak{H}P+\mathfrak{H}P^2+\mathfrak{H}P^3+\mathfrak{H}P^4+\mathfrak{H}P^5,$$

$$\mathfrak{K}_4=\mathfrak{H}+\mathfrak{H}R,$$

$$\mathfrak{K}_5=\mathfrak{H}+\mathfrak{H}P^3+\mathfrak{H}R+\mathfrak{H}P^3R$$

$$\mathfrak{K}_6=\mathfrak{H}+\mathfrak{H}P^2+\mathfrak{H}P^4+\mathfrak{H}R+\mathfrak{H}P^2R+\mathfrak{H}P^4R;$$

而與是相對應之非原系，分別爲

0, 3 (1, 4; 2, 5; 0′, 3′; 1′, 4′; 2′, 5′),

0, 2, 4 (1, 3, 5; 0′, 2′, 4′; 1′, 3′, 5′),

0, 1, 2, 3, 4, 5 (0′, 1′, 2′, 3′, 4′, 5′),

0, 0′ (1, 1′; 2, 2′; 3, 3′; 4, 4′; 5, 5′),

0, 3, 0′, 3′ (1, 4, 1′, 4′; 2, 5, 2′, 5′),

0, 2, 4, 0′, 2′, 4′ (1, 3, 5, 1′, 3′, 5′)

但括弧內者,爲由含0之非原系當然應有者也.此最後兩非原系之共通文字爲0與0′之二.而此二者,如上之第四中者然,作一非原系也.

第十四章　可遷約羣與羣之可遷重複度

86. 定理. 可遷羣之含轉換者,爲非原的或爲對稱的

證明. 設𝔊爲n文字$a, a_1, \cdots\cdots, a_{n-1}$之可遷羣. 𝔊若含$n-1$個之轉換

$$(aa_1), (aa_2), \cdots\cdots, (aa_{n-1})$$

時,則𝔊爲對稱的(參照第65節).

復次請就𝔊雖含$m-1$個轉換

(1)　　$(aa_1), (aa_2), \cdots\cdots, (aa_{m-1})$ $[m<n]$,

而卻不含

(2)　　$(aa_m), \cdots\cdots, (aa_{n-1})$

者論之.此時𝔊不得含由

(3)　　$a, a_1, \cdots\cdots, a_{m-1}$

之文字與不屬於此之文字而成之轉換:

$$(a_i a_{m+l}) \quad [i\leqq m-1, 0\leqq l\leqq n-m-1].$$

蓋若以(aa_i)將此變形,則有

$$(aa_i)(a_i a_{m+l})(aa_i)=(aa_{m+l}),$$

故若$(a_i a_{m+l})$含於$\mathfrak{G}$，則$(a a_{m+l})$亦必含於$\mathfrak{G}$，是與假定反也.

今於$\mathfrak{G}$，試取任意一置換S之將a置換爲(3)之文字a_i者，且以爲由S，(3)之文字a_j得爲x所置換，即

$$S=\begin{pmatrix} a \cdots\cdots a_j \cdots\cdots \\ a_i \cdots\cdots x \cdots\cdots \end{pmatrix}.$$

於是以S變$(a a_j)$之形，則得

$$S^{-1}(a a_j)S=(a_i x).$$

而由假定a_i屬於(3)；故由上述，x亦非屬於(3)不可. 因之由置換S之以(3)之文字置換a者，(3)之文字僅於其自身間移動. 故由第83節第一定理系2，(3)乃作一非原系. 是即$\mathfrak{G}$雖含$m-1$個之轉換(1)而卻不含(2)中者時，則$\mathfrak{G}$爲非原的也.

定理. *n次可遷羣之含三項巡回置換者，或爲非原的，或則含一n次交代羣以爲其約羣.*

證明. 設$\mathfrak{G}$爲n文字$a, a_1, \cdots\cdots, a_{n-1}$之可遷羣. 若$\mathfrak{G}$含有$n-2$個之三項巡回置換

$$(a a_1 a_2), (a a_1 a_3), \cdots\cdots, (a a_1 a_{n-1})$$

之全部時，則$\mathfrak{G}$或爲n次交代羣或爲對稱羣(參照第65節).

次請就$\mathfrak{G}$雖含$m-2$個之三項巡回置換

(1) $$(a a_1 a_2), (a a_1 a_3), \cdots\cdots, (a a_1 a_{m-1}),$$

而卻不含

(2) $$(a a_1 a_m), \cdots\cdots, (a a_1 a_{n-1})$$

者一論之.此時 $\mathfrak{G}$ 不得含由

(3)　　$a, a_1, \cdots\cdots, a_{m-1}$

之文字與不屬於此之文字而成之三項巡回置換 $(a_i a_j a_{m+l})$ 或 $(a_i a_{m+k} a_{m+l})$ $[i, j \leqq m-1;\ 0 \leqq k,\ l \leqq n-m-1]$. 蓋因 $\mathfrak{G}$ 含有 $m-2$ 個之巡回置換 (1), 故其非含由 (3) 之文字而成之三項巡回置換之全部不可 (參照第 65 節).是故 $\mathfrak{G}$ 若含前者,則亦不得不含以三項巡回置換 $(a_i a_r a_t)$ 之由 (3) 之文字而成者變其形所得之

$$(a_i a_r a_t)^{-1}(a_i a_j a_{m+l})(a_i a_r a_t) = (a_r a_j a_{m+l}) = (a_j a_{m+l} a_r)$$

也.於是對於 r, 與以 $0, 1, 2, \cdots\cdots, m-1$ 中 i, j 以外全部之數, 便得 $m-2$ 個之三項巡回置換.再加先頭之置換 $(a_i a_j a_{m+l})$, 則 $\mathfrak{G}$ 遂成爲含有 $m-1$ 個之三項巡回置換

$$(a_j a_{m+l} a_r),\ r = 0, 1, \cdots\cdots, j-1, j+1, \cdots\cdots, m-1,$$

卽 $\mathfrak{G}$ 不得不含由 $m+1$ 文字

$$a, a_1, \cdots\cdots, a_{m-1}, a_{m+l}$$

上所行置換而成之交代羣也(參照第 65 節). 因之 $\mathfrak{G}$ 遂含 $(a a_1 a_{m+l})$, 是與假定反. 又 $\mathfrak{G}$ 含 $(a_i a_{m+k} a_{m+l})$ 時,乃以 (3) 之文字之三項巡回置換 $(a_i a_s a_t)$ 變其形,則得

$$(a_i a_s a_t)^{-1}(a_i a_{m+k} a_{m+l})(a_i a_s a_t) = (a_s a_{m+k} a_{m+l}).$$

於是令 $s = 0, 1. \cdots\cdots, i-1, i+1, \cdots\cdots, m-1$, 而再加 $(a_i a_{m+k} a_{m+l})$, 則 $\mathfrak{G}$ 遂成爲含有 m 個之巡回置換

$$(a a_{m+k} a_{m+l}), (a_1 a_{m+k} a_{m+l}), \cdots\cdots, (a_{m-1} a_{m+k} a_{m+1}).$$

即 $\mathfrak{G}$ 不得不含由 $m+2$ 文字

$$a,\ a_1,\ \cdots\cdots,\ a_{m-1},\ a_{m+k},\ a_{m+l}$$

上所行置換而成之交代羣也. 是則 $\mathfrak{G}$ 含 (aa_1a_{m+l}), 而亦與假定反. 以故 $\mathfrak{G}$ 不得含由 (3) 之文字與不屬於此之文字而成之三項巡回置換焉.

今於 $\mathfrak{G}$ 試取一將 a 置換爲 (3) 之文字 a_i 之任意置換 S, 且以爲由 S, (3) 之文字 a_j, a_k 得分別爲 x, y 所置換, 即

$$S=\begin{pmatrix} a & \cdots\cdots & a_j & \cdots\cdots & a_k & \cdots\cdots \\ a_i & \cdots\cdots & x & \cdots\cdots & y & \cdots\cdots \end{pmatrix}$$

者. 於是以 S 將 (aa_ja_k) 變形, 則得

$$S^{-1}(aa_ja_k)\,S=(a_ixy).$$

但由假設, a_i 屬於 (3). 故由上述, x, y 亦非爲 (3) 之文字不可. 因之由 a 得以 (3) 之文字置換之之置換 S, (3) 之文字僅於其自身間移動. 故由第 83 節第一定理系 2, (3) 於 $\mathfrak{G}$ 形成一非原系. 即謂 $\mathfrak{G}$ 雖含 $m-2$ 個之三項巡回置換 (1) 而不含 (2) 中者時 $\mathfrak{G}$ 爲非原的也.

例 1. 於四次可遷羣

$$\begin{array}{cccc} 1 & (abcd) & (ac)(bd) & (adcb) \\ (ac) & (ab)(cd) & (bd) & (ad)(bc), \end{array}$$

其含 a 之轉換僅 (ac) 也. 故二文字 a, c 作非原系, 因之此羣爲非原的. 又他之非原系則爲 b, d.

例 2. 於六次可遷羣

1	(ace)	(bdf)
$(abcdef)$	$(abefcd)$	$(adebcf)$
$(ace)(bdf)$	$(aec)(bdf)$	$(ace)(bfd)$
$(ad)(be)(cf)$	$(adcfeb)$	$(afcbed)$
$(aec)(bfd)$	(bfd)	(aec)
$(afedcb)$	$(af)(bc)(de)$	$(ab)(cd)(ef)$,

其第一第二項分別爲 a, c 之三項巡回置換，僅 (ace). 故由第二定理，a, c, e 作非原系，因之此羣爲非原的. 又他之非原系則爲 b, d, f.

注意 1. 例 1 之羣，乃由正方形 $abcd$ 之運動而作之羣也. 又第二例之羣，乃有兩個巡回羣 $\{(ace)\}$, $\{(bdf)\}$ 之直乘積(非遷的)以爲其正常約羣. 卽

$$(ab)(cd)(ef)[\{(ace)\}\{(bdf)\}](ab)(cd)(ef)=\{(ace)\}\{(bdf)\}.$$

而其羣則爲

$$\{(ace)\}\{(bdf)\}+\{(ace)\}\{(bdf)\}(ab)(cd)(ef).$$

又此羣中 $\{(ace)\}$ 所屬之共軛系，則爲

$$\{(ace)\},\quad \{(bdf)\}.$$

注意 2. 本節之兩定理，雖由次節定理，以之爲系，直可得之；然爲使讀者容易了解起見，故不顧重複，作爲定理，揭諸此，且與以證明焉.

87. 羣之有可遷約羣者之可遷置複度.

設 $\mathfrak{G}$ 爲 n 次可遷羣，$\mathfrak{H}$ 爲 q 次可遷約羣. 但 $q<n$.

於$\mathfrak{G}$作$\mathfrak{T}$所屬之共軛約羣系. 以之爲

(1) $\mathfrak{T}', \mathfrak{T}'', \cdots\cdots.$

(此等羣爲同值. 參照第76節注意).

1.° 任取此共軛系中任何二羣皆無有共通之文字(施行置換者)時.

此時若以$\mathfrak{T}'$之施行置換之文字爲

(2) $\alpha, \alpha_1, \cdots\cdots, \alpha_{q-1},$

則此諸文字於$\mathfrak{G}$作一非原系.

蓋若取文字α置換爲(2)之文字α_i之任意置換($\mathfrak{G}$的)

$$S=\begin{pmatrix} \alpha & \alpha_1 \cdots\cdots \alpha_{q-1} \cdots\cdots \\ \alpha_i & x_1 \cdots\cdots x_{q-1} \cdots\cdots \end{pmatrix}$$

而以此將$\mathfrak{T}'$變形, 則$S^{-1}\mathfrak{T}'S$之置換, 乃爲在

$$\alpha_i, x_1, \cdots\cdots, x_{q-1}$$

上所行者也. 卽$S^{-1}\mathfrak{T}'S$與$\mathfrak{T}'$共有文字α_i. 然由假設, 共軛系之二羣無有共通文字. 故

$$S^{-1}\mathfrak{T}'\,S=\mathfrak{T}'$$

爲必要, 因之$x_1, x_2, \cdots\cdots, x_{q-1}$不得不含於(2)也. 卽$\mathfrak{G}$之置換中將$\alpha$置換爲(2)之文字之置換, 乃使(2)之文字於其自身間移動. 故由第83節第一定理系2, (2)之文字於$\mathfrak{G}$作非原系焉.*

*此款之例請觀前節例2及其注意可.

2°. 共軛約羣之有共通文字(施行置換者)者爲存在時.

由共軛系(1)中選其共通文字爲最多數者之二羣,而以之爲$\mathfrak{T}'$, $\mathfrak{T}''$;且以$\mathfrak{T}'$之置換,爲於文字

(3)　$\alpha_1, \alpha_2, \cdots\cdots, \alpha_\mu, \beta_1, \beta_2, \cdots\cdots, \beta_\nu \ (\mu+\nu=q)$

上,而$\mathfrak{T}''$之置換爲於文字

(4)　$\alpha_1, \alpha_2, \cdots\cdots, \alpha_\mu, \gamma_1, \gamma_2, \cdots\cdots, \gamma_\nu$

上所施行者. (但共通文字多於μ個者之二羣,則以爲不存在於(1).) 於是因$\mathfrak{T}'$及$\mathfrak{T}''$共爲可遷的,故由兩者之元素所生成之羣* $\{\mathfrak{T}', \mathfrak{T}''\}$,對於$\mu+2\nu\ (=q+\nu)$個之文字

(5)　$\alpha_1, \alpha_2, \cdots\cdots, \alpha_\mu, \beta_1, \beta_2, \cdots\cdots, \beta_\nu, \gamma_1, \cdots\cdots, \gamma_\nu$

之爲可遷的甚明.

(i)　$\nu=1$時.

$\{\mathfrak{T}', \mathfrak{T}''\}$之次數爲$q+1$. 故若$\mathfrak{T}$,隨之$\mathfrak{T}'$之可遷重複度爲$t(\geqq 1)$,則$\{\mathfrak{T}', \mathfrak{T}''\}$爲$t+1$重可遷(第64節第四定理).

(ii)　$\nu>1$時.

試取$\{\mathfrak{T}', \mathfrak{T}''\}$之置換中$\beta_1$置換爲$\beta_i$者之任意置換T,而以之變$\mathfrak{T}''$之形,則因$\mathfrak{T}''$不使$\beta_1$動,故$T^{-1}\mathfrak{T}''T$亦不使$\beta_i$動. 是則$\beta_1, \beta_2, \cdots\cdots, \beta_\nu$之中以$T^{-1}\mathfrak{T}''T$之置換而移動者,

---

*羣之生成之意義,請參照第42節. 而由二羣$\mathfrak{H}, \mathfrak{H}'$之元素所生成之羣,則以$\{\mathfrak{H}, \mathfrak{H}'\}$表之焉.

至多不出$\nu-1$個. 因之$\alpha_1, \alpha_2, \cdots\cdots, \alpha_\mu, \gamma_1, \gamma_2, \cdots\cdots, \gamma_\nu$之中以$T^{-1}\mathfrak{T}''T$之置換而移動者, 至少非有$\mu+\nu-(\nu-1)$卽$\mu+1$個存在不可也. 然(1)中兩羣之共通文字之最大限度, 由假設爲μ個. 故$T^{-1}\mathfrak{T}''T$不得不與$\mathfrak{T}''$一致. 爲此之故, 則由$T, \beta_1, \beta_2, \cdots\cdots, \beta_\nu$必於其自身間移動. (否則$T^{-1}\mathfrak{T}''T$之施行置換之文字中遂含有$\beta$之一個, 是不合理.) 因之由第83節第一定理系2, 則$\beta_1, \beta_2, \cdots\cdots, \beta_\nu$於$\{\mathfrak{T}', \mathfrak{T}''\}$作一非原系也.

又上記之T, 若特別由$\mathfrak{T}'$中採取之, 則雖於$\mathfrak{T}', \beta_1, \beta_2, \cdots\cdots, \beta_\nu$亦作非原系可知也. (以故若$\mathfrak{T}$, 隨之$\mathfrak{T}'$, 爲本原的, 則$\nu>1$者之款無有.)

3°. $\{\mathfrak{T}', \mathfrak{T}''\}$之次數$q+\nu$與羣$\mathfrak{G}$之次數$n$一致時, 若$\nu=1$, 則由(2°, i), $\{\mathfrak{T}', \mathfrak{T}''\}$爲$t+1$重可遷($t$爲$\mathfrak{T}$之可遷重複度), 因之$\mathfrak{G}$亦至少爲$t+1$重可遷. 反之若$\nu>1$, 則由$\mathfrak{G}$之置換中, 取其將$\beta_1$置換爲$\beta_i$者之U, 而以之變$\mathfrak{T}''$之形, 於是與(2°)中同樣, $U^{-1}\mathfrak{T}''U=\mathfrak{T}''$, 因之$\beta_1, \beta_2, \cdots\cdots, \beta_\nu$於$\mathfrak{G}$作一非原系.

$\{\mathfrak{T}', \mathfrak{T}''\}$之次數小於$n$時, 以此羣爲$\mathfrak{T}_1$, 而作其所屬之共軛系

$$\mathfrak{T}_1', \quad \mathfrak{T}_1'', \quad \cdots\cdots$$

若取此中任何兩羣皆無有共通之文字(施行置換者)時, 則$\mathfrak{T}_1'$之施行置換之文字, 與(1°)中所示者同樣, 於$\mathfrak{G}$作非

原系也. 反之,上之共軛約羣系中,其有共通文字者爲存在時,則取其共通文字爲最多數者之二羣. 以之爲$\mathfrak{T}_1'$, $\mathfrak{T}_1''$,而就$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$一論. 若非共通文字爲一個,則$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$爲$t_1+1$重可遷,但$t_1$爲示$\mathfrak{T}_1$之可遷重複度者. 若非共通文字有二個以上,則$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$及$\mathfrak{T}_1'$爲非原的. 特別若$\mathfrak{T}$爲本原的,則如(2°)所述,$\mathfrak{T}_1$爲$t+1$重可遷的,因之爲本原的. 於是$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$爲$t+2$重可遷也.

$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$之次數尙小於$n$時,則以此羣爲$\mathfrak{T}_2$. 乃以前同樣之手段反覆之. 於是遂得達$\mathfrak{G}$或爲非原的,或至少爲二重可遷的之結論也.

4'. 特別,與羣$\mathfrak{G}$爲本原的時,則(1°)之情況不生也. 又若$\mathfrak{T}$亦爲本原的時,則(2°, ii)之情況亦無由起. 因之由(2°, i), $\{\mathfrak{T}', \mathfrak{T}''\}$卽$\mathfrak{T}_1$爲$q+1$次$t+1$重可遷($t$爲$\mathfrak{T}$之可遷重複度),當然爲本原的也. 同樣,$\{\mathfrak{T}_1', \mathfrak{T}_1''\}$卽$\mathfrak{T}_2$爲$q+2$次$t+2$重可遷,順次推之,遂得$\mathfrak{T}_{n-q}$爲$n$次$t+n-q$重可遷. 故$\mathfrak{G}$之可遷重複度不在$t+n-q$以下.

總合上述,得次

定理. 若n次可遷羣$\mathfrak{G}$含有$q(<n)$次可遷約羣$\mathfrak{T}$時,則$\mathfrak{G}$或爲非原的或至少爲二重可遷的. 特別若$\mathfrak{G}$及$\mathfrak{T}$爲本原的,$\mathfrak{T}$之可遷重複度爲t時,則$\mathfrak{G}$至少爲$n-q+t$重可遷的.

系. 本原羣含有轉換時,則此羣爲對稱的. 又含三

項巡回置換之本原羣，則或爲交代的，或爲對稱的.

證明. 轉換 (ab) 所生成之羣 $\{(ab)\}$ 爲二次本原的. 故 n 次本原羣若含轉換 (ab)，隨之含本原的約羣 $\{(ab)\}$ 時，則其可遷重複度由定理爲 $n-2+1=n-1$. 即對稱的也(第65節). 次之，三項巡回置換 (abc) 所生成之羣 $\{(abc)\}$ 爲三次本原的，故 n 次本原羣如含此時，則其可遷重複度至少爲 $n-3+1=n-2$，因之爲交代羣或爲對稱羣(第65節定理).

注意. 非交代的 n 次可遷羣 $\mathfrak{S}$ 如含有低於 n 次之交代羣以爲其約羣時，若以交代約羣中最高次者爲 $\mathfrak{A}$，則 $\mathfrak{A}$ 之共軛約羣決無有共通之置換文字. (蓋若不然，則由 2°，或 $\mathfrak{A}$ 爲非原的，或較 $\mathfrak{A}$ 高一次之交代約羣爲存在故也.) 因之由 (1°)，$\mathfrak{A}$ 之施行置換之文字於 $\mathfrak{S}$ 作非原系. 是即與前節第二定理之證明中所述者一致也. 又若含較 n 爲低次之對稱羣以爲約羣時，其同樣之事亦得言焉.

88. 前節 (2°, ii) 款之例.

於兩羣

$$\mathfrak{A}: \quad 1, \quad (ab), \quad (cd), \quad (ef),$$
$$(ab)(cd), \quad (ab)(ef), \quad (cd)(ef), \quad (ab)(cd)(ef);$$

$$\mathfrak{B}: \quad 1, \quad (ac)(bd), \quad (ae)(bf), \quad (ce)(df),$$
$$(ace)(bdf), \quad (aec)(bfd),$$
$$(ac)(bd)\cdot(ab)\cdot(ac)(bd)=(cd),$$
$$(ae)(bf)\cdot(ab)\cdot(ae)(bf)=(ef),$$

$$(ce)(df)\cdot(ab)\cdot(ce)(df)=(ab).$$

就其他言,同樣以$\mathfrak{B}$之元素將$\mathfrak{A}$之元素變形,其結果仍爲$\mathfrak{A}$之元素. 卽$\mathfrak{B}$之各元素與$\mathfrak{A}$爲交換可能也. 且兩羣除1外無共通之元素. 故積$\mathfrak{A}\mathfrak{B}$成一48元羣. 此羣以$\mathfrak{G}$表之. 則$\mathfrak{G}$之爲六次可遷的明矣.

試取$\mathfrak{G}$之四次可遷約羣

$$\mathfrak{T}:\quad 1,\ (ab(cd),(ac)(bd),(ad)(bc),$$

則於$\mathfrak{G}$,$\mathfrak{T}$之正常化羣爲

$$\mathfrak{T}+\mathfrak{T}(cd)+\mathfrak{T}(ef)+\mathfrak{T}(cd)(ef).$$

茲以$\mathfrak{U}$表之,而就$\mathfrak{U}$分$\mathfrak{G}$爲傍系,則得

$$\mathfrak{G}=\mathfrak{U}+\mathfrak{U}(ae)(bf)+\mathfrak{U}(ce)(df).$$

故$\mathfrak{T}$所屬之共軛系爲

$$\begin{aligned}
\mathfrak{T}:&\qquad 1,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc);\\
\mathfrak{T}'=(ae)(bf)\mathfrak{T}(ae)(bf):&\qquad 1,\ (ef)(cd),\ (ce)(df),\ (ed)(fc);\\
\mathfrak{T}''=(ce)(df)\mathfrak{T}(ce)(df):&\qquad 1,\ (ab)(ef),\ (ae)(bf),\ (af)(be).
\end{aligned}$$

是中$\mathfrak{T}$及$\mathfrak{T}'$共有二文字c,d;$\mathfrak{T}$及$\mathfrak{T}''$共有a,b;$\mathfrak{T}'$及$\mathfrak{T}''$共有e,f. 是就其任何二者言,其共通文字皆爲二個. 故雖任選其二以爲共通文字之最多數者之二羣,皆無所不可. 若取$\mathfrak{T}$及$\mathfrak{T}'$則因其共通文字爲c,d之故,由前節(2°, ii)之所證明,a,b乃於$\mathfrak{T}$及$\{\mathfrak{T},\mathfrak{T}'\}$作一非原系也. 且在$\mathfrak{T}$中

$$a,b;\ c,d$$

之作非原系,就$\mathfrak{T}$之置換而觀之自明. 又於$\{\mathfrak{T},\mathfrak{T}\}'$中

$$a, b; c, d; e, f$$

之作非原系，則將$\{\mathfrak{T}, \mathfrak{T}'\}$之置換書出之亦可明瞭．爲此之故，試就$\{\mathfrak{T}, \mathfrak{T}'\}$之構成一論之．此羣之含四元約羣

$$\mathfrak{C}: \quad 1, (ab)(cd), (cd)(ef), (ab)(ef)\,[=(ab)(cd)\cdot(cd)(ef)]$$

甚明，而復以含

$$(ce)(df)\cdot(ac)(bd)\cdot(ce)(df)=(ae)(bf)$$

之故，是亦含羣$\mathfrak{B}$也．因之$\{\mathfrak{T}, \mathfrak{T}'\}$含有積$\mathfrak{C}\mathfrak{B}$．然$\mathfrak{C}$與$\mathfrak{B}$之元素爲交換可能，* 而兩羣除1以外無共通之元素．故積$\mathfrak{C}\mathfrak{B}$成爲$\{\mathfrak{T}, \mathfrak{T}'\}$中之24元羣也．而

$$\mathfrak{C}\mathfrak{B}=\mathfrak{C}+\mathfrak{C}(ac)(bd)+\mathfrak{C}(ae)(bf)+\mathfrak{C}(ce)(df)$$
$$+\mathfrak{C}(ace)(bdf)+\mathfrak{C}(aec)(bfd).$$

即$\mathfrak{C}\mathfrak{B}$之置換爲

$1,$	$(ab)(cd),$	$(cd)(ef),$	$(ab)(ef),$
$(ac)(bd),$	$(ad)(bc),$	$(acbd)(ef),$	$(adbc)(ef),$
$(ae)(bf),$	$(afbe)(cd),$	$(aebf)(cd),$	$(af)(be),$
$(ce)(df),$	$(ab)(cfde),$	$(cf)(de),$	$(ab)(cedf),$
$(ace)(bdf),$	$(ade)(bcf),$	$(acf)(bde),$	$(adf)(bce),$
$(aec)(bfd),$	$(afd)(bec),$	$(aed)(bfc),$	$(afc)(bed).$

由此以觀，$\mathfrak{T}$及$\mathfrak{T}'$之置換全部皆含在內，故$\{\mathfrak{T}, \mathfrak{T}'\}$非含於$\mathfrak{C}\mathfrak{B}$不可也．因之

---

*是蓋因$\mathfrak{C}$爲$\mathfrak{A}$之約羣，而如前所述，$\mathfrak{A}$與$\mathfrak{B}$之各元素爲交換可能故也．

$$\{\mathfrak{T}, \mathfrak{T}'\} = \mathfrak{GB}.$$

試檢此24置換，則於 $\{\mathfrak{T}, \mathfrak{T}'\}$

$$a, b;\ c, d;\ e, f$$

之作非原系甚明.

次之，因 $\{\mathfrak{T}, \mathfrak{T}'\}$ 不含 (ab)，且 $\mathfrak{G}$ 之元數爲48，故

$$\mathfrak{G} = \{\mathfrak{T}, \mathfrak{T}'\} + \{\mathfrak{T}, \mathfrak{T}'\}(ab).$$

然 a, b 兩文字於 $\{\mathfrak{T}, \mathfrak{T}'\}$ 作非原系，因之 $\{\mathfrak{T}, \mathfrak{T}'\}$ 中置換 a 爲 b 者之置換，亦置換 b 爲 a. 故就傍系 $\{\mathfrak{T}, \mathfrak{T}'\}(ab)$ 之置換言，其爲同樣亦甚明. 是則二文字 a, b 雖於 $\mathfrak{G}$ 亦作非原系. 是與前節(2°, ii)所證者一致也.

第十五章　與可遷羣之各置換交換可能者之置換

89. 在正置換表示時.

設 $\mathfrak{G}$ 爲 g 元羣，其元素爲

$$(1) \qquad G_0, G_1, \cdots\cdots, G_{g-1} \quad (G_0 = 1),$$

而作 $\mathfrak{G}$ 之正置換表示

$$(2) \quad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}, \quad i = 0, 1, 2, \cdots\cdots, g-1.$$

今試於元素(1)上所行之置換中，求其與置換(2)之各個爲交換可能者.

乃取(1)上所行之置換

$$(3)\qquad \begin{pmatrix} G_0G_1 & \cdots\cdots & G_{g-1} \\ G_0'G_1' & \cdots\cdots & G'_{g-1} \end{pmatrix},$$

而以置換(2)變其形，則得

$$(4)\quad \begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}^{-1}\begin{pmatrix} G_0G_1 & \cdots\cdots & G_{g-1} \\ G_0'G_1' & \cdots\cdots & G'_{g-1} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$$

$$=\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}^{-1}\begin{pmatrix} G_0G_1 & \cdots\cdots & G_{g-1} \\ G_0'G_1' & \cdots\cdots & G'_{g-1} \end{pmatrix}\begin{pmatrix} G_r' \\ G_r'G_i \end{pmatrix}$$

$$=\begin{pmatrix} G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \\ G_0'G_i & G_1'G_i & \cdots\cdots & G'_{g-1}G_i \end{pmatrix},\quad i=0,\ 1,\ 2,\ \cdots\cdots,\ g-1.*$$

就此結果而觀，因 $G_0G_i=G_i$，故 G_i 得爲 $G_0'G_i$ 所置換. 爲此須與(3)一致起見，卽(3)須與(2)之各個爲交換可能者，

$$G_i'=G_0'G_i\quad (i=0,\ 1,\ 2,\ \cdots\cdots,\ g-1)$$

爲必要也. 以之代入(3)，則得

$$(5)\qquad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0'G_0 & G_0'G_1 & \cdots\cdots & G_0'G_{g-1} \end{pmatrix}.\dagger$$

反之，對於㊂卽(1)之任意元素 G_0'，(5)乃表元素(1)間之置換，而與(2)之各置換爲交換可能者. 蓋因

$$G_0'G_0,\ G_0'G_1,\ \cdots\cdots\ G_0'G_{g-1}$$

之任何個皆與㊂之元素等且彼此互異，故(5)之爲表示元素(1)間之置換者甚明. 而於(4)令 $G_r'=G_0'G_r$，則得

---

*置換(2)乃以 G_rG_i 置換 G_r 者，故略記之表以 $\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$ 爲.

†此置換略記爲 $\begin{pmatrix} G_r \\ G_0'G_r \end{pmatrix}$.

$$\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_0'G_r \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}=\begin{pmatrix} G_rG_i \\ G_0'G_rG_i \end{pmatrix}=\begin{pmatrix} G_s \\ G_0'G_s \end{pmatrix},$$

卽(5)與(2)之各置換爲交換可能也.

於置換(5), 取 $G_0, G_1, \cdots\cdots, G_{g-1}$ 以爲 G_0', 則得與正置換表示(2)之各置換爲交換可能之 g 個置換

$$(6)\quad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_jG_0 & G_jG_1 & \cdots\cdots & G_jG_{g-1} \end{pmatrix},\quad j=0,1,2,\cdots\cdots,g-1.$$

是卽所求者也. 至此各個之相互各異, 明甚.

復次, 此諸置換乃成羣也. 蓋因

$$(7)\quad \begin{pmatrix} G_r \\ G_iG_r \end{pmatrix}\begin{pmatrix} G_r \\ G_jG_r \end{pmatrix}=\begin{pmatrix} G_r \\ G_iG_r \end{pmatrix}\begin{pmatrix} G_jG_r \\ G_j\cdot G_iG_r \end{pmatrix}=\begin{pmatrix} G_r \\ G_jG_i\cdot G_r \end{pmatrix}$$

故. 更於此羣中以置換 $\begin{pmatrix} G_r \\ G_jG_r \end{pmatrix}$ 與 $\mathfrak{G}$ 之元素 G_j^{-1} 對應, 則對 $\mathfrak{G}$ 之二元素 G_i^{-1} 及 G_j^{-1} 之積 $(G_jG_i)^{-1}$, 乃有 $\begin{pmatrix} G_r \\ G_jG_iG_r \end{pmatrix}$ 與之對應, 而此由(7)又與對應於 G_i^{-1} 及 G_j^{-1} 之置換之積等. 因之羣(6)與 $\mathfrak{G}$ 隨之與正置換表示(2)爲單純同態也. 又由(6)之置換, G_0 得分別爲 $G_0, G_1, \cdots\cdots, G_{g-1}$ 所置換. 故(6)爲可遷的. 且若 $j\neq 0$, 則 $G_jG_r\neq G_r$, 故不動置換 $\begin{pmatrix} G_r \\ G_0G_r \end{pmatrix}$ 以外之置換, 皆足使全部元素移動. 故(6)爲正置換羣焉.

總合上述, 得次

定理. 在 g 元羣 $\mathfrak{G}$ 之元素 $G_0, G_1, \cdots\cdots, G_{g-1}$ 上所行置換之中, 與 $\mathfrak{G}$ 之正置換表示

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}, \quad i=0, 1, 2, \cdots\cdots, g-1$$

爲交換可能者，乃次之 g 個：

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_jG_0 & G_jG_1 & \cdots\cdots & G_jG_{g-1} \end{pmatrix}, \quad j=0, 1, 2, \cdots\cdots, g-1.$$

而此諸個，又作與 $\mathfrak{G}$ 爲單純同態之正置換羣.

由第 74 節中所述，則凡正置換羣皆得視爲一個羣之表示. 故由本定理直得次

系. 與 n 次正置換羣之各置換爲交換可能之置換(同 n 文字上所行者)，又作一 n 次正置換羣. 而兩羣爲同態. (Jordan 氏之定理.)

本系中正置換羣之各個稱曰其他個之**接合羣**. 又兩羣中共通之元素於各羣皆爲自己共軛. 特別在 Abel 氏正置換羣中，則此與其接合羣一致.

例. 試取六次正置換羣

$$1, \quad \begin{pmatrix} 012345 \\ 120534 \end{pmatrix}, \quad \begin{pmatrix} 012345 \\ 201453 \end{pmatrix},$$

$$\begin{pmatrix} 012345 \\ 345012 \end{pmatrix}, \quad \begin{pmatrix} 012345 \\ 453201 \end{pmatrix}, \quad \begin{pmatrix} 012345 \\ 534120 \end{pmatrix}.$$

對於文字 0, 1, 2, 3, 4, 5, 分別使元素

(1) $\qquad G_0, G_1, G_2, G_3, G_4, G_5$

與之對應，且利用上之置換，而依第 74 節所述之方法，則此等元素間之結合得定義如次：

G_0	G_1	G_2	G_3	G_4	G_5	
G_0	G_1	G_2	G_3	G_4	G_5	G_0
G_1	G_2	G_0	G_5	G_3	G_4	G_1
G_2	G_0	G_1	G_4	G_5	G_3	G_2
G_3	G_4	G_5	G_0	G_1	G_2	G_3
G_4	G_5	G_3	G_2	G_0	G_1	G_4
G_5	G_3	G_4	G_1	G_2	G_0	G_5

此表中如與右欄之G_1同列者，乃示右乘G_1於上段之元素所得之積者也．他準此．既若是以定結合之義，則如第74節所述，此等六元素成羣，而其正置換表示

$$(2)\quad \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_0G_i & G_1G_i & G_2G_i & G_3G_i & G_4G_i & G_5G_i \end{pmatrix},\ i=0,1,2,3,4,5$$

則與此羣同值．與此羣之置換爲交換可能之置換，由定理爲

$$(3)\quad \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_jG_0 & G_jG_1 & G_jG_2 & G_jG_3 & G_jG_4 & G_jG_5 \end{pmatrix},\quad j=0,1,2,3,4,5.$$

此各個用上之乘法表而計算之，則爲

$$\begin{pmatrix} G_r \\ G_0G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \end{pmatrix}=1,$$

$$\begin{pmatrix} G_r \\ G_1G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_1 & G_2 & G_0 & G_4 & G_5 & G_3 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_2G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_2 & G_0 & G_1 & G_5 & G_3 & G_4 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_3G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_3 & G_5 & G_4 & G_0 & G_2 & G_1 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_4 G_r \end{pmatrix} = \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_4 & G_3 & G_5 & G_1 & G_0 & G_2 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_5 G_r \end{pmatrix} = \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_5 & G_4 & G_3 & G_2 & G_1 & G_0 \end{pmatrix}.$$

於是因與羣與羣(2)爲同值，故於此諸置換中，以文字0, 1, 2, 3, 4, 5代元素(1)，則得與羣之接合如次：

$$1, \quad \begin{pmatrix} 0\,1\,2\,3\,4\,5 \\ 1\,2\,0\,4\,5\,3 \end{pmatrix}, \begin{pmatrix} 0\,1\,2\,3\,4\,5 \\ 2\,0\,1\,5\,3\,4 \end{pmatrix},$$

$$\begin{pmatrix} 0\,1\,2\,3\,4\,5 \\ 3\,5\,4\,0\,2\,1 \end{pmatrix}, \begin{pmatrix} 0\,1\,2\,3\,4\,5 \\ 4\,3\,5\,1\,0\,2 \end{pmatrix}, \begin{pmatrix} 0\,1\,2\,3\,4\,5 \\ 5\,4\,3\,2\,1\,0 \end{pmatrix}.$$

90. 在傍系置換表示時.

令$\mathfrak{G}$爲g元羣，其元素爲

(1) $$G_0, G_1, G_2, \cdots\cdots, G_{g-1} \quad (G_0 = 1).$$

次之取約羣$\mathfrak{H}$，而就之分$\mathfrak{G}$爲傍系，以之爲

(2) $$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}S_1 + \cdots\cdots + \mathfrak{H}S_{n-1},$$

而關於$\mathfrak{H}$之傍系置換表示

(3) $$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix}, \quad i = 0, 1, 2, \cdots\cdots, g-1,$$

則以$(\mathfrak{G})$表之. 本節之目的，乃在求n傍系

(4) $$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{n-1}$$

上所行之置換中之與$(\mathfrak{G})$各置換爲交換可能者也.

茲取傍系(4)上所行之置換

(5) $$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ (\mathfrak{H})' & (\mathfrak{H}S_1)' & \cdots\cdots & (\mathfrak{H}S_{n-1})' \end{pmatrix},$$

但 $(\mathfrak{H}S_r)'$ 爲傍系(4)中得以置換 $\mathfrak{H}S_r$ 者. 此置換,以(𝔊)之置換 $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}$ 變其形,則得

$$(6)\quad \begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}^{-1}\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ (\mathfrak{H})' & (\mathfrak{H}S_1)' & \cdots\cdots & (\mathfrak{H}S_{n-1})'\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i\\ (\mathfrak{H})'G_i & (\mathfrak{H}S_1)'G_i & \cdots\cdots & (\mathfrak{H}S_{n-1})'G_i\end{pmatrix}.$$

然

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ (\mathfrak{H})' & (\mathfrak{H}S_1)' & \cdots\cdots & (\mathfrak{H}S_{n-1})'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i\\ (\mathfrak{H}G_i)' & (\mathfrak{H}S_1G_i)' & \cdots\cdots & (\mathfrak{H}S_{n-1}G_i)'\end{pmatrix}.$$

故置換(5)如欲與(𝔊)之各置換爲交換可能,則由(6)式,

$$\begin{pmatrix}\mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i\\ (\mathfrak{H}G_i)' & (\mathfrak{H}S_1G_i)' & \cdots\cdots & (\mathfrak{H}S_{n-1}G_i)'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i\\ (\mathfrak{H})'G_i & (\mathfrak{H}S_1)'G_i & \cdots\cdots & (\mathfrak{H}S_{n-1})'G_i\end{pmatrix}$$

$$i=0,\ 1,\ 2,\cdots\cdots,\ g-1,$$

因之

$$(7)\quad (\mathfrak{H}S_rG_i)'=(\mathfrak{H}S_r)'G_i\begin{cases}r=0,\ 1,\ 2,\cdots\cdots,\ n-1\ (S_0=1)\\ i=0,\ 1,\ 2,\cdots\cdots,\ g-1\end{cases}$$

爲必要也.

(7) 式中若取 $\mathfrak{H}$ 之任意元素 H 以爲 G_i,再令 $r=0$,則得

$$(\mathfrak{H})'=(\mathfrak{H})'H.$$

然 $(\mathfrak{H})'$ 乃關於 $\mathfrak{H}$ 之傍系之一. 卽

$$(8)\qquad (\mathfrak{H})'=\mathfrak{H}K,$$

但 K 爲 𝔊 之一元素. 故由前式,對於 $\mathfrak{H}$ 之任意元素 H,

$$\mathfrak{H}K=\mathfrak{H}KH$$

爲能成立. 由此得

$$H'K=KH \quad (H' \text{ 爲 } \mathfrak{H} \text{ 之一元素}).$$

$$\therefore \quad KHK^{-1}=H'.$$

此乃示對於$\mathfrak{H}$之任意元素H, KHK^{-1}屬於$\mathfrak{H}$者也. 故

$$K\mathfrak{H}K^{-1}=\mathfrak{H},$$

卽謂置換(5)與(𝔊)之各置換爲交換可能時,若由此置換,$\mathfrak{H}$得置換爲傍系$\mathfrak{H}K$,則K與$\mathfrak{H}$之爲變換可能爲必要也.

次之,於(7)取S_r^{-1}以爲G_i,則

$$(\mathfrak{H})'=(\mathfrak{H}S_r)'S_r^{-1}.$$

$$\therefore \quad (\mathfrak{H}S_r)'=(\mathfrak{H})'S_r.$$

故由(8)得

$$(\mathfrak{H}S_r)'=\mathfrak{H}K\cdot S_r.$$

因之置換(5)若欲與(𝔊)之各置換爲交換可能,則可取次形:

$$(9) \qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}K & \mathfrak{H}KS_1 & \cdots\cdots & \mathfrak{H}KS_{n-1} \end{pmatrix},$$

或

$$(9') \qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ K\mathfrak{H} & K\mathfrak{H}S_1 & \cdots\cdots & K\mathfrak{H}S_{n-1} \end{pmatrix},$$

但

$$K^{-1}\mathfrak{H}K=\mathfrak{H},$$

卽K爲$\mathfrak{H}$之正常化羣之元素.

反之,𝔊之元素K與$\mathfrak{H}$爲交換可能時,則(9)乃表示n傍系(4)上所行之置換者也. 蓋因

$$\mathfrak{H}K,\ \mathfrak{H}KS_1,\ \cdots\cdots\ \mathfrak{H}KS_{n-1}$$

之任何個皆爲屬於$\mathfrak{H}$之傍系,且$\mathfrak{H}K=K\mathfrak{H}$,故此諸個分別與

$$K\mathfrak{H},\ K\mathfrak{H}S_1,\ \cdots\cdots,\ K\mathfrak{H}S_{n-1}$$

等，而此各個又相互各異故．（若 $K\mathfrak{H}S_r=K\mathfrak{H}S_t$；則 $\mathfrak{H}S_r=\mathfrak{H}S_t$ 故．）

斯時也，置換(9)乃與(𝔊)之各置換爲交換可能焉．蓋因

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}KS_r\\ \mathfrak{H}KS_rG_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_rG_i\end{pmatrix},$$

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ K\mathfrak{H}S_r\end{pmatrix}\quad[\because\ \mathfrak{H}K=K\mathfrak{H}]$$

$$=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_rG_i\\ K\mathfrak{H}S_rG_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ K\mathfrak{H}S_rG_i\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_rG_i\end{pmatrix}\qquad[\because\ K\mathfrak{H}=\mathfrak{H}K].$$

$$\therefore\quad\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}S_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}.$$

試再求(9)所表示之置換中之互異者．茲以𝔊之正常化羣爲$\mathfrak{N}$，而就𝔊分之爲傍系，以之爲

$$(10)\qquad \mathfrak{N}=\mathfrak{H}T_0+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{m-1}\quad(T_0=1),$$

則因$\mathfrak{N}$之元素K等於HT_j（H爲𝔊之元素）之故，遂得

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}HT_jS_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}T_jS_r\end{pmatrix}.$$

故(9)所表示之置換中之互異者不多於次之m個：

$$(11)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}T_j & \mathfrak{H}T_jS_1 & \cdots\cdots & \mathfrak{H}T_jS_{n-1}\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ m-1.$$

且此各個皆互異．蓋若

$$\begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}T_iS_r \end{pmatrix} = \begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}T_jS_r \end{pmatrix},$$

則

$$\mathfrak{H}T_iS_r = \mathfrak{H}T_jS_r,$$

因之

$$\mathfrak{H}T_i = \mathfrak{H}T_j$$

故也. 總合上述, 得次

定理. 與一羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之傍系置換表示

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix}, \quad i=0, 1, 2, \cdots\cdots, g-1$$

之各置換爲交換可能之置換(同傍系上所行者), 得以

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}K & \mathfrak{H}KS_1 & \cdots\cdots & \mathfrak{H}KS_{n-1} \end{pmatrix}$$

與之, 但K爲$\mathfrak{H}$之正常化羣$\mathfrak{N}$之元素. 若

$$\mathfrak{N} = \mathfrak{H} + \mathfrak{H}T_1 + \cdots\cdots + \mathfrak{H}T_{m-1},$$

則此諸置換中之互異者, 爲

$$\begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}S_r \end{pmatrix}, \begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}T_1S_r \end{pmatrix}, \cdots\cdots, \begin{pmatrix} \mathfrak{H}S_r \\ \mathfrak{H}T_{m-1}S_r \end{pmatrix}.$$

即此數與$\mathfrak{H}$對$\mathfrak{N}$之指數等.

系. $\mathfrak{H}$之正常化羣爲$\mathfrak{H}$自身時, 則與傍系置換表示$(\mathfrak{G})$之各置換爲交換可能者之置換, 僅爲不動置換.

注意. 上所求得置換之數m乃與$\mathfrak{H}$對$\mathfrak{N}$之指數等; 而又爲$(\mathfrak{G})$之次數即$\mathfrak{H}$對$\mathfrak{G}$之指數n之約數, 幸留意焉.

91. 前節中所求得之置換, 即其與傍系置換表示$(\mathfrak{G})$

之各置換爲交換可能者之置換，乃相集而成羣也．蓋若以 K_1, K_2 爲 $\mathfrak{H}$ 之正常化羣 $\mathfrak{N}$ 之二元素，則有

$$(12)\quad \begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_1S_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_2S_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_1S_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ K_2\mathfrak{H}S_r\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_1S_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}K_1S_r\\ K_2\mathfrak{H}K_1S_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ K_2\mathfrak{H}K_1S_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_2K_1S_r\end{pmatrix},$$

而積 K_2K_1 屬於 $\mathfrak{N}$ 故．

名此羣曰 $(\mathfrak{P})$，而就其與 $\mathfrak{N}$ 之關係一論．

對 $\mathfrak{N}$ 之元素 K^{-1}，使 $(\mathfrak{P})$ 之置換 $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}KS_r\end{pmatrix}$ 與之對應，則對 $\mathfrak{N}$ 之二元素 K_1^{-1}, K_2^{-1} 以及積 $K_1^{-1}K_2^{-1}$ $[=(K_2K_1)^{-1}]$，分別便有 $(\mathfrak{P})$ 之置換 $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_1S_r\end{pmatrix}$, $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_2S_r\end{pmatrix}$ 以及 $\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}(K_2K_1)S_r\end{pmatrix}$ 相與對應也．然由 (12),

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_1S_r\end{pmatrix}\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}K_2S_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}(K_2K_1)S_r\end{pmatrix}.$$

故 $(\mathfrak{P})$ 與 $\mathfrak{N}$ 爲同態．

欲察此同態關係之單複，乃以 $\mathfrak{N}$ 就 $\mathfrak{H}$ 分爲傍系，而與前節同樣，以之爲

$$(10)\quad \mathfrak{N}=\mathfrak{H}T_0+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{m-1}\quad (T_0=1),$$

而以 $\mathfrak{H}$ 之元素爲

$$H_0,\quad H_1, \cdots\cdots, H_{h-1}\quad (H_0=1),$$

則

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}H_sT_jS_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}T_jS_r\end{pmatrix}.$$

故對$\mathfrak{N}$中h個之元素

$$(H_0T_j)^{-1},\quad (H_1T_j)^{-1},\ \cdots\cdots,\ (H_{h-1}T_j)^{-1},$$

同一置換$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}T_jS_r\end{pmatrix}$相與對應也. 然$m$個之置換.

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}T_jS_r\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ m-1$$

互異(前節定理). 因之$\mathfrak{N}$與$(\mathfrak{P})$爲h重同態,而對$(\mathfrak{P})$之不動置換,$\mathfrak{N}$之約羣$\mathfrak{H}$相與對應. 於是$(\mathfrak{P})$與$\mathfrak{N}/\mathfrak{H}$爲單純同態也. 爰得次

定理. 與一羣$\mathfrak{G}$關於約羣$\mathfrak{H}$者之傍系置換表示之各置換成交換可能之置換(關於$\mathfrak{H}$之傍系上所行者),形成一與$\mathfrak{N}/\mathfrak{H}$爲單純同態之羣. 但$\mathfrak{N}$乃示$\mathfrak{H}$之正常化羣者.

92. 羣$(\mathfrak{P})$之可遷性及非遷性.

令$\mathfrak{G}$,$(\mathfrak{G})$,$\mathfrak{H}$,$\mathfrak{N}$,$(\mathfrak{P})$爲有與前二節中者同一意義之各羣.

1°. $\mathfrak{H}$於$\mathfrak{G}$爲正常者時.

此時$\mathfrak{H}$之正常化羣$\mathfrak{N}$與$\mathfrak{G}$一致. 故羣$(\mathfrak{P})$,由第90節定理,爲

$$(13)\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}G_j & \mathfrak{H}G_jS_1 & \cdots\cdots & \mathfrak{H}G_jS_{n-1}\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ g-1,$$

或

$$(13')\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1}\\ G_j\mathfrak{H} & G_j\mathfrak{H}S_1 & \cdots\cdots & G_j\mathfrak{H}S_{n-1}\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ g-1$$

於(13)取S_0, S_1, ……, S_{n-1}以爲G_j,則$\mathfrak{H}$得分別爲$\mathfrak{H}$, $\mathfrak{H}S_1$, ……,

$\mathfrak{H}S_{n-1}$ 所置換. 故羣 $(\mathfrak{P})$ 爲可遷的.

又因 $\mathfrak{R}=\mathfrak{G}$, 由前節定理, 知此羣與 $\mathfrak{G}/\mathfrak{H}$ 爲單純同態自他方言, $\mathfrak{H}$ 爲正常時, 則關於 $\mathfrak{H}$ 之傍系置換表示 $(\mathfrak{G})$, 亦與 $\mathfrak{G}/\mathfrak{H}$ 爲單純同態也(參照第 75 節). 因之得次

定理. 若 $\mathfrak{H}$ 爲羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之正常約羣, 而

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1}$$

時, 則與傍系置換表示 $(\mathfrak{G})$ 之各置換

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i\end{pmatrix},\quad i=0, 1, 2, \cdots\cdots, g-1$$

爲交換可能者之置換, 得以

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}G_j & \mathfrak{H}G_jS_1 & \cdots\cdots & \mathfrak{H}G_jS_{n-1}\end{pmatrix},\quad j=0, 1, 2, \cdots\cdots; g-1$$

與之. 而此諸個, 又形成一與 $(\mathfrak{G})$ 爲單純同態之可遷羣.

在本定理中, 若取 $\mathfrak{H}$ 爲主元素羣, 則得第 89 節之定理. 又本定理中之兩羣, 其初一個, 如第 75 節之所述, 乃正置換羣. 因之後一個乃前者之接合羣也.

2°. $\mathfrak{H}$ 於 $\mathfrak{G}$ 非正常, 且其正常化羣 $\mathfrak{R}$ 與 $\mathfrak{H}$ 不一致時.

將 $\mathfrak{R}$ 就 $\mathfrak{H}$ 分爲傍系, 乃與前同樣以之爲

$$(10)\qquad \mathfrak{R}=\mathfrak{H}+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{m-1};$$

次以 $\mathfrak{G}$ 就 $\mathfrak{R}$ 分爲傍系, 以之爲

$$(14)\qquad \mathfrak{G}=\mathfrak{R}+\mathfrak{R}U_1+\cdots\cdots+\mathfrak{R}U_{l-1}.$$

於是

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{m-1}$$

$$+\mathfrak{H}U_1+\mathfrak{H}T_1U_1+\cdots\cdots+\mathfrak{H}T_{m-1}U_1$$
$$+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$+\mathfrak{H}U_{l-1}+\mathfrak{H}T_1U_{l-1}+\cdots\cdots+\mathfrak{H}T_{m-1}U_{l-1}$$

而對$\mathfrak{R}$之任意元素K, 則有

$$(15)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}K & \mathfrak{H}KS_1 & \cdots\cdots & \mathfrak{H}KS_{n-1}\end{pmatrix}$$
$$=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1} & \mathfrak{H}U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1 & \mathfrak{H}U_2 & \cdots\cdots\\ \mathfrak{H}K & \mathfrak{H}KT_1 & \cdots\cdots & \mathfrak{H}KT_{m-1} & \mathfrak{H}KU_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}U_1 & \mathfrak{H}KU_2 & \cdots\cdots\end{pmatrix}.$$

自他方言, 因$\mathfrak{H}$爲$\mathfrak{R}$之正常約羣, 故由前定理, 則

$$(16)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K & \mathfrak{H}KT_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}\end{pmatrix},$$

乃表示與$\mathfrak{R}$關於$\mathfrak{H}$者之傍系置換表示之置換

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K' & \mathfrak{H}T_1K' & \cdots\cdots & \mathfrak{H}T_{m-1}K'\end{pmatrix}\quad [K'\text{爲}\mathfrak{R}\text{之任意元素}].$$

爲交換可能之置換者也. (此則於前定理以$\mathfrak{R}$代$\mathfrak{G}$卽得.)

且若$\mathfrak{H}KT_r=\mathfrak{H}T_s$, 則$\mathfrak{H}KT_rU_i=\mathfrak{H}T_sU_i$, 故置換

$$\begin{pmatrix}\mathfrak{H}U_i & \mathfrak{H}T_1U_i & \cdots\cdots & \mathfrak{H}T_{m-1}U_i\\ \mathfrak{H}KU_i & \mathfrak{H}KT_1U_i & \cdots\cdots & \mathfrak{H}KT_{m-1}U_i\end{pmatrix},\quad i=1, 2, \cdots\cdots, l-1$$

可於置換(16), 以$\mathfrak{H}U_i$, $\mathfrak{H}T_1U_i$, ……, $\mathfrak{H}T_{m-1}U_i$代其$\mathfrak{H}$, $\mathfrak{H}T_1$, ……, $\mathfrak{H}T_{m-1}$, 而由同置換而得. 因之(15)式得換書如次:

$$(17)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}K & \mathfrak{H}KS_1 & \cdots\cdots & \mathfrak{H}KS_{n-1}\end{pmatrix}$$
$$=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K & \mathfrak{H}KT_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}\end{pmatrix}\begin{pmatrix}\mathfrak{H}U_1 & \mathfrak{H}T_1U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1\\ \mathfrak{H}KU_1 & \mathfrak{H}KT_1U_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}U_1\end{pmatrix}\cdots$$
$$\cdots\begin{pmatrix}\mathfrak{H}U_{l-1} & \mathfrak{H}T_1U_{l-1} & \cdots\cdots & \mathfrak{H}T_{m-1}U_{l-1}\\ \mathfrak{H}KU_{l-1} & \mathfrak{H}KT_1U_{l-1} & \cdots\cdots & \mathfrak{H}KT_{m-1}U_{l-1}\end{pmatrix}.$$

以故若$\mathfrak{R}$之元素表以

$$K_0,\ K_1,\ \cdots\cdots,\ K_{k-1}\quad (K_0=1),$$

則羣$(\mathfrak{P})$之置換,得以

$$(18)\quad \begin{pmatrix}\mathfrak{H}T_s\\ \mathfrak{H}K_jT_s\end{pmatrix}\begin{pmatrix}\mathfrak{H}T_sU_1\\ \mathfrak{H}K_jT_sU_1\end{pmatrix}\cdots\cdots\begin{pmatrix}\mathfrak{H}T_sU_{l-1}\\ \mathfrak{H}K_jT_sU_{l-1}\end{pmatrix},\ j=0,1,2,\cdots\cdots,k-1$$

與之也. 此中爲其第一因子者之k個置換

$$(19)\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K_j & \mathfrak{H}K_jT_1 & \cdots\cdots & \mathfrak{H}K_jT_{m-1}\end{pmatrix},\ j=0,1,2,\cdots\cdots,k-1,$$

因$\mathfrak{H}$爲$\mathfrak{R}$之正常約羣,故由前定理,乃作$\mathfrak{R}$關於$\mathfrak{H}$者之傍系置換表示

$$(20)\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K_i & \mathfrak{H}T_1K_i & \cdots\cdots & \mathfrak{H}T_{m-1}K_i\end{pmatrix},\quad i=0,1,2,\cdots\cdots,k-1$$

之接合羣. 而爲其第二因子者之k個置換

$$\begin{pmatrix}\mathfrak{H}U_1 & \mathfrak{H}T_1U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1\\ \mathfrak{H}K_jU_1 & \mathfrak{H}K_jT_1U_1 & \cdots\cdots & \mathfrak{H}K_jT_{m-1}U_1\end{pmatrix},\ j=0,1,2,\cdots\cdots,k-1,$$

則由上述乃作與(19)同值之羣. 他因子準此. 於是於羣$(\mathfrak{P})$,其傍系得分爲l個之可遷系:

$$(21)\quad \left\{\begin{array}{cccc}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}U_1 & \mathfrak{H}T_1U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \mathfrak{H}U_{l-1} & \mathfrak{H}T_1U_{l-1} & \cdots\cdots & \mathfrak{H}T_{m-1}U_{l-1},\end{array}\right.$$

因之$(\mathfrak{P})$爲非遷的. 而其可遷構成羣,則爲(19)及與之同值者也. 爰得次

定理. 若約羣$\mathfrak{H}$於羣$\mathfrak{G}$非正常,且其正常化羣與$\mathfrak{H}$不一致時,則與$\mathfrak{G}$關於$\mathfrak{H}$者之傍系置換表示之各置換爲交換可能之置換所作之羣爲非遷的. 而各可遷構成羣,則與$\mathfrak{R}$關於$\mathfrak{H}$之傍系置換表示之接合羣同值.

注意. 如上所述,$(\mathfrak{P})$之可遷構成羣(19)乃正置換羣,而$(\mathfrak{P})$之置換,任何個皆n次正置換. 又取可遷系(21)之一,則得

$$\mathfrak{H}U_s+\mathfrak{H}T_1U_s+\cdots\cdots+\mathfrak{H}T_{m-1}U_s=\mathfrak{R}U_s.$$

故各可遷系乃作$\mathfrak{G}$關於$\mathfrak{R}$之傍系. 因之(21)於$(\mathfrak{G})$爲非原系也.

93. 在一般可遷羣時.

前三節所得之結果,由第83節所示之方針,匪特可直應用之於一般可遷羣,卽由與之同時所與之可遷羣以求與其各置換爲交換可能者之置換之方法,亦以是而自明也.

令$\mathfrak{G}$爲n文字$\alpha,\alpha_1,\cdots\cdots,\alpha_{n-1}$之可遷羣,其$\alpha$不動之約羣爲$\mathfrak{H}$,而以

$$(1)\qquad \mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1},$$

但式中S_i乃示將α置換爲α_i之置換之一者. 又與前同樣,其關於$\mathfrak{H}$之傍系置換表示,以$(\mathfrak{G})$表之;其由與$(\mathfrak{G})$之各置換爲交換可能之置換而成之羣,則以$(\mathfrak{P})$表之焉.

$\mathfrak{H}$之正常化羣,得以彼文字之雖由$\mathfrak{H}$之全部置換而均

不動者之數而定. 即$\mathfrak{H}$不使m個定文字(以之爲$a, a_1, \cdots\cdots, a_{m-1}$)移動時,則$\mathfrak{H}$之正常化羣爲

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1} \tag{2}$$

(參照第63節第三定理(iii).)

$m=1$時. 此時$\mathfrak{N}=\mathfrak{H}$,由第90節定理系,$(\mathfrak{N})=1$.

$m>1$時. 由第90節定理,$(\mathfrak{P})$中互異之置換爲次之m個:

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}S_j & \mathfrak{H}S_jS_1 & \cdots\cdots & \mathfrak{H}S_jS_{n-1} \end{pmatrix}, \quad j=0, 1, 2, \cdots\cdots, m-1;\ S_0=1. \tag{3}$$

而如前節之所注意,此諸個之任何個,皆n次正置換也.

又自他面言,$\mathfrak{G}$與$(\mathfrak{G})$爲同值. 故由上述,直可得次之定理以爲Jordan氏定理之擴張.

定理. 與n次可遷羣$\mathfrak{G}$之各置換爲交換可能之置換(與在$\mathfrak{G}$中者爲同一之文字上所行之置換),皆爲n次正置換. 而其數,乃與雖以一約羣$(\mathfrak{G}$的$)$之爲一個定文字不動者中所有之置換而均不移動之文字之數等. 而此數則爲次數n之約數.

系1. 與原羣之各置換爲交換可能之置換(與該羣爲同一文字上所行者)僅爲不動置換. 因之,原羣除主元素外,無自己共軛元素.

證明. 由本定理及第83節定理系1即得.

系2. Abel氏可遷羣爲正置換羣.

證明. 若以 n 次 Abel 氏可遷羣 $\mathfrak{G}$ 之元數爲 g, 則與 $\mathfrak{G}$ 之各置換爲交換可能之置換之數 m, 至少爲 g 個. 故由定理,

$$g \leqq m \leqq n.$$

但自他方言, 因 $\mathfrak{G}$ 爲可遷的, 故

$$g \geqq n.$$

因之

$$g = n.$$

卽 $\mathfrak{G}$ 爲正置換羣也.

系 3. 可解的原羣之次數, 與素數之冪等. 而此羣只有唯一個極小正常約羣; 而極小正常約羣之元數, 則等於羣之次數.

證明. 設 $\mathfrak{G}$ 爲 n 次可解的原羣. 因 $\mathfrak{G}$ 爲可解的, 故其極小正常約羣 $\mathfrak{N}$, 乃元數等於素數冪 P^m 之 Abel 氏羣(第 52 節系). 又因 $\mathfrak{G}$ 爲本原的, 故其正常約羣 $\mathfrak{N}$ 須爲 n 次可遷的(第 84 節定理系). 然 Abel 氏可遷羣爲正置換羣. 故 $\mathfrak{N}$ 爲正置換羣, 因之其元數 P^m 不得不與 $\mathfrak{G}$ 之次數 n 一致也.

次之若以 $\mathfrak{G}$ 爲有異於 $\mathfrak{N}$ 之極小正常約羣 $\mathfrak{N}'$, 則 $\mathfrak{N}'$ 與 $\mathfrak{N}$ 之最大公約羣須爲主元素羣. 故由第 32 節第一定理, $\mathfrak{N}'$ 之各元素非與 $\mathfrak{N}$ 之各元素爲交換可能不可. 但 $\mathfrak{N}$ 爲 Abel 氏正置換羣, 故此爲不可能(參照第 89 節之系). 因之 $\mathfrak{G}$ 只有唯一個極小正常約羣也.

94. 由前四節之所論, 則求與已知可遷羣之各置換爲交換可能者之置換亦爲容易.

於前節之可遷羣$\mathfrak{G}$, 其約羣$\mathfrak{H}$之正常化羣爲

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}\ (m>1)$$

時, 乃以$\mathfrak{G}$分爲傍系, 而以之爲

$$\begin{aligned}\mathfrak{G}&=\mathfrak{N}+\mathfrak{N}U_1+\cdots\cdots+\mathfrak{N}U_{l-1}\\&=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}\\&+\mathfrak{H}U_1+\mathfrak{H}S_1U_1+\cdots\cdots+\mathfrak{H}S_{m-1}U_1\\&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&=\mathfrak{H}U_{l-1}+\mathfrak{H}S_1U_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}U_{l-1},\end{aligned}$$

則如第92節所述,

$$(4)\qquad \begin{cases}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1}\\ \mathfrak{H}U_1 & \mathfrak{H}S_1U_1 & \cdots\cdots & \mathfrak{H}S_{m-1}U_1\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \mathfrak{H}U_{l-1} & \mathfrak{H}S_1U_{l-1} & \cdots\cdots & \mathfrak{H}S_{m-1}U_{l-1},\end{cases}$$

於羣$(\mathfrak{P})$作可遷系[因之於$(\mathfrak{G})$作非原系]. 而前節之置換(3), 依第92節(17), 分解爲l個之因子如次:

$$(5)\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}S_j & \mathfrak{H}S_jS_1 & \cdots\cdots & \mathfrak{H}S_jS_{n-1}\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1}\\ \mathfrak{H}S_j & \mathfrak{H}S_jS_1 & \cdots\cdots & \mathfrak{H}S_jS_{m-1}\end{pmatrix}\begin{pmatrix}\mathfrak{H}U_1 & \mathfrak{H}S_1U_1 & \cdots\cdots & \mathfrak{H}S_{m-1}U_1\\ \mathfrak{H}S_jU_1 & \mathfrak{H}S_jS_1U_1 & \cdots\cdots & \mathfrak{H}S_jS_{m-1}U_1\end{pmatrix}$$

$$\cdots\cdots\begin{pmatrix}\mathfrak{H}U_{l-1} & \mathfrak{H}S_1U_{l-1} & \cdots\cdots & \mathfrak{H}S_{m-1}U_{l-1}\\ \mathfrak{H}S_jU_{l-1} & \mathfrak{H}S_jS_1U_{l-1} & \cdots\cdots & \mathfrak{H}S_jS_{m-1}U_{l-1}\end{pmatrix}$$

$$j=0,\ 1,\ 2,\ \cdots\cdots,\ m-1\ (S_0=1).$$

式中右邊第二因子以下, 乃於第一因子之$\mathfrak{H}$, $\mathfrak{H}S_1$, ……,

$\mathfrak{H}S_{m-1}$, 將(4)中他之可遷系順次代入之卽得. 故當求所要之置換時,若利用此點,則可省煩勞而有利也.

下例中,以所與之置換羣爲$\mathfrak{G}$,其一個定文字不動之約羣爲$\mathfrak{H}$,$\mathfrak{G}$之關於$\mathfrak{H}$之傍系置換表示爲$(\mathfrak{G})$,其與$(\mathfrak{G})$之各置換爲交換可能者之置換所作之羣爲$(\mathfrak{P})$.

例 1. 試取屢次引用之六次可遷羣

$$1 \qquad Q=(a_1a_5)(a_2a_4)$$

$$P=(aa_1a_2a_3a_4a_5) \qquad PQ=(aa_5)(a_1a_4)(a_2a_3)$$

$$P^2=(aa_2a_4)(a_1a_3a_5) \qquad P^2Q=(aa_4)(a_1a_3)$$

$$P^3=(aa_3)(a_1a_4)(a_2a_5) \qquad P^3Q=(aa_3)(a_1a_2)(a_4a_5)$$

$$P^4=(aa_4a_2)(a_1a_5a_3) \qquad P^4Q=(aa_2)(a_3a_5)$$

$$P^5=(aa_5a_4a_3a_2a_1) \qquad P^5Q=(aa_1)(a_2a_5)(a_3a_4).$$

是中文字a不動之約羣爲

$$\mathfrak{H}: \quad 1, \quad (a_1a_5)(a_2a_4),$$

而
$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P+\mathfrak{H}P^2+\mathfrak{H}P^3+\mathfrak{H}P^4+\mathfrak{H}P^5.$$

且$\mathfrak{H}$不使a, a_3二文字移動. 故其正常化羣爲

$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}\,(aa_3)(a_1a_4)(a_2a_5)=\mathfrak{H}+\mathfrak{H}P^3.$$

而
$$\mathfrak{G}=\mathfrak{K}+\mathfrak{K}P+\mathfrak{K}P^2$$
$$=(\mathfrak{H}+\mathfrak{H}P^3)+(\mathfrak{H}P+\mathfrak{H}P^4)+(\mathfrak{H}P^2+\mathfrak{H}P^5).$$

故$(\mathfrak{P})$中之可遷系爲

$$\mathfrak{H},\ \mathfrak{H}P^3;\ \mathfrak{H}P,\ \mathfrak{H}P^4;\ \mathfrak{H}P^2,\ \mathfrak{H}P^5.$$

以故$(\mathfrak{P})$之置換之第一因子爲

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}P^3 \\ \mathfrak{H} & \mathfrak{H}P^3 \end{pmatrix}=1. \quad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P^3 \\ \mathfrak{H}P^3 & \mathfrak{H}P^3P^3 \end{pmatrix}=(\mathfrak{H}, \mathfrak{H}P^3);$$

於此而代入他之可遷系，便得

第二因子　　1. $(\mathfrak{H}P, \mathfrak{H}P^4)$,

第三因子　　1. $(\mathfrak{H}P^2, \mathfrak{H}P^5)$.

以之相乘得

$$1. \quad (\mathfrak{H}, \mathfrak{H}P^3)(\mathfrak{H}P, \mathfrak{H}P^4)(\mathfrak{H}P^2, \mathfrak{H}P^5),$$

是卽表示$(\mathfrak{R})$中互異之置換者也.

最後，於此等置換中，代 $\mathfrak{H}$, $\mathfrak{H}P$, $\mathfrak{H}P^2$, ……, $\mathfrak{H}P^5$ 以 a, a_1, a_2, ……, a_5, 得

$$1. \quad (aa_3)(a_1a_4)(a_2a_5).$$

此卽與$\mathfrak{G}$之各置換爲交換可能之置換也.

注意. 如本例之羣含有六次巡回羣 $\{P\}$ 者然，凡可遷羣若含有與之同次之 Abel 氏可遷羣時，則與此可遷羣之各置換爲交換可能者之置換，皆屬於該羣也. 蓋因其與 Abel 氏可遷羣之各置換爲交換可能者之置換，非屬於同羣不可故(第89節參照).

例2. 試取六次可遷羣

1	(03)(14)	(03)(25)	(14)(25)
(012)(345)	(042)(153)	(045)(123)	(015)(234)
(021)(354)	(054)(132)	(051)(243)	(024)(135).

此中文字0不動之約羣爲

$$\mathfrak{H}: \quad 1, \quad (14)(25).$$

而 $$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}(012)(345)+\mathfrak{H}(021)(354)$$
$$+\mathfrak{H}(03)(14)+\mathfrak{H}(042)(153)+\mathfrak{H}(054)(132).$$

$\mathfrak{H}$ 不能使二文字 0, 3 動也。故其正常化羣爲

$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}(03)(14).$$

而 $$\mathfrak{G}=\mathfrak{K}+\mathfrak{K}(012)(345)+\mathfrak{K}(021)(354)$$
$$=\mathfrak{H}+\mathfrak{H}(03)(14)$$
$$+\mathfrak{H}(012)(345)+\mathfrak{H}(042)(153)$$
$$+\mathfrak{H}(021)(354)+\mathfrak{H}(054)(132)$$

故 $(\mathfrak{P})$ 中之可遷系爲

$$\mathfrak{H}, \qquad \mathfrak{H}(03)(14);$$
$$\mathfrak{H}(012)(345) \qquad \mathfrak{H}(042)(153);$$
$$\mathfrak{H}(021)(354) \qquad \mathfrak{H}(054)(132).$$

其次, $(\mathfrak{P})$ 之第一因子之置換分別爲

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}(03)(14)\\ \mathfrak{H} & \mathfrak{H}(03)(14)\end{pmatrix}=1.$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}(03)(14)\\ \mathfrak{H}(03)(14) & \mathfrak{H}(03)(14)\cdot(03)(14)\end{pmatrix}=(\mathfrak{H},\ \mathfrak{H}(03)(14)).$$

於此而代入他之可遷系, 則得第二因子

$$1,\quad (\mathfrak{H}(012)(345),\ \mathfrak{H}(042)(153))$$

及第三因子

$$1,\quad (\mathfrak{H}(021)(354),\ \mathfrak{H}(054)(132))$$

以之相乘, 得

$$1,\quad (\mathfrak{H},\ \mathfrak{H}(03)(14)(\mathfrak{H}(012)(345),\ \mathfrak{H}(042)(153))$$

$$\times\big(\mathfrak{H}(021)(354),\ \mathfrak{H}(054)(132)\big).$$

再於此代傍系以文字,得

$$1,\quad (03)(14)(25).$$

是卽與$\mathfrak{G}$之各置換爲交換可能者也.

第十六章　自己同態,全形

95. 一羣中,其元素間所立之對應,適合次之條件時,則曰此對應決定羣之**自己同態**云. 卽對於羣之一元素,僅有羣之一而且唯一之元素與之對應,於相異之元素,則有相異者與之對應,而於羣之二元素之積AB則有各別對應之元素之積相與對應者是也.

自己同態中,其各元素與其自身對應者,則名曰**不動同態**.

於一自己同態中,對羣之元素

$$G_0, G_1, \cdots\cdots, G_{g-1}\quad (G_0=1),$$

分別有

$$G_0', G_1', \cdots\cdots, G_{g-1}'$$

與之對應時,則此同態以記號

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G_{g-1}' \end{bmatrix}$$

記之,或略記爲

$$\begin{bmatrix} G_r \\ G_r' \end{bmatrix}.$$

二羣之單純同態中，其兩羣之一致者，卽自己同態也．故雖在自己同態者言，其主元素亦常與其自身對應．又互爲對應之二元素，則有同一之巡回率焉．

例. (i) $\begin{bmatrix} 1 & (abc) & (acb) & (bc) & (ca) & (ab) \\ 1 & (acb) & (abc) & (ca) & (bc) & (ab) \end{bmatrix}$.

(ii) $\begin{bmatrix} 1 & (abcd) & (ac)(bd) & (adcb) \\ 1 & (adcb) & (ac)(bd) & (abcd) \end{bmatrix}$.

(iii) $\begin{bmatrix} 1 & (ab)(cd) & (ac)(bd) & (ad)(bc) \\ 1 & (ac)(bd) & (ad)(bc) & (ab)(cd) \end{bmatrix}$.

96. 內外同態.

設 G 爲羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之任意之元素．若對 $\mathfrak{G}$ 之元素 G_i，使 $G^{-1}G_iG$ 相與對應時，則生次之自己同態

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G^{-1}G_0G & G^{-1}G_1G & \cdots\cdots & G^{-1}G_{g-1}G \end{bmatrix}$$

明甚．是種之自己同態名曰**內同態**；對此而言，則其他者概名曰**外同態**．

如 $(ab)(abc)(ab)=(acb)$, $(ab)(acb)(ab)=(abc)$,

$(ab)(bc)(ab)=(ca)$, $(ab)(ca)(ab)=(bc)$, $(ab)(ab)(ab)=(ab)$,

職是之故，則前節第一例，乃表示三次對稱羣

$$\mathfrak{S}: \quad 1, (abc), (acb), (bc), (ca), (ab)$$

之內同態也．又以各元素將此羣變形，則得

$$\mathfrak{S} \quad : \quad 1, (abc), (acb), (bc), (ca), (ab);$$

$$(abc)^{-1}\,\mathfrak{S}\,(abc): \quad 1, (abc), (acb), (ca), (ab), (bc);$$

$$(acb)^{-1}\ \mathfrak{S}\ (acb):\quad 1,\ (abc),\ (acb),\ (ab),\ (bc),\ (ca);$$

$$(bc)^{-1}\ \mathfrak{S}\ (bc):\quad 1,\ (acb),\ (abc),\ (bc),\ (ab),\ (ca);$$

$$(ca)^{-1}\ \mathfrak{S}\ (ca):\quad 1,\ (acb),\ (abc),\ (ab),\ (ca),\ (bc);$$

$$(ab)^{-1}\ \mathfrak{S}\ (ab):\quad 1,\ (acb),\ (abc),\ (ca),\ (bc),\ (ab).$$

故對三次對稱羣，得生六種之內同態也.

上記之羣 $\mathfrak{G}$ 若爲 Abel 氏羣，是乃一特例. 此時 $G^{-1}G_iG=G_i$，因之 $\left[\begin{matrix}G_r\\G^{-1}G_rG\end{matrix}\right]$ 爲不動同態. 故 Abel 氏羣之自己同態，除不動的者以外，其他皆外同態也. 前節例 (ii), (iii) 皆就 Abel 氏羣論之者. 故二者皆表示外同態.

又就羣之種類言，其不容有外同態者亦有之. 三次對稱羣，卽其一例. 蓋因

$$(abc)^2=(acb),\ (abc)(bc)=(ac),\ (abc)^2(bc)=(ab),$$

故三文字 a, b, c 之對稱羣 $\mathfrak{S}$，乃由二置換 $(abc), (bc)$ 所生成. 是則 $\mathfrak{S}$ 之自己同態，若其與此兩置換之相對應者定，則由之得一意的而決定也. 然 $\mathfrak{S}$ 之六置換之中，其得與 (abc) 對應者爲 (abc) 或 (acb); 與 (bc) 對應者爲 $(bc), (ca)$ 以及 (ab) (因對應元素之巡回率爲同一故). 故對應之可能者，總共不過六種. 但自他面觀，$\mathfrak{S}$ 有如上述，乃有六種之內同態. 故外同態爲所不容耳.

97. 同態羣.

在羣之自己同態中，其與相異元素對應者常相異也.

故與羣$\mathfrak{G}$之自己同態

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G'_{g-1} \end{bmatrix}$$

應,元素之置換

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G'_{g-1} \end{pmatrix}$$

生焉. 此則名曰$\mathfrak{G}$之同態置換;或簡曰同態,爲便利計也.

定理. 一羣中所有同態置換之集合成羣.

此羣名曰與羣之同態羣.

證明. 令 $\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G'_{g-1} \end{bmatrix}$及$\begin{bmatrix} G_0' & G_1' & \cdots\cdots & G'_{g-1} \\ G_0'' & G_1'' & \cdots\cdots & G''_{g-1} \end{bmatrix}$

爲羣$\mathfrak{G}$之二自己同態. 於是於前者,則積G_iG_j有$G_i'G_j'$與之對應;於後者,則積$G_i'G_j'$有$G_i''G_l''$與之對應. 故對G_i若使G_i''與之對應,則由之得自己同態

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0'' & G_1'' & \cdots\cdots & G''_{g-1} \end{bmatrix}.$$

但自他面言,其與兩同態$\begin{bmatrix} G_r \\ G_r' \end{bmatrix}$及$\begin{bmatrix} G_r' \\ G_r'' \end{bmatrix}$相伴之置換相乘,則得

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G'_{g-1} \end{pmatrix}\begin{pmatrix} G_0' & G_1' & \cdots\cdots & G'_{g-1} \\ G_0'' & G_1'' & \cdots\cdots & G''_{g-1} \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0'' & G_1'' & \cdots\cdots & G''_{g-1} \end{pmatrix},$$

而此積乃由同態$\begin{bmatrix} G_r \\ G_r'' \end{bmatrix}$而生之置換也. 故定理云云.

定理. 一羣$\mathfrak{G}$之內同態置換之集合,成一與$\mathfrak{G}$同態之羣,(此名曰內同態羣.) 而此羣於同態羣中爲正常的.

證明. 設 $G_0, G_1, \cdots\cdots, G_{g-1}$ 爲 $\mathfrak{G}$ 之元素. 將 $\mathfrak{G}$ 之內同態置換之二相乘, 則有

$$\begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ G_i^{-1}G_0G_i & G_i^{-1}G_1G_i & \cdots & G_i^{-1}G_{g-1}G_i \end{pmatrix}\begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ G_j^{-1}G_0G_j & G_j^{-1}G_1G_j & \cdots & G_j^{-1}G_{g-1}G_j \end{pmatrix}$$

$$=\begin{pmatrix} G_0 & \cdots & G_{g-1} \\ G_i^{-1}G_0G_i & \cdots & G_i^{-1}G_{g-1}G_i \end{pmatrix}\begin{pmatrix} G_i^{-1}G_0G_i & \cdots & G_i^{-1}G_{g-1}G_i \\ G_j^{-1}\cdot G_i^{-1}G_0G_i\cdot G_j & \cdots & G_j^{-1}\cdot G_i^{-1}G_{g-1}G_i\cdot G_j \end{pmatrix}$$

$$=\begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ G_j^{-1}G_i^{-1}G_0G_iG_j & G_j^{-1}G_i^{-1}G_1G_iG_j & \cdots & G_j^{-1}G_i^{-1}G_{g-1}G_iG_j \end{pmatrix}$$

$$=\begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ (G_iG_j)^{-1}G_0(G_iG_j) & (G_iG_j)^{-1}G_1(G_iG_j) & \cdots & (G_iG_j)^{-1}G_{g-1}(G_iG_j) \end{pmatrix},$$

而此積仍爲內同態置換. 故內同態置換

$$\begin{pmatrix} G_r \\ G_r \end{pmatrix},\ \begin{pmatrix} G_r \\ G_1^{-1}G_rG_1 \end{pmatrix},\ \cdots\cdots,\ \begin{pmatrix} G_r \\ G_{g-1}^{-1}G_rG_{g-1} \end{pmatrix}$$

成羣也.

次之, 對 $\mathfrak{G}$ 之元素 G_i, 使內同態羣之置換 $\begin{pmatrix} G_r \\ G_i^{-1}G_rG_i \end{pmatrix}$ 相與對應, 則由上式, 可知兩羣之爲同態甚明. 而於此同態關係, 與內同態羣之主元素對應者, 則爲 $\mathfrak{G}$ 之中核焉.*

最後, 取 $\mathfrak{G}$ 之同態置換 $\begin{pmatrix} G_r \\ G_r' \end{pmatrix}$, 而以之變內同態置換 $\begin{pmatrix} G_r \\ G_i^{-1}G_rG_i \end{pmatrix}$ 之形, 則得

$$\begin{pmatrix} G_r \\ G_r' \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_i^{-1}G_rG_i \end{pmatrix}\begin{pmatrix} G_r \\ G_r' \end{pmatrix}=\begin{pmatrix} G_r' \\ G_r \end{pmatrix}\begin{pmatrix} G_r \\ G_i^{-1}G_rG_i \end{pmatrix}\begin{pmatrix} G_i^{-1}G_rG_i \\ G_i'^{-1}G_r'G_i' \end{pmatrix}$$

$$=\begin{pmatrix} G_r' \\ G_i'^{-1}G_r'G_i' \end{pmatrix}=\begin{pmatrix} G_s \\ G_i'^{-1}G_sG_i' \end{pmatrix},$$

---

*由羣 $\mathfrak{G}$ 中所有自己共軛元素而成之約羣, 名曰 $\mathfrak{G}$ 之中核.

此結果仍爲內同態也. 故內同態羣, 於同態羣中爲正常的.

定理. 設$(\mathfrak{G})$爲羣$\mathfrak{G}$之正置換表示,$(\mathfrak{G}')$爲$(\mathfrak{G})$之接合羣,$(\mathfrak{H})$爲$\mathfrak{G}$之內同態羣,則

$$(\mathfrak{G}')(\mathfrak{G})=(\mathfrak{H})(\mathfrak{G}).$$

證明. 與前定理同樣,以$G_0(=1), G_1, \cdots\cdots, G_{g-1}$爲$\mathfrak{G}$之元素,則由第89節,$(\mathfrak{G}')$之置換爲

$$\begin{pmatrix} G_r \\ G_j\, G_r \end{pmatrix},\quad j=0, 1, 2, \cdots\cdots, g-1.$$

故積$(\mathfrak{G}')(\mathfrak{G})$之置換,得以

$$\begin{pmatrix} G_r \\ G_j\, G_r \end{pmatrix}\begin{pmatrix} G_r \\ G_r\, G_i \end{pmatrix}=\begin{pmatrix} G_r \\ G_j\, G_r\, G_i \end{pmatrix},\quad i, j=0, 1, 2\cdots\cdots, g-1$$

與之. 此中不使$G_0(=1)$動者爲次之g個

$$(1)\qquad \begin{pmatrix} G_r \\ G_i^{-1}\, G_r\, G_i \end{pmatrix},\quad i=0, 1, 2\cdots\cdots, g-1$$

甚明. 然$(\mathfrak{G}')$之各元素與$(\mathfrak{G})$爲交換可能,故積$(\mathfrak{G}')(\mathfrak{G})$成羣也. 而其之爲可遷的亦甚明. 故置換(1),於可遷羣$(\mathfrak{G}')(\mathfrak{G})$中作一不使$G_0$動之約羣焉. 茲以$(\mathfrak{H})$表之,而就之分$(\mathfrak{G}')(\mathfrak{G})$爲傍系,則得

$$(\mathfrak{G}')(\mathfrak{G})=(\mathfrak{H})+(\mathfrak{H})\begin{pmatrix} G_r \\ G_r G_1 \end{pmatrix}+\cdots\cdots+(\mathfrak{H})\begin{pmatrix} G_r \\ G_r G_{g-1} \end{pmatrix}.$$

故

$$(\mathfrak{G}')(\mathfrak{G})=(\mathfrak{H})(\mathfrak{G}).$$

自他面言,$(\mathfrak{H})$卽(1)明爲$\mathfrak{G}$之內同態羣,故由最後之式遂

得本定理也.

98. 正置換羣之全形.

與前節同樣,令羣 $\mathfrak{G}$ 之元素爲 $\mathfrak{G}_0(=1), G_1, \cdots\cdots, G_{g-1}$. 以任意之同態置換 $\begin{pmatrix} G_r \\ G'_r \end{pmatrix}$ 將 $\mathfrak{G}$ 之正置換表示之一置換 $\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$ 變形,則得

$$\begin{pmatrix} G_r \\ G'_r \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\begin{pmatrix} G_r \\ G'_r \end{pmatrix}=\begin{pmatrix} G'_r \\ G_r \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\begin{pmatrix} G_rG_i \\ G'_rG'_i \end{pmatrix}=\begin{pmatrix} G_r \\ G'_rG'_i \end{pmatrix}=\begin{pmatrix} G_s \\ G_sG'_i \end{pmatrix}.$$

而此結果乃 $\mathfrak{G}$ 之正置換表示之一置換. 因之得次

定理. 一羣之同態置換,與其羣之正置換表示爲交換可能.

今以羣 $\mathfrak{G}$ 之正置換表示爲 $(\mathfrak{G})$,同態羣爲 $(\mathfrak{L})$,則由本定理,$(\mathfrak{L})(\mathfrak{G})$ 成羣,而以 $(\mathfrak{G})$ 爲其正常約羣. 此羣名曰 $(\mathfrak{G})$ 之**全形**.

定理. g 元羣之正置換表示 $(\mathfrak{G})$ 之全形,爲 g 次對稱羣中 $(\mathfrak{G})$ 之正常化羣.

證明. 在 g 元羣 $\mathfrak{G}$ 之元素 $G_0(=1), G_1, \cdots\cdots, G_{g-1}$ 上所行置換之中,其與正置換表示 $(\mathfrak{G})$ 爲交換可能者乃作 $(\mathfrak{G})$ 之正常化羣(於 g 次對稱羣中). 茲以 $(\mathfrak{H})$ 表之.

$(\mathfrak{H})$ 之含 $(\mathfrak{G})$ 明矣,因之爲可遷的. 故於 $(\mathfrak{H})$,其不使 G_0 動者之約羣以爲 $(\overline{\mathfrak{L}})$,則

$$(1)\quad (\mathfrak{H})=(\overline{\mathfrak{L}})+(\overline{\mathfrak{L}})\begin{pmatrix} G_r \\ G_rG_1 \end{pmatrix}+\cdots\cdots+(\overline{\mathfrak{L}})\begin{pmatrix} G_r \\ G_rG_{g-1} \end{pmatrix}.$$

今取$(\overline{\mathfrak{Q}})$之任意置換

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \end{pmatrix} \quad [G_0=\overline{G}_0=1],$$

而以之變$(\mathfrak{G})$之置換$\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$之形，則得

$$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \end{pmatrix}^{-1} \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix} \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \end{pmatrix}$$

$$= \begin{pmatrix} \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \\ \overline{G_0G_i} & \overline{G_1G_i} & \cdots\cdots & \overline{G_{g-1}G_i} \end{pmatrix},$$

但$\overline{G_rG_i}$乃示於$\begin{pmatrix} G_r \\ \overline{G}_r \end{pmatrix}$中，積$G_rG_i$得爲其所置換者. 然由假設，$(\mathfrak{H})$之置換與$(\mathfrak{G})$爲交換可能，故$\begin{pmatrix} G_r \\ \overline{G_rG_i} \end{pmatrix}$不得不屬於$(\mathfrak{G})$也. 卽

$$\begin{pmatrix} \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \\ \overline{G_0G_i} & \overline{G_1G_i} & \cdots\cdots & \overline{G_{g-1}G_i} \end{pmatrix} = \begin{pmatrix} \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \\ \overline{G}_0A_i & \overline{G}_1A_i & \cdots\cdots & \overline{G}_{g-1}A_i \end{pmatrix},$$

$$i=0, 1, 2, \cdots\cdots, g-1,$$

但A_i乃表$\mathfrak{G}$之某元素者. 故

$$\overline{G_0G_i}=\overline{G}_0A_i,$$

$$\overline{G_rG_i}=\overline{G}_rA_i \quad (r=1, 2, \cdots\cdots, g-1;\ i=0, 1, 2, \cdots\cdots, g-1).$$

然 $\overline{G}_0=G_0=1$. 故由第一式，

$$\overline{G}_i=A_i \quad (i=0, 1, 2, \cdots\cdots, g-1).$$

以此代入上式，得

$$\overline{G_0G_i}=\overline{G}_0\cdot\overline{G}_i,$$

$$\overline{G_rG_i}=\overline{G}_r\cdot\overline{G}_i \quad (r=1, 2, \cdots\cdots, g-1;\ i=0, 1, 2, \cdots\cdots, g-1).$$

是卽示於置換$\begin{pmatrix}G_r\\G_r\end{pmatrix}$，積$G_rG_i$得以能置換各因子者之元素之積而置換之者也．故此之置換爲同態置換．因之$(\overline{\mathfrak{Q}})$爲僅由同態置換而成．

自他面言，因$\mathfrak{G}$之同態置換與$(\mathfrak{G})$爲交換可能，故其非含於$(\mathfrak{H})$不可．加以其爲不使主元素G_0動者．故同態置換統含於$(\overline{\mathfrak{Q}})$也．由此與上述，則$(\overline{\mathfrak{Q}})$與$\mathfrak{G}$之同態羣$(\mathfrak{Q})$一致可知．故由(1)，

$$(\mathfrak{H})=(\mathfrak{Q})(\mathfrak{G}).$$

是卽定理之所主張也．

定理．若$(\mathfrak{H})$爲羣$\mathfrak{G}$之內同態羣，則商$\dfrac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})(\mathfrak{H})}$與$\dfrac{(\mathfrak{Q})}{(\mathfrak{H})}$爲單純同態．

證明．因同態置換，乃不使主元素動者，故$(\mathfrak{Q})$與$(\mathfrak{G})$無有共通置換(非爲不動的)．故$(\mathfrak{Q})$之置換若以

$$L_0, L_1, \cdots\cdots, L_{l-1}$$

表之，則得

$$(\mathfrak{G})(\mathfrak{Q})=(\mathfrak{G})L_0+(\mathfrak{G})L_1+\cdots\cdots+(\mathfrak{G})L_{l-1}.$$

故其由$(\mathfrak{G})$之商爲

$$\frac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})}:\ L_0, L_1, \cdots\cdots, L_{l-1}\ \ (\mathrm{mod}.(\mathfrak{G})),$$

而其與$(\mathfrak{Q})$之爲單純同態明也．同樣，$\dfrac{(\mathfrak{G})(\mathfrak{H})}{(\mathfrak{G})}$與$(\mathfrak{H})$爲單純同態．故

$$\frac{\frac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})}}{\frac{(\mathfrak{G})(\mathfrak{H})}{(\mathfrak{G})}} \sim \frac{(\mathfrak{Q})}{(\mathfrak{H})}$$ [~爲單純同態之記號].

然由第46節第二定理系2,

$$\frac{\frac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})}}{\frac{(\mathfrak{G})(\mathfrak{H})}{(\mathfrak{G})}} \sim \frac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})(\mathfrak{H})},$$

$$\therefore \quad \frac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})(\mathfrak{H})} \sim \frac{\mathfrak{Q}}{\mathfrak{H}}.$$

且正置換羣之爲一個羣之正置換表示乃既知者已. 故於本節中所討論之置換,其元素$G_0, G_1, \cdots\cdots, G_{g-1}$代以$g$個文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{g-1}$,則$(\mathfrak{G})$遂爲此$g$文字之正置換羣(名曰$\overline{\mathfrak{G}}$),而其全形$(\mathfrak{H})$則由本節第二定理,爲於同$g$文字之對稱羣中$\mathfrak{G}$之正常化羣也. 於是全形者,雖如次定義之,亦無所不可. 卽:

若$\overline{\mathfrak{G}}$爲g文字之正置換羣時,則於此g文字上所行之置換中,其與$\overline{\mathfrak{G}}$爲交換可能者成羣也. 此羣名曰$\overline{\mathfrak{G}}$之**全形**.

定理. 正置換表示之全形,與其接合羣之全形一致.

證明. 設$(\mathfrak{G}')$爲羣$\mathfrak{G}[G_0(=1), G_1, \cdots\cdots, G_{g-1}]$之正置換表示$(\mathfrak{G})$之接合羣. $\mathfrak{G}$之同態羣$(\mathfrak{Q})$之各置換,與$(\mathfrak{G}')$爲交換可能也. 反之,與$(\mathfrak{G}')$爲交換可能之置換($\mathfrak{G}$之元素上所行者)中,其不使G_0動者之屬於$(\mathfrak{Q})$,則與第一及第二定

理中者同樣得以證明，由是而本定理得告成立焉.

系.　$(\mathfrak{F})=(\mathfrak{Q})(\mathfrak{G}')$.

99. 全形之可遷置複度.

如前節第二定理之所證明，在$(\mathfrak{G})$之全形$(\mathfrak{F})$中，其主元素G_0不動者之約羣，乃同態羣$(\mathfrak{Q})$也. 故

$$(\mathfrak{F})=(\mathfrak{Q})+(\mathfrak{Q})\left(\frac{G_r}{G_rG_1}\right)+\cdots\cdots+(\mathfrak{Q})\left(\frac{G_r}{G_rG_{g-1}}\right).$$

1°. $(\mathfrak{F})$爲二重可遷時

此時$(\mathfrak{Q})$就元素$G_1, G_2, \cdots\cdots, G_{g-1}$言爲可遷的(第64節). 乃取此$g-1$個元素中其巡回率爲素數(以之爲$p$)之元素G. 因$(\mathfrak{Q})$爲可遷的，故其含有將G分別置換爲$G_1, G_2, \cdots\cdots, G_{g-1}$者之置換. 然在自己同態中，其相對應之元素乃有同一巡回率. 故此$g-1$個元素，非皆與G具有同一之巡回率不可也. 因之$\mathfrak{G}$之元數不得不與素數冪p^m等. 但自他面言，p^m元羣含有自己共軛元素(非主元素者). 以其一爲G，則於自己同態中，其得與G對應之元素$G_1, G_2, \cdots\cdots, G_{g-1}$，亦必自己共軛也. 是則$\mathfrak{G}$爲Abel氏羣已.

以故若全形$(\mathfrak{F})$爲二重可遷，隨之$(\mathfrak{Q})$亦爲可遷的，則羣$\mathfrak{G}$爲Abel氏羣，而所有之元素(除主元素外)非皆以同一之素數爲巡回率不可也.

2°. $(\mathfrak{F})$爲三重可遷時.*

*$\mathfrak{G}$爲3元時，則於次節自明. 故現僅就4元以上者論之.

此時(𝔔)乃二重可遷(第64節). 茲取$G_1, G_2, \cdots\cdots, G_{g-1}$中之任意者之G. 若假定$G^2 \neq 1$, 則$g-1$個元素中, 其異於G, G^2之兩者者必定存在. 試取其一, G'. 因(𝔔)爲二重可遷, 故(𝔔)之置換中, 將G, G^2分別換置爲G, G'者亦得存在. 是則與自己同態之定義反. (因若以G與G相對應, 則G^2與G^2相對應故.) 故$G^2=1$爲必要也. 因之, (𝔖)若爲三重可遷, 隨之(𝔔)爲二重可遷, 則𝔊乃各元素之巡回率爲2者之Abel氏羣也. (但𝔊爲3元時則除外.)

3°. 若𝔊爲素數冪P^m元Abel氏羣, 且其元素之巡回率爲P, 則(𝔊)之正置換表示(𝔊)之全形(𝔖)爲多重可遷. 而p若爲奇數, 則(𝔖)爲二重可遷; p若爲2, 則爲三重可遷. 此則由後所述自明也(參照第130, 135節).

100. 亞巡回羣.

試取素數元巡回羣

(1) $A^0, A, A^2, \cdots\cdots, A^{p-1}$ $(A^0=1, A^p=1)$.

但$p \neq 2$.

1°. {A}之同態羣.

在{A}之自己同態中, 與元素A相對應者以爲A^α, 則與他之元素A^r相對應者乃爲$A^{r\alpha}$. 反之, 對1, 2, $\cdots\cdots$, $p-1$中任意之數α, 則

$$\begin{bmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^\alpha & A^{2\alpha} & \cdots\cdots & A^{(p-1)\alpha} \end{bmatrix}$$

乃表示自己同態也. 是蓋因 p 爲素數,故得

$$\{A^a\}=\{A\},$$

而由是自明耳. 以故 $\{A\}$ 之同態羣之置換,得以

$$(2)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^a & A^{2a} & \cdots\cdots & A^{(p-1)a} \end{pmatrix},\quad (a=1,2,\cdots\cdots,p-1)$$

與之也. 此羣以 $(\mathfrak{S})$ 表之.

欲明 $(\mathfrak{S})$ 之構成,乃取 p 之原根* 之一,ρ. 於是數列

$$(3)\quad \rho^0(=1),\ \rho,\ \rho^2,\ \cdots\cdots,\ \rho^{p-2}\quad [\rho^{p-1}\equiv 1\ (\mathrm{mod.}\ p)],$$

若就法 p 而取之,則於某順序言,乃與數列

$$(4)\qquad 1,\ 2,\ 3,\ \cdots\cdots,\ p-1$$

一致. 故羣(1)得換書爲

$$A^0,\ A,\ A\rho,\ A\rho^2,\ \cdots\cdots,\ A\rho^{p-2},$$

因之,得

$$(5)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^a & A^{2a} & \cdots\cdots & A^{(p-1)a} \end{pmatrix}=\begin{pmatrix} A^0 & A & A\rho & A\rho^2 & \cdots\cdots & A\rho^{p-2} \\ A^0 & A^a & A^{a\rho} & A^{a\rho^2} & \cdots\cdots & A^{a\rho^{p-2}} \end{pmatrix}$$

$$a=1,\ 2,\ \cdots\cdots,\ p-1.$$

---

*設 a 爲不能以 p 整除之整數. 於是由 Fermat 氏定理,

$$a^{p-1}\equiv 1\ (\mathrm{mod.}\ p).$$

故 a 者,若以之高至適當之冪,則爲與 1 合同(法 p) 也. 在若是之冪中,其最低者爲 a^d 時,卽

$$a^d\equiv 1\ (\mathrm{mod.}\ p.),\quad a^x\not\equiv 1\ (\mathrm{mod.}\ p\ )\ [0<x<d]$$

時,則 d 名曰 a 對法 p 之所屬之指數. 此指數恰與 $p-1$ 等者常存在. 若 a 所屬之指數等於 $p-1$ 時,則 a 名曰 p 之原根.

更於此將α所可取得之值(4)以(3)代之，則同態羣之置換再得換書爲

$$(6)\quad \begin{pmatrix} A^0 & A & A^{\rho} & A^{\rho^2} & \cdots\cdots & A^{\rho^{p-2}} \\ A^0 & A^{\rho^s} & A^{\rho^{1+s}} & A^{\rho^{2+s}} & \cdots\cdots & A^{\rho^{p-2+s}} \end{pmatrix} \quad (s=0,\ 1,\ 2,\ \cdots\cdots,\ p-2).$$

然

$$\begin{pmatrix} A^0 & A & A^{\rho} & \cdots\cdots & A^{\rho^{p-2}} \\ A^0 & A^{\rho} & A^{\rho^2} & \cdots\cdots & A^{\rho^{p-1}} \end{pmatrix} = (A\ A^{\rho}\ A^{\rho^2}\ \cdots\cdots A^{\rho^{p-2}}),$$

而此置換若以Q表之，則得

$$\begin{pmatrix} A^0 & A & A^{\rho} & \cdots\cdots & A^{\rho^{p-2}} \\ A^0 & A^{\rho^s} & A^{\rho^{1+s}} & \cdots\cdots & A^{\rho^{p-2+s}} \end{pmatrix} = Q^s.$$

故巡回羣$\{A\}$之同態羣$(\mathfrak{Q})$爲

$$(7)\qquad Q^0,\ Q,\ Q^2,\ \cdots\cdots,\ Q^{p-2}\quad (Q^0=1,\ Q^{p-1}=1),$$

即$p-1$次$p-1$元之巡回羣也. 因之，對$p-1$個元素A, A^{ρ}, $\cdots\cdots$, A^{p-1}爲可遷的.

2'. 全形，亞巡回羣.

羣$\{A\}$之正置換表示爲

$$(8)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^{\beta} & A^{1+\beta} & A^{2+\beta} & \cdots\cdots & A^{p-1+\beta} \end{pmatrix} \quad (\beta=0,\ 1,\ 2,\ \cdots\cdots,\ p-1).$$

茲以$(\mathfrak{P})$表之. 將$(\mathfrak{P})$之各置換乘於同態羣$(\mathfrak{Q})$之置換(2)，得

$$\begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^{\alpha} & A^{2\alpha} & \cdots\cdots & A^{(p-1)\alpha} \end{pmatrix} \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^{\beta} & A^{1+\beta} & A^{2+\beta} & \cdots\cdots & A^{p-1+\beta} \end{pmatrix}$$

$$= \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^{\beta} & A^{\alpha+\beta} & A^{2\alpha+\beta} & \cdots\cdots & A^{(p-1)\alpha+\beta} \end{pmatrix} \quad \begin{cases} \alpha=1,\ 2,\ \cdots\cdots,\ p-1 \\ \beta=0,\ 1,\ 2,\ \cdots\cdots,\ p-1 \end{cases}.$$

故$(\mathfrak{P})$之全形之置換爲

$$(9)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^\beta & A^{\alpha+\beta} & A^{2\alpha+\beta} & \cdots\cdots & A^{(p-1)\alpha+\beta} \end{pmatrix} \begin{cases} \alpha=1,2,\cdots\cdots,p-1 \\ \beta=0,1,2,\cdots\cdots,p-1 \end{cases}.$$

(對於 α, β 與以一組之值，則一置換由此而定). 就此置換而觀，若適當的取 α, β 之值，則二元素 A^0, A 得爲任意兩元素所置換甚明. 故此全形爲二重可遷的也.*

又與 A 對應之 $(\mathfrak{P})$ 之置換爲

$$\begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A & A^2 & A^3 & \cdots\cdots & A^p \end{pmatrix} = (A^0 A\ A^2 \cdots\cdots A^{p-1}).$$

將此以 P 示之，則因 $(\mathfrak{P})$ 爲 p 元巡回羣之故，其置換得以

$$(10)\quad P^0, P, P^2, \cdots\cdots, P^{p-1} \quad (P^0=1, P^p=1)$$

與之也. 以此乘於 $(\mathfrak{Q})$ 之置換 (7)，則得 $p(p-1)$ 個之積

$$(11)\quad Q^i P^j \begin{cases} i=0,1,2,\cdots\cdots,p-2 \\ j=0,1,2,\cdots\cdots,p-1. \end{cases}$$

是卽將全形以其母元素† 表之者也.

一般，素數次正置換羣(卽素數次素數元巡回羣)之全形，名曰**亞巡回羣**. 上記 $(\mathfrak{P})$ 之全形 (9) 卽 (11)，乃 p 次亞巡回羣焉.

3°. 今爲使亞巡回羣之置換更易明瞭起見，乃於 2° 所討論之置換，將元素 $A^0, A, A^2, \cdots\cdots, A^{p-1}$ 代以文字 0, 1, 2,

---

*全形 (9) 之爲二重可遷，雖不觀此置換，但因同態羣 $(\mathfrak{Q})$ 如 1° 之所示爲可遷的，故直由之亦可得知.

†母元素之意義請參閱第 42 節.

……, $p-1$, 則 P 遂爲 $(0, 1, 2, \cdots\cdots, p-1)$; 隨而正置換表示 (10) 爲

$$1, (0, 1, 2, \cdots\cdots, p-1), (0, 1, 2, \cdots\cdots, p-1)^2, \cdots\cdots,$$
$$(0, 1, 2, \cdots\cdots, p-1)^{p-1};$$

而全形 (9) 爲

$$(12)\quad \begin{pmatrix} 0 & 1 & 2 & \cdots\cdots & p-1 \\ \beta & \alpha+\beta & 2\alpha+\beta & \cdots\cdots & (p-1)\alpha+\beta \end{pmatrix} \begin{cases} \alpha=1, 2, \cdots\cdots, p-1, \\ \beta=0, 1, 2, \cdots\cdots, p-1. \end{cases}$$

(但此置換中之下列爲就法 p 而取之者.) 此乃 p 次 p 元巡回羣 $\{(0, 1, 2, \cdots\cdots, p-1)\}$ 之全形卽 p 次亞巡回羣也.

由上同一之代入, 置換 Q 乃爲 $(1, \rho, \rho^2, \cdots\cdots, \rho^{p-2})$,* 因之由 (11), 亞巡回羣又得以

$$(13)'\quad (1, \rho, \rho^2, \cdots, \rho^{p-2})^i (0, 1, 2, \cdots, p-1)^j \begin{cases} i=0, 1, 2, \cdots, p-2 \\ j=0, 1, 2, \cdots, p-1 \end{cases}$$

之形表之焉.

更以 x 表示 0, 1, 2, ……, $p-1$ 中任意之數, 則置換 (12) 乃示 x 得爲 $ax+\beta \pmod{p}$ 所置換者. 故若令

$$(14)\qquad x' \equiv ax+\beta \pmod{p.} \begin{cases} a=1, 2, \cdots\cdots, p-1 \\ \beta=0, 1, 2, \cdots\cdots, p-1 \end{cases}$$

則 x' 表示由 $\{(0, 1, 2, \cdots\cdots, p-1)\}$ 之全形之置換, x 得爲所置換之數. 以故此又爲亞巡回羣之一表示焉. 由 (14) 式以求置換, 先於 a 與以 $1, 2, \cdots\cdots, p-1$ 之一數, 於 β 與以 $0, 1, 2, \cdots\cdots, p-1$ 之一數, 然後令 $x=0, 1, 2, \cdots\cdots, p-1$, 則 x' 得算出之.

---

*此置換中各數皆爲就法 p 而取者, 固不待論.

例.　$p=3$ 時.

α	β	$x'\equiv\alpha x+\beta \pmod 3$	置換
1	0	$x'\equiv x$	$\begin{pmatrix}012\\012\end{pmatrix}=1$
1	1	$x'\equiv x+1$	$\begin{pmatrix}012\\120\end{pmatrix}=(012)$
1	2	$x'\equiv x+2$	$\begin{pmatrix}012\\201\end{pmatrix}=(021)$
2	0	$x'\equiv 2x$	$\begin{pmatrix}012\\021\end{pmatrix}=(12)$
2	1	$x'\equiv 2x+1$	$\begin{pmatrix}012\\102\end{pmatrix}=(01)$
2	2	$x'\equiv 2x+2$	$\begin{pmatrix}012\\210\end{pmatrix}=(20)$

故巡回羣 $\{(012)\}$ 之全形，即三次亞巡回羣爲

$$1,\quad (012),\quad (021),\quad (12),\quad (01),\quad (20).$$

4°. 母元素之關係.

由巡回置換 $(1, \rho, \rho^2, \cdots\cdots, \rho^{p-2})$，則各數(0以外者)得以其乘 ρ 之積(法 p)而置換之者也. 故

$$(1, \rho, \rho^2, \cdots\cdots \rho^{p-2})=\begin{pmatrix}0 & 1 & 2 & \cdots\cdots & p-1\\ 0 & \rho & 2\rho & \cdots\cdots & (p-1)\rho\end{pmatrix}.$$

以此變置換 $(0, 1, 2, \cdots\cdots, p-1)$ 之形，則得

$$\begin{pmatrix}0 & 1 & 2 & \cdots\cdots & p-1\\ 0 & \rho & 2\rho & \cdots\cdots & (p-1)\rho\end{pmatrix}^{-1}(0, 1, 2, \cdots\cdots, p-1)\begin{pmatrix}0 & 1 & 2 & \cdots\cdots & p-1\\ 0 & \rho & 2\rho & \cdots\cdots & (p-1)\rho\end{pmatrix}$$

$$=(0, \rho, 2\rho, \cdots\cdots, (p-1)\rho)=(0, 1, 2, \cdots\cdots p-1)^{\rho}.$$

故若令亞巡回羣(13)[卽(12)]之母元素爲

$$(0, 1, 2, \cdots\cdots, p-1)=S_1,\ (1, \rho, \rho^2, \cdots\cdots, \rho^{p-2})=T_1,$$

則此等得滿足次之條件:

$$(15)\qquad S_1^{\,p}=1,\ T_1^{\,p-1}=1,\ T_1^{-1}S_1T_1=S_1^{\,\rho},$$

但 ρ 爲 p 之原根之一.

101. 一般羣之全形,亞巡回羣之生成的定義.

爲討論一般羣及論其性質之際之便利計,乃將第98節所與之全形之定義稍事擴張. 卽將凡與一羣 $\mathfrak{G}$ 之正置換表示之全形(該節中之意義者)爲單純同態之羣,總稱之曰**羣 $\mathfrak{G}$ 之全形**;特別在 $\mathfrak{G}$ 爲素數元巡回羣時,則其全形名之曰**亞巡回羣**焉.

今於此就亞巡回羣一言. 令二元素 S, T 爲滿足與前節 S_1, T_1 之同一條件卽

$$(1)\qquad S^p=1,\ T^{p-1}=1,\ T^{-1}ST=S^{\rho}\ (\rho \text{ 爲 } p \text{ 之原根})$$

者. 但第一,第二式,乃表示 S 及 T 之巡回率分別爲 p 及 $p-1$; 而 S, T 除滿足此三條件以外不再受任何限制,隨之亦無表示置換之必要者也.

因 ρ 不能以素數 p 整除,故 $\{S^{\rho}\}=\{S\}$. 因之由 (1) 之第三條件,得

$$T^{-1}\{S\}T=\{S\}.$$

故二巡回羣 $\{T\}$, $\{S\}$ 之積成羣. 而因 p 爲素數,故兩巡回羣除主元素外無共通之元素. 是故積 $\{T\}\{S\}$ 之元數爲

$p(p-1)$, 其元數爲

$$(2)\qquad T^iS^j \quad \begin{cases} i=0, 1, 2, \cdots\cdots, p-2 \\ j=0, 1, 2, \cdots\cdots, p-1 \end{cases} \quad (\text{第 27 節參照}).$$

此羣以 $\mathfrak{M}$ 表之, 而前節之亞巡回羣則以 $\mathfrak{M}_1$ 表示. 對 $\mathfrak{M}$ 之元素 T^iS^j, 使 $\mathfrak{M}_1$ 之元素 $T_1{}^iS_1{}^j$ 相與對應, 則兩羣元素間之一一對應成立, 而由 (1) 及前 (15) 之第三條件, 分別乃有

$$(T^iS^j)(T^hS^k)=T^{i+h}S^{j\rho^h+k},$$

$$(T_1{}^iS_1{}^j)(T_1{}^hS_1{}^k)=T_1{}^{i+h}S_1{}^{j\rho^h+k}.*$$

故 $\mathfrak{M}$ 與 $\mathfrak{M}_1$ 爲單純同態. 因之條件 (1), 乃將亞巡回羣, 由母元素, 生成的而定義之者也. 第於此, ρ 雖爲 p 之原根之一, 然此值對於一羣乃非一定者, 若母元素之選擇方法變更, 則亦隨之而變化. 茲示之如下.

以 m 爲與 $p-1$ 互素之數, 則

---

*茲取 (1) 之第三條件

(i)　　$T^{-1}ST=S^{\rho}$.

將兩邊 m 乘, 得

(ii)　　$T^{-1}S^mT=S^{m\rho}$.

次之以 T 將 (i) 之兩邊變形, 則

$$T^{-2}ST^2=T^{-1}S^{\rho}T. \qquad \therefore\ T^{-2}ST^2=S^{\rho^2}.$$

再以 T 將兩邊變形, 得

$$T^{-3}ST^3=T^{-1}S^{\rho^2}T. \qquad \therefore\ T^{-3}ST^3=S^{\rho^3}.$$

反覆行之, 得

(iii)　　$T^{-h}ST^h=S^{\rho^h}$.

將兩邊 j 乘, 得

$$T^{-h}S^jT^h=S^{j\rho^h}, \quad \text{或} \quad S^jT^h=T^hS^{j\rho^h}$$

$$\{T^m\}=\{T\},$$

因之

$$\{T^m\}\{S\}=\{T\}\{S\}.$$

故 S, T^m 亦生成亞巡回羣 $\mathfrak{M}$ 者也. 然

$$T^{-m}\,S\,T^m=S^{\rho^m} \qquad \text{(參照上面脚注)}$$

故若令

$$\rho^m\equiv\sigma \pmod{p},\ T^m=U,$$

則得

$$(3)\qquad S^p=1,\ U^{p-1}=1,\ U^{-1}SU=S^\sigma,$$

是又定 $\mathfrak{M}$ 之義也. 若將 m 之值適當選擇之, 則 σ 得與 p 之原根中之任何個合同(法 p). 換言之, 若 ρ 爲 p 之原根, 則不論其值如何, 條件(1)所定之羣皆爲同態也.

注意. 於條件(1), 若 ρ 非 p 之原根時, 則由之所定義之羣非亞巡回羣, 且亦非其約羣. 但 T 之巡回率不爲 $p-1$, 如爲 d, 如 ρ 以此 d 爲其指數(對於法 p 者)時, 則以

$$S^p=1,\ T^d=1,\ T^{-1}ST=S^\rho$$

所定義之羣, 乃亞巡回羣之約羣焉.

102. 羣之全形之即含其羣者.

在羣 $\mathfrak{G}$ 之全形中而即以 $\mathfrak{G}$ 爲其約羣者可作也. 茲欲示此, 乃採用第98節之記號, 以 $(\mathfrak{G})$ 爲羣 $\mathfrak{G}$ $[G_0(=1), G_1, G_2, \cdots, G_{g-1}]$ 之正置換表示, $(\mathfrak{L})$ 爲 $\mathfrak{G}$ 之同態羣, $(\mathfrak{H})$ 爲 $(\mathfrak{G})$ 之全形[即 $(\mathfrak{L})(\mathfrak{G})$], 而 $(\mathfrak{L})$ 之元數爲 l, 其置換爲

$$(1)\qquad \begin{pmatrix} G_r \\ G_r^{(0)} \end{pmatrix}\cdot \begin{pmatrix} G_r \\ G_r^{(1)} \end{pmatrix}, \cdots\cdots \begin{pmatrix} G_r \\ G_r^{(l-1)} \end{pmatrix} \quad [G_r^{(0)}=G_r].$$

次於$\mathfrak{G}$之元素外，又新取$(l-1)g$個之元素，乃以之與$\mathfrak{G}$之元素合，而就其總數lg個元素論之．以此爲

$$(2)\qquad \begin{cases} F_{00} & F_{10} & \cdots\cdots F_{l-1,\,0} \\ F_{01} & F_{11} & \cdots\cdots F_{l-1,\,1} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ F_{0,\,g-1} & F_{1,\,g-1} & \cdots\cdots F_{l-1,\,g-1} \end{cases}$$

其集合爲$\mathfrak{F}$．但以爲

$$(3)\qquad F_{0i}=G_i\ (i=0,\,1,\,2,\,\cdots\cdots,\,g-1)$$

者．對於$(\mathfrak{F})$之元素$\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$，使$\mathfrak{F}$之元素$F_{ji}$相與對應，而

$$\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\cdot\begin{pmatrix} G_r \\ G_r^{(q)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_p \end{pmatrix}=\begin{pmatrix} G_r \\ G_r^{(u)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_t \end{pmatrix}$$

時，若以

$$F_{ji}\cdot F_{qp}=F_u$$

而定義，則$\mathfrak{F}$之作與$(\mathfrak{F})$爲單純同態之羣，且復含$\mathfrak{G}$明已．即$\mathfrak{F}$者，乃含$\mathfrak{G}$而又爲$\mathfrak{G}$之全形者也．

由上之對應，則$\mathfrak{F}$中之主元素爲F_{00}，而與$(\mathfrak{L})$之元素相對應者爲

$$F_{00},\ F_{10},\ \cdots\cdots,\ F_{l-1,\,0}.$$

今將此分別以

$$(4)\qquad L_0,\ L_1,\ \cdots\cdots,\ L_{l-1}\ (L_0=1)$$

表之，則由(3)式以及

$$\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_0 \end{pmatrix}\cdot\begin{pmatrix} G_r \\ G_r^{(0)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}=\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix},$$

得

$$F_{j0}\cdot F_{0i}=F_{ji},$$

即

$$L_j\,G_i=F_{ji}\quad\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1. \end{cases}$$

因之，若將與(Ω)對應之約羣(4)以Ω表之，則得

$$(5)\qquad \mathfrak{H}=\Omega\mathfrak{G}.$$

更就(Ω)，(𝔊)之元素之關係而觀，如第98節所示，因

$$(6)\quad \begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}=\begin{pmatrix} G_r \\ G_rG_i^{(j)} \end{pmatrix}\quad\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1 \end{cases}$$

之故，對於𝔊之元素之結合，由上所述之定義乃有

$$(7)\qquad L_j^{-1}\,G_i\,L_j=G_i^{(j)}\quad\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1 \end{cases}$$

茲利用此關係，則𝔊之同態羣(Ω)之置換，得換書之如次：

$$(8)\quad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ L_j^{-1}G_0L_j & L_j^{-1}G_1L_j & \cdots\cdots & L_j^{-1}G_{g-1}L_j \end{pmatrix},\quad j=0,1,2,\cdots,l-1.$$

換言之，即𝔊之自己同態者，得以Ω之各元素變𝔊之形而得者也.

夫如是，以Ω之元素變𝔊之形，由之不僅可得𝔊之自己同態之全部，且可知Ω在𝔊與(𝔊)之單純同態關係上，乃爲與(𝔊)之約羣(Ω)相對應者也. 故當討論含𝔊之全形𝔊時，便宜上對於Ω，與以與(Ω)同一之名稱，而呼之曰同態羣；若兩者有區別之必要時，則(Ω)名曰同態置換羣；而與(Ω)之約羣

中內同態羣($\mathfrak{H}$)相對應者，則稱曰內同態羣焉.

在$\mathfrak{H}$中，與$\mathfrak{G}$之各元素爲交換可能者之元素所作之羣，於$\mathfrak{H}$與($\mathfrak{H}$)之同態關係中，乃對應於($\mathfrak{G}$)之接合羣者也. 故此復與上同樣，呼曰$\mathfrak{G}$之接合羣. 茲以$\mathfrak{G}'$記之，則由第98節第四定理系，得

$$\mathfrak{H}=\mathfrak{L}\,\mathfrak{G}'=\mathfrak{G}'\,\mathfrak{L},$$

而$\mathfrak{H}$爲$\mathfrak{G}'$之全形.

此外則對內同態尙有一言. 設J爲$\mathfrak{G}$之內同態羣(以$\mathfrak{H}$表之)之一元素，則在$\mathfrak{H}$與($\mathfrak{H}$)之同態關係上，其與J相對應者，乃內同態置換$\begin{pmatrix} G_r \\ G^{-1}G_rG \end{pmatrix}$也，但G爲$\mathfrak{G}$之一元素. 然由(6)，

$$\begin{pmatrix} G_r \\ G^{-1}G_rG \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\begin{pmatrix} G_r \\ G^{-1}G_rG \end{pmatrix}=\begin{pmatrix} G_r \\ G_r\cdot G^{-1}G_iG \end{pmatrix}$$

$$(i=0,1,2,\cdots\cdots,g-1),$$

故由$\mathfrak{H}$中之結合之定義，則得

$$J^{-1}G_rJ=G^{-1}G_iG\quad(i=0,1,2,\cdots\cdots,g-1).$$

故$\begin{bmatrix} G_r \\ J^{-1}G_rJ \end{bmatrix}$即以示$\mathfrak{G}$之內同態者也. 試更就J與G之關係觀，由上式乃有

$$(JG^{-1})^{-1}G_i(JG^{-1})=G_i\quad(i=0,1,2,\cdots\cdots,g-1),$$

JG^{-1}與$\mathfrak{G}$之各元素爲交換可能，因之即屬於$\mathfrak{G}$之接合羣$\mathfrak{G}'$.

即　　$JG^{-1}=G'$　(G'爲$\mathfrak{G}'$之一元素).

$$\therefore\quad J=G'G=GG'.$$

於是內同態羣$\mathfrak{H}$之元素,乃等於$\mathfrak{G}$之元素與其接合羣之元素之積也. 至其逆之爲眞亦明(參照第97節第三定理).

定理. 若羣$\mathfrak{A}$之各元素雖與羣$\mathfrak{G}$爲交換可能,而$\mathfrak{A}$之元素之中與$\mathfrak{G}$之各元素爲交換可能者僅爲主元素時,則積$\mathfrak{A}\mathfrak{G}$或爲$\mathfrak{G}$之全形,或爲其約羣. 但$\mathfrak{A}$及$\mathfrak{G}$之共通元素僅爲主元素.

證明. 令$\mathfrak{G}$之元素爲$G_0, G_1, \cdots\cdots, G_{g-1}$,$\mathfrak{A}$之元素爲$A_0, A_1, \cdots\cdots, A_{\alpha-1}$. 因$\mathfrak{A}$之元素與$\mathfrak{G}$爲交換可能,故置換

$$(9)\quad \begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ A_j^{-1}G_0A_j & A_j^{-1}G_1A_j & \cdots & A_j^{-1}G_{g-1}A_j \end{pmatrix} (j=0,1,2,\cdots,\alpha-1)$$

爲$\mathfrak{G}$之同態置換. 且此各個皆互異. 蓋若

$$\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix} = \begin{pmatrix} G_r \\ A_i^{-1}G_rA_i \end{pmatrix},$$

則
$$A_j^{-1}G_rA_j = A_i^{-1}G_rA_i \quad (r=0,1,2,\cdots\cdots,g-1),$$

因之
$$(A_jA_i^{-1})^{-1}G_r(A_jA_i^{-1}) = G_r \quad (r=0,1,2,\cdots\cdots,g-1).$$

然由假設,$\mathfrak{A}$之元素中與$\mathfrak{G}$之各元素爲交換可能者僅主元素. 故
$$A_jA_i^{-1}=1.$$
$$\therefore \qquad A_j=A_i.$$

是故置換(9)中相等者不存在也.

次之,$\mathfrak{A}$既爲羣,故α個同態置換(9)之成羣,是無論已. 茲以$(\mathfrak{A})$表之. 乃於積$\mathfrak{A}\mathfrak{G}$之元素A_jG_i,使積$(\mathfrak{A})(\mathfrak{G})$之置換

$\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$ 與之對應，則因兩積之元數共爲 ag，是兩者之元素間，一一對應成立；而由

$$A_jG_i\cdot A_qG_p=(A_jA_q)(A_q^{-1}G_iA_q\cdot G_p)$$

及

$$\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix}\begin{pmatrix} G_i \\ G_rG_i \end{pmatrix}\cdot\begin{pmatrix} G_r \\ A_q^{-1}G_rA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_p \end{pmatrix}$$

$$=\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix}\begin{pmatrix} G_r \\ G_q^{-1}G_rA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rA_q^{-1}G_iA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_p \end{pmatrix}\quad[\text{第(6)式參照}]$$

$$=\begin{pmatrix} G_r \\ (A_jA_q)^{-1}G_r(A_jA_q) \end{pmatrix}\begin{pmatrix} G_r \\ G_r(A_q^{-1}G_iA_q\cdot G_p) \end{pmatrix},$$

則兩積之爲單純同態可知．然如上所記，$(\mathfrak{A})$ 之置換，全部皆爲 $\mathfrak{G}$ 之同態置換，故 $(\mathfrak{A})$ 或爲同態羣，或爲其約羣．因之 $(\mathfrak{A})(\mathfrak{G})$ 或爲 $(\mathfrak{G})$ 之全形或爲其約羣．由是便得本定理．

注意．若用本定理，則前節(1)之定亞巡回羣之義者一見自明．

103．特性約羣．

設 $\mathfrak{H}$ 爲羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之約羣，其元素爲

$$(1)\qquad H_0, H_1, \cdots\cdots, H_{h-1}$$

乃再取前節中所作之 $\mathfrak{G}$ 之全形 $\mathfrak{F}$．在以同態羣 $\mathfrak{L}$ 之元素 L_j 將 $\mathfrak{G}$ 之元素變形所生之自己同態

$$(2)\qquad \begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ L_j^{-1}G_0L_j & L_j^{-1}G_1L_j & \cdots\cdots & L_j^{-1}G_{g-1}L_j \end{bmatrix}$$

中，$\mathfrak{H}$ 之元素(1)乃分別與

$$(3)\qquad L_j^{-1}H_0L_j, L_j^{-1}H_1L_j, \cdots\cdots, L_j^{-1}H_{h-1}L_j$$

對應. 而此諸元素當然成羣. 爰呼之曰在自己同態(2)中與$\mathfrak{H}$對應之約羣. 特別在$\mathfrak{H}$於所有之自己同態中常與其自身對應時,換言之,即在

$$L_j^{-1}\mathfrak{H}L_j=\mathfrak{H}\quad(j=0,1,2,\cdots\cdots,l-1)$$

時,則$\mathfrak{H}$名曰$\mathfrak{G}$之特性約羣焉.

今以F爲全形$\mathfrak{F}$之任意之元素,則因

$$\mathfrak{F}=\mathfrak{G}'\mathfrak{L}\quad(\mathfrak{G}'\text{爲}\mathfrak{G}\text{之接合羣}),$$

故

$$F=G'L,$$

但G'爲$\mathfrak{G}'$之元素,L爲$\mathfrak{L}$之元素. 故

$$F^{-1}\mathfrak{H}F=(G'L)^{-1}\mathfrak{H}(G'L)$$

$$=L^{-1}G'^{-1}\mathfrak{H}G'L=L^{-1}\mathfrak{H}L.$$

因之在$\mathfrak{F}$中與$\mathfrak{G}$之約羣$\mathfrak{H}$共軛者,乃於$\mathfrak{G}$之自己同態之一中與$\mathfrak{H}$對應之約羣也. 特別若約羣$\mathfrak{H}$於$\mathfrak{G}$爲特性的時,則

$$L^{-1}\mathfrak{H}L=\mathfrak{H},$$

因之

$$F^{-1}\mathfrak{H}F=\mathfrak{H}.$$

故$\mathfrak{H}$於$\mathfrak{F}$爲正常. 反之,若$\mathfrak{H}$於$\mathfrak{F}$爲正常,則此之爲$\mathfrak{G}$之特性約羣甚明. 爰得

定理. 一羣$\mathfrak{G}$之特性約羣,爲$\mathfrak{G}$之全形(含$\mathfrak{G}$者)之正常約羣. 反之,$\mathfrak{G}$之全形之正常約羣中,其含於$\mathfrak{G}$者,於$\mathfrak{G}$爲特性的.

系. 羣之除主元素羣外無特性約羣者,或爲單羣,或爲單純同態之單羣之直乘積.

證明. 由定理,羣之無特性約羣者,乃於其全形中爲極小正常者也. 故由第52節第二定理,遂得本系.

特性約羣之例. (i) 中核. 因在一羣之自己同態中其與自己共軛元素對應者,仍爲自己共軛故.

(ii) 換位羣. 在自己同態中,與二元素A, B對應者,分別爲A′, B′時,則對A及B之換位元素$B^{-1}A^{-1}BA$,乃有$B'^{-1}A'^{-1}B'A'$相與對應,而後者爲A′, B′之換位元素. 是卽換位元素互相對應也. 故由之所生成之羣爲特性的.

(iii) 若一羣之Sylow氏約羣爲正常,則此約羣爲特性的. 蓋因此時,同元數之約羣,由Sylow氏定理只有唯一個故. 如在p次亞巡回羣中,其p元約羣爲特性的也.

104. 特性約羣列.

羣$\mathfrak{G}$之特性約羣之列

$$(1)\qquad \mathfrak{G}, \mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots, \mathfrak{C}_{\mu-1}, 1,$$

若適合次之二條件時,則名曰$\mathfrak{G}$之**特性約羣列**.

(i) 各羣均含於其先一羣內.

(ii) 含於一項$\mathfrak{C}_{i-1}$而又含其次項$\mathfrak{C}_i$之特性約羣($\mathfrak{G}$的)除$\mathfrak{C}_{i-1}$及$\mathfrak{C}_i$以外不復存在.

元來$\mathfrak{G}$之特性約羣,在$\mathfrak{G}$之全形$\mathfrak{H}$中爲正常的. 故上之羣列(1)中,含於$\mathfrak{C}_{i-1}$而又含$\mathfrak{C}_i$之$\mathfrak{G}$之特性約羣,卽$\mathfrak{H}$之正常約羣乃不存在. 是故得作含羣列(1)者之

$$(2)\qquad \mathfrak{H}, \mathfrak{H}_1, \cdots\cdots, \mathfrak{H}_\lambda, \mathfrak{G}, \mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots, \mathfrak{C}_{\mu-1}, 1$$

以爲$\mathfrak{F}$之主組成列也. 若於(1)之外, 尙有$\mathfrak{G}$之特性約羣列

(3) $\mathfrak{G}, \mathfrak{C}_1', \mathfrak{C}_2', \cdots\cdots, \mathfrak{C}'_{\nu-1}, 1$

存在時, 乃與前同樣, 作$\mathfrak{F}$之主組成列

(4) $\mathfrak{F}, \mathfrak{F}_1, \cdots\cdots, \mathfrak{F}_\lambda, \mathfrak{G}, \mathfrak{C}_1', \mathfrak{C}_2', \cdots\cdots, \mathfrak{C}'_{\nu-1}, 1,$

則由此兩主組成列所導出之商羣列

(5) $\frac{\mathfrak{F}}{\mathfrak{F}_1}, \frac{\mathfrak{F}_1}{\mathfrak{F}_2}, \cdots\cdots, \frac{\mathfrak{F}_\lambda}{\mathfrak{G}}, \frac{\mathfrak{G}}{\mathfrak{C}_1}, \frac{\mathfrak{C}_1}{\mathfrak{C}_2}, \cdots\cdots,$

(6) $\frac{\mathfrak{F}}{\mathfrak{F}_1}, \frac{\mathfrak{F}_1}{\mathfrak{F}_2}, \cdots\cdots, \frac{\mathfrak{F}_\lambda}{\mathfrak{G}}, \frac{\mathfrak{G}}{\mathfrak{C}_1'}, \frac{\mathfrak{C}_1'}{\mathfrak{C}_2'}, \cdots\cdots,$

由第51節定理, 爲一致也. 故由羣列(1)及(3)所導出之商羣列

(7) $\frac{\mathfrak{G}}{\mathfrak{C}_1}, \frac{\mathfrak{C}_1}{\mathfrak{C}_2}, \cdots\cdots,$

(8) $\frac{\mathfrak{G}}{\mathfrak{C}_1'}, \frac{\mathfrak{C}_1'}{\mathfrak{C}_2'}, \cdots\cdots$

一致.* 又由第53節定理, (5), (6)之各項, 或爲單羣, 或則與互爲單純同態之單羣之直乘積等. 因之就商羣列(7), (8)言, 亦復同樣. 爰得次

定理. 由特性約羣列所導出之商羣列, 不問特性約羣之選擇方法如何, 常爲一定. 但商羣列中各項之順序, 則在所不論.

---

*一致之意義, 與第51節中者同樣.

105. 全羣.

若一羣除主元素外,無有自己共軛元素,而其自己同態又皆爲內的時,則其羣曰**全羣**.

如亞巡回羣

(1)　$S^p=1,\ T^{p-1}=1,\ T^{-1}ST=S^\rho$ (ρ 爲 p 之原根)

乃全羣也,示如下.

今以 $\mathfrak{M}$ 表此羣. 乃先取 $\mathfrak{M}$ 之一元素

$$T^jS^i\ (0\leqq i\leqq p-1,\ 0\leqq j\leqq p-2),$$

而以 S 及 T 變其形,則由(1)之第三條件,得

$$S^{-1}\cdot T^jS^i\cdot S=T^jS^{-\rho^j}S^iS=T^jS^{1+i-\rho^j},$$

$$T^{-1}\cdot T^jS^i\cdot T=T^{-1}T^jTS^{i\rho}=T^jS^{i\rho}$$

(參照第101節中之腳注). 故此元素若欲與 S 及 T 二者爲交換可能,則須

$$1+i-\rho^j\equiv i \text{ 卽 } \rho^j\equiv 1\ (\mathrm{mod.}\ p)$$

及

$$i\rho\equiv i\ (\mathrm{mod.}\ p)$$

也. 然 ρ 乃 p 之原根,因之 $\rho\not\equiv 1\ (\mathrm{mod.}\ p)$. 故

$$j\equiv 0\ (\mathrm{mod.}\ p-1),\ i\equiv 0\ (\mathrm{mod.}\ p),$$

隨之

$$T^jS^i=1.$$

是故 $\mathfrak{M}$ 中之自己共軛元素僅爲主元素.

次之 p 元巡回約羣 $\{S\}$,如前節之例所示,在 $\mathfrak{M}$ 中爲特性的. 故於 $\mathfrak{M}$ 之自己同態中,其與 S 相對應者乃 S 之冪也. 今以 S^λ $(0<\lambda<p)$ 爲對應於 S,而 $T^\beta S^\alpha$ $(0\leqq\alpha\leqq p-1,$

$0\leqq\beta\leqq p-2$) 爲對應於 T 者. 於是與 $T^{-1}ST$ 相對應者爲

$$(2)\qquad (T^{\beta}S^{\alpha})^{-1}(S^{\lambda})(T^{\beta}S^{\alpha})=S^{-\alpha}\cdot T^{-\beta}S^{\lambda}T^{\beta}\cdot S^{\alpha}$$

$$=S^{-\alpha}S^{\lambda\rho^{\beta}}S^{\alpha}=S^{\lambda\rho^{\beta}}$$

(參照第 101 節中之腳注). 然此, 由 (1) 之第三條件, 得與 S^{ρ} 對應.

故 $$S^{\rho^{\beta}}=S^{\rho}$$

爲必要. 因之

$$\lambda\rho^{\beta}\equiv\lambda\rho \pmod{p}.$$

$$\therefore\quad \rho^{\beta}\equiv\rho \pmod{p} \qquad [\because\ \lambda\not\equiv 0 \pmod{p}].$$

$$\therefore\quad \beta\equiv 1 \pmod{p-1} \qquad [\rho \text{ 爲 } p \text{ 之原根故}].$$

$$\therefore\quad \beta=1 \qquad [\because\ 0\leqq\beta\leqq p-2].$$

故在此自己同態中, 其得與 T 對應者爲 TS. 於是在此時, 由 (2) 式, 乃得

$$(TS^{\alpha})^{-1}(S^{\lambda})(TS^{\alpha})=(S^{\lambda})^{\rho}.$$

再就 TS^{α} 之巡回率而觀, 由 (1) 之第三條件,

$$(TS^{\alpha})^{2}=TS^{\alpha}TS^{\alpha}=TTS^{\alpha\rho}S^{\alpha}=T^{2}S^{\alpha(\rho+1)}$$

$$(TS^{\alpha})^{3}=T^{2}S^{\alpha(\rho+1)}TS^{\alpha}=T^{2}TS^{\alpha(\rho+1)\rho}S^{\alpha}=T^{3}S^{\alpha(\rho^{2}+\rho+1)}$$

$$\cdots\cdots\cdots\cdots\qquad \cdots\cdots\cdots\cdots$$

$$(TS^{\alpha})^{m}=\cdots\cdots=T^{m}S^{\alpha(\rho^{m-1}+\rho^{m-2}+\cdots+\rho+1)}=T^{m}S^{\alpha\frac{\rho^{m}-1}{\rho-1}}.$$

故 m 爲 $p-1$ 之倍數時, 且唯此時

$$(TS^{\alpha})^{m}=1.$$

是卽 TS^{α} 之巡回率爲 $p-1$ 也.

於是在 $\mathfrak{M}$ 中使 S^{λ} $(0<\lambda<p)$ 與 S 對應, TS^{α} $(0\leqq\alpha\leqq p-1)$ 與 T 對應, 則以

$$(3)\qquad (S^{\lambda})^{p}=1,\ (TS^{\alpha})^{p-1}=1,\ (TS^{\alpha})^{-1}(S^{\lambda})(TS^{\alpha})=(S^{\lambda})^{\rho}$$

之故, 便生自己同態

$$(4)\qquad \begin{bmatrix} S & \cdots\cdots & T & \cdots\cdots \\ S^{\lambda} & \cdots\cdots & TS^{\alpha} & \cdots\cdots \end{bmatrix}$$

(參照第 101 節). 於此而令

$$\lambda=1,2,\cdots\cdots,p-1;\quad \alpha=0,1,\cdots\cdots,p-1,$$

則得 $p(p-1)$ 種之自己同態. 此卽 $\mathfrak{M}$ 中自己同態之全部也.

欲示此等同態概爲內的, 則只示能滿足

$$(T^{y}S^{x})^{-1}S(T^{y}S^{x})=S^{\lambda},\quad (T^{y}S^{x})^{-1}T(T^{y}S^{x})=TS^{\alpha}$$

者之元素 $T^{y}S^{x}$ 或二整數 x,y 克以求得便足. 茲計算其左邊, 乃有

$$(T^{y}S^{x})^{-1}S(T^{y}S^{x})=S^{-x}\cdot T^{-y}ST^{y}\cdot S^{x}=S^{-x}S^{\rho^{y}}S^{x}=S^{\rho^{y}}$$

$$(T^{y}S^{x})^{-1}T(T^{y}S^{x})=S^{-x}T^{-y}TT^{y}S^{x}=S^{-x}TS^{x}=TS^{x(1-\rho)}.$$

但 ρ 爲 p 之原根. 故 $\rho\not\equiv 1\ (\mathrm{mod}.\ p)$, 因之適合

$$x(1-\rho)\equiv\alpha\ (\mathrm{mod}.\ p)$$

者之數 x 存在, 而滿足

$$\rho^{y}\equiv\lambda\ (\mathrm{mod}.\ p)$$

之數 y 亦能求得者也.

夫如是, 亞巡回羣之自己同態皆爲內的, 且其自己共

輒元素僅爲主元素. 故亞巡回羣爲全羣也.

特別$p=3$時,亞巡回羣爲三次對稱羣,此之不容有外同態,則於第96節已示之矣.

106. 定理. 全羣$\mathfrak{G}$之全形,乃$\mathfrak{G}$與其接合羣之直乘積. 反之,在羣之除主元素外無有自己共輒元素者之羣中,若其全形與$\mathfrak{G}$及他羣之直乘積相等時,則$\mathfrak{G}$爲全羣.

證明. 令羣$\mathfrak{G}$爲全羣. 因$\mathfrak{G}$不容有外同態,故其全形與內同態羣及羣之積等. 然此積,由第97節第三定理,乃等於$\mathfrak{G}$與其接合羣之積. 而$\mathfrak{G}$則除主元素外無有自己共輒元素. 故$\mathfrak{G}$與其接合羣無共有元素(主元素以外). 因之$\mathfrak{G}$之全形乃$\mathfrak{G}$與其接合羣之直乘積.

反之,設羣$\mathfrak{G}$無自己共輒元素,其全形$\mathfrak{H}$爲羣$\overline{\mathfrak{G}}$與$\mathfrak{G}$之直乘積. 於是如第102節所述,$\mathfrak{G}$之自己同態,統可以$\mathfrak{H}$之元素將其元素變形而得. 今以$\mathfrak{H}$之任意一元素$\overline{G}G$($\overline{G}$, G分別爲$\overline{\mathfrak{G}}$, $\mathfrak{G}$之元素)將$\mathfrak{G}$之元素G_r ($r=0, 1, 2, \cdots\cdots, g-1$)變形,則有

$$(\overline{G}G)^{-1}G_r(\overline{G}G)=G^{-1}\overline{G}^{-1}G_r\overline{G}G=G^{-1}G_rG$$

$$(r=0, 1, 2, \cdots\cdots, g-1)$$

(由假設$\overline{\mathfrak{G}}$之各元素與$\mathfrak{G}$之各元素爲交換可能故). 故以$\overline{G}G$變$\mathfrak{G}$之形其所生之自己同態,爲

$$\begin{bmatrix} G_r \\ (\overline{G}G)^{-1}G_r(\overline{G}G) \end{bmatrix}=\begin{bmatrix} G_r \\ G^{-1}G_rG \end{bmatrix},$$

是卽皆爲內的也. 因此$\mathfrak{G}$爲全羣.

定理. 一羣$\mathfrak{A}$有全羣$\mathfrak{G}$爲其正常約羣時,則$\mathfrak{A}$與$\mathfrak{G}$及他羣之直乘積等.

證明. 在$\mathfrak{A}$中,其元素之與$\mathfrak{G}$各元素爲交換可能者之集合,以$\mathfrak{B}$表之,則$\mathfrak{B}$爲$\mathfrak{A}$之約羣明已. 且$\mathfrak{G}$爲全羣,故$\mathfrak{B}$與$\mathfrak{G}$除主元素外無共通之元素. 再次則$\mathfrak{G}$既於$\mathfrak{A}$爲正常,故以$\mathfrak{A}$之任意元素A將$\mathfrak{G}$之元素$G_0, G_1, \cdots\cdots, G_{g-1}$變形,乃得$\mathfrak{G}$之自己同態$\begin{bmatrix} G_r \\ A^{-1}G_rA \end{bmatrix}$. 然$\mathfrak{G}$不容外同態. 故

$$\begin{bmatrix} G_r \\ A^{-1}G_rA \end{bmatrix} = \begin{bmatrix} G_r \\ G^{-1}G_rG \end{bmatrix},$$

式中G爲$\mathfrak{G}$之或一元素. 由是

$$A^{-1}G_rA = G^{-1}G_rG \quad (r=0, 1, 2, \cdots\cdots, g-1).$$

$$\therefore \quad (AG^{-1})^{-1}G_r(AG^{-1}) = G_r \quad (r=0, 1, 2, \cdots\cdots, g-1),$$

卽AG^{-1}與$\mathfrak{G}$之各元素爲交換可能也. 故AG^{-1}不得不屬於$\mathfrak{B}$. 卽

$$AG^{-1} = B \quad (B\text{爲}\mathfrak{B}\text{之一元素}).$$

$$\therefore \quad A = BG.$$

故$\mathfrak{A}$含於積$\mathfrak{B}\mathfrak{G}$. 反之,積$\mathfrak{B}\mathfrak{G}$當然含於$\mathfrak{A}$. 因之

$$\mathfrak{A} = \mathfrak{B}\mathfrak{G}.$$

而如上述,$\mathfrak{B}$, $\mathfrak{G}$兩羣之元素既相互交換可能,且兩者無共通元素(1以外者). 故定理云云.

107. 與傍系置換表示交換可能者之置換.

設 $\mathfrak{G}$ 爲 g 元羣,其元素爲

(1) $\qquad G_0, G_1, \cdots\cdots, G_{g-1} \quad (G_0=1);$

又 $\mathfrak{H}$ 爲 $\mathfrak{G}$ 之約羣,而

(2) $\qquad \mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1+\cdots\cdots+\mathfrak{H}P_{n-1};$

且 $\mathfrak{H}$ 爲不含 $\mathfrak{G}$ 之正常約羣者(主元素羣以外者). 於是關於 $\mathfrak{H}$ 之傍系置換表示

(3) $\qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{n-1}G_i \end{pmatrix}, \quad i=0, 1, 2, \cdots\cdots, g-1$

乃與 $\mathfrak{G}$ 爲單純同態. (此 g 個置換之爲互異,參照第 75 節.) 今將此表示以 $((\mathfrak{G}))$ 記之,更就傍系

(4) $\qquad \mathfrak{H}, \mathfrak{H}P_1, \cdots\cdots, \mathfrak{H}P_{n-1}$

上所行置換之中,求其與 $((\mathfrak{G}))$ 爲交換可能者. 此諸所求之置換之成羣明已. 乃以 $((\Omega))$ 示之. $((\Omega))$ 之含 $((\mathfrak{G}))$ 乃當然也,因之就傍系 (4) 言爲可遷的. 於 $((\Omega))$ 其令 $\mathfrak{H}$ 不動者之約羣以爲 $((\mathfrak{N}))$, 則由第 63 節第四定理,得

(5) $\qquad ((\Omega))=((\mathfrak{N}))((\mathfrak{G})).$

故若 $((\mathfrak{N}))$ 得知,則 $((\Omega))$ 之置換自明.

茲試取 $((\mathfrak{N}))$ 之任意置換

(6) $\qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1} \\ (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \end{pmatrix}.$

但 $(\mathfrak{H})'=\mathfrak{H}$. 乃以此將表示 (3) 之一置換 $\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}$ 變形,則得

$$(7)\qquad \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_rG_i \\ (\mathfrak{H}P_rG_i)' \end{pmatrix}$$

$$= \begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H}G_i)' & (\mathfrak{H}P_1G_i)' & \cdots\cdots & (\mathfrak{H}P_{n-1}G_i)' \end{pmatrix},$$

但$(\mathfrak{H}P_rG_i)'$乃示傍系(4)中由置換(6)$\mathfrak{H}P_rG_i$得爲所置換者. 然由假設置換(6)與$((\mathfrak{G}))$爲交換可能. 故上式右邊之置換不得不屬於$((\mathfrak{G}))$. 卽

$$(8)\qquad \begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H}G_i)' & (\mathfrak{H}P_1G_i)' & \cdots\cdots & (\mathfrak{H}P_{n-1}G_i)' \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_r & \cdots\cdots & \mathfrak{H}P_{n-1} \\ \mathfrak{H}G_{i'} & \mathfrak{H}P_1G_{i'} & \cdots\cdots & \mathfrak{H}P_{n-1}G_{i'} \end{pmatrix},$$

但$G_{i'}$爲$\mathfrak{G}$之一元素. 故由(7),

$$(9)\qquad \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} = \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r\mathfrak{G}_{i'} \end{pmatrix}.$$

於此而令

$$i=0, 1, 2, \cdots\cdots, g-1,$$

則與右邊之置換相應,得g個之元素

$$(10)\qquad G_0', G_1', \cdots\cdots, G'_{g-1}.$$

且此諸元素互異. 蓋若假定

$$G_{i'}=G_{j'} \quad (i\neq j),$$

則由(9),

$$\begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} = \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix},$$

$$\therefore \quad \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} = \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix},$$

是則與表示(3)中 g 個置換互異之事實相反,爲不合理. 夫如是(10)之元素既互異,則其不外乎(1)之元素換列於某順序者可知. 故

$$(11) \qquad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0' & G_1' & \cdots\cdots & G_{g-1}' \end{pmatrix}$$

乃表示 $\mathfrak{G}$ 之元素間之置換者也. 於此有須留意者,則爲 G_i 與 G_i' 之關係由(9)而定之一點是. 更就此置換而觀,因

$$\begin{aligned} &\begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r\cdot G_iG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} \\ &= \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} \\ &= \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} \cdot \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} \\ &= \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i' \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j' \end{pmatrix} \qquad [\text{由 (9) 式}] \\ &= \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r\cdot G_i'G_j' \end{pmatrix}, \end{aligned}$$

故積 G_iG_j 得以 $G_i'G_j'$ (卽 G_i,G_j 各個所置換者之積) 置換. 是故(11)爲同態置換也.

次就(6),(11)兩置換之關係而討論之,由(8),

$$\begin{aligned} &\begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H}G_i) & (\mathfrak{H}P_1G_i)' & \cdots\cdots & (\mathfrak{H}P_{n-1}G_i)' \end{pmatrix} \\ &= \begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H})'G_i & (\mathfrak{H}P_1)'G_i' & \cdots\cdots & (\mathfrak{H}P_{n-1})'G_i' \end{pmatrix}, \end{aligned}$$

故

$$(12)\qquad (\mathfrak{H}G_i)'=(\mathfrak{H})'G_i'=\mathfrak{H}G_i' \quad [\because\ (\mathfrak{H})'=\mathfrak{H}].$$

因之

$$(\mathfrak{H}P_r)'=\mathfrak{H}P_r' \quad (r=1,2,\cdots\cdots,n-1),$$

但 P_r' 乃示置換(11)中與 P_r 相對應者. 由是, 置換(6)得換書如次:

$$(6')\qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1} \\ \mathfrak{H} & \mathfrak{H}P_1' & \cdots\cdots & \mathfrak{H}P_{n-1}' \end{pmatrix}.$$

又於(11)中其與 $\mathfrak{H}$ 之元素 H 相對應者以爲 H', 則由(12), 得

$$\mathfrak{H}H'=(\mathfrak{H}H)'=(\mathfrak{H})'=\mathfrak{H}.$$

故 H' 亦屬於 $\mathfrak{H}$. 卽謂由置換(11), $\mathfrak{H}$ 之元素只於其自身間移動也. 而傍系 $\mathfrak{H}P_r$ 之元素, 則由(11)得以 $\mathfrak{H}P_r'$ 之元素置換之焉.

要之, 在與表示(3)爲交換可能之置換中, 其令 $\mathfrak{H}$ 不動者之(6)卽(6'), 乃將傍系 $\mathfrak{H}, \mathfrak{H}P_1, \cdots\cdots, \mathfrak{H}P_{n-1}$, 以同態置換(11)中之與是等相對應之傍系而置換之者也. 但在同態(11)中, 約羣 $\mathfrak{H}$ 乃與其自身對應.

再就其逆而論之, 乃以(11)爲表 $\mathfrak{G}$ 之同態置換, 而於其中則 $\mathfrak{H}$ 爲與其自身對應者. 於是由自己同態之定義, 對於傍系 $\mathfrak{H}G_i$, 其相對應者之爲 $\mathfrak{H}G_i'$ 甚明. 故若以 $P_1', P_2', \cdots\cdots, P_{n-1}'$ 爲分別與 $P_1, P_2, \cdots\cdots, P_{n-1}$ 相對應者, 則得

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1'+\cdots\cdots+\mathfrak{H}P_{n-1}',$$

(6')遂表傍系之置換. 而

$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}^{-1}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}^{-1}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_rG_i\\ \mathfrak{H}(P_rG_i)'\end{pmatrix}\quad\begin{bmatrix}(P_rG_i)'\text{乃於(11)中與積}\\ P_rG_i\text{相對應者.}\end{bmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}P_r'\\ \mathfrak{H}(P_rG_i)'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_{r'}\\ \mathfrak{H}P_{r'}G_i'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_s\\ \mathfrak{H}P_sG_i'\end{pmatrix},$$

即是此結果屬於(3)也. 故(6′)與表示(3)爲交換可能.

且羣之自己同態得以同態羣之元素將其羣變形而得(第102節). 故由上述正反兩方面,得次定理以作其結論.

定理. 若羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之約羣$\mathfrak{H}$不含$\mathfrak{G}$之正常約羣時(主元素羣以外者),則在與傍系置換之關於$\mathfrak{H}$者

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1}\\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{n-1}G_i\end{pmatrix}\quad(i=0, 1, 2, \cdots\cdots, g-1)$$

得以交換之置換(在關於$\mathfrak{H}$之傍系上所施行者)中,其不使$\mathfrak{H}$動者爲

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1}\\ \mathfrak{H} & \mathfrak{H}R^{-1}P_1R & \cdots\cdots & \mathfrak{H}R^{-1}P_{n-1}R\end{pmatrix},$$

且僅得爲此,但R爲$\mathfrak{G}$之同態羣(第102節之意義下者)中與$\mathfrak{H}$爲交換可能者.

系. 在$\mathfrak{G}$之同態羣中,以$\mathfrak{H}$之正常化羣爲$\mathfrak{N}$,其元素爲$R_0, R_1, \cdots\cdots$,則$((\mathfrak{N}))$得以

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1}\\ \mathfrak{H} & \mathfrak{H}R_j^{-1}P_1R_j & \cdots\cdots & \mathfrak{H}R_j^{-1}P_{n-1}R_j\end{pmatrix}\quad(j=0, 1, 2, \cdots\cdots)$$

與之. 但$((\mathfrak{R}))$乃有第(5)式中之意義者.

108. 置換表示之同值.

與前節同樣, 將羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$就約羣$\mathfrak{H}$分爲傍系, 以之爲

$$(1)\qquad \mathfrak{G}=\mathfrak{H}+\mathfrak{H}P_1+\cdots\cdots+\mathfrak{H}P_{n-1},$$

而作關於$\mathfrak{H}$之傍系置換表示

$$(2)\quad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{n-1}G_i \end{pmatrix} \quad (i=0, 1, 2, \cdots\cdots, g-1).$$

復次以$\mathfrak{G}$之同態羣$\mathfrak{L}$(在第102節之意義下者)之任意之元素L將$\mathfrak{G}$變形, 則由(1)得

$$(3)\qquad \mathfrak{G}=\mathfrak{H}'+\mathfrak{H}'P'_1+\cdots\cdots+\mathfrak{H}'P'_{n-1},$$

但　　$\mathfrak{H}'=L^{-1}\mathfrak{H}L,\ P_r'=L^{-1}P_rL \quad (r=1, 2, \cdots\cdots, n-1);$

而關於$\mathfrak{H}'$之傍系置換表示, 則得以

$$(4)\quad \begin{pmatrix} \mathfrak{H}' & \mathfrak{H}'P'_1 & \cdots\cdots & \mathfrak{H}'P'_{n-1} \\ \mathfrak{H}'G_i' & \mathfrak{H}'P'_1G_i' & \cdots\cdots & \mathfrak{H}'P'_{n-1}G_i' \end{pmatrix} \quad (i=0, 1, 2, \cdots\cdots, g-1)$$

與之. 但$G_i'=L^{-1}G_iL\ (i=0, 1, 2, \cdots\cdots, g-1).$

試就兩表示(2)及(4)而觀, 若

$$\mathfrak{H}P_rG_i=\mathfrak{H}P_s \quad (P_0=1),$$

則
$$\mathfrak{H}'P_r'G_i'=L^{-1}\mathfrak{H}L\cdot L^{-1}P_rL\cdot L^{-1}G_iL=L^{-1}\mathfrak{H}P_rG_iL$$
$$=L^{-1}\mathfrak{H}P_sL=L^{-1}HL\cdot L^{-1}P_sL=\mathfrak{H}'P'_s.$$

故表示(4), 得在(2)之置換中將傍系$\mathfrak{H}, \mathfrak{H}P_1, \cdots\cdots, \mathfrak{H}P_{n-1}$分別代以$\mathfrak{H}'P'_1, \cdots\cdots, \mathfrak{H}'P'_{n-1}$而得也. 又自他面觀, $\mathfrak{G}$中$\mathfrak{H}$之共

軛約羣,乃得以$\mathfrak{L}$之元素將此變形而得(參照第103節). 因是得次

定理. 若羣$\mathfrak{G}$之兩約羣$\mathfrak{H}$及$\mathfrak{H}'$,於$\mathfrak{G}$之全形(含$\mathfrak{G}$者)中爲共軛,則關於此兩約羣之$\mathfrak{G}$之傍系置換表示爲同值.

互爲同值之置換表示若視爲同一,則由第76節定理(可遷羣得視爲傍系置換表示者)直得次

系. 一羣$\mathfrak{G}$之可遷置換表示之數,不多於在$\mathfrak{G}$之全形中之共軛約羣系內屬於$\mathfrak{G}$之約羣之共軛系之數.

上定理之逆未見其必成立. 以故本系中表示之數,較共軛約羣系(屬於$\mathfrak{G}$之約羣者)之數少者亦有之焉. 如在由二巡回置換

$$P=(012\cdots\cdots 8),\quad Q=(abc)$$

所生成之27元羣$\{P, Q\}$中,其關於9元約羣$\{P\}$之傍系置換表示以及關於他之9元約羣$\{P^3, Q\}$之傍系置換表示,共爲三傍系之巡回羣. 因之兩者爲同值. 然$\{P\}$雖爲九元巡回羣,而$\{P^3, Q\}$則否. (因後者不含巡回率9之置換故.) 故兩約羣不得爲共軛. 是則對於$\{P, Q\}$,定理之逆不成立也. 但於上,若$\mathfrak{H}$不含$\mathfrak{G}$之正常約羣(主元素羣以外者)時,因之即其關於$\mathfrak{H}$之傍系置換表示與$\mathfrak{G}$爲單純同態時(第75節定理),則如次所證,其逆定理亦成立焉.

令$\overline{\mathfrak{H}}$爲$\mathfrak{G}$之約羣,而

$$(5)\qquad \mathfrak{G}=\overline{\mathfrak{H}}+\overline{\mathfrak{H}}\,\overline{P}_1+\cdots\cdots+\overline{\mathfrak{H}}\,\overline{P}_{n-1},$$

其關於$\mathfrak{H}$之$\mathfrak{G}$之傍系置換表示

$$(6)\quad \begin{pmatrix} \overline{\mathfrak{H}} & \overline{\mathfrak{H}}\overline{P}_1 & \cdots\cdots & \overline{\mathfrak{H}}\overline{P}_{n-1} \\ \overline{\mathfrak{H}}G_i & \overline{\mathfrak{H}}\overline{P}_1G_i & \cdots\cdots & \overline{\mathfrak{H}}\overline{P}_{n-1}G_i \end{pmatrix} \quad (i=0,\ 1,\ 2,\ \cdots\cdots,\ g-1),$$

則爲與表示(2)爲同值,即於置換$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}$中,將傍系$\mathfrak{H}$, $\mathfrak{H}P_1$, ……, $\mathfrak{H}P_{n-1}$代以$\overline{\mathfrak{H}}$, $\overline{\mathfrak{H}}\overline{P}_1$, ……, $\overline{\mathfrak{H}}\overline{P}_{n-1}$遂成$\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_i \end{pmatrix}$者. 但$G_0$, G_1, ……, G_{g-1}則爲將G_0, G_1, ……, G_{g-1}自某順序而取之者焉.

茲於表示(2)及(6),分別作其兩個置換之積,乃有

$$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix}=\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_iG_j \end{pmatrix},$$

$$\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_i \end{pmatrix}\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_j \end{pmatrix}=\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_iG_j \end{pmatrix}.$$

然由關於兩表示之同值之假設,使$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}$與$\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_i \end{pmatrix}$對應,則兩表示爲單純同態.故

$$(7)\qquad G_iG_j=G_k.$$

以故若

$$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_iG_j \end{pmatrix}=\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_k \end{pmatrix},$$

則由上式,

$$\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_iG_j \end{pmatrix}=\begin{pmatrix} \overline{\mathfrak{H}}\overline{P}_r \\ \overline{\mathfrak{H}}\overline{P}_rG_k \end{pmatrix}.$$

因之　　$\overline{\mathfrak{H}}\overline{P}_rG_iG_j=\overline{\mathfrak{H}}\overline{P}_rG_k \quad (r=0,\ 1,\ 2,\ \cdots\cdots,\ n-1)$

爲必要也.由是得

$$\overline{P}_r\overline{G}_i\overline{G}_j=\overline{H}_r\overline{P}_r\overline{G}_k \quad (r=0, 1, 2, \cdots\cdots, n-1).$$

但 $\overline{H}_r$ 爲 $\overline{\mathfrak{H}}$ 之元素. 復由此得

$$\overline{G}_i\overline{G}_j=\overline{P}_r^{-1}\overline{H}_r\overline{P}_r\overline{G}_k \quad (r=0, 1, 2, \cdots\cdots, n-1).$$

故

$$\overline{G}_i\overline{G}_j=\overline{D}\overline{G}_k. \tag{8}$$

式中 $\overline{D}$ 爲共軛約羣

$$\overline{\mathfrak{H}}, \overline{P}_1^{-1}\overline{\mathfrak{H}}\overline{P}_1, \cdots\cdots, \overline{P}_{n-1}^{-1}\overline{\mathfrak{H}}\overline{P}_{n-1} \tag{9}$$

全部共通之元素.

今假設 $\mathfrak{H}$ 爲不含有 $\mathfrak{G}$ 之正常約羣. 於是 $\mathfrak{G}$ 之關於 $\mathfrak{H}$ 之傍系置換表示, 因之與其關於 $\overline{\mathfrak{H}}$ 者爲單純同態也. 故共軛約羣(9)之最大公約羣須爲主元素羣. 因之於(8)則有 $\overline{D}=1$, 遂得

$$\overline{G}_i\overline{G}_j=\overline{G}_k.$$

由此式與(7)式而觀, 可

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0 & G_1 & \cdots\cdots & G_{g-1} \end{bmatrix} \tag{10}$$

爲表 $\mathfrak{G}$ 之自己同態可知. 在此同態中, 以與 $\mathfrak{H}$ 之元素 H_0, H_1, ……, H_{h-1} 相對應者分別爲 $\overline{H}_0$, $\overline{H}_1$, ……, $\overline{H}_{h-1}$, 則後者之集合爲 $\overline{\mathfrak{H}}$ 也. 此何故歟?

蓋在表示(2)中, 置換

$$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rH_j \end{pmatrix}, \quad j=0, 1, 2, \cdots\cdots, h-1$$

乃不使 $\mathfrak{H}$ 動者. 故由關於兩表示(2), (6)之同值之假設, 則

與此各個對應之置換

$$\left(\frac{\overline{\mathfrak{H}}\overline{P}_r}{\overline{\mathfrak{H}}\overline{P}_r\overline{H}_j}\right),\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1$$

亦不使 $\overline{\mathfrak{H}}$ 動也. 是則

$$\overline{\mathfrak{H}}\,\overline{H}_j=\overline{\mathfrak{H}},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1$$

爲必要矣. 以故 $\overline{H}_j$ $(j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1)$ 均屬於 $\overline{\mathfrak{H}}$. 而 $\mathfrak{H}$ 與 $\overline{\mathfrak{H}}$ 爲同元數 $\left(h=\frac{g}{n}\right)$.

故

$$\overline{\mathfrak{H}}=H_0+H_1+\cdots\cdots+H_{h-1}.$$

因之由第103節 $\overline{\mathfrak{H}}$ 在 $\mathfrak{G}$ 之全形中與 $\mathfrak{H}$ 爲共軛焉. 爰得

定理. 若羣 $\mathfrak{G}$ 之關於約羣 $\mathfrak{H}$ 之傍系置換表示與其關於他之約羣 $\mathfrak{H}'$ 者爲同值, 且 $\mathfrak{H}$ 不含 $\mathfrak{G}$ 之正常約羣(主元素羣以外者)時, 則兩約羣 $\mathfrak{H}$, $\mathfrak{H}'$ 於 $\mathfrak{G}$ 之全形(含 $\mathfrak{G}$ 者)中爲共軛.

系. 羣 $\mathfrak{G}$ 之可遷置換表示中, 其與 $\mathfrak{G}$ 爲單純同態者之數乃與在 $\mathfrak{G}$ 之全形內之共軛約羣系中其不含 $\mathfrak{G}$ 之正常約羣者之約羣($\mathfrak{G}$ 的)所屬共軛系之數相等.