大學叢書

羣論

著造正圓
譯絳君蕭

商務印書館發行

大學叢書

羣論

著造正圓
譯絳君蕭

商務印書館發行

中華民國二十三年五月初版

（一〇二七四）

大學叢書（教本）羣論一冊

每冊定價大洋伍元

外埠酌加運費匯費

原著者 圓正造

譯述者 蕭君絳 上海河南路

發行人 王雲五 上海河南路

印刷所 商務印書館 上海河南路

發行所 商務印書館 上海及各埠

（本書校對者胡達聰）

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, 雖尙有擴張之餘地, 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. 此雖爲 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, 是爲區區之徵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

第二篇　置換羣

第十章　可遷羣

第十一章　非遷羣

第十二章 羣之置換表示

第十三章 可遷羣之本原性及非原性

第十四章 可遷約羣與羣之可遷重複度

第十五章 與可遷羣之各置換交換可能者之置換

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

第四篇 特殊羣

第二十一章 Abel 氏羣

第二十二章 素數冪元羣之型,四元數

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

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 α 爲 β 所置換, $a_1, a_2, \cdots\cdots, a_{n-1}$ 爲 $\beta_1, \beta_2, \cdots, \beta_{n-1}$ 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 $\alpha, \alpha_1, \alpha_2, \cdots\cdots, \alpha_{n-1}$ 上所行之兩置換.由 T, 文字 β 爲 γ' 所置換, $\beta_1, \beta_2, \cdots, \beta_{n-1}$ 爲 $\gamma'_1, \gamma'_2, \cdots\cdots \gamma'_{n-1}$ 所置換時,則 T 可換書如次:

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

茲 n 個文字

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

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

$$P=\begin{pmatrix}\alpha & \alpha_1 & \cdots\cdots & \alpha_{n-1}\\ \gamma' & \gamma'_1 & \cdots\cdots & \gamma'_{n-1}\end{pmatrix}$$

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

$$\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a & a_1 & \cdots\cdots & a_{n-1} \end{pmatrix}=1$$

是也.今取任意一置換

$$S=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}.$$

此時

$$1\cdot S=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a & a_1 & \cdots\cdots & a_{n-1} \end{pmatrix}\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots & \beta_{n-1} \end{pmatrix}=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}=S.$$

又

$$S\cdot 1=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a & a_1 & \cdots\cdots & a_{n-1} \end{pmatrix}$$

$$=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}\begin{pmatrix} \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}=S$$

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

$$S=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ \beta & \beta_1 & \cdots\cdots & \beta_{n-1} \end{pmatrix}.$$

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

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

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

是即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 $a, a_1, \cdots\cdots, a_{n-1}$ 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

$$SX=1$$

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,羃及其逆.

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 乘羃.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 乘羃 $(S^{-1})^m$,以 S^{-m} 表示之,則 S^{-m} 者,遂成爲 S^m 之逆置換矣.卽

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

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

$$\begin{pmatrix} a & a_1 & a_2 & \cdots\cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \cdots\cdots & a_{n-1} & a \end{pmatrix}$$

而觀,則見 a 爲 a_1, a_1 爲 a_2, ……, a_{n-2} 爲 a_{n-1} 所置換,而最後 a_{n-1} 爲 a 所置換者也.此置換名曰在 n 個文字.

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

上所施行之**巡回置換**,而以

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

表示之焉.

巡回置換

$$\begin{pmatrix} a & a_1 & a_2 & \cdots\cdots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \cdots\cdots & a_{n-1} & a \end{pmatrix}$$

又可換書之如

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{n-1} & a \\ a_2 & a_3 & \cdots\cdots & a & a_1 \end{pmatrix},\ \cdots\cdots,\ \begin{pmatrix} a_{n-1} & a & \cdots\cdots & a_{n-3} & a_{n-2} \\ a & a_1 & \cdots\cdots & a_{n-2} & a_{n-1} \end{pmatrix}$$

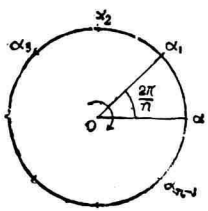
也,故依上之記法,則

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

$$(a_{n-1}\ a \cdots\ a_{n-3}\ a_{n-2})$$

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 a, a_1, a_2, …… a_{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 a_1, a_2, ……, a_{n-1}, a, 各自來到 a, a_1, ……, a_{n-2}, a_{n-1} 始初所占之位置,爰產生一巡回置換 $(a\ a_1 \cdots\cdots\ a_{n-2}\ a_{n-1})$ 焉.



6. 巡回置換之積.

茲有兩個巡回置換

$$(a\ a_1 \cdots\cdots\ a_{n-2}\ a_{n-1}),\ (a'\ a'_1\ \cdots\ a'_{m-2}\ a'_{m-1});$$

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

$$(a\ a_1\ \cdots\cdots\ a_{n-1})=\begin{pmatrix}a & a_1 & \cdots\cdots & a_{n-1}\\ a_1 & a_2 & \cdots\cdots & a\end{pmatrix},$$

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

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,卽可視爲

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

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

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

卽以是定兩巡回置換 (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

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

請表示之爲巡回置換之積,而示其方法焉.今於 α, α_1, ……, α_{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, ……, s 而所與之 n 個文字 α, α_1, ……, α_{n-1} 爲能盡時,則

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

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

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

故由第 6 節末所述,

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

若以 $p, q, r, \cdots, s, p', q', \cdots\cdots, s'$ 尚不能盡所與之 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

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

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

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

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

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

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

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

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_r-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 $(\alpha_r\ \alpha_s)$,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,$(\alpha_r-\alpha_k)$, $(\alpha_k-\alpha_s)$,由轉換 $(\alpha_r\ \alpha_s)$ 各別變爲

$$\alpha_s-\alpha_k=-(\alpha_k-\alpha_s),\ \alpha_k-\alpha_r=-(\alpha_r-\alpha_k),$$

因之兩者之積不變也.故凡屬於(4)因數之積,亦由轉換 $(\alpha_r\ \alpha_s)$ 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 α_r, α_s 之兩個或僅含其一者之積,由轉換 $(\alpha_r\ \alpha_s)$,只變其符號已也.至若 Δ 中不含 α_r, α_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 $(\alpha_r\ \alpha_s)$,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.

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

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

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

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

$$1^2=1.$$

一般,若於 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 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, $a_1, \cdots\cdots, a_{n-1}$ 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, $a_1, \cdots\cdots, a_{n-1}$ 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卽對稱羣者而思之,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

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

此諸置換之爲奇數置換也明甚.且彼此互異.蓋若(2)中,$S_i(a\ a_1)=S_j(aa_1)$,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.卽

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

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

$$g+g=n!,$$

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

卽謂 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

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

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,

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

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

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

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$(b\,c\,d)$,乘以$(a\,b)$,則成爲$(a\,b\,c\,d)$,此由形式上觀,乃由$(b\,c\,d)$與$(a\,b)$兩置換而想定$(a\,b\,c\,d)$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$(a\,b)$於$(b\,c\,d)$者,兩者之結合也;其積$(a\,b\,c\,d)$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,再加該節所擧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𝔊,若滿足次之四條件時,則𝔊曰羣

(i) 𝔊之任意兩元素(相等者或不等者)之積仍屬於𝔊.

(ii) 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𝔊之何元素以爲元素A,而常有

$$AE=A$$

之關係之元素E,𝔊之中至少有一個.

(iv) 對於𝔊之一元素A而滿足

$$AX=E$$

之元素X,存在於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).

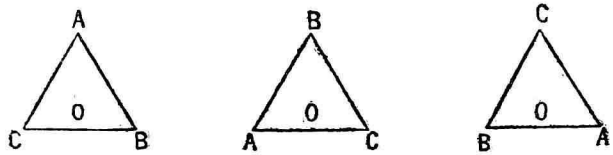
若干元素相集以成羣,若其互異元素之數爲有限,則此名曰**有限羣**,若其數爲無限,則曰**無限羣**,有限羣中,其互異元素之總數,名曰羣之**元數**,而元數g之羣,則曰g元之羣或g元羣焉.

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

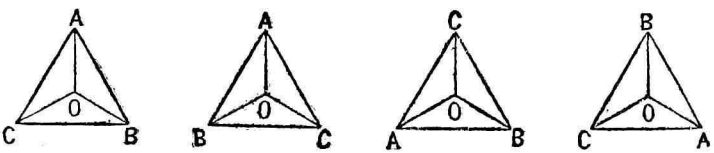
者(與時鐘之指針成反對方向行之).



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.

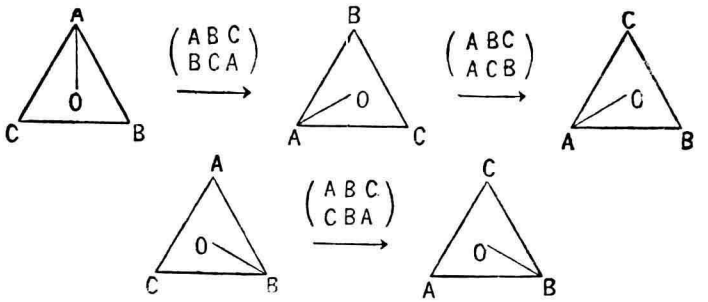
(ii) 在固定於三角形之三軸 OA, OB, OC 之周,作 180° 之迴轉者.

以 OA 爲軸作 180° 之迴轉,則頂點 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.

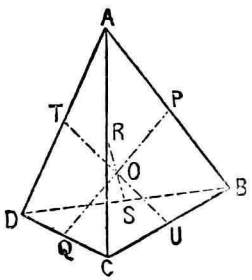
注意. 由上之運動,頂點A,B,C乃爲他之頂點所置換.故此運動者,正以示三文字A,B,C間之置換;而運動之記

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:

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

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

(ii) 以 PQ, RS, TU 爲軸之 180° 之三迴轉:

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

(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$\mathfrak{G}$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

(1)　$$EA=B.$$

由第15節羣之成立條件(iv),則滿足

(2)　$$AX=E$$

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,

(3)　$$BX=AX.$$

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. 茲以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.即若A爲一元素,

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

則又有

$$XA=E$$

也.換言之,即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,卽以A^{-1}表之.

證明. 以A爲一元素,及

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

則
$$X(AX')=XE,$$

卽
$$(XA)X'=XE.$$

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.即:

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

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

$$1 \qquad (abc) \qquad (acb)$$

$$(de) \qquad (abc)(de) \quad (acb)(de),$$

由實際計算,卽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

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

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

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

因之

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

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,則尙需一言之說明.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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

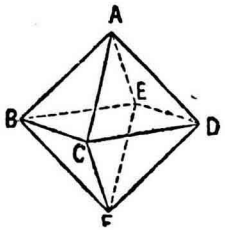
今於此而令左右對立之置換相對應,則對於左欄兩置換之積,右欄相應兩置換之積便與之對應也.如

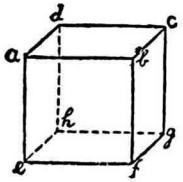
$$\begin{pmatrix} A & B & C & D & E & F \\ A & C & D & E & B & F \end{pmatrix}\begin{pmatrix} A & B & C & D & E & F \\ B & C & A & E & F & D \end{pmatrix} = \begin{pmatrix} A & B & C & D & E & F \\ B & A & E & F & C & D \end{pmatrix},$$

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

故此兩羣爲同態.

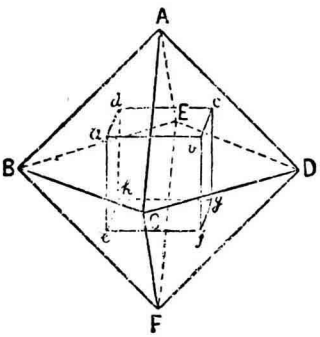
又關於此兩羣,尙欲一言.今取正八面體 ABCDEF 而就其在運動之前後仍占同一空間之運動討論之,若其相等不等以及結合之定義,與論正四面體者同樣,則是等運動相集乃成羣也.且各運動之表示,若仍照第17節之方法,是卽以左欄中所記之置換而克示;而右欄則同樣視爲表示立方體 $abcd-efgh$ 之運動羣者可.





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

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

乃於此之各個以$\mathfrak{G}$之元素A右乘之,則其所得h個之積

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

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

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

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

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

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

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

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

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.

26. 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

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

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

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:

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

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

$$\cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots$$

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

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

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

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 $\mathfrak{K}$ 爲交換可能,故 $H^{-1}K^{-1}H$ 屬於 $\mathfrak{K}$, 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 $\mathfrak{K}$ 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

$$HK=KH.$$

卽 $\mathfrak{H}$ 之各元素與 $\mathfrak{K}$ 之各元素爲交換可能也故云云.

於兩約羣 $\mathfrak{H}$ 及 $\mathfrak{K}$, 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 $\mathfrak{H}\mathfrak{K}$ 名曰 $\mathfrak{H}$ 及 $\mathfrak{K}$ 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,卽適合於

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

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

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

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

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

.....

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

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　$G^{-1}A^aG=1$,

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

$\therefore$　$A^a=1$.

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

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

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 $\mathfrak{H}$ 也.茲令

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

則

$$P_i=KP_j,$$

此卽謂 P_i 得屬於傍系 $\mathfrak{H}P_j$ 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 $\mathfrak{H}$ 於 $\mathfrak{G}$ 之指數.故與 A 共軛元素之數乃與 $\mathfrak{H}$ 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^sQ^t 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.

如是者之由 $\mathfrak{G}$ 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

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

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$\mathfrak{K}$,則$\mathfrak{K}$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$\mathfrak{K}$,而就$\mathfrak{K}$將$\mathfrak{G}$分爲傍系,

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

以傍系$\mathfrak{K}P_i$之任意之元素K_sP_i(K_s爲$\mathfrak{K}$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

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

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

故

$$P_i=KP_j.$$

是卽示 P_i 屬於傍系 $\mathfrak{R}P_j$ 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 $\mathfrak{R}$, 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

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

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

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

即　　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 $\mathfrak{H}$ 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.

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

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

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

卽 $\mathfrak{D}$ 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

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

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,卽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$(\neq 1)$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$(\neq 1)$.

---

* 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,如元數等於素數之冪者(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

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

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$\mathfrak{H}S_2\mathfrak{K}$,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

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

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

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

如是,$\mathfrak{G}$之元素,乃於屬於$\mathfrak{H}$及$\mathfrak{K}$之若干重傍系而得分類也.此之謂將$\mathfrak{G}$就$\mathfrak{H}$及$\mathfrak{K}$**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24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 $A\equiv B$, $B\equiv C$, 則 $A\equiv C$.

(II) 若 $A\equiv B$, $A'\equiv B'$, 則 $AA'\equiv BB'$.

(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 $\mathfrak{G}$ 之元素中,其與主元素合同者之全體,作成 $\mathfrak{G}$ 之正常約羣 $\mathfrak{N}$.

(ii) 就 $\mathfrak{N}$ 言,其屬於同一傍系之元素,互爲合同.

(iii) 互爲合同之元素,就 $\mathfrak{N}$ 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

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

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 $N(\equiv 1)$ 變形,則由(I, i),

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

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

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

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,皆與 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 $\frac{\mathfrak{H}}{\mathfrak{L}}$ 爲同態.但 $\mathfrak{L}$ 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

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

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 $\mathfrak{R}$ 之元素，乃由假設而知 $H^{-1}LH$ 屬於 $\mathfrak{R}$；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 $\mathfrak{R}$ 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 $\frac{\mathfrak{H}\mathfrak{R}}{\mathfrak{R}}$, $\frac{\mathfrak{H}}{\mathfrak{L}}$ 之爲同態.試以

(1)　　A, B, C, ……

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

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

是卽謂 AB^{-1} 非屬於 $\mathfrak{R}$ 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 $\mathfrak{H}$, $\mathfrak{R}$ 之所共通，因之卽必屬於 $\mathfrak{L}$，卽

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

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

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 $\mathfrak{R}$ 爲非合同.

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

(2)　　$HK\equiv H \pmod{\mathfrak{R}}$

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 $\mathfrak{R}$ 之約羣，故若以 H 爲屬於 $\mathfrak{H}\mathfrak{R}$，則 H 便與(1)之一元素合同(法 $\mathfrak{R}$).因之由(2)，HK 乃與(1)之一元素合同(法 $\mathfrak{R}$).

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

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

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

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

更使兩羣之元素對應,對於$\frac{\mathfrak{H}}{\mathfrak{L}}$之A, B, C, ……,分別以$\frac{\mathfrak{H}\mathfrak{K}}{\mathfrak{K}}$之A, B, C,…對應之,若$AB\equiv C \pmod{\mathfrak{L}}$, 則$AB\equiv C \pmod{\mathfrak{K}}$ (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$\frac{\mathfrak{H}\mathfrak{K}}{\mathfrak{K}}$之二元素之積對應也.因之$\frac{\mathfrak{H}}{\mathfrak{L}}$與$\frac{\mathfrak{H}\mathfrak{K}}{\mathfrak{K}}$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)　　$T_1, T_2, \cdots\cdots, T_{\mathfrak{R}}$

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$T_1, T_2, \cdots\cdots, T_{\mathfrak{R}}$,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(即(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,便產生不屬於(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,其所生之羣卽商 $\mathfrak{G}/\mathfrak{N}$ 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$\mathfrak{A}$)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),

$$G^{m-1}\sim G'^{m-1},$$

$$\therefore\qquad G^{-1}\sim G'^{-1}$$

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:

$$\mathfrak{G}=\mathfrak{N}Q_0+\mathfrak{N}Q_1+\cdots\cdots+\mathfrak{N}Q_{\mu-1}, \tag{1}$$

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

$$\mathfrak{N}'Q_0',\mathfrak{N}'Q_1',\cdots\cdots\mathfrak{N}'Q'_{\mu-1}, \tag{2}$$

則得

$$\mathfrak{G}'=\mathfrak{N}'Q_0'+\mathfrak{N}'Q_1'+\cdots\cdots+\mathfrak{N}'Q'_{\mu-1} \tag{3}$$

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.即若 $Q_iQ_j\equiv Q_k\pmod{\mathfrak{N}}$,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$\mathfrak{E}/\mathfrak{N}$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$\mathfrak{E}/\mathfrak{N}$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

$$G'^{-1}A'G',\quad G'^{-1}B'G',\quad G'^{-1}C'G', \cdots$$

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

$$\mathfrak{G}:\begin{cases} 1,\ (abc),\ (acb), \\ (bc),\ (ca),\ (ab), \\ (de),\ (abc)(de),\ (acb)(de), \\ (bc)(de),\ (ca)(de),\ (ab)(de), \end{cases};$$

$$\mathfrak{G}':\begin{cases} 1,\ (ABC),\ (ACB), \\ (BC),\ (CA)\quad (AB) \end{cases}$$

對於$\mathfrak{G}'$之主元素,以$\mathfrak{G}$之正常約羣

$$\mathfrak{N}:\quad 1,\ (de)$$

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 $G'^{-1}H'G'$, 卽將 $\mathfrak{H}'$ 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)　$\mathfrak{H}=\mathfrak{N}S_0+\mathfrak{N}S_1+\cdots\cdots\cdots+\mathfrak{N}S_{e-1}$,

(2)　$\mathfrak{H}'=\mathfrak{N}'S_0'+\mathfrak{N}'S_1'+\cdots\cdots\cdots+\mathfrak{N}'S_e'_{-1}$,

而　(3)　$\mathfrak{G}=\mathfrak{H}P_0+\mathfrak{H}P_1+\cdots\cdots\cdots+\mathfrak{H}P_{\nu-1}$,

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)　$\mathfrak{G}'=\mathfrak{H}'P_0'+\mathfrak{H}'P_1'+\cdots\cdots+\mathfrak{H}'P'_{\nu-1}$

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$P_0', P_1', \cdots, P'_{\nu-1}$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 $\mathfrak{L}_{i+l}$ 爲不含於 $\mathfrak{H}$ 者之最初一個,乃作其積 $\mathfrak{H}\mathfrak{L}_{i+l}$. 於是以 $\mathfrak{L}_{i+l}$ 於 $\mathfrak{G}$ 爲正常之故,$\mathfrak{H}\mathfrak{L}_{i+l}$ 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^{m_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 Γ，則與 Γ 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，$\mathfrak{Q}$ 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 $\mathfrak{Q}$ 表之，則得

$$\mathfrak{R}=\mathfrak{Q}+\mathfrak{Q}(def)+\mathfrak{Q}(dfe)$$

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}(def)+\mathfrak{H}(dfe).$$

由是則有

$$\mathfrak{R}/\mathfrak{Q}:\quad 1,\quad (def),\quad (dfe)\quad (\mathrm{mod}.\ \mathfrak{Q}),$$

$$\mathfrak{G}/\mathfrak{H}:\quad 1,\quad (def),\quad (dfe)\quad (\mathrm{mod}.\ \mathfrak{H}).$$

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.

$$(2)\qquad \frac{\mathfrak{G}}{\mathfrak{G}_1},\quad \frac{\mathfrak{G}_1}{\mathfrak{G}_2},\quad \cdots\cdots,\quad \frac{\mathfrak{G}_{\nu-1}}{1}\quad \left(\frac{\mathfrak{G}_{\nu-1}}{1}=\mathfrak{G}_{\nu-1}\right)$$

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

$$g,\ g_1,\ g_2,\ \cdots\cdots\ g_{\nu-1},\ 1,$$

則商羣列(2)之各項之元數分別爲

$$(3)\qquad \frac{g}{g_1},\ \frac{g_1}{g_2},\ \cdots\cdots,\ \frac{g_{\nu-1}}{1}.$$

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

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

$\mathfrak{W}$ 爲 $\mathfrak{B}$ 之正常約羣

$$1,\ (ab)(cd).$$

於是　　$\mathfrak{S},\ \mathfrak{A},\ \mathfrak{B},\ \mathfrak{W},\ 1$

爲對稱羣 $\mathfrak{S}$ 之組成列. 而其商羣列爲

$$\frac{\mathfrak{S}}{\mathfrak{A}},\ \frac{\mathfrak{A}}{\mathfrak{B}},\ \frac{\mathfrak{B}}{\mathfrak{W}},\ \frac{\mathfrak{W}}{1},$$

但　　$\frac{\mathfrak{S}}{\mathfrak{A}}$:　1, (ab) (mod. $\mathfrak{A}$),

$\frac{\mathfrak{A}}{\mathfrak{B}}$:　1, (bcd), (bdc) (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

$$\mathfrak{G},\ 1,$$

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) $\mathfrak{G},\ \mathfrak{G}_1,\ 1,$

(10) $\mathfrak{G},\ \mathfrak{G}_1',\ \mathfrak{G}_2',\ \cdots\cdots$

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) $\mathfrak{G},\ \mathfrak{G}_1',\ 1,$

而由(9)及(11)以作商羣列,則得

(12) $\dfrac{\mathfrak{G}}{\mathfrak{G}_1},\ \dfrac{\mathfrak{G}_1}{1},$

(13) $\dfrac{\mathfrak{G}}{\mathfrak{G}_1'},\ \dfrac{\mathfrak{G}_1'}{1}.$

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) $\mathfrak{G}$, $\mathfrak{H}_1$, 1

(b) $\mathfrak{G}$, $\mathfrak{H}_1'$, $\mathfrak{H}_2'$, ...

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) $\mathfrak{G}$, $\mathfrak{H}_1'$, 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 $\mathfrak{R}$ 爲羣 $\mathfrak{G}$ 之正常約羣. 若 $\mathfrak{G}$ 除 $\mathfrak{R}$ 及主元素羣以外,無有含於 $\mathfrak{R}$ 之正常約羣時,則 $\mathfrak{R}$ 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$\mathfrak{H}$爲羣$\mathfrak{G}$之極小正常約羣, 則$\mathfrak{G}$之正常約羣$\mathfrak{N}$, 或含$\mathfrak{H}$, 或僅與$\mathfrak{H}$有主元素公共. 而以後者論, 則此時$\mathfrak{N}$之各元素與$\mathfrak{H}$之各元素爲交換可能.

證明. $\mathfrak{G}$之二正常約羣$\mathfrak{H}$及$\mathfrak{N}$之最大公約羣, 在$\mathfrak{G}$中乃正常也. 但$\mathfrak{H}$爲極小. 故$\mathfrak{H}$及$\mathfrak{N}$之公約羣, 或爲$\mathfrak{H}$自身, 或則爲主元素羣, 是爲必要.

復次, 既$\mathfrak{H}$, $\mathfrak{N}$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$\mathfrak{H}$爲$\mathfrak{G}$之極小正常約羣.$\mathfrak{H}$不爲單羣時,則以$\mathfrak{L}$爲$\mathfrak{H}$之極小正常約羣之一,而以

$$(1) \qquad \mathfrak{L}, \mathfrak{L}_1, \cdots\cdots, \mathfrak{L}_{e-1}$$

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$\mathfrak{H}$之極小正常約羣.蓋若

$$Q_i^{-1}\mathfrak{L}Q_i=\mathfrak{L}_i \quad (Q_i \text{爲} \mathfrak{G} \text{之元素}),$$

則於兩羣$\mathfrak{H}$及$Q_i^{-1}\mathfrak{H}Q_i$,以$Q_i^{-1}\mathfrak{H}Q_i$之元素$Q_i^{-1}KQ_i$使與$\mathfrak{H}$之元素K對應,於是兩羣之單純同態關係便告成立,而$\mathfrak{H}$之約羣$\mathfrak{L}$與$Q_i^{-1}\mathfrak{H}Q_i$之約羣$Q_i^{-1}\mathfrak{L}Q_i$對應.但$\mathfrak{L}$爲$\mathfrak{H}$之極小正常約羣.故$Q_i^{-1}\mathfrak{L}Q_i$於$Q_i^{-1}\mathfrak{H}Q_i$不得不爲極小正常也.然由假設,$\mathfrak{H}$於$\mathfrak{G}$爲正常,因之$Q_i^{-1}\mathfrak{H}Q_i=\mathfrak{H}$.故$Q_i^{-1}\mathfrak{L}Q_i$卽$\mathfrak{L}_i$乃$\mathfrak{H}$之極小正常約羣也.

次之,因(1)之各羣既均於$\mathfrak{H}$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$\mathfrak{L}$及$\mathfrak{L}_1$之直乘積$\mathfrak{L}\mathfrak{L}_1$,而以$\mathfrak{G}$之任意元素G變其形,乃有

$$G^{-1}\mathfrak{L}\mathfrak{L}_1G=G^{-1}\mathfrak{L}G\cdot G^{-1}\mathfrak{L}_1G$$

卽與$\mathfrak{L}$之共軛約羣之積等也.於是若積$\mathfrak{L}\mathfrak{L}_1$含有與$\mathfrak{L}$共軛之所有之約羣時,則$G^{-1}\mathfrak{L}\mathfrak{L}_1G$非含於$\mathfrak{L}\mathfrak{L}_1$不可,因之$\mathfrak{L}\mathfrak{L}_1$爲

---

*因$\mathfrak{H}$爲$\mathfrak{G}$之極小正常約羣,故$\mathfrak{L}$於$\mathfrak{G}$非正常.因之$\mathfrak{L}$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($\neq$),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 $\frac{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_s}{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{s-1}}$ 與 $\frac{\mathfrak{Q}_s}{1}\left(=\mathfrak{Q}_s\right)$ 爲單純同態. 然 $\mathfrak{Q}_s$ 乃單羣. 故 $\frac{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_s}{\mathfrak{Q}\mathfrak{Q}_1 \cdots\cdots \mathfrak{Q}_{s-1}}$ 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)　$\mathfrak{H}_{i-1},\ \mathfrak{G}_{i-1,1},\ \mathfrak{G}_{i-1,2},\ \cdots\cdots,\ \mathfrak{G}_{i-1,s},\ \mathfrak{H}_i$

以作商羣列

(4)　$\frac{\mathfrak{H}_{i-1}}{\mathfrak{H}_i},\ \frac{\mathfrak{G}_{i-1,1}}{\mathfrak{H}_i},\ \frac{\mathfrak{G}_{i-1,2}}{\mathfrak{H}_i},\ \cdots\cdots,\ \frac{\mathfrak{G}_{i-1,s}}{\mathfrak{H}_i},\ 1$

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)　$\frac{\mathfrak{H}_{i-1}}{\mathfrak{G}_{i-1,1}},\ \frac{\mathfrak{G}_{i-1,1}}{\mathfrak{G}_{i-1,2}},\ \cdots\cdots,\ \frac{\mathfrak{G}_{i-1,s}}{\mathfrak{H}_i}.$

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 $g=p^\alpha m$ $(m \not\equiv o \pmod{p})$. 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

$$\mathfrak{C},\ \mathfrak{C}_1,\ \cdots\cdots,\ \mathfrak{C}_{l-1},$$

其各個所屬元素之數分別爲

$$c,\ c_1,\ \cdots\cdots,\ c_{t-1}.$$

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$\mathfrak{N}'$，則$\mathfrak{N}'$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$\mathfrak{N}'$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

$$(6) \qquad m=p^{\alpha-\gamma_0}+p^{\alpha-\gamma_1}+p^{\alpha-\gamma_2}+\cdots\cdots$$

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 $\mathfrak{K}$, 而其元數爲 $p^\alpha m'$ (參照第 33 節).

$m'=m$ 時, 則 $\mathfrak{K}=\mathfrak{G}$, 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 $\mathfrak{K}$ 分爲重傍系:

$$(7) \qquad \mathfrak{G}=\mathfrak{K}T_0\mathfrak{H}+\mathfrak{K}T_1\mathfrak{H}+\mathfrak{K}T_2\mathfrak{H}+\cdots\cdots \quad (T_0=1).$$

因 $\mathfrak{H}$ 之元數爲 p^α, 故 $T_i^{-1}\mathfrak{K}T_i$ 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

$$\frac{g}{p^{\alpha}m'} = p^{\alpha-\delta_0}+p^{\alpha-\delta_1}+p^{\alpha-\delta_2}+\cdots\cdots \tag{8}$$

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 $\mathfrak{N}$ 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})成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

$$[S_1^{-1}\mathfrak{H}S_1, \mathfrak{L}]=\mathfrak{L},$$

卽謂 $\mathfrak{L}$ 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:

$$(3) \quad \{A\},\ \{AB\},\ \{AB^2\},\ \cdots\cdots,\ \{AB^{p-1}\},\ \{B\}.$$

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$\mathfrak{H}$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$\mathfrak{H}$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$\mathfrak{H}$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$\mathfrak{H}$中p元約羣之總數爲

$$r_1=n_1+p^\tau+p^{\tau'}+\cdots\cdots\equiv 1 \pmod{p}.$$

4°. $\mathfrak{L}$爲p^β元約羣$(\beta<\alpha-1)$時, 則含$\mathfrak{L}$之$p^{\beta+1}$元約羣之數, 對法p乃與1合同.

茲以含$\mathfrak{L}$之$p^{\beta+1}$元約羣之任意一個爲$\mathfrak{M}$以與$\mathfrak{L}$成交換可能之$\mathfrak{H}$之元素所作之羣爲$\mathfrak{C}$. 因$\mathfrak{L}$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$\mathfrak{L}$者之$p^{\beta+1}$元約羣皆含於$\mathfrak{C}$.

自他方面觀,$\mathfrak{C}$之元數爲$p^{\beta+\delta}(\delta\geqq 1)$(第47節第二定理). 因之商$\mathfrak{C}/\mathfrak{Q}$之元數爲$p^{\delta}$. 故由3°, $\mathfrak{C}/\mathfrak{Q}$乃含有$1+xp$個之$p$元約羣在. 然$\mathfrak{C}$與$\mathfrak{C}/\mathfrak{Q}$爲$p^{\beta}$重同態. 故$\mathfrak{C}$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°. $\qquad r_{\beta}\equiv 1\ (\mathrm{mod.}\ p).\quad (\beta\leqq\alpha-1).$

茲以

(4) $\qquad \mathfrak{Q}_1, \mathfrak{Q}_2, \cdots\cdots, \mathfrak{Q}_{r_\beta}$

爲$\mathfrak{H}$中p^{β}元約羣之全數$(\beta<\alpha-1)$;

(5) $\qquad \mathfrak{M}_1, \mathfrak{M}_2, \cdots\cdots, \mathfrak{M}_{r_{\beta+1}}$

爲$\mathfrak{H}$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) $\qquad l_1+l_2+\cdots\cdots+l_{r_\beta}=m_1+m_2+m_{r_{\beta+1}}$

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)　　$\mathfrak{L}, \mathfrak{L}_1, \cdots\cdots, \mathfrak{L}_{n-1}$

爲 p^{β} 元約羣 $(\beta<\alpha)$ 之全數.

由 Sylow 氏定理系 2, 則 $\mathfrak{L}$ 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 $\mathfrak{L}$ 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 $\mathfrak{L}$ 之最大公約羣爲 $\mathfrak{D}$, 及其元數爲 p^{δ} $(\delta<\beta)$. 由是, $\mathfrak{L}$ 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 $\mathfrak{L}$ 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} 爲高冪之羣, 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 $\mathfrak{L}$ 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 $\mathfrak{L}$ 之元素) 屬於第一組, 卽含有 $\mathfrak{L}$, 則 $L(L^{-1}\mathfrak{H}_tL)L^{-1}=\mathfrak{H}_t$ 亦含 $\mathfrak{L}$, 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 $\mathfrak{L}$ 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，屬於第二組者尙存在時，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.

又自他而觀，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°，$r_\beta\equiv 1 \pmod{p}$. 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 $\mathfrak{N}$ 之元數爲 $p^\alpha q$ 或 p^α. 以前者論, 則 $\mathfrak{N}=\mathfrak{G}$, 而 $\mathfrak{H}$ 爲正常; 以後者論, 則 $\mathfrak{N}=\mathfrak{H}$, 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.

共軛$\mathfrak{D}$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

$$1,\quad Q,\quad Q^2,\ \cdots\cdots,\ Q^{q-1}.$$

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

$$(2)\qquad \mathfrak{H},\quad Q^{-1}\mathfrak{H}Q,\ \cdots\cdots,\ Q^{-q+1}\mathfrak{H}Q^{q-1}.$$

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. 吾人只須示 $p^{\alpha}q$ 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:

$$\mathfrak{H}: \quad 1, \ (ad)(be)(cf), \ (bf)(ce), \ (ad)(bc)(ef);$$

$$P^{-1}\mathfrak{H}P: \quad 1, \ (ad)(be)(cf), \ (ca)(df), \ (be)(cd)(fa);$$

$$P^{-2}\mathfrak{H}P^2: \quad 1, \ (ad)(be)(cf), \ (db)(ea), \ (cf)(de)(ab).$$

斯三者含有公約羣

$$1, \ (ad)(be)(cf),$$

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$\mathfrak{H}$分成傍系而以之爲

$$\mathfrak{G}=\mathfrak{H}Q_0+\mathfrak{H}Q_1+\cdots\cdots+\mathfrak{H}Q_{a''b''-1}\quad Q_0=1),$$

則$\mathfrak{P}$所屬之共軛約羣系爲

(1) $Q_0^{-1}\mathfrak{P}Q_0(=\mathfrak{P}),\quad Q_1^{-1}\mathfrak{P}Q_1,\cdots\cdots,\quad Q_{a''b''-1}^{-1}\mathfrak{P}Q_{a''b''-1}.$

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) $Q_0^{-1}\mathfrak{H}Q_0(=\mathfrak{H}),\quad Q_1^{-1}\mathfrak{H}Q_1,\cdots\cdots,\quad Q_{a''b''-1}^{-1}\mathfrak{H}Q_{a''b''-1}$

形成$\mathfrak{H}$所屬之共軛系,而其一羣$Q_i^{-1}\mathfrak{H}Q_i$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$Q_i^{-1}\mathfrak{H}Q_i$.

次之,若假定此元素R爲含於(2)中二羣如$Q_i^{-1}\mathfrak{H}Q_i$, $Q_j^{-1}\mathfrak{H}Q_j$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$\mathfrak{H}$,其巡回率爲pb'之約數之元素,與P爲交換可能.

茲以$\mathfrak{H}$之元素S之巡回率s爲pb'之約數. s爲p之倍

數 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

$$S,\ PS,\ P^{2}S,\ \cdots\cdots,\ P^{p-1}S, \tag{3}$$

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$\mathfrak{H}$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$\mathfrak{H}$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$\mathfrak{H}$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

$$a''(p-1)b<pb.$$

$$\therefore\ (a''-1)(p-1)<1.$$

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之約數之元素共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.

58. 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

$$\mathfrak{G}_{n+1},\quad \mathfrak{G}_{n+2},\quad \cdots\cdots,\quad \mathfrak{G}_{n+\alpha-1},$$

則(參照第47節第一定理)

$$\mathfrak{G},\quad \mathfrak{G}_1,\quad \mathfrak{G}_2,\quad \cdots\cdots,\quad \mathfrak{G}_n,\quad \mathfrak{G}_{n+1},\quad \cdots\cdots,\quad \mathfrak{G}_{n+\alpha-1},\quad 1$$

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

$$Q^{3}=1.$$

$$\therefore \quad x^{3}\equiv 1 \pmod 5.$$

$$\therefore \quad x\equiv 1 \pmod 5.$$

$$\therefore \quad Q^{-1}PQ=P.$$

卽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.

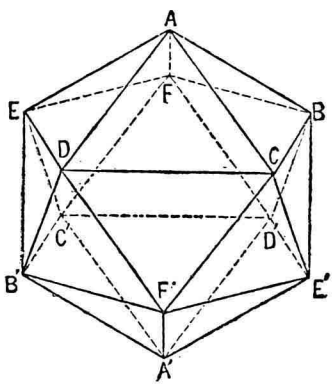
(iv) 60 元羣.

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 $a, a_1, \cdots\cdots, a_{n-1}$ 上所行之置換而成之羣. 若將某文字如 a, 分別置換於他之文字 $a_1, a_2, \cdots\cdots, a_{n-1}$ 者之置換存在於 $\mathfrak{G}$ 中時, 則 $\mathfrak{G}$ 便含有將任意之文字 a_i 置換於他之任意文字 a_j 者之置換. 蓋若以 a 置換於 a_i 之置換之一爲 S, a 置換於 a_j 之置換之一爲 T, 則積 $S^{-1}T$ 乃置換 a_i 於 a_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.

63. 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 α_i 置換之之時,則 $S^{-1}\mathfrak{H}S$ 之置換,皆不足以動 α_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

$$(1) \qquad \alpha, \ \alpha_1, \cdots\cdots, \alpha_{m-1}$$

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

$$S^{-1}\mathfrak{H}S=\mathfrak{H}_i=\mathfrak{H},$$

卽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($\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$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. 卽與$\mathfrak{H}$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卽$\mathfrak{H}$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$\mathrm{S}_1, \mathrm{S}_2, \cdots\cdots, \mathrm{S}_{m-1}$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$\mathfrak{K}$時,若$\mathfrak{G}$中一個定文字不動之約羣爲$\mathfrak{H}$,則

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

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$\mathfrak{K}$,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$\mathfrak{K}$爲可遷的,故$\mathfrak{K}$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$\mathfrak{H}\mathfrak{K}$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

$$1,\quad (\alpha\alpha_1\alpha_2),\quad (\alpha\alpha_2\alpha_1),$$
$$(\alpha_1\alpha_2),\quad (\alpha\alpha_2),\quad (\alpha\alpha_1)$$

中,一個定文字不動之約羣爲

$$\mathfrak{H}\ :\ 1,\quad (\alpha_1\alpha_2);$$
$$\mathfrak{H}_1\ :\ 1,\quad (\alpha\alpha_2);$$
$$\mathfrak{H}_2\ :\ 1,\quad (\alpha\alpha_1).$$

又若令 $S_1=(\alpha\alpha_1)$, $S_2=(\alpha\alpha_2)$, 則

$$\mathfrak{H}S_1:\quad (\alpha\alpha_1),\quad (\alpha\alpha_1\alpha_2);$$
$$\mathfrak{H}S_2:\quad (\alpha\alpha_2),\quad (\alpha\alpha_2\alpha_1).$$

例 2. 於六次可遷羣

$$1,\qquad (\alpha_1\alpha_5)(\alpha_2\alpha_4),$$
$$(\alpha\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5),\qquad (\alpha\alpha_5)(\alpha_1\alpha_4)(\alpha_2\alpha_3),$$
$$(\alpha\alpha_2\alpha_4)(\alpha_1\alpha_3\alpha_5),\qquad (\alpha\alpha_4)(\alpha_1\alpha_3),$$
$$(\alpha\alpha_3)(\alpha_1\alpha_4)(\alpha_2\alpha_5),\qquad (\alpha\alpha_3)(\alpha_1\alpha_2)(\alpha_4\alpha_5),$$
$$(\alpha\alpha_4\alpha_2)(\alpha_1\alpha_5\alpha_3),\qquad (\alpha\alpha_2)(\alpha_3\alpha_5),$$
$$(\alpha\alpha_5\alpha_4\alpha_3\alpha_2\alpha_1),\qquad (\alpha\alpha_1)(\alpha_2\alpha_5)(\alpha_3\alpha_4),$$

$$\mathfrak{H}\ :\ 1,\quad (\alpha_1\alpha_5)(\alpha_2\alpha_4);$$
$$\mathfrak{H}_1\ :\ 1,\quad (\alpha\alpha_2)(\alpha_3\alpha_5);$$

$$\mathfrak{H}_2 : 1,\quad (\alpha\alpha_4)\alpha_1\alpha_3);$$

$$\mathfrak{H}_2 : 1,\quad (\alpha_1\alpha_5)(\alpha_2\alpha_4);$$

$$\mathfrak{H}_4 : 1,\quad (\alpha\alpha_2)(\alpha_3\alpha_5);$$

$$\mathfrak{H}_5 : 1,\quad (\alpha\alpha_4)(\alpha_1\alpha_3).$$

64. 多重可遷羣.

設 $\mathfrak{G}$ 爲 n 個文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之置換羣.若此之文字中某 m 個

$$\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1},$$

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

$$\alpha', \alpha_1', \cdots\cdots, \alpha'_{m-1}$$

以任意之 m 個文字

$$\alpha'', \alpha_1'', \cdots\cdots, \alpha''_{m-1}$$

置換之之置換.蓋若

$$S=\begin{pmatrix}\alpha\ \alpha_1,\cdots\cdots\alpha_{m-1}\ \cdots\cdots\\ \alpha'\alpha_1'\cdots\cdots\alpha'_{m-1}\cdots\cdots\end{pmatrix},\quad T=\begin{pmatrix}\alpha\ \alpha_1\ \cdots\cdots\alpha_{m-1}\ \cdots\cdots\\ \alpha''\alpha_1''\cdots\cdots\alpha''_{m-1}\cdots\cdots\end{pmatrix},$$

則得

$$S^{-1}T=\begin{pmatrix}\alpha'\ \alpha_1'\ \cdots\cdots\alpha'_{m-1}\ \cdots\cdots\\ \alpha''\alpha_1''\cdots\cdots\alpha''_{m-1}\cdots\cdots\end{pmatrix}$$

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 $\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$ 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

$$S=\begin{pmatrix} a'a'_1\cdots\cdots a'_{m-1}\cdots\cdots \\ aa_1''\cdots\cdots a''_{m-1}\cdots\cdots \end{pmatrix},$$

次之因$\mathfrak{H}$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

$$T=\begin{pmatrix} aa_1''a_2''\cdots\cdots a''_{m-1}\cdots\cdots \\ aa_1\ a_2\ \cdots\cdots a_{m-1}\ \cdots\cdots \end{pmatrix},$$

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

$$(a_ra_s)=(aa_r)(aa_s)(aa_r).$$

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$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$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α_{n-1}不動之約羣$\mathfrak{B}$,由前節第一定理,爲$n-1$文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-2}$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

$$(\alpha\alpha_1\alpha_2),\quad (\alpha\alpha_1\alpha_3),\quad \cdots\cdots,\quad (\alpha\alpha_1\alpha_{n-2}).$$

同樣,於$\mathfrak{A}$,其α_{n-2}不動之約羣乃$n-1$文字$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-3}, \alpha_{n-1}$之$n-3$重可遷羣,因之含有三項巡回置換

$$(\alpha\alpha_1\alpha_2),\quad \cdots\cdots,\quad (\alpha\alpha_1\alpha_{n-3}),\quad (\alpha\alpha_1\alpha_{n-1}).$$

此之結果,遂爲$\mathfrak{A}$含有$n-2$個之三項巡回置換

$$(\alpha\alpha_1\alpha_i),\ i=2, 3, \cdots\cdots, n-1,$$

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

$$1,\quad (\alpha\alpha_1\alpha_2),\quad (\alpha\alpha_2\alpha_1)$$

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

$$\mathrm{A}_i=\begin{pmatrix}123\cdots\cdots\\12i\cdots\cdots\end{pmatrix}.$$

以是變(123)之形,則有

$$\mathrm{A}_i^{-1}(123)\,\mathrm{A}_i=(12i),$$

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

$$\mathrm{L}=\mathrm{N}^{-1}\mathrm{A}^{-1}\mathrm{NA}.$$

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，$\mathfrak{A}$ 者單純羣也. 故 $\mathfrak{D}$ 爲 $\mathfrak{A}$ 或爲1，是所必要. 若 $\mathfrak{D}=\mathfrak{A}$，則 $\mathfrak{N}$ 不得不與 $\mathfrak{S}$ 一致；若 $\mathfrak{D}=1$，則以 $\mathfrak{N}/\mathfrak{D}$ $(=\mathfrak{N})$ 與 $\mathfrak{S}/\mathfrak{A}$ 爲單純同態之故，$\mathfrak{N}$ 之元數不得不爲2也。即

$$\mathfrak{N}:\quad 1,\quad \mathrm{N}.$$

於是N之巡回率既爲2，故若以巡回表示示之，則如

$$\mathrm{N}=(12)(34)\cdots\cdots,$$

其巡回因子皆二項也. 此N以 $\mathfrak{S}$ 之置換(23)變其形，則得

$$(23)\mathrm{N}(23)=(13)(24)\cdots\cdots,$$

是與N異者也. 但 $\mathfrak{N}$ 於 $\mathfrak{S}$ 爲正常. 故 $(23)\mathrm{N}(23)$ 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 $\mathfrak{A}$ 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

$$\mathrm{T}_i=\begin{pmatrix} rst\cdots\cdots \\ 12i\cdots\cdots \end{pmatrix}\quad i=3,\ 4,\ \cdots\cdots,\ n.$$

故此時若 $\mathfrak{G}$ 含有三項巡回置換 (rst)，則以 T_i 變其形，乃有

$$\mathrm{T}_i^{-1}(rst)\mathrm{T}_i=(12i),\quad i=3,\ 4,\ \cdots\cdots,\ n,$$

而 $\mathfrak{G}$ 遂含 $n-2$ 個之三項巡回置換

$$(123),\ (124),\ \cdots\cdots,\ (12n).$$

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. 可遷重複度之限界.

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 $\quad 1, 2, 3, \cdots\cdots, c-1, d$ (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

$$S^{-1}T^{-1}ST=(j+1, c, d).$$

是卽$\mathfrak{G}$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. 卽

$$S=(12\cdots)\cdots(\cdots, i-1, i)(i+1, \cdots, m-1, m, \cdots)\cdots,$$

$$S=(12\cdots)\cdots(\cdots, m-2)(m-1, m, \cdots)\cdots,$$

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,卽其中有$m-1$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, $\mathfrak{G}$ 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 $\mathfrak{G}_\alpha$ 爲 α 文字

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

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_i) 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:

$$\mathfrak{G}_\alpha=\mathfrak{H}_\alpha+\mathfrak{H}_\alpha P_1+\cdots\cdots+\mathfrak{H}_\alpha P_{\nu-1},$$

$$\mathfrak{G}_\beta=\mathfrak{H}_\beta+\mathfrak{H}_\beta Q_1+\cdots\cdots+\mathfrak{H}_\beta Q_{\nu-1},$$

而更作其積

(4) $\mathfrak{H}_\alpha\mathfrak{H}_\beta,\ \mathfrak{H}_\alpha P_1\mathfrak{H}_\beta Q_1,\ \cdots\cdots,\ \mathfrak{H}_\alpha P_{\nu-1}\mathfrak{H}_\beta Q_{\nu-1},$

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 $(a+b)$ 次之非遷羣焉.

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, $(\alpha\alpha_1\alpha_2)$, $(\alpha\alpha_2\alpha_1)$;

$\mathfrak{G}_\beta$: 1, $(\beta\beta_1\beta_2)$, $(\beta\beta_2\beta_1)$

時, 則

$$1,\quad (\alpha\alpha_1\alpha_2)(\beta\beta_1\beta_2),\quad (\alpha\alpha_2\alpha_1)(\beta\beta_2\beta_1)$$

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.

$$\mathfrak{G}_\alpha : \begin{cases} 1, & (\alpha\alpha_1\alpha_2), & (\alpha\alpha_2\alpha_1), \\ (\alpha\alpha_1), & (\alpha_1\alpha_2), & (\alpha\alpha_2); \end{cases}$$

$$\mathfrak{H}_\alpha : \quad 1, \quad (\alpha\alpha_1\alpha_2), \quad (\alpha\alpha_2\alpha_1);$$

$$\mathfrak{H}_\alpha(\alpha\alpha_1) : \quad (\alpha\alpha_1), \quad (\alpha_1\alpha_2), \quad (\alpha\alpha_2);$$

$$\mathfrak{G}_\alpha = \mathfrak{H}_\alpha + \mathfrak{H}_\alpha(\alpha\alpha_1).$$

$$\mathfrak{G}_\beta : \quad 1, \quad (\beta\beta_2)(\beta_1\beta_3), \quad (\beta\beta_1\beta_2\beta_3), \quad (\beta\beta_3\beta_2\beta_1);$$

$$\mathfrak{H}_\beta : \quad 1, \quad (\beta\beta_2)(\beta_1\beta_3);$$

$$\mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3) : \quad (\beta\beta_1\beta_2\beta_3), \quad (\beta\beta_3\beta_2\beta_1);$$

$$\mathfrak{G}_\beta = \mathfrak{H}_\beta + \mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3).$$

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 $\mathfrak{H}_\alpha(\alpha\alpha_1)$, 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:

$$\mathfrak{H}_\alpha\mathfrak{H}_\beta:\begin{cases}1, & (\alpha\alpha_1\alpha_2), & (\alpha\alpha_2\alpha_1)\\ (\beta\beta_2)(\beta_1\beta_3), & (\alpha\alpha_1\alpha_2)(\beta\beta_2)(\beta_1\beta_3), & (\alpha\alpha_2\alpha_1)(\beta\beta_2)(\beta_1\beta_3);\end{cases}$$

$$\mathfrak{H}_\alpha(\alpha\alpha_1)\mathfrak{H}_\beta(\beta\beta_1\beta_2\beta_3):\begin{cases}(\alpha\alpha_1)(\beta\beta_1\beta_2\beta_3), & (\alpha_1\alpha_2)(\beta\beta_1\beta_2\beta_3),\\ (\alpha\alpha_2)(\beta\beta_1\beta_2\beta_3)\\ (\alpha\alpha_1)(\beta\beta_3\beta_2\beta_1) & (\alpha_1\alpha_2)(\beta\beta_3\beta_2\beta_1),\\ (\alpha\alpha_2)(\beta\beta_3\beta_2\beta_1),\end{cases}$$

則此所得之12個置換作一七次非遷羣也.

由a次可遷羣$\mathfrak{G}_\alpha$與b次可遷羣$\mathfrak{G}_\beta$,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$\mathfrak{G}_\gamma$. 於是由$\mathfrak{G}$以及$\mathfrak{G}_\gamma$,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) $$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}.$$

而由$\mathfrak{G}$之置換,一文字α雖得分別置換爲

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

但若以之置換爲他之文字$\alpha_a, \alpha_{a+1}, \cdots\cdots, \alpha_{n-1}$,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α_i $(i<a)$爲置換於α'者,則$\mathfrak{G}$乃含以α置換於α_i之置換H,而因HG置換α於α',故由假設,則α'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, $\mathfrak{G}$ 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 $\mathfrak{G}$, 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

$$(3) \qquad \alpha_a, \alpha_{a+1}, \cdots\cdots, \alpha_{a+b-1} \quad (a+b \leqq n).$$

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 $\mathfrak{G}$ 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 $\mathfrak{G}$ 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

$$(1) \qquad \alpha, \alpha_1, \cdots\cdots, \alpha_{a-1},$$

其他則爲由剩餘之文字

$$(2) \qquad \beta, \beta_1, \cdots\cdots, \beta_{b-1}$$

而成者. 於是取 $\mathfrak{G}$ 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_j' 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$\mathfrak{H}_\alpha P_i\mathfrak{H}_\beta Q_i$, $\mathfrak{G}_\beta$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

$$\mathfrak{G}:\begin{cases} 1, & (ab), & (cd), & (ef), & (ab)(cd)(ef), \\ (ab)(cd), & (ab)(ef), & (cd)(ef) \end{cases}$$

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

$$\mathfrak{G}_\alpha :\quad 1,\ (ab);$$

而僅着眼於他文字之移動,則爲

$$\mathfrak{G}_\beta :\quad 1,\ (cd),\ (ef),\ (cd)(ef);$$

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

$$\mathfrak{G}:\begin{cases} 1, & (12)(34), & (56), & (12)(34)(56), \\ (13)(24)(78), & (13)(24)(56)(78), \\ (14)(23)(78), & (14)(23)(56)(78) \end{cases}$$

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

$$\mathfrak{G}_\alpha:\ 1,\quad (12)(34),\quad (13)(24),\quad (14)(23);$$

若僅視(β)之文字之移動,則爲

$$\mathfrak{G}_\beta:\ 1,\quad (56),\quad (78),\quad (56)(78).$$

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

$$\mathfrak{H}_\alpha:\ 1,\quad (12)(34);$$

而對應於$\mathfrak{G}_\alpha$之主元素者爲

$$\mathfrak{H}_\beta:\ 1,\quad (56)$$

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
$$\mathfrak{H}_\alpha\mathfrak{H}_\beta:\ 1,\quad (12)(34),\quad (56),\quad (12)(34)(56);$$
$$\mathfrak{H}_\alpha(13)(24)\cdot\mathfrak{H}_\beta(78):\begin{cases}(13)(24)(78),\quad (13)(24)(56)(78),\\ (14)(23)(78),\quad (14)(23)(56)(78);\end{cases}$$

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a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a於a_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

$$\mathfrak{G}_\alpha: \quad A_iP_s\begin{cases}i=0, 1, 2, \cdots\cdots, h_\alpha-1 & [\mu h_\alpha=g_\alpha]\\ s=0, 1, 2, \cdots\cdots, \mu-1 & [P_0=1]\end{cases}$$

$$\mathfrak{G}_\beta: \quad B_jQ_s\begin{cases}j=0, 1, 2, \cdots\cdots, h_\beta-1 & [\mu h_\beta=g_\beta]\\ s=0, 1, 2, \cdots\cdots, \mu-1 & [Q_0=1]\end{cases}$$

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

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

$$\nu_0=3,\quad \nu_1=8,\quad \nu_2=0,\quad \nu_3=0,\quad \nu_4=1,$$

$$\therefore\quad \nu_1+2\nu_2+3\nu_3+4\nu_4=8+4\cdot1=12.$$

例 2. 於十二元七次非遷羣 (第 68 節例 4 參照)

$$\begin{array}{ccc} 1 & (xyz) & (xzy) \\ (ac)(bd) & (xyz)(ac)(bd) & (xzy)(ac)(bd) \\ (xy)(abcd) & (yz)(abcd) & (zx)(abcd) \\ (xy)(adcb) & (yz)(adcb) & (zx)(adcb), \end{array}$$

$$\nu_0=2,\ \nu_1=6,\ \nu_2=0,\ \nu_3=1,\ \nu_4=2,\ \nu_5=0,\ \nu_6=0,\ \nu_7=1.$$

$$\therefore\quad \nu_1+2\nu_2+\cdots\cdots+7\nu_7=6+3\cdot1+4\cdot2+7\cdot1=2\cdot12.$$

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

$$G=(a\alpha_1\cdots\cdots\alpha_{\alpha-1})(\beta\beta_1\cdots\beta_{b-1})\cdots\cdots.$$

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a不動且非不動置換. 故在此可遷羣中,文字a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) $$\begin{pmatrix} G \\ GG_j \end{pmatrix} = \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_j & G_1G_j & \cdots\cdots & G_{g-1}G_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \\ G_0G_i \cdot G_j & G_1G_i \cdot G_j & \cdots\cdots & G_{g-1}G_i \cdot G_j \end{pmatrix}$$

之故,* 遂得

(5) $$\begin{pmatrix} G \\ GG_i \end{pmatrix}\begin{pmatrix} G \\ GG_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}\begin{pmatrix} G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \\ G_0G_i \cdot G_j & G_1G_i \cdot G_j & \cdots\cdots & G_{g-1}G_iG_j \end{pmatrix}$$

$$= \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0 \cdot G_iG_j & G_1 \cdot G_iG_j & \cdots\cdots & G_{g-1} \cdot G_iG_j \end{pmatrix} = \begin{pmatrix} G \\ G \cdot G_iG_j \end{pmatrix}.$$

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 $\begin{pmatrix} G \\ GG_k \end{pmatrix}$ 卽 $\begin{pmatrix} G \\ G\cdot G_iG_j \end{pmatrix}$ 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. 卽 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. 卽

(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a分別置換爲$a, a_1, \cdots\cdots, a_{n-1}$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:

$$(3)\qquad S_i=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ aa_i & a_1a_i & \cdots\cdots & a_{n-1}a_i \end{pmatrix} \quad i=0, 1, 2, \cdots\cdots, n-1,$$

或

$$(3')\qquad S_i=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a_i & a_1a_i & \cdots\cdots & a_{n-1}a_i \end{pmatrix} \quad i=0, 1, 2, \cdots\cdots, n-1,$$

但$a_0=a$. 於$\mathfrak{G}$, 其使a不動之置換僅爲主元素, 故得

$$(4)\qquad a_ia=a_i, \quad i=0, 1, 2, \cdots\cdots, n-1,$$

因之

$$S_0=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ aa & a_1a & \cdots\cdots & a_{n-1}a \end{pmatrix}=1.$$

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).

$$\text{(ii)}\quad S_iS_j=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ aa_i & a_1a_i & \cdots\cdots & a_{n-1}a_i \end{pmatrix}\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ aa_j & a_1a_j & \cdots\cdots & a_{n-1}a_j \end{pmatrix}$$

$$=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a_i & a_1a_i & \cdots\cdots & a_{n-1}a_i \end{pmatrix}\begin{pmatrix} a_i & a_1a_i & \cdots\cdots & a_{n-1}a_i \\ a_i\cdot a_j & a_1a_i\cdot a_j & \cdots\cdots & a_{n-1}a_i\cdot a_j \end{pmatrix}$$

$$=\begin{pmatrix} a & a_1 & \cdots\cdots & a_{n-1} \\ a_ia_j & a_1a_i\cdot a_j & \cdots\cdots & a_{n-1}a_i\cdot a_j \end{pmatrix}.$$

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a於a_ia_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a,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

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

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

$$(7) \qquad \mathfrak{H},\ P_1^{-1}\mathfrak{H}P_1, \cdots\cdots, P_{\nu-1}^{-1}\mathfrak{H}P_{\nu-1}$$

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)　$\mathfrak{G}=\mathfrak{D}Q_0+\mathfrak{D}Q_1+\cdots\cdots+\mathfrak{D}Q_{\mu-1}\quad(Q_0=1)$

於是對$\mathfrak{D}$之任意一元素D，乃有

(9)　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rDQ_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rD\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}.$$

故由$\mathfrak{G}$之元素所得之置換，不過次之μ個：

(10)　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_0\end{pmatrix},\ \begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_1\end{pmatrix},\ \cdots\cdots,\ \begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_{\mu-1}\end{pmatrix}.$$

且此各個皆互異。蓋若

$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{pmatrix},$$

則

(11)　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{pmatrix}^{-1}=1.$$

然

$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_rQ_j^{-1}\\ \mathfrak{H}P_rQ_j^{-1}\cdot Q_j\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_rP_j^{-1}\\ \mathfrak{H}P_r\end{pmatrix},$$

因之

$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j\end{pmatrix}^{-1}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_j^{-1}\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_iQ_j^{-1}\end{pmatrix}.$$

故由(11)，　$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rQ_iQ_j^{-1}\end{pmatrix}=1.$$

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$\mathfrak{D}$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

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

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 $\mathfrak{A}/\mathfrak{B}$ 卽

$$1,\quad (bcd),\quad (bdc)\quad (\text{mod. }\mathfrak{B})$$

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,

$$\begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}G & \mathfrak{B}(bcd)G & \mathfrak{B}(bdc)G \end{pmatrix} = \begin{pmatrix} \mathfrak{B} & \mathfrak{B}(bcd) & \mathfrak{B}(bdc) \\ \mathfrak{B}(bdc) & \mathfrak{B} & \mathfrak{B}(bcd) \end{pmatrix}.$$

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

$$\mathfrak{H},\ S_1^{-1}\mathfrak{H}S_1,\ \cdots\cdots,\ S_{n-1}^{-1}\mathfrak{H}S_{n-1},$$

乃分別爲$\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$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

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

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α爲$\alpha_r^{(i)}$也. 因之$\mathfrak{H}S_rG_i$卽爲在$\mathfrak{G}$中將α置換爲$\alpha_r^{(i)}$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α置換爲α_r者之傍系$\mathfrak{H}S_r$,得以α置換爲$\alpha_r^{(i)}$者之傍系$\mathfrak{H}S_rG_i$而置換之者也. 以故於n文字

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

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$\alpha, \alpha_1, \cdots\cdots,$

*對於文字α_i使α置換爲α_i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

$$\begin{pmatrix}\mathrm{ABCD}\\ \mathrm{ABCD}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{BCDA}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{CDAB}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{DABC}\end{pmatrix},$$
$$\| \qquad \| \qquad \| \qquad \|$$
$$1 \qquad (\mathrm{ABCD}) \quad (\mathrm{AC})(\mathrm{BD}) \quad (\mathrm{ADCB})$$

$$\begin{pmatrix}\mathrm{ABCD}\\ \mathrm{ADCB}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{DCBA}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{CBAD}\end{pmatrix}, \begin{pmatrix}\mathrm{ABCD}\\ \mathrm{BADC}\end{pmatrix}.$$
$$\| \qquad \| \qquad \| \qquad \|$$
$$(\mathrm{BD}) \quad (\mathrm{AD})(\mathrm{BC}) \quad (\mathrm{AC}) \quad (\mathrm{AB})(\mathrm{CD})$$

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 a,

$\alpha_1, \cdots\cdots, \alpha_{m-1}$, 代以他之文字 $\beta, \beta_1, \cdots\cdots, \beta_{m-1}$ 時所生之置換羣, 名曰與 $\mathfrak{T}$ **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,

$$(1) \qquad G_0, G_1, \cdots\cdots, G_{g-1}$$

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

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}_1 & \cdots\cdots & \mathfrak{H}_{\nu-1} \\ G_i^{-1}\mathfrak{H}G_i & G_i^{-1}\mathfrak{H}_1G_i & \cdots\cdots & G_i^{-1}\mathfrak{H}_{\nu-1}G_i \end{pmatrix}.$$

便宜上以 $\begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_rG_i \end{pmatrix}$ 記之,則對 $\mathfrak{G}$ 之 g 元素,g 個之置換

$$(3)\quad \begin{pmatrix} \mathfrak{H}_r \\ G_0^{-1}\mathfrak{H}_rG_0 \end{pmatrix}, \begin{pmatrix} \mathfrak{H}_r \\ G_1^{-1}\mathfrak{H}_rG_1 \end{pmatrix}, \cdots\cdots, \begin{pmatrix} \mathfrak{H}_r \\ G_{g-1}^{-1}\mathfrak{H}_rG_{g-1} \end{pmatrix}$$

生焉. 且其成羣也. 蓋因作其任意二者之積,乃成爲次之(4):

$$(4)\quad \begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_rG_i \end{pmatrix}\begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}\mathfrak{H}_rG_j \end{pmatrix} = \begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_rG_i \end{pmatrix}\begin{pmatrix} G_i^{-1}\mathfrak{H}_rG_i \\ G_j^{-1}\cdot G_i^{-1}\mathfrak{H}_rG_i\cdot G_j \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}G_i^{-1}\mathfrak{H}_rG_iG_j \end{pmatrix} = \begin{pmatrix} \mathfrak{H}_r \\ (G_iG_j)^{-1}\mathfrak{H}_r(G_iG_j) \end{pmatrix},^*$$

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 $\begin{pmatrix} \mathfrak{H}_r \\ G_i^{-1}\mathfrak{H}_rG_i \end{pmatrix}$ 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

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}_1 & \cdots\cdots & \mathfrak{H}_{\nu-1} \\ G_t^{-1}\mathfrak{H}G_t & G_t^{-1}\mathfrak{H}_1G_t & \cdots\cdots & G_t^{-1}\mathfrak{H}_{\nu-1}G_t \end{pmatrix} = 1,$$

---

*置換 $\begin{pmatrix} \mathfrak{H}_r \\ G_j^{-1}\mathfrak{H}_rG_j \end{pmatrix}$,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) $$\mathfrak{K},\mathfrak{K}_1,\cdots\cdots,\mathfrak{K}_{\nu-1}$$

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) $$\left(Q_0^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_0\right),\ \left(Q_1^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_1\right),\ \cdots\cdots,\ \left(Q_{\mu-1}^{-1}\overset{\mathfrak{H}_r}{\mathfrak{H}_r}Q_{\mu-1}\right).$$

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, $\begin{pmatrix}\mathfrak{H}_r\\ G^{-1}\mathfrak{H}_rG\end{pmatrix}=\begin{pmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\end{pmatrix}=1;$

屬於 $\mathfrak{D}P_1$ 時, $\left(G^{-1}\mathfrak{H}_rG\right)=\left(\begin{smallmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}_1\mathfrak{H}_2\mathfrak{H}\end{smallmatrix}\right)=(\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2)$;

屬於 $\mathfrak{D}P_2$ 時, $\left(G^{-1}\mathfrak{H}_rG\right)=\left(\begin{smallmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}_2\mathfrak{H}\mathfrak{H}_1\end{smallmatrix}\right)=(\mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1)$;

屬於 $\mathfrak{D}Q$ 時, $\left(G^{-1}\mathfrak{H}_rG\right)=\left(\begin{smallmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1\end{smallmatrix}\right)=(\mathfrak{H}_1\mathfrak{H}_2)$;

屬於 $\mathfrak{D}Q_4$ 時, $\left(G^{-1}\mathfrak{H}_rG\right)=\left(\begin{smallmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}_2\mathfrak{H}_1\mathfrak{H}\end{smallmatrix}\right)=(\mathfrak{H}_2\mathfrak{H})$;

屬於 $\mathfrak{D}Q_2$ 時, $\left(G^{-1}\mathfrak{H}_rG\right)=\left(\begin{smallmatrix}\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2\\ \mathfrak{H}_1\mathfrak{H}\mathfrak{H}_2\end{smallmatrix}\right)=(\mathfrak{H}\mathfrak{H}_1)$.

故表示羣如次:

1, $(\mathfrak{H}\mathfrak{H}_1\mathfrak{H}_2)$, $(\mathfrak{H}\mathfrak{H}_2\mathfrak{H}_1)$, $(\mathfrak{H}_1\mathfrak{H}_2)$, $(\mathfrak{H}_2\mathfrak{H})$, $(\mathfrak{H}\mathfrak{H}_1)$.

78. 元數 36, 72, 90 者之羣之複合性.

(i) 元數 36, 72 者.

因 $36=2^2\cdot3^2$, $72=2^3\cdot3^2$,

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.　$(90=2\cdot 3^2\cdot 5)$

由 Sylow 氏定理, 5 元約羣之數, 得以 $1+5\lambda$ 形表之, 且爲 $2\cdot 3^2$ 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 $\mathfrak{N}$ 表之. $\mathfrak{N}$ 中 3 元約羣(以 $\{Q\}$ 表之), 由 Sylow 氏定理, 於 $\mathfrak{N}$ 爲正常. 故 $\{Q\}$ 與 P 爲交換可能. 又 $\{P\}$ 於 $\mathfrak{N}$ 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

$$(PQ)^5=P^5Q^5=Q^2\neq 1,$$

$$(PQ)^3=P^3Q^3=P^3\neq 1.$$

然積 PQ 屬於 $\mathfrak{N}$, 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

$$1 \qquad Q=(a_1a_5)(a_2a_4)$$

$$P_1=(aa_1a_2a_3a_4a_5) \qquad Q_1=(aa_5)(a_1a_4)(a_2a_3)$$

$$P_2=(aa_2a_4)(a_1a_3a_5) \qquad Q_2=(aa_4)(a_1a_3)$$

$$P_3=(aa_3)(a_1a_4)(a_2a_5) \qquad Q_3=(aa_3)(a_1a_2)(a_4a_5)$$

$$P_4=(aa_4a_2)(a_1a_5a_3) \qquad Q_4=(aa_2)(a_3a_5)$$

$$P_5=(aa_5a_4a_3a_2a_1) \qquad Q_5=(aa_1)(a_2a_5)(a_3a_4)$$

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. 次以$\mathfrak{H}$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)　　$\mathfrak{H}$, $\mathfrak{H}S_1$. ……, $\mathfrak{H}S_{m-1}$　$(1<m<n)$.

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)　　$$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1},$$

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

$$(6)\qquad \mathfrak{G}=\mathfrak{R}+\mathfrak{R}T_1+\cdots\cdots+\mathfrak{R}T_{l-1}\quad (l>1),$$

則(2)式得換書之爲

$$(7)\qquad \begin{aligned}\mathfrak{G}=\mathfrak{H}&+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}\\&+\mathfrak{H}T_1+\mathfrak{H}S_1T_1+\cdots\cdots+\mathfrak{H}S_{m-1}T_1\\&+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&+\mathfrak{H}T_{l-1}+\mathfrak{H}S_1T_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}T_{l-1},\end{aligned}$$

而(𝔊)之置換(3)乃得表示如次:

$$(8)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots & \mathfrak{H}S_{m-1} & \mathfrak{H}T_1 & \cdots & \mathfrak{H}S_{m-1}T_1 & \cdots & \mathfrak{H}T_{l-1} & \cdots & \mathfrak{H}S_{m-1}T_{l-1}\\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots & \mathfrak{H}S_{m-1}G_i & \mathfrak{H}T_1G_i & \cdots & \mathfrak{H}S_{m-1}T_1G_i & \cdots & \mathfrak{H}T_{l-1}G_i & \cdots & \mathfrak{H}S_{m-1}T_{l-1}G_i\end{pmatrix}.$$

由此置換,則含於傍系* $\mathfrak{R}T_r$之傍系(關於$\mathfrak{H}$者)

$$(9)\qquad \mathfrak{H}T_r,\ \mathfrak{H}S_1T_r,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_r$$

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$\mathfrak{R}T_0=\mathfrak{R}$.

$$(11)\quad \begin{cases} \mathfrak{H},\ \mathfrak{H}S_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1} \\ \mathfrak{H}T_1,\ \mathfrak{H}S_1T_1,\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{H}T_{l-1},\ \mathfrak{H}S_1T_{l-1},\ \cdots\cdots,\ \mathfrak{H}S_{m-1}T_{l-1}, \end{cases}$$

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($\mathfrak{G}$)中,傍系

(4) $$\mathfrak{H}, \mathfrak{H}S_1, \cdots\cdots, \mathfrak{H}S_{m-1} \quad (1<m<n)$$

作一非原系時,則如前節之所述,

(5) $$\mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}$$

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) $$\begin{cases} \mathfrak{K}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1} \\ \mathfrak{K}T_1=\mathfrak{H}T_1+\mathfrak{H}S_1T_1+\cdots\cdots+\mathfrak{H}S_{m-1}T_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{K}T_{l-1}=\mathfrak{H}T_{l-1}-\mathfrak{H}S_1T_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}T_{l-1} \end{cases}$$

因之關於$\mathfrak{K}$之傍系,直視之爲非原系可.

且由$\mathfrak{G}$之置換(8),傍系

(9) $$\mathfrak{H}T_r, \mathfrak{H}S_1T_r, \cdots\cdots, \mathfrak{H}S_{m-1}T_r,$$

分別爲

(10) $$\mathfrak{H}T_r G_i, \mathfrak{H}S_1T_rG_i, \cdots\cdots, \mathfrak{H}S_{m-1}T_rG_i$$

所置換. 然(9)與(10)共於($\mathfrak{G}$)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($\mathfrak{G}$)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):

$$(13)\qquad \begin{pmatrix} \mathfrak{R} & \mathfrak{R}T_1 & \cdots\cdots & \mathfrak{R}T_{l-1} \\ \mathfrak{R}G_i & \mathfrak{R}T_1G_i & \cdots\cdots & \mathfrak{R}T_{l-1}G_i \end{pmatrix}.$$

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 $(\mathfrak{M})$ 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

$$(14)\qquad \begin{pmatrix} \mathfrak{R} & \mathfrak{R}T_1 & \cdots\cdots & \mathfrak{R}T_{l-1} \\ \mathfrak{R}C_j & \mathfrak{R}T_1C_j & \cdots\cdots & \mathfrak{G}T_{l-1}C_j \end{pmatrix} \quad (j=0, 1, 2; \cdots\cdots, c-1)$$

皆爲不動的也(參照第75節). 故 $(\mathfrak{G})$ 中 c 個之置換

$$(15)\qquad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1} & \mathfrak{H}T_1 & \mathfrak{H}S_1T_1 & \cdots\cdots \\ \mathfrak{H}C_j & \mathfrak{H}S_1C_j & \cdots\cdots & \mathfrak{H}S_{m-1}C_j & \mathfrak{H}T_1C_j & \mathfrak{H}S_1T_1C_j & \cdots\cdots \end{pmatrix}$$

$$j=0, 1, \cdots\cdots, c-1$$

---

*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$\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$作非原系時, 若令

$$\mathfrak{R}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1} \quad (1<m<n),$$

則$\mathfrak{R}$爲$\mathfrak{G}$之約羣, 但$\mathfrak{H}$爲α不動之約羣, 而S_i爲將α置換爲α_i之置換之一. 反之, 若$\mathfrak{R}$爲$\mathfrak{G}$之約羣時, 則$\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$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$\mathfrak{R}$, 呼曰與非原系$\alpha, \alpha_1, \cdots\cdots, \alpha_{m-1}$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,

$$0,\ 3,\ 6$$

作一非原系. 而他之非原系, 分別爲

$$1,\ 4,\ 7$$

及

$$2,\ 5,\ 8$$

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 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 上所行置換而成之可遷羣. $\mathfrak{G}$ 中 α 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)　　$a,\ a_1,\ \cdots\cdots,\ a_{m-1}\quad (1<m<n).$

(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$a, a_1, \cdots\cdots, a_{m-1}$置換之,則得本系焉.

例. 於第80節中所示之羣,取其三文字

$$a,\quad a_2,\quad a_4,$$

其將a置換爲a, a_2或a_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a, a_2, a_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𝔊, $\mathfrak{H}, S_i$爲具有本節開始所示之同一意義者,而m文字$a, a_1, \cdots\cdots, a_{m-1}$則於𝔊中作非原系. 於是因(𝔊)與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𝔊之置換而生之非原系之置換,乃作(𝔊)中非原系之置換羣,卽與關於$\mathfrak{R}(=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1})$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$\mathfrak{R}$,而與$\mathfrak{R}$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

$$\mathfrak{R}=\mathfrak{H}+\mathfrak{H}P_3.$$

因之

$$\mathfrak{G}=\mathfrak{R}+\mathfrak{R}P_1+\mathfrak{R}P_2.$$

復次作$\mathfrak{H}$之共軛約羣,則有

$$\mathfrak{H}: 1, Q, P_3, Q_3 (=QP_3);$$

$$P_1^{-1}\mathfrak{H}P_1: 1, Q_4, P_3, Q_1;$$

$$P_2^{-1}\mathfrak{H}P_2: 1, Q_2, P_3, Q_5;$$

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$\mathfrak{H}$之傍系置換表示中之互異之置換爲次之六個(參照第75節).

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\end{pmatrix}=1,$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_1 & \mathfrak{H}P_1P_1 & \mathfrak{H}P_2P_1\end{pmatrix}=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_1 & \mathfrak{H}P_2 & \mathfrak{H}\end{pmatrix}=(\mathfrak{H}, \mathfrak{H}P_1, \mathfrak{H}P_2),$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_2 & \mathfrak{H}P_1P_2 & \mathfrak{H}P_2P_2\end{pmatrix}=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_2 & \mathfrak{H} & \mathfrak{H}P_1\end{pmatrix}=(\mathfrak{H}, \mathfrak{H}P_2, \mathfrak{H}P_1),$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}Q & \mathfrak{H}P_1Q & \mathfrak{H}P_2Q\end{pmatrix}=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H} & \mathfrak{H}P_2 & \mathfrak{H}P_1\end{pmatrix}=(\mathfrak{H}P_1, \mathfrak{H}P_2),$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}Q_4 & \mathfrak{H}P_1Q_4 & \mathfrak{H}P_2Q_4\end{pmatrix}=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_2 & \mathfrak{H}P_1 & \mathfrak{H}\end{pmatrix}=(\mathfrak{H}P_2, \mathfrak{H}),$$

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}Q_2 & \mathfrak{H}P_1Q_2 & \mathfrak{H}P_2Q_2\end{pmatrix}=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}P_1 & \mathfrak{H}P_2\\ \mathfrak{H}P_1 & \mathfrak{H} & \mathfrak{H}P_2\end{pmatrix}=(\mathfrak{H}, \mathfrak{H}P_1).$$

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$\mathfrak{H}$之傍系之置換
1, P_3	1	1
P_1, P_4 $(=P_3P_1)$	(ABΓ)	($\mathfrak{H}$, $\mathfrak{H}P_1$, $\mathfrak{H}P_2$)
P_2, P_5 $(=P_3P_2)$	(AΓB)	($\mathfrak{H}$, $\mathfrak{H}P_2$, $\mathfrak{H}P_1$)
Q, Q_3 $(=P_3Q)$	(BΓ)	($\mathfrak{H}P_1$, $\mathfrak{H}P_2$)
Q_4, Q_1 $(=P_3Q_4)$	(ΓA)	($\mathfrak{H}P_2$, $\mathfrak{H}$)
Q_2, Q_5 $(=P_3Q_2)$	(AB)	($\mathfrak{H}$, $\mathfrak{H}P_1$)

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$\mathfrak{H}$之對應於非原系a, a_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

$$A:\ a, a_1, \cdots\cdots, a_{m-1}.$$

而以a爲系A之文字a_i所置換之任意置換爲S; 且由是而系A之文字a_j得爲x所置換者. 卽

$$S=\begin{pmatrix} a \cdots\cdots a_j \cdots\cdots \\ a_i \cdots\cdots x \cdots\cdots \end{pmatrix},$$

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a置換爲a_j之置換. 以其一爲

$$N=\begin{pmatrix} a \cdots\cdots \\ a_j \cdots\cdots \end{pmatrix};$$

而以S變其形,則得

$$S^{-1}NS=\begin{pmatrix} a_i \cdots\cdots \\ x \cdots\cdots \end{pmatrix},$$

卽$S^{-1}NS$者乃以x置換a_i者也. 然$\mathfrak{N}$爲正常,故此置換屬於$\mathfrak{N}$. 是則x非與a_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a, a_2, a_4以及a_1, a_3, a_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a, a_2, a_4及a_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$\mathfrak{G}$爲n文字$a, a_1, \cdots\cdots, a_{n-1}$之可遷羣. $\mathfrak{G}$若含$n-1$個之轉換

$$(aa_1), (aa_2), \cdots\cdots, (aa_{n-1})$$

時,則$\mathfrak{G}$爲對稱的(參照第65節).

復次請就$\mathfrak{G}$雖含$m-1$個轉換

(1) $$(aa_1), (aa_2), \cdots\cdots, (aa_{m-1}) \quad [m<n],$$

而卻不含

(2) $$(aa_m), \cdots\cdots, (aa_{n-1})$$

者論之.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(αa_{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α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

$$S=\begin{pmatrix} \alpha \cdots\cdots a_j \cdots\cdots \\ a_i \cdots\cdots x \cdots\cdots \end{pmatrix}.$$

於是以S變(αa_j)之形，則得

$$S^{-1}(\alpha a_j)S=(a_i x).$$

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α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. 是卽$\mathfrak{G}$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$\alpha, a_1, \cdots\cdots, a_{n-1}$之可遷羣. 若$\mathfrak{G}$含有$n-2$個之三項巡回置換

$$(\alpha a_1 a_2), (\alpha a_1 a_3), \cdots\cdots, (\alpha a_1 a_{n-1})$$

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) $$(\alpha a_1 a_2), (\alpha a_1 a_3), \cdots\cdots, (\alpha a_1 a_{m-1}),$$

而卻不含

(2) $$(\alpha a_1 a_m), \cdots\cdots, (\alpha a_1 a_{n-1})$$

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$(a_ia_ja_{m+l})$或$(a_ia_{m+k}a_{m+l})$ $[i, j\leqq m-1;\ 0\leqq k,\ l\leqq n-m-1]$. 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$(a_ia_ra_t)$之由(3)之文字而成者變其形所得之

$$(a_ia_ra_t)^{-1}(a_ia_ja_{m+l})(a_ia_ra_t)=(a_ra_ja_{m+l})=(a_ja_{m+l}a_r)$$

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$(a_ia_ja_{m+l})$,則$\mathfrak{G}$遂成爲含有$m-1$個之三項巡回置換

$$(a_ja_{m+l}a_r),\ r=0, 1, \cdots\cdots, j-1, j+1, \cdots\cdots, m-1,$$

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(aa_1a_{m+l}),是與假定反.又$\mathfrak{G}$含$(a_ia_{m+k}a_{m+l})$時,乃以(3)之文字之三項巡回置換$(a_ia_sa_t)$變其形,則得

$$(a_ia_sa_t)^{-1}(a_ia_{m+k}a_{m+l})(a_ia_sa_t)=(a_sa_{m+k}a_{m+l}).$$

於是令$s=0, 1. \cdots\cdots, i-1, i+1, \cdots\cdots, m-1$,而再加$(a_ia_{m+k}a_{m+l})$,則$\mathfrak{G}$遂成爲含有$m$個之巡回置換

$$(aa_{m+k}a_{m+l}),\ (a_1a_{m+k}a_{m+l}),\ \cdots\cdots,\ (a_{m-1}a_{m+k}a_{m+1}).$$

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重複度.

設 $\mathfrak{G}$ 爲 n 次可遷羣，$\mathfrak{T}$ 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

$$\mathfrak{T}', \mathfrak{T}'', \cdots\cdots. \tag{1}$$

(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

$$\alpha, \alpha_1, \cdots\cdots, \alpha_{q-1}, \tag{2}$$

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(S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. 即$S^{-1}\mathfrak{T}'S$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. 即$\mathfrak{G}$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$n-2+1=n-1$. 卽對稱的也(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$\mathfrak{G}$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$\mathfrak{G}$作非原系. 是卽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

$$\mathfrak{A}: \quad 1, \quad (ab), \quad (cd), \quad (ef),$$
$$(ab)(cd), \quad (ab)(ef), \quad (cd)(ef), \quad (ab)(cd)(ef);$$

$$\mathfrak{B}: \quad 1, \quad (ac)(bd), \quad (ae)(bf), \quad (ce)(df),$$
$$(ace)(bdf), \quad (acc)(bfd),$$
$$(ac)(bd)\cdot(ab)\cdot(ac)(bd)=(cd),$$
$$(ae)(bf)\cdot(ab)\cdot(ae)(bf)=(ef),$$

$$(ce)(df)\cdot(ab)\cdot(ce)(df)=(ab).$$

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)　　$G_0, G_1, \cdots\cdots, G_{g-1}$　$(G_0 = 1)$,

而作$\mathfrak{G}$之正置換表示

(2)　$\begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ G_0G_i & G_1G_i & \cdots\cdots & G_{g-1}G_i \end{pmatrix}$,　$i = 0, 1, 2, \cdots\cdots, g-1.$

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 $\mathfrak{G}$ 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 $\mathfrak{G}$ 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 $\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}$ 焉.

†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

$$(2)\qquad \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_0G_i & G_1G_i & G_2G_i & G_3G_i & G_4G_i & G_5G_i \end{pmatrix},\quad i=0,1,2,3,4,5$$

則與此羣同值．與此羣之置換爲交換可能之置換，由定理爲

$$(3)\qquad \begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_jG_0 & G_jG_1 & G_jG_2 & G_jG_3 & G_jG_4 & G_jG_5 \end{pmatrix},\quad j=0,1,2,3,4,5.$$

此各個用上之乘法表而計算之，則爲

$$\begin{pmatrix} G_r \\ G_0G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \end{pmatrix}=1,$$

$$\begin{pmatrix} G_r \\ G_1G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_1 & G_2 & G_0 & G_4 & G_5 & G_3 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_2G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_2 & G_0 & G_1 & G_5 & G_3 & G_4 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_3G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_3 & G_5 & G_4 & G_0 & G_2 & G_1 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_4G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_4 & G_3 & G_5 & G_1 & G_0 & G_2 \end{pmatrix},$$

$$\begin{pmatrix} G_r \\ G_5G_r \end{pmatrix}=\begin{pmatrix} G_0 & G_1 & G_2 & G_3 & G_4 & G_5 \\ G_5 & G_4 & G_3 & G_2 & G_1 & G_0 \end{pmatrix}.$$

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) $$G_0,\ G_1,\ G_2,\ \cdots\cdots,\ G_{g-1}\ (G_0=1).$$

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) $$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}S_1G_i & \cdots\cdots & \mathfrak{H}S_{n-1}G_i \end{pmatrix},\ i=0, 1, 2, \cdots\cdots, g-1,$$

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 $(\mathfrak{G})$ 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 $(\mathfrak{G})$ 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 $\mathfrak{G}$ 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$\mathfrak{H}$之爲交換可能爲必要也.

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$\mathfrak{H}$之正常化羣爲$\mathfrak{N}$，而就$\mathfrak{H}$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$\mathfrak{H}$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$\mathfrak{K}$之元素. 若

$$\mathfrak{K} = \mathfrak{H} + \mathfrak{H}T_1 + \cdots\cdots + \mathfrak{H}T_{m-1},$$

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$\mathfrak{K}$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$\mathfrak{K}$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

$$\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}H_iT_jS_r\end{pmatrix}=\begin{pmatrix}\mathfrak{H}S_r\\ \mathfrak{H}T_jS_r\end{pmatrix}.$$

故對$\mathfrak{R}$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$\mathfrak{R}$與$(\mathfrak{P})$爲h重同態, 而對$(\mathfrak{P})$之不動置換, $\mathfrak{R}$之約羣$\mathfrak{H}$相與對應. 於是$(\mathfrak{P})$與$\mathfrak{R}/\mathfrak{H}$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$\mathfrak{R}/\mathfrak{H}$爲單純同態之羣. 但$\mathfrak{R}$乃示$\mathfrak{H}$之正常化羣者.

92. 羣$(\mathfrak{P})$之可遷性及非遷性.

令$\mathfrak{G}$, $(\mathfrak{G})$, $\mathfrak{H}$, $\mathfrak{R}$, $(\mathfrak{P})$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$\mathfrak{R}$與$\mathfrak{G}$一致. 故羣$(\mathfrak{P})$, 由第90節定理, 爲

$$\textbf{(13)}\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}G_j & \mathfrak{H}G_jS_1 & \cdots\cdots & \mathfrak{H}G_jS_{n-1}\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ g-1,$$

或

$$\textbf{(13')}\quad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{m-1}\\ G_j\mathfrak{H} & G_j\mathfrak{H}S_1 & \cdots\cdots & G_j\mathfrak{H}S_{n-1}\end{pmatrix},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ g-1$$

於(13)取S_0, S_1, $\cdots\cdots$, S_{n-1}以爲U_j, 則$\mathfrak{H}$得分別爲$\mathfrak{H}$, $\mathfrak{H}S_1$, $\cdots\cdots$,

$\mathfrak{H}S_{n-1}$ 所置換. 故羣$(\mathfrak{P})$爲可遷的.

又因$\mathfrak{N}=\mathfrak{G}$, 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$\mathfrak{N}$與$\mathfrak{H}$不一致時.

將$\mathfrak{N}$就$\mathfrak{H}$分爲傍系, 乃與前同樣以之爲

$$\mathfrak{N}=\mathfrak{H}+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{m-1};\tag{10}$$

次以$\mathfrak{G}$就$\mathfrak{N}$分爲傍系, 以之爲

$$\mathfrak{G}=\mathfrak{N}+\mathfrak{N}U_1+\cdots\cdots+\mathfrak{N}U_{l-1}.\tag{14}$$

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

$$\begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K' & \mathfrak{H}T_1K' & \cdots\cdots & \mathfrak{H}T_{m-1}K'\end{pmatrix}\quad [K'爲\mathfrak{R}之任意元素].$$

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:

$$(17)\qquad \begin{pmatrix}\mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1}\\ \mathfrak{H}K & \mathfrak{H}KS_1 & \cdots\cdots & \mathfrak{H}KS_{n-1}\end{pmatrix}$$
$$=\begin{pmatrix}\mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}K & \mathfrak{H}KT_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}\end{pmatrix}\begin{pmatrix}\mathfrak{H}U_1 & \mathfrak{H}T_1U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1\\ \mathfrak{H}KU_1 & \mathfrak{H}KT_1U_1 & \cdots\cdots & \mathfrak{H}KT_{m-1}U_1\end{pmatrix}\cdots$$
$$\cdots\begin{pmatrix}\mathfrak{H}U_{l-1} & \mathfrak{H}T_1U_{l-1} & \cdots\cdots & \mathfrak{H}T_{m-1}U_{l-1}\\ \mathfrak{H}KU_{l-1} & \mathfrak{H}KT_1U_{i-1} & \cdots\cdots & \mathfrak{H}KT_{m-1}U_{l-1}\end{pmatrix}.$$

以故若$\mathfrak{R}$之元素表以

$$K_0,\ K_1,\ \cdots\cdots,\ K_{k-1}\quad (K_0=$$

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:

$$(21)\quad \begin{cases} \mathfrak{H} & \mathfrak{H}T_1 & \cdots\cdots & \mathfrak{H}T_{m-1}\\ \mathfrak{H}U_1 & \mathfrak{H}T_1U_1 & \cdots\cdots & \mathfrak{H}T_{m-1}U_1\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \mathfrak{H}U_{l-1} & \mathfrak{H}T_1U_{l-1} & \cdots\cdots & \mathfrak{H}T_{m-1}U_{l-1}, \end{cases}$$

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. 卽$\mathfrak{H}$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, $(\mathfrak{P})=1$.

$m>1$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卽得.

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

$$\begin{aligned}\mathfrak{G}&=\mathfrak{N}+\mathfrak{N}U_1+\cdots\cdots+\mathfrak{N}U_{l-1}\\&=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{m-1}\\&\quad+\mathfrak{H}U_1+\mathfrak{H}S_1U_1+\cdots\cdots+\mathfrak{H}S_{m-1}U_1\\&\quad+\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\&=\mathfrak{H}U_{l-1}+\mathfrak{H}S_1U_{l-1}+\cdots\cdots+\mathfrak{H}S_{m-1}U_{l-1},\end{aligned}$$

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$\mathfrak{H}$, $\mathfrak{H}S_1$, $\cdots\cdots$,

$\mathfrak{H}S_{m-1}$, 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

$$\begin{array}{ll} 1 & Q=(a_1a_5)(a_2a_4) \\ P=(aa_1a_2a_3a_4a_5) & PQ=(aa_5)(a_1a_4)(a_2a_3) \\ P^2=(aa_2a_4)(a_1a_3a_5) & P^2Q=(aa_4)(a_1a_3) \\ P^3=(aa_3)(a_1a_4)(a_2a_5) & P^3Q=(aa_3)(a_1a_2)(a_4a_5) \\ P^4=(aa_4a_2)(a_1a_5a_3) & P^4Q=(aa_2)(a_3a_5) \\ P^5=(aa_5a_4a_3a_2a_1) & P^5Q=(aa_1)(a_2a_5)(a_3a_4). \end{array}$$

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
$$\begin{aligned}\mathfrak{G}&=\mathfrak{K}+\mathfrak{K}P+\mathfrak{K}P^2\\&=(\mathfrak{H}+\mathfrak{H}P^3)+(\mathfrak{H}P+\mathfrak{H}P^4)+(\mathfrak{H}P^2+\mathfrak{H}P^5).\end{aligned}$$

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$(\mathfrak{P})$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

$$1,\ (\mathfrak{H}(012)(345),\ \mathfrak{H}(042)(153))$$

及第三因子

$$1,\ (\mathfrak{H}(021)(354),\ \mathfrak{H}(054)(132))$$

以之相乘,得

$$1,\ (\mathfrak{H},\ \mathfrak{H}(03)(14)(\mathfrak{H}(012)(345),\ \mathfrak{H}(042)(153))$$

$$\times\big(\mathfrak{S}(021)(354),\ \mathfrak{S}(054)(132)\big).$$

再於此代傍系以文字,得

$$1,\quad (03)(14)(25).$$

是卽與$\mathfrak{S}$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

$$\mathfrak{S} \quad : \quad 1, (abc), (acb), (bc), (ca), (ab);$$

$$(abc)^{-1}\,\mathfrak{S}\,(abc): \quad 1, (abc), (acb), (ca), (ab), (bc);$$

$(acb)^{-1}\,\mathfrak{S}\,(acb)$: 1, (abc), (acb), (ab), (bc), (ca);

$(bc)^{-1}\,\mathfrak{S}\,(bc)$: 1, (acb), (abc), (bc), (ab), (ca);

$(ca)^{-1}\,\mathfrak{S}\,(ca)$: 1, (acb), (abc), (ab), (ca), (bc);

$(ab)^{-1}\,\mathfrak{S}\,(ab)$: 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$\mathfrak{S}$若爲Abel氏羣,是乃一特例. 此時$G^{-1}G_iG=G_i$, 因之$\begin{bmatrix}G_r\\G^{-1}G_rG\end{bmatrix}$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 $(\mathfrak{L})$,則

$$(1)\quad (\mathfrak{H})=(\mathfrak{L})+(\mathfrak{L})\begin{pmatrix} G_r \\ G_rG_1 \end{pmatrix}+\cdots\cdots+(\mathfrak{L})\begin{pmatrix} G_r \\ G_rG_{g-1} \end{pmatrix}.$$

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，$(\mathfrak{F})$之置換與$(\mathfrak{G})$爲交換可能，故$\begin{pmatrix} \overline{G}_r \\ \overline{G_rG_i} \end{pmatrix}$不得不屬於$(\mathfrak{G})$也. 即

$$\begin{pmatrix} \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \\ \overline{G_0G_i} & \overline{G_1G_i} & \cdots\cdots & \overline{G_{g-1}G_i} \end{pmatrix} = \begin{pmatrix} \overline{G}_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0A_i & \overline{G}_1A_i & \cdots\cdots & \overline{G}_{g-1}A_i \end{pmatrix},$$

$$i=0, 1, 2, \cdots\cdots, g-1,$$

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 $(\mathfrak{F})$ 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)，

$$(\mathfrak{F})=(\mathfrak{Q})(\mathfrak{G}).$$

是卽定理之所主張也．

定理．若 $(\mathfrak{F})$ 爲羣 $\mathfrak{G}$ 之內同態羣，則商 $\dfrac{(\mathfrak{G})(\mathfrak{Q})}{(\mathfrak{G})(\mathfrak{F})}$ 與 $\dfrac{(\mathfrak{Q})}{(\mathfrak{F})}$ 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，$\dfrac{(\mathfrak{G})(\mathfrak{F})}{(\mathfrak{G})}$ 與 $(\mathfrak{F})$ 爲單純同態．故

$$\frac{\dfrac{(\mathfrak{G})(\mathfrak{L})}{(\mathfrak{G})}}{\dfrac{(\mathfrak{G})(\mathfrak{H})}{(\mathfrak{G})}} \sim \frac{(\mathfrak{L})}{(\mathfrak{H})}$$ [~爲單純同態之記號].

然由第46節第二定理系2,

$$\frac{\dfrac{(\mathfrak{G})(\mathfrak{L})}{(\mathfrak{G})}}{\dfrac{(\mathfrak{G})(\mathfrak{H})}{(\mathfrak{G})}} \sim \frac{(\mathfrak{G})(\mathfrak{L})}{(\mathfrak{G})(\mathfrak{H})},$$

$$\therefore \quad \frac{(\mathfrak{G})(\mathfrak{L})}{(\mathfrak{G})(\mathfrak{H})} \sim \frac{\mathfrak{L}}{\mathfrak{H}}.$$

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$\overline{\mathfrak{G}}$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$(\mathfrak{L})$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$(\mathfrak{L})$,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.　$(\mathfrak{F})=(\mathfrak{L})(\mathfrak{G}')$.

99. 全形之可遷重複度.

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$(\mathfrak{L})$也. 故

$$(\mathfrak{F})=(\mathfrak{L})+(\mathfrak{L})\left(\frac{G_r}{G_rG_1}\right)+\cdots\cdots+(\mathfrak{L})\left(\frac{G_r}{G_rG_{g-1}}\right).$$

1°. $(\mathfrak{F})$爲二重可遷時

此時$(\mathfrak{L})$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$(\mathfrak{L})$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$(\mathfrak{L})$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(𝔖)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(𝔖)爲二重可遷, 故(𝔖)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(𝔖)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,……, $p-1$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

$$\{A^{\alpha}\}=\{A\},$$

而由是自明耳. 以故 $\{A\}$ 之同態羣之置換,得以

$$(2)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^{\alpha} & A^{2\alpha} & \cdots\cdots & A^{(p-1)\alpha} \end{pmatrix},\quad (\alpha=1,2,\cdots\cdots,p-1)$$

與之也. 此羣以 $(\mathfrak{L})$ 表之.

欲明 $(\mathfrak{L})$ 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

$$(5)\quad \begin{pmatrix} A^0 & A & A^2 & \cdots\cdots & A^{p-1} \\ A^0 & A^{\alpha} & A^{2\alpha} & \cdots\cdots & A^{(p-1)\alpha} \end{pmatrix}=\begin{pmatrix} A^0 & A & A^{\rho} & A^{\rho^2} & \cdots\cdots & A^{\rho^{p-2}} \\ A^0 & A^{\alpha} & A^{\alpha\rho} & A^{\alpha\rho^2} & \cdots\cdots & A^{\alpha\rho^{p-2}} \end{pmatrix}$$

$$\alpha=1,\ 2,\ \cdots\cdots,\ p-1.$$

---

*設 α 爲不能以 p 整除之整數. 於是由 Fermat 氏定理,

$$\alpha^{p-1}\equiv 1\ (\mathrm{mod.}\ p).$$

故 α 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 α^d 時,卽

$$\alpha^d\equiv 1\ (\mathrm{mod.}\ p.),\ \alpha^x\not\equiv 1\ (\mathrm{mod.}\ p)\ [0<x<d]$$

時,則 d 名曰 α 對法 p 之所屬之指數. 此指數恰與 $p-1$ 等者常存在. 若 α 所屬之指數等於 $p-1$ 時,則 α 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

$$(6)\quad \begin{pmatrix} A^0 & A & A^{\rho} & A^{\rho^2} & \cdots\cdots & A^{\rho^{p-2}} \\ A^0 & A^{\rho^s} & A^{\rho^{1+s}} & A^{\rho^{2+s}} & \cdots\cdots & A^{\rho^{p-2+s}} \end{pmatrix} (s=0, 1, 2, \cdots\cdots, p-2).$$

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

$$(7)\qquad Q^0, Q, Q^2, \cdots\cdots, Q^{p-2} \quad (Q^0=1, Q^{p-1}=1),$$

卽$p-1$次$p-1$元之巡回羣也. 因之,對$p-1$個元素$A, A^2, \cdots\cdots, A^{p-1}$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(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(𝔓)爲p元巡回羣之故，其置換得以

$$(10)\qquad P^0, P, P^2, \cdots\cdots, P^{p-1} \quad (P^0=1, P^p=1)$$

與之也. 以此乘於(𝔔)之置換(7)，則得$p(p-1)$個之積

$$(11)\qquad Q^i P^j \begin{cases} i=0,1,2,\cdots\cdots,p-2 \\ j=0,1,2,\cdots\cdots,p-1. \end{cases}$$

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(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(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

$$(14)\qquad x' \equiv ax+\beta \pmod{p.} \begin{cases} \alpha=1, 2, \cdots\cdots, p-1 \\ \beta=0, 1, 2, \cdots\cdots, p-1 \end{cases}$$

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 α 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, 卽三次亞巡回羣爲

$$1,\ (012),\ (021),\ (12),\ (01),\ (20).$$

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$\rho$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

$$(T^iS^j)(T^hS^k)=T^iT^hS^{j\rho^h}S^k,$$

$$(T_1{}^iS_1{}^j)(T_1{}^hS_1{}^k)=T_1{}^iT_1{}^hS_1{}^{j\rho^h}S_1{}^k.*$$

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

$$S^p=1,\ U^{p-1}=1,\ U^{-1}SU=S^\sigma, \tag{3}$$

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. 羣之全形之卽含其羣者.

在羣 $\mathfrak{G}$ 之全形中而卽以 $\mathfrak{G}$ 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[卽 $(\mathfrak{L})(\mathfrak{G})$], 而 $(\mathfrak{L})$ 之元數爲 l, 其置換爲

$$\binom{G_r}{G_r^{(0)}},\ \binom{G_r}{G_r^{(1)}},\ \cdots\cdots\ \binom{G_r}{G_r^{(l-1)}}\ [G_r^{(0)}=G_r]. \tag{1}$$

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

$$F_{ji}\cdot F_{qp}=F_{ut}$$

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．卽$\mathfrak{F}$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

$$L_j G_i=F_{ji}\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1. \end{cases}$$

因之,若將與(𝔔)對應之約羣(4)以𝔔表之,則得

$$(5)\qquad \mathfrak{F}=\mathfrak{Q}\mathfrak{G}.$$

更就(𝔔),(𝔊)之元素之關係而觀,如第98節所示,因

$$(6)\quad \begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}^{-1}\begin{pmatrix} G_r \\ G_rG_i \end{pmatrix}\begin{pmatrix} G_r \\ G_r^{(j)} \end{pmatrix}=\begin{pmatrix} G_r \\ G_rG_i^{(j)} \end{pmatrix}\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1 \end{cases}$$

之故,對於𝔉之元素之結合,由上所述之定義乃有

$$(7)\qquad L_j^{-1}G_iL_j=G_i^{(j)}\begin{cases} i=0,1,2,\cdots\cdots,g-1 \\ j=0,1,2,\cdots\cdots,l-1 \end{cases}$$

茲利用此關係,則𝔊之同態羣(𝔔)之置換,得換書之如次:

$$(8)\quad \begin{pmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ L_j^{-1}G_0L_j & L_j^{-1}G_1L_j & \cdots\cdots & L_j^{-1}G_{g-1}L_j \end{pmatrix},\ j=0,1,2,\cdots,l-1.$$

換言之,即𝔊之自己同態者,得以𝔔之各元素變𝔊之形而得者也.

夫如是,以𝔔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𝔔在𝔉與(𝔉)之單純同態關係上,乃爲與(𝔉)之約羣(𝔔)相對應者也.故當討論含𝔊之全形𝔉時,便宜上對於𝔔,與以與(𝔔)同一之名稱,而呼之曰同態羣;若兩者有區別之必要時,則(𝔔)名曰同態置換羣;而與(𝔔)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

$$\mathfrak{H}=\mathfrak{Q}\,\mathfrak{G}'=\mathfrak{G}'\,\mathfrak{Q},$$

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

$$J^{-1}G_iJ=G^{-1}G_iG\quad(i=0,1,2,\cdots\cdots,g-1).$$

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$A_0, A_1, \cdots\cdots, A_{a-1}$. 因$\mathfrak{A}$之元素與$\mathfrak{G}$爲交換可能,故置換

$$(9)\quad \begin{pmatrix} G_0 & G_1 & \cdots & G_{g-1} \\ A_j^{-1}G_0A_j & A_j^{-1}G_1A_j & \cdots & A_j^{-1}G_{g-1}A_j \end{pmatrix} \quad (j=0,1,2,\cdots,a-1)$$

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a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

$$\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix}\begin{pmatrix} G_i \\ G_rG_i \end{pmatrix}\cdot\begin{pmatrix} G_r \\ A_q^{-1}G_rA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_p \end{pmatrix}$$

$$=\begin{pmatrix} G_r \\ A_j^{-1}G_rA_j \end{pmatrix}\begin{pmatrix} G_r \\ G_q^{-1}G_rA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rA_q^{-1}G_iA_q \end{pmatrix}\begin{pmatrix} G_r \\ G_rG_p \end{pmatrix}$$ [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)　　$H_0, H_1, \cdots\cdots, H_{h-1}$

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)　　$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ L_j^{-1}G_0L_j & L_j^{-1}G_1L_j & \cdots\cdots & L_j^{-1}G_{g-1}L_j \end{bmatrix}$

中，$\mathfrak{H}$ 之元素(1)乃分別與

(3)　　$L_j^{-1}H_0L_j, L_j^{-1}H_1L_j, \cdots\cdots, L_j^{-1}H_{h-1}L_j$

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,卽在

$$L_j^{-1}\mathfrak{H}L_j=\mathfrak{H}\quad(j=0,1,2,\cdots\cdots,l-1)$$

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)　$\mathfrak{G}, \mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots, \mathfrak{C}_{\mu-1}, 1,$

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)　$\mathfrak{H}, \mathfrak{H}_1, \cdots\cdots, \mathfrak{H}_\lambda, \mathfrak{G}, \mathfrak{C}_1, \mathfrak{C}_2, \cdots\cdots, \mathfrak{C}_{\mu-1}, 1$

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) $\mathfrak{G}, \mathfrak{E}_1', \mathfrak{C}_2', \cdots\cdots, \mathfrak{C}'_{\nu-1}, 1$

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

$$(2)\qquad (T^{\beta}S^{\alpha})^{-1}(S\backslash)(T^{\beta}S^{\alpha})=S^{-\alpha}\cdot T^{-\beta}S^{\lambda}T^{\beta}\cdot S^{\alpha}$$
$$=S^{-\alpha}S\backslash\rho^{\beta}S^{\alpha}=S\backslash\rho^{\beta}$$

(參照第 101 節中之脚注). 然此, 由 (1) 之第三條件, 得與 S^{ρ} 對應.

故 $$S\backslash\rho^{\beta}=S\backslash\rho$$

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

$$(TS^{\alpha})^{-1}(S\backslash)(TS^{\alpha})=(S\backslash)^{\rho}.$$

再就 TS^{α} 之巡回率而觀, 由 (1) 之第三條件,

$$(TS^{\alpha})^{2}=TS^{\alpha}TS^{\alpha}=TTS^{\alpha\rho}S^{\alpha}=T^{2}S^{\alpha(\rho+1)}$$
$$(TS^{\alpha})^{3}=T^{2}S^{\alpha(\rho+1)}TS^{\alpha}=T^{2}TS^{\alpha(\rho+1)\rho}S^{\alpha}=T^{3}S^{\alpha(\rho^{2}+\rho+1)}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(TS^{\alpha})^{m}=\cdots\cdots=T^{m}S^{\alpha(\rho^{m-1}+\rho^{m-2}+\cdots+\rho+1)}=T^{m}S^{\alpha\frac{(\rho^{m}-1)}{\rho-1}}$$

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

軛元素僅爲主元素. 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軛元素者之羣中,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軛元素. 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$\mathfrak{G}$無自己共軛元素,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

$$A^{-1}G_rA=G^{-1}G_rG \quad (r=0, 1, 2, \cdots\cdots, g-1).$$

$$\therefore\ (AG^{-1})^{-1}G_r(AG^{-1})=G_r \quad (r=0, 1, 2, \cdots\cdots, g-1),$$

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 $((\mathfrak{Q}))$ 示之. $((\mathfrak{Q}))$ 之含 $((\mathfrak{G}))$ 乃當然也,因之就傍系 (4) 言爲可遷的. 於 $((\mathfrak{Q}))$ 其令 $\mathfrak{H}$ 不動者之約羣以爲 $((\mathfrak{R}))$,則由第 63 節第四定理,得

(5) $\qquad ((\mathfrak{Q}))=((\mathfrak{R}))((\mathfrak{G})).$

故若 $((\mathfrak{R}))$ 得知,則 $((\mathfrak{Q}))$ 之置換自明.

茲試取 $((\mathfrak{R}))$ 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

$$\begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r \cdot G_iG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix} \cdot \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}^{-1} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ (\mathfrak{H}P_r)' \end{pmatrix}$$

$$= \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i' \end{pmatrix} \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j' \end{pmatrix} \qquad [\text{由 (9) 式}]$$

$$= \begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r \cdot G_i'G_j' \end{pmatrix},$$

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),

$$\begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H}G_i)' & (\mathfrak{H}P_1G_i)' & \cdots\cdots & (\mathfrak{H}P_{n-1}G_i)' \end{pmatrix}$$

$$= \begin{pmatrix} (\mathfrak{H})' & (\mathfrak{H}P_1)' & \cdots\cdots & (\mathfrak{H}P_{n-1})' \\ (\mathfrak{H})'G_i' & (\mathfrak{H}P_1)'G_i' & \cdots\cdots & (\mathfrak{H}P_{n-1})'G_i' \end{pmatrix},$$

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$\mathfrak{H}$, $\mathfrak{H}P_1$, ……, $\mathfrak{H}P_{n-1}$, 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'……, P'_{n-1}爲分別與P_1, P_2, ……, 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

$$\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}^{-1}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}$$

$$=\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_{r'}\end{pmatrix}^{-1}\begin{pmatrix}\mathfrak{H}P_r\\ \mathfrak{H}P_rG_i\end{pmatrix}\begin{pmatrix}\mathfrak{H}P_rG_i\\ \mathfrak{H}(P_rG_i)'\end{pmatrix}\quad\left[\begin{matrix}(P_rG_i)'\text{乃於(11)中與積}\\ P_rG_i\text{相對應者.}\end{matrix}\right]$$

$$=\begin{pmatrix}\mathfrak{H}P_{r'}\\ \mathfrak{H}(P_rG_i)'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_{r'}\\ \mathfrak{H}P_{r'}G_i'\end{pmatrix}=\begin{pmatrix}\mathfrak{H}P_s\\ \mathfrak{H}P_sG_i'\end{pmatrix},$$

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((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

$$(2)\quad \begin{pmatrix} \mathfrak{H} & \mathfrak{H}P_1 & \cdots\cdots & \mathfrak{H}P_{n-1} \\ \mathfrak{H}G_i & \mathfrak{H}P_1G_i & \cdots\cdots & \mathfrak{H}P_{n-1}G_i \end{pmatrix} (i=0, 1, 2, \cdots\cdots, g-1).$$

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

$$(4)\quad \begin{pmatrix} \mathfrak{H}' & \mathfrak{H}'P'_1 & \cdots\cdots & \mathfrak{H}'P'_{n-1} \\ \mathfrak{H}'G_i' & \mathfrak{H}'P'_1G_i' & \cdots\cdots & \mathfrak{H}'P'_{n-1}G_i' \end{pmatrix} (i=0, 1, 2, \cdots\cdots, g-1)$$

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, $\mathfrak{H}$ 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,因之卽其關於$\mathfrak{H}$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

$$(6)\quad \begin{pmatrix} \bar{\mathfrak{H}} & \bar{\mathfrak{H}}\bar{P}_1 & \cdots\cdots & \bar{\mathfrak{H}}\bar{P}_{n-1} \\ \bar{\mathfrak{H}}\bar{G}_i & \bar{\mathfrak{H}}\bar{P}_1\bar{G}_i & \cdots\cdots & \bar{\mathfrak{H}}\bar{P}_{n-1}\bar{G}_i \end{pmatrix} \quad (i=0,\ 1,\ 2,\ \cdots\cdots,\ g-1),$$

則爲與表示(2)爲同值,卽於置換$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}$中,將傍系$\mathfrak{H}$, $\mathfrak{H}P_1$, ……, $\mathfrak{H}P_{n-1}$代以$\bar{\mathfrak{H}}$, $\bar{\mathfrak{H}}\bar{P}_1$, ……, $\bar{\mathfrak{H}}\bar{P}_{n-1}$遂成$\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_i \end{pmatrix}$者. 但$\bar{G}_0$, $\bar{G}_1$, ……, $\bar{G}_{g-1}$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

$$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_i \end{pmatrix}\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_j \end{pmatrix}=\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_iG_j \end{pmatrix},$$

$$\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_i \end{pmatrix}\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_j \end{pmatrix}=\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_i\bar{G}_j \end{pmatrix}.$$

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$\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_i \end{pmatrix}$對應則兩表示爲單純同態.故

$$(7)\qquad G_iG_j=G_k.$$

以故若

$$\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_r\cdot G_iG_j \end{pmatrix}=\begin{pmatrix} \mathfrak{H}P_r \\ \mathfrak{H}P_rG_k \end{pmatrix},$$

則由上式,

$$\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\cdot\bar{G}_i\bar{G}_j \end{pmatrix}=\begin{pmatrix} \bar{\mathfrak{H}}\bar{P}_r \\ \bar{\mathfrak{H}}\bar{P}_r\bar{G}_k \end{pmatrix}.$$

因之　　$\bar{\mathfrak{H}}\bar{P}_r\bar{G}_i\bar{G}_j=\bar{\mathfrak{H}}\bar{P}_r\bar{G}_k \quad (r=0,\ 1,\ 2,\ \cdots\cdots,\ n-1)$

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, 則

$$\begin{bmatrix} G_0 & G_1 & \cdots\cdots & G_{g-1} \\ \overline{G}_0 & \overline{G}_1 & \cdots\cdots & \overline{G}_{g-1} \end{bmatrix} \tag{10}$$

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

$$\left(\frac{\overline{\mathfrak{H}}\overline{\mathrm{P}}_r}{\overline{\mathfrak{H}}\overline{\mathrm{P}}_r\mathrm{H}_j}\right),\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1$$

亦不使$\overline{\mathfrak{H}}$動也. 是則

$$\overline{\mathfrak{H}}\,\overline{\mathrm{H}}_j=\overline{\mathfrak{H}},\quad j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1$$

爲必要矣. 以故$\overline{\mathrm{H}}_j$ $(j=0,\ 1,\ 2,\ \cdots\cdots,\ h-1)$均屬於$\overline{\mathfrak{H}}$. 而$\mathfrak{H}$與$\overline{\mathfrak{H}}$爲同元數$\left(h=\frac{g}{n}\right)$.

故

$$\overline{\mathfrak{H}}=\overline{\mathrm{H}}_0+\overline{\mathrm{H}}_1+\cdots\cdots+\overline{\mathrm{H}}_{h-1}.$$

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.

第 三 篇

合 同 羣

第十七章 母式之合同乘法

109. 母式.

將 n^2 個之文字 a_{ij} $(i, j=1, 2, \cdots\cdots, n)$ 括爲一起，而照次之樣式排列者，曰 n 次之**母式**.

$$(1) \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{pmatrix}$$

而由是所導出之行列式

$$(2) \qquad \begin{vmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{vmatrix}$$

曰母式(1)之**行列式**. (1)及(2)略記之，則分別令之爲

$$(a_{ij}), \quad |a_{ij}| \quad (i, j=1, 2, \cdots\cdots, n).$$

在同次之二母式 $(a_{ij}), (a'_{ij})$ 中，若其各項分別相等，即

$$a_{ij}=a'_{ij} \quad (i, j=1, 2, \cdots\cdots, n)$$

時，則兩者名曰相等.

母式中特別如

$$\begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & 1 \end{pmatrix}$$

者，名曰**主母式**. 若令

$$e_{ij}=\begin{cases} 1 & (i=j) \\ 0 & (i\neq j), \end{cases}$$

則主母式得以

$$(e_{ij}) \quad (i, j=1, 2, \cdots\cdots, n)$$

表之；而

$$\begin{pmatrix} \lambda_1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & \lambda_n \end{pmatrix}$$

則得以

$$(\lambda_i e_{ij}) \quad (i, j=1, 2, \cdots\cdots, n)$$

表之. 此名曰**倍乘母式**，其 $\lambda_1, \lambda_2, \cdots\cdots, \lambda_n$ 名曰**倍乘數**. 特別在 $\lambda_1=\lambda_2=\cdots\cdots=\lambda_n=\lambda$ 時，則此 (λe_{ij}) 名曰**相似母式**.

由母式(1)及

$$(3)\qquad \begin{pmatrix} b_{11} & b_{12} & \cdots\cdots & b_{1n} \\ b_{21} & b_{22} & \cdots\cdots & b_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ b_{n1} & b_{n2} & \cdots\cdots & b_{nn} \end{pmatrix}$$

以作一第三母式

$$(4)\qquad \begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots\cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots\cdots & a_{2n}+b_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1}+b_{n1} & a_{n2}+b_{n2} & \cdots\cdots & a_{nn}+b_{nn} \end{pmatrix}$$

或略記爲

$$(a_{ij}+b_{ij})\quad (i, j=1, 2, \cdots\cdots, n)$$

者,曰加母式(3)於(1)而(4)曰其和. 表之如次:

$$(a_{ij})+(b_{ij})=(a_{ij}+b_{ij})$$

復次由母式(1)及(3),用

$$(5)\qquad c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots\cdots+a_{in}b_{nj}$$
$$(i, j=1, 2, \cdots\cdots, n)$$

之關係以導出母式

$$(6)\qquad \begin{pmatrix} c_{11} & c_{12} & \cdots\cdots & c_{1n} \\ c_{21} & c_{22} & \cdots\cdots & c_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ c_{n1} & c_{n2} & \cdots\cdots & c_{nn} \end{pmatrix}$$

則此名曰右乘(3)於母式(1)而(6)曰其積. 表之如次

$$(a_{ij})(b_{ij})=(c_{ij}).$$

由(5), 則母式之積之行列式, 等於各因子之行列式之積甚明. 卽

$$|a_{ij}|\cdot|b_{ij}|=|c_{ij}|$$

特別, 乘(λe_{ij})於母式(1)時則此以$(a_{ij})\lambda$表之.

卽

$$(a_{ij})\lambda=(a_{ij})(\lambda e_{ij})=\left(\sum_{s=1}^{n}\lambda a_{is}e_{sj}\right)=(\lambda a_{ij}).$$

又二母式(a_{ij}), $(\bar{a}_{ij})$之積等於主母式時, 則$(\bar{a}_{ij})$名曰(a_{ij})之逆母式, 而以$(a_{ij})^{-1}$表之. 母式(a_{ij})欲有其逆, 則其行列式不能爲零爲必要也. 蓋若令

$$(a_{ij})(\bar{a}_{ij})=(e_{ij}), \tag{7}$$

則由上述, 得

$$|a_{ij}|\cdot|\bar{a}_{ij}|=|e_{ij}|=1,$$

因之

$$|a_{ij}|\neq 0$$

故. 反之, 在此時, 母式(a_{ij})乃有其逆. 蓋$|a_{ij}|\neq 0$時, 則能滿足聯立方程式

$$\sum_{k=1}^{n}a_{ik}\bar{a}_{kj}=e_{ij}\quad(i=1, 2, \cdots\cdots, n) \tag{8}$$

者之n個數

$$\bar{a}_{1j}, \bar{a}_{2j}, \cdots\cdots, \bar{a}_{nj}$$

得以決定. 復於(8), 令 $j=1, 2, \cdots\cdots, n$, 卽得滿足

$$\sum_{k=1}^{n} a_{ik}\bar{a}_{kj}=e_{ij}$$

者之 n^2 個數 $\bar{a}_{ij}$ $(i, j=1, 2, \cdots\cdots, n)$, 而其所作之母式 $(\bar{a}_{ij})$ 滿足(7)焉. 且滿足(8)之 $\bar{a}_{ij}$ 之值只一組, 故 (a_{ij}) 之逆亦唯一個.

此外則由加法, 乘法之定義, 其組合法則

$$\{(a_{ij})+(b_{ij})\}+(c_{ij})=(a_{ij})+\{(b_{ij})+(c_{ij})\},$$

$$\{(a_{ij})(b_{ij})\}(c_{ij})=(a_{ij})\{(b_{ij})(c_{ij})\}$$

以及分配法則

$$\{(a_{ij})+(b_{ij})\}(c_{ij})=(a_{ij})(c_{ij})+(b_{ij})(c_{ij})$$

之得成立, 明也.

注意. n 次母式中, 其有其逆者相集, 成羣也, 此時主母式乃爲羣之主元素. 以故若 $(a_{ij})(\bar{a}_{ij})=1$, 則 $(\bar{a}_{ij})(a_{ij})=1$ (第18節參照).

110. 母式之合同, 乘法之一意的條件.

試取各項皆爲整數之母式

(1) (l_{ij}) $(i, j=1, 2, \cdots\cdots, n)$.

若各項皆爲整數之兩母式*

(2) (a_{ij}) $(i, j=1, 2, \cdots\cdots n)$

*本篇所論, 僅及各項皆爲整數之母式.

及

(3)　　(a'_{ij})　$(i, j=1, 2, \cdots\cdots n)$

對於母式(1)有

(4)　　$a_{ij}\equiv a'_{ij}$　(mod. l_{ij})　$(i, j=1, 2, \cdots\cdots, n)$

之關係時，則曰此兩母式關於法(l_{ij})爲合同，而以

(5)　　$(a_{ij})\equiv(a'_{ij})$　(mod. (l_{ij}))

表之．如

$$\begin{pmatrix}-2 & 5\\ 8 & 1\end{pmatrix}\equiv\begin{pmatrix}5 & 2\\ 3 & 1\end{pmatrix}\quad\left(\text{mod. }\begin{pmatrix}7 & 3\\ 5 & 2\end{pmatrix}\right),$$

$$\begin{pmatrix}10 & 1\\ -4 & 3\end{pmatrix}\equiv\begin{pmatrix}3 & 4\\ 1 & 1\end{pmatrix}\quad\left(\text{mod. }\begin{pmatrix}7 & 3\\ 5 & 2\end{pmatrix}\right)$$

者是．特別在

$$a_{ij}\equiv 0\quad(\text{mod. } l_{ij})\quad(i, j=1, 2, \cdots\cdots, n)$$

時，則曰母式(a_{ij})關於法(l_{ij})與零合同，而以

$$(a_{ij})\equiv 0\quad(\text{mod. } (l_{ij}))$$

表之焉．

就法母式言，特別在(l_{ij})之各項皆等於同一數(如l)時，則(5)中兩母式(a_{ij})，(a'_{ij})曰關於法l爲合同，而以

$$(a_{ij})\equiv(a'_{ij})\quad(\text{mod. } l)$$

表之，如

$$\begin{pmatrix}5 & 2\\ 3 & 1\end{pmatrix}\equiv\begin{pmatrix}2 & -1\\ 0 & 1\end{pmatrix}\quad(\text{mod. } 3)$$

者是．復次將前例之兩邊各各相乘，乃有

$$\begin{pmatrix}-2 & 5\\ 8 & 1\end{pmatrix}\begin{pmatrix}10 & 1\\ -4 & 3\end{pmatrix}=\begin{pmatrix}-40 & 13\\ 76 & 11\end{pmatrix}\equiv\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}\quad\left(\text{mod.}\begin{pmatrix}7 & 3\\ 5 & 2\end{pmatrix}\right),$$

$$\begin{pmatrix}5 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 4\\ 1 & 1\end{pmatrix}=\begin{pmatrix}17 & 22\\ 10 & 13\end{pmatrix}\equiv\begin{pmatrix}3 & 1\\ 0 & 1\end{pmatrix}\quad\left(\text{mod.}\begin{pmatrix}7 & 3\\ 5 & 2\end{pmatrix}\right),$$

因之

$$\begin{pmatrix}-2 & 5\\ 8 & 1\end{pmatrix}\begin{pmatrix}10 & 1\\ -4 & 3\end{pmatrix}\not\equiv\begin{pmatrix}5 & 2\\ 3 & 1\end{pmatrix}\begin{pmatrix}3 & 4\\ 1 & 1\end{pmatrix}\quad\left(\text{mod.}\begin{pmatrix}7 & 3\\ 5 & 2\end{pmatrix}\right).$$

夫如是,則關於合同之乘法,一般非一意的*也. 爲要一意的起見,則法以及他兩母式之間.須有特殊之關係在.

定理. *n次母式$(a_{ij}),(b_{ij})$之積,爲要與他母式之關於法(l_{ij}),於此各各爲合同者之積相合同(法(l_{ij}))起見,則*

$$l_{ij}\,l_{jk}\equiv 0,\ a_{ij}\,l_{jk}\equiv 0,\ l_{ij}\,b_{jk}\equiv 0\ (\text{mod. } l_{ik})$$

$$(i, j, k=1, 2, \cdots\cdots, n)$$

爲必要而且充分.

證明. 試取關於法(l_{ij})與$(a_{ij}),(b_{ij})$分別相合同之任意母式$(a'_{ij}),(b'_{ij})$,則有

$$a'_{ij}=a_{ij}+x_{ij}\,l_{ij},\quad b'_{ij}=b_{ij}+y_{ij}\,l_{ij}$$

$$(i, j=1, 2, \cdots\cdots, n).$$

但x_{ij}, y_{ij}爲任意之整數. 而

$$\sum_{j=1}^{n} a'_{ij}b'_{jk}=\sum_{j}(a_{ij}+x_{ij}l_{ij})(b_{jk}+y_{jk}l_{jk})$$

*關於一意的之意義請參照第14節.

$$=\sum_j a_{ij}b_{jk}+\sum_j x_{ij}y_{jk}l_{ij}l_{jk}$$

$$+\sum_j a_{ij}l_{jk}y_{jk}+\sum_j x_{ij}l_{ij}b_{jk}.$$

故欲

$$(a'_{ij})(b'_{ij})\equiv(a_{ij})(b_{ij}) \pmod{(l_{ij})},$$

則對於任意之整數 x_{ij}, y_{ij},

$$(6)\qquad \sum_j x_{ij}y_{jk}l_{ij}l_{jk}+\sum_j a_{ij}l_{jk}y_{jk}+\sum_j x_{ij}l_{ij}b_{jk}$$

$$\equiv 0 \pmod{l_{ik}} \quad (i, k=1, 2, \cdots\cdots, n)$$

爲必要也,而此如成立,則復爲充分焉.

茲先以 x_{ij}, y_{ij} $(i, j=1, 2, \cdots\cdots, n)$ 之任意一 y_{jk} 置爲 1,其他全部皆置爲零,則由 (6) 得

$$(7)\qquad a_{ij}l_{jk}\equiv 0 \pmod{l_{ik}}.$$

次於 (6) 令 $x_{ij}=1$,而以其他爲零,則得

$$(8)\qquad l_{ij}b_{jk}\equiv 0 \pmod{l_{ik}}.$$

以 (7) 及 (8) 代入 (6) 得

$$\sum_{j=1}^{n} x_{ij}y_{jk}l_{ij}l_{jk}\equiv 0 \pmod{l_{ik}},$$

於此而令 $x_{ij}=y_{jk}=1$,其他 x, y 之值皆爲零,則得

$$(9)\qquad l_{ij}l_{jk}\equiv 0 \pmod{l_{ik}}.$$

反之,若 (7), (8) 及 (9) 成立,則 (6) 亦成立,因之關於法 (l_{ij}) 之乘法,遂爲一意的也.

系. 若 l 爲整數時,則關於法 l 之母式之乘法常爲一意的.

蓋因法母式(l_{ij})之各項皆等於l時,則定理之條件自能滿足故也.

定理. 對於n次母式之集合

$$(a_{ij}^{(1)}),\quad (a_{ij}^{(2)}),\quad (a_{ij}^{(3)}),\quad \cdots\cdots$$

中之任意二者,欲使其關於法(l_{ij})之乘法爲一意的,則次之條件爲必要. 卽母式之對應項

$$l_{ij},\ a_{ij}^{(1)},\ a_{ij}^{(2)},\ a_{ij}^{(3)},\ \cdots\cdots$$

之最大公約數若爲d_{ij},則

$$d_{ij}l_{jk}\equiv 0,\quad l_{ij}d_{jk}\equiv 0\quad (\mathrm{mod.}\ l_{ik})$$
$$(i, j, k=1, 2, \cdots\cdots, n).$$

反之,此條件若得滿足,則復爲充分. 但法母式(l_{ij}),爲能滿足前定理之條件(9)者.

證明. 集合中任意兩母式$(a_{ij}^{(s)})$, $(a_{ij}^{(t)})$之乘法(法(l_{ij}))須爲一意的之條件,由前定理乃爲

$$(9)\qquad l_{ij}l_{jk}\equiv 0\quad (\mathrm{mod.}\ l_{ik})$$

$$(10)\qquad a_{ij}^{(s)}l_{jk}\equiv 0,\ l_{ij}a_{jk}^{(t)}\equiv 0\quad (\mathrm{mod.}\ l_{ik}).$$

將(9)式乘以整數z,(10)之第一式乘以z_s,再令$s=1, 2, 3, \cdots\cdots$,然後以此所得之式相加.則得

$$(11)\qquad (zl_{ij}+z_1\,a_{ij}^{(1)}+z_2\,a_{ij}^{(2)}+\cdots\cdots)\,l_{jk}\equiv 0\quad (\mathrm{mod.}\ l_{ik}).$$

然由假設l_{ij}, $a_{ij}^{(1)}$, $a_{ij}^{(2)}$, $\cdots\cdots$之最大公約數爲d_{ij}. 故對於$z, z_1, z_2, \cdots\cdots$,能使

$$zl_{ij}+z_1\,a_{ij}^{(1)}+z_2\,a_{ij}^{(2)}+\cdots\cdots=d_{ij}$$

然而與以整數值也. 而對此諸值,(11)遂成爲

$$d_{ij}l_{jk}\equiv 0 \pmod{l_{ik}}, \tag{12}$$

同樣由(9)及(10)之第二式得

$$l_{ij}d_{jk}\equiv 0 \pmod{l_{ik}}. \tag{13}$$

反之,(12)及(13)成立時,則(10)當然滿足. 蓋因$a_{ij}^{(s)}$及$a_{jk}^{(t)}$分別爲d_{ij}及d_{jk}之倍數故也.

系 1. 若將l_{ij}及d_{ij}分爲素數之積:

$$l_{ij}=p^{m_{ij}}q^{n_{ij}}\cdots\cdots \quad (m_{ij},\ n_{ij},\ \cdots\cdots\geqq 0)$$

$$d_{ij}=p^{\mu_{ij}}q^{\nu_{ij}}\cdots\cdots \quad (\mu_{ij},\ \nu_{ij},\ \cdots\cdots\geqq 0),$$

則對定理中集合之母式,其關於法(l_{ij})之乘法使爲一意的之條件(必要而且充分者)乃爲

$$m_{ij}+m_{jk}\geqq m_{ik},\ n_{ij}+n_{jk}\geqq n_{ik},\ \cdots\cdots \tag{14}$$

$$\mu_{ij}\geqq \begin{cases} m_{ik}-m_{jk} \\ m_{kj}-m_{ki}, \end{cases} \qquad \nu_{ij}\geqq \begin{cases} n_{ik}-n_{jk} \\ n_{kj}-n_{ki} \end{cases}, \ \cdots\cdots \tag{15}$$

$$(i,\ j,\ k=1,\ 2,\ \cdots\cdots,\ n).$$

(但 $p, q, \cdots\cdots$ 爲互異之素數.)

證明. 由定理中之條件(9),

$$l_{ij}l_{jk}=p^{m_{ij}+m_{jk}}q^{n_{ij}+n_{ik}}\cdots\cdots\equiv 0 \pmod{p^{m_{ik}}q^{n_{ik}}\cdots\cdots}.$$

$$\therefore\quad m_{ij}+m_{jk}\geqq m_{ik},\ n_{ij}+n_{jk}\geqq n_{ik},\ \cdots\cdots.$$

次由條件(12),

$$d_{ij}l_{jk}=p^{\mu_{ij}+m_{jk}}q^{\nu_{ij}+n_{jk}}\cdots\cdots\equiv 0 \pmod{p^{m_{ik}}q^{n_{ik}}\cdots\cdots}.$$

$$\therefore\ \mu_{ij}+m_{jk}\geqq m_{ik},\ \nu_{ij}+n_{jk}\geqq n_{ik},\ \cdots\cdots.$$

$$\therefore\ \mu_{ij}\geqq m_{ik}-m_{jk},\ \nu_{ij}\geqq n_{ik}-n_{jk},\ \cdots\cdots.$$

是卽(15)之前半也. 又由(13),

$$l_{ij}d_{jk}=p^{m_{ij}+\mu_{jk}}q^{n_{ij}+\nu_{jk}}\cdots\cdots\equiv 0 \pmod{p^{m_{ik}}q^{n_{ik}}\cdots\cdots}.$$

$$\therefore\ m_{ij}+\mu_{jk}\geqq m_{ik},\ n_{ij}+\nu_{jk}\geqq n_{ik},\ \cdots\cdots.$$

$$\therefore\ \mu_{jk}\geqq m_{ik}-m_{ij},\ \nu_{jk}\geqq n_{ik}-n_{ij},\ \cdots\cdots.$$

將各項之添數變更之,得

$$\mu_{ij}\geqq m_{kj}-m_{ki},\ \nu_{ij}\geqq n_{kj}-n_{ki},\ \cdots\cdots,$$

此卽(15)之後半也.

系 2. 定理中法母式之項爲

$$l_{1j}=l_{2j}=\cdots\cdots=l_{nj}=l_j \quad (j=1, 2, \cdots\cdots, n)$$

時,則乘法須爲一意的之條件爲

$$l_jd_{jk}\equiv 0 \pmod{l_k} \quad (j, k=1, 2, \cdots\cdots, n).$$

蓋此時定理中之條件(9)及(12)自能滿足,而條件(13)亦自如上故也.

111. 含最多數之母式者之集合.

母式之集合適合前節第二定理之條件時,取其一母式(a_{ij}),則

$$a_{ij}=a_{ii}d_{ij} \quad (a_{ij}\text{爲整數}),$$

而a_{ij}又得就法l_{ij}而取之;以故d_{ij}愈小,則對a_{ij}得以賦與之值愈多,因之集合中便得較多之母式(互爲非合同者)也.

今取最小之正整數得以滿足前節之條件(12), (13)者以爲d_{ij}, 而以f_{ij}表之. 乃於母式(a_{ij}), 令

$$a_{ij}=a_{ij}f_{ij},$$

而對a_{ij}與以所有之整數值, 其所得母式之集合以$\mathfrak{M}_f$表之, 則$\mathfrak{M}_f$乃含關於法(l_{ij})之乘法爲一意的者之母式之最多數(互爲非合同者)者也.

f_{ij}之求法如次. 如前節第二定理系1中者然, 將l_{ij}分解爲素因數, 以之爲

$$l_{ij}=p^{m_{ij}}q^{n_{ij}}\cdots\cdots \quad (m_{ij}, n_{ij}\cdots\cdots\geqq 0).$$

再取$2n+1$個數

$$0,\ m_{i1}-m_{j1},\ m_{i2}-m_{j2},\ \cdots\cdots,\ m_{in}-m_{jn},$$
$$m_{1j}-m_{1i},\ m_{2j}-m_{2i},\ \cdots\cdots,\ m_{nj}-m_{ni}$$

中之最大者, 以之爲φ_{ij}. 於是

$$(1)\qquad \varphi_{ij}\geqq\begin{cases} m_{ik}-m_{jk} \\ m_{kj}-m_{ki}\end{cases}\quad (i, j, k=1, 2, \cdots\cdots, n).$$

次取$2n+1$個數

$$0,\ n_{i1}-n_{j1},\ n_{i2}-n_{j2},\ \cdots\cdots,\ n_{in}-n_{jn},$$
$$n_{1j}-n_{1i},\ n_{2j}-n_{2i},\ \cdots\cdots,\ n_{nj}-n_{ni}$$

中之最大者, 以之爲ψ_{ij}, 則

$$(2)\qquad \psi_{ij}\geqq\begin{cases} n_{ik}-n_{jk} \\ n_{kj}-n_{ki}\end{cases}\quad (i, j, k=1, 2, \cdots\cdots, n).$$

以下行以同樣之方法, 而令

(3) $$p^{\varphi_{ij}} q^{\psi_{ij}} \cdots\cdots = f_{ij},$$

則 f_{ij} 爲所求也. 而

(4) $$f_{ij} l_{jk} \equiv 0,\ l_{ij} f_{jk} \equiv 0 \pmod{l_{ik}}$$
$$(i, j, k = 1, 2, \cdots\cdots, n).$$

由上之決定方法,則

$$\varphi_{ii} = \psi_{ii} = \cdots\cdots = 0 \quad (i = 1, 2, \cdots\cdots, n)$$

甚明. 因之

(5) $$f_{ii} = 1 \quad (i = 1, 2, \cdots\cdots, n).$$

由是, $\mathfrak{M}_f$ 之含主母式 (e_{ij}) 可知也.

茲更就 f_{ij} $(i, j = 1, 2, \cdots\cdots, n)$ 間以及此與 l_{ij} 間之關係一言. 由 (1),

$$\varphi_{ij} \geqq 0,\ m_{ir} - m_{jr}; \qquad \varphi_{ij} \geqq 0,\ m_{rj} - m_{ri},$$
$$\varphi_{jk} \geqq 0,\ m_{jr} - m_{kr}; \qquad \varphi_{jk} \geqq 0,\ m_{rk} - m_{rj}.$$
$$\therefore\quad \varphi_{ij} + \varphi_{jk} \geqq 0,\ m_{ir} - m_{kr}; \quad \varphi_{ij} + \varphi_{jk} \geqq 0,\ m_{rk} - m_{ri}.$$

因之由 φ_{ik} 之決定方法,

(6) $$\varphi_{ij} + \varphi_{jk} \geqq \varphi_{ik} \qquad (i, j, k = 1, 2, \cdots\cdots, n).$$

同樣

(6) $$\psi_{ij} + \psi_{jk} \geqq \psi_{ik} \qquad (i, j, k = 1, 2, \cdots\cdots, n),$$
$$\cdots\cdots\cdots\cdots \qquad \cdots\cdots\cdots\cdots\cdots\cdots$$

故由 (3) 得

(7) $$f_{ij} f_{jk} \equiv 0 \pmod{f_{ik}}$$
$$(i, j, k = 1, 2, \cdots\cdots, n).$$

復次令母式 (l_{ij}) 爲能滿足前節定理系 1 之條件 (14) 者. 於是

$$m_{ij}+m_{jr}\geqq m_{ir},\quad m_{ri}+m_{ij}\geqq m_{rj}.$$

$$\therefore\quad m_{ij}\geqq m_{ir}-m_{jr},\quad m_{ij}\geqq m_{ri}-m_{rj},$$

而 $m_{ij}\geqq 0$. 故

(8)　$\varphi_{ij}\leqq m_{ij}\quad (i,j=1,2,\cdots\cdots,n)$.

同樣

(8)　$\psi_{ij}\leqq n_{ij}\quad (i,j=1,2,\cdots\cdots,n)$,

…… ……

因之由 (3),

(9)　$l_{ij}\equiv 0\pmod{f_{ij}}\quad (i,j=1,2,\cdots\cdots,n)$

由此關係,則 $\mathfrak{M}_f$ 之母式,與對 a_{ij} 賦以

$$0,1,2,\cdots\cdots,\frac{l_{ij}}{f_{ij}}-1$$

所得之母式之一相合同 (法 (l_{ij})) 可知也.

注意. 由 f_{ij} 之決定方法以及前節第二定理系 1,則其適合該節 (12), (13) 之 d_{ij}, 乃爲 f_{ij} 之倍數,明已. 卽

$$d_{ij}\equiv 0\pmod{f_{ij}}\qquad (i,j=1,2,\cdots\cdots,n).$$

故以 $(a_{ij}\ d_{ij})$ 形所表示之母式之集合爲含於 $\mathfrak{M}_f$ 也. 但 a_{ij} 爲整數.

112. 在前節所述之集合 $\mathfrak{M}_f$ 中,就其法母式之各項爲素數冪者一論. 卽 p 爲素數,而以

(1)　$l_{ij}=p^{m_{ij}}\qquad (i,j=1,2,\cdots\cdots,n)$.

法母式應滿足之條件，由第110節(14)爲

$$(2)\qquad m_{ij}+m_{jk}\geqq m_{ik}\qquad (i,j,k=1,2,\cdots\cdots,n).$$

其次，f_{ij} 由前節(3)爲

$$(3)\qquad f_{ij}=p^{\varphi_{ij}}\qquad (i,j=1,2,\cdots\cdots,n),$$

而 φ_{ij} 乃 $2n+1$ 個數

$$(4)\qquad \begin{matrix}0,\ m_{i1}-m_{j1},\ m_{i2}-m_{j2},\ \cdots\cdots,\ m_{in}-m_{jn},\\ m_{1j}-m_{1i},\ m_{2j}-m_{2i},\ \cdots\cdots,\ m_{nj}-m_{ni}\end{matrix}$$

中之最大者. 又由同節(5)，(6)，

$$(5)\qquad \varphi_{ii}=0\qquad (i=1,2,\cdots\cdots,n),$$

$$(6)\qquad \varphi_{ij}+\varphi_{jk}\geqq\varphi_{ik}\qquad (i,j,k=1,2,\cdots\cdots,n).$$

特別當

$$m_{1j}=m_{2j}=\cdots\cdots=m_{nj}=m_j\qquad (j=1,2,\cdots\cdots,n),$$

$$m_1\geqq m_2\geqq\cdots\cdots\geqq m_n$$

時，則(4)中最大數 φ_{ij} 爲

$$(7)\qquad \begin{cases}\varphi_{ij}=0 & (i\leqq j)\\ \varphi_{ij}=m_j-m_i & (i>j),\end{cases}$$

此時 $\mathfrak{M}_f$ 之母式，乃取次形焉：

$$(8)\qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots\cdots & a_{1n}\\ a_{21}p^{m_1-m_2} & a_{22} & a_{23} & \cdots\cdots & a_{2n}\\ a_{31}p^{m_1-m_3} & a_{32}p^{m_2-m_3} & a_{33} & \cdots\cdots & a_{3n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ a_{n1}p^{m_1-m_n} & a_{n2}p^{m_2-m_n} & a_{n3}p^{m_3-m_n} & \cdots\cdots & a_{nn}\end{pmatrix}$$

但 a_{ij} 爲整數.

又有一特例, 卽

$$l_{1j}=l_{2j}=\cdots\cdots=l_{nj}=l_j \qquad (j=1, 2, \cdots\cdots, n)$$

時, 由第 110 節第二定理系 2, 則 f_{jk} 爲滿足

$$l_j d_{jk}\equiv 0 \pmod{l_k} \tag{9}$$

者之 d_{jk} 之最小值也. 此外尙有一特例, 乃

$$l_1=l_2=\cdots\cdots=l_n,$$

卽法母式之各項咸相等時, 則

$$f_{ij}=1 \qquad (i, j=1, 2, \cdots\cdots, n).$$

蓋因適合 (9) 之 d_{jk} 之最小值爲 1 故. (此與第 110 節第一定理系中所述一致也.)

又有一特例, 卽

$$l_{11}=l_{22}=\cdots\cdots=l_{nn}=1$$

時, 於前節 (4) 令 $k=j$, 則得

$$f_{ij}\equiv 0 \pmod{l_{ij}}.$$

因之 $\mathfrak{M}_f$ 之母式遂皆與零母式

$$\begin{pmatrix} 0\ 0\ \cdots\cdots \\ 0\ 0\ \cdots\cdots \\ \cdots\cdots\cdots\cdots \end{pmatrix}$$

合同 (法 (l_{ij})) 也.

於集合 $\mathfrak{M}_f$, 若母式之次數以及法母式有明示之必要時, 則其以 n 次母式 (l_{ij}) 爲法之集合, 乃以 $\mathfrak{M}_f(n, l_{ij})$ 表之焉.

例. 試取 $\begin{pmatrix}9 & 15\\ 9 & 15\end{pmatrix}$ 以爲法母式. 依第110節第二定理系2之證明中所述,可知此能滿足爲法者之條件也. 今求與此相應之 f_{ij} 之值,乃由上述,知 f_{12}, f_{21} 分別爲適合

$$9d_{12}\equiv 0 \pmod{15}, \quad 15d_{21}\equiv 0 \pmod{9}$$

者之 d_{12}, d_{21} 之最小值,故得

$$f_{12}=5, \qquad f_{21}=3.$$

而由前節(5),

$$f_{11}=f_{22}=1.$$

因之關於法 $\begin{pmatrix}9 & 15\\ 9 & 15\end{pmatrix}$ 之乘法爲一意的者之母式之集合如次:

$$\begin{pmatrix}a_{11} & 5a_{12}\\ 3a_{21} & a_{22}\end{pmatrix}, \quad \begin{matrix}a_{11}=0, 1, \cdots\cdots, 8; \ a_{12}=0, 1, 2;\\ a_{21}=0, 1, 2, 3, 4; \ a_{22}=0, 1, \cdots\cdots, 14.\end{matrix}$$

第十八章 母式合同羣

113. 母式合同羣.

對於集合 $\mathfrak{M}_f(n, l_{ij})$ 之母式 (a_{ij}), 其滿足

$$(a_{ij})(\bar{a}_{ij})\equiv(e_{ij}) \pmod{(l_{ij})}$$

之母式 $(\bar{a}_{ij})$ 存在於 $\mathfrak{M}_f$ 時,則此母式名曰 (a_{ij}) 關於法 (l_{ij}) 之**逆母式**,而以 $(a_{ij})^{-1}$ 記之.

$\mathfrak{M}_f(n, l_{ij})$ 之母式中,有有此逆者,有無此逆者. 爰有

定理. 在屬於 $\mathfrak{M}_f(n, l_{ij})$ 之母式中,其關於法 (l_{ij}) 有逆

者,相集成羣. 但(l_{ij})則爲適合條件

$$l_{ij}\,l_{jk}\equiv 0 \pmod{l_{ik}} \quad (i, j, k=1, 2, \cdots\cdots, n)$$

者.

此羣名曰關於法(l_{ij})之母式合同羣.

證明. 於$\mathfrak{M}(n, l_{ij})$,其有逆者之母式之集合,以$\mathfrak{M}$表之.

(i) $\mathfrak{M}_f$中互爲非合同(法(l_{ij}))者之母式之數爲有限的. 故就$\mathfrak{M}_f$言亦復同樣.

(ii) 一般母式之乘法乃服從組合法則者.

(iii) 試取$\mathfrak{M}$中任意二母式$(\alpha_{ij}f_{ij})$, $(\beta_{ij}f_{ij})$,以之相乘而令其爲

$$(\alpha_{ij}f_{ij})(\beta_{ij}f_{ij})=(c_{ij}),$$

則

$$c_{ij}=\sum_{t=1}^{n}\alpha_{it}f_{it}\,\beta_{tj}f_{tj}.$$

然由第111節(7),

$$f_{it}f_{tj}\equiv 0 \pmod{f_{ij}}.$$

$$\therefore \quad c_{ij}\equiv 0 \pmod{f_{ij}}.$$

即

$$c_{ij}=\gamma_{ij}f_{ij} \quad (\gamma_{ij}\text{爲整數}).$$

故二母式之積(c_{ij})屬於$\mathfrak{M}_f$. 其次

$$(c_{ij})\{(\beta_{ij}f_{ij})^{-1}(\alpha_{ij}f_{ij})^{-1}\}\equiv\{(\alpha_{ij}f_{ij})(\beta_{ij}f_{ij})\}\{(\beta_{ij}f_{ij})^{-1}(\alpha_{ij}f_{ij})^{-1}\}$$
$$\equiv(e_{ij}) \pmod{(l_{ij})}.$$

故$\{(\beta_{ij}f_{ij})^{-1}(\alpha_{ij}f_{ij})^{-1}\}$,乃兩母式$(\alpha_{ij}f_{ij})$, $(\beta_{ij}f_{ij})$之積(c_{ij})之逆

(法(l_{ij}))也. 因之此積屬於$\mathfrak{M}$.

(iv) 若 $(\alpha_{ij}f_{ij})(\beta_{ij}f_{ij})\equiv(\alpha'_{ij}f_{ij})(\beta_{ij}f_{ij})\pmod{(l_{ij})}$,

則 $$(\alpha_{ij}f_{ij})\equiv(\alpha'_{ij}f_{ij})\pmod{(l_{ij})}.$$

蓋於前式之兩邊以$(\beta_{ij}f_{ij})^{-1}$右乘之,則由組合法則遂得後式故也.

由上記之四項,故$\mathfrak{M}$成羣焉.

復就羣$\mathfrak{M}$而觀,可知其含主母式(e_{ij}). (蓋因主母式屬於$\mathfrak{M}_f$,且其自身爲逆母式故.) 因之(e_{ij})在$\mathfrak{M}$中實司主元素之務者也. 但如後之實例所示,在屬於$\mathfrak{M}_f$者之母式所作之羣(就其關於法(l_{ij})之乘法言)中,其主元素不爲主母式者亦得存在焉. 若羣含有主母式,則其羣爲$\mathfrak{M}$之約羣. 蓋若羣$\mathfrak{G}$爲關於法(l_{ij})之乘法者含有主母式,則於此羣中,主母式之充主元素之任也甚明. 故由一般羣之定義,$\mathfrak{G}$之各元素,非有合乎本節開端所示之意義者之逆母式(法(l_{ij}))不可. 因之由羣$\mathfrak{M}$之定義,則其無論如何,不得不屬於$\mathfrak{M}$. 卽$\mathfrak{G}$乃$\mathfrak{M}$之約羣也, 要之,母式合同羣$\mathfrak{M}$,乃以主母式爲主元素者之羣(爲關於法(l_{ij})之乘法者)中之最大者焉.

至其關於n次母式(l_{ij})之母式合同羣$\mathfrak{M}$,乃與記$\mathfrak{M}_f$者同樣. 以$\mathfrak{M}(n, l_{ij})$表示之.

特別若

$$l_{ii}=1 \quad (i=1, 2, \cdots\cdots, n),$$

則如前節末所述,$\mathfrak{M}_f(n, l_{ij})$之母式,皆與零相合同(法$(l_{ij})$),

而此時，合同羣 $\mathfrak{M}(n, l_{ij})$ 僅由唯一個元素零(法(l_{ij}))，即

$$\begin{pmatrix} 0 & 0 & \cdots\cdots\cdots \\ 0 & 0 & \cdots\cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \end{pmatrix} \quad (\mathrm{mod.}\ (l_{ij}))$$

而成，故 $\mathfrak{M}=1$. 反之，若 $\mathfrak{M}(n, l_{ij})$ 之母式皆與零合同(法(l_{ij}))時，則

$$(e_{ij})\equiv 0 \quad (\mathrm{mod}, (l_{ij})).$$

$$\therefore \qquad 1\equiv 0 \quad (\mathrm{mod}.\ l_{ii}) \qquad (i=1, 2, \cdots\cdots, n).$$

因之　　$l_{11}=l_{22}=\cdots\cdots=l_{nn}=1$

爲必要也.

114. 定理. 令 n 次母式 (l_{ij}) 之第 s 行與第 t 行交換，同時第 s 列與第 t 列交換，其所得之母式以爲 (l'_{ij}). 於是其關於法 (l_{ij}) 之母式合同羣與關於法 (l'_{ij}) 之羣爲單純同態.

證明. 由假設

$$l'_{ss}=l_{tt}, \quad l'_{st}=l_{ts},$$

$$l'_{tt}=l_{ss}, \quad l'_{ts}=l_{st},$$

$$\left.\begin{aligned} l'_{sj}&=l_{tj} \\ l'_{tj}&=l_{sj} \end{aligned}\right\} \ (j\neq s, t), \qquad \left.\begin{aligned} l'_{is}&=l_{it} \\ l'_{it}&=l_{is} \end{aligned}\right\} \ (i\neq s, t),$$

$$l'_{ij}=l_{ij} \quad (i, j\neq s, t).$$

故由

$$l_{ij}l_{jk}\equiv 0 \quad (\mathrm{mod}.\ l_{ik}) \quad (i, j, k=1, 2, \cdots\cdots, n),$$

則　　$l'_{ij}l'_{jk}\equiv 0 \quad (\mathrm{mod}.\ l'_{ik}) \quad (i, j, k=1, 2, \cdots\cdots, n)$

之成立可知. 卽對於法母式之條件得以滿足者也.

其次令母式(f_{ij})之第s行與第t行交換. 其第s列與第t列交換, 乃以其所得者爲(f'_{ij}), 則與於l'_{ij}者同樣, 由

$$f_{ij}l_{jk}\equiv 0,\quad l_{ij}f_{jk}\equiv 0\quad (\mathrm{mod.}\ l_{ik})$$
$$(i, j, k=1, 2, \cdots\cdots, n)$$

得知

$$f'_{ij}l'_{jk}\equiv 0,\quad l'_{ij}f'_{jk}\equiv 0\quad (\mathrm{mod.}\ l'_{ik})$$
$$(i, j, k=1, 2, \cdots\cdots, n)$$

也. 又由f_{ij}之決定法, 可知f'_{ij}之爲能適合

$$d'_{ij}l'_{jk}\equiv 0,\ l'_{ij}d'_{jk}\equiv 0\ (\mathrm{mod.}\ l'_{ik})\ (i, j, k=1, 2, \cdots\cdots, n)$$

者之d'_{ij}之值(正整數)中之最小值者易明. 今乃以$(a'_{ij}f'_{ij})$形(a'_{ij}爲整數)所表示之母式之集合, 以$\mathfrak{M}'_f$表之, 則由上述, 可知$\mathfrak{M}'_f$者, 在關於法(l'_{ij})之乘法爲一意的者之母式之集合中, 爲含有最多數之母式者也. (若用前述之記號, 則$\mathfrak{M}'_f$不外乎$\mathfrak{M}_f(n, l'_{ij})$.) 茲取此集合之一母式$(a'_{ij}f'_{ij})$, 令其第$s$行與第$t$行交換, 第$s$列與第$t$列交換, 則其所得者之屬於$\mathfrak{M}_f$甚明. 蓋由是交換, (f_{ij})遂爲(f'_{ij})故. 依此交換所得之母式乃以$(a_{ij}f_{ij})$表之. 反之, 對於$\mathfrak{M}_f$之母式施以同樣之交換, 則可得屬於$\mathfrak{M}'_f$者. 於是$\mathfrak{M}'_f$之母式與$\mathfrak{M}_f$之母式之間, 一一對應遂告成立. 而如下所示, 對於$\mathfrak{M}'_f$之二母式之積, 乃有與其各個相對應者之母式($\mathfrak{M}_f$者)之積相與對應焉.

以$\mathfrak{M}_f$之母式(a_{ij}), (b_{ij})之積爲(c_{ij}), 而對此三者施以上

揭之交換，以其所得分別爲 (a'_{ij}), (b'_{ij}), (c'_{ij}). 於是

$$\sum_{j=1}^{n} a'_{ij}b'_{jk}=a'_{i1}b'_{1j}+\cdots\cdots+\overbrace{a'_{is}b'_{sj}+\cdots\cdots+a'_{it}b'_{tj}}+\cdots\cdots+a'_{in}b'_{nj}$$

$$=\sum_{j} a_{ij}b_{jk}=c_{ik}=c'_{ik} \quad (i,\ k\neq s,\ t),$$

$$\sum_{j} a'_{ij}b'_{js}=\sum_{j} a_{ij}b_{jt}=c_{it}=c'_{is} \quad (i\neq s,\ t),$$

$$\sum_{j} a'_{ij}b'_{jt}=\sum_{j} a_{ij}b_{js}=c_{is}=c'_{it} \quad (i\neq s,\ t).$$

$$\sum_{j} a'_{sj}b'_{jk}=\sum_{j} a_{tj}b_{jk}=c_{tk}=c'_{sk} \quad (k\neq s,\ t),$$

$$\sum_{j} a'_{tj}b'_{jk}=\sum_{j} a_{sj}b_{jk}=c_{sk}=c'_{tk} \quad (k\neq s,\ t),$$

$$\sum_{j} a'_{sj}b'_{jt}=\sum_{j} a_{tj}b_{js}=c_{ts}=c'_{st},$$

$$\sum_{j} a'_{tj}b'_{js}=\sum_{j} a_{sj}b_{jt}=c_{st}=c'_{ts}.$$

故
$$(a'_{ij})\,(b'_{ij})=(c'_{ij}).$$

復次，若 $\mathfrak{M}_f$ 之母式 (a_{ij}) 對於法 (l_{ij}) 有其逆時，則與 (a_{ij}) 對應者之 $\mathfrak{M}'_f$ 之母式 (a'_{ij}) 亦對法 (l'_{ij}) 而有其逆也. 蓋若

$$(a_{ij})\,(\bar{a}_{ij})\equiv(e_{ij}) \quad (\mathrm{mod.}\ (l_{ij})),$$

則
$$(a_{ij})\,(\bar{a}_{ij})=(e_{ij}+h_{ij}l_{ij}) \quad (h_{ij}\text{ 爲整數}).$$

故由上所示，

$$(a'_{ij})\,(\bar{a}'_{ij})=(e'_{ij}+h'_{ij}\,l'_{ij}).$$

$\therefore$
$$(a'_{ij})\,(\bar{a}'_{ij})\equiv(e'_{ij}) \quad (\mathrm{mod.}\ (l'_{ij})).$$

然
$$(e'_{ij})=(e_{ij}).$$

故 $$(a'_{ij})(\bar{a}_{ij})\equiv(e_{ij}) \pmod{(l'_{ij})}.$$

反之，$\mathfrak{M}'_f$之母式(a'_{ij})關於法(l'_{ij})有逆時，則與是對應之$\mathfrak{M}_f$之母式，亦關於法(l_{ij})有逆也．因之在$\mathfrak{M}_f$與$\mathfrak{M}'_f$之對應中，其有逆者兩相對應．然$\mathfrak{M}_f$中之有逆者之母式之集合，由前節定理，乃爲母式合同羣$\mathfrak{M}(n, l_{ij})$；而其在$\mathfrak{M}'_f$中者，則爲關於法(l'_{ij})之母式合同羣$\mathfrak{M}(n, l'_{ij})$也．且如上述，對於$\mathfrak{M}$之母式之積，其相對應者，爲與此各個相對應之母式($\mathfrak{M}'_f$者)之積．故$\mathfrak{M}(n, l_{ij})$與$\mathfrak{M}(n, l'_{ij})$爲單純同態．故定理云云．

又當討論母式合同羣時，由本定理，則法母式(l_{ij})視爲適合

$$l_{11}\geqq l_{22}\geqq\cdots\cdots\geqq l_{nn}$$

之條件者亦無不可．

定理．*於n次母式(l_{ij})，若*

$$l_{m+1,\,m+1}=l_{m+2,\,m+2}=\cdots\cdots=l_{nn}=1$$

時，則關於法(l_{ij}) $(i, j=1, 2, \cdots\cdots, n)$之$n$次母式合同羣，與關於法$(l_{ij})$ $(i, j=1, 2, \cdots\cdots, m)$之$m$次母式合同羣或其自身之約羣爲單純同態．

證明．$l_{ss}=1$時，因

$$f_{is}\,l_{ss}\equiv 0 \pmod{l_{is}},\quad l_{ss}\,f_{sj}\equiv 0 \pmod{l_{sj}},\quad l_{ij}\equiv 0 \pmod{f_{ij}}$$
$$(i, j=1, 2, \cdots\cdots, n),$$

故 $$f_{is}=l_{is}, f_{sj}=l_{sj}\quad (i, j=1, 2, \cdots\cdots, n).$$

故若 $$l_{m+1,\,m+1}=l_{m+2,\,m+2}=\cdots\cdots=l_{nn}=1$$

時,則母式合同羣$\mathfrak{M}(n, l_{ij})$之母式,皆有次形也:

$$\begin{pmatrix} a_{11}f_{11} & \cdots\cdots & a_{1m}f_{1m} & 0 & \cdots\cdots & 0 \\ \cdots\cdots & & & & & \\ a_{m1}f_{m1} & \cdots\cdots & a_{mm}f_{mm} & 0 & \cdots\cdots & 0 \\ 0 & \cdots\cdots & 0 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots\cdots & & \cdots\cdots & & \\ 0 & \cdots\cdots & 0 & 0 & \cdots\cdots & 0 \end{pmatrix}$$

若對於此母式,使m次母式

$$\begin{pmatrix} a_{11}f_{11} & \cdots\cdots & a_{1m}f_{1m} \\ \cdots\cdots & & \\ a_{m1}f_{m1} & \cdots\cdots & a_{mm}f_{mm} \end{pmatrix}$$

與之對應,則與$\mathfrak{M}(n, l_{ij})$之母式相應乃得一m次母式之集合;而此集合關於法

$$\begin{pmatrix} l_{11} & \cdots\cdots & l_{1m} \\ \cdots\cdots & & \\ l_{m1} & \cdots\cdots & l_{mm} \end{pmatrix}$$

成一與$\mathfrak{M}$爲單純同態之羣焉. 茲以$\mathfrak{M}'$表之.

由第111節(5),因$f_{ii}=1$,故$\mathfrak{M}'$含有與主母式相合同之母式. 以故f_{ij}爲能滿足

$$d_{ij}\,l_{jk}\equiv 0,\ l_{ij}\,d_{jk}\equiv 0 \pmod{l_{ik}}$$
$$(i, j, k=1, 2, \cdots\cdots, m)$$

者之d_{ij}之最小值時,則$\mathfrak{M}'$乃關於法(l_{ij}) $(i, j=1, 2, \cdots\cdots, m)$

之母式合同羣,否則爲$\mathfrak{M}$之約羣也(參照前節)

系. 於n次母式(l_{ij}),若除本定理之假設外,又有

$$l_{1j}=l_{2j}=\cdots\cdots=l_{nj}=l_j \quad (j=1, 2, \cdots\cdots, n)$$

時,則關於此法之母式合同羣,與m次母式合同羣爲單純同態.

證明. 此時f_{jk} $(j, k=1, 2, \cdots\cdots, n)$乃滿足聯立合同式

(1) $$l_j d_{jk}\equiv 0 \pmod{l_k} \quad (j, k=1, 2, \cdots\cdots, n)$$

之d_{jk}之最小值(參照第112節). 適合(1)之d_{jk}之值,其能滿足合同式

(2) $$l_j d_{jk}\equiv 0 \pmod{l_k} \quad (j, k=1, 2, \cdots\cdots, m)$$

甚明. 反之,適合(2)之d_{jk},對於(1)中令

$$j, k=1, 2, \cdots\cdots, m$$

而得之m^2個之合同式亦能滿足. 故滿足合同式(1)之d_{jk}之最小值f_{jk}乃合同式(2)之最小根. 因之在本定理之證明中之羣$\mathfrak{M}'$,遂爲m次合同羣$\mathfrak{M}(m, l_{ij})$,爰得本系.

注意. 定理證明中之羣$\mathfrak{M}'$爲$\mathfrak{M}(n, l_{ij})$之眞約羣者,實際亦自存在. 如以p爲素數,而取一三次母式

$$\begin{pmatrix} l_{11} & l_{12} & l_{13} \\ l_{21} & l_{22} & l_{23} \\ l_{31} & l_{32} & l_{33} \end{pmatrix} = \begin{pmatrix} p^2 & p^2 & p^2 \\ p^2 & p^2 & p \\ p & p & 1 \end{pmatrix},$$

則此具備爲法之條件. 其滿足

(3)　$d_{ij}\,l_{jk}\equiv 0,\quad l_{ij}\,d_{jk}\equiv 0 \pmod{l_{ik}}$

$$(i, j, k=1, 2)$$

者之 d_{ij} 之最小值爲

$$f_{ij}=1 \quad (i, j=1, 2).$$

然對 f_{ij} 之此一值，

$$f_{12}\,l_{23}=p\not\equiv 0 \pmod{l_{13}}.$$

故在滿足聯立合同式

$$d_{ij}\,l_{jk}\equiv 0,\quad l_{ij}\,d_{jk}\equiv 0 \pmod{l_{ik}}$$

$$(i, j, k=1, 2, 3)$$

之 d_{ij} 之最小值中，$f_{ij}\,(i, j=1, 2)$ 等於 1 時不可得也．故 $\mathfrak{M}'$ 不得與以二次母式

$$\begin{pmatrix} p^2 & p^2 \\ p^2 & p^2 \end{pmatrix}$$

爲法之合同羣一致．

115. 特殊母式.

以 r, s 爲 n 個數 $1, 2, \cdots\cdots, n$ 中之特別者，且 $r\neq s$．對於此 r, s，用次之方法以決定 n^2 個之數 $g_{ij\lambda}\,(i, j=1, 2, \cdots\cdots, n)$．即

(1)　$g_{rs\lambda}=\lambda$　(λ 爲正負整數或零*)，

(2)　$g_{11\lambda}=g_{22\lambda}=\cdots\cdots=g_{nn\lambda}=1.$

---

*λ 雖以之爲整數，然本節之公式，實對 λ 之任意數值而皆成立者也．

對於他之 i, j, 則令

$$g_{ij\lambda}=0 \quad (i\neq j). \tag{3}$$

而其以此等數爲項之 n 次母式

$$(g_{ij\lambda}) \qquad (i, j=1, 2, \cdots\cdots, n)$$

則以 $G_{rs\lambda}$ 表之焉.

爲示關於此母式之乘法公式, 卽可知

$$G_{rs\lambda}\, G_{rs\mu}=G_{rs(\lambda+\mu)}. \tag{4}$$

蓋若令

$$G_{rs\lambda}\, G_{rs\mu}=(c_{ij}) \qquad (i, j=1, 2, \cdots\cdots, n),$$

則

$$c_{ij}=\Sigma\, g_{ik\lambda}\, g_{kj\mu} \qquad (k=1, 2, \cdots\cdots, n).$$

而由 (3),

$$c_{rs}=\sum_k g_{rk\lambda}\, g_{ks\mu}=g_{rs\lambda}\, g_{ss\mu}+g_{rr\lambda}\, g_{rs\mu}$$

$$=\lambda+\mu \qquad [\text{由 (1) 及 (2)}].$$

同樣

$$c_{ii}=\sum_k g_{ik\lambda}\, g_{ki\mu}=g_{ii\lambda}\, g_{ii\mu}=1.$$

又對 $i\neq r$, $i\neq j$, 則由 (3) 及 (2),

$$c_{ij}=\sum_k g_{ik\lambda}\, g_{kj\mu}=g_{ij\lambda}\, g_{jj\mu}+g_{ii\lambda}\, g_{ij\mu}=0.$$

因之

$$c_{ij}=g_{ij}\,(\lambda+\mu),$$

卽得 (4) 也.

於 (4), 令 $\mu=-\lambda$, 則得

(5)　　$G_{rs\lambda}\,G_{r,\,s,-\lambda}=G_{rs0}=(e_{ij}).$

由之得

$$(G_{rs\lambda})^{-1}=G_{r,\,s,-\lambda}.$$

以故不論 x 之值爲正爲負，由(4)可得

(6)　　$$(G_{rs\lambda})^{x}=G_{r,\,s,\,x\lambda}$$

也*.

復次，取任意之 n 次母式

$$(a_{ij})\qquad(i,j=1,2,\cdots\cdots,n),$$

而以A表之．於是

$$(7)\quad AG_{rs\lambda}=\begin{pmatrix} a_{11}\ a_{12}\cdots\cdots a_{1s}+\lambda a_{1r}\ a_{1,s+1}\cdots\cdots \\ a_{21}\ a_{22}\cdots\cdots a_{2s}+\lambda a_{2r}\ a_{2,s+1}\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{n1}\ a_{n2}\cdots\cdots a_{ns}+\lambda a_{nr}\ a_{n,s+1}\cdots\cdots \end{pmatrix}$$

蓋若令

$$AG_{rs\lambda}=(c_{ij})\quad(i,j=1,2,\cdots\cdots,n),$$

則由(1), (2), (3),

$$c_{is}=\sum_{k}a_{ik}g_{ks\lambda}=a_{is}g_{ss\lambda}+a_{ir}g_{rs\lambda}=a_{is}+\lambda a_{ir};$$

而 $j\neq s$ 時，則

---

*對母式 (a_{ij}) 其能滿足

$$(a_{ij})(\bar{a}_{ij})=(e_{ij})$$

者之母式 $(\bar{a}_{ij})$ 稱曰 (a_{ij}) 之逆，以 $(a_{ij})^{-1}$ 表之．又母式之正整數冪 $(a_{ij})^{m}$ 之逆，則以 $(a_{ij})^{-m}$ 表之．於是 $(a_{ij})^{-m}=\{(a_{ij})^{-1}\}^{m}$ 也(參照第18節).

$$c_{ij}=\sum_k a_{ik}g_{kj\lambda}=a_{ij}g_{jj\lambda}=a_{ij}$$

故也.

於(7)令 $r=1$ 及 $s=1$, 則

$$(8)\quad \mathrm{AG}_{1s\lambda}=\begin{pmatrix} a_{11}\ a_{12}\cdots\cdots a_{1s}+\lambda a_{11}\ a_{1,s+1}\cdots\cdots \\ a_{21}\ a_{22}\cdots\cdots a_{2s}+\lambda a_{21}\ a_{2,s+1}\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{n1}\ a_{n2}\cdots\cdots a_{ns}+\lambda a_{n1}\ a_{n,s+1}\cdots\cdots \end{pmatrix},$$

$$(9)\quad \mathrm{AG}_{r1\lambda}=\begin{pmatrix} a_{11}+\lambda a_{1r}\ a_{12}\ \cdots\cdots \\ a_{21}+\lambda a_{2r}\ a_{22}\ \cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{n1}+\lambda a_{nr}\ a_{n2}\ \cdots\cdots \end{pmatrix}.$$

再由與前同樣之計算,

$$(10)\quad \mathrm{G}_{rs\lambda}\mathrm{A}=\begin{pmatrix} a_{11}\ a_{12}\cdots\cdots \\ a_{21}\ a_{22}\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{r1}+\lambda a_{s1}\ a_{r2}+\lambda a_{s2}\cdots\cdots \\ a_{r+1,1}\ a_{r+1,2}\cdots\cdots \\ \cdots\cdots\cdots\cdots \end{pmatrix}.$$

116. 合同羣之母元素.

母式合同羣 $\mathfrak{M}(n, l_{ij})$ 者, 乃由若干母元素所生成者也. 茲分次之三段說明之.

1.° 在前節所定義之母式 $\mathrm{G}_{rs\lambda}$ 中, 其令

$$\lambda=f_{rs}$$

者以 G_{rs} 表之. 但 f_{rs} 爲有第111節中所定之意義者, 因 $f_{ii}=1$, 故 G_{rs} 之項 $g_{ij\lambda}$ 乃 f_{ij} 之倍數. 不僅此也, 由前節(5)則 G_{rs} 之有關於法 (l_{ij}) 之逆甚明. 故 G_{rs} 屬於羣 $\mathfrak{M}(n, l_{ij})$. 而由(6),* 則有

$$G^{x}_{rs}=G_{r,s,x\lambda}\quad(\lambda=f_{rs}).\tag{11}$$

今於公式(7), (8), (9), (10), 取屬於 $\mathfrak{M}(n, l_{ij})$ 者之母式

$$(a_{ij}f_{ij})\quad(i, j=1, 2, \cdots\cdots, n)$$

以爲A, 則得:

$$(a_{ij}f_{ij})G^{x}_{rs}=\begin{pmatrix} a_{11}f_{11}\cdots\cdots a_{1s}f_{1s}+xa_{1r}f_{1r}f_{rs}\cdots\cdots \\ a_{21}f_{21}\cdots\cdots a_{2s}f_{2s}+xa_{2r}f_{2r}f_{rs}\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{n1}f_{n1}\cdots\cdots a_{ns}f_{ns}+xa_{nr}f_{nr}f_{rs}\cdots\cdots \end{pmatrix}\tag{12}$$

$$(a_{ij}f_{ij})G^{x}_{1s}=\begin{pmatrix} a_{11}f_{11}\cdots\cdots a_{1s}f_{1s}+xa_{11}f_{11}f_{1s}\cdots\cdots \\ a_{21}f_{21}\cdots\cdots a_{2s}f_{2s}+xa_{21}f_{21}f_{1s}\cdots\cdots \\ \cdots\cdots\cdots\cdots \\ a_{n1}f_{n1}\cdots\cdots a_{ns}f_{ns}+xa_{n1}f_{n1}f_{1s}\cdots\cdots \end{pmatrix}\tag{13}$$

$$(a_{ij}f_{ij})G^{x}_{r1}=\begin{pmatrix} a_{11}f_{11}+xa_{1r}f_{1r}f_{r1} & a_{12}f_{12}\cdots\cdots \\ a_{21}f_{21}+xa_{2r}f_{2r}f_{r1} & a_{22}f_{22}\cdots\cdots \\ \cdots\cdots & \cdots\cdots \\ a_{n1}f_{n1}+xa_{nr}f_{nr}f_{r1} & a_{n2}f_{n2}\cdots\cdots \end{pmatrix}\tag{14}$$

*本式以及他式之號數則由前節以至於本節概行通用.

$$(15)\quad G^{x}_{rs}(a_{ij}f_{ij})=\begin{pmatrix} a_{11}f_{11} & a_{12}f_{12} & \cdots\cdots \\ \cdots\cdots & & \\ a_{r1}f_{r1}+xa_{s1}f_{s1}f_{rs} & a_{r2}f_{r2}+xa_{s2}f_{s2}f_{rs} & \cdots\cdots \\ a_{r+1,1}f_{r+1,1} & a_{r+1,2}f_{r+1,2} & \cdots\cdots \\ \cdots\cdots & & \end{pmatrix}$$

而此諸積任何個皆屬於$\mathfrak{M}$也.

2.° 法母式所有之項l_{ij} $(i,j=1,2,\cdots\cdots,n)$之最小公倍數以l表之. 在羣$\mathfrak{M}(n,l_{ij})$之母式$(a_{ij}f_{ij})$中,若其一項$a_{ii}f_{ii}$ $(=a_{ii})$對於l_{ii} (>1)爲互素,則由適當的選擇整數z,可使

$$a_{ii}f_{ii}+zl_{ii}$$

對於l爲互素也. 蓋若l分解爲二因數,如

$$l=l'l'',$$

但l'對l_{ii}互素,而l''之素因數,則其任何個皆爲含於l_{ii}者. 乃選整數z,使$a_{ii}f_{ii}+zl_{ii}$對l'爲互素(因l_{ii}對l'爲互素,故常可能.) 於是$a_{ii}f_{ii}+zl_{ii}$對l爲互素,明已.

故如上選擇整數z,雖代$(a_{ij}f_{ij})$之項$a_{ii}f_{ii}$入以$a_{ii}f_{ii}+zl_{ii}$,則由此所得之母式,其與$(a_{ij}f_{ij})$相合同(法(l_{ij}))乃當然也.

3°. 於法母式(l_{ij}),令

$$l_{11},\ l_{22},\ \cdots\cdots,\ l_{mm}>1\quad (m\leqq n),$$

而當$m<n$時,則令

$$l_{m+1,\ m+1}=\cdots\cdots=l_{nn}=1.$$

乃取羣$\mathfrak{M}(n,l_{ij})$之母式

$$A=(a_{ij}\,f_{ij}).$$

關於法(l_{ij}), A之逆以爲$(\bar{a}_{ij}\,f_{ij})$, 則

$$\sum_j a_{1j}f_{1j}\,\bar{a}_{j1}f_{j1}\equiv 1 \pmod{l_{11}}.$$

故在n個之積

$$(16)\quad a_{11}f_{11}f_{11}\,(=a_{11}),\ a_{12}f_{12}f_{21},\ \cdots\cdots,\ a_{1n}f_{1n}f_{n1}$$

中, 其對l_{11}互素者非存在不可也. 若a_{11}對l_{11}爲互素時, 則選擇整數z_1, 使$a_{11}f_{11}+z_1l_{11}$對l爲互素, 而令

$$B=\begin{pmatrix} a_{11}f_{11}+z_1l_{11} & a_{12}f_{12}\cdots\cdots \\ a_{21}f_{21} & a_{22}f_{22}\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \end{pmatrix}$$

此B當然與A合同(法(l_{ij})). a_{11}對l_{11}不爲互素時, 乃於(16)中取其對l_{11}爲互素者之$a_{1u}f_{1u}f_{u1}$, 而作$AG_{u1}^{y_{u1}}$. 於是由(14),

$$AG_{u1}^{y_{u1}}=\begin{pmatrix} a_{11}f_{11}+a_{1u}f_{1u}f_{u1}\,y_{u1} & a_{12}f_{12}\cdots\cdots \\ a_{21}f_{21}+a_{2u}f_{2u}f_{u1}\,y_{u1} & a_{22}f_{22}\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & \\ a_{n1}f_{n1}+a_{nu}f_{nu}f_{u1}\,y_{u1} & a_{n2}f_{n2}\cdots\cdots \end{pmatrix}$$

若適當的選擇y_{u1}, 則$a_{11}f_{11}+a_{1u}f_{1u}f_{u1}\,y_{u1}$對$l_{11}$爲互素. 於是與前同樣, 選擇$z_1$, 使

$$a_{11}f_{11}+a_{1u}f_{1u}f_{u1}\,y_{u1}+z_1\,l_{11}$$

對l爲互素; 乃以之代入$AG_{u1}^{y_{u1}}$之第一列第一項$a_{11}f_{11}+a_{1u}f_{1u}f_{u1}\,y_{u1}$, 而以其所得名曰B. 是卽在上二者, 若令

$$\mathrm{B}=(\beta_{ij}f_{ij})\quad(i,j=1,2,\cdots\cdots,n),$$

則 $\beta_{11}f_{11}$ 對 l 爲互素. 因之,其能適合

$$\beta_{12}f_{12}+x_{12}\beta_{11}f_{11}f_{12}\equiv 0\pmod{l_{12}}$$
$$\beta_{13}f_{13}+x_{13}\beta_{11}f_{11}f_{13}\equiv 0\pmod{l_{13}}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\beta_{1m}f_{1m}+x_{1m}\beta_{11}f_{11}f_{1m}\equiv 0\pmod{l_{1m}}$$

者之整數

$$x_{12},\ x_{13},\ \cdots\cdots,\ x_{1m}$$

克以求得也.

對此諸整數,由 (13), 乃有

$$(17)\quad \mathrm{B}\mathrm{G}_{12}^{x_{12}}\mathrm{G}_{13}^{x_{13}}\cdots\cdots\mathrm{G}_{1m}^{x_{1m}}\equiv\begin{pmatrix}\beta_{11}f_{11} & 0 & \cdots\cdots & 0\\ \gamma_{21}f_{21} & \gamma_{22}f_{22} & \cdots\cdots & \gamma_{2n}f_{2n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \gamma_{n1}f_{n1} & \gamma_{n2}f_{n2} & \cdots\cdots & \gamma_{nn}f_{nn}\end{pmatrix}^{*}$$

此之右邊名曰 C.

在屬於 $\mathfrak{M}(n,l_{ij})$ 之母式中,其得以與 C 同形而表示之者(第一橫列之第二項以下皆與零合同者)相集成羣(法

---

*因 $l_{ii}=1$ $(i>m)$, 故由第 114 節第二定理之證明中所述, $\mathfrak{B}(n,l_{ij})$ 之母式 $(a_{ij}f_{ij})$ 之項對 $j>m$ 爲

$$a_{ij}f_{ij}\equiv 0\pmod{l_{ij}}.$$

本式之計算以及爾後之計算均請留意及此. 又 (17) 之左邊因其屬於 $\mathfrak{B}$, 故右邊之 γ_{ij} 當然爲整數.

至以下母式之合同皆爲就法 (l_{ij}) 而取之者.

(l_{ij}))甚明. 在此羣中,以C之逆母式爲

$$\begin{pmatrix} \overline{\gamma}_{11}f_{11} & 0 & \cdots\cdots & 0 \\ \overline{\gamma}_{21}f_{21} & \overline{\gamma}_{22}f_{22} & \cdots\cdots & \overline{\gamma}_{2n}f_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \overline{\gamma}_{n1}f_{n1} & \overline{\gamma}_{n2}f_{n2} & \cdots\cdots & \overline{\gamma}_{nn}f_{nn} \end{pmatrix},$$

則

$$\sum_{j=2}^{n}\gamma_{2j}f_{2j}\overline{\gamma}_{j2}f_{j2}\equiv 1 \pmod{l_{22}}.$$

故在

(18)　$\gamma_{22}f_{22}f_{22}\ (=\gamma_{22}),\ \gamma_{23}f_{23}f_{32},\ \cdots\cdots,\ \gamma_{2n}f_{2n}f_{n2}$

之中,其對l_{22}爲互素者非存在不可也(但$m\geqq 2$). γ_{22}若如斯,此時乃選整數z_2使$\gamma_{22}f_{22}+z_2l_{22}$對$l$爲互素,而母式C之項$\gamma_{22}f_{22}$代以$\gamma_{22}f_{22}+z_2l_{22}$者名曰D. 卽

$$\mathrm{D}=\begin{pmatrix} \beta_{11}f_{11} & 0 & 0 & \cdots\cdots \\ \gamma_{21}f_{21} & \gamma_{22}f_{22}+z_2l_{22} & \gamma_{23}f_{23} & \cdots\cdots \\ \gamma_{31}f_{31} & \gamma_{32}f_{32} & \gamma_{33}f_{33} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \end{pmatrix}.$$

反之,若γ_{22}對l_{22}非爲互素時,乃於(18)中取其與l_{22}互素者之$\gamma_{2v}f_{2v}f_{v2}$而作$\mathrm{CG}_{v2}^{y_{v2}}$. y_{v2}若適當取之,則此之第二列第二項對l_{22}得成互素. 再加z_2l_{22}於是項,使第二列第二項對l成互素,而以是所得者名之曰D. 在上二者,總之令

$$\mathrm{D}=(\delta_{ij}f_{ij})\quad (i,j=1,2,\cdots\cdots,n),$$

則$\delta_{11}f_{11}=\beta_{11}f_{11}$, $\delta_{22}f_{22}$對l爲互素. 於是乃使滿足

$$\delta_{23}f_{23}+x_{23}\delta_{22}f_{22}f_{23}\equiv 0 \pmod{l_{23}}$$

$$\delta_{24}f_{24}+x_{24}\delta_{22}f_{22}f_{24}\equiv 0 \pmod{l_{24}}$$

$$\cdots\cdots\cdots\cdots$$

$$\delta_{2m}f_{2m}+x_{2m}\delta_{22}f_{22}f_{2m}\equiv 0 \pmod{l_{2m}}$$

而求整數

$$x_{23},\ x_{24},\ \cdots\cdots,\ x_{2m},$$

則對此諸數,由(12)便得

$$DG_{28}^{x_{23}}G_{24}^{x_{24}}\cdots\cdots G_{2m}^{x_{2m}}\equiv\begin{pmatrix}\delta_{11}f_{11} & 0 & 0 & \cdots\cdots & 0\\ \varepsilon_{21}f_{21} & \delta_{22}f_{22} & 0 & \cdots\cdots & 0\\ \varepsilon_{31}f_{31} & \varepsilon_{32}f_{32} & \varepsilon_{33}f_{33} & \cdots\cdots & \varepsilon_{3n}f_{3n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \varepsilon_{n1}f_{n1} & \varepsilon_{n2}f_{n2} & \varepsilon_{n3}f_{n3} & \cdots\cdots & \varepsilon_{nn}f_{nn}\end{pmatrix}.$$

而$\mathfrak{M}$之母式中,其得以此右邊之形而表示之者相集乃成羣也. 因之與前同樣,在

$$\varepsilon_{33}f_{33}f_{33}(=\varepsilon_{33}),\ \varepsilon_{34}f_{34}f_{43},\ \cdots\cdots,\ \varepsilon_{3n}f_{3n}f_{n3}$$

之中,其對l_{33}爲互素者非存在不可. 於是依同樣之手續反覆行之,遂得

(19)
$$AG_{u1}^{y_{u1}}G_{12}^{x_{12}}G_{18}^{x_{13}}\cdots\cdots G_{1m}^{x_{1m}}$$

$$\times G_{v2}^{y_{v2}}G_{23}^{x_{23}}\cdots\cdots G_{2m}^{x_{2m}}$$

$$\cdots\cdots\cdots\cdots$$

$$\times G_{w,m-1}^{y_{w,m-1}}G_{m-1,m}^{x_{m-1,m}}$$

$$\equiv\begin{pmatrix}\xi_{11}f_{11} & 0 & 0 & \cdots\cdots & 0\\ \xi_{21}f_{21} & \xi_{22}f_{22} & 0 & \cdots\cdots & 0\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \xi_{n1}f_{n1} & \xi_{n2}f_{n2} & \xi_{n3}f_{n3} & \cdots\cdots & \xi_{nn}f_{nn}\end{pmatrix}$$

但 $m<n$ 時，則

$$\xi_{ij}f_{ij}\equiv 0 \pmod{l_{ij}} \quad (i,j>m).$$

此右邊之母式以 X 表之．由上記之計算，則於 X 之項中，

$$\xi_{11}f_{11}=\beta_{11}f_{11},\ \xi_{22}f_{22}=\delta_{22}f_{22},\ \cdots\cdots,$$

甚明，因之

$$\xi_{11}f_{11},\ \xi_{22}f_{22},\ \cdots\cdots,\ \xi_{m-1,\,m-1}f_{m-1,\,m-1}$$

均對於 l 爲互素也．而 $\mathfrak{M}(n,l_{ij})$ 之母式中，其有與 X 同形者乃成羣（法 (l_{ij})），以故 $\xi_{mm}f_{mm}$ 對 l_{mm} 互素．乃選整數 z_m，使 $\xi_{mm}f_{mm}+z_m l_{mm}$ 對 l 互素；然後將 X 之 $\xi_{mm}f_{mm}$ 代以此數，而以其所得者名曰 Y．即

$$\mathrm{Y}=\begin{pmatrix}\eta_{11}f_{11} & 0 & 0 & \cdots\cdots & 0\\ \eta_{21}f_{21} & \eta_{22}f_{22} & 0 & \cdots\cdots & 0\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \eta_{n1}f_{n1} & \eta_{n2}f_{n2} & \eta_{n3}f_{n3} & \cdots\cdots & \eta_{nn}f_{nn}\end{pmatrix}.$$

但

$$\eta_{mm}f_{mm}=\xi_{mm}f_{mm}+z_m l_{mm},$$

而其他則

$$\eta_{ij}f_{ij}=\xi_{ij}f_{ij}.$$

於 Y，其對角線上之 m 項

(20) $\eta_{11}f_{11},\ \eta_{22}f_{22},\ \cdots\cdots,\ \eta_{mm}f_{mm}$

由上述,知均對 l 互素. 故得求整數 x_{21} 使

$$\eta_{21}f_{21}+x_{21}\eta_{22}f_{22}f_{21}\equiv 0 \pmod{l_{21}}$$

也. 對此數,由 (14) 遂得

$$\mathrm{YG}_{21}^{x_{21}}\equiv\begin{pmatrix}\eta_{11}f_{11} & 0 & 0 & 0 & \cdots\cdots\\ 0 & \eta_{22}f_{22} & 0 & 0 & \cdots\cdots\\ \eta'_{31}f_{31} & \eta_{32}f_{32} & \eta_{33}f_{33} & 0 & \cdots\cdots\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\end{pmatrix}$$

復次,取能滿足

$$\eta'_{31}f_{31}+x_{31}\eta_{33}f_{33}f_{31}\equiv 0 \pmod{l_{31}}$$

$$\eta_{32}f_{32}+x_{32}\eta_{33}f_{33}f_{32}\equiv 0 \pmod{l_{32}}$$

者之整數 x_{31}, x_{32}, 則由 (12) 得

$$\mathrm{YG}_{21}^{x_{21}}\mathrm{G}_{31}^{x_{31}}\mathrm{G}_{32}^{x_{32}}\equiv\begin{pmatrix}\eta_{11}f_{11} & 0 & 0 & 0 & 0 & \cdots\cdots\\ 0 & \eta_{22}f_{22} & 0 & 0 & 0 & \cdots\cdots\\ 0 & 0 & \eta_{33}f_{33} & 0 & 0 & \cdots\cdots\\ \eta''_{41}f_{41} & \eta''_{42}f_{42} & \eta_{43}f_{43} & \eta_{44}f_{44} & 0 & \cdots\cdots\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\end{pmatrix}.$$

以下準此,遂得

(21) $$\mathrm{YG}_{21}^{x_{21}}\mathrm{G}_{31}^{x_{31}}\mathrm{G}_{32}^{x_{32}}\mathrm{G}_{41}^{x_{41}}\mathrm{G}_{42}^{x_{42}}\mathrm{G}_{43}^{x_{43}}\cdots\mathrm{G}_{m1}^{x_{m1}}\mathrm{G}_{m2}^{x_{m2}}\cdots\mathrm{G}_{m,\,m-1}^{x_{m,\,m-1}}$$

$$\equiv(\eta_{ij}f_{ij}\,e_{ij})\equiv(\eta_{ij}\,e_{ij}).$$

但 $m<n$ 時, 對 $i>m$ 則 $\eta_{ii}\equiv 0 \pmod{l_{ii}}$.

右邊之母式 $(\eta_{ij}e_{ij})$ 表以 J，則於(19)，(21)以 z_{ij} 代其 $-x_{ij}$，則得

$$(22)\qquad A\equiv JG_{m,\,m-1}^{z_{m,\,m-1}}G_{m,\,m-2}^{z_{m,\,m-2}}\cdots\cdots G_{m1}^{z_{m1}}$$

$$G_{m-1,\,m-2}^{z_{m-1,\,m-2}}\cdots\cdots G_{m-1,\,1}^{z_{m-1,\,1}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$G_{21}^{z_{21}}$$

$$G_{m-1,\,m}^{z_{m-1,\,m}}G_{w,\,m-1}^{-y_{w,\,m-1}}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$G_{2m}^{z_{2m}}\cdots\cdots G_{23}^{z_{23}}G_{v2}^{-y_{v2}}$$

$$G_{1m}^{z_{1m}}G_{1,\,m-1}^{z_{1,\,m-1}}\cdots\cdots G_{12}^{z_{12}}G_{u1}^{-y_{u1}}.$$

因之得次

定理. 於母式合同羣 $\mathfrak{M}(n, l_{ij})$ 之法母式 (l_{ij})，若

$$l_{11}, l_{22}, \cdots\cdots, l_{mm}>1 \quad (m\leqq n),$$

而 $m<n$，則

$$l_{m+1,\,m+1}=\cdots\cdots=l_{nn}=1$$

時，則合同羣得由 $m(m-1)$ 個之母式

$$G_{rs} \quad (r\neq s;\ r, s=1, 2\cdots\cdots, m)$$

以及有次形

$$J=(\eta_{ij}\,e_{ij})$$

之母式而生成之.

此定理中之特須留意者，即倍乘母式 J 可選擇之，使 J

之行列式 $\eta_{11}\eta_{22}\cdots\cdots\eta_{nn}$ 對於法母式之項之最小公倍數 l 爲互素是也. 是蓋因倍乘數 $\eta_{11}, \eta_{22}, \cdots\cdots, \eta_{mm}$, 有如上述, 得選擇之使對 l 互素; 而 $m<n$ 時, 則因 $l_{m+i,\ m+i}=1$ 之故, 對 $\eta_{m+i,\ m+i}$ 得與以任意之值故耳.

117. $\mathfrak{M}(n, l)$ **之母元素.**

在關於法 l 之母式合同羣中, 則

$$f_{ij}=1 \qquad (i, j=1, 2, \cdots\cdots, n)$$

也 (參照第 112 節). 故前節定理之母式 G_{rs}, 乃有

$$G_{rs}=(g_{ij})$$

之形焉. 但 $g_{rs}=1$, $g_{11}=g_{22}=\cdots\cdots=g_{nn}=1$, 而對其他之 i, j, 則 $g_{ij}=0$. 而倍乘母式 J 之形, 亦由是得導出更簡單者, 示之如次.

此時, 前節 (16) 乃成

(1) $$a_{11},\ a_{12},\ \cdots\cdots,\ a_{1n},$$

而其中對 l 互素者非存在不可也. 若 (1) 之第二項以下對 l 互素者如 a_{1u} 存在時, 則選適合

$$a_{11}+x_1\ a_{1u}\equiv 1 \pmod{l}$$

者之整數 x_1, 而令

$$B=(a_{ij})G_{u1}^{x_1}.$$

於是由前節 (14),

(2) $$B\equiv\begin{pmatrix} 1 & \beta_{12} & \cdots\cdots \\ \beta_{21} & \beta_{22} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \end{pmatrix} \pmod{l}.$$

反之,(1) 中對 l 互素者僅爲 a_{11} 時,則令

$$B=(a_{ij}),G_{12}^{y_1}G_{21}^{x_1},$$

而選擇能適合

$$a_{11}+x_1(a_{12}+y_1a_{11})\equiv 1 \pmod{l}$$

者之整數以爲 x_1, y_1,則由前節 (13), (14) 知 B 復取 (2) 之形也.

復次與前節同樣,決定 $x_{12}, x_{13}, \cdots\cdots, x_{1n}$ 乃得

$$(4)\quad BG_{12}^{x_{12}}G_{13}^{x_{13}}\cdots G_{1n}^{x_{1n}}\equiv\begin{pmatrix}1 & 0 & \cdots\cdots & 0\\ \gamma_{21} & \gamma_{22} & \cdots\cdots & \gamma_{2n}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ \gamma_{n1} & \gamma_{n2} & \cdots\cdots & \gamma_{nn}\end{pmatrix}\pmod{l}.$$

此之右邊名曰 C. 同理

$$\gamma_{22}, \gamma_{23}, \cdots\cdots, \gamma_{2n}$$

之中,其對 l 互素者亦非存在不可. 若此互素者僅爲 γ_{22},則令

$$D=CG_{23}^{y_2}G_{32}^{x_2},\quad \gamma_{22}+x_2(\gamma_{23}+y_2\gamma_{22})\equiv 1 \pmod{l},$$

而於其他如 γ_{2v} 對 l 爲互素時,若令

$$D=CG_{v2}^{x_2},\quad \gamma_{22}+x_2\gamma_{2v}\equiv 1 \pmod{l},$$

則

$$D\equiv\begin{pmatrix}1 & 0 & 0 & \cdots\cdots\\ \delta_{21} & 1 & \delta_{23} & \cdots\cdots\\ \delta_{31} & \delta_{32} & \delta_{33} & \cdots\cdots\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\end{pmatrix}\pmod{l}.$$

由是，與前節 3° 同樣，遂得

$$(a_{ij})\prod_{r,s} G_{rs}^{z_{rs}} \equiv \begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & \triangle \end{pmatrix} \pmod{l}.$$

乃有次

定理. 母式合同羣 $\mathfrak{M}(n, l)$，得由 $n(n-1)$ 個之母式

$$G_{rs}=(g_{ij}) \quad (r \neq s;\ r, s=1, 2, \cdots\cdots, n)$$

及有次形之母式

$$J = \begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & \triangle \end{pmatrix}$$

而生成之. 但 G_{rs} 乃有本節開端所述之意義者.

系. 母式合同羣 $\mathfrak{M}(n, l)$ 中之自己共軛元素，乃有 (γe_{ij}) 之形.

證明. 令 (a_{ij}) 爲 $\mathfrak{M}(n, l)$ 之自己共軛元素，則對母元素 G_{rs}，乃有

$$(a_{ij})\, G_{rs} \equiv G_{rs}\, (a_{ij}) \pmod{l}$$

$$(r, s=1, 2, \cdots\cdots, n;\ r \neq s),$$

故由第 115 節 (7) 及 (10)，則

$$\left.\begin{aligned} a_{rs}+a_{rr}&\equiv a_{rs}+a_{ss}\\ a_{rj}&\equiv a_{rj}+a_{sj}\end{aligned}\right\}\ (\mathrm{mod.}\ l)$$

$$(j=1,\ 2,\ \cdots\cdots,\ s-1,\ s+1,\ \cdots\cdots,\ n)$$

爲必要也. 由是,

$$\left.\begin{aligned} a_{rr}&\equiv a_{ss}\\ a_{ij}&\equiv 0\quad (j\neq s)\end{aligned}\right\}\ (\mathrm{mod.}\ l).$$

故若令　$a_{11}\equiv a_{22}\equiv\cdots\cdots\equiv a_{nn}\equiv\gamma\ \ (\mathrm{mod.}\ l)$,

則　$(a_{ij})\equiv(\gamma e_{ij})\ \ (\mathrm{mod.}\ l)$.

118. 逆母式存在之條件.

定理. 集合 $\mathfrak{M}_f(n, l_{ij})$ 之母式 $(a_{ij}f_{ij})$, 關於法 (l_{ij}) 而有其逆時, 則在與之相合同(法 (l_{ij}))之母式中, 其行列式對於法母式之各項之爲互素者非存在不可. 反之, 於此時, 母式 $(a_{ij}f_{ij})$ 乃有其逆.

證明. 茲分三段論之.

法母式所有之項 $l_{ij}\ (i, j=1, 2, \cdots\cdots, n)$ 之最小公倍數以 l 示之.

1°. 試以 $\mathfrak{M}_f(n, l_{ij})$ 之母式 (a_{ij}) 爲關於法 (l_{ij}) 有其逆者, 則其非屬於羣 $\mathfrak{M}(n, l_{ij})$ 不可也. 因之由前前節(22)得

(1)　$$(a_{ij})\equiv \mathrm{J}\prod_{r,s}\mathrm{G}_{rs}^{z_{rs}}\ \ (\mathrm{mod.}\ (l_{ij})).$$

但　$$\mathrm{J}=(\eta_{ij}\,e_{ij}).$$

在(1)之右邊, G_{rs} 之行列式之等於1甚明. 故右邊之行列

式, 與 J 之行列式

$$\eta_{11}\,\eta_{22}\cdots\cdots\,\eta_{nn}$$

等. 然由前前節之所注意者然, 其 J 得以決定之, 能使此行列式對 l 爲互素也. 故定理前半之爲眞, 可知也已.

2°. 條件之充分性.

因屬於 $\mathfrak{M}_f(n, l_{ij})$ 之母式之乘法(法(l_{ij}))爲一意的, 故若

$$(2)\qquad (a_{ij}\,f_{ij})(\beta_{ij}\,f_{ij})\equiv(e_{ij})\pmod{(l_{ij})}$$

時, 則對於與 $(a_{ij}\,f_{ij})$ 相合同(法(l_{ij}))之母式 $(a'_{ij}\,f_{ij})$, 亦得

$$(a'_{ij}\,f_{ij})(\beta_{ij}\,f_{ij})\equiv(e_{ij})\pmod{(l_{ij})}$$

也. 以故若母式 $(a_{ij}\,f_{ij})$ 之行列式對 l 爲互素時, 使能示克滿足 (2) 而得選擇母式 $(\beta_{ij}\,f_{ij})$, 則定理後半之爲眞又可知矣.

今先令行列式 $|\,a_{ij}\,f_{ij}\,|$ 爲對 l 互素者. 因

$$(a_{ij}\,f_{ij})(\beta_{ij}\,f_{ij})=(\sum_{k}a_{ik}\,\beta_{kj}\,f_{ik}\,f_{kj}),$$

故若以此換書爲聯立合同式之形, 則 (2) 遂成爲

$$(3)\qquad \sum_{k=1}^{n}a_{ik}\,\beta_{kj}\,f_{ik}\,f_{kj}\equiv e_{ij}\pmod{l_{ij}}$$

$$(i, j=1, 2, \cdots\cdots, n).$$

然由第 111 節 (5), (7), 及 (9),

$$f_{ii}=1,\ f_{ik}\,f_{kj}\equiv 0,\ l_{ij}\equiv 0\pmod{f_{ij}},$$

故 (3) 之兩邊以 f_{ij} 除之, 得

$$(4)\qquad \sum_k a_{ik}\,\beta_{kj}\,f_{ik}\,f_{kj}\,f_{ij}^{-1}\equiv e_{ij}\quad(\mathrm{mod.}\ l_{ij}\,f_{ij}^{-1})$$

$$(i,\ j=1,\ 2,\ \cdots\cdots,\ n).^{*}$$

乃從此 n^2 個合同式之中，取出 n 個：

$$(5)\qquad \sum_k a_{ik}\,\beta_{kj}\,f_{ik}\,f_{kj}\,f_{ij}^{-1}\equiv e_{ij}\quad(\mathrm{mod.}\ l_{ij}\,f_{ij}^{-1})$$

$$(i=1,\ 2,\ \cdots\cdots,\ n),$$

而就其係數之行列式而觀，

$$\begin{vmatrix} a_{11}f_{11}f_{1j}f_{1j}^{-1} & a_{12}f_{12}f_{2j}f_{1j}^{-1} & \cdots\cdots & a_{1n}f_{1n}f_{nj}f_{1j}^{-1} \\ a_{21}f_{21}f_{1j}f_{2j}^{-1} & a_{22}f_{22}f_{2j}f_{2j}^{-1} & \cdots\cdots & a_{2n}f_{2n}f_{nj}f_{2j}^{-1} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1}f_{n1}f_{1j}f_{nj}^{-1} & a_{n2}f_{n2}f_{2j}f_{nj}^{-1} & \cdots\cdots & a_{nn}f_{nn}f_{nj}f_{nj}^{-1} \end{vmatrix}$$

$$=f_{1j}f_{2j}\cdots\cdots f_{nj}f_{1j}^{-1}f_{2j}^{-1}\cdots\cdots f_{nj}^{-1}\left|\ a_{ij}f_{ij}\ \right| = \left|\ a_{ij}f_{ij}\ \right|,$$

即知其與母式 $(a_{ij}f_{ij})$ 之行列式等. 故由假設，此行列式對 l 互素. 因之如次段 3° 所示，吾人得定

$$\beta_{1j},\ \beta_{2j},\ \cdots\cdots,\ \beta_{nj}$$

之值而使之能滿足聯立合同式 (5) 也. 於此而令 $j=1, 2, \cdots\cdots, n$，則由是可得適合聯立合同式 (4)，隨之即適合(2)之 β_{ij} 之值，而母式 $(\beta_{ij}f_{ij})$ 遂爲 $(a_{ij}f_{ij})$ 之逆焉.

---

* 因 $e_{ij}=\begin{cases}1 & (i=j)\\ 0 & (i\neq j)\end{cases}$，故 $e_{ij}\equiv 0\ (\mathrm{mod.}\ f_{ij})$.

3°. 聯立一次合同式.

在關於 n 個未知數 $z_1, z_2, \cdots\cdots, z_n$ 之聯立一次合同式

$$(6)\qquad \left.\begin{aligned} &c_{11}z_1+c_{12}z_2+\cdots\cdots+c_{1n}z_n\equiv c_1\\ &c_{21}z_1+c_{22}z_2+\cdots\cdots+c_{2n}z_n\equiv c_2\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ &c_{n1}z_1+c_{n2}z_2+\cdots\cdots+c_{nn}z_n\equiv c_n \end{aligned}\right\}\ (\mathrm{mod.}\ l)$$

中, 其係數之行列式 $|c_{ij}|$ 對於法 l 爲互素時, 則此聯立合同式關於法 l 乃有一組之根.

蓋於行列式 $|c_{ij}|$, 若以屬於其項 c_{ij} 之小行列式示以 Δ_{ij}, 則

$$c_{1j}\Delta_{1j}+c_{2j}\Delta_{2j}+\cdots\cdots+c_{nj}\Delta_{nj}=|c_{ij}|,$$
$$c_{1k}\Delta_{1j}+c_{2k}\Delta_{2j}+\cdots\cdots+c_{nk}\Delta_{nj}=0\quad(k\neq j).$$

故於 (6) 之兩邊各各以 $\Delta_{1j}, \Delta_{2j}, \cdots\cdots, \Delta_{nj}$ 乘之, 然後邊邊相加, 得

$$(7)\quad |c_{ij}|z_j\equiv c_1\Delta_{1j}+c_2\Delta_{2j}+\cdots\cdots+c_n\Delta_{nj}\quad(\mathrm{mod.}\ l)$$
$$(j=1, 2, \cdots\cdots, n).$$

然 $|c_{ij}|$ 對 l 互素. 故其滿足

$$\lambda|c_{ij}|\equiv 1\quad(\mathrm{mod.}\ l)$$

者之數 λ 克以求得也. 以此 λ 乘 (7) 之兩邊, 遂得

$$(8)\quad z_j\equiv\lambda(c_1\Delta_{1j}+c_2\Delta_{2j}+\cdots\cdots+c_n\Delta_{nj})\quad(\mathrm{mod.}\ l)$$
$$(j=1, 2, \cdots\cdots, n).$$

以故若 $|c_{ij}|$ 對 l 爲互素時, 則 (6) 乃有根, 而且唯 (8) 之一組也.

今若行列式$|a_{ij}f_{ij}|$對l爲互素,則關於$\beta_{1j}, \beta_{2j}, \cdots\cdots, \beta_{nj}$之聯立合同式

$$\sum_k a_{ik}\beta_{kj}f_{ik}f_{kj}f_{ij}^{-1}\equiv e_{ij} \pmod{l} \quad (i=1, 2, \cdots\cdots, n)$$

乃有根,而由此之根,聯立合同式(5)亦得滿足自明. 蓋因l爲l_{ij}之倍數故也.

系1. $m_{ij}\geqq 1\ (i, j=1, 2, \cdots\cdots, n)$時,則屬於集合$\mathfrak{M}_f(n, p^{m_{ij}})$之母式$(a_{ij}p^{\varphi_{ij}})$關於法$(p^{m_{ij}})$而有其逆之條件(必要而且充分者)爲

$$|a_{ij}p^{\varphi_{ij}}| \not\equiv 0 \pmod{p}.$$

但p爲素數.

蓋若取關於法$(p^{m_{ij}})$而與$(a_{ij}p^{\varphi_{ij}})$合同之任意母式

$$(a_{ij}p^{\varphi_{ij}}+x_{ij}p^{m_{ij}}) \qquad [x_{ij}\text{爲整數}],$$

則因$m_{ij}>0$, 故

$$|a_{ij}p^{\varphi_{ij}}+a_{ij}p^{m_{ij}}| \equiv |a_{ij}p^{\varphi_{ij}}| \pmod{p}.$$

以故$|a_{ij}p^{\varphi_{ij}}|$對p爲互素或非互素,則與之合同之母式之行列式$|a_{ij}p^{\varphi_{ij}}+x_{ij}p^{m_{ij}}|$亦隨之對$p$爲互素或非互素也. 因之卽得本系.

系2. 整數l爲已知時,則母式(a_{ij})關於法l而有其逆之條件(必要而且充分者)爲其行列式$|a_{ij}|$對l須互素.

證明與前系者同樣. 但於此須留意者,卽法旣爲一整數l時,則

$$f_{ij}=1 \quad (i,j=1,2,\cdots\cdots,n)$$

(第112節), 因之整數項之母式皆含於集合$\mathfrak{M}_f(n,l)$[第111節者]者是也.

由本系則n次母式之中,其行列式對所與整數l互素者之相集成羣(關於法l)可知. 是卽關於法l之母式合同羣也.

系3. 於母式合同羣$\mathfrak{M}(n,l)$,其行列式與1合同(法l)者之母式相集乃作一正常約羣,而此約羣得由$n(n-1)$個之母元素

$$G_{rs} \quad (r\neq s;\ r,s=1,2,\cdots\cdots,n)$$

生成之.

證明. 在屬於$\mathfrak{M}(n,l)$之母式中,其行列式與1合同(法l)者之集合以$\mathfrak{U}$表之. $\mathfrak{U}$之二母式(a_{ij}), (b_{ij})之積之行列式爲

$$|a_{ij}|\cdot|b_{ij}|\equiv 1 \pmod{l}.$$

故$\mathfrak{U}$爲$\mathfrak{M}$之約羣,

復次,以(k_{ij})爲$\mathfrak{M}(n,l)$之任意之母式,以$(\overline{k}_{ij})$爲其逆(法l),則

$$|k_{ij}|\cdot|\overline{k}_{ij}|\equiv 1 \pmod{l}.$$

故在$\mathfrak{U}$之母式(a_{ij})爲(k_{ij})所變形之結果$(\overline{k}_{ij})(a_{ij})(k_{ij})$中,其行列式爲

$$|\overline{k}_{ij}|\cdot|a_{ij}|\cdot|k_{ij}|\equiv|a_{ij}|\equiv 1 \pmod{l}.$$

故 $(\overline{k_{ij}})(a_{ij})(k_{ij})$ 屬於 $\mathfrak{U}$, 因之 $\mathfrak{U}$ 於 $\mathfrak{M}(n, l)$ 爲正常也.

再次, 由前節定理,

$$(a_{ij}) \equiv \mathrm{J} \prod_{r,s} \mathrm{G}_{rs}^{z_{rs}},$$

$$\mathrm{J} = \begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & \triangle \end{pmatrix},$$

而 G_{rs} 之行列式明等於 1. 故

$$|a_{ij}| \equiv |\mathrm{J}| \equiv \triangle \pmod{l}.$$

故 (a_{ij}) 屬於 $\mathfrak{U}$ 時, 則

$$\triangle \equiv 1, \text{ 隨之 } \mathrm{J} \equiv (e_{ij}) \pmod{l}$$

爲必要, 卽 (a_{ij}) 得表之爲 G_{rs} 之積者也.

119. 母式之分解.

茲試就第 111 節之集合 $\mathfrak{M}_f(n, l_{ij})$, 其法母式之項 l_{ij} $(i, j=1, 2, \cdots\cdots, n)$ 之最小公倍數爲 l, 而 l 有二以上之相異素因數者論之.

令 l 分爲互素之兩因數

$$l = l^{(1)} l^{(2)} \quad (l^{(1)}, l^{(2)} > 1). \tag{1}$$

而選擇滿足

$$l^{(1)}x + l^{(2)}y = 1 \tag{2}$$

者之二整數 x, y. 若以

$$(3) \qquad l^{(1)}x=\kappa, \quad l^{(2)}y=\lambda,$$

則由上式得次之關係:

$$(4) \qquad \kappa+\lambda=1,$$

$$(5) \qquad \kappa\lambda\equiv 0, \quad \kappa^2\equiv\kappa, \quad \lambda^2\equiv\lambda \pmod{l},$$

$$(6) \qquad \begin{cases} \kappa\equiv 0, & \lambda\equiv 1 \pmod{l^{(1)}} \\ \kappa\equiv 1, & \lambda\equiv 0 \pmod{l^{(2)}}. \end{cases}$$

今母式 (a_{ij}) 屬於集合 $\mathfrak{M}_f(n, l_{ij})$ 時,則 $(a_{ij})\lambda$ 及 $(a_{ij})\kappa$ 亦復同樣.* 而 (a_{ij}) 由(4)分解爲 $\mathfrak{M}_f$ 之二母式之和,得

$$(7) \qquad (a_{ij})=(a_{ij})\lambda+(a_{ij})\kappa.$$

更以 (b_{ij}) 爲屬於 $\mathfrak{M}_f$ 之任意一母式,則由(5)得

$$(8) \qquad \left.\begin{aligned} &\{(a_{ij})\lambda\}\{(b_{ij})\kappa\}\equiv 0 \\ &\{(a_{ij})\lambda\}\{(b_{ij})\lambda\}\equiv\{(a_{ij})(b_{ij})\}\lambda \\ &\{(a_{ij})\kappa\}\{(b_{ij})\kappa\}\equiv\{(a_{ij})(b_{ij})\}\kappa \end{aligned}\right\} \pmod{(l_{ij})}.$$

茲於此而令 (a_{ij}) 及 (b_{ij}) 爲 (e_{ij}),則得

$$(9) \qquad \left.\begin{aligned} &\{(a_{ij})\lambda\}\{(e_{ij})\lambda\}\equiv(a_{ij})\lambda \\ &\{(e_{ij})\lambda\}\{(a_{ij})\lambda\}\equiv(a_{ij})\lambda \\ &\{(a_{ij})\kappa\}\{(e_{ij})\kappa\}\equiv(a_{ij})\kappa \\ &\{(e_{ij})\kappa\}\{(a_{ij})\kappa\}\equiv(a_{ij})\kappa \end{aligned}\right\} \pmod{(l_{ij})}.$$

再由(8),(9)得次之關係:

---

* 蓋因 $(a_{ij})\lambda=(x_{ij}f_{ij})\lambda=(\lambda a_{ij}f_{ij})$ 故.

$$(10)\qquad \{(a_{ij})\lambda+(e_{ij})\kappa\}\{(b_{ij})\lambda+(e_{ij})\kappa\}$$
$$\equiv\{(a_{ij})(b_{ij})\}\lambda+(e_{ij})\kappa \pmod{(l_{ij})},$$

$$(11)\qquad \{(a_{ij})\lambda+(e_{ij})\kappa\}\{(e_{ij})\lambda+(a_{ij})\kappa\}$$
$$\equiv(a_{ij})\lambda+(a_{ij})\kappa\equiv(a_{ij}) \pmod{(l_{ij})}.$$

此最後之式乃示當法母式之項之最小公倍數 l 有互異之素因數時，則集合 $\mathfrak{M}_f(n, l_{ij})$ 之母式 (a_{ij})，用 λ, κ，得以表示爲屬於同集合之二母式

$$(12)\qquad (a_{ij})\lambda+(e_{ij})\kappa,\quad (e_{ij})\lambda+(a_{ij})\kappa$$

之積者也.

特別當 (a_{ij}) 屬於合同羣 $\mathfrak{M}(n, l_{ij})$ 時，即其含有第 113 節之意義之逆時，則如次所示，(a_{ij}) 之因子 (12) 亦有逆，隨之亦屬於 $\mathfrak{M}$ 也.

$$(13)\qquad \left.\begin{aligned}&\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(a_{ij})^{-1}\lambda+(e_{ij})\kappa\}\equiv(e_{ij})\\&\{(e_{ij})\lambda+(a_{ij})\kappa\}\{(e_{ij})\lambda+(a_{ij})^{-1}\kappa\}\equiv(e_{ij})\end{aligned}\right\}\pmod{(l_{ij})}.$$

蓋由 (10)，則

$$\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(a_{ij})^{-1}\lambda+(e_{ij})\kappa\}\equiv\{(a_{ij})(a_{ij})^{-1}\}\lambda+(e_{ij})\kappa$$
$$\equiv(e_{ij})\lambda+(e_{ij})\kappa\equiv(e_{ij}) \pmod{(l_{ij})}$$

故.

120. 母式合同羣之分解.

茲以合同羣 $\mathfrak{M}(n, l_{ij})$ 之母式爲

$$(1)\qquad (a_{ij}),\quad (b_{ij}),\quad (c_{ij}),\quad \cdots\cdots;$$

而用前節所示之方法，將其各個均分解爲因子，以之爲

$$(2)\qquad \begin{aligned}(a_{ij})&\equiv\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(e_{ij})\lambda+(a_{ij})\kappa\},\\ (b_{ij})&\equiv\{(b_{ij})\lambda+(e_{ij})\kappa\}\{(e_{ij})\lambda+(b_{ij})\kappa\},\\ (c_{ij})&\equiv\{(c_{ij})\lambda+(e_{ij})\kappa\}\{(e_{ij})\lambda+(c_{ij})\kappa\},\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots.\end{aligned}$$

但均係就法(l_{ij})而取之者. 右邊之第一因子之集合

$$(3)\qquad (a_{ij})\lambda+(e_{ij})\kappa,\quad (b_{ij})\lambda+(e_{ij})\kappa,\quad (c_{ij})\lambda+(e_{ij})\kappa,\ \cdots\cdots$$

表以$\mathfrak{L}$; 第二因子之集合

$$(4)\qquad (e_{ij})\lambda+(a_{ij})\kappa,\quad (e_{ij})\lambda+(b_{ij})\kappa,\quad (e_{ij})\lambda+(c_{ij})\kappa,\ \cdots\cdots$$

表以$\mathfrak{K}$. 集合(3)之二母式相乘, 由前節(10), 得

$$\begin{aligned}&\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(b_{ij})\lambda+(e_{ij})\kappa\}\\ &\equiv\{(a_{ij})(b_{ij})\}\lambda+(e_{ij})\kappa\pmod{(l_{ij})},\end{aligned}$$

而此右邊亦屬於$\mathfrak{L}$. 蓋因母式$(a_{ij}),(b_{ij})$屬於羣$\mathfrak{M}$, 故其積$(a_{ij})(b_{ij})$亦與(1)之一個相合同(法(l_{ij}))故. 因之$\mathfrak{L}$形成$\mathfrak{M}$之約羣. 同樣, $\mathfrak{K}$亦$\mathfrak{M}$之約羣. 而(2)式乃所以示合同羣$\mathfrak{M}$之母式得以表之爲$\mathfrak{L}$之母式與$\mathfrak{K}$之母式之積者也. 然$\mathfrak{K},\mathfrak{L}$共爲$\mathfrak{M}$之約羣, 因之其積$\mathfrak{L}\mathfrak{K}$亦含於$\mathfrak{M}$. 故

$$(5)\qquad \mathfrak{M}(n,l_{ij})=\mathfrak{L}\mathfrak{K}.$$

欲明$\mathfrak{K},\mathfrak{L}$兩羣之關係, 乃作屬於各個之元素之積, 於是由前節(8),(9)得

$$\begin{aligned}\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(e_{ij})\lambda+(b_{ij})\kappa\}&\equiv(a_{ij})\lambda+(b_{ij})\kappa\pmod{(l_{ij})},\\ \{(e_{ij})\lambda+(b_{ij})\kappa\}\{(a_{ij})\lambda+(e_{ij})\kappa\}&\equiv(a_{ij})\lambda+(b_{ij})\kappa\pmod{(l_{ij})},\end{aligned}$$

而$\mathfrak{L}$之各母式與$\mathfrak{K}$之各母式爲交換可能也. 次求兩羣之

共通元素. 若

$$(a_{ij})\lambda+(e_{ij})\kappa\equiv(e_{ij})\lambda+(b_{ij})\kappa \pmod{(l_{ij})},$$

則兩邊乘以$(e_{ij})\lambda$, 而由前節(8)及(9)

$$(a_{ij})\lambda\equiv(e_{ij})\lambda \pmod{(l_{ij})}.$$

$$\therefore\quad (a_{ij})\lambda+(e_{ij})\kappa\equiv(e_{ij})\lambda+(e_{ij})\kappa\equiv(e_{ij}) \pmod{(l_{ij})}.$$

是卽兩羣之共通元素僅爲主母式. 因之, $\mathfrak{M}$等於$\mathfrak{L}$, $\mathfrak{R}$兩羣之直乘積可知也.

更進而就$\mathfrak{L}$及$\mathfrak{R}$一論. 乃以法母式(l_{ij})之項分解爲因數, 令之爲

$$l_{ij}=l_{ij}^{(1)}\,l_{ij}^{(2)}, \tag{6}$$

但$l_{ij}^{(1)}$爲含於$l^{(1)}$; $l_{ij}^{(2)}$爲含於$l^{(2)}$者. 同樣將f_{ij}分解, 令之爲

$$f_{ij}=f_{ij}^{(1)}\,f_{ij}^{(2)}.$$

(因f_{ij}乃l_{ij}之約數, 故此爲可能.) 然$l^{(1)}$, $l_{ij}^{(1)}$, $f_{ij}^{(1)}$ $(i, j=1, 2, \cdots\cdots, n)$之各個對於$l^{(2)}$, $l_{st}^{(2)}$, $f_{st}^{(2)}$ $(s, t=1, 2, \cdots\cdots, n)$之各個爲互素, 故由第110節(9)及第111節(4), 得

$$l_{ij}^{(1)}\,l_{jk}^{(1)}\equiv 0,\quad f_{ij}^{(1)}\,l_{jk}^{(1)}\equiv 0,\quad l_{ij}^{(1)}\,f_{jk}^{(1)}\equiv 0 \pmod{l_{ik}^{(1)}}$$

$$(i, j, k=1, 2, \cdots\cdots, n).$$

以故有

$$a_{ij}^{(1)}\,f_{ij}^{(1)}\quad (i, j=1, 2, \cdots\cdots, n)\quad [a_{ij}^{(1)}\text{爲整數}]$$

形者之母式, 關於法$(l_{ij}^{(1)})$之乘法爲一意的也. 且由f_{ij}之定法, 則$f_{ij}^{(1)}$乃適合

$$d_{ij}^{(1)} l_{jk}^{(1)} \equiv 0, \quad l_{ij}^{(1)} d_{jk}^{(1)} \equiv 0 \pmod{l_{ik}^{(1)}}$$

$$(i, j, k = 1, 2, \cdots\cdots, n)$$

之正整數 $d_{ij}^{(1)}$ 之最小值甚明. 因之此母式之集合,爲含有關於法 $(l_{ij}^{(1)})$ 之乘法爲一意的者之母式之最多數(互爲非合同者)者也. 於是依第112節之記法,此集合以 $\mathfrak{M}_f(n, l_{ij}^{(1)})$ 表之焉.

試取集合(1)之母式 (a_{ij}),則因此屬於 $\mathfrak{M}(n, l_{ij})$, 故 a_{ij} 爲 f_{ij} 之倍數. 然 f_{ij} 乃 $f_{ij}^{(1)}$ 之倍數. 故 a_{ij} 爲 $f_{ij}^{(1)}$ 之倍數,因之 (a_{ij}) 屬於 $\mathfrak{M}_f(n, l_{ij}^{(1)})$. 他之母式準此. 而(1)之母式,若係就法 $(l_{ij}^{(1)})$ 而取之者,則關於此乘法成羣焉. 是蓋因集合(1),就關於法 (l_{ij}) 之乘法言,本來成羣;加以因

$$(a_{ij})(b_{ij}) \equiv (c_{ij}), \quad (a_{ij})(\bar{a}_{ij}) \equiv (e_{ij}) \pmod{(l_{ij})},$$

即隨有

$$(a_{ij})(b_{ij}) \equiv (c_{ij}), \quad (a_{ij})(\bar{a}_{ij}) \equiv (e_{ij}) \pmod{l_{ij}^{(1)}})$$

故也. 此羣以 $\mathfrak{M}^{(1)}$ 示之. 然如上述,(1)之母式皆屬於 $\mathfrak{M}_f(n, l_{ij}^{(1)})$, 故 $\mathfrak{M}^{(1)}$ 或爲關於法 $(l_{ij}^{(1)})$ 之母式合同羣 $\mathfrak{M}(n, l_{ij}^{(1)})$, 或爲其約羣. 欲明其爲何,乃以 (h_{ij}) 爲 $\mathfrak{M}(n, l_{ij}^{(1)})$ 之任意母式,則

$$h_{ij} \equiv 0 \pmod{f_{ij}^{(1)}}.$$

然 $$\lambda \equiv 0 \pmod{l^{(2)}}, \quad l^{(2)} \equiv 0 \pmod{f_{ij}^{(2)}}, \quad f_{ij}^{(1)} f_{ij}^{(2)} = f_{ij}.$$

故 $$\lambda h_{ij} \equiv 0 \pmod{f_{ij}}.$$

以故母式$(h_{ij})\lambda$, 因之$(h_{ij})\lambda+(e_{ij})\kappa$屬於$\mathfrak{M}_f(n, l_{ij})$也. 復次, 乃以$(\bar{h}_{ij})$爲$(h_{ij})$之逆(法$(l_{ij}^{(1)})$), 卽

$$(h_{ij})(\bar{h}_{ij})=(e_{ij}+x_{ij}\, l_{ij}^{(1)}) \qquad [x_{ij} \text{爲整數}],$$

則與前同樣, $(\bar{h}_{ij})\lambda+(e_{ij})\kappa$亦屬於$\mathfrak{M}_f(n, l_{ij})$. 而

$$\begin{aligned}
&\{(h_{ij})\lambda+(e_{ij})\kappa\}\{(\bar{h}_{ij})\lambda+(e_{ij})\kappa\}\\
&=(h_{ij})(\bar{h}_{ij})\lambda^2+(e_{ij})^2\kappa^2+(h_{ij})(e_{ij})\lambda\kappa+(e_{ij})(\bar{h}_{ij})\kappa\lambda\\
&=(e_{ij}+x_{ij}\, l_{ij}^{(1)})\lambda^2+(e_{ij})\kappa^2+(h_{ij})\lambda\kappa+(\bar{h}_{ij})\kappa\lambda\\
&\equiv(e_{ij})\lambda+(e_{ij})k \pmod{(l_{ij})} \quad [\text{由前節 (5), (6)}]\\
&\equiv(e_{ij}) \pmod{(l_{ij})}.
\end{aligned}$$

夫如是, 母式$(h_{ij})\lambda+(e_{ij})\kappa$屬於$\mathfrak{M}_f(n, l_{ij})$, 而關於法$(l_{ij})$乃有其逆也. 故此屬於合同羣$\mathfrak{M}(n, l_{ij})$焉. 且由前節(6),

$$(h_{ij})\lambda+(e_{ij})\kappa\equiv(h_{ij}) \pmod{(l_{ij}^{(1)})}.$$

因之與$\mathfrak{M}(n, l_{ij}^{(1)})$之任意母式$(h_{ij})$相合同(法$(l_{ij}^{(1)})$)者必存在於集合(1)之中也. 卽羣$\mathfrak{M}^{(1)}$含有合同羣$\mathfrak{M}(n, l_{ij}^{(1)})$所有之母式. 故

$$\mathfrak{M}^{(1)}=\mathfrak{M}(n, l_{ij}^{(1)}). \tag{7}$$

總之, 集合(1)之母式, 若係就法$(l_{ij}^{(1)})$而取之者, 則關於其乘法, 乃作合同羣$\mathfrak{M}(n, l_{ij}^{(1)})$焉.

復次請就羣$\mathfrak{M}(n, l_{ij}^{(1)})$與$\mathfrak{L}$之關係一論. 今先比較兩者之元數. 於(3)之母式, 若

$$(a_{ij})\lambda+(e_{ij})\kappa\equiv(a'_{ij})\lambda+(e_{ij})\kappa \pmod{(l_{ij})},$$

則由前節(6),

$$(a_{ij})\equiv(a'_{ij}) \pmod{(l_{ij}^{(1)})}$$

爲必要也. 反之,於此時,若以 λ 乘之,則

$$(a_{ij})\lambda\equiv(a'_{ij})\lambda \pmod{(\lambda l_{ij}^{(1)})}.$$

然

$$\lambda\equiv 0 \pmod{l_{ij}^{(2)}}.$$

故

$$(a_{ij})\lambda\equiv(a'_{ij})\lambda \pmod{(l_{ij})}.$$

$$\therefore\ (a_{ij})\lambda+(e_{ij})\kappa\equiv(a'_{ij})\lambda+(e_{ij})\kappa \pmod{(l_{ij})}.$$

因之集合(3)之母式中,其關於法 (l_{ij}) 爲非合同者之數,與集合(1)之母式內關於法 $(l_{ij}^{(1)})$ 爲非合同者之數相等也. 故 $\mathfrak{L}$, $\mathfrak{M}(n, l_{ij}^{(1)})$ 兩羣之元數一致. 次若

$$\{(a_{ij})\lambda+(e_{ij})\kappa\}\{(b_{ij})\lambda+(e_{ij})\kappa\}\equiv(c_{ij})\lambda+(e_{ij})\kappa \pmod{(l_{ij})},$$

則由前節(10),得

$$(a_{ij})(b_{ij})\equiv(c_{ij}) \pmod{(l_{ij}^{(1)})}.$$

故若對(3)之母式

$$(a_{ij})\lambda+(e_{ij})\kappa,\quad (b_{ij})\lambda+(e_{ij})\kappa,\quad \cdots\cdots,$$

分別以(1)之母式

$$(a_{ij}),\quad (b_{ij}),\quad \cdots\cdots$$

使與對應,則 $\mathfrak{L}$ 與 $\mathfrak{M}(n, l_{ij}^{(1)})$ 之爲單純同態可知.

同樣,$\mathfrak{R}$ 之與關於法 $(l_{ij}^{(2)})$ 者之母式合同羣爲同型,亦同上得證. 綜合上述,得次

定理. 令 $l_{ij}(i, j=1, 2, \cdots\cdots, n)$ 之最小公倍數爲 l, 其分

解爲互素之因數乃爲

$$l=l^{(1)}l^{(2)}$$

而 l_{ij} 分解爲因數，則爲

$$l_{ij}=l_{ij}^{(1)}\,l_{ij}^{(2)},$$

但 $l_{ij}^{(1)}$ 爲含於 $l^{(1)}$；$l_{ij}^{(2)}$ 爲含於 $l^{(2)}$ 者. 於是其關於法 (l_{ij}) 之母式合同羣，乃與關於法 $(l_{ij}^{(1)})$ 之母式合同羣之同型羣，以及關於法 $(l_{ij}^{(2)})$ 之母式合同羣之同型羣之直乘積等.

由本定理即得次

定理. 若 $l_{ij}=p^{m_{ij}}q^{n_{ij}}\cdots\cdots$，則關於法 (l_{ij}) 之母式合同羣，與以

$$(p^{m_{ij}}),\quad (q^{n_{ij}}),\quad \cdots\cdots$$

分別爲法之母式合同羣之同型羣之直乘積等. 但 $p, q, \cdots\cdots$ 爲互異之素數.

系. $l=p^{\mu}q^{\nu}\cdots\cdots$ ($p,q,\cdots\cdots$ 爲互異之素數)時，則關於法 l 之母式合同羣，與以 $p^{\mu}, q^{\nu}, \cdots\cdots$ 分別爲法之母式合同羣之同型羣之直乘積等. (Jordan 氏之定理.)

在第二定理中之分解，其可能固已示之矣，但實際行之，則如次也可.

將法母式之項 l_{ij} 以及其最小公倍數 l 分解爲素因數:

$$l=p^{m}p_1{}^{m'}\cdots\cdots \quad (p,p_1,\cdots\cdots \text{爲互異之素數})$$
$$=qq'\cdots\cdots \quad (q=p^{m},\ q'=p_1{}^{m'},\ \cdots\cdots)$$

$$l_{ij}=q_{ij}q'_{ij}\cdots\cdots\quad(q_i=p^{m_{ij}},\ q'_{ij}=p_1^{m'_{ij}},\ \cdots\cdots).$$

於是 $\frac{l}{q}$, $\frac{l}{q'}$, …… 之最大公約數爲1.

故適合

$$\frac{lx}{q}+\frac{lx_1}{q'}+\cdots\cdots=1$$

者之整數 $x, x_1, \cdots\cdots$ 得以選擇之也. 若令

$$\frac{lx}{q}=\lambda,\quad \frac{lr_1}{q'}=\lambda_1,\ \cdots\cdots,$$

則得

$$\lambda+\lambda_1+\cdots\cdots=1,$$

$$\left.\begin{aligned}&\lambda_i\lambda_j\equiv 0\quad(i\neq j)\\&\lambda_i^2\equiv\lambda_i\end{aligned}\right\}\ (\mathrm{mod.}\ l)$$

$$(i, j=0, 1, 2, \cdots\cdots),$$

$$\lambda_i\equiv 1,\quad \lambda_j\equiv 0\quad(\mathrm{mod.}\ q^{(i)})\quad[j\neq i].$$

以是諸λ, 則母式 (a_{ij}) 得表之爲次之各個之積也:

$$(a_{ij})\lambda+(e_{ij})\lambda_1+(e_{ij})\lambda_2+\cdots\cdots,$$

$$(e_{ij})\lambda+(a_{ij})\lambda_1+(e_{ij})\lambda_2+\cdots\cdots,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots.$$

此中第一因子之集合, 乃形成與 $\mathfrak{M}(n, q_{ij})$ 同型之羣(關於法 (l_{ij}) 者), 第二因子之集合, 則形成與 $\mathfrak{M}(n, q'_{ij})$ 同型之羣(法 (l_{ij}))以下準此.

121. 若有若干個母式爲屬於第111節所定義之集合

$\mathfrak{M}_f(n, l_{ij})$者，就其關於法$(l_{ij})$之乘法言形成一羣時，* 則此羣(名之曰$\mathfrak{G}$)與合同羣$\mathfrak{M}(n, l_{ij})$或有共通之母式，或則無有. 以後者論，則$\mathfrak{G}$之主元素不得爲主母式. 嚴格言之，卽$\mathfrak{G}$之主元素，關於法$(l_{ij})$，不與主母式$(e_{ij})$相合同也. 以前者言，以$\mathfrak{G}$與$\mathfrak{M}$之最大公約羣爲$\mathfrak{D}$，則$\mathfrak{D}$之不得不含$\mathfrak{M}$之主元素卽主母式也甚明.† 故$\mathfrak{G}$亦含主母式，因之爲$\mathfrak{M}$之約羣(參照第113節). 爰得

定理. 由集合$\mathfrak{M}_f(n, l_{ij})$中若干個母式所成之羣(關於法$(l_{ij})$之乘法者)，隨其主元素之與主母式相合同(法$(l_{ij})$)與否，而爲合同羣$\mathfrak{M}(n, l_{ij})$之約羣或全然與之無共通之母式.

今欲示本定理以實例及關於$\mathfrak{M}(n, l_{ij})$之分解一·言，乃就彼取前節(3)中各母式之第一項而作成之集合

$$(1) \qquad (a_{ij})\lambda, \quad (b_{ij})\lambda, \quad (c_{ij})\lambda, \cdots\cdots$$

一論. 由第119節(8), (9)，則有

$$\left.\begin{aligned} &\{(a_{ij})\lambda\}\{(b_{ij})\lambda\} \equiv \{(a_{ij})(b_{ij})\}\lambda \\ &\{(a_{ij})\lambda\}\{(e_{ij})\lambda\} \equiv (a_{ij})\lambda \\ &\{(a_{ij})\lambda\}\{(a_{ij})^{-1}\lambda\} \equiv (e_{ij})\lambda \end{aligned}\right\} (\text{mod. } (l_{ij})),$$

故集合(1)，就關於法(l_{ij})之乘法言，乃成羣也；而於其中，則

---

*凡關於法(l_{ij})而相合同之母式$(\mathfrak{M}_f$的)概以其視爲同一者而討論之爲便. 故如母式(a_{ij})屬於$\mathfrak{G}$時，則凡與是相合同(法(l_{ij}))之母式，概視爲含於$\mathfrak{G}$者也. 至用語則亦因此而以簡略者行之.

†以有限羣之約羣必含其羣之主元素故也.

$(e_{ij})\lambda$ 爲羣之主元素. 此羣以 $\mathfrak{H}$ 表之. $\mathfrak{H}$ 之元數與 $\mathfrak{L}$ 之元數一致. 蓋於(1), 若

$$(a_{ij})\lambda \equiv (a'_{ij})\lambda \pmod{(l_{ij})},$$

則對前節(3)之母式, 乃有

$$(a_{ij})\lambda + (e_{ij})\kappa \equiv (a'_{ij})\lambda + (e_{ij})\kappa \pmod{(l_{ij})},$$

而其逆亦成立故也. 至 $\mathfrak{H}$ 與 $\mathfrak{L}$ 爲同態亦甚明焉.

$\mathfrak{H}$ 含於 $\mathfrak{M}$ 與否, 由其主元素與主母式合同(法 (l_{ij}))與否而定. 若以 $\mathfrak{H}$ 之主元素爲與主母式合同(法 (l_{ij}))者, 則有

$$(2) \qquad (e_{ij})\lambda \equiv (e_{ij}) \equiv (e_{ij})\lambda + (e_{ij})\kappa \pmod{(l_{ij})}.$$

故

$$(3) \qquad (e_{ij})\kappa \equiv 0 \pmod{(l_{ij})}$$

爲必要也, 因之 $\mathfrak{H}$ 與 $\mathfrak{L}$ 一致. 更就(3)之成立而討論之. 因由此, 乃有

$$\kappa \equiv 0 \pmod{l_{ii}} \qquad (i=1, 2, \cdots\cdots, n).$$

$$\therefore \quad \kappa \equiv 0 \pmod{l_{ii}^{(2)}} \qquad (i=1, 2, \cdots\cdots, n).$$

然由第119節(6),

$$\kappa \equiv 1 \pmod{l_{ii}^{(2)}} \qquad (i=1, 2, \cdots\cdots, n).$$

故

$$1 \equiv 0 \pmod{l_{ii}^{(2)}} \qquad (i=1, 2, \cdots\cdots, n).$$

因之

$$(4) \qquad l_{11}^{(2)} = l_{22}^{(2)} = \cdots\cdots = l_{nn}^{(2)} = 1.$$

是卽 $\mathfrak{H}$ 之主元素與主母式合同(法 (l_{ij}))之條件也. 反之, 此

條件得滿足時，則 $\mathfrak{S}$ 之主元素與主母式合同(法 (l_{ij})).

又條件(4)如成立時，則就 $\mathfrak{M}(n, l_{ij})$ 尚有一言. 此時 $\mathfrak{R}$ 乃主元素羣也. 蓋若取 $\mathfrak{R}$ 之一母式(前節(4))，則有

$$(e_{ij})\lambda+(a_{ij})\kappa=\{(e_{ij})\lambda+(a_{ij})\kappa\}(e_{ij})$$
$$=(e_{ij})\lambda+(a_{ij})\cdot(e_{ij})\kappa$$
$$\equiv(e_{ij}) \quad (\text{mod. } (l_{ij})) \quad [\text{由 (2) 及 (3)}]$$

故耳(參照第113節末). 而由前節(5)，乃有

$$\mathfrak{M}(n, l_{ij})=\mathfrak{L}\mathfrak{R}=\mathfrak{L}\cdot 1.$$

因之此時 $\mathfrak{M}$ 與 $\mathfrak{L}$ 爲單純同態也.

第十九章. 法母式之項爲素數羃者

122. 母式合同羣之元數(法爲 p^{μ} 時).

由第112節所述，$m_{ij}=\mu$ $(i, j=1, 2, \cdots\cdots, n)$ 時，$f_{ij}=1$，因之合同羣 $\mathfrak{M}(n, p^{\mu})$ 之母式乃有次形:

$$(1) \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{pmatrix} \quad (\text{mod. } p^{\mu});$$

而此羣之元數，則與對 a_{ij} 與以

$$(2) \qquad 0, 1, 2, \cdots\cdots, p^{\mu}-1,$$

於其所得 $p^{\mu n^2}$ 個之母式中，其行列式 $|a_{ij}|$ 不能以 p 整除

者之個數等. 此數以 $g(n, p^\mu)$ 表之,而求之之法,分爲次之三段.

1°. 於 $\mathfrak{M}(n, p^\mu)$, 其有

$$(3)\qquad a_{11}\equiv 1,\ a_{12}\equiv a_{13}\equiv\cdots\cdots\equiv a_{1n}\equiv 0 \pmod{p^\mu}$$

者之母式

$$(4)\qquad \begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ a'_{21} & a'_{22} & a'_{23} & \cdots\cdots & a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a'_{n1} & a'_{n2} & a'_{n3} & \cdots\cdots & a'_{nn} \end{pmatrix} \pmod{p^\mu}$$

之集合,形成 $\mathfrak{M}$ 之約羣甚明. 此以 $\mathfrak{M}'$ 表之. 母式(4)之行列式乃等於

$$(5)\qquad \begin{vmatrix} a'_{22} & a'_{23} & \cdots\cdots & a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a'_{n2} & a'_{n3} & \cdots\cdots & a'_{nn} \end{vmatrix}$$

故(4)之行列式欲對 p 爲互素,則行列式(5)之不得以 p 整除爲必要而且充分也. 因之對其 $n-1$ 個項 $a'_{21}, a'_{31}, \cdots\cdots, a'_{n1}$, 雖以(2)中之任何值與之亦無所不可. 然(5)不能以 p 整除時,則其以

$$\begin{pmatrix} a'_{22} & a'_{23} & \cdots\cdots & a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a'_{n2} & a'_{n3} & \cdots\cdots & a'_{nn} \end{pmatrix} \pmod{p^\mu}$$

所表示之母式之集合,乃成一 $n-1$ 次合同羣(法 p^μ);而其元數,用上述之記號,則爲 $g(n-1, p^\mu)$. 此數也,卽表示選擇

a'_{ij} $(i, j=2, 3, \cdots\cdots, n)$, 使行列式(5)不爲零(法 p)者之方法之數者也. 但 $a'_{21}, a'_{31}, \cdots\cdots, a'_{n1}$ 之選法有 $p^{(n-1)\mu}$ 種. 故 $\mathfrak{M}'$ 之元數爲

$$p^{(n-1)\mu}\, g\,(n-1, p^{\mu}). \tag{6}$$

2°. 試求 $\mathfrak{M}(n, p^{\mu})$ 之元數與 $\mathfrak{M}'$ 之元數之關係.

以母式(1)右乘於(4), 則其積爲

$$\begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a''_{21} & a''_{22} & \cdots\cdots & a''_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a''_{n1} & a''_{n2} & \cdots\cdots & a''_{nn} \end{pmatrix} \pmod{p^{\mu}},$$

而其第一列又與(1)中者同一. 故(1)若示以 A, 則屬於傍系 $\mathfrak{M}'$A 之母式之第一列與 A 之第一列同一也. 反之, 若母式 A′ 之第一列與於 A 者同一時, 則積 A′A^{-1} 取(4)之形, 因而 A′ 屬於 $\mathfrak{M}'$A 也. 蓋若令 A$^{-1}=(\bar{a}_{ij})$, 則積 A′A^{-1} 之第一列爲

$$\sum_{j=1}^{n} a_{ij}\,\bar{a}_{jk} \pmod{p^{\mu}} \qquad (k=1, 2, \cdots\cdots, n).$$

然 AA$^{-1}\equiv(e_{ij})$ (mod. p^{μ}), 故

$$\sum_{j=1}^{n} a_{1j}\,\bar{a}_{jk}\equiv e_{1k} \pmod{p^{\mu}}.$$

故積 A′A^{-1} 之第一列爲 e_{1k} (mod. p^{μ}), 卽

$$1, 0, 0, \cdots\cdots, 0 \pmod{p^{\mu}},$$

因之此積屬於 $\mathfrak{M}'$.

於是將 $\mathfrak{M}$ 就 $\mathfrak{M}'$ 分爲傍系,則得

$$\mathfrak{M}=\Sigma\,\mathfrak{M}'\,\mathrm{A}. \tag{7}$$

故 A (卽 (1)) 要屬於 $\mathfrak{M}$, 則 $\alpha_{11}, \alpha_{12}, \cdots\cdots, \alpha_{1n}$ 不得有 p 爲公約數也. 反之,若此諸數不有 p 爲其公約數時,則以此諸數爲第一列之母式,必存在於 $\mathfrak{M}$. 蓋若 $\alpha_{11}\not\equiv 0 \pmod{p}$, 則取

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots\cdots & \alpha_{1n} \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 1 & \cdots\cdots & 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 & 0 & 0 & \cdots\cdots & 1 \end{pmatrix};$$

而若 $\alpha_{1i}\not\equiv 0 \pmod{p}$, 則於 (1) 令

$$\alpha_{i1}=1,\ \alpha_{22}=\cdots\cdots=\alpha_{i-1,\,i-1}=\alpha_{i+1,\,i+1}=\cdots\cdots=\alpha_{nn}=1,$$ 而

以其他爲零(但第一橫列則仍舊),於是此行列式爲 $\pm\alpha_{1i}$, 而不能以 p 整除故也. 因之 (7) 之右邊中傍系之數,與自 p^{μ} 個數 (2) 之中選擇 n 個數之不以 p 爲公約數者之選法(容許同一數之重複者)爲同數.

由 p^{μ} 個數 (2) 選 n 個數(容許同一數之重複)之方法乃有 $p^{n\mu}$ 種. 此中以 p 爲公約數者,僅爲 p 之倍數者也. 然 (2) 中 p 之倍數,有

$$0,\ p,\ \ 2p,\ \cdots\cdots,\ (p^{\mu-1}-1)p$$

之 $p^{\mu-1}$ 個,而由之以選 n 個(同一數之重複爲所允許),其方法有 $p^{n(\mu-1)}$ 種. 故以 $p^{n\mu}-p^{n(\mu-1)}$ 種之方法,得自 (2) 中選擇

不以 p 爲公約數者之 n 個數也. 因之 $\mathfrak{M}$ 之元數, 由 (7), 爲 $\mathfrak{M}'$ 之元數之 $p^{n\mu}-p^{n(\mu-1)}$ 倍. 故由 (6) 得

$$(8)\quad g(n, p^{\mu})=(p^{n\mu}-p^{n(\mu-1)})p^{(n-1)\mu}\, g(n-1, p^{\mu})$$
$$=p^{(2n-1)\mu}\left(1-\frac{1}{p^{n}}\right) g(n-1, p^{\mu}).$$

3°. 由 (8),

$$g(n, p^{\mu})=p^{(2n-1)\mu}\left(1-\frac{1}{p^{n}}\right) g(n-1, p^{\mu}),$$

$$g(n-1, p^{\mu})=p^{(2n-3)\mu}\left(1-\frac{1}{p^{n-1}}\right) g(n-2, p^{\mu}),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$g(2, p^{\mu})=p^{3\mu}\left(1-\frac{1}{p^{2}}\right) g(1, p^{\mu});$$

而一次母式

$$(0), (1), \cdots\cdots, (p^{\mu}-1)$$

之中, 行列式 (分別爲 0, 1, ……, $p^{\mu}-1$) 之對 p 爲互素者之數有 $p^{\mu}\left(1-\frac{1}{p}\right)$ 個. 故

$$g(1, p^{\mu})=p^{\mu}\left(1-\frac{1}{p}\right).$$

上式邊邊相乘且簡約之, 得

$$(9)\quad g(n, p^{\mu})=p^{\mu(1+3+\cdots\cdots+\overline{2n-1})}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^{2}}\right)\cdots\cdots\left(1-\frac{1}{p^{n}}\right)$$
$$=p^{n^{2}\mu}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^{2}}\right)\cdots\cdots\left(1-\frac{1}{p^{n}}\right).$$

是卽所要之數, 卽 n 次母式合同羣 (法 p^{μ}) 之元數也.

特別 $\mu=1$ 時, 則

(10) $g(n, p)=(p^n-1)(p^n-p)\cdots\cdots(p^n-p^{n-1})$.

例. 關於法5之二次母式合同羣之元數,由(10)爲

$$g(2, 5)=(5^2-1)(5^2-5)=480.$$

又關於法3^2之二次母式合同羣之元數,由(9)爲

$$g(2, 3^2)=3^{2^2\cdot 2}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3^2}\right)=3^5\cdot 2^4=3888.$$

123. $m_{ij}=m_j$ **時.**

令 $m_1\geqq m_2\geqq\cdots\cdots\geqq m_n$. 此時 n 次母式合同羣 $\mathfrak{M}(n, p^{m_{ij}})$ 之元素,乃有

$$(1)\qquad \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots\cdots a_{1n} \\ a_{21}p^{m_1-m_2} & a_{22} & a_{23} & \cdots\cdots a_{2n} \\ a_{31}p^{m_1-m_3} & a_{32}p^{m_2-m_3} & a_{33} & \cdots\cdots a_{3n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1}p^{m_1-m_n} & a_{n2}p^{m_2-m_n} & a_{n3}p^{m_3-m_n} & \cdots\cdots a_{nn} \end{pmatrix}$$

之形(第112節). 此中 a_{ij}, 當 $i\leqq j$ 時,就法 p^{m_j} 而取之; 而 $i>j$ 時,則就 p^{m_i} 而取之可. 爲求此羣之元數計,先以 $m_1, m_2, \cdots\cdots, m_n$ 中之相等者爲一組,而此組數以爲 ν 個. 其最初之 n_1 個 $m_1, m_2, \cdots\cdots, m_{n_1}$ 令等於 μ_1, 次之 (n_2-n_1) 個等於 μ_2, $\cdots\cdots$, 最後之 $(n_\nu-n_{\nu-1})$ 個令等於 μ_ν (但 $\mu_1>\mu_2>\cdots\cdots>\mu_\nu$), 卽以 $m_1, m_2, \cdots\cdots, m_n$, 換書之爲

$$\underbrace{\mu_1, \mu_1, \cdots\cdots, \mu_1}_{n_1},\ \underbrace{\mu_2, \mu_2, \cdots\cdots, \mu_2}_{n_2-n_1},\ \cdots\cdots,\ \underbrace{\mu_\nu, \mu_\nu, \cdots\cdots, \mu_\nu}_{n_\nu-n_{\nu-1}} \quad (n_\nu=n)$$

者. 於是母式(1)之項如次:

$$1\leqq i, j\leqq n_1: \quad a_{ij} \pmod{p^{\mu_1}},$$
$$n_1+1\leqq i, j\leqq n_2: \quad a_{ij} \pmod{p^{\mu_2}},$$
$$\cdots\cdots\cdots\cdots \quad \cdots \quad \cdots\cdots\cdots\cdots$$
$$n_{\nu-1}+1\leqq i, j\leqq n_\nu: \quad a_{ij} \pmod{p^{\mu_\nu}},$$

$$\left.\begin{matrix} n_1+1\leqq i\leqq n_2 \\ 1\leqq j\leqq n_1 \end{matrix}\right\}: \ a_{ij}p^{\mu_1-\mu_2} \pmod{p^{\mu_1}}, \text{ 因之 } a_{ij} \pmod{p^{\mu_2}},$$

$$\left.\begin{matrix} \left.\begin{matrix} n_2+1\leqq i\leqq n_3 \\ 1\leqq j\leqq n_1 \end{matrix}\right\}: \ a_{ij}p^{\mu_1-\mu_3} \pmod{p^{\mu_1}} \\ \left.\begin{matrix} n_2+1\leqq i\leqq n_3 \\ n_1+1\leqq j\leqq n_2 \end{matrix}\right\}: \ a_{ij}p^{\mu_2-\mu_3} \pmod{p^{\mu_2}} \end{matrix}\right\}, \text{ 因之 } a_{ij} \pmod{p^{\mu_3}},$$

$$\cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots$$

$$\left.\begin{matrix} n_{\nu-1}+1\leqq i\leqq n_\nu \\ 1\leqq j\leqq n_1 \end{matrix}\right\}: \ a_{ij}p^{\mu_1-\mu_\nu} \pmod{p^{\mu_1}}$$

$$\left.\begin{matrix} \left.\begin{matrix} n_{\nu-1}+1\leqq i\leqq n_\nu \\ n_1+1\leqq j\leqq n_2 \end{matrix}\right\}: \ a_{ij}p^{\mu_2-\mu_\nu} \pmod{p^{\mu_2}} \\ \cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots \\ \left.\begin{matrix} n_{\nu-1}+1\leqq i\leqq n_\nu \\ n_{\nu-2}+1\leqq j\leqq n_{\nu-1} \end{matrix}\right\}: \ a_{ij}p^{\mu_{\nu-1}-\mu_\nu} \pmod{p^{\mu_{\nu-1}}} \end{matrix}\right\} \text{ 因之 } a_{ij} \pmod{p^{\mu_\nu}},$$

$$\left.\begin{matrix} 1\leqq i\leqq n_1 \\ n_1+1\leqq j\leqq n_2 \end{matrix}\right\}: \ a_{ij} \pmod{p^{\mu_2}},$$

$$\left.\begin{matrix} 1 \leqq i \leqq n_2 \\ n_2+1 \leqq j \leqq n_3 \end{matrix}\right\} : a_{ij} \pmod{p^{\mu_3}},$$

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

$$\left.\begin{matrix} 1 \leqq i \leqq n_{\nu-1} \\ n_{\nu-1}+1 \leqq j \leqq n_\nu \end{matrix}\right\} : a_{ij} \pmod{p^{\mu_\nu}}.$$

若爲更易明了起見,則記載之如次表:

	n_1	n_2-n_1	n_3-n_2		$n_\nu-n_{\nu-1}$
n_1	a_{ij} (mod. p^{μ_1})	a_{ij} (mod. p^{μ_2})	a_{ij} (mod. p^{μ_3})		
n_2-n_1	$a_{ij}p^{\mu_1-\mu_2}$ (mod. p^{μ_1})	a_{ij} (mod. p^{μ_2})			
n_3-n_2	$a_{ij}p^{\mu_1-\mu_3}$ (mod. p^{μ_1})	$a_{ij}p^{\mu_2-\mu_3}$ (mod. p^{μ_2})	a_{ij} (mod. p^{μ_3})		a_{ij} (mod. p^{μ_ν})
$n_\nu-n_{\nu-1}$	$a_{ij}p^{\mu_1-\mu_\nu}$ (mod. p^{μ_1})	$a_{ij}p^{\mu_2-\mu_\nu}$ (mod. p^{μ_2})		$a_{ij}p^{\mu_{\nu-1}-\mu_\nu}$ (mod. $p^{\mu_{\nu-1}}$)	a_{ij} (mod. p^{μ_ν})

母式(1)以A亦之;其中沿對角線之小母式:

$$(a_{ij})\quad i,j=1,2,\cdots\cdots,n_1\qquad (n_1\text{次}),$$

$$(a_{ij})\quad i,j=n_1+1,\cdots\cdots,n_2\qquad (n_2-n_1\text{次}),$$

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

$$(a_{ij})\quad i,j=n_{\nu-1}+1,\cdots\cdots,n_\nu\qquad (n_\nu-n_{\nu-1}\text{次}),$$

卽上圖表中用粗線所識者,分別以 $A_1, A_2, \cdots\cdots, A_\nu$ 表之;而其行列式又分別以 $|A_1|, |A_2|, \cdots\cdots, |A_\nu|$ 表之,則A之行列式 $|A|$,由上表,爲

$$|A| \equiv |A_1| \cdot |A_2| \cdot \cdots\cdots |A_\nu| \pmod{p}.$$

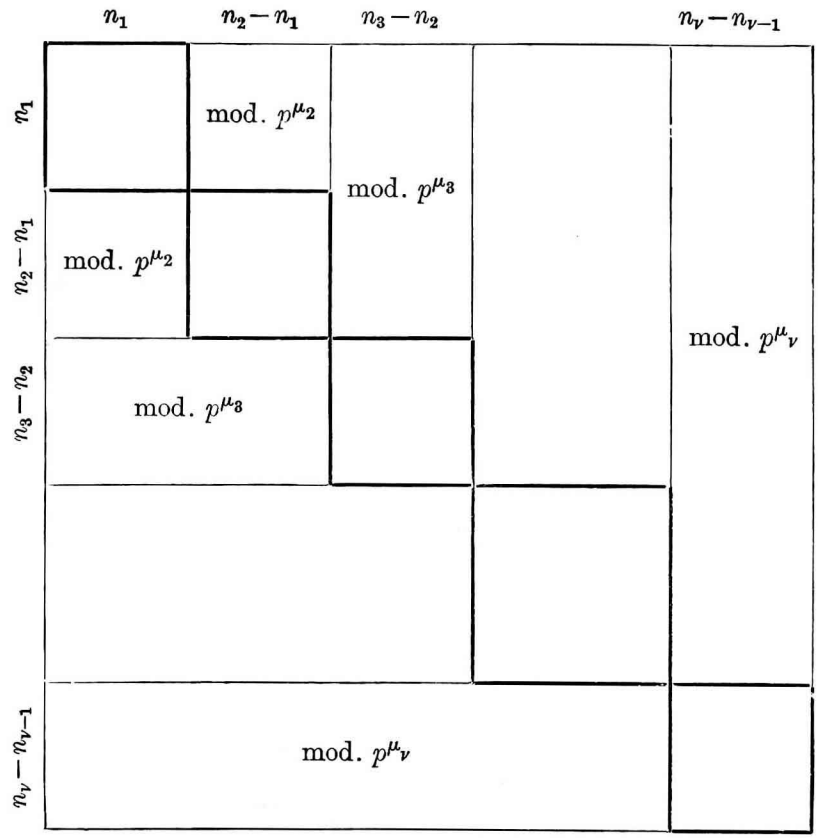
(應用行列式之展開定理.) 故 $|A|$ 欲對 p 互素,則 $|A_1|, |A_2|, \cdots\cdots, |A_\nu|$ 各個之不能以 p 整除爲必要而且充分者也. 因之對於不屬諸此等小行列式之項,雖以任何值與之,亦無所不可.

且選擇其項 a_{ij} 使 $|A_i|$ 不能以 p 整除者之選法,換言之,在關於法 p^{μ_i} 互爲非合同者之 (n_i-n_{i-1}) 次母式中,其行列式不能以 p 整除者之數,如前節所示爲

$$g(n_i-n_{i-1}, p^{\mu_i})=p^{(n_i-n_{i-1})^2\mu_i}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\cdots\left(1-\frac{1}{p^{n_i-n_{i-1}}}\right).$$

但 $n_0=0$.

其次在A之項中,其不屬於小母式 $A_1, A_2, \cdots\cdots, A_\nu$ 者之因子 a_{ij} 果須就如何之法而始得取之乎? 則由上表,知爲



也. 故若是者之 a_{ij} 之選法, 總計之有

$$\{p^{n_1(n_2-n_1)\mu_2}p^{n_2(n_3-n_2)\mu_3}\cdots\cdots p^{n_{\nu-1}(n_\nu-n_{\nu-1})\mu_\nu}\}^2.$$

種. 因之選擇 a_{ij} 使 $|A|$ 不能以 p 整除者之選法之數, 卽在關於法 $(p^{m_{ij}})$ 互爲非合同者之 n 次母式中, 其行列式對 p 爲互素者之數爲

$$\prod_{i=1}^{\nu} g\,(n_i-n_{i-1},\ p^{\mu_i}) \prod_{k=1}^{\nu} p^{2n_k-1\ (n_k-n_{k-1})\mu_k} \qquad [n_0=0]$$

也. 計算之則爲

$$(2)\quad p^{\sum_{i=1}^{\nu}(n_i^2-n_{i-1}^2)\mu_i} \prod_{i=1}^{\nu}\prod_{k=1}^{n_i-n_{i-1}}\left(1-\frac{1}{p^k}\right) \qquad [n_0=0]$$

焉. 爰得

定理. 於 n 次母式 $(p^{m_{ij}})$, 若

$$m_{ij}=m_j \quad (i, j=1, 2, \cdots\cdots, n),$$

$$m_{n_{k-1}+1}=m_{n_{k-1}+2}=\cdots\cdots=m_{n_k}=\mu_k$$

$$(n_\nu=n,\ n_0=0;\ k=1, 2, \cdots\cdots, \nu)$$

時, 則關於法 $(p^{m_{ij}})$ 之母式合同羣之元數, 得以上之(2)與之.

例. 以 $\begin{pmatrix}3^2 & 3\\ 3^2 & 3\end{pmatrix}$ 爲法時, 則合同羣之元數, 於(2)令 $p=3$, $n_1=1$, $\mu_1=2$, $n_2-n_1=1$, $\mu_2=1$, 知爲

$$3^{1^2\cdot 2+(2^2-1^2)\cdot 1}\left(1-\frac{1}{3}\right)\left(1-\frac{1}{3}\right)=108.$$

注意. 定理之證明, 乃就法母式之指數爲

$$m_1\geqq m_2\geqq\cdots\cdots\geqq m_n$$

時而論之者. 若此關係不能滿足, 可將母式之縱行交換, 由左移右, 使 p 之冪降下而換書之; 再適用上記之方法可得到全然同樣之結果(參照第114節第一定理). 又法母式雖不適合定理之條件時, 然在同一方針之下, 合同羣之元

數可以求得,而其結果亦全然類似也.

124. 指數列.

就關於法 p^μ ($\mu \geqq 1$) 之母式合同羣 $\mathfrak{M}(n, p^\mu)$ 言,其指數列分次之五段述之.

1°. 令合同羣 $\mathfrak{M}(n, p^\mu)$ 之母式爲

$$(a_{ij}),\ (b_{ij}),\ (c_{ij}),\ \cdots\cdots, \tag{1}$$

此中若

$$(a_{ij})(b_{ij}) \equiv (c_{ij}) \pmod{p^\mu}, \tag{2}$$

則因 $\mu \geqq 1$ 之故,

$$(a_{ij})(b_{ij}) \equiv (c_{ij}) \pmod{p}, \tag{3}$$

明已. 故 (1) 之母式,就關於法 p 之乘法言,成羣也;且此羣又不外乎母式合同羣 $\mathfrak{M}(n, p)$ 焉. 蓋若 (d_{ij}) 爲 $\mathfrak{M}(n, p)$ 之一母式,則由第 118 節系 2,

$$|d_{ij}| \not\equiv 0 \pmod{p}$$

爲必要,因之由同系,則與 (d_{ij}) 合同(法 p^μ)之母式不得不含於 (1) 中故也.

茲對於 $\mathfrak{M}(n, p^\mu)$ 之母式

$$(a_{ij}),\ (b_{ij}),\ (c_{ij}),\ \cdots\cdots \pmod{p^\mu},$$

---

*關於此請參閱 Ranum, The groups of classes of congruent matrices, with application of the group of isomorphisms of any abelian group. Trans. Amer Math. Soc. Vol. 8 (1907).

分別使 $\mathfrak{M}(n, p)$ 之母式

$$(a_{ij}), (b_{ij}), (c_{ij}), \cdots\cdots \pmod{p}$$

相與對應，則由(2)及(3)之關係，$\mathfrak{M}(n, p^{\mu})$ 與 $\mathfrak{M}(n, p)$ 之爲同態可知. 然 $\mathfrak{M}(n, p^{\mu})$ 之元數，由第122節之關係，爲

$$g(n, p^{\mu}) = p^{n^2\mu}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\cdots\left(1-\frac{1}{p^n}\right),$$

而 $\mathfrak{M}(n, p)$ 之元數爲

$$g(n, p) = p^{n^2}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{p^2}\right)\cdots\cdots\left(1-\frac{1}{p^n}\right).$$

故其同態之重複度爲

$$\frac{g(n, p^{\mu})}{g(n, p)} = p^{n^2(\mu-1)}. \tag{4}$$

故 $\mu>1$ 時，若以對應於 $\mathfrak{M}(n, p)$ 之主元素者之 $\mathfrak{M}(n, p^{\mu})$ 之約羣爲 $\mathfrak{N}$，則其元數爲素數冪 $p^{n^2(\mu-1)}$. 因之 $\mathfrak{N}$ 爲可解的. 卽其指數列爲僅由素數 p 而成者也(參照第49節).

再就屬於 $\mathfrak{N}$ 之母式之形而觀，若以 (h_{ij}) 爲 $\mathfrak{N}$ 之一母式，則

$$(h_{ij}) \equiv (e_{ij}) \pmod{p}. \tag{5}$$

$$\therefore\ h_{ij} = e_{ij} + \lambda_{ij} p \quad (\lambda_{ij} \text{ 爲整數}).$$

因之

$$(h_{ij}) \equiv (e_{ij} + \lambda_{ij} p) \pmod{p^{\mu}} \tag{6}$$

爲必要也. 反之則此時 (h_{ij}) 屬於 $\mathfrak{N}$. 蓋因不論 λ_{ij} 之值如何，常爲

$$|e_{ij}+\lambda_{ij}p| \equiv |e_{ij}| \equiv 1 \not\equiv 0 \pmod{p},$$

因之母式 $(e_{ij}+\lambda_{ij}p)$ 屬於 $\mathfrak{M}(n, p^{\mu})$, 而 (5) 之成立甚明故耳. 又 $(e_{ij}+\lambda_{ij}p)$ 之各項得就 p^{μ} 而取之. 故若令

$$\lambda_{ij}=0, 1, 2, \cdots\cdots, p^{\mu-1}-1 \quad (i, j=1, 2, \cdots\cdots, n),$$

則在屬於 $\mathfrak{N}$ 之母式中其互爲非合同者(法 p^{μ})之全部可由是而得也. 因之 $\mathfrak{N}$ 之元數爲 $p^{n^2(\mu-1)}$, 明已.

2°. 如上所述, $\mu>1$ 時, $\mathfrak{N}$ 之指數列, 僅由 p 而成者也. 故 $\mathfrak{M}(n, p^{\mu})$ 之指數列, 若就商 $\mathfrak{M}(n, p^{\mu})/\mathfrak{N}$ 或與之同型之 $\mathfrak{M}(n, p)$ 者得知時, 則爲自明焉.

(i) $n=2$, $p=2$ 時.

$\mathfrak{M}(2, 2)$ 者其元數爲

$$g(2, 2)=2^4\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2^2}\right)=6,$$

而含三元正常約羣

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix} \pmod{2}$$

者也. 故 $\mathfrak{M}(2, 2)$ 之指數列爲

$$2, \quad 3,$$

因之 $\mu>1$ 時, $\mathfrak{M}(2, 2^{\mu})$ 之指數列爲

(7) $$2, 3, 2, 2, \cdots\cdots, 2.$$

此時羣爲可解的也.

(ii) $n>2$, $p=2$ 時.

此時$\mathfrak{M}(n, 2)$如後所證明爲單純的(第128節系). 故$\mathfrak{M}(n, 2^\mu)$之指數列爲

(8)　$(2^n-1)(2^n-2)\cdots\cdots(2^n-2^{n-1}), 2, 2, \cdots\cdots, 2.$

3.°　$p>2$時.

在屬於$\mathfrak{M}(n, p)$之母式中,其行列式與1合同(法p)者之集合,以$\mathfrak{U}(n, p)$或單以$\mathfrak{U}$表之. 於是$\mathfrak{U}$爲$\mathfrak{M}(n, p)$之正常約羣(第118節系3).

今取$\mathfrak{U}$之母式(a_{ij})及$\mathfrak{M}$之母式(k_{ij}),因其積$(a_{ij})(k_{ij})$之行列式爲

$$|a_{ij}|\cdot|k_{ij}|\equiv|k_{ij}| \pmod{p},$$

故屬於傍系$\mathfrak{U}(k_{ij})$之母式之行列式均與$|k_{ij}|$合同(法p)也. 反之,若(k'_{ij})之行列式與$|k_{ij}|$合同(法p),則$(k'_{ij})(k_{ij})^{-1}$之行列式爲

$$|k'_{ij}|\cdot|\overline{k}_{ij}|\equiv|k_{ij}|\cdot|\overline{k}_{ij}|\equiv 1 \pmod{p}.$$

故$(k'_{ij})(k_{ij})^{-1}$屬於$\mathfrak{U}$,因之(k'_{ij})屬於傍系$\mathfrak{U}(k_{ij})$. 今以ρ爲p之原根而令

$$(9)\qquad \mathrm{R}\equiv\begin{pmatrix} \rho & 0 & 0 & \cdots\cdots & 0 \\ 0 & 1 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 1 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & 1 \end{pmatrix} \pmod{p},$$

則此行列式爲

$$|\mathrm{R}| \equiv \rho \pmod{p}.$$

因之

$$|\mathrm{R}^{\alpha}| \equiv \rho^{\alpha} \pmod{p},$$

而 R^{α} ($\alpha=1, 2, \cdots\cdots, p-2$) 屬於 $\mathfrak{M}(n, p)$. 若以此等之母式, 作屬於 $\mathfrak{U}(n, p)$ 之傍系:

$$\mathfrak{U}, \mathfrak{U}\mathrm{R}, \mathfrak{U}\mathrm{R}^2, \cdots\cdots, \mathfrak{U}\mathrm{R}^{p-2}, \tag{10}$$

則屬於此各個之母式之行列式, 分別與

$$1, \rho, \rho^2, \cdots\cdots, \rho^{p-2} \tag{11}$$

合同(法 p). 然此諸數互爲非合同(法 p); 而對於 p 互素之數, 則與此中之或一個合同(法 p). 故(10)之傍系互異; 而由上述則 $\mathfrak{M}(n, p)$ 之母式, 不得不屬於(10)中之某一個也. 因之得

$$\mathfrak{M}(n, p)=\mathfrak{U}+\mathfrak{U}\mathrm{R}+\mathfrak{U}\mathrm{R}^2+\cdots\cdots+\mathfrak{U}\mathrm{R}^{p-2}. \tag{12}$$

由此式, 則 $\mathfrak{U}(n, p)$ 之元數之爲

$$\frac{g(n, p)}{p-1} \tag{13}$$

可知. 更用(12)以作商 $\mathfrak{M}/\mathfrak{U}$, 則爲

$$1, \mathrm{R}, \mathrm{R}^2, \cdots\cdots, \mathrm{R}^{p-2} \pmod{\mathfrak{U}}, \tag{14}$$

卽 $p-1$ 元巡回羣也. 因之將 $p-1$ 分解爲素因數, 而以之爲

$$p-1=p_1 p_2 \cdots\cdots p_r,$$

則上之商羣之指數列爲

$$p_1, p_2, \cdots\cdots, p_r \tag{15}$$

焉.* 於是,問題遂歸於求 $\mathfrak{U}(n,p)$ 之指數列者已.

4.° 由第118節系3,因 $\mathfrak{U}(n,p)$ 由 $n(n-1)$ 個母式 G_{rs} 所生成,故 $\mathfrak{U}(n,p)$ 之自己共軛元素,由第117節系之證明,得有 (γe_{ij}) 之形甚明,因其行列式與1合同(法 p),故

$$\gamma^n \equiv 1 \pmod{p} \tag{16}$$

爲必要. 反之,若 γ 滿足此合同式時,則母式 (γe_{ij}) 於 $\mathfrak{U}$ 爲自己共軛. 然 n 與 $p-1$ 之最大公約數若爲 d,則合同式(16)之根得以

$$1,\ \rho^{\frac{p-1}{d}},\ \rho^{\frac{2(p-1)}{d}},\ \cdots\cdots,\ \rho^{\frac{(d-1)(p-1)}{d}} \pmod{p}. \tag{17}$$

與之.† 但 ρ 爲 p 之原根. 於是若令

$$C \equiv (\rho^{\frac{p-1}{d}} e_{ij}) \pmod{p},$$

則 $\mathfrak{U}(n,p)$ 之自己共軛元素,得以

$$1,\ C,\ C^2,\ \cdots\cdots,\ C^{d-1} \pmod{p} \tag{18}$$

與之也. 而其所作之約羣(卽中核)以 $\mathfrak{C}$ 表之. 因 $\mathfrak{C}$ 爲 d 元巡回羣,故 d 若分解爲素因數而爲

---

*$n=pp'\cdots\cdots$ ($p,p',\cdots\cdots$ 爲素數)時,則 n 元巡回羣 $\{A\}$ 之組成列,得以 $\{A\}$, $\{A^p\}$, $\{A^{pp'}\}$, $\cdots\cdots$ 與之甚明.

†以 ρ^x 爲(16)之根,則 $\rho^{nx}\equiv 1 \pmod{p}$,因之 $nx\equiv 0 \pmod{p-1}$. 然 n 與 $p-1$ 之最大公約數爲 d. 故 $x \equiv 0 \left(\mathrm{mod.}\ \frac{p-1}{d}\right)$ 爲必要也. 反之,此時 ρ^x 之能滿足(16)則甚明焉.

$$d=q_1\,q_2\cdots\cdots q_s,$$

則$\mathfrak{C}$之指數列爲

$$(19)\qquad q_1,\ q_2,\ \cdots\cdots,\ q_s.$$

然如次章之所證明, $p>2$時, 除$[n=2,\ p=3]$者外, $\mathfrak{C}$於$\mathfrak{U}$爲極大正常也. 故$\mathfrak{U}(n,p)$之指數列爲

$$(20)\qquad \frac{g(n,p)}{(p-1)d},\ q_1,\ q_2,\ \cdots\cdots,\ q_s;$$

因之由 (15), $\mathfrak{M}(n,p)$之指數列爲

$$(21)\qquad p_1,\ p_2,\ \cdots\cdots,\ p_r,\ \frac{g(n,p)}{(p-1)d},\ q_1,\ q_2,\ \cdots\cdots,\ q_s;$$

而$\mathfrak{M}(n,p^\mu)$之指數列, 由1°, 爲

$$(22)\qquad p_1,\ \cdots\cdots,\ p_r,\ \frac{g(n,p)}{(p-1)d},\ q_1,\ \cdots\cdots,\ q_s,\ p,\ \cdots\cdots,\ p.$$

5°. 最後就$n=2, p=3$時者一論.

3之原根爲-1(法3), 故若令

$$\mathrm{R}\equiv\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}\pmod 3,$$

則由(12)得

$$(23)\qquad \mathfrak{M}(2,3)=\mathfrak{U}(2,3)+\mathfrak{U}(2,3)\cdot\mathrm{R}.$$

今取$\mathfrak{U}$之母式

$$\left.\begin{aligned}&\mathrm{C}\equiv\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix},\quad \mathrm{S}\equiv\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\\ &\mathrm{T}\equiv\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix},\quad \mathrm{U}\equiv\begin{pmatrix}0 & 1\\ -1 & 1\end{pmatrix}\end{aligned}\right\}\pmod 3,$$

則得

$$\left.\begin{array}{l} S^2\equiv C,\ S^4\equiv C^2\equiv 1, \\ T^2\equiv C,\ T^4\equiv 1,\ T^{-1}ST\equiv S^3, \\ U^3\equiv C,\ U^6\equiv 1,\ U^{-1}SU\equiv ST,\ U^{-1}TU\equiv S \end{array}\right\} \text{(mod. 3)}.$$

故

$$\text{(24)}\qquad \{C\},\ \{S\},\ \{S, T\},\ \{S, T, U\},$$

分別作元數爲

$$2,\ 4,\ 8,\ 24$$

之羣,而各個皆爲其次一個之正常約羣焉. 且

$$\{S,\ T,\ U\}=\mathfrak{U}(2, 3),$$

蓋因$\mathfrak{U}(2, 3)$之元數爲$\frac{g(2, 3)}{3-1}=24$故. 故$\mathfrak{U}(2, 3)$之指數列,由(24)爲

$$3\left(=\frac{24}{8}\right),\ 2\left(=\frac{8}{4}\right),\ 2\left(=\frac{4}{2}\right),\ 2.$$

因之$\mathfrak{M}(2, 3)$之指數列爲

$$\text{(25)}\qquad 2,\ 3,\ 2,\ 2,\ 2.$$

第二十章. 一次變換合同羣

125. 一次變換.

將n個文字(或變數)

$$\text{(1)}\qquad x_1, x_2, \cdots\cdots, x_n$$

以由一次關係

$$(2)\qquad \begin{cases} x_1' = a_{11}x_1 + a_{12}x_2 + \cdots\cdots + a_{1n}x_n \\ x_2' = a_{21}x_1 + a_{22}x_2 + \cdots\cdots + a_{2n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ x_n' = a_{n1}x_1 + a_{n2}x_2 + \cdots\cdots + a_{nn}x_n \end{cases}$$

所定之 n 個文字

$$(3)\qquad x_1',\ x_2',\ \cdots\cdots,\ x_n'$$

而置換之之演算,名曰文字(1)上所行之**一次變換**. 此中之係數 a_{ij} $(i, j=1, 2, \cdots\cdots, n)$, 對文字(1)而爲獨立之數者,是無俟論. 此變換由係數之母式

$$(4)\qquad \begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{pmatrix}$$

完全得定. 爰名之曰變換(2)之母式,而其行列式

$$(5)\qquad \begin{vmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{vmatrix}$$

名曰變換(2)之行列式. 至對兩變換言,若其母式相等時,則兩者曰相等. 於是,變換與母式之間,一一對應既得成

立,則如變換(2)名以A時,則其母式(4),遂亦以同一記號表之也.

變換(2),略記之爲

$$x_i' = \sum_{j=1}^{n} a_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n) \tag{2'}$$

對此右邊之變數 x_j $(j=1, 2, \cdots\cdots, n)$ 施以變換

$$x_i' = \sum_{j=1}^{n} b_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n), \tag{6}$$

則變換(2')遂成爲

$$x_i' = \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{n} b_{jk}\, x_k \right) = \sum_{k} \left(\sum_{j} a_{ij}\, b_{jk} \right) x_k.$$

將此換書之,得

$$x_i' = \sum_{j=1}^{n} c_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n), \tag{7}$$

但

$$c_{ij} = \sum_{l=1}^{n} a_{il}\, b_{lj} \qquad (i, j=1, 2, \cdots\cdots, n). \tag{8}$$

由變換(2')及(6)以導出變換(7),名曰右乘(6)於(2),而(7)曰其積焉. 由(8),則積之母式 (c_{ij}) 等於兩變換之母式之積 (a_{ij}) (b_{ij}) 甚明. 換言之,卽變換之乘法得由其母式之乘法而定者也. 因之三變換之乘法間,其組合法則之成立是爲當然.

與主母式相應之變換

$$x_i' = x_i \quad (i=1, 2, \cdots\cdots, n)$$

名曰**主變換**,以1表之. 若兩變換

$$\mathrm{A}: \quad x_i' = \sum_j a_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n),$$

$$\overline{\mathrm{A}}: \quad x_i' = \sum_j \overline{a}_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n)$$

之積等於主變換, 卽

$$\mathrm{A}\,\overline{\mathrm{A}} = 1$$

時, 則 $\overline{\mathrm{A}}$ 名曰 A 之**逆變換**而以 A^{-1} 表之. 因對變換之積, 則母式之積相與對應, 故此時母式 $\overline{\mathrm{A}}$ 乃母式 A 之逆. 因之若變換須有其逆, 則其行列式之不爲零在所必要, 而此際 A 遂有唯一之逆焉(參照第 109 節).

126. 變換之變形.

茲取兩變換

$$\mathrm{A}: \quad x_i' = \sum_{j=1}^{n} a_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n),$$

$$\mathrm{B}: \quad y_i = \sum_{j=1}^{n} b_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n);$$

而令

$$(1) \qquad y_i' = \sum_{j=1}^{n} b_{ij}\, x_j' \qquad (i=1, 2, \cdots\cdots, n).$$

以 B 爲有逆者, 由此三組之式以消去 x_j, x_j' $(j=1, 2, \cdots\cdots, n)$.

先以 B 之逆爲

$$\mathrm{B}^{-1}: \quad y_i = \sum_j \overline{b}_{ij}\, x_j \qquad (i=1, 2, \cdots\cdots, n),$$

則因

$$\sum_i \overline{b}_{ki}\, b_{ij} = e_{kj}$$

之故, 於 B 之兩邊乘以 $\overline{b}_{ki}$, 而將其就 i 以加之, 則得

(2)　$$\sum_i \overline{b}_{ki}\, y_i = \sum_{i,j} \overline{b}_{ki}\, b_{ij}\, x_j = \sum_j e_{kj}\, x_j = x_k.$$

再於(1)之右邊代入A, 則得

$$y_i' = \sum_j b_{ij} \sum_k a_{jk}\, x_k = \sum_{j,k} b_{ij}\, a_{jk}\, x_k.$$

以(2)代入之, 遂得

(3)　$$y_i' = \sum_{j,k} b_{ij} a_{jk} \sum_l \overline{b}_{kl} y_l = \sum_l \left(\sum_{j,k} b_{ij} a_{jk} \overline{b}_{kl}\right) y_l.$$

是卽所求之結果也. 且就此而觀, 右邊之母式等於BAB^{-1}, 因之(3), 乃以B^{-1}將變換A變形者也. 故以B^{-1}將變換A變形, 不過將A之變數x, 變更爲由B所定義之新變數y而已.

127. 一次變換合同羣.

於係數爲整數之兩變換

$$\mathrm{A}: \quad x_i' = \sum_j a_{ij} x_j \quad (i = 1, 2, \cdots\cdots, n),$$

$$\mathrm{A}': \quad x_i' = \sum_j a'_{ij} x_j \quad (i = 1, 2, \cdots\cdots, n)$$

中, 其母式就法l(一整數)爲合同, 卽

$$(a_{ij}) \equiv (a'_{ij}) \pmod{l}$$

時, 則此兩變換曰對法l爲合同, 而以

$$\mathrm{A} \equiv \mathrm{A}' \pmod{l}$$

表之. 整數l爲已知時, 在n個變數之一次變換(整數係數)中, 其行列式對l爲互素者相集成羣也(就其關於法l之乘法者); 而此羣與關於l之n次母式合同羣爲單純同態. 蓋因變換與母式之間, 一一對應成立, 而積與積對應; 且n次

母式中,其行列式對 l 互素者,又成 n 次母式合同羣(法 l)故也. (第 118 節系 2). 於此所得之羣,呼曰關於法 l 之**一次變換合同羣**,便宜上乃以 $\mathfrak{L}(n,l)$ 表之焉.

因一次變換合同羣 $\mathfrak{L}(n,l)$ 與 $\mathfrak{M}(n,l)$ 爲單純同態,故由第120節第二定理系,若

$$l=p^{\mu}q^{\nu}\cdots\cdots \quad (p,q \text{ 爲互異之素數})$$

時,則關於法 l 之一次變換合同羣,乃與以

$$p^{\mu},\ q^{\nu},\ \cdots\cdots$$

分別爲法之一次變換合同羣之同型羣之直乘積相等也. 此卽 Jordan 氏之定理.

又就合同羣言,其變換之變形,亦不外變數之變更,是與前節同樣.

128. $\mathfrak{U}/\mathfrak{C}$ **之單純性**

在一次變換合同羣 $\mathfrak{L}(n,p)$ 中,其行列式與 1 合同(法 p)者之變換,由第 118 節系 3,相集乃作 $\mathfrak{L}$ 之正常約羣也. 此約羣,用第124節 3° 中同一之記號,以 $\mathfrak{U}(n,p)$ 或單以 $\mathfrak{U}$ 表之. 此 $\mathfrak{U}$ 也,如該系之所示,乃由 $n(n-1)$ 個之母元素.

$$G_{rs}:\ \begin{cases} x_r'\equiv x_r+x_s & (r\neq s) \\ x_i'\equiv x_i & (i=1,2,\cdots\cdots,n;\ i\neq r) \end{cases}$$

所生成. 但上之合同式均係就法 p 而取之者. 而 $\mathfrak{U}$ 之自己共軛元素,由第124節 4° 所示,得以

$$x_i'\equiv\gamma x_i \pmod{p} \quad (i=1,2,\cdots\cdots,n)$$

$$\gamma^n\equiv 1 \pmod{p}$$

與之，而其數乃與 n 及 $p-1$ 之最大公約數等.* 此等之集合卽 $\mathfrak{U}$ 之中核以 $\mathfrak{C}$ 表之. 除 $n=2, p=2$ 及 $n=2, p=3$ 兩者外，乃有

定理. $\mathfrak{U}(n, p)$ 中，其中核爲極大正常.

證明. 設 $\mathfrak{N}$ 爲 $\mathfrak{U}$ 之正常約羣. 以 $\mathfrak{U}$ 之變換 S 將 $\mathfrak{N}$ 之變換 A 變形而作 $S^{-1}AS$ 及 $S^{-1}AS\cdot A^{-1}$，則此各個皆屬於 $\mathfrak{N}$. 證明之方針，在示：$\mathfrak{N}$ 若含 $\mathfrak{U}$ 之自己共軛元素以外之變換時，乃適當的選擇 S，而將上演算反覆行之，遂得母元素之一；由是，他之母元素皆含於 $\mathfrak{N}$，因而 $\mathfrak{N}$ 與 $\mathfrak{U}$ 一致也. 此方法與交代羣之單純性之證明，全無二致(參照第66節).

1.° 令 $A\equiv(\alpha_{ij})$, $A^{-1}\equiv(\bar{\alpha}_{ij})$，以 A^{-1} 將第115節之母式 $G_{rs\lambda}$ 變形，而令

$$AG_{rs\lambda}\,A^{-1}\equiv R,\quad R\equiv(\rho_{ij}),$$

則

$$(1)\quad \rho_{ij}\equiv\sum_{k,l}\alpha_{ik}g_{kl\lambda}\bar{\alpha}_{lj}\equiv\sum_{k}\alpha_{ik}g_{kk\lambda}\bar{\alpha}_{kj}+\alpha_{ir}g_{rs\lambda}\bar{\alpha}_{sj}\equiv e_{ij}+\lambda\alpha_{ir}\bar{\alpha}_{sj}.$$

又令

$$G_{rs\lambda}^{-1}\,AG_{rs\lambda}\,A^{-1}\equiv G_{rs\lambda}^{-1}R\equiv B,\quad B\equiv(\beta_{ij}),$$

則

$$(2)\quad \begin{cases}\beta_{rj}\equiv\rho_{rj}-\lambda\,\rho_{sj}\equiv e_{rj}+\lambda\alpha_{rr}\bar{\alpha}_{sj}-\lambda\,(e_{sj}+\lambda\alpha_{sr}\bar{\alpha}_{sj})\\ \beta_{ij}\equiv\rho_{ij}\equiv e_{ij}+\lambda\alpha_{ir}\bar{\alpha}_{sj}\quad (i\neq r).\end{cases}$$

---

*本節中亦以法 p 爲素數者.

上之合同式, 皆係就法 p 而取之者. 以下亦同樣.

2 先就 $n>2$ 時將定理證明之.

設正常約羣 $\mathfrak{H}$ 爲含有非 $\mathfrak{U}$ 之自己共軛元素之變換

$$\mathrm{A}: \quad x'_i \equiv \sum_j a_{ij} x_j \quad (i=1, 2, \cdots\cdots, n),$$

而 A 與 G_{12} 不爲交換可能者.* 於是令

$$G_{12}^{-1} A G_{12} A^{-1} \equiv B, \quad B \equiv (\beta_{ij}),$$

則 B 與主變換不相合同, 而由 (2) 得

$$\mathrm{B}: \begin{cases} x'_1 \equiv \sum_j \beta_{1j} x_j \\ x'_i \equiv x_i + \sum_j a_{i1} \bar{a}_{2j} x_j \equiv x_i + a_{i1} \varphi \end{cases}$$

$$(i=2, 3, \cdots\cdots, n).$$

$a_{21}, \cdots\cdots, a_{n1}$ 之全部皆爲零 (法 p) 時, 則 B 卽名曰 C, 而其母式以 (γ_{ij}) 記之. 否則以 $a_{21} \not\equiv 0$, 而取†

$$\mathrm{S}: \quad y_1 \equiv x_1, \ y_2 \equiv x_2, \ y_i \equiv x_i - \frac{a_{i1}}{a_{21}} x_2 \qquad (i=3, 4, \cdots\cdots, n);$$

乃以 SBS^{-1} 名曰 C, 而其母式以 (γ_{ij}) 記之. 於是由第 126 節所述之計算法, 得

---

*因 A 非自己共軛, 故母元素 G_{rs} 之中, 其與之不爲交換可能者定存在也. 以其一爲 G_{12}.

†其適合 $ax \equiv b \pmod{p}$ 之 x 以 $\frac{b}{a}$ 表之.

$$\mathrm{C}:\begin{cases} y'_1\equiv x'_1\equiv\sum\limits_j \beta_{1j}x_j\equiv\sum\limits_j \gamma_{1j}y_j \\ y'_2\equiv\sum\limits_j \gamma_{2j}y_j \\ y'_i\equiv x'_i-\dfrac{a_{i1}}{a_{21}}x'_2\equiv(x_i+a_{i1}\varphi)-\dfrac{a_{i1}}{a_{21}}(x_2+a_{21}\varphi) \\ \quad\equiv x_i-\dfrac{a_{i1}}{a_{21}}x_2\equiv y_i \qquad (i=3,\ 4,\ \cdots\cdots,\ n). \end{cases}$$

總之無論如何，對於 $i\geqq 3$ 者，皆爲

$$\gamma_{ii}\equiv 1,\quad \gamma_{ij}\equiv 0\quad (i\neq j)$$

也．因之若以 $(\overline{\gamma}_{ij})$ 爲 (γ_{ij}) 之逆母式則得

$$\overline{\gamma}_{ii}\equiv 1\quad (i\geqq 3),\quad \overline{\gamma}_{3j}\equiv 0\quad (j\neq 3).$$

次令

$$\mathrm{G}_{13}^{-1}\,\mathrm{C}\mathrm{G}_{13}\,\mathrm{C}^{-1}\equiv \mathrm{D}_1,\quad \mathrm{D}_1\equiv(\delta_{ij}),$$

則由 (2),

$$\delta_{1j}\equiv e_{1j}+\gamma_{11}\overline{\gamma}_{3j}-(e_{3j}+\gamma_{31}\overline{\gamma}_{3j}),$$
$$\delta_{ij}\equiv e_{ij}+\gamma_{i1}\overline{\gamma}_{3j}\qquad (i=2,\ 3,\ \cdots\cdots,\ n).$$

因之

$$\mathrm{D}_1:\begin{cases} y'_1\equiv y_1+(\gamma_{11}-1)y_3 \\ y'_2\equiv y_2+\gamma_{21}y_3 \\ y'_i\equiv y_i \qquad (i=3,\ 4,\ \cdots\cdots,\ n). \end{cases}$$

又以

$$\mathrm{G}_{23}^{-1}\,\mathrm{C}\mathrm{G}_{23}\,\mathrm{C}^{-1}\equiv \mathrm{D}_2,$$

則

$$\mathrm{D}_2:\begin{cases} y'_1\equiv\sum\limits_j (e_{1j}+\gamma_{12}\overline{\gamma}_{3j})\,y_i\equiv y_1+\gamma_{12}y_3 \\ y'_2\equiv\sum\limits_j \{e_{2j}+\gamma_{22}\overline{\gamma}_{3j}-(e_{3j}+\gamma_{32}\overline{\gamma}_{3j})\}\,y_j\equiv y_2+(\gamma_{22}-1)y_3 \\ y'_i\equiv y_i \qquad (i=3,\ 4,\ \cdots\cdots,\ n) \end{cases}$$

上二變換 D_1, D_2 共有

$$D:\begin{cases} y'_1\equiv y_1+\delta_1 y_3 \\ y'_2\equiv y_2+\delta_2 y_3 \\ y'_i\equiv y_i \qquad\qquad (i=3,\ 4,\ \cdots\cdots,\ n) \end{cases}$$

之形焉.

特別, $D_1\equiv D_2\equiv 1$ 時, 則須

$$\gamma_{11}\equiv 1,\quad \gamma_{21}\equiv 0,\quad \gamma_{12}\equiv 0,\quad \gamma_{22}\equiv 1,$$

因之 C 乃有次形:

$$C_1:\begin{cases} y'_1\equiv y_1+\gamma_{13}\, y_3+\cdots\cdots+\gamma_{1n}\, y_n \\ y'_2\equiv y_2+\gamma_{23}\, y_3+\cdots\cdots+\gamma_{2n}\, y_n \\ y'_i\equiv y_i \qquad\qquad (i=3,\ 4,\ \cdots\cdots,\ n). \end{cases}$$

此中若

$$\gamma_{1j}\equiv\gamma_{2j}\equiv 0 \quad (j\geqq 4)$$

則 C_1 與 D 同形.* 否則以 γ_{14}, γ_{24} 之一不爲零(法 p), 而用(2)計算 $G_{43}^{-1}\, C_1\, G_{43}\, C_{1,}^{-1}$ 則得

$$\begin{cases} y'_1\equiv\sum\limits_j (e_{1j}+\gamma_{14}\,\overline{\gamma}_{3j})\, y_j\equiv y_1+\gamma_{14}\, y_3 \\ y'_2\equiv\sum\limits_j (e_{2j}+\gamma_{24}\,\overline{\gamma}_{3j})\, y_j\equiv y_2+\gamma_{24}\, y_3 \\ y'_4\equiv\sum\limits_j \{e_{4j}+\gamma_{44}\,\overline{\gamma}_{3j}-(e_{3j}+\gamma_{34}\,\overline{\gamma}_{3j})\}\, y_j\equiv y_4 \\ y'_i\equiv\sum\limits_j (e_{ij}+\gamma_{i4}\,\overline{\gamma}_{3j})\, y_j\equiv y_i \qquad (i=3,\ 5,\ 6,\ \cdots\cdots,\ n), \end{cases}$$

---

*若 $n=3$, 則 C_1 當然與 D 同形.

此與主變換不相合同而與D同形. 故自己共軛約羣$\mathfrak{N}$不得不含具有D形之變換(非不動的)也.

因D非爲不動的, 故δ_1, δ_2中有一個不爲零(法p). 以之爲$\delta_1 \neq 0$. 試以變換

$$\mathrm{T}: \quad z_1 \equiv y_1,\ z_2 \equiv y_2 - \frac{\delta_2}{\delta_1} y_1,\ z_i \equiv y_i \quad (i = 3, 4, \cdots\cdots, n)$$

將D變形, 則由第126節之計算法, 得

$$\mathrm{TDT}^{-1}: \begin{cases} z'_1 \equiv y'_1 \equiv y_1 + \delta_1 y_3 \equiv z_1 + \delta_1 z_3, \\ z'_2 \equiv y'_2 - \dfrac{\delta_2}{\delta_1} y'_1 \equiv y_2 + \delta_2 y_3 - \dfrac{\delta_2}{\delta_1}(y_1 + \delta_1 y_3), \\ \quad \equiv y_2 - \dfrac{\delta_2}{\delta_1} y_1 \equiv z_2, \\ z'_i \equiv y'_i \equiv y_i \equiv z_i \qquad (i = 3, 4, \cdots\cdots, n). \end{cases}$$

故

$$\mathrm{TDT}^{-1} \equiv \mathrm{G}_{13\,\delta_1}.$$

此中因$\delta_1 \neq 0$, 故若取如$x\delta_1 \equiv 1 \pmod{p}$者之$x$, 則由第115節(6), 得

$$(\mathrm{G}_{13\,\delta_1})^x \equiv \mathrm{G}_{1,\,3,\,x\,\delta_1} \equiv \mathrm{G}_{131} \equiv \mathrm{G}_{13}.$$

夫如是, 則$\mathfrak{N}$含有母元素

$$\mathrm{G}_{13}: \quad z'_1 \equiv z_1 + z_3,\ z'_i \equiv z_i \quad (i = 2, 3, \cdots\cdots, n)$$

也. 將此, 用變換

$$w_1 \equiv z_r,\ w_r \equiv z_1,\ w_i \equiv z_i \quad (i \neq 1, r)$$

而變其形, 則得

$$\begin{cases} w'_1 \equiv z'_r \equiv z_r \equiv w_1 \\ w'_r \equiv z'_1 \equiv z_1 + z_3 \equiv w_r + w_3 \\ w'_i \equiv z'_i \equiv z_i \equiv w_i \qquad (i \neq 1, r), \end{cases}$$

卽 G_{r3}. 更將此用變換

$$v_3\equiv w_s,\ v_s\equiv w_3,\ v_i\equiv w_i\quad (i\neq 3,\ s)$$

而變其形, 則得

$$\begin{cases} v'_r\equiv w'_r\equiv w_r+w_3\equiv v_r+v_s \\ v'_3\equiv w'_s\equiv w_s\equiv v_3 \\ v'_s\equiv w'_3\equiv w_3\equiv v_s \\ v'_i\equiv w'_i\equiv w_i\equiv v_i \qquad (i\neq 3,\ r,\ s), \end{cases}$$

卽 G_{rs}. 如是, 若 $\mathfrak{N}$ 含有不屬於 $\mathfrak{U}$ 之中核之變換時, 則 $\mathfrak{N}$ 不得不含任意之母元素 ($\mathfrak{U}$ 的) G_{rs} 也, 因之 $\mathfrak{N}$ 與 $\mathfrak{U}$ 一致.

3°. $n=2,\ p>3$ 時.

今以 $\mathfrak{U}$ 之正常約羣 $\mathfrak{N}$ 爲除含主變換及相似變換*

$$\mathrm{J}:\quad x'_1\equiv -x_1,\ x'_2\equiv -x_2$$

外, 再含有變換

$$\mathrm{A}:\begin{cases} x'_1\equiv a_{11}\,x_1+a_{12}\,x_2 \\ x'_2\equiv a_{21}\,x_1+a_{22}\,x_2 \end{cases}$$

者. 但

$$(3)\qquad a_{11}\,a_{22}-a_{12}\,a_{21}\equiv 1\pmod{p}.$$

(i) $a_{12}\equiv 0,\ a_{22}\equiv \pm 1$ 時.

此時由 (3), $a_{11}\equiv\pm 1$ 爲必要, 而 A 則爲

$$(4)\qquad x'_1\equiv x_1,\quad x'_2\equiv a_{21}\,x_1+x_2,$$

---

*與倍乘母式 $(\lambda_i\, e_{ij})$ 相應之變換曰倍乘變換; 其與相似母式相應者曰相似變換.

或

(5)　　$x'_1 \equiv -x_1, \quad x'_2 \equiv a_{21}\, x_1 - x_2.$

此中不能有 $a_{21} \equiv 0$. (蓋因 $A \neq 1$, $A \neq J$ 故.) 由第115節, (4) 爲 G_{21} 之 a_{21} 乘冪. 故若取適合於 $a_{21}\lambda \equiv 1 \pmod{p}$ 者之 λ, 則由同節(6), 乃得 $A^{\lambda} \equiv G_{21}$. 又在(5)時, 積 AJ 與 G_{21} 之 $-a_{21}$ 乘冪相合同, 此當然屬於 $\mathfrak{N}$. 而 $(AJ)^{-\lambda} \equiv G_{21}$. 是無論如何, $\mathfrak{N}$ 含母元素 G_{21} 也.

(ii)　$a_{12} \equiv 0$, $a_{22} \neq \pm 1$ 時.

因　A:　$x'_1 \equiv a_{11}\, x_1, \quad x'_2 \equiv a_{21}\, x_1 + a_{22}\, x_2 \qquad (a_{11}\, a_{22} \equiv 1),$

故　A^{-1}:　$x'_1 \equiv a_{22}\, x_1, \quad x'_2 \equiv -a_{21}\, x_1 + a_{11}\, x_2.$

今令　　$G_{21}^{-1}\, A G_{21}\, A^{-1} \equiv B, \quad B \equiv (\beta_{ij}),$

則由(2)得

$$\beta_{11} \equiv e_{11} + a_{12}\, \bar{a}_{11} \equiv 1,$$

$$\beta_{12} \equiv e_{12} + a_{12}\, \bar{a}_{12} \equiv 0,$$

$$\beta_{21} \equiv e_{21} + a_{22}\, \bar{a}_{11} - (e_{11} + a_{12}\, \bar{a}_{11}) \equiv a_{22}^2 - 1,$$

$$\beta_{22} \equiv e_{22} + a_{22}\, \bar{a}_{12} - (e_{12} + a_{12}\, \bar{a}_{12}) \equiv 1.$$

即 B 爲 G_{21} 之 $a_{22}^2 - 1$ 乘冪也. 然 $a_{22}^2 \neq 1$. 故與前同樣, $\mathfrak{N}$ 非含 G_{21} 不可.

(iii)　$a_{12} \neq 0$ 時.

試取

$$T: \quad x_1' \equiv \kappa\, a_{11}\, x_1 + \kappa\, a_{12}\, x_2, \quad x'_2 \equiv -\frac{1 + \kappa^2\, a^2_{11}}{\kappa\, a_{12}} x_1 - \kappa\, a_{11}\, x_2.$$

因此行列式與1合同,故T屬於羣$\mathfrak{U}(2,p)$. 而其逆則爲

$$T^{-1}:\quad x'_1\equiv-\kappa a_{11}x_1-\kappa a_{12}x_2,\quad x'_2\equiv\frac{1+\kappa^2a^2_{11}}{\kappa a_{12}}x_1+\kappa a_{11}x_2.$$

用此以計算$ATAT^{-1}$,則得

$$ATAT^{-1}:\begin{cases}x'_1\equiv-\dfrac{1}{\kappa^2}x_1\\[2ex] x'_2\equiv-\dfrac{(1+\kappa^2)(a_{22}+\kappa^2a_{11})}{\kappa^2a_{12}}x_1-\kappa^2x_2.\end{cases}$$

此則當然屬於$\mathfrak{N}$也.

若$p>5$,乃取p之原根以爲κ. 於是因

$$\kappa^4\not\equiv1,\text{ 即 }\kappa^2\not\equiv\pm1,$$

故變換$ATAT^{-1}$與(ii)中之A爲同形者也. 因之由(ii)則$\mathfrak{N}$不得不含G_{21}焉.

$p=5$時,令$\kappa\equiv1$,則得

$$ATAT^{-1}J:\quad x'_1\equiv x_1,\ x'_2\equiv\frac{2(a_{22}+a_{11})}{a_{12}}x_1+x_2.$$

此中若$a_{22}+a_{11}\not\equiv0\pmod5$,則此置換爲$G_{21}$之羃,因之$\mathfrak{N}$遂含$G_{21}$. 反之,在$a_{22}+a_{11}\equiv0$時,則令

$$G_{21}^{-1}AG_{21}A^{-1}\equiv C,\ C\equiv(\gamma_{ij}),$$

乃代A取C而作$CTCT^{-1}J$. 於是因A之逆爲

$$A^{-1}:\quad x'_1\equiv a_{22}x_1-a_{12}x_2,\ x'_2\equiv-a_{21}x_1+a_{11}x_2$$

之故,如(ii)之計算然,得

$$\gamma_{11}\equiv e_{11}+a_{12}\bar{a}_{11}\equiv1+a_{12}a_{22},$$

$$\gamma_{22}\equiv e_{22}+\alpha_{22}\bar{\alpha}_{12}-(e_{12}+\alpha_{12}\bar{\alpha}_{12})\equiv 1-\alpha_{22}\alpha_{12}+\alpha^2{}_{12},$$

因之　　$\gamma_{11}+\gamma_{22}\equiv 2+\alpha^2{}_{12}\not\equiv 0 \pmod 5$.*

故 $CTCT^{-1}J$ 與前述同樣爲 G_{21} 之冪。是則 $\mathfrak{N}$ 不得不含 G_{21} 也. 如上所述，雖在任何情形中，$\mathfrak{N}$ 均含 G_{21}. 乃將 G_{21}，用變換

$$y_1\equiv x_2,\quad y_2\equiv -x_1$$

而變其形，則得

$$y'_1\equiv x'_2\equiv x_1+x_2\equiv y_1-y_2,\quad y'_2\equiv -x'_1\equiv -x_1\equiv y_2,$$

即 G_{12}^{-1}. 因之 $\mathfrak{N}$ 必含 G_{12} 也. 夫如是，正常約羣 $\mathfrak{N}$，若含 $\mathfrak{U}$ 之中核以及不屬於其中之元素時. 則含 $\mathfrak{U}$ 之母元素 G_{21} 及 G_{12}，因之 $\mathfrak{N}$ 非與 $\mathfrak{U}$ 一致不可也.

系. $n>2$ 時，則 $\mathfrak{L}(n, 2)$ 爲單羣.

蓋因不得以 2 整除之數即奇數，均與 1 合同(法 2)，故 $\mathfrak{U}(n, 2)=\mathfrak{L}(n, 2)$；而 $\mathfrak{L}$ 之自己共軛元素即相似變換(第 117 節系)須與主變換合同故也.

129. 由前節之定理，若 $\mathfrak{C}$ 爲 $\mathfrak{U}(n, p)$ 之中核，則 $\mathfrak{U}/\mathfrak{C}$ 爲單羣. 而此商之元數，由第 124 節 (20) 及第 122 節 (10)，爲

$$\frac{g(n, p)}{(p-1)d}=\frac{(p^n-1)(p^n-p)\cdots\cdots(p^n-p^{n-1})}{(p-1)d}.$$

---

*因將 0, 1, 2, 3, 4 (mod. 5) 各各自乘，遂分別爲 0, 1, 4, 9, 16；而加 2 於此之任一個，均決不能以 5 整除故也.

但 d 爲 n 與 $p-1$ 之最大公約數. 對於 n, p 之小值, 則此元數計算之如次表:

n	p	$\mathfrak{U}/\mathfrak{C}$ 之元數	n	p	$\mathfrak{U}/\mathfrak{C}$ 之元數
2	5	60	2	41	34440
2	7	168	2	43	39732
2	11	660	2	47	51888
2	13	1092	3	2	168
2	17	2448	3	3	5616
2	19	3420	3	5	372000
2	23	6072	3	7	1876896
2	29	12180	4	2	20160
2	31	14880	4	3	6065280
2	37	25308	5	2	9999360

第 四 篇

特 殊 羣

第二十一章 Abel 氏羣

130. 母元素, 基底.

於十二元 Abel 氏羣(以 $\mathfrak{A}$ 表之)

$$1, \quad (pq)(rs), \quad (pr)(qs), \quad (ps)(qr),$$
$$(xyz), \quad (pq)(rs)(xyz), \quad (pr)(qs)(xyz), \quad (ps)(qr)(xyz),$$
$$(xzy), \quad (pq)(rs)(xzy), \quad (pr)(qs)(xzy), \quad (ps)(qr)(xzy),$$

中取三個置換

$$(1) \qquad (pq)(rs), \quad (pr)(qs), \quad (xyz),$$

而以之作積

$$(2) \qquad [(pq)(rs)]^{\alpha}[(pr)(qs)]^{\beta}(xyz)^{\gamma}.$$

令

$$\alpha=0, 1; \quad \beta=0, 1; \quad \gamma=0, 1, 2,$$

則由之可得 $\mathfrak{A}$ 全部之元素. 故 $\mathfrak{A}$ 者由三元素(1)得以生成者也. 而積(2), 當

$$\alpha\equiv 0 \pmod 2, \quad \beta\equiv 0 \pmod 2, \quad \gamma\equiv 0 \pmod 3$$

時, 雖表示不動置換者; 然不如是, 則非爲不動的焉.

一般於Abel氏羣$\mathfrak{G}$之若干元素A, B, ……, L(其巡回率分別爲$a, b, \cdots\cdots, l$)間,若只限於

$$\alpha\equiv 0 \pmod{a},\ \beta\equiv 0 \pmod{b},\ \cdots\cdots,\ \lambda\equiv 0 \pmod{l}$$

時,始得

$$A^{\alpha}B^{\beta}\cdots\cdots L^{\lambda}=1,$$

則此等元素曰互爲**獨立**. A, B, ……, L互爲獨立時,乃以之作$ab\cdots\cdots l$個之積

$$A^{\alpha}\,B^{\beta}\cdots\cdots L^{\lambda}\begin{cases}\alpha=0, 1, \cdots\cdots, a-1,\\ \beta=0, 1, \cdots\cdots, b-1,\\ \cdots\cdots\cdots\cdots\cdots\cdots\\ \lambda=0,\ 1, \cdots\cdots, l-1,\end{cases}$$

則此諸積互異且成羣,明已. 若此羣與所設之羣$\mathfrak{G}$一致,即$\mathfrak{G}=\{A, B, \cdots\cdots, L\}$時,則A, B, ……, L名曰$\mathfrak{G}$之**獨立母元素**,而此諸母元素之一組,名曰此Abel氏羣之**基底**或單曰**底**. 因此術語,則三元素(1),即$\mathfrak{A}$之獨立母元素也.

定理. 凡Abel氏羣皆有底. 即其元素皆得以獨立母元素之積表之.

證明. 素數冪元時.

設$\mathfrak{P}$爲元數爲素數冪p^m之Abel氏羣. 乃取一巡回率最高者之元素之一,而以之爲P_1,其巡回率以爲p^{m_1}. 於是$\mathfrak{P}$之元素之巡回率,皆爲p^{m_1}之約數. 即對$\mathfrak{P}$之任意元素P,皆爲

(3)　　$P^{p^{m_1}}=1$

也. 蓋因P之巡回率乃p之冪, 故若此巡回率不爲p^{m_1}之約數, 則須較p^{m_1}爲大故耳. 其次P_1之冪

(4)　　$1, P_1, P_1^2, \cdots\cdots, P_1^{p^{m_1}-1},$

乃形成$\mathfrak{P}$之巡回約羣$\{P_1\}$. 若以此諸冪克盡$\mathfrak{P}$之元素時, 則$\mathfrak{P}=\{P_1\}$. 因之P, 乃以唯一個而爲$\mathfrak{P}$之底也. 若不然, 則在不屬於$\{P_1\}$之元素中, 取其關於$\{P_1\}$之相對巡回率* 爲最高者之一. 以之爲S, 其相對巡回率以爲p^{m_2}, 卽

(5)　　$S^{p^{m_2}}=P_1^{\lambda'}$

者. 相對巡回率旣爲巡回率之約數, 故p^{m_2}爲p^{m_1}之約數. 因之

$$m_2 \leqq m_1.$$

將(5)式之兩邊$p^{m_1-m_2}$方乘之, 得

$$S^{p^{m_1}}=P_1^{\lambda' p^{m_1-m_2}}.$$

故由(3)得

$$P_1^{\lambda' p^{m_1-m_2}}=1.$$

$$\therefore\ \lambda' p^{m_1-m_2}\equiv 0 \pmod{p^{m_1}}$$

$$\therefore\ \lambda'\equiv 0 \pmod{p^{m_2}}$$

卽

(6)　　$\lambda'=\lambda p^{m_2}$　(λ爲整數)

---

*關乎此定義, 請參閱第25節. 如該節之所示, 一元素之相對巡回率, 乃其巡回率之約數也. 因之於$\mathfrak{P}$, 乃爲p之冪焉.

爲必要也. 今以

$$P_2 = S P_1^{-\lambda}, \tag{7}$$

則由(5)及(6), 得

$$P_2^{p^{m_2}} = S^{p^{m_2}} P_1^{-\lambda p^{m_2}} = 1.$$

且 P_2 關於 $\{P_1\}$ 之相對巡回率爲 p^{m_2}, 因之其巡回率亦爲同一. 蓋若令 $P_2^{\alpha} = P_1^{\beta}$, 則由(7)得

$$S^{\alpha} P_1^{-\alpha\lambda} = P_1^{\beta}, \quad 或 \quad S^{\alpha} = P_1^{\beta+\alpha\lambda}.$$

因 S 關於 $\{P_1\}$ 之相對巡回率爲 p^{m_2}, 故 α 須爲 p^{m_2} 之倍數故也.

以兩元素 P_1, P_2 作 $p^{m_1+m_2}$ 個之積

$$P_1^{\alpha_1} P_2^{\alpha_2} \begin{cases} \alpha_1 = 0, 1, 2, \cdots\cdots, p^{m_1}-1 \\ \alpha_2 = 0, 1, 2, \cdots\cdots, p^{m_2}-1, \end{cases} \tag{8}$$

則因兩元素之巡回率分別爲 p^{m_1}, p^{m_2} 之故, 此諸積乃作 $\mathfrak{P}$ 之約羣 $\{P_1, P_2\}$ 也. 且 P_2 關於 $\{P_1\}$ 之相對巡回率爲 p^{m_2}, 故(8)中之積互異, 因之 P_1, P_2 互相獨立. 以故若

$$\mathfrak{P} = \{P_1, P_2\},$$

則二元素 P_1, P_2 爲 $\mathfrak{P}$ 之底也.

反之, 若除積(8)以外, $\mathfrak{P}$ 之元素尙存在時, 則於其中取關於 $\{P_1, P_2\}$ 之相對巡回率爲最高者之一. 以之爲 T, 而其巡回率以爲 p^{m_3}, 卽

$$T^{p^{m_3}} = P_1^{\lambda'_1} P_2^{\lambda'_2} \tag{9}$$

者. 因關於$\{P_1\}$之最高相對巡回率爲p^{m_2}, 故

$$p^{m_3} \leqq p^{m_2}, \text{ 卽 } m_3 \leqq m_2.$$

又p^{m_3}乃λ'_1, λ'_2之約數. 蓋若將(9)之兩邊$p^{m_2-m_3}$方乘之, 則得

$$(10) \qquad T^{p^{m_2}} = P_1^{\lambda'_1 p^{m_2-m_3}} P_2^{\lambda'_2 p^{m_2-m_3}}.$$

然p^{m_2}乃關於$\{P_1\}$之最高相對巡回率. 故$T^{p^{m_2}}$不得不屬於$\{P_1\}$也. 卽

$$T^{p^{m_2}} = P_1^{\mu}.$$

以之代入(10), 得

$$P_1^{\mu-\lambda'_1 p^{m_2-m_3}} P_2^{-\lambda'_2 p^{m_2-m_3}} = 1.$$

然P_1, P_2相互獨立. 故

$$\lambda'_2 p^{m_2-m_3} \equiv 0 \pmod{p^{m_2}}.$$

$$\therefore \quad \lambda'_2 \equiv 0 \pmod{p^{m_3}},$$

或

$$\lambda'_2 = \lambda_2 p^{m_3} \quad (\lambda_2 \text{ 爲整數}).$$

更將(9)之兩邊$p^{m_1-m_3}$方乘之, 得

$$T^{p^{m_1}} = P_1^{\lambda'_1 p^{m_1-m_3}} P_2^{\lambda'_2 p^{m_1-m_3}} = P_1^{\lambda'_1 p^{m_1-m_3}} P_2^{\lambda_2 p^{m_1}}.$$

故由(3)式, 得

$$1 = P_1^{\lambda'_1 p^{m_1-m_3}}.$$

$$\therefore \quad \lambda'_1 p^{m_1-m_3} \equiv 0 \pmod{p^{m_1}}.$$

$$\therefore \quad \lambda'_1 \equiv 0 \pmod{p^{m_3}},$$

或

$$\lambda'_1 = \lambda_1 p^{m_3} \quad (\lambda_1 \text{ 爲整數}).$$

如是, λ'_1, λ'_2皆爲p^{m_3}之倍數. 而(9)則爲

$$(9') \qquad T^{p^{m_3}} = P_1^{\lambda_1 p^{m_3}} P_2^{\lambda_2 p^{m_3}}.$$

今以

$$(11) \qquad P_3 = TP_1^{-\lambda_1} P_2^{-\lambda_2},$$

則由 (9'), 得

$$P_3^{p^{m_3}} = T^{p^{m_3}} P_1^{-\lambda_1 p^{m_3}} P_2^{-\lambda_2 p^{m_3}} = 1,$$

而 P_3 關於 $\{P_1, P_2\}$ 之相對巡回率爲 p^{m_3}, 因之其巡回率亦爲同一. 蓋若令

$$P_3^{\alpha} = P_1^{\beta_1} P_2^{\beta_2},$$

則由 (11) 得

$$T^{\alpha} = P_1^{\beta_1 + \alpha\lambda_1} P_2^{\beta_2 + \alpha\lambda_2},$$

而 T 關於 $\{P_1, P_2\}$ 之相對巡回率爲 p^{m_3}, 故

$$\alpha \equiv 0 \pmod{p^{m_3}}$$

爲必要故也.

茲以三元素 P_1, P_2, P_3 作 $p^{m_1+m_2+m_3}$ 個之積:

$$(12) \quad P_1^{\alpha_1} P_2^{\alpha_2} P_3^{\alpha_3} \begin{cases} \alpha_1 = 0, 1, 2, \cdots\cdots, p^{m_1} - 1, \\ \alpha_2 = 0, 1, 2, \cdots\cdots, p^{m_2} - 1, \\ \alpha_3 = 0, 1, 2, \cdots\cdots, p^{m_3} - 1, \end{cases}$$

則因此三元素之巡回率分別爲 $p^{m_1}, p^{m_2}, p^{m_3}$ 之故, 此諸積遂作 $\mathfrak{P}$ 之約羣 $\{P_1, P_2, P_3\}$ 也. 且此三元素相互獨立. 蓋因 P_3 關於 $\{P_1, P_2\}$ 之相對巡回率爲 p^{m_3}, 故若

$$P_1^{\beta_1} P_2^{\beta_2} P_3^{\beta_3} = 1, \quad \text{卽} \quad P_3^{\beta_3} = P_1^{-\beta_1} P_2^{-\beta_2},$$

則 $\beta_3 \equiv 0 \pmod{p^{m_3}}$ 爲必要; 又因 P_1, P_2 相互獨立, 若

$$P_1^{\beta_1} P_2^{\beta_2} = 1,$$

則須 $\beta_2 \equiv 0 \pmod{p^{m_2}}$, $\beta_1 \equiv 0 \pmod{p^{m_1}}$ 故也.

若以積 (12) 而 $\mathfrak{P}$ 之元素克盡時, 則得

$$\mathfrak{P} = \{P_1, P_2, P_3\},$$

而三元素 P_1, P_2, P_3 遂爲 $\mathfrak{P}$ 之底也. 反之, 除 (12) 之元素外, $\mathfrak{P}$ 之元素尙存在時, 則於其中取其關於 $\{P_1, P_2, P_3\}$ 之相對巡回率爲最高者, 而以上同樣之手續返覆之. 於是因 $\mathfrak{P}$ 之元數爲有限之故, 終能得到生成 $\mathfrak{P}$ 之有限個獨立元素 P_1, P_2, ……, P_r 也.

對此證明, 欲求形式上之嚴密, 則用歸納法可. 此時先假定適合次條件之獨立元素所生成之約羣 $\{P_1, P_2, \cdots\cdots, P_i\}$ 爲存在. 卽 (i) $P_1, P_2, \cdots\cdots, P_i$ 之巡回率分別爲

$$p^{m_1} \geqq p^{m_2} \geqq \cdots\cdots \geqq p^{m_i},$$

(ii) 對於 $\mathfrak{P}$ 之任意元素 P, 則有

$$P^{p^{m_i}} = P_1^{\lambda_1 p^{m_i}} P_2^{\lambda_2 p^{m_i}} \cdots\cdots P_{i-1}^{\lambda_{i-1} p^{m_i}},$$

但 $\lambda_1, \lambda_2, \cdots\cdots, \lambda_{i-1}$ 爲整數者. 於是若以關於約羣 $\{P_1, P_2, \cdots\cdots, P_i\}$ 之最高巡回率爲 p^{m_i+1}, 則如能示: 於 $\mathfrak{P}$, 尙有元素 P_{i+1}, 其巡回率以及其關於 $\{P_1, P_2, \cdots\cdots, P_i\}$ 之相對巡回率共爲 $p^{m_{i+1}}$ 者存在; 且羣 $\{P_1, P_2, \cdots\cdots, P_i, P_{i+1}\}$ 與 $\{P_1, P_2, \cdots\cdots, P_i\}$ 適合同一之條件, 爲已足也. 此方法, 與就 $\{P_1, P_2, P_3\}$ 所論者全然同樣.

2°. Abel 氏羣 $\mathfrak{G}$ 之元數爲 $g = p^m q^n \cdots\cdots$, 時 (但 $p, q, \cdots$

爲表互異之素數者).

茲以 p^m 元, q^n 元, …… 之 Sylow 氏約羣分別爲 $\mathfrak{P}$, $\mathfrak{Q}$, …… 則因此諸羣之元數爲互素之故, 雖取其任二羣, 皆除主元素以外無共通之元素者也. 故 $\mathfrak{G}$ 爲此諸 Sylow 氏約羣之直乘積. 卽

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

於是以 $\mathfrak{P}$, $\mathfrak{Q}$, …… 之底分別爲

$$\mathrm{P}_1, \mathrm{P}_2, \cdots\cdots, \mathrm{P}_r \quad (\mathrm{P}_i \text{ 之巡回率 } p^{m_i}),$$
$$\mathrm{Q}_1, \mathrm{Q}_2, \cdots\cdots, \mathrm{Q}_s \quad (\mathrm{Q}_j \text{ 之巡回率 } q^{n_j}),$$
$$\cdots\cdots\cdots\cdots \quad \cdots\cdots\cdots\cdots,$$

而以之作 p^mq^n …… 個之積:

$$(13) \qquad \mathrm{P}_1^{\alpha_1}\mathrm{P}_2^{\alpha_2}\cdots\cdots\mathrm{P}_r^{\alpha_r}\mathrm{Q}_1^{\beta_1}\mathrm{Q}_2^{\beta_2}\cdots\cdots\mathrm{Q}_s^{\beta_s}\cdots\cdots$$

$$\alpha_i=0, 1, 2, \cdots\cdots, p^{m_i}-1; \quad \beta_j=0, 1, 2, \cdots\cdots, q^{n_j}-1; \cdots\cdots,$$

則其皆互異; 而 $\mathfrak{G}$ 全部之元素, 得由是而與之焉. 卽

$$\mathrm{P}_1, \mathrm{P}_2, \cdots\cdots, \mathrm{P}_r, \quad \mathrm{Q}_1, \mathrm{Q}_2, \cdots\cdots, \mathrm{Q}_s, \cdots\cdots,$$

是爲 $\mathfrak{G}$ 之母元素也. 至此各個之爲相立獨立, 則由 (13) 中之各積互異自明, 因而以此諸元素爲一組, 則足以供 $\mathfrak{G}$ 之底焉.

系. 在素數冪元 Abel 氏羣 $\mathfrak{P}$ 中, 以其巡回率最高者之元素之一爲 P, 則 $\mathfrak{P}$ 與巡回羣 $\{\mathrm{P}\}$ 及他羣之直乘積等.

蓋若以此 P 爲定理之證明 1° 中之 P_1, 則得

$$\mathfrak{P}=\{\mathrm{P}\}\{\mathrm{P}_2, \mathrm{P}_3, \cdots\cdots, \mathrm{P}_r\},$$

而 $P, P_2, \cdots\cdots, P_r$ 又相互獨立故也. 又此系, 雖在 $\mathfrak{P}$ 不爲素數冪元時亦能成立.

注意. 在 Abel 氏羣 $\mathfrak{G}$, 選擇其關於約羣 $\mathfrak{H}$ 之有最高相對巡回率者之元素時, 先將 $\mathfrak{G}$ 就分爲傍系, 以之爲

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

再就 $P_1, P_2, \cdots\cdots, P_{\nu-1}$ 中而取其相對巡回率之最高者可也.

131. 不變系.

於前節開端所揭之羣 $\mathfrak{A}$ 中, 取兩個置換

$$(pq)(rs)(xyz),\ (ps)(qr),$$

以作 12 個之積:

$$[(pq)(rs)(xyz)]^{\alpha}[(ps)(qr)]^{\beta}\begin{cases}\alpha=0, 1, 2, 3, 4, 5,\\ \beta=0, 1,\end{cases}$$

則以是而 $\mathfrak{A}$ 之元素克盡. 故上記之兩置換乃 $\mathfrak{A}$ 之獨立母元素, 而卻與該節中所示者異也. 夫如是, 則於 Abel 氏羣, 其底不一定, 而其選擇之方法亦有種種也; 雖然此其間尙有一定不變之關係者在, 試就下而說明之焉.

1.° 素數冪元時.

令 $\mathfrak{P}$ 爲 p^m 元 (p 爲素數) 之 Abel 氏羣. 對於 $\mathfrak{P}$ 之任意二元素 A, B, 乃有

$$A^{p^x}B^{p^x}=(AB)^{p^x}.$$

故若將 $\mathfrak{P}$ 之各元素 p^x 方乘之, 其所得之冪之集合, 卽作 $\mathfrak{P}$ 之約羣也. 試以 $\mathfrak{P}^{(x)}$ 表之.

今以$\mathfrak{P}$之底爲

(1) $$P_1, P_2, \cdots\cdots, P_r,$$

以其各母元素之巡回率分別爲

(2) $$p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_r} \quad (m_1+m_2+\cdots\cdots+m_r=m).$$

但

(3) $$m_1 \geqq m_2 \geqq \cdots\cdots \geqq m_r.$$

於是因$\mathfrak{P}$之任意元素P得以

$$P=P_1^{\alpha_1}P_2^{\alpha_2}\cdots\cdots P_r^{\alpha_r}$$

表之之故,乃於指數列(3),在其較x大之諸項內,以其最後者爲m_y,卽

(4) $$m_y > x \geqq m_{y+1},$$

則得

$$P^{p^x}=(P_1^{p^x})^{\alpha_1}(P_2^{p^x})^{\alpha_2}\cdots\cdots(P_y^{p^x})^{\alpha_y}.$$

而

(5) $$P_1^{p^x}, P_2^{p^x}, \cdots\cdots, P_y^{p^x}$$

分別有巡回率

$$p^{m_1-x}, p^{m_2-x}, \cdots\cdots, p^{m_y-x} \text{(無論何個皆大於1)},$$

且相互獨立. 故(5)者,卽表示約羣$\mathfrak{P}^{(x)}$之底者也. 因而若$\mathfrak{P}^{(x)}$之元數示以$p^{f(x)}$,則得

(6) $$f(x)=(m_1-x)+(m_2-x)+\cdots\cdots+(m_y-x)$$
$$=m_1+m_2+\cdots\cdots+m_y-yx.$$

復次於(1)之外任意取$\mathfrak{P}$之底

(7) $$P'_1, P'_2, \cdots\cdots, P'_s,$$

而各母元素之巡回率分別以爲

(8)　$p^{m'_1}, p^{m'_2}, \cdots\cdots, p^{m'_s}$　$(m'_1+m'_2+\cdots\cdots+m'_s=m)$.

但

(9)　$m'_1 \geqq m'_2 \geqq \cdots\cdots \geqq m'_s$.

在此數列中,以其較 x 大者之最後之項爲 m'_z,卽

(10)　$m'_z > x \geqq m'_{z+1}$

則與前同樣,得

(11)　$f(x)=(m'_1-x)+(m'_2-x)+\cdots\cdots+(m'_s-x)$

$=m'_1+m'_2+\cdots\cdots+m'_z-zx$.

且$\mathfrak{P}$之元素之巡回率中之最高者,由底(1)而觀爲 p^{m_1},而由(7)而觀,則爲 $p^{m'_1}$; 故

$$p^{m_1}=p^{m'_1},\quad \text{因之}\quad m_1=m'_1$$

爲必要也. 今假定

(12)　$m_1=m'_1,\ m_2=m'_2,\ m_i=m'_i$

爲已證明者. 此時若再假定 $m_{i+1}<m'_{i+1}$,則因

$$m_i=m'_i \geqq m'_{i+1} > m_{i+1}$$

之故,對於 $x=m_{i+1}$,由(4)得 $y=i$; 而由(6)則得

(13)　$f(m_{i+1})=m_1+m_2+\cdots\cdots+m_i-im_{i+1}$.

又以 $m'_{i+1}, m'_{i+2}, \cdots\cdots, m'_s$ 中之較 m_{i+1} 大者爲

(14)　$m'_{i+1}, \cdots\cdots, m'_{i+d}$　$(d \geqq 1)$,

則對 $x=m_{i+1}$,由(10)得 $z=i+d$,而由(11)則得

$$f(m_{i+1})=m'_1+m'_2+\cdots\cdots+m'_{i+d}-(i+d)m_{i+1}.$$

由此與(13)得

$$m_1+m_2+\cdots\cdots+m_i-im_{i+1}=m'_1+m'_2+\cdots\cdots+m'_{i+d}-(i+d)m_{i+1}.$$

故由假定(12),

$$m'_{i+1}+\cdots\cdots+m'_{i+d}-dm_{i+1}=0.$$

$$\therefore\ (m'_{i+1}-m_{i+1})+\cdots\cdots+(m'_{i+d}-m_{i+1})=0.$$

然由關於(14)之條件,此式之左邊乃較零大. 故本式不得成立. 此矛盾係由 $m_{i+1}<m'_{i+1}$ 之假定而起. 然卽假定 $m_{i+1}>m'_{i+1}$, 亦同樣生不合理之結果. 是故在 $m_1=m'_1$, $m_2=m'_2$, ……, $m_i=m'_i$ 時 $m_{i+1}=m'_{i+1}$ 爲必要也. 然 $m_1=m'_1$ 已證之矣. 故指數列(3)之各項順次與(9)之各項等, 因之 $r=s$ 所必要焉.

夫如是在素數冪元之Abel氏羣中,不論其底之選擇如何,而其作底者之獨立母元素之巡回率則一定也. 此各巡回率稱曰**不變率**;而將作底者之獨立母元素之巡回率以爲一組,則名之曰羣之**不變系**. 上記羣$\mathfrak{P}$之不變系,卽

$$p^{m_1},\ p^{m_2},\ \cdots\cdots,\ p^{m_r}$$

也.

2°. 一般者.

設Abel氏羣$\mathfrak{G}$之元數爲 $g=p^mq^n\cdots\cdots$. 但 $p, q, \cdots\cdots$ 爲互異之素數. 乃取$\mathfrak{G}$之任意之底

(15) $$A_1,\ A_2,\ \cdots\cdots,\ A_t.$$

以各母元素之巡回率分別爲

(16)　　$a_1, a_2, \cdots\cdots, a_t,$

而此各個所含之 p 之最高冪分別爲

$$p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_t} \quad (m_i \geqq 0),$$

又以其中之指數不爲零者爲

(17)　　$p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_r}.$

今取 r 個之冪

(18)　　$A_1{}^{a_1 p-m_1}, \quad A_2{}^{a_2 p-m_2}, \quad \cdots\cdots, \quad A_r{}^{a_r p-m_r},$

則此各個之相互獨立甚明，而其巡回率則以(17)得與之也. 故此諸冪乃生成一 $p^{m_1+m_2+\cdots\cdots+m_r}$ 元之約羣焉. 然

$$a_1 a_2 \cdots\cdots a_t = g = p^m q^n \cdots\cdots.$$

因之

$$p^{m_1+m_2+\cdots\cdots m_r} = p^m.$$

故(18)所以表 p^m 元 Sylow 氏約羣之底，因而(17)卽爲約羣之不變系. 但自他面言，Abel 氏羣 $\mathfrak{G}$，僅有唯一之 p^m 元約羣(參照第 54 節). 以故不論底(15)之選擇方法如何，p 之冪列(17)須一定也. (但順序則在所不論.) 換言之，卽謂其含在 $\mathfrak{G}$ 之獨立母元素之巡回率中者之 p 之冪，與底之選擇無關而常爲一定者也. 又對他之素數因子($q, \cdots\cdots$)言，亦復如是. 爰得

定理. 在 Abel 氏羣中，其含在爲底之獨立母元素之巡回率中者之素數之冪，不論底之選法如何，常爲一定.

本定理中素數冪之各個名曰 Abel 氏羣之**不變率**，而

由其爲底者之獨立母元素之全部所得之不變率以爲一組,而名之曰同羣之**不變系**.

如在前節開端之例中,其選以充底者,或取

$$(pq)(rs),\quad (pr)(qs),\quad (xyz),$$

或選

$$(pq)(rs)(xyz),\quad (ps)(qr),$$

其不變系共爲

$$2, 2, 3$$

也.

132. Abel 氏羣之型.

定理. 若兩 Abel 氏羣,其不變系爲同一,則兩羣爲單純同態.

證明. 1°. 素數冪元時.

設 p^m 元 Abel 氏羣 $\mathfrak{P}'$ 與前節 1° 中之 $\mathfrak{P}$ 有同一之不變系,卽 $\mathfrak{P}'$ 之獨立母元素

$$P'_1,\ P'_2,\ \cdots\cdots,\ P'_r$$

之巡回率分別爲

$$p^{m_1},\ p^{m_2},\ \cdots\cdots,\ p^{m_r}$$

者. 於是對 $\mathfrak{P}$ 之元素 $P_1^{\alpha_1}\ P_2^{\alpha_2}\cdots\cdots P_r^{\alpha_r}$ 使 $\mathfrak{P}'$ 之元素 $P_1'^{\alpha_1}\ P_2'^{\alpha_2}\cdots\cdots P_r'^{\alpha_r}$ 相與對應,則兩羣之爲單純同態明已.

2°. 一般者.

以 Abel 氏羣 $\mathfrak{G}$ 之元數爲 $g=p^m q^n\cdots\cdots$; 而其 p^m 元, q^n 元, …… 之 Sylow 氏約羣則分別以 $\mathfrak{P}$, $\mathfrak{Q}$, …… 表之. 又他之

Abel 氏羣 $\mathfrak{G}'$ 之元數以爲 $g'=p^{m'}q^{n'}\cdots\cdots$，而其 $p^{m'}$ 元，$q^{n'}$ 元，…… 之 Sylow 氏約羣則分別以 $\mathfrak{P}'$, $\mathfrak{Q}'$, …… 表之．於是用前節 2° 中同樣之方法以生成 $\mathfrak{P}$ 及 $\mathfrak{P}'$，則因兩羣 $\mathfrak{G}$ 及 $\mathfrak{G}'$ 之不變系爲同一之故，其 Sylow 氏約羣 $\mathfrak{P}$ 及 $\mathfrak{P}'$ 之不變系亦不得不一致也．故由 1°，$\mathfrak{P}$ 與 $\mathfrak{P}'$ 爲同型焉．其他 Sylow 氏約羣準此．

於 $\mathfrak{G}$, $\mathfrak{G}'$，兩羣之 Sylow 氏約羣之同態關係中，若對 $\mathfrak{P}$ 之元素 P，$\mathfrak{P}'$ 之元素 P′ 相與對應，於 $\mathfrak{Q}$ 之元素 Q 則 $\mathfrak{Q}'$ 之元素 Q′ 相與對應時，使對 $\mathfrak{G}$ 之元素 PQ …… 令 $\mathfrak{G}'$ 之元素 P′Q′ …… 相與對應，則 $\mathfrak{G}$ 與 $\mathfrak{G}'$ 之爲同態明已．故定理云云．

系．於二 Abel 氏羣，若各個之 Sylow 氏約羣之不變系一致時，則兩羣爲同型．

復次，於元數爲已知者之 Abel 氏羣中，就其有相異之型者之數一言之：

$p^m q^n$ …… 元之 Abel 氏羣，乃 p^m 元，q^n 元，……，Sylow 氏約羣之直乘積也．故若以 p^m 元 Abel 氏羣之數爲 M，q^n 元 Abel 氏羣之數爲 N，……，則 $p^m q^n$ …… 元 Abel 氏羣之數等於 MN …….

就素數冪元 Abel 氏羣而觀，在 p^m 元者時，其不變系，乃由 p 之冪

$$p^{m_1},\ p^{m_2},\ \cdots\cdots,\ p^{m_r}\quad (m_1+m_2+\cdots\cdots+m_r=m)$$

而成者也．而此諸數則以指數

$$m_1, m_2, \cdots\cdots, m_r$$

而定. 然由本節定理, Abel 氏羣乃一意的由不變系而定. 故在 p^m 元 Abel 氏羣之中,其不同型者之個數,與適合於

$$m_1+m_2+\cdots\cdots+m_r=m$$

$$m_1 \geqq m_2 \geqq \cdots\cdots \geqq m_r$$

者之 m 之分法 $(m_1, m_2, \cdots\cdots, m_r)$ 之數等. 如 $m=3$ 時, 則適合上條件之 3 之分法爲

$$(3),\ (2, 1),\ (1, 1, 1)$$

之三種.故 p^3 元 Abel 氏羣中有三異型者存在也.又若 $m=2$, 則其分法有二:

$$(2),\quad (1, 1)$$

因之 $p^3 q^2$ 元 $(p \neq q)$ Abel 氏羣之數(異型者)爲 $3\times 2=6$ 焉.

注意. 不變系爲 $p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_r}$ 者之 Abel 氏羣, 略稱之曰 $[p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_r}]$ 型或 $[m_1, m_2, \cdots\cdots, m_r]$ 型之 Abel 氏羣.

133. 約羣之型.

羣 $\mathfrak{G}$ 之約羣之 Sylow 氏約羣,乃含於 $\mathfrak{G}$ 之 Sylow 氏約羣中者也(第 54 節系 2). 而 Abel 氏羣則爲 Sylow 氏約羣之直乘積. 故 Abel 氏羣約羣之型, 只就素數冪元者討論之, 則關於一般 Abel 氏羣者亦自明也.

茲再取第 131 節所論之 Abel 氏羣 $\mathfrak{P}$. $\mathfrak{P}$ 中能滿足

(1) $$P^p=1$$

者之元素P之形成一羣，明已．乃以$\mathfrak{P}_1$表之而求其元數．

若　$$P^p=P_1^{\alpha_1 p}P_2^{\alpha_2 p}\cdots\cdots P_r^{\alpha_r p}=1.$$

則　$$\alpha_i p\equiv 0 \pmod{p^{m_i}} \quad (i=1,2,\cdots\cdots,r),$$

或　$$\alpha_i=\lambda_i p^{m_i-1} \qquad (i=1,2,\cdots\cdots,r)$$

爲必要也．故

(2)　$$P=(P_1^{p^{m_1-1}})^{\lambda_1}(P_2^{p^{m_2-1}})^{\lambda_2}\cdots\cdots(P_r^{p^{m_r-1}})^{\lambda_r}.$$

反之，P若有是形，則P之滿足(1)甚明．然

$$P_1^{p^{m_1-1}},\ P_2^{p^{m_2-1}},\ \cdots\cdots,\ P_r^{p^{m_r-1}}$$

之巡回率任何個皆爲p．故以(2)所表之元素之數，即$\mathfrak{P}_1$之元數乃p^r也．

其次取$\mathfrak{P}$之任意一約羣$\mathfrak{T}$，以其型爲$[n_1\geqq n_2\geqq\cdots\cdots\geqq n_s]$．於$\mathfrak{T}$，其由滿足

$$T^p=1$$

者之元素T所成之約羣(以$\mathfrak{T}_1$表之)之元數與前同樣爲p^s．然$\mathfrak{T}_1$之元素均含於$\mathfrak{P}_1$甚明．故

$$p^s\leqq p^r,$$

或　$$s\leqq r.$$

即謂約羣$\mathfrak{T}$中獨立母元素(作一底者)之數不得超過$\mathfrak{P}$中獨立母元素(作一底者)之數也．

更就不變率之大小關係論之．

茲假定　$$m_i<n_i.$$

在$m_1,\cdots\cdots,m_i$之中其與m_i等者以爲

$$m_{i-d}, \cdots\cdots, m_i \quad (d \geqq 0),$$

而於 $n_1, \cdots\cdots, n_i, \cdots\cdots, n_s$ 中其較 m_i 大者以爲

$$n_1, \cdots\cdots, n_i, \cdots\cdots, n_{i+e} \quad (e \geqq 0),$$

則將 $\mathfrak{P}$ 之各元素 p^{m_i} 方乘之,其所得約羣 $\mathfrak{P}^{(m_i)}$ 得由 $(i-1-d)$ 個獨立母元素

$$P_1^{p^{m_i}}, P_2^{p^{m_i}}, \cdots\cdots, P_{i-1-d}^{p^{m_i}} \quad (d \geqq 0)$$

生成之;而將 $\mathfrak{T}$ 之各元素 p^{m_i} 方乘之,其所得約羣 $\mathfrak{T}^{(m_i)}$ 得由 $i+e$ 個獨立母元素

$$T_1^{p^{m_i}}, T_2^{p^{m_i}}, \cdots\cdots, T_{i+e}^{p^{m_i}} \quad (e \geqq 0)$$

而生成之也. 但 $T_1, T_2, \cdots\cdots, T_s$ 爲表示 $\mathfrak{T}$ 之底者. 以此是觀,可知爲底者之母元素之數,在 $\mathfrak{T}^{(m_i)}$ 方言較 $\mathfrak{P}^{(m_i)}$ 者多也. 然 $\mathfrak{T}^{(m_i)}$ 明爲 $\mathfrak{P}^{(m_i)}$ 之約羣,因之由上述,$\mathfrak{T}^{(m_i)}$ 中獨立母元素之數應不能超過 $\mathfrak{P}^{(m_i)}$ 中者之數. 是豈非矛盾耶? 是則 $m_i < n_i$ 之假定不合理也. 卽 $m_i \geqq n_i$ 者無疑.

反之,$s \leqq r$, $n_i \leqq m_i$ $(i=1, 2, \cdots\cdots)$ 時,則 Abel 氏羣 $[m_1, m_2, \cdots\cdots, m_r]$ 含約羣 $[n_1, n_2, \cdots\cdots, n_s]$. 蓋因

$$P_1^{p^{m_1-n_1}}, P_2^{p^{m_2-n_2}}, \cdots\cdots, P_s^{p^{m_s-n_s}}$$

生成 $[n_1, n_2, \cdots\cdots, n_s]$ 型之約羣故也. 因之得次

定理. 凡含於 $[m_1 \geqq m_2 \geqq \cdots\cdots \geqq m_r]$ 型之素數冪元 Abel 氏羣 $\mathfrak{P}$ 者之約羣之型 $[n_1 \geqq n_2 \geqq \cdots\cdots \geqq n_s]$ 必滿足次之條件:

$$s \leqq r; \quad n_i \leqq m_i \quad (i=1, 2, \cdots\cdots).$$

反之，若 $n_1, n_2, \cdots\cdots, n_s$ 適合此條件時，則 $\mathfrak{P}$ 卽有 $[n_1, n_2, \cdots\cdots, n_s]$ 型之約羣.

注意. 相異約羣之有同一之型者乃有之也. 如於 p^6 元 Abel 氏羣 $\{P, Q, R\}$ (但 $P^{p^3}=1$, $Q^{p^2}=1$, $R^p=1$) 其二約羣 $\{P^p, Q^p\}$, 及 $\{Q, R\}$ 共爲 $[2, 1]$ 型者是.

134. $[1, 1, \cdots\cdots, 1]$ **型 Abel 氏羣中約羣之數.**

設 $\mathfrak{G}$ 爲 p^m 元 $[1, 1, \cdots\cdots, 1]$ 型之 Abel 氏羣，其中 p^s 元約羣之數，則以 $N(m, s)$ 表之.

$\mathfrak{G}$ 之元素(除主元素外)之巡回率皆爲 p. 卽於 $\mathfrak{G}$ 其巡回率爲 p 者之元素之數爲 p^m-1 也. 又自他方言，相異之 p 元約羣無有共通元素(主元素以外者). 故 $\mathfrak{G}$ 中 p 元約羣之個數爲

$$N(m, 1)=\frac{p^m-1}{p-1}. \tag{1}$$

次爲求 p^s 元約羣之數計，乃取 p^{s-1} 元約羣之一 $\mathfrak{H}_{s-1}$. p 元約羣內含於 $\mathfrak{H}_{s-1}$ 者之個數爲

$$N(s-1, 1)=\frac{p^{s-1}-1}{p-1}.$$

因之 $\mathfrak{G}$ 中 p 元約羣之內其不含於 $\mathfrak{H}_{s-1}$ 者之個數爲

$$N(m, 1)-N(s-1, 1)=\frac{p^m-p^{s-1}}{p-1}.$$

將後者之一乘於 $\mathfrak{H}_{s-1}$，則得 p^s 元約羣. 故若乘 p 元約羣於 $\mathfrak{H}_{s-1}$，則由之可生 $\frac{p^m-p^{s-1}}{p-1}$ 個之 p^s 元約羣也. 但此等之中

得有相等者存在. 故欲於此 $\frac{p^m-p^{s-1}}{p-1}$ 個中求其相異者之個數, 乃取含 $\mathfrak{H}_{s-1}$ 者之 p^s 元約羣 $\mathfrak{H}_s$ 焉. 於是含於 $\mathfrak{H}_s$ 而不含於 $\mathfrak{H}_{s-1}$ 者之元 p 約羣之個數爲

$$\frac{p^s-1}{p-1}-\frac{p^{s-1}-1}{p-1}=p^{s-1}$$

也. 將此等 p^{s-1} 個約羣之任何個乘於 $\mathfrak{H}_{s-1}$ 皆得 $\mathfrak{H}_s$. 故上述之 $\frac{p^m-p^{s-1}}{p-1}$ 個之 p^s 元約羣中, 每 p^{s-1} 個皆相等. 故含 $\mathfrak{H}_{s-1}$ 者之 p^s 元約羣之數(互異者)爲

$$\frac{p^m-p^{s-1}}{p-1}\div p^{s-1}=\frac{p^{m-s+1}-1}{p-1}.$$

然 $\mathfrak{G}$ 含有 $\mathrm{N}(m, s-1)$ 個之 p^{s-1} 元約羣. 故若乘 p 元約羣於此諸羣, 其所得 p^s 元約羣之總數爲

$$\mathrm{N}(m, s-1)\times\frac{p^{m-s+1}-1}{p-1}$$

也. 但此等之中又得有相等者存在, 試討論之. 因 $\mathfrak{H}_s$ 含有 $\mathrm{N}(s, s-1)$ 個之 p^{s-1} 元約羣, 故由相異之 $\mathrm{N}(s, s-1)$ 個 p^{s-1} 元約羣得作同一之 p^s 元約羣也. 故上所得 p^s 元約羣之總數中, 其相異者之數爲

$$\mathrm{N}(m, s-1)\times\frac{p^{m-s+1}-1}{p-1}\div\mathrm{N}(s, s-1).$$

以故

$$(2)\qquad \mathrm{N}(m, s)=\frac{\mathrm{N}(m, s-1)}{\mathrm{N}(s, s-1)}\cdot\frac{p^{m-s+1}-1}{p-1}.$$

於此式, 若令 $s=2$, 且利用(1), 則得

$$N(m,2)=\frac{N(m,1)}{N(2,1)}\cdot\frac{p^{m-1}-1}{p-1}=\frac{(p^m-1)(p^{m-1}-1)}{(p-1)(p^2-1)}.$$

更於(2)令$s=3$且用本式,復得

$$N(m,3)=\frac{N(m,2)}{N(3,2)}\cdot\frac{p^{m-2}-1}{p-1}=\frac{(p^m-1)(p^{m-1}-1)(p^{m-2}-1)}{(p-1)(p^2-1)(p^3-1)}.$$

將此反覆行之遂得

$$(3)\qquad N(m,s)=\frac{(p^m-1)(p^{m-1}-1)\cdots\cdots(p^{m-s+1}-1)}{(p-1)(p^2-1)\cdots\cdots(p^s-1)}.$$

是卽$[1,1,\cdots\cdots,1]$型p^m元Abel氏羣中p^s元約羣之個數也.

關於(3)式導出之方法,若欲求其形式的嚴密,則可假定對於任意之正整數m,以及不大於$r(<m)$之各整數s,(3)式爲眞,而再利用(2)以示雖在$s=r+1$時本式亦得成立者可也.

又由(3)卽可以得到

$$N(m,m-s)=N(m,s)$$

亦不可不知.

注意. 上之證明,乃利用p^s元約羣必含p^{s-1}元約羣,而p^{s-1}元約羣定含於某一個之p^s元約羣(第47節定理)者而爲之者也. 又於上之p^s元約羣皆有同一之型$[1,1,\cdots\cdots(s個)]$焉.

135. Abel氏羣之同態羣.

設$\mathfrak{G}$爲Abel氏羣,

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

爲其底,(1)之巡回率則分別以爲

$$a_1,\ a_2,\ \cdots\cdots,\ a_n.$$

$\mathfrak{G}$之自己同態,若其與母元素(1)之各個相對應者得定時,則由是得一意的而決定之也. 今對於(1)之各個,有

$$(2) \qquad A'_1,\ A'_2,\ \cdots\cdots,\ A'_n$$

相與對應時,則其自己同態,以

$$(3) \qquad \begin{bmatrix} A_1 & A_2 & \cdots\cdots & A_n \\ A'_1 & A'_2 & \cdots\cdots & A'_n \end{bmatrix}$$

表之,或略記爲$\begin{bmatrix} A_i \\ A'_i \end{bmatrix}$;而伴此之同態置換,則以

$$(4) \qquad \begin{pmatrix} A_1 & A_2 & \cdots\cdots & A_n \\ A'_1 & A'_2 & \cdots\cdots & A'_n \end{pmatrix} \text{ 或 } \begin{pmatrix} A_i \\ A'_i \end{pmatrix}$$

表之焉.

因(1)爲$\mathfrak{G}$之底,故

$$(5) \qquad A'_i = A_1^{a_{i1}} A_2^{a_{i2}} \cdots\cdots A_n^{a_{in}} \quad (i=1,\ 2,\ \cdots\cdots,\ n).$$

故與A_i相對應之元素A'_i,得由此右邊之指數$a_{i1},\ a_{i2},\ \cdots\cdots,\ a_{in}$而決定. 因之以(5)右邊之指數作母式

$$(6) \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn} \end{pmatrix},$$

則由此而以(5)之關係乃得$A'_1,\ A'_2,\ \cdots\cdots,\ A'_n$,因而自己同態(3)亦告決定. 是卽自己同態(3)以及同態置換(4)均得

以此母式而表之者也.

今有兩母式(a_{ij})及(b_{ij})爲表二同態置換(4)及

(7)　$\begin{pmatrix} A_i \\ A''_i \end{pmatrix}$,　$A''_i = A_1^{b_{i1}} A_2^{b_{i2}} \cdots\cdots A_n^{b_{in}}$

者. 若兩者對於法

(8)　$$\begin{pmatrix} a_1\ a_2 \cdots\cdots a_n \\ a_1\ a_2 \cdots\cdots a_n \\ \cdots\cdots\cdots\cdots \\ a_1\ a_2 \cdots\cdots a_n \end{pmatrix}$$

相合同,則

$$A''_i = A'_i \quad (i=1, 2, \cdots\cdots, n),$$

兩同態爲同一也. 反之,若此兩母式爲非合同,則兩同態互異. 故表示自己同態或同態置換之母式,得以(8)之母式爲法而討論之焉. 在本節中,母式(8)爲便宜計特記爲**M**.

將(7)右乘於同態置換(4),以所得之結果爲

(9)　$$\begin{pmatrix} A_i \\ A'_i \end{pmatrix}\begin{pmatrix} A_i \\ A''_i \end{pmatrix} = \begin{pmatrix} A_i \\ A_i''' \end{pmatrix},$$

則

(10)　$A_i''' = A_1^{c_{i1}} A_2^{c_{i2}} \cdots\cdots A_n^{c_{in}} \quad (i=1, 2, \cdots\cdots, n).$

但

(11)　$c_{ij} \equiv a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots\cdots + a_{in}b_{nj} \pmod{a_j}$

$$(i, j=1, 2, \cdots\cdots, n).$$

由此最後之關係,

(12) $$(a_{ij})(b_{ij})\equiv(c_{ij}) \pmod{\mathbf{M}}.$$

故以(a_{ij}), (b_{ij})所表示之兩同態置換之積,得以兩母式之積(法**M**)表之也. 然同態置換之乘法爲一意的. 故表此之母式之乘法(法**M**)亦不得不爲一意的也.

以同態置換$\begin{pmatrix}A_i\\A'_i\end{pmatrix}$之逆爲$\begin{pmatrix}A_i\\\bar{A}_i\end{pmatrix}$, 則

$$\begin{pmatrix}A_i\\A'_i\end{pmatrix}\begin{pmatrix}A_i\\\bar{A}_i\end{pmatrix}=\begin{pmatrix}A_i\\A_i\end{pmatrix}=1.$$

然表不動同態之母式,乃與主母式合同(法**M**)者. 故若以表$\begin{pmatrix}A_i\\A'_i\end{pmatrix}$及$\begin{pmatrix}A_i\\A_i\end{pmatrix}$者之母式分別爲$(a_{ij})$及$(\bar{a}_{ij})$, 則由(12)得

$$(a_{ij})(\bar{a}_{ij})\equiv(e_{ij}) \pmod{\mathbf{M}}.$$

卽表示同態置換者之母式,就關於法**M**之乘法言,乃有逆者也.

於是表示同態置換者之母式,旣關於法**M**其乘法爲一意的,且復有其逆母式. 以故若是者之母式,必全部均屬於關於法**M**之母式合同羣也(參照第113節). 然同態置換相集而成同態羣. 故表同態者之母式之集合,或爲母式合同羣(法**M**),或爲其約羣焉.

復次乃取一屬於合同羣(法**M**)之任意母式(a_{ij}),而令

$$A'_i=A_1^{a_{i1}}A_2^{a_{i2}}\cdots\cdots A_n^{a_{in}} \qquad (i=1, 2, \cdots\cdots, n).$$

若以母式$(\bar{a}_{ij})$爲(a_{ij})之逆(法**M**), 則

$$\sum_{s=1}^{n} \bar{a}_{is} a_{sj} \equiv e_{ij} \pmod{a_j}.$$

故由之得

$$(A'_1)^{\bar{a}_{i1}} (A'_2)^{a_{i2}} \cdots\cdots (A'_n)^{\bar{a}_{in}} = A_i.$$

因之羣$\mathfrak{G}$之元素得以$A'_1, A'_2, \cdots\cdots, A'_n$之積表之也. 是則此各個卽爲$\mathfrak{G}$之母元素者矣. 欲知各個之巡回率, 乃將$A_i'$而$a_i$方乘之, 則得

$$(A'_i)^{a_i} = A_1^{a_i a_{i1}} A_2^{a_i a_{i2}} \cdots\cdots A_n^{a_i a_{in}}.$$

然由第111, 第112節所述,

$$a_{ij} = a_{ij} f_{ij}, \quad a_i f_{ij} \equiv 0 \pmod{a_j}.$$

故

$$(A'_i)^{a_i} = 1.$$

因之A'_i之巡回率或爲a_i或爲其約數也. 若以之爲小於a_i, 則$\mathfrak{G}$之元數遂較$a_1 a_2 \cdots\cdots a_n$爲小, 是不合理. 故母元素$A'_1, A'_2, \cdots\cdots, A'_n$之巡回率分別爲$a_1, a_2 \cdots\cdots, a_n$; 因而此各個皆獨立, 卽作基底. 因之

$$\begin{pmatrix} A_1 & A_2 & \cdots\cdots & A_n \\ A'_1 & A'_2 & \cdots\cdots & A'_n \end{pmatrix}$$

卽爲$\mathfrak{G}$之同態置換. 是則凡屬於合同羣(法**M**)之母式, 皆表示同態置換者也.

綜合上述, 得次

定理. 設$A_1, A_2, \cdots\cdots, A_n$爲Abel氏羣$\mathfrak{G}$之底, $a_1, a_2, \cdots\cdots, a_n$分別爲其各個之巡回率, 則$\mathfrak{G}$之同態羣乃與以母式

$$\begin{pmatrix} a_1 & a_2 & \cdots\cdots & a_n \\ a_1 & a_2 & \cdots\cdots & a_n \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_1 & a_2 & \cdots\cdots & a_n \end{pmatrix}$$

爲法之母式合同羣爲單純同態.

注意. 此定理乃在 $A_1, A_2, \cdots\cdots, A_n$ 爲底卽此各個皆相互獨立之假設下而證明之者. 但此諸母元素雖不爲獨立時,然在某條件之下,定理亦得成立也. 如有若干個主元素含在此諸母元素之中,而主元素以外之元素則互爲獨立者是. 此之證明與上全然同樣.

136. Sylow 氏約羣之同態羣.

與前節同樣,仍以 $A_1, A_2, \cdots\cdots, A_n$ 爲 Abel 氏羣 $\mathfrak{G}$ 之底, $a_1, a_2, \cdots\cdots, a_n$ 爲其巡回率. 在含於巡回率之最小公倍數之素因數之中,以其互異者爲 $p, q, \cdots\cdots$,而令

$$(1) \qquad a_i = p^{m_i} q^{n_i} \cdots\cdots \qquad (i=1, 2, \cdots\cdots n).$$

但 $m_i, n_i, \cdots\cdots$ 之中等於零者得存在. 今以 p^{m_i} 除 a_i, 其所得之商示以 α_i, 則

$$(2) \qquad A_1^{\alpha_1}, A_2^{\alpha_2}, \cdots\cdots, A_n^{\alpha_n}$$

之巡回率分別爲

$$(3) \qquad p^{m_1}, p^{m_2}, \cdots\cdots, p^{m_n}.$$

而屬於 p 之 Sylow 氏約羣 ($\mathfrak{G}$ 的) 得以 (2) 之元素之積表之

甚明. 於是由前節定理及其注意,知此Sylow氏約羣(名之曰$\mathfrak{P}$)之同態羣乃與以母式

$$\mathbf{P}=\begin{pmatrix} p^{m_1} & p^{m_2} & \cdots\cdots & p^{m_n} \\ p^{m_1} & p^{m_2} & \cdots\cdots & p^{m_n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ p^{m_1} & p^{m_2} & \cdots\cdots & p^{m_n} \end{pmatrix}$$

爲法之母式合同羣爲單純同態也.

同樣,屬於q之Sylow氏約羣則與以母式

$$\mathbf{Q}=\begin{pmatrix} q^{n_1} & q^{n_2} & \cdots\cdots & q^{n_n} \\ q^{n_1} & q^{n_2} & \cdots\cdots & q^{n_n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ q^{n_1} & q^{n_2} & \cdots\cdots & q^{n_n} \end{pmatrix}$$

爲法之母式合同羣爲單純同態. 其他準此. 然由第120節第二定理,其關於法$\mathbf{M}$(前節母式(8))之母式合同羣,乃與關於法$\mathbf{P}$,法$\mathbf{Q}$,……之合同羣之直乘積等. 故得

定理. Abel氏羣之同態羣,乃與Sylow氏約羣之同態羣之直乘積爲單純同態.

更就Sylow氏約羣一言. 以(3)內較1大者爲

$$p^{m_1},\ p^{m_2},\ \cdots\cdots,\ p^{m_r},$$

則此各個形成屬於p之不變系($\mathfrak{S}$的),而

$$\mathrm{A}^{\alpha_1},\ \mathrm{A}^{\alpha_2},\ \cdots\cdots,\ \mathrm{A}^{\alpha_r}$$

作 $\mathfrak{P}$ 之底. 故 $\mathfrak{P}$ 之同態羣, 由前節定理, 乃與以 r 次母式

$$\begin{pmatrix} p^{m_1}, p^{m_2}, \cdots\cdots p^{m_r} \\ p^{m_1}, p^{m_2}, \cdots\cdots p^{m_r} \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ p^{m_1}, p^{m_2}, \cdots\cdots p^{m_r} \end{pmatrix}$$

爲法之母式合同羣爲單純同態. 因之此羣乃與以 $\mathbf{P}$ 爲法之合同羣同型也. 而此則與第 114 節第二定理系中所述者一致焉. 就他之 Sylow 氏約羣之同態羣言, 亦復同樣. 以故 Abel 氏羣之同態羣, 由其不變系容易得以決定之也.

又上之定理, 不由母式合同羣, 直接的亦得證明之. 卽以

$$\mathfrak{P}: \quad P_0, P_1, P_2, \cdots\cdots$$
$$\mathfrak{Q}: \quad Q_0, Q_1, Q_2, \cdots\cdots$$
$$\cdots\cdots \quad \cdots\cdots\cdots\cdots$$

分別爲屬於 $p, q, \cdots\cdots$ 之 Sylow 氏約羣, 則 $\mathfrak{G}$ 之元素得一意的表之爲 $P_i Q_j \cdots\cdots$ 之形 (第 130 節 2°). 但自他面言, Abel 氏羣中之 Sylow 氏約羣皆係特性的 (第 103 節). 故於 $\mathfrak{G}$ 之任意的同態置換 L, 若 $\mathfrak{P}$ 之元素 $P_0, P_1, \cdots\cdots$ 分別得以 $P'_0, P'_1, \cdots\cdots$ 置換; $\mathfrak{Q}$ 之元素 $Q_0, Q_1, \cdots\cdots$ 分別得以 $Q'_0, Q'_1, \cdots\cdots$ 置換之, 則

$$(4) \qquad \begin{pmatrix} P_0 & P_1 & \cdots\cdots \\ P'_0 & P'_1 & \cdots\cdots \end{pmatrix}, \begin{pmatrix} Q_0 & Q_1 & \cdots\cdots \\ Q'_0 & Q'_1 & \cdots\cdots \end{pmatrix}, \cdots\cdots$$

分別表示 $\mathfrak{P}, \mathfrak{Q}, \cdots\cdots$ 之同態置換，因之 L 非有 (4) 之置換之積

$$(5)\qquad \begin{pmatrix} P_0 & P_1 & \cdots\cdots \\ P'_0 & P'_1 & \cdots\cdots \end{pmatrix}\begin{pmatrix} Q_0 & Q_1 & \cdots\cdots \\ Q'_0 & Q'_1 & \cdots\cdots \end{pmatrix}\cdots\cdots$$

以爲其因子不可也．即

$$L=\begin{pmatrix} P_0 & P_1 & \cdots\cdots \\ P'_0 & P'_1 & \cdots\cdots \end{pmatrix}\begin{pmatrix} Q_0 & Q_1 & \cdots\cdots \\ Q'_0 & Q'_1 & \cdots\cdots \end{pmatrix}\cdots\cdots\begin{pmatrix} P_i & Q_j & \cdots\cdots \\ P'_i & Q'_j & \cdots\cdots \end{pmatrix}\cdots\cdots$$

反之，若 (4) 表示 $\mathfrak{P}, \mathfrak{Q}, \cdots\cdots$ 之同態置換時，將 $\mathfrak{G}$ 之元素 $P_i Q_j \cdots\cdots$ 以 $P'_i Q'_j \cdots\cdots$ 置換之，由是乃得 $\mathfrak{G}$ 之同態置換，而此置換則有積 (5) 以爲其因子也．又 (5) 所表示之積之集合，乃 $\mathfrak{P}, \mathfrak{Q}, \cdots\cdots$ 之同態羣之直乘積．以故對於 $\mathfrak{G}$ 之同態置換 L，使 $\mathfrak{P}, \mathfrak{Q}, \cdots\cdots$ 之同態置換 (伴 L 而生者) 之積 (5) 相與對應，則 $\mathfrak{G}$ 之同態羣與 Sylow 氏約羣之同態羣之直乘積之間，一一對應遂成立也．由此對應，則兩羣之爲單純同態易知焉．

137. 巡回羣之同態羣.

α 元巡回羣

$$\mathfrak{A}:\quad 1, A, A^2, \cdots\cdots, A^{\alpha-1}\quad (A^\alpha=1)$$

之同態羣與關於一次母式 (α) 之母式合同羣爲單純同態．然就一次母式 $(\alpha), (\beta)$ 言，

$$(\alpha)(\beta)\equiv(\alpha\ \beta)\quad (\mathrm{mod.}\ (\alpha)).$$

故關於法 (α) 之一次母式之乘法，乃歸於關於法 α 之數之乘法也．是故 $\mathfrak{A}$ 之同態羣乃與關於 α 之乘法者之數之合同羣爲單純同態．而與不動同態對應者，則明與 1 相合同

(法 a) 焉. 今有一數 a, 就關於法 a 之乘法言, 須有其逆, 卽其適合

$$ax\equiv 1 \pmod{a}$$

者之數 x 須存在時, 則 a 對 a 之爲互素是所必要. 反之在此時 a 乃有其逆(法 a). 故若以

$$\rho_1, \rho_2, \cdots\cdots, \rho_\nu, \tag{1}$$

爲在 $0, 1, 2, \cdots\cdots, a-1$ 中對 a 爲互素之數, 則此諸數就關於 a 之乘法言, 成羣也(便宜上遂名之曰關於法 a 之數合同羣), 而此羣乃與 $\mathfrak{A}$ 之同態羣同型焉.* 而 $\mathfrak{A}$ 之同態置換, 則以

$$\begin{pmatrix} A \\ A^{\rho_i} \end{pmatrix} \quad (i=1, 2, \cdots\cdots, \nu) \tag{2}$$

與之.

其次乃求同態羣之元數. 試以 a 分解爲素因數, 而以之爲

$$a=p^m q^n \cdots\cdots. \tag{3}$$

於是其屬於 p 之 Sylow 氏約羣之同態羣, 乃與關於法 p^m 之數合同羣同型. 然

$$0, 1, 2, \cdots\cdots, p^m-1 \tag{4}$$

---

*(1) 之數對 a 爲互素; 反之, 對 a 互素之數任何個均與 (1) 之一數合同(法 a). 且 (1) 之任二數皆互爲非合同 (法 a). 具備此三條件之一組之數名曰關於法 a 之旣約系. 若用此術語, 則旣約系 (法 a) 者就關於同法之乘法言成羣也. 此羣卽名曰與 a 元巡回羣之同態羣爲同型焉.

之中對p^m爲互素者之數爲$p^{m-1}(p-1)$. 蓋以(4)中p之倍數爲

$$0, p, 2p, \cdots\cdots, (p^{m-1}-1)p$$

之p^{m-1}個故. 以故此Sylow氏約羣之同態羣之元數爲

$$p^{m-1}(p-1).$$

同樣其屬於q之Sylow氏約羣之元數爲$q^{n-1}(q-1)$. 因之由前節定理, a元巡回羣$\mathfrak{A}$之同態羣之元數爲

$$p^{m-1}(p-1)q^{m-1}(q-1)\cdots\cdots = a\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\cdots\cdots.$$

此數通常以$\varphi(a)$表之.

更檢Sylow氏約羣之同態羣之型, 當p爲奇數時, 乃以p^m之原根之一爲π, 則此之冪

$$1, \pi, \pi^2, \cdots\cdots, \pi^{\mu-1} \quad [\mu = p^{m-1}(p-1)]$$

作一關於p^m之既約系. 故關於法p^m之數合同羣, 因之則其屬於p之Sylow氏約羣之同態羣爲$\varphi(p^m)$元巡回羣也.

其次若$p=2, m=1$則$\varphi(2)=1$, 故二元巡回羣之同態羣爲主元素羣. $p=2, m=2$時, 既約系(法4)爲

$$1, 3 \pmod 4,$$

而$3^2 \equiv 1 \pmod 4$. 故四元巡回羣之同態羣爲二元巡回羣.

最後就$p=2, m \geqq 3$者一論. 屬於法2^m之最大指數爲

$$\frac{1}{2}\varphi(2^m) = 2^{m-2},$$

其以此爲指數者之一爲5. 而既約系(法2^m)得以

$$(-1)^x 5^y \pmod{2^m}, \begin{cases} x=0, 1 \\ y=0, 1, \cdots\cdots, 2^{m-2}-1 \end{cases}$$

與之(證略). 此諸數就關於法 2^m 之乘法言,形成一 $[1, m-2]$ 型之 Abel 氏羣甚明. 故屬於 2 之 Sylow 氏約羣爲 $[1, m-2]$ 型之 Abel 氏羣也.

第二十二章 素數冪元羣之型.四元數

138. 本章乃就以素數冪爲元數之羣中之特殊者,卽其有最大元數之巡回約羣之一爲正常者而論其羣之型焉. 請就其要用之定理始. 但全章中皆以 p 爲表奇素數者.

定理. 設 A, P 爲 p^m 元羣之元素,而令*

$$A^{p^\alpha}=1, \quad P^{-1}AP=A^\alpha.$$

於是

(i) $\alpha=1+kp^{a-c}$ $[k\not\equiv 0 \pmod{p}; a>c\geqq 0]$.

(ii) 除上之假設外,又 $P^{p^b}=A^{\lambda p^b}$ 時,則羣† $\{A, P\}$ 含有適合次之條件之元素 B.

---

*一般, $A^n=1$ 時,則此乃示 A 之巡回率爲 n 也.

†$\{A, P\}$ 者乃示由 A, P 之二元素而生成之羣者也. 而此羣之等於積 $\{P\}\{A\}$ 甚明.

$$B^{p^b}=1,\quad B^{-1}AB=A^{\alpha}\quad [\alpha=1+kp^{a-c};\ c\leqq b]$$

而

$$\{A, B\}=\{A, P\}.$$

(iii) 上之元素B得選擇之，使$a\geqq 2c$時則$\alpha=1+p^{a-c}$者.

證明. 與第101節(參照293頁腳註)中者同樣，由$P^{-1}AP=A^{\alpha}$，則得

$$P^{-x}A^{y}P^{x}=A^{y\alpha^{x}}. \tag{1}$$

(i) 作P之冪P, P^2, ……，則於此中其與A爲交換可能者必定存在.* 以其最低冪爲P^{β}，則β須爲p之冪也. 蓋若P^{hp^c} [$h\not\equiv 0 \pmod{p}$]與A爲交換可能，則P^{zhp^c}亦復同樣. 乃取適合

$$zh\equiv 1 \quad (法爲P之巡回率)$$

者以爲其z之值，則得$P^{zhp^c}=P^{p^c}$. 故β者p之冪也. 以之爲p^c. 而對之則有

$$P^{-p^c}AP^{p^c}=A. \tag{2}$$

然由(1)及假設

$$P^{-p^c}AP^{p^c}=A^{\alpha^{p^c}},\quad A^{p^a}=1.$$

故

$$\alpha^{p^c}\equiv 1 \pmod{p^a}. \tag{3}$$

然由Fermat氏定理.†

---

*P爲p^m元羣之元素，因之其巡回率爲p之冪也. 而主元素之與A爲交換可能是無論已. 故云.

†因$P^{-1}AP=A^{\alpha}$，故A^{α}與A非有同一之巡回率不可. 故α對p互素. 因之Fermat氏定理乃告成立.

$$a^{p^{a-1}(p-1)}\equiv 1 \pmod{p^a}.$$

故 p^c 須爲 $p^{a-1}(p-1)$ 之約數, 因之 $c<a$. 更由同定理,

$$a^p\equiv a \pmod{p},\ \text{因之}\ a^{p^c}\equiv a \pmod{p}.$$

故 $$a\equiv 1 \pmod{p}.$$

卽 $$a=1+kp^t \quad (k\not\equiv 0 \pmod{p},\ t\geqq 1).$$

爲決定此中 t 之值計, 乃將 a 而 p^c 方乘之, 則得

$$a^{p^c}=1+kp^{t+c}\left[1+\frac{p^c-1}{2}kp^t+\cdots\cdots\right].$$

故由(3),

(4) $$t+c\geqq a,$$

自他面觀, P 之 p^{c-1} 乘冪, 由上述, 乃不與 A 交換可能. 卽由(1),

$$\mathrm{A}^{a^{p^{c-1}}}=\mathrm{P}^{-p^{c-1}}\mathrm{A}\mathrm{P}^{p^{c-1}}\neq \mathrm{A}.$$

故 $$a^{p^{c-1}}\not\equiv 1 \pmod{p^a}.$$

然 $$a^{p^{c-1}}=1+kp^{t+c-1}\ [1+p\ \text{之倍數}].$$

故 $$t+c-1<a.$$

由此與(4)得 $$t=a-c.$$

而

(5) $$a=1+kp^{a-c}.$$

(ii) 茲計算屬於羣 $\{\mathrm{A},\mathrm{P}\}$ 之元素 PA^y 之冪. 由(1),

$$(\mathrm{PA}^y)^2=\mathrm{PA}^y\mathrm{PA}^y=\mathrm{PPA}^{y\alpha}\mathrm{A}^y=\mathrm{P}^2\mathrm{A}^{y(1+\alpha)},$$

$$(PA^y)^3=PA^yP^2A^{y(1+\alpha)}=PP^2A^{y\alpha^2}A^{y(1+\alpha)}=P^3A^{y(1+\alpha+\alpha^2)},$$

……

(6)　$$(PA^y)^n=\cdots\cdots=P^nA^{y(1+\alpha+\cdots\cdots+\alpha^{n-1})}.$$

以(5)之值代入α而計算右邊之指數,則得

$$1+\alpha+\cdots\cdots+\alpha^{n-1}=\frac{\alpha^n-1}{\alpha-1}=n+\binom{n}{2}kp^{a-c}+\cdots\cdots.$$

於此而令$n=p^b$,則右邊爲

$$p^b\left(1+\frac{p^b-1}{2}kp^{a-c}+\cdots\cdots\right)=p^b\mu\quad[\mu\not\equiv 0\ (\mathrm{mod.}\ p)].$$

因之由(6),

$$(PA^y)^{p^b}=P^{p^b}A^{\mu yp^b}$$

以故若$P^{p^b}=A^{\lambda p^b}$, 則

$$(PA^y)^{p^b}=A^{(\lambda+\mu y)p^b}.$$

於是乃取適合$\lambda+\mu y\equiv 0\pmod{p^{a-b}}$之$y$之值而令$PA^y=B$,則得

$$B^{p^b}=1.$$

而

(7)　$$B^{-1}AB=A^{-y}P^{-1}APA^y$$
$$=A^{-y}A^{\alpha}A^y=A^{\alpha}\quad(\alpha=1+kp^{a-c}).$$

且　$$\{A,P\}=\{A,B\}$$

甚明. 故得定理(ii).

於上,在$b\geqq a$時,則直取P以爲B可.

又因$P^{p^b}=A^{\lambda p^b}$,故$c\leqq b$是毋俟論.

(iii) 由 (7),

$$B^{-x}AB^{x}=A^{\alpha x} \qquad (\alpha=1+kp^{a-c}).$$

然 $a\geqq 2c$ 時,

$$\alpha^{x}=1+xkp^{a-c}+\binom{x}{2}k^{2}p^{2(a-c)}+\cdots\cdots\equiv 1+xkp^{a-c} \pmod{p^{a}}.$$

故若取適合 $xk\equiv 1 \pmod{p^{c}}$ 之 x 之值, 而令 $B^{x}=B_{1}$, 則得

$$B_{1}^{-1}AB_{1}=A^{1+p^{a-c}},$$

遂得定理 (iii).

系. $A^{p^{a}}=1$, $P^{-1}AP=A^{\alpha}$ 時, 則與 P 交換可能之 A 之最低羃之指數乃小於 p^{a}. 但 P 之巡回率亦以爲 p 之羃者.

證明. 由本定理,

$$\alpha=1+kp^{a-c} \quad [c<a].$$

故由 (1), 則

$$P^{-1}A^{p^{c}}P=A^{p^{c}(1+kp^{a-c})}=A^{p^{a}}$$

故也.

139. 含 p^{m-1} 元巡回羣之 p^{m} 元羣.

p^{m} 元羣含有 p^{m-1} 元巡回約羣時, 若在 Abel 氏羣, 則由前章此羣或爲巡回的, 或爲 $[m-1,1]$ 型. 反之, 若在非 Abel 氏羣時, 則爲次定理所示之型也.

定理. 凡含 p^{m-1} 元巡回約羣之 p^{m} 元非 Abel 氏羣 ($m>2$), 得以

$$A^{p^{m-1}}=1, \quad B^{p}=1, \quad B^{-1}AB=A^{1+p^{m-2}}$$

而定其義.

證明. 以A爲p^m元非Abel氏羣$\mathfrak{G}$之元素,其巡回率以爲p^{m-1}. 卽

$$A^{p^{m-1}}=1. \tag{1}$$

由第47節第二定理系1,巡回約羣$\{A\}$於$\mathfrak{G}$爲正常也. 故若取不屬於$\{A\}$之元素P,則得

$$P^{-1}AP=A^{\alpha}. \tag{2}$$

而P關於$\{A\}$之相對巡回率爲p. 卽

$$P^{p}=A^{\beta}.$$

蓋若P之相對巡回率小於p,則P不得不含於$\{A\}$;又若大於p,則羣$\{A, P\}$之元數超過$\mathfrak{G}$之元數p^m故也.

復次於上式中,其β必爲p之倍數也. 蓋苟不如是,則P之巡回率爲p^m,因之巡回羣$\{P\}$與$\mathfrak{G}$一致,是與$\mathfrak{G}$爲非Abel氏羣之假設相反故耳. 因之

$$P^{p}=A^{\lambda p}. \tag{3}$$

對上述(1), (2), (3)之關係而適用前節定理(iii),卽得本定理.

系. 若p^m元羣只有唯一個p^s元約羣$(s<m)$時,則其羣爲巡回的.

證明. 設$\mathfrak{G}$爲p^m元羣,$\mathfrak{H}$爲p^s元約羣,而$\mathfrak{G}$中之p^s元約羣又僅爲$\mathfrak{H}$者. 試取一不屬於$\mathfrak{H}$之元素P,則其巡回率不得在p^s以下. 蓋若P之巡回率小於p^s則由第47節第二定理,$\mathfrak{G}$非有含巡回羣$\{P\}$者之p^s元約羣不可,而此約羣

明與$\mathfrak{H}$異,因之與假設相反故也. 以P之巡回率爲$p^r(r\geqq s)$,則巡回羣$\{P^{p^{r-s}}\}$爲p^s元,因之由假設,不得不與$\mathfrak{H}$一致. 故$\mathfrak{H}$爲巡回羣.

其次,在含$\mathfrak{H}$者之巡回約羣中,以其元數最大者之一爲$\mathfrak{R}$,而$\mathfrak{R}$之元數爲p^t. 若$t<m$,則$\mathfrak{G}$定有含$\mathfrak{R}$之p^{t+1}元約羣(名之曰$\mathfrak{L}$). 而由本定理,則在$\mathfrak{L}$之元素中,其不屬於$\mathfrak{R}$且其巡回率等於p者非存在不可. 以此元素爲Q. 由第47節第二定理,則$\mathfrak{G}$又非有含巡回羣$\{Q\}$之p^s元約羣不可. 此約羣之與$\mathfrak{H}$異,是不待論. 此豈非與假設反而不合理者耶? 是則$t=m$爲必要,因而$\mathfrak{G}$爲巡回的也.

例. 含9元巡回約羣者之27元羣.

$$A=(012345678),\ B=(147)(285),\ B^{-1}AB=(048372615)=A^4.$$

140. 含p^{m-2}元巡回正常約羣者之p^m元羣.

設A爲p^m元非Abel氏羣$\mathfrak{G}$之元素,其巡回率爲p^{m-2},即

$$A^{p^{m-2}}=1, \tag{1}$$

而巡回約羣$\{A\}$則於$\mathfrak{G}$爲正常的. 但$\mathfrak{G}$則假設其爲無有p^{m-1}元巡回約羣者.

本節乃就商$\mathfrak{G}/\{A\}$爲巡回的時而討論$\mathfrak{G}$之型焉. 此時$\mathfrak{G}$非含有關於$\{A\}$之相對巡回率爲p^2者之元素不可以其一爲P,則

$$\mathfrak{G}=\{A\}+\{A\}P+\cdots\cdots+\{A\}P^{p^2-1}$$

甚明,但因 $\mathfrak{G}$ 不含巡回率爲 p^{m-1} 之元素,故

(2)　　$$P^{p^2}=A^{\lambda p^2}$$

爲必要也. 其次因 $\{A\}$ 於 $\mathfrak{G}$ 爲正常,故

(3)　　$$P^{-1}AP=A^{\alpha}.$$

由 (1), (2), (3) 之關係, $\mathfrak{G}$ 乃含適合次條件之元素 B 而 $\mathfrak{G}=\{A, B\}$ (前前節定理).

(4)　　$$B^{p^2}=1,\ B^{-1}AB=A^{\alpha}.$$

但　　$$\alpha=1+kp^{m-2-c},\ c\leqq 2,\ c<m-2.$$

由上之不等式以定 c 之值,則

$$m=4 \text{ 時},\quad c=0,\ 1;$$

$$m>4 \text{ 時},\quad c=0,\ 1,\ 2.$$

然 $c=0$, 則 B 與 A 交換可能,因之 $\mathfrak{G}$ 爲 Abel 氏羣,是與假定反. 故此值不能採用. $c=1$ 時,則 $m-2\geqq 2c$, 故由前前節定理 (iii) 得選擇元素 B 使 $k=1$ 也. 於是由之得定 $\mathfrak{G}$ 之義如次:

(5)　　$$A^{p^{m-2}}=1,\ B^{p^2}=1,\ B^{-1}AB=A^{1+p^{m-3}}.$$

復次 $c=2$ 時,若 $m-2\geqq 4$ 卽 $m\geqq 6$, 則由同定理 (iii), $\mathfrak{G}$ 得以

(6)　　$$A^{p^{m-2}}=1,\ B^{p^2}=1,\ B^{-1}AB=A^{1+p^{m-4}}$$

定其義也. 更就 $c=2$, $m=5$ 者而觀,由 (1), (4), 得

$$\mathfrak{G}:\quad A^{p^3}=1,\ B^{p^2}=1,\ B^{-1}AB=A^{\alpha},\ \alpha=1+kp.$$

而此時亦得選擇母元素 B 使 $k=1$ 也，因之遂成 (6) 之型焉．示之如下：

因 $$B^{-x}AB^{x}=A^{\alpha^{x}},$$

$$\alpha^{x}=(1+kp)^{x}\equiv 1+\left[xk+\frac{x(x-1)}{2}k^{2}p\right]p \pmod{p^{3}},$$

故若求其滿足

$$xk+\frac{x(x-1)}{2}k^{2}p\equiv 1 \pmod{p^{2}} \tag{7}$$

者之 x 之值，而以 B^{x} 代 B，且復改此名曰 B，則得

$$B^{-1}AB=A^{1+p}.$$

再次就合同式 (7) 之有根在者一論．先令

$$xk\equiv 1+yp \pmod{p^{2}}, \tag{8}$$

以之代入 (7)，得

$$1+yp+\frac{(1+yp)(1+yp-k)p}{2}\equiv 1 \pmod{p^{2}}.$$

簡約之，得

$$2y+1-k\equiv 0 \pmod{p}.$$

乃求適合此之 y 之值，以之代入 (8)，以求 x 之值，則此 x 滿足 (7) 式也．

更進而就 (5)，(6) 兩羣之不含 p^{m-1} 元巡回羣以及兩者之爲異型各點說明之．由 (5) 或 (6) 之第三式，

$$B^{-x}A^{y}B^{x}=A^{y\alpha^{x}} \quad (\alpha=1+p^{m-3},\ 1+p^{m-4}). \tag{9}$$

故與第 138 節中者同樣，

(10)　　$(B^xA^y)^n=B^{nx}A^{\mu}.$

但

$$\mu=1+\alpha^x+\cdots\cdots+\alpha^{(n-1)x}=\frac{\alpha^{nx}-1}{\alpha^x-1}.$$

然

$$(11)\quad \alpha^{rx}\equiv\begin{cases}1+rxp^{m-3} & (\alpha=1+p^{m-3}),\\ 1+rxp^{m-4} & (m>5;\ \alpha=1+p^{m-4}),\\ 1+rxp+\dfrac{1}{2}rx(rx-1)p^2 & (m=5;\ \alpha=1+p),\end{cases}$$

但此諸合同式均係就法 p^{m-2} 而取之者. 故若令 $n=p^{m-2}$, 則得

$$\mu\equiv 0 \pmod{p^{m-2}},$$

因之 B^xA^y 之 p^{m-2} 乘冪乃與1等. 卽羣之元素之巡回率不得超過 p^{m-2} 也.

其次 $\alpha=1+p^{m-3}$ 時, 若令 $n=p$, 則得

$$\mu\equiv p \pmod{p^{m-2}},$$

由(10), 又得

(12)　　$(B^xA^y)^p=B^{px}A^{py}.$

然由(9)及(11),

$$B^{-1}A^pB=A^{p\alpha}=A^p,\ B^{-p}AB^p=A^{\alpha^p}=A,$$

卽 A^p, B^p 於羣爲自己共軛也. 故由(12), 羣之元素之 p 乘冪皆自己共軛. 反之, 在 $\alpha=1+p^{m-4}$ 時, 由(6)之第三式

$$B^{-1}A^pB=A^{p(1+p^{m-4})}\neq A^p,$$

卽羣(6)之元素中, 其 p 乘冪不爲自己共軛者乃存在也. 是

故(6)不得定義之爲與(5)同型之羣焉.

141. 再就商$\mathfrak{G}/\{A\}$之不爲巡回的者一論以作前節之續. 試取含巡回羣$\{A\}$之p^{m-1}元約羣,而名之曰$\mathfrak{H}$. 若$\mathfrak{H}$爲Abel氏羣,則其型爲$[m-2,1]$. 卽得以

$$A^{p^{m-2}}=1,\quad B^p=1,\quad B^{-1}AB=A \tag{13}$$

定其義也. 若在非Abel氏羣時,則其型由第139節定理爲

$$A^{p^{m-2}}=1,\quad B^p=1,\quad B^{-1}AB=A^{1+p^{m-3}} \tag{14}$$

次取不屬於$\mathfrak{H}$之元素P,因p^2元羣$\mathfrak{G}/\{A\}$爲非巡回的,故P關於$\{A\}$之相對巡回率不得不爲p也. 以故羣$\{A,P\}$之元數爲p^{m-1}.* 以此羣名曰$\mathfrak{K}$,則$\mathfrak{K}$與於$\mathfrak{H}$者全然同樣,非屬於次記二型之一不可.

$$A^{p^{m-2}}=1,\quad C^p=1,\quad C^{-1}AC=A \tag{15}$$

$$A^{p^{m-2}}=1,\quad C^p=1,\quad C^{-1}AC=A^{1+p^{m-3}} \tag{16}$$

於此因$\{A,C\}=\mathfrak{K}=\{A,P\}$,故元素C之不得屬於$\mathfrak{H}$是不待論. 因之

$$\{A,B,C\}=\mathfrak{G}$$

甚明. [因$\{A,B\}$卽$\mathfrak{H}$爲p^{m-1}元,而C又不屬於$\mathfrak{H}$故.] 然A,B之關係得以(13)或(14)與之;而A,C之關係則得以(15)或(16)與之. 故若知B與C間之關係,則$\mathfrak{G}$之型由之而得明也. 茲分下三段說明之. 但假定$m\geqq 4$者.

---

*因$\{A\}$於$\mathfrak{G}$爲正常,故$\{A,P\}=\{A\}+\{A\}P+\cdots\cdots+\{A\}P^{p-1}$.

1°. A, B之關係爲(13), A, C之關係爲(15)時.

因商$\mathfrak{G}/\{A\}$爲Abel氏羣, 故$\{A\}$必含$\mathfrak{G}$之換位羣(第42節第二定理). 故二元素B, C之換位元素爲A之冪. 卽

(17). $$C^{-1}BC=BA^{\alpha}.$$

將此兩邊p方乘之得

$$C^{-1}B^{p}C=B^{p}A^{\alpha p} \quad [\text{爲A, B交換可能故}].$$

然$B^{p}=1$. 故$A^{\alpha p}=1$. 因之

$$\alpha p\equiv 0 \pmod{p^{m-2}}.$$

卽 $$\alpha=\lambda p^{m-3} \quad [\because m>3].$$

若$\lambda\equiv 0 \pmod{p}$, 則由(17)式B與C爲交換可能, 因之$\mathfrak{G}$爲Abel氏羣. 此則與假設相反者也. 故省之; 而僅取$\lambda\not\equiv 0 \pmod{p}$者. 今以$A^{\lambda}$代A, 而更改此名曰A, 則由(13), (15)以及(17), 遂得

(18)
$$\begin{cases} A^{p^{m-2}}=1, & B^{p}=1, \quad C^{p}=1, \\ B^{-1}AB=A, & C^{-1}AC=A, \quad C^{-1}BC=BA^{p^{m-3}}, \end{cases}$$

而以此得定$\mathfrak{G}$之義.

2°. A, B之關係爲(13); A, C之關係爲(16)時.

因$\{A\}$含換位羣, 故與前同樣,

$$C^{-1}BC=BA^{\alpha}, \quad \alpha=\lambda p^{m-3}.$$

由本式以及(16),

$$C^{-1}(BA^{-\lambda})C=C^{-1}BC\cdot C^{-1}A^{-\lambda}C=BA^{-\lambda}$$

卽 $BA^{-\lambda}$ 爲自己共軛也. 而 $\lambda \not\equiv 0 \pmod{p}$ 時, 此元素之巡回率, 由(13)自明爲 p^{m-2}. 故此時以 $BA^{-\lambda}$ 代 A, 則因此元素與 B 及 C 爲交換可能之故, ㊂得歸於1°也. 於是若㊂須與前款者爲異型, 則 $\lambda \equiv 0 \pmod{p}$ 爲必要. 卽 C 與 B 爲交換可能, 而由(13), (16), ㊂遂得定義之如次:

$$(19)\quad \begin{cases} A^{p^{m-2}}=1, \quad B^{p}=1, \quad C^{p}=1, \\ B^{-1}AB=A, \quad C^{-1}AC=A^{1+p^{m-3}}, \quad C^{-1}BA=B \end{cases}$$

於此所得之羣是否與前者(18)爲異型, 試討論之.

由上之關係,

$$C^{-1}A^{p}C=A^{p(1+p^{m-3})}=A^{p}.$$

故 A^{p}, B, C 互爲交換可能. 因之 $A^{px}B^{y}C^{z}$ 之 p^{m-3} 乘冪乃與1等. 以故若羣(19)之元素 $A^{x}B^{y}C^{z}$ 之巡回率須爲 p^{m-2}, 則 $x \not\equiv 0 \pmod{p}$ 爲必要, 而對之乃有

$$C^{-1}(A^{x}B^{y}C^{z})C=A^{x(1+p^{m-3})}B^{y}C^{z} \not= A^{x}B^{y}C^{z}.$$

卽巡回率 p^{m-2} 之元素於羣(19)非自己共軛. 反之, 羣(18)則有巡回率爲 p^{m-2} 之自己共軛元素. 故(18), (19)兩羣不得爲同型也.

3°. A, B 之關係爲(14), A, C 之關係爲(15)時, 則將 B 與 C 交換便歸於2°款. 其次若以 A, B 之關係爲(14), A, C 之關係爲(16), 卽

$$B^{-1}AB=A^{1+p^{m-3}}, \quad C^{-1}AC=A^{1+p^{m-3}},$$

則得

$$(BC^{-1})^{-1}A(BC^{-1})=CB^{-1}ABC^{-1}=CA^{1+p^{m-3}}C^{-1}=A.$$

故若以 $\{A, BC^{-1}\}$ 代 $\{A, B\}$ 而爲約羣 $\mathfrak{H}$, 則此遂爲 $[m-1, 1]$ 型之 Abel 氏羣卽 (13) 之型也. 若將此 $\mathfrak{H}$ 與羣 (16) 組合之則歸於 2° 款.

綜合本節及前節之事項, 遂得次

定理. 凡有 p^{m-2} 元巡回正常約羣者之 p^m 元非 Abel 氏羣之型, 乃爲次之四種: (但假定其不含有 p^{m-1} 元巡回羣者.)

(i) $A^{p^{m-2}}=1, \quad B^{p^2}=1, \quad B^{-1}AB=A^{1+p^{m-3}};$

(ii) $A^{p^{m-2}}=1, \quad B^{p^2}=1, \quad B^{-1}AB=A^{1+p^{m-4}};$

(iii) $$\begin{cases} A^{p^{m-2}}=1, & B^p=1, & C^p=1, \\ B^{-1}AB=A, & C^{-1}AC=A, & C^{-1}BC=BA^{p^{m-3}}; \end{cases}$$

(iv) $$\begin{cases} A^{p^{m-2}}=1, & B^p=1, & C^p=1, \\ B^{-1}AB=A, & C^{-1}AC=A^{1+p^{m-3}}, & C^{-1}BC=B. \end{cases}$$

注意. 由前節及本節之記述, 可知對於 $m>4$, 雖可得定理中之四型, 而 $m=4$ 時, 則 (ii) 之型不得生也. 至 $m=3$ 時, 則 p^3 元非 Abel 氏羣 $\mathfrak{G}$ 或有 p^2 元之巡回約羣, 或則無有. 以前者論, 由第 139 節定理, 則

$$\mathfrak{G}: \quad A^{p^2}=1, \quad B^p=1, \quad B^{-1}AB=A^{1+p}.$$

以後者論, 乃取 $\mathfrak{G}$ 之自己共軛元素 A, 而與本節同樣, 就含 $\{A\}$ 之 p^2 元約羣 $\mathfrak{H}$ 及 $\mathfrak{K}$ 討論之. 此時

$$\mathfrak{H}: \quad A^p=1, \ B^p=1, \ B^{-1}AB=A;$$

$$\mathfrak{K}: \quad A^p=1, \ C^p=1, \ C^{-1}AC=A.$$

而 B 與 C 之關係，與本節 1° 中同樣爲

$$C^{-1}BC=BA^{\alpha}, \quad \alpha\not\equiv 0 \pmod{p}.$$

$\alpha\not\equiv 1 \pmod{p}$ 時，乃以 A^{α} 代 A，而改此名曰 A，則 $\mathfrak{G}$ 得以三元素 A, B, C 而定義如次：

$$\begin{cases} A^p=1, & B^p=1, & C^p=1, \\ B^{-1}AB=A, & C^{-1}AC=A, & C^{-1}BC=BA \end{cases}$$

其故 p^3 元非 Abel 氏羣僅有在此所得之二型也.

142. 2^m **元羣.**

就 2^m 元羣之型言，則茲僅論其有 2^{m-1} 元巡回約羣者而止.* 設 A 爲 2^m 元非 Abel 氏羣 $\mathfrak{G}$ 之元素,† 其巡回率爲 2^{m-1}. 卽

$$A^{2^{m-1}}=1. \tag{1}$$

若取一不屬於巡回約羣 $\{A\}$ 之元素 P，則與第 139 節中者同樣得

---

*若讀者欲進而知關於素數冪元羣穉種之型，則請讀下記雜誌所載之論文可.

Miller, Trans. Amer. Math. Soc. 2, 3, 6.

Neikirk, Trans. Amer. Math. Soc. 6.

Sono, Mem. Col. Sci. and Eng. Kyoto Imp. Univ. 5.

†因 $\mathfrak{G}$ 爲非 Abel 氏羣，故 $m>2$.

(2)　　$P^{-1}AP=A^{\alpha}$,　$P^{2}=A^{2\lambda}$.

顧此第二關係,而將第一式之兩邊再用P而變其形得

$$A=A^{\alpha^2}.$$

因之

(3)　　$\alpha^{2}\equiv 1 \pmod{2^{m-1}}$

爲必要也. 欲決定適合此式之α之值,乃將本式換書爲

$$(\alpha-1)(\alpha+1)\equiv 0 \pmod{2^{m-1}}.$$

$m>3$時,由此式得

$$\frac{\alpha-1}{2}\cdot\frac{\alpha+1}{2}\equiv 0 \pmod{2^{m-3}}.$$

然左邊因數之差爲1. 故非因數之一方爲奇數他方爲偶數不可也. 因之爲上式之成立計,則須

$$\frac{\alpha-1}{2}\equiv 0 \pmod{2^{m-3}},\text{ 因之 }\alpha=1+k2^{m-2},$$

或

$$\frac{\alpha+1}{2}\equiv 0 \pmod{2^{m-3}},\text{ 因之 }\alpha=-1+k2^{m-2}.$$

故

(4)　　$\alpha\equiv\pm 1,\ \pm 1+2^{m-2} \pmod{2^{m-1}}$.

此中$\alpha=1$者不能採用(因$\mathfrak{G}$爲非Abel氏羣故). 又$m=3$時,則僅有

(5)　　$\alpha\equiv -1 \pmod{4}$

甚明.

1°.　　$\alpha\equiv -1 \pmod{2^{m-1}}$ 時 $(m\geqq 3)$.

此時(2)之第一式爲

(6) $$P^{-1}AP=A^{-1}.$$

將兩邊 2λ 方乘之,

$$P^{-1}A^{2\lambda}P=A^{-2\lambda}.$$

於此而用(2)之第二關係, 則左邊等於 $A^{2\lambda}$. 故

$$A^{2\lambda}=A^{-2\lambda}. \quad \therefore \quad A^{4\lambda}=1.$$

$$\therefore \quad 4\lambda\equiv 0 \pmod{2^{m-1}}. \quad \therefore \quad 2\lambda\equiv 0 \pmod{2^{m-2}}.$$

$$\therefore \quad 2\lambda\equiv 0,\ 2^{m-2} \pmod{2^{m-1}}.$$

以此 λ 之值代入(2)之第二式, 則對於 $\mathfrak{G}$ 之構成, 便有次之二種情形出現. 卽

(7) $$A^{2^{m-1}}=1,\ P^2=1,\ P^{-1}AP=A^{-1};$$

(8) $$A^{2^{m-1}}=1,\ P^2=A^{2^{m-2}},\ P^{-1}AP=A^{-1}.$$

由此關係所定之兩羣, 如次所示, 乃有相異之型者焉.

就 $\{A\}$ 而分爲傍系, 則兩羣共爲 $\{A\}+P\{A\}$. 將屬於傍系 $P\{A\}$ 之元素 PA^y 自乘, 得

$$(PA^y)^2=PA^yPA^y=P^2.$$

故 PA^y 之巡回率就(7)言爲 2 也. 因之該羣乃含有巡回率 2 之元素 $2^{m-1}+1$ 個(屬於傍系 $P\{A\}$ 之元素並 $A^{2^{m-2}}$). 於羣(8), PA^y 之巡回率爲 4. 故羣(8)中巡回率 2 之元素僅爲 $A^{2^{m-2}}$. 因之(7), (8)兩羣不得爲同態也.

2°. $\alpha\equiv 1+2^{m-2} \pmod{2^{m-1}}$ 時 $(m>3)$.

將傍系 $P\{A\}$ 之元素 PA^y 自乘, 則由(2).

$$(PA^y)^2=P^2A^{y(1+\alpha)}=A^{2\lambda+y(1+\alpha)},$$

而

$$2\lambda+y(1+\alpha)\equiv 2\{\lambda+y(1+2^{m-3})\} \pmod{2^{m-1}}.$$

故對於適合

$$\lambda+y(1+2^{m-3})\equiv 0 \pmod{2^{m-2}}$$

之 y 之值, 則得

$$(PA^y)^2=1.$$

而

$$(PA^y)^{-1}A(PA^y)=A^{1+2^{m-2}}.$$

故若令 $PA^y=B$, 則 $\mathfrak{G}$ 得以

$$(9)\qquad A^{2^{m-1}}=1,\ B^2=1,\ B^{-1}AB=A^{1+2^{m-2}}$$

定其義也.

3°. $\alpha\equiv -1+2^{m-2} \pmod{2^{m-1}}$ 時 $(m>3)$.

此時由 (2) 之第一式,

$$P^{-1}A^{2\lambda}P=A^{2\lambda\alpha}=P^{-2\lambda}.$$

故與 1° 同樣,

$$(10)\qquad 2\lambda\equiv 0 \pmod{2^{m-2}}$$

爲必要也. 而

$$(PA^y)^2=A^{2\lambda+y(1+\alpha)}=A^{2\lambda+y2^{m-2}}.$$

於此而取適合於 $2\lambda+y2^{m-2}\equiv 0 \pmod{2^{m-1}}$ 之 y 之值 (由 (10) 常爲可能), 則得

$$(PA^y)^2=1,\ (PA^y)^{-1}A(PA^y)=A^{-1+2^{m-2}}.$$

故若令 $PA^y=B$, 則 $\mathfrak{G}$ 爲次型:

$$(11)\qquad A^{2^{m-1}}=1,\ B^2=1,\ B^{-1}AB=A^{-1+2^{m-2}}.$$

綜合上述,得次

定理. 凡有2^{m-1}元巡回約羣者之2^m元非 Abel 氏羣,乃爲以(7),(8),(9),(11)分別所定義之四種. 但$m=3$時,則只限於(7),(8)兩種.

例 1. 令 $A=(abcd)$, $B=(bd)$, 則

$$A^4=1,\ B^2=1,\ B^{-1}AB=(adcb)=A^{-1},$$

遂得有(7)型之四次可遷羣$\{A, B\}$焉. 而其置換則爲

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

此卽四次對稱羣之 Sylow 氏約羣也. 因之其得表之爲四次置換羣之8元羣皆爲同型.

例 2. 令 $A=(abcd)(efgh)$, 而 B 則取之如次,遂得分別爲(7),(8)兩型之8元羣.

(i) $$B=(ah)(bg)(cf)(de),$$
$$B^2=1,\ B^{-1}AB=(hgfe)(dcba)=A^{-1};$$

(ii) $$B=(aecg)(bhdf),$$
$$B^2=(ac)(eg)(bd)(hf)=A^2,\ B^{-1}AB=(ehgf)(cbad)=A^{-1}.$$

例 3. 令 $A=(01234567)$, 而 B 則取之如次,遂得分別爲(9),(11)兩型之16元羣.

(i) $$B=(15)(37),$$
$$B^2=1,\quad B^{-1}AB=(05274163)=A^5;$$

(ii)　　$B=(13)(26)(57),$

$$B^2=1,\quad B^{-1}AB=(03614725)=A^3.$$

系. 2^m 元羣僅含唯一之 2^s 元約羣 ($s>1$) 時，則此羣爲巡回的.

證明. 設 2^m 元羣 $\mathfrak{G}$ 爲僅含唯一個 2^s 元約羣 $\mathfrak{H}$ 者. 於是與第139節系中同樣，$\mathfrak{H}$ 不得不爲巡回羣也. 在含 $\mathfrak{H}$ 者之巡回約羣中，以其元數之最大者爲 $\{T\}$，T 之巡回率爲 2^t. 若 $t<m$，則 $\mathfrak{G}$ 定有含 $\{T\}$ 之 2^{t+1} 元約羣(名之曰 $\mathfrak{L}$)也. $\mathfrak{L}$ 之型，乃本定理所示之四種. 若爲(7), (9), (11)之一，則與第139節系中同樣，產生矛盾而不合理. 若 $\mathfrak{L}$ 爲(8)型，卽

$$T^{2^t}=1\quad U^2=T^{2^{t-1}},\quad U^{-1}TU=T^{-1},$$

$$(t+1\geqq s+1\geqq 3),$$

則屬於傍系 $U\{T\}$ 者之元素 UT 之巡回率如前所述爲4也. 而4元巡回羣 $\{UT\}$ 不含於 $\{T\}$，因之其不含於 $\mathfrak{H}$，是不俟論. 於是含 $\{UT\}$ 之 2^s 元約羣與 $\mathfrak{H}$ 異，此乃違反假設之結果. 故不得 $t<m$ 也. 卽須 $\{T\}=\mathfrak{G}$. 故本系云云.

注意. 2^m 元羣僅含唯一個2元約羣時，則或爲巡回的，或有(8)型.

143. 四元數，四元數羣.

羣之元數爲8時，則前節定理四羣中之(8)爲

(1)　　$A^4=1,\quad B^2=A^2,\quad B^{-1}AB=A^{-1},$

而其元素則得以

(2) $1, A, A^2, A^3, B, AB, A^2B, A^3B$

與之. 與此羣同型者總稱曰**四元數羣**焉.

變更元素之記號, 將 A, B, AB, A^2 分別表以 $i, j, k, -1$, 則由(1)得次之關係:*

$$(3)\qquad \begin{cases} i^2=j^2=k^2=-1, \quad (-1)^2=1, \\ ij=k=-ji, \quad jk=i=-kj, \quad ki=j=-ik; \end{cases}$$

而(2)之元素遂分別得換書如次:

$$(4)\qquad 1, i, -1, -i, j, k, -j, -k.$$

今 a, b, c, d 爲正負之實數時試就以 $d+ai+bj+ck$ 所表者而究之. 乃將此視爲一種之數, 再留意關係(3)而與普通之多項式同樣處理之可. 卽若令

$$(5)\qquad q=d+ai+bj+ck, \quad q'=d'+a'i+b'j+c'k$$

時, 則

$$(6)\qquad q\pm q'=(d\pm d')+(a\pm a')i+(b\pm b')j+(c\pm c')k,$$

$$(7)\qquad \begin{aligned} qq'=&dd'+da'i+db'j+dc'k \\ &+ad'i+aa'i^2+ab'ij+ac'ik \\ &+bd'j+ba'ji+bb'j^2+bc'jk \\ &+cd'k+ca'ki+cb'kj+cc'k^2 \\ =&d''+a''i+b''j+c''k. \end{aligned}$$

---

* $(-1)i=-i$, 其他準此.

但

$$(8)\quad \begin{cases} d''=dd'-aa'-bb'-cc', & a''=da'+ad'+bc'-cb', \\ b''=db'+bd'+ca'-ac', & c''=dc'+cd'+ab'-ba'. \end{cases}$$

由此擴張所得之數稱曰Hamilton氏**四元數**. 上記之羣(4), 乃由四元數之構成要素i, j, k之乘法而生成者也. 以故以四元數羣之名與之焉.

於四元數$d+ai+bj+ck$, 其$\sqrt{d^2+a^2+b^2+c^2}$名曰**其絶對值**或曰**伸縮率**,* 以$|d+ai+bj+ck|$表之. 其絶對值等於1者, 特名曰**單位四元數**.

由(8)易知

$$(9)\quad d''^2+a''^2+b''^2+c''^2=(d^2+a^2+b^2+c^2)(d'^2+a'^2+b'^2+c'^2),$$

卽二數之積之絶對值等於各數之絶對值之積也.

又若以

$$\bar{q}=\frac{d-ai-bj-ck}{d^2+a^2+b^2+c^2},$$

則由(7)及(8)卽得

$$q\bar{q}=\bar{q}q=1.$$

若是凡不爲零者之四元數常有其逆數.

又四元數之乘法, 如(3)所示, 不服從交換法則者也. 但組合法則之成立, 則用(7)易得而證明之.

144. 四元數與二次毋式之關係.

---

*伸縮率一語乃關連向量(vector)與四元數之乘法而生.

單位四元數之積復爲單位四元數，此由前節(9)而易知者也. 而 $d+ai+bj+ck$ 爲單位四元數時，則由同節所述，得

$$(d+ai+bj+ck)(d-ai-bj-ck)=1.$$

故單位四元數關於乘法乃成羣焉. 然含於此之羣中，其有限者果有何型乎? 欲解決此問題，則利用其與二次母式之關係爲便利也. 今對四元數

$$q=d+ai+bj+ck,$$

使二次母式

$$\mathrm{Q}=\begin{pmatrix} d+a\sqrt{-1} & c-b\sqrt{-1} \\ -c-b\sqrt{-1} & d-a\sqrt{-1} \end{pmatrix}$$

相與對應. 於是對於四元數之積，則是種母式之積相與對應也. 蓋用前節(8)之記號，令

$$\begin{aligned} qq' &=(d+ai+bj+ck)(d'+a'i+b'j+c'k) \\ &=d''+a''i+b''j+c''k, \end{aligned}$$

則與 q, q' 對應之母式之積爲

$$\begin{aligned} \mathrm{QQ}' &=\begin{pmatrix} d+a\sqrt{-1} & c-b\sqrt{-1} \\ -c-b\sqrt{-1} & d-a\sqrt{-1} \end{pmatrix}\begin{pmatrix} d'+a'\sqrt{-1} & c'-b'\sqrt{-1} \\ -c'-b'\sqrt{-1} & d'-a'\sqrt{-1} \end{pmatrix} \\ &=\begin{pmatrix} d''+a''\sqrt{-1} & c''-b''\sqrt{-1} \\ -c''-b''\sqrt{-1} & d''-a''\sqrt{-1} \end{pmatrix}, \end{aligned}$$

而此母式則與四元數 $d''+a''i+b''j+c''k$ 相對應故耳.

母式 Q 之行列式爲 $d^2+a^2+b^2+c^2$. 而此值之等於1者，則特名之曰 **Cayley 形之母式**. 然 $d^2+a^2+b^2+c^2$ 乃四元數

q之絕對值之平方. 故由上記之對應得次定理.

定理. 單位四元數關於乘法所作之羣,與Cayley形母式羣爲單純同態.

例. 與四元數羣

$$\pm 1,\quad \pm i,\quad \pm j,\quad \pm k$$

相對應之母式羣如次:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \begin{pmatrix}\sqrt{-1}&0\\0&-\sqrt{-1}\end{pmatrix},\ \begin{pmatrix}0&-\sqrt{-1}\\-\sqrt{-1}&0\end{pmatrix},\ \begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

$$\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\ \begin{pmatrix}-\sqrt{-1}&0\\0&\sqrt{-1}\end{pmatrix},\ \begin{pmatrix}0&\sqrt{-1}\\\sqrt{-1}&0\end{pmatrix},\ \begin{pmatrix}0&-1\\1&0\end{pmatrix}.$$

至Cayley形母式果作如何有限羣,則俟後說之(第156節);本節不過示四元數與二次母式之關係而已.

145. Hamilton氏羣.

由第143節(4),可知四元數羣中之2元約羣僅爲$\{-1\}$;而四元約羣則爲$\{i\}$, $\{j\}$, $\{k\}$之三,甚明. 而此諸約羣皆爲正常的. 一般,其約羣皆爲正常者之非Abel氏羣,依Dedekind氏之命名,總稱之曰**Hamilton氏羣**焉.

定理. Hamilton氏羣,乃四元數羣,$[1,1,\cdots\cdots 1]$型之2^m元Abel氏羣以及奇數元Abel氏羣之直乘積.

證明. 下分四段論之.

1°. 設$\mathfrak{G}$爲一Hamilton氏羣. 乃取$\mathfrak{G}$中兩Sylow氏約羣(屬於異素數者)$\mathfrak{H}$及$\mathfrak{K}$,由Hamilton氏羣之定義,則$\mathfrak{H}$與

$\mathfrak{R}$之各元素爲交換可能,$\mathfrak{R}$與$\mathfrak{H}$之各元素亦交換可能. 然兩約羣乃屬於相異素數者,故除主元素以外無共通之元素. 因之$\mathfrak{H}$之各元素與$\mathfrak{R}$之各元素不得不爲交換可能也(第27節第四定理). 故$\mathfrak{G}$爲此Sylow氏約羣之直乘積.

2°. 令$\mathfrak{H}$爲屬於奇素數p之Sylow氏約羣($\mathfrak{G}$的). 若$\mathfrak{H}$非爲Abel氏羣,則此必含非自己共軛之元素. 乃取其中巡回率之最高者,以之爲A,而其巡回率爲p^a. 卽

$$A^{p^a}=1. \tag{1}$$

又取不與A交換可能之元素P($\mathfrak{H}$的),以P關於{A}之相對巡回率爲p^b,則

$$P^{p^b}=A^{\lambda p^b} \tag{2}$$

爲必要. (否則非自己共軛元素P之巡回率較p^a爲大,是不合理.) 而{A}由Hamilton氏羣之定義,於$\mathfrak{G}$爲正常的. 因之得

$$P^{-1}AP=A^{\alpha},\quad \alpha\not\equiv 1 \pmod{p^a}. \tag{3}$$

由(1), (2), (3)之關係,巡回羣之積{P}{A}作p^{a+b}元之非Abel氏羣. 然此羣,依第138節定理,乃由A及適合次條件之元素B所生成.

$$B^{p^b}=1,\quad B^{-1}AB=A^{\alpha}. \tag{4}$$

而{A, B}卽{A, P}之元數爲p^{a+b},故兩巡回羣{A}及{B}除主元素外無有共通之元素也.

復自他面言,{B}爲$\mathfrak{G}$之正常約羣(由Hamilton氏羣之

定義). 故{B}與元素A爲交換可能. 於是{A},{B}之各羣乃與他羣之元素爲交換可能,且其共通元素僅爲主元素. 因之A與B不得不交換可能也(第27節第四定理). 此乃與(4)之第二關係矛盾. 此矛盾,係由假定非自己共軛元素存在於$\mathfrak{H}$所生之結果. 是則$\mathfrak{H}$非爲Abel氏羣不可也.

3.° 令$\mathfrak{R}$爲屬於素數2之Sylow氏約羣($\mathfrak{G}$的),且以之爲非Abel氏羣. 乃於$\mathfrak{R}$,在其非自己共軛元素中,取其巡回率最高者之S而以其巡回率爲2^s.* 於是$\mathfrak{R}$之元素之中,其與S雖非交換可能,然其自乘與S爲交換可能者定存在也.† 以其一爲T,則得

$$T^{-2}ST^2=S. \tag{5}$$

若以T關於{S}之相對巡回率爲2^t,則與2° 中者同樣,得

$$T^{2^t}=S^{\lambda 2^t} \quad (t\leqq s). \tag{6}$$

又因{S}於$\mathfrak{R}$爲正常,故

$$T^{-1}ST=S^{\alpha}, \quad \alpha\not\equiv 1 \pmod{2^s}. \tag{7}$$

將此式之兩邊再以T變形,則得

$$T^{-2}ST^2=S^{\alpha^2}.$$

由此與(5),

---

*由Hamilton氏羣之定義{S}於$\mathfrak{G}$爲正常. 故若$s=1$,則S與$\mathfrak{G}$之各元素爲交換可能. 是與假設反. 故非$s>1$不可也.

†若元素U不與S爲交換可能,而其2^u乘冪始與S爲交換可能,則取U之2^{u-1}乘冪可也.

$$a^2 \equiv 1 \pmod{2^s}.$$

故與第142節同樣,

$$a \equiv \pm 1,\ \pm 1 + 2^{s-1} \pmod{2^s}.$$

但 $s=2$ 時, $a \equiv \pm 1 \pmod 4$. 又此諸值之中,其 $a \equiv 1$ 者由(7)乃棄之.

(i) $a \equiv 1 + 2^{s-1} \pmod{2^s}$ 時 $(s>2)$.

由(7),

$$(TS^y)^2 = T^2 S^{y(1+\alpha)}$$

利用(5)而將此 2^{t-1} 方乘之,則

$$(TS^y)^{2^t} = T^{2^t} S^{y(1+\alpha)2^{t-1}}$$

$$= S^{[2\lambda + y(1+\alpha)]2^{t-1}} \quad [\text{由 (6)}].$$

然 $$1 + \alpha \equiv 2 \not\equiv 0 \pmod 4.$$

故適合 $$2\lambda + y(1+\alpha) \equiv 0 \pmod{2^s}.$$

者之 y 之整數值存在,而對此值則

$$(TS^y)^{2^t} = 1.$$

故若令 $TS^y = R$, 則

$$R^{2^t} = 1, \quad R^{-1} S R = S^{\alpha},$$

而 $\{S, R\} = \{S, T\}$. 由此,與 2° 中全然同樣, S 須與 R 爲交換可能,因之 S 與 T 亦交換可能,乃生與(7)式矛盾之結果. 故不能 $a \equiv 1 + 2^{s-1} \pmod{2^s}$.

(ii) $a \equiv -1, -1 + 2^{s-1} \pmod{2^s}$ 時.

由 Hamilton 氏羣之定義, $\{T\}$ 於 $\mathfrak{R}$ 亦爲正常的. 故

$$S^{-1}TS\equiv T^{\beta}.$$

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

然由(7)　　$T^{-1}S^{-1}TS=S^{1-\alpha}.$

故　　$S^{1-\alpha}=T^{\beta-1}.$

然　　$1-\alpha\equiv 2,\ 2(1-2^{s-2})\pmod{2^s}.$

因之以前者言　　$S^2=T^{\beta-1},$

以後者論，乃取適合

$$(1-2^{s-2})x\equiv 1\pmod{2^{s-1}}$$

者之整數 x，則得

$$S^2=T^{x(\beta-1)}.$$

是無論如何，皆

$$S^2=T^{\mu}.$$

故　　$T^{-1}S^2T=T^{-1}T^{\mu}T=T^{\mu}=S^2.$

然以(7)之兩邊自乘，則

$$T^{-1}S^2T=S^{2\alpha}=S^{-2}\quad[\because\ \alpha\equiv -1,\ -1+2^{s-1}].$$

故　　$S^2=S^{-2}$，因之 $S^4=1$，

即S之巡回率爲4或爲2也．若爲2，則羣$\{S, T\}$爲4元，因之則須爲Abel氏羣．是違反T與S非爲交換可能之假定而不合理也．故S之巡回率不得不爲4焉．因此之故，則只有

$$\alpha\equiv -1\pmod{4}.$$

(因如前述，$\alpha\equiv -1+2^{s-1}$者僅限於$s>2$時故．)故

(8) $$T^{-1}ST=S^{-1}.$$

復次，因S之巡回率爲4，即於(6)，$s=2$，故 t 爲1或2. 若 $t=2$，則二羣 $\{S\}$，$\{T\}$ 除主元素外，不得有共通元素. 然此二者之各個皆與他個之元素爲交換可能. 故S與T不得不交換可能. 是與假定反而不合理. 因之 $t=1$ 爲必要，而(6)遂爲

$$T^2=S^{2\lambda}.$$

於此，若 λ 爲偶數則 $T^2=1$，乃與前同樣，便生S與T爲交換可能之結果而不合理. 故 λ 爲奇數，而上式非爲

(9) $$T^2=S^2$$

不可也($S^4=1$ 故).

因上記之(8)，(9)以及

(10) $$S^4=1,$$

羣 $\{S, T\}$ 遂爲四元數羣(由第143節之定義). 是故屬於2之Sylow氏約羣 $\mathfrak{S}$ 非有四元數羣以爲其約羣不可.

4°. 用前段之記號，以 $\{S, T\}$ 爲含於 $\mathfrak{S}$ 之四元數羣，而以 $\mathfrak{Q}$ 示之. 在 $\mathfrak{S}$ 之元素中，其與S，T二者爲交換可能者，與 $\mathfrak{Q}$ 之各元素爲交換可能甚明. 以若斯之元素之集合表以 $\mathfrak{L}$，則 $\mathfrak{L}$ 爲 $\mathfrak{S}$ 之約羣無疑矣. 今取 $\mathfrak{L}$ 之任意元素L，則

(11) $$T^{-1}(SL)T=T^{-1}ST\cdot T^{-1}LT=S^{-1}L.$$

然 $$S^{-1}L\neq SL \quad [\because S^2\neq 1].$$

故積SL於 $\mathfrak{S}$ 非自己共軛. 因之以3°中對S所行之同樣推

論行之於SL, 遂得

$$(SL)^4=1,\quad T^{-1}(SL)T=(SL)^{-1}.$$

以此第二式與(11)比較, 得

$$(SL)^{-1}=S^{-1}L$$

然L與S爲交換可能. 故

$$L^2=1.$$

卽$\mathfrak{L}$之元素之巡回率皆爲2也. 因之$\mathfrak{L}$不得不爲Abel氏羣. 蓋因以L_1, L_2爲$\mathfrak{L}$之二元素, 則得

$$L_1L_2=(L_1L_2)^{-1}=L_2^{-1}L_1^{-1}=L_2L_1$$

故.

今取$\mathfrak{L}$之任意元素K. 若此與S, T之兩者爲交換可能, 則K屬於$\mathfrak{L}$. 若K與S交換可能, 與T非交換可能, 則非

$$K^{-1}TK=T^{-1}$$

不可. 此之理由, 若以3° 中對S所行之推論同樣施之於T, 便得知焉. 然由(8)及(9),*

$$ST^{-1}S^{-1}=T.$$

由此與前式,

$$(KS^{-1})^{-1}T(KS^{-1})=SK^{-1}TKS^{-1}=T.$$

而因K與S爲交換可能, 故KS^{-1}當然與S爲交換可能. 故KS^{-1}屬於$\mathfrak{L}$. 卽

---

*由(8), $T^{-1}S^{-1}T=S$. 故 $ST^{-1}S^{-1}=S^2T^{-1}=T$.

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

$$\therefore\quad K=LS=SL.$$

其次若K與T交換可能，與S非交換可能，則與前同樣

$$K=TL\ (L\text{ 爲 }\mathfrak{L}\text{ 之元素}).$$

又若K雖與積ST交換可能，然與S及T皆非交換可能時，則

$$K=(ST)L.$$

然$\mathfrak{L}$之元素乃或與S, T, ST之三者爲交換可能，或僅與其一爲交換可能者. 蓋若與二者爲交換可能，則與第三者亦交換可能故也.* 故$\mathfrak{L}$之元素乃有次形:

$$1\cdot L,\ SL,\ TL,\ (ST)L,$$

卽屬於積$\Omega\mathfrak{L}$者也. 反之，$\mathfrak{G}\mathfrak{L}$之元素乃含於$\mathfrak{L}$. 故

$$\mathfrak{L}=\Omega\mathfrak{L}. \tag{12}$$

更就$\mathfrak{L}$而討論之. S^2, 於Ω爲自己共軛甚明，故含於$\mathfrak{L}$. 而$\mathfrak{L}$乃[1, 1,……1]型之Abel氏羣. 故由第130節系，$\mathfrak{L}$與巡回羣$\{S^2\}$及他羣(名之曰$\mathfrak{M}$)之直乘積等. 故由(12),

$$\mathfrak{L}=\Omega\{S^2\}\mathfrak{M}=\Omega\mathfrak{M}\quad[\because\ \Omega S^2=\Omega]. \tag{13}$$

然Ω中之自己共軛元素(主元素以外者)僅爲S^2. 此則因在第143節所與之四元數羣(4)中，其自己共軛元素之爲1及-1，由同節(3)之關係直可知之；而與-1對應者，於Ω爲S^2故也. 因之Ω與$\mathfrak{L}$之共通元素僅爲1及S^2. 隨而$\mathfrak{M}$與Ω

*如K與S, ST爲交換可能，則遂與$S^3\cdot ST=T$亦交換可能也.

除主元素外無共通之元素. 故由(13), $\mathfrak{R}$ 爲 $\mathfrak{Q}$ 與 $\mathfrak{M}$ 之直乘積. 而以 $\mathfrak{M}$ 爲 $\mathfrak{L}$ 之約羣故, 當然爲 $[1, 1, \cdots\cdots, 1]$ 型之 Abel 氏羣也. 綜合上記四段之結果, 遂得定理.

第二十三章　母式之指標根

146. 極, 指標方程式.

試取 n 次母式

$$(1) \qquad (a_{ij}) \qquad (i, j=1, 2, \cdots\cdots, n)$$

及與是對應之變換

$$(2) \qquad x'_i=a_{i1}x_1+a_{i2}x_2+\cdots\cdots+a_{in}x_n \qquad (i=1, 2, \cdots\cdots, n).$$

於(2)以適合

$$x'_i=\lambda x_i \qquad (i=1, 2, \cdots\cdots, n)$$

者之 $x_1, x_2, \cdots\cdots, x_n$ 之值, 卽以滿足聯立方程式

$$(3) \quad \begin{cases} \lambda x_1=a_{11}x_1+a_{12}x_2+\cdots\cdots+a_{1n}x_n \\ \lambda x_2=a_{21}x_1+a_{22}x_2+\cdots\cdots+a_{2n}x_n \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \lambda x_n=a_{n1}x_1+a_{n2}x_2+\cdots\cdots+a_{nn}x_n \end{cases}$$

者之 $x_1, x_2, \cdots\cdots, x_n$ 爲一組, 而名之曰變換(2)之**極**.* 但(3)

---

*變換(2)之極, 便宜上卽呼曰母式(1)之極.

之解中，其

$$x_1=x_2=\cdots\cdots=x_n=0$$

者，不取之以爲極焉．欲求是極，乃由(3)消去 $x_1, x_2, \cdots\cdots, x_n$，遂得

$$(4)\qquad \begin{vmatrix} a_{11}-\lambda & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22}-\lambda & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{n1} & a_{n2} & \cdots\cdots & a_{nn}-\lambda \end{vmatrix}=0.$$

或略記之爲

$$(4)\qquad |a_{ij}-\lambda e_{ij}|=0 \quad (i,j=1,2,\cdots\cdots,n).$$

將此就 λ 而解之，以其值代入(3)而算出 $x_1, x_2, \cdots\cdots, x_n$ 可．方程式(4)名曰母式(1)或變換(2)之**指標方程式**，而其根曰**指標根**．至(4)之左邊之行列式則曰**指標行列式**．

因(3)爲一次齊次方程式，故對於適合(4)之 λ 之值之一如 λ_1，乃生無數之解．茲以相應於 λ_1 之二解爲 $(X_1, X_2, \cdots\cdots, X_n)$ 及 $(Y_1, Y_2, \cdots\cdots, Y_n)$，則

$$X_1 : X_2 : \cdots\cdots : X_n = Y_1 : Y_2 : \cdots\cdots : Y_n.$$

若是者連比相等之極，均視之爲同一者．卽與同指標根相應之極，則以之爲同一者是也．於是若指標方程式(4)之根互異時，則變換(2)乃有 n 個之極焉．

特別就二次母式言，則母式 $\begin{pmatrix}\alpha & \beta \\ \gamma & \delta\end{pmatrix}$ 之指標方程式爲

$$(5)\qquad \lambda^2-(\alpha+\delta)\lambda+(\alpha\delta-\beta\gamma)=0.$$

而此之判別式

$$(\alpha+\delta)^2-4(\alpha\delta-\beta\gamma)$$

寄於零時，則變換

$$x'=\alpha x+\beta y,\qquad y'=\gamma x+\delta y$$

僅有唯一之極*；否則乃有二極．如母式 $\begin{pmatrix}0&2\\-1&3\end{pmatrix}$ 之指標根爲1, 2，而與之相應之極，則分別爲(2, 1)及(1, 1)．又 $\begin{pmatrix}3&-2\\2&-1\end{pmatrix}$ 之指標根爲1(等根)，因之變換 $x'=3x-2y$, $y'=2x-y$ 之極爲(1, 1).

例1.　$\begin{pmatrix}1&-1&1\\4&0&-1\\4&-2&1\end{pmatrix}$, $\begin{cases}x'=x-y+z,\\y'=4x-z,\\z'=4x-2y+z.\end{cases}$

此之指標方程式爲

$$\begin{vmatrix}1-\lambda&-1&1\\4&-\lambda&-1\\4&-2&1-\lambda\end{vmatrix}=0,$$

其根爲2, 1, −1．今若求與 $\lambda=2$ 相應之極，則解聯立方程式

$$2x=x-y+z,\ 2y=4x-z,\ 2z=4x-2y+z,$$

而得　　$x:y:z=1:1:2.$

故與根2相應之極爲(1, 1, 2)．同樣與他二根相應之二極

此時乃視兩極爲已一致者．

爲 (1, 2, 2), (0, 1, 1).

例 2.
$$\begin{pmatrix} 0 & 2 & 5 \\ 0 & 0 & -1 \\ -1 & 0 & 4 \end{pmatrix}, \qquad \begin{cases} x' = 2y + 5z \\ y' = -z \\ z' = -x + 4z. \end{cases}$$

此之指標行列式爲

$$\begin{vmatrix} -\lambda & 2 & 5 \\ 0 & -\lambda & -1 \\ -1 & 0 & 4-\lambda \end{vmatrix} = -(\lambda-1)^2(\lambda-2).$$

因之指標根爲 1, 1, 2. 而與 $\lambda=1$ 相應之極爲 (3, −1, 1); 與 $\lambda=2$ 相應者爲 (4, −1, 2).

147. 定理. 凡母式雖以任何母式將其變形, 其指標方程式不變. 因之指標根與變形無關係.

證明. 以 $(\bar{l}_{ij})$ 爲母式 (l_{ij}) 之逆, 以 (l_{ij}) 變 (a_{ij}) 之形, 則

$$(l_{ij})^{-1}(a_{ij})(l_{ij}) = (\sum_{s,t} \bar{l}_{is} a_{st} l_{tj}) \quad (i, j = 1, 2, \cdots\cdots, n).$$

計算此之指標行列式, 則得

$$| \sum_{s,t} \bar{l}_{is} a_{st} l_{tj} - \lambda e_{ij} | = | \sum_{s,t} \bar{l}_{is} a_{st} l_{tj} - \sum_{s,t} \lambda \bar{l}_{is} e_{st} l_{tj} |$$

$$= | \bar{l}_{ij} | \cdot | a_{ij} - \lambda e_{ij} | \cdot | l_{ij} | = | a_{ij} - \lambda e_{ij} |.$$

因之遂得定理.

系. 於母式 (a_{ij}), 在其主對角線上之項之和 $a_{11}+a_{22}+\cdots\cdots+a_{nn}$, 對於變形而不變.

蓋由前節之指標方程式(4)而觀，此和之與指標根之和相等者卽爲得知故也．此系中所舉之和名曰母式(a_{ij})之指標．

定理．以$(l_{ij})^{-1}$變母式(a_{ij})之形，則極由變換(l_{ij})而移動．

爲使更易明了起見，再述之如次：

在(a_{ij})之極中，以其與指標根λ相應者爲$(X_1, X_2, \cdots\cdots, X_n)$，而作

$$(1)\qquad Y_i=l_{i1}X_1+l_{i2}X_2+\cdots\cdots+l_{in}X_n\quad (i=1, 2, \cdots\cdots, n),$$

則$(Y_1, Y_2, \cdots\cdots, Y_n)$乃爲與$\lambda$相應之$(l_{ij})(a_{ij})(l_{ij})^{-1}$之極．

證明．以$(\bar{l}_{ij})$爲(l_{ij})之逆，而令

$$(2)\qquad (l_{ij})(a_{ij})(l_{ij})^{-1}=(b_{ij}).$$

因$(X_1, X_2, \cdots\cdots, X_n)$爲與$\lambda$相應之$(a_{ij})$之極，故

$$\lambda X_s=\sum_t a_{st}X_t\quad (s=1, 2, \cdots\cdots, n).$$

於此而乘以l_{is}，再就s而加之，得

$$\lambda\sum_s l_{is}X_s=\sum_{s,t} l_{is}a_{st}X_t=\sum_{s,t,u} l_{is}a_{su}e_{ut}X_t.$$

然

$$\sum_j \bar{l}_{uj}l_{jt}=e_{ut}.$$

故

$$\lambda\sum_s l_{is}X_s=\sum_{s,t,u,j} l_{is}a_{su}\bar{l}_{uj}l_{jt}X_t$$

$$=\sum_j\{\sum_{s,u} l_{is}a_{su}\bar{l}_{uj}\}\{\sum_t l_{it}X_t\}.$$

以(1), (2)代入此中，得

$$\lambda Y_i=\sum_j b_{ij}Y_j,$$

故 $(Y_1, Y_2, \cdots\cdots, Y_n)$ 爲相應於 λ 之 (b_{ij}) 之極.

定理. 若將母式 m 方乘之,則其指標根亦高 m 方冪.

證明. 乘 $|a_{ij}+\lambda e_{ij}|$ 於母式 (a_{ij}) 之指標行列式,則得

$$(3)\qquad \begin{aligned}&|a_{ij}-\lambda e_{ij}|\cdot|a_{ij}+\lambda e_{ij}|\\ &=|\sum_s(a_{is}a_{sj}-\lambda e_{is}a_{sj}+\lambda a_{is}e_{sj}-\lambda^2 e_{is}e_{sj})|\\ &=|\sum_s a_{is}a_{sj}-\lambda a_{ij}+\lambda a_{ij}-\lambda^2 e_{ij}|\\ &=|\sum_s a_{is}a_{sj}-\lambda^2 e_{ij}|.\end{aligned}$$

然 $(a_{ij})^2$ 之指標方程式爲

$$(4)\qquad |\Sigma a_{is}a_{sj}-\mu e_{ij}|=0.$$

故若以 $\lambda_1, \lambda_2, \cdots\cdots, \lambda_n$ 爲 (a_{ij}) 之指標根,則各平方 $\lambda^2_1, \lambda^2_2, \cdots\cdots, \lambda^2_n$, 由 (3), 得滿足 (4) 甚明. 關於 (a_{ij}) 之三乘四乘等亦復同樣.

系. 若母式須有有限之巡回率,則其指標根之爲 1 之冪根是所必要.

蓋因主母式之指標根爲 1 (等根), 故若 $(a_{ij})^m=(e_{ij})$, 則

$$\lambda_1{}^m=\lambda_2{}^m=\cdots\cdots=\lambda_n{}^m=1$$

爲必要故也.

此系之逆不成立. 如取母式 $\begin{pmatrix}11\\01\end{pmatrix}$, 其指標根雖爲 1, 然

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}^2=\begin{pmatrix}1&2\\0&1\end{pmatrix},\ \begin{pmatrix}1&1\\0&1\end{pmatrix}^3=\begin{pmatrix}1&2\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&3\\0&1\end{pmatrix},\ \cdots\cdots,$$

$$\begin{pmatrix}1&1\\0&1\end{pmatrix}^m=\begin{pmatrix}1&m-1\\0&1\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&m\\0&1\end{pmatrix},$$

不得有有限之巡回率也.

148. 母式之正常形.

以 $\lambda_1, \lambda_2, \cdots\cdots, \lambda_n$ 爲 n 次母式 (a_{ij}) 之指標根(等根亦所容許). 以與 λ_1 相應之變換之極爲 $(X_{11}, X_{21}, \cdots\cdots, X_{n1})$, 則由前前節 (3) 得

$$(1)\qquad \lambda_1 X_{i1}=a_{i1}X_{11}+a_{i2}X_{21}+\cdots\cdots+a_{in}X_{n1}$$
$$(i=1, 2, \cdots\cdots, n).$$

乃作一以 $X_{11}, X_{21}, \cdots\cdots, X_{n1}$ 爲第一縱列, 而其行列式不爲零者之母式

$$\begin{pmatrix}X_{11}&X_{12}&\cdots\cdots&X_{1n}\\X_{21}&X_{22}&\cdots\cdots&X_{2n}\\\cdots\cdots&\cdots\cdots&\cdots\cdots&\cdots\cdots\\X_{n1}&X_{n2}&\cdots\cdots&X_{nn}\end{pmatrix}$$

而以之右乘於 (a_{ij}), 則由 (1) 得

$$(a_{ij})(X_{ij})=\begin{pmatrix}\lambda_1X_{11}&X'_{12}&\cdots\cdots&X'_{1n}\\\lambda_1X_{21}&X'_{22}&\cdots\cdots&X'_{2n}\\\cdots\cdots&\cdots\cdots&\cdots\cdots&\cdots\cdots\\\lambda_1X_{n1}&X'_{n2}&\cdots\cdots&X'_{nn}\end{pmatrix}$$

次令 $(\overline{X}_{ij})$ 爲 (X_{ij}) 之逆, 而左乘之於上式, 則得

(2) $$(X_{ij})^{-1}(a_{ij})(X_{ij})$$

$$=\begin{pmatrix} \lambda_1 \sum_s \overline{X}_{1s}X_{s1} & b_{12} & \cdots\cdots & b_{1n} \\ \lambda_1 \sum_s \overline{X}_{2s}X_{s1} & b_{22} & \cdots\cdots & b_{2n} \\ \cdots\cdots & & & \\ \lambda_1 \sum_s \overline{X}_{ns}X_{s1} & b_{n2} & \cdots\cdots & b_{nn} \end{pmatrix}$$

$$=\begin{pmatrix} \lambda_1 & b_{12} & \cdots\cdots & b_{1n} \\ 0 & b_{22} & \cdots\cdots & b_{2n} \\ \cdots\cdots & & & \\ 0 & b_{n2} & \cdots\cdots & b_{nn} \end{pmatrix}$$

此母式之指標根乃由 λ_1 及母式

(3) $$\begin{pmatrix} b_{22} & \cdots\cdots & b_{2n} \\ \cdots\cdots & & \\ b_{n2} & \cdots\cdots & b_{nn} \end{pmatrix}$$

之指標根而成. 然由前節第一定理,此諸根與母式 (a_{ij}) 之指標根一致. 故(3)之指標根爲 $\lambda_2, \cdots\cdots, \lambda_n$. 以相應於 λ_2 之(3)之極爲 $(Y_{22}, Y_{32}, \cdots\cdots, Y_{n2})$ 而作母式

$$\begin{pmatrix} 1 & 0 & 0 & \cdots\cdots & 0 \\ 0 & Y_{22} & Y_{23} & \cdots\cdots & Y_{2n} \\ 0 & Y_{32} & Y_{33} & \cdots\cdots & Y_{3n} \\ \cdots\cdots & & & & \\ 0 & Y_{n2} & Y_{n3} & \cdots\cdots & Y_{nn} \end{pmatrix}, \quad |Y_{ij}| \neq 0,$$

再以此將(2)之右邊變形，則與前同樣，其結果爲

$$\begin{pmatrix} \lambda_1 & c_{12} & c_{13} & \cdots\cdots & c_{1n} \\ 0 & \lambda_2 & c_{23} & \cdots\cdots & c_{2n} \\ 0 & 0 & c_{33} & \cdots\cdots & c_{3n} \\ \cdots\cdots & & & & \\ 0 & 0 & c_{n3} & \cdots\cdots & c_{nn} \end{pmatrix}$$

更將同樣之手續反覆之，則(a_{ij})遂變爲次形：

$$(4) \qquad \begin{pmatrix} \lambda_1 & k_{12} & k_{13} & \cdots\cdots & k_{1n} \\ 0 & \lambda_2 & k_{23} & \cdots\cdots & k_{2n} \\ 0 & 0 & \lambda_3 & \cdots\cdots & k_{3n} \\ \cdots\cdots & & & & \\ 0 & 0 & 0 & \cdots\cdots & \lambda_n \end{pmatrix}$$

此形之母式稱曰**正常形**.* 因之得

定理. 凡母式皆由變形得導之爲正常形.

正常形，其主對角線上之項皆爲指標根，須注意. 又正常形之積亦爲正常形，此則易於證明者也.

例. 若將前前節例1之母式

$$\begin{pmatrix} 1 & -1 & 1 \\ 4 & 0 & -1 \\ 4 & -2 & 1 \end{pmatrix}$$

*對變換言，亦用此同一之語.

變爲正常形，乃取與指標根2相應之極(1, 1, 2)，而以之作母式

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}$$

再以此將上母式變形，則得

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & -1 & 1 \\ 4 & 0 & -1 \\ 4 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 1 \\ 0 & 1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

主對角線上之項，如上述，乃表指標根者也.

系. 若兩個二變數變換共有一極時，則兩者得以同一之變換而變形爲正常形.

證明. 設(X, Y)爲二變換

$$x'=\alpha x+\beta y, \qquad y'=\gamma x+\delta y$$

及

$$x'=\alpha' x+\beta' y, \quad y'=\gamma' x+\delta' y$$

之共通極，則如本定理之證明中所示，若以 $\begin{pmatrix} X & 0 \\ Y & 1 \end{pmatrix}$ 將母式 $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, $\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ 變形，則共爲正常形.

特別就二次母式言，乃取正常形 $\begin{pmatrix} \lambda_1 & \beta \\ 0 & \lambda_2 \end{pmatrix}$，而以 $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ 變其形，則得

$$\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} \lambda_1 & \beta \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \beta+h(\lambda_1-\lambda_2) \\ 0 & \lambda_2 \end{pmatrix}.$$

$\lambda_1 \neq \lambda_2$ 時，乃選適合於

$$\beta+h(\lambda_1-\lambda_2)=0$$

者之h之值，則變形之結果爲$\begin{pmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{pmatrix}$．然母式皆得變形爲正常形．故二次母式之有相異指標根者皆得以之變形而爲倍乘母式也.* 反之，若兩根相等時，則此類變形未見其必爲可能．如$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$，任以何母式變其形，不得爲$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$即主母式是也．但在母式有有限巡回率時，則常爲可能．蓋因

$$\begin{pmatrix}\lambda & \beta\\ 0 & \lambda\end{pmatrix}^2=\begin{pmatrix}\lambda^2 & 2\beta\lambda\\ 0 & \lambda^2\end{pmatrix},\ \begin{pmatrix}\lambda & \beta\\ 0 & \lambda\end{pmatrix}^3=\begin{pmatrix}\lambda^3 & 3\beta\lambda^2\\ 0 & \lambda^3\end{pmatrix},\ \cdots\cdots,$$

$$\begin{pmatrix}\lambda & \beta\\ 0 & \lambda\end{pmatrix}^n=\begin{pmatrix}\lambda^n & n\beta\lambda^{n-1}\\ 0 & \lambda^n\end{pmatrix}.$$

故$\begin{pmatrix}\lambda & \beta\\ 0 & \lambda\end{pmatrix}$欲有有限巡回率，則$\beta=0$爲必要．由此是觀，指標根相等之二次母式有有限之巡回率時，若以此變形爲正常形，則自成相似母式也.† 夫若是，則二次母式之有有限巡回率者，無論指標根之等否，常得由變形而導成倍乘母式焉.‡

---

*倍乘母式之定義，參照第109節．又不限於二次母式，一般，指標根互異者之母式用上同樣之方法，得以之變形爲倍乘母式也.

†參照第109節.

‡此不限於二次者，雖一般之母式皆得成立，俟次篇自明.

第二十四章 分數變換羣

149. 共線變換.

於一母式(a_{ij})乘以相似母式(μe_{ij}),其所得之積(μa_{ij})名曰與(a_{ij})**相似**. 對變換言,亦以同樣之定義與之. 兩母式(或變換)若與第三之母式(或變換)相似,則兩者互相似.

於一變換*

$$(1)\qquad x'_i=a_{i1}x_1+a_{i2}x_2+\cdots\cdots+a_{in}x_n$$
$$(i=1,2,\cdots\cdots,n),$$

若以比$x_1:x_2:\cdots\cdots:x_n$爲表$n-1$次空間(呼之曰甲)之點之坐標,又比$x'_1:x'_2:\cdots\cdots:x'_n$爲表乙空間之點之坐標,則(1)之關係乃以示射影幾何學上所謂兩空間之**共線變換**者也. 若取與(1)相似之變換

$$(2)\quad x''_i=\mu(a_{i1}x_1+a_{i2}x_2+\cdots\cdots+a_{in}x_n)\quad(i=1,2,\cdots\cdots,n),$$

則
$$x''_1:x''_2:\cdots\cdots:x''_n=x'_1:x'_2:\cdots\cdots:x'_n$$

甚明. 故若以比$x''_1:x''_2:\cdots\cdots:x''_n$亦視爲表示乙空間中之點之坐標者,則(2)乃定一與(1)同一之共線變換. 故吾人以互相似之母式(或變換)爲一組,而轉用幾何學之用語,與之以**共線變換**之名稱焉.

---

*本節所論,僅其行列式不等於零者.

且於變換所作之有限羣$\mathfrak{F}$中，其與主變換相似者，相似變換也．其集合以$\mathfrak{M}$表之．因相似變換與任何變換皆交換可能，故$\mathfrak{M}$於$\mathfrak{F}$爲正常．就$\mathfrak{M}$分$\mathfrak{F}$爲傍系而以之爲

$$\mathfrak{F}=\mathfrak{M}+\mathfrak{M}\mathrm{P}+\mathfrak{M}\mathrm{Q}+\cdots\cdots,$$

則屬於同一傍系之變換互相似，而屬於異傍系者則否．於是各傍系名曰$\mathfrak{F}$中之共線變換，而商$\mathfrak{F}/\mathfrak{M}$則名曰$\mathfrak{F}$中之**共線變換羣**焉．

$\mathfrak{F}$之變換A之行列式爲a時，乃取a之n乘根，而以其逆數乘於A*再令

$$a^{-\frac{1}{n}}\mathrm{A}=\mathrm{A}', \tag{3}$$

則A′之行列式等於1．但a之n乘根有n個，故由A可得n個之A′也．將此對$\mathfrak{F}$之各變換施行之，以由之所得變換之集合表以$\mathfrak{F}'$．於是此集合$\mathfrak{F}'$成羣也．蓋若以

$$b^{-\frac{1}{n}}\mathrm{B}=\mathrm{B}'\ (b\text{爲B之行列式}),$$

則得

$$\mathrm{A}'\mathrm{B}'=(ab)^{-\frac{1}{n}}\mathrm{AB} \tag{4}$$

故也．又AB之行列式等於ab．故對變換A, B, ……，令A′, B′, …… 相與對應，則由(4)，對於積AB，乃有A′B′相對應．

---

*乘相似變換$x'_i=lx_i\ (i=1, 2, \cdots\cdots)$於變換A，名曰乘數$l$於A，其結果以$l$A表之．即與論母式者全然同樣者也．至$n$則即示$\mathfrak{F}$之變換中之變數之個數者焉．

卽 $\mathfrak{G}'$ 與 $\mathfrak{G}$ 同態也. 於此同態關係, 則 $\mathfrak{G}'$ 之共線變換與 $\mathfrak{G}$ 之共線變換相對應. 蓋若 A 相似於 B, 則 A′ 相似於 B′, 而其逆亦成立故. 因之, 若以 $\mathfrak{M}'$ 爲 $\mathfrak{G}'$ 中相似變換之集合, 則 $\mathfrak{M}'$ 對應於 $\mathfrak{G}$ 之正常約羣 $\mathfrak{M}$ ($\mathfrak{G}$ 中相似變換之集合), 隨之商 $\mathfrak{G}/\mathfrak{M}$ 與 $\mathfrak{G}'/\mathfrak{M}'$ 爲單純同態也. 爰得

定理. 共線變換羣, 得由行列式爲 1 之變換所作之羣而導出之.

特別在二變數 x, y 時, 則

$$\mathfrak{M}': \quad \left.\begin{matrix} x'=x \\ y'=y \end{matrix}\right\}, \quad \left.\begin{matrix} x'=-x \\ y'=-y \end{matrix}\right\}.$$

蓋因 1 之平方根僅爲 ±1 故.

150. 分數變換.

共線變換, 乃在變換中, 不論其變數之各個, 而只注目於其比者也. 在二變數時, 由變換

(1) $\qquad x'=\alpha x+\beta y, \quad y'=\gamma x+\delta y \quad (\alpha\delta-\beta\gamma\neq 0)$

則變數之比 $x:y$ 果如何而變乎? 爲明此故, 乃以 (1) 之第二式除其第一式而作

$$\frac{x'}{y'}=\frac{\alpha\left(\frac{x}{y}\right)+\beta}{\gamma\left(\frac{x}{y}\right)+\delta}$$

可. 於此而令 $\frac{x}{y}=z$, $\frac{x'}{y'}=z$, 則得

(2)　　$z'=\dfrac{\alpha z+\beta}{\gamma z+\delta}$　　$(\alpha\delta-\beta\gamma\neq 0)$.

由此關係,將變數 z 置換爲 z' 之演算,名曰**分數變換**,而 $\alpha\delta-\beta\gamma$,名曰此變換之行列式. 試取與(1)相似之變換

$$x'=\mu(\alpha x+\beta y),\quad y'=\mu(\gamma x+\delta y),$$

而由之所導出之分數變換,亦(2)也. 故一個共線變換,僅得以唯一個分數變換而表之焉.

變換(1)與一第二變換

(3)　　$x'=\alpha' x+\beta' y,\quad y'=\gamma' x+\delta' y$

之積爲

$$x'=\alpha'' x+\beta'' y,\quad y'=\gamma'' x+\delta'' y$$

時,則由此所導出之分數變換

$$z'=\frac{\alpha'' z+\beta''}{\gamma'' z+\delta''},$$

得定爲乘分數變換[由(3)所導出者]

(4)　　$z'=\dfrac{\alpha' z+\beta'}{\gamma' z+\delta'}$

於(2)之積. 是積也,不外乎以(4)之右邊代(2)之 z 者而已也. 乘法既若是定義則共線變換羣乃與分數變換羣爲單純同態焉.

茲以 λ_1 爲變換(1)之指標根,其與是相應之極以爲 (X_1, Y_1),則

(5)　　$\lambda_1 X_1=\alpha X_1+\beta Y_1,\quad \lambda_1 Y_1=\gamma X_1+\delta Y_1$.

故若令 $\frac{X_1}{Y_1}=p$, 則由是得

$$p=\frac{\alpha p+\beta}{\gamma p+\delta}.$$

即 p 對分數變換 (2) 爲不變也. 若是之 p, 名曰 (2) 之極. 特別在 $Y_1=0$ 時, 則 $p=\infty$. 欲 $Y_1=0$, 則由 (5) 須 $\gamma=0$, 因之分數變換, 遂成爲次形:

$$z'=\frac{\alpha z+\beta}{\delta}.$$

變換 (1) 乃有兩指標根. 故與是相應, 則得分數變換 (2) 之二極. 兩指標根相異時, 以他之一個爲 λ_2, 則由第 148 節所述, 變換 (1) 遂變形爲倍乘變換

$$x=\lambda_2 x,\quad y'=\lambda_1 y. \tag{6}$$

即適合

$$\begin{pmatrix}a & b\\ c & d\end{pmatrix}^{-1}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}\lambda_2 & 0\\ 0 & \lambda_1\end{pmatrix}$$

者之母式 $\begin{pmatrix}a & b\\ c & d\end{pmatrix}$ 爲存在也. 以與此母式相應之分數變換

$$z'=\frac{az+b}{cz+d}$$

將分數變換 (2) 變形, 則得與 (6) 相應之分數變換

$$z'=\frac{\lambda_2}{\lambda_1}z \tag{7}$$

甚明. 此形之變換, 與 (6) 同樣仍呼曰倍乘變換, 而指標根之比 $\frac{\lambda_2}{\lambda_1}$ 則名曰分數變換 (2) 之倍乘數. 倍乘數之絕對值等於 1 時, 變換 (2) 曰橢圓的, 倍乘數爲正之實數時, 則名曰

雙曲的，其他者則名曰 **loxodromic 線的**. 二指標根中雖選其任一個爲 λ_1，然除此三種外不得生別之變化，明也.

其次變換 (1) 之指標根相等時，分數變換 (2) 之兩極一致. 此時分數變換名曰**拋物的**. 以 (1) 之指標根爲 λ (等根)，而將其變形爲正常形，則得

$$x'=\lambda x+\beta' y,\quad y'=\lambda y.\quad (\text{參照第 148 節}).$$

而與是相應之分數變換則爲

$$z'=z+\frac{\beta'}{\lambda}.$$

不僅此也，若 (1) 之巡回率爲有限，則如第 148 節所示，$\beta'=0$ 爲必要也. 故拋物的變換之有有限巡回率者不得存在焉.

例. (於下乃以 μ 表倍乘數; p, q 表極.)

(i) $z'=-\dfrac{1}{z}$; $\mu=-1$; $p=\sqrt{-1}, q=-\sqrt{-1}$　(橢圓的);

(ii) $z'=\dfrac{2z+1}{z+1}$: $\mu=\dfrac{7-3\sqrt{5}}{2}>0$; $p=\dfrac{1+\sqrt{5}}{2}, q=\dfrac{1-\sqrt{5}}{2}$

(雙曲的);

(iii) $z'=\dfrac{\sqrt{-1}\,z+2}{-z+\sqrt{-1}}$: $\mu=2\sqrt{2}-3<0$, $p=-\sqrt{-2}, q=\sqrt{-2}$

(loxodromic 線的);

(iv) $z'=\dfrac{z}{z+1}$:　$p=q=0$　(拋物的).

母式者乃以任何母式變其形其指標根亦不變者也. 故分數變換之種類與變形無關係也.

注意. 分數變換(2)之極,乃滿足方程式

$$z=\frac{\alpha z+\beta}{\gamma z+\delta}. \tag{8}$$

反之,若 p 爲此方程式之根時,則因

$$\frac{p}{1}=\frac{\alpha p+\beta}{\gamma p+\delta}$$

之故,$(p, 1)$ 之爲變換(1)之極明已. 因之,分數變換(2)之極,乃適合(8)之 z 之值也. $\gamma\neq 0$ 時,解方程式(8),遂得兩個有限極. 反之,$\gamma=0$ 時,有限極雖只一個,然吾人容許 ∞ 爲(8)之根;而以之爲他一極焉.

151. 有限巡回率之條件.Cayley 氏變換.

母式之有有限巡回率者之指標根乃1之冪根(第147節). 故分數變換須有有限巡回率時,則其倍乘數爲1之冪根是所必要,因之變換爲橢圓的也.

試求分數變換

$$z'=\frac{\alpha z+\beta}{\gamma z+\delta} \qquad (\alpha\delta-\beta\gamma=1) \tag{1}$$

爲橢圓的之條件. 因母式 $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ 之指標方程式爲

$$\lambda^2-(\alpha+\delta)\lambda+1=0, \tag{2}$$

故以此之二根爲 λ_1, λ_2,則 $\lambda_1\lambda_2=1$,而變換又須爲橢圓的,則

$$\left|\frac{\lambda_2}{\lambda_1}\right|=1.$$

故 $|\lambda_2|=1$. 因之

(3)　$\lambda_2=\cos\omega+i\sin\omega,\ \lambda_1=\cos\omega-i\sin\omega\quad(i=\sqrt{-1}).$

故

(4)　$$\alpha+\delta=\lambda_1+\lambda_2=2\cos\omega.$$

反之，此時方程式(2)之根爲(3)之λ_1,λ_2，因而倍乘數爲

(5)　$$\frac{\lambda_2}{\lambda_1}=\cos 2\omega+i\sin 2\omega=e^{2\omega i},$$

於是上之分數變換(非主變換)若須爲橢圓的，則$\frac{\alpha+\delta}{2}$爲實數其絕對值又小於1爲必要而且充分也.*

其次將對橢圓變換(1)變形爲倍乘變換，則得

(6)　$$z'=e^{2\omega i}z.$$

而此之n方乘爲

$$z'=e^{2n\omega i}z.$$

故(1)，隨之(6)之巡回率若爲n，則

$$2n\omega=2k\pi\quad(k\text{對於}n\text{爲互素之整數}).$$

$$\therefore\qquad\omega=\frac{k\pi}{n}.$$

以之代入(4)，遂得變換(1)之巡回率爲n之條件：

(7)　$$\alpha+\delta=2\cos\frac{k\pi}{n}.$$

而此時$\begin{pmatrix}\alpha&\beta\\\gamma&\delta\end{pmatrix}$之指標根由(3)爲

(8)　$$\lambda_2=\cos\frac{k\pi}{n}+i\sin\frac{k\pi}{n},\ \lambda_1=\cos\frac{k\pi}{n}-i\sin\frac{k\pi}{n}.$$

---

*參照第147節第一定理之系.

例. 試取與Cayley形母式*相應之分數變換

$$z'=\frac{(d+ai)z+(c-bi)}{-(c+bi)z+(d-ai)} \quad (d^2+a^2+b^2+c^2=1),$$

因其能滿足上記之條件,故爲橢圓的;若令 $d=\cos\omega$,則其倍乘數得以(15)與之. 此形之變換名曰**Cayley氏變換**. 其巡回率爲 n 時,則 $\cos^{-1}d=\frac{k\pi}{n}$,

152. 分數變換之有限羣.

定理. 在分數變換之有限羣中,其變換之共有同一極者,形成一巡回約羣.

證明. 令 p 爲兩個分數變換

$$z'=\frac{\alpha z+\beta}{\gamma z+\delta}. \quad z'=\frac{\alpha' z+\beta'}{\gamma' z+\delta'}$$

之共通極,而以

$$z'=\frac{\alpha'' z+\beta''}{\gamma'' z+\delta''}$$

爲上兩變換之積. 於是

$$p=\frac{\alpha p+\beta}{\gamma p+\delta}, \quad p=\frac{\alpha' p+\beta'}{\gamma' p+\delta'}.$$

$$\therefore \quad p=\frac{\alpha\left(\frac{\alpha' p+\beta'}{\gamma' p+\delta'}\right)+\beta}{\gamma\left(\frac{\alpha' p+\beta'}{\gamma' p+\delta'}\right)+\delta}=\frac{\alpha'' p+\beta''}{\gamma'' p+\delta''}.$$

即 p 又爲積之極也. 因之在分數變換之有限羣$\mathfrak{G}$中,其共

*參照第144節.

有極 p 者之變換形成一約羣也. 以之爲 $\mathfrak{H}$, 其元數爲 n.

其次由第148節系, $\mathfrak{H}$ 之變換皆得以同一變換同時變形爲正常形. 以之爲

$$(1)\qquad z'=z,\ z'=\varepsilon_1 z+c_1,\ \cdots\cdots,\ z'=\varepsilon_{n-1}z+c_{n-1},$$

而分別名之曰

$$(2)\qquad 1, S_1, \cdots\cdots, S_{n-1}.$$

於是

$$(3)\qquad \begin{aligned} S_iS_j&:\quad z'=\varepsilon_i\varepsilon_j z+(\varepsilon_i c_j+c_i)\\ S_i{}^{\lambda}&:\quad z'=\varepsilon_i{}^{\lambda}z+c_i(\varepsilon_i{}^{\lambda-1}+\varepsilon_i{}^{\lambda-2}+\cdots\cdots+1),\\ S_i{}^{-1}&:\quad z'=\varepsilon_i{}^{-1}z-\varepsilon_i{}^{-1}c_i. \end{aligned}$$

然 $\mathfrak{H}$ 之元數爲 n. 故由上第二式,

$$(4)\qquad 1,\ \varepsilon_1,\ \varepsilon_2,\ \cdots\cdots,\ \varepsilon_{n-1}$$

皆須爲1之 n 乘根也. 此中若以其爲無原根*者, 則其間定有相等者在. 茲假定 $\varepsilon_i=\varepsilon_j$, 則由上式得

$$S_iS_j{}^{-1}:\quad z'=z+(c_i-c_j).$$

然此若須有有限巡回率, 則 $c_i=c_j$ 爲必要. 因之 $S_i=S_j$. 卽(4)中不得有相等者存在也, 是則非含原根不可. 以 ε_1 爲原根, 則變換

$$(5)\qquad 1,\ S_1,\ S_1{}^2,\ \cdots\cdots,\ S_1{}^{n-1},$$

由(3)之第二式知其互異, 因之以是則(2)之變換定能盡也. 故 $\mathfrak{H}$ 爲巡回羣.

---

*在1之 n 乘根中, 其 n 方乘始等於1者曰原根.

系. 在分數變換有限羣中,兩變換若共有一極,則亦共有其他極.

定理. 分數變換之有限羣,若以適當之變換而變其形,則由是其所屬之變換皆得導之爲 Cayley 形者.

證明. 1°. 設 $\mathfrak{G}$ 爲分數變換之有限羣.* 其屬於 $\mathfrak{G}$ 之變換之行列式皆得取之爲 1. 蓋因

$$\frac{\mu(\alpha z+\beta)}{\mu(\gamma z+\delta)}=\frac{\alpha z+\beta}{\gamma z+\delta} \qquad (\alpha\delta-\beta\gamma\neq 0),$$

而左邊之行列式爲 $\mu^2(\alpha\delta-\beta\gamma)$. 因之若適當的選擇 μ, 則此行列式遂等於 1 故.

於 $\mathfrak{G}$, 若以其變換之共有一定極者之集合爲 $\mathfrak{H}$, 則由前定理, $\mathfrak{H}$ 爲巡回羣. 乃以屬於 $\mathfrak{H}$ 之變換爲

$$(6) \qquad 1,\ S,\ S^2,\ \cdots\cdots,\ S^{n-1}.$$

將 S 變形得導之爲倍乘變換. 卽若令

$$A^{-1}SA:\quad z'=\frac{\lambda z}{\bar{\lambda}},\qquad \begin{cases}\lambda=\cos\dfrac{\pi}{n}+i\sin\dfrac{\pi}{n},\\ \bar{\lambda}=\cos\dfrac{\pi}{n}-i\sin\dfrac{\pi}{n},\end{cases}$$

則 $A^{-1}\mathfrak{H}A$ 之變換得以

$$(7) \qquad 1,\quad z'=\frac{\lambda z}{\bar{\lambda}},\quad z'=\frac{\lambda^2 z}{\bar{\lambda}^2},\ \cdots\cdots,\quad z'=\frac{\lambda^{n-1}z}{\bar{\lambda}^{n-1}}$$

與之, 而此諸個皆爲 Cayley 形者也. 故以 (7) 而 $A^{-1}\mathfrak{G}A$ 之變換得盡時, 則定理之爲眞可知已.

---

*乃行列式不爲零之變換所作之羣.

反之若 $A^{-1}\mathfrak{G}A$ 含有(7)以外之變換時,以其一爲

$$T': \quad z'=\frac{\alpha z+\beta}{\gamma z+\delta} \qquad (\alpha\delta-\beta\gamma=1).$$

於是 β 與 γ 皆不得爲零. 蓋若 $\beta=0$, 則 T′ 與(7)之變換共有極 0; 若 $\gamma=0$, 則與(7)之變換共有極 ∞. 因之無論如何, T′ 非屬於(7)不可故也. 次因 $A^{-1}\mathfrak{G}A$ 爲有限羣,隨之 T′ 乃有有限巡回率,故由前節之所述,

$$\alpha+\delta=2\cos\omega \quad (\text{實數})$$

因之

$$\delta=\bar{\alpha}+r.$$

但 r 表實數, $\bar{\alpha}$ 爲表 α 之共軛複素數者. 今於 T′ 乘以 $A^{-1}SA$,

$$T'A^{-1}SA: \qquad z'=\frac{\alpha\lambda z+\beta\bar{\lambda}}{\gamma\lambda z+\delta\bar{\lambda}}.$$

此積亦屬於 $A^{-1}\mathfrak{G}A$, 故其巡回率亦非有限不可. 以故 $\alpha\lambda+\delta\bar{\lambda}$ 須爲實數. 卽

$$(\alpha\lambda+\bar{\alpha}\bar{\lambda})+r\bar{\lambda}=\text{實數}.$$

於是

$$r=0, \qquad \text{因之} \qquad \delta=\bar{\alpha}.$$

而

$$\beta\gamma=\alpha\delta-1=\alpha\bar{\alpha}-1=\text{實數}.$$

故

$$\gamma=-s\bar{\beta}.$$

但 s 表實數($\neq 0$), $\bar{\beta}$ 表 β 之共軛數.

復次取 $A^{-1}\mathfrak{G}A$ 之任意一置換

$$U': \quad z'=\frac{\alpha_1 z+\beta_1}{\gamma_1 z+\delta_1} \qquad (\alpha_1\delta_1-\beta_1\gamma_1=1),$$

則由上述,

$$\delta_1=\bar{\alpha}_1, \quad \gamma_1=-s_1\bar{\beta}_1 \quad (s_1 \text{ 爲不爲零之實數}).$$

將此變換乘於T′, 則得

$$T'U': \quad z'=\frac{(\alpha\alpha_1-s_1\beta\bar{\beta}_1)z+(\alpha\beta_1+\beta\bar{\alpha}_1)}{-(s\bar{\beta}\alpha_1+s_1\bar{\alpha}\bar{\beta}_1)z+(-s\bar{\beta}\beta_1+\alpha\alpha_1)}.$$

然由上述, 此第四係數$(-s\bar{\beta}\beta_1+\bar{\alpha}\alpha_1)$須與第一係數$(\alpha\alpha_1-s_1\beta\bar{\beta}_1)$共軛. 爲此之故, 則非$s_1=s$不可. 因之$A^{-1}\mathfrak{G}A$之變換皆有

$$T': \quad z'=\frac{\alpha z+\beta}{-s\bar{\beta}z+\bar{\alpha}} \qquad (\alpha\bar{\alpha}+s\beta\bar{\beta}=1)$$

之形. 此中s乃所有變換之共通的實數. (特別當T′屬於$A^{-1}\mathfrak{H}A$時, 則$\beta=0$.)

更以變換

$$B: \quad z'=\frac{z}{\sqrt{s}}$$

變$A^{-1}\mathfrak{G}A$之形, 則$B^{-1}A^{-1}\mathfrak{G}AB$之變換皆爲次形:

$$B^{-1}T'B: \quad z'=\frac{\alpha z+\sqrt{s}\,\beta}{-\sqrt{s}\,\bar{\beta}z+\bar{\alpha}}.$$

然如下所證明s乃爲正數. 故$B^{-1}T'B$爲Cayley形. 故定理遂告成立.

2°. 因$\alpha\bar{\alpha}+s\beta\bar{\beta}=1$, 故欲證$s$爲正, 則只證$|\alpha|\leqq 1$爲已足. 爲此之故, 試假定對於$A^{-1}\mathfrak{G}A$之某一變換

$$T': \quad z'=\frac{\alpha z+\beta}{-s\bar{\beta}z+\bar{\alpha}},$$

$|\alpha|>1$, 則示其由此遂生矛盾可也. 茲令

$$\alpha=\rho(\cos\theta+i\sin\theta), \quad \rho>1.$$

當 $|\rho\cos\theta|>\frac{1}{2}$ 時,乃作 T′ 之自乘,則

$$z'=\frac{\alpha_2 z+\beta_2}{\gamma_2 z+\delta_2},\quad \alpha_2=\alpha^2-s\beta\bar{\beta}.$$

名此曰 T_2. 於是

$$|\alpha_2|^2=|\alpha^2-s\beta\bar{\beta}|^2=|\alpha^2+\alpha\bar{\alpha}-1|^2$$
$$=4\rho^2(\rho^2-1)\cos^2\theta+1>\rho^2=|\alpha|^2.$$

即 T'^2 之第一係數之絕對值較 T′ 之第一係數之絕對值爲大也.

當 $|\rho\cos\theta|\leqq\frac{1}{2}$ 時, 乃於 T′ 乘以 $A^{-1}\mathfrak{S}A$ 之變換 $A^{-1}S^kA$,

$$T'\cdot A^{-1}S^kA:\quad z'=\frac{\alpha\lambda^k z+\beta\bar{\lambda}^k}{-s\bar{\beta}\lambda^k z+\bar{\alpha}\bar{\lambda}^k}.$$

於是

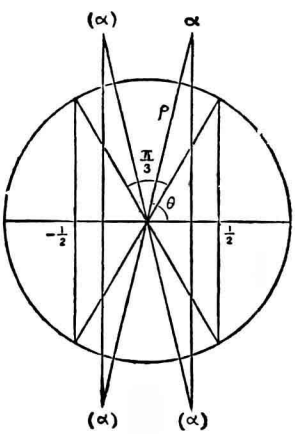
$$\alpha\lambda^k=\rho\left\{\cos\left(\theta+\frac{k\pi}{n}\right)+i\sin\left(\theta+\frac{k\pi}{n}\right)\right\}.$$

而 θ 爲第一,第三象限之角時,則隨 n 之爲偶數或奇數,而令

$$k=\frac{n}{2}\text{ 又 }\frac{n-1}{2};$$

又其爲第二,第四象限之角時,則令

$$k=-\frac{n}{2}\text{ 或 }-\frac{n-1}{2}.$$



於是 $\left|\frac{k\pi}{n}\right|\geqq\frac{\pi}{3}$, 故無論其如何, 皆爲

$$\left|\rho\cos\left(\theta+\frac{k\pi}{n}\right)\right|>\frac{1}{2}$$

也. 故將 $T'A^{-1}S^kA$ 自乘,而用前同一

之記號幷令

$$(T'A^{-1}S^kA)^2:\ z'=\frac{\alpha_2 z+\beta_2}{\gamma_2 z+\delta_2},$$

則與前同樣

$$|\alpha_2|>|\alpha\lambda^k|=|\alpha|.$$

此時其自乘亦名曰T_2. 於是雖在上記之任何情形中,T_2皆屬於$A^{-1}\mathfrak{G}A$,而其第一係數之絕對值較T'之第一係數之絕對值爲大也.

更用T_2,則其第一係數之絕對值較T_2者爲大之變換T_3,於$A^{-1}\mathfrak{G}A$中可以求得. 將此反覆行之,遂得無數之變換

$$T',\ T_2,\ T_3,\ \cdots\cdots.$$

而此諸個之任何個皆屬於$A^{-1}\mathfrak{G}A$,且以其第一係數之絕對值漸次較大,故互異也. 是則與$A^{-1}\mathfrak{G}A$爲有限羣之假設相反,豈非不合理乎? 故不能$|\alpha|>|$. 卽s爲正數也.

153. 有限羣之種類.

令$\mathfrak{G}$爲分數變換所作之有限羣,其元數爲g. 若以p爲屬於$\mathfrak{G}$之一變換之極,則以p爲極之變換($\mathfrak{G}$的)形成一巡回約羣(前節第一定理). 以之爲

$$\mathfrak{H}:\ 1, S, S^2, \cdots\cdots, S^{n-1},$$

而就$\mathfrak{H}$分$\mathfrak{G}$爲傍系;

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}T_1+\cdots\cdots+\mathfrak{H}T_{\nu-1}.$$

今以

$$T_i:\ z'=\frac{\alpha_i z+\beta_i}{\gamma_i z+\delta_i}\quad (i=1, 2, \cdots\cdots, \nu-1),$$

而令

$$p_i=\frac{\alpha_i p+\beta_i}{\gamma_i p+\delta_i}\quad (i=1,2,\cdots\cdots,\nu-1),$$

則因T_i不屬於$\mathfrak{H}$,故$p_i\neq p$. 而由第147節定理,p_i乃$T_iST_i^{-1}$之極. 故對於$\mathfrak{G}$之極*p行以$\mathfrak{G}$之變換,則由是可得ν個之極

$$p,\ p_1,\cdots\cdots,\ p_{\nu-1}\quad (\nu=g/n).$$

至此各個之互異則爲易知,而名之曰與p共軛之極焉.

計算羣$\mathfrak{G}$之極之數,因上記之極p爲$\mathfrak{G}$中$n-1$個變換$(\neq 1)$之所共通,故p爲$n-1$個. 於是p之共軛極p_i亦爲$n-1$個. (蓋因巡回約羣之共有p_i極者由上述明爲$T_i\mathfrak{H}T_i^{-1}$故也.) 因之由此計算法,則與p共軛之極之數爲$(n-1)\nu$個. 若與p不共軛之極p'存在於$\mathfrak{G}$時,則與之共軛之極之個數由上述爲$(n'-1)\nu'$. 但n'表以p'爲極之巡回約羣之元數,而ν'爲其指數. 以此所得兩組之共軛極,$\mathfrak{G}$之極尙不能盡時,則更取他之極而計其共軛極之個數. 反覆行之,則$\mathfrak{G}$之極之總數得以

$$(n-1)\nu+(n'-1)\nu'+\cdots\cdots$$

與之可知. 但自他面言,一變換$(\neq 1)$乃有二極,因之$\mathfrak{G}$總計有$2(g-1)$個極. 故

$$2(g-1)=(n-1)\nu+(n'-1)\nu'+\cdots\cdots.$$

換書之,因

---

*其屬於羣之變換之極,單呼之曰羣之極.

$$n\nu=n'\nu'=\cdots\cdots=g$$

之故,若以共軛極之組數爲h,則爲

(1) $$2g-2=hg-\nu-\nu'-\cdots\cdots.$$

然$n, n', \cdots\cdots$任何個皆不小於2,因之

$$1\leqq\nu\leqq\frac{g}{2},\quad 1\leqq\nu'\leqq\frac{g}{2},\ \cdots\cdots$$

故由(1),

$$\frac{hg}{2}\leqq 2g-2\leqq h(g-1).$$

由是

$$2\leqq h\leqq 4-\frac{4}{g}.$$

適合此之h之值,僅2或3焉.

1°. $h=2$時.

以此值代入於(1),

$$2=\nu+\nu'.$$

故 $$\nu=\nu'=1.$$

因之 $$g=n.$$

卽$\mathfrak{G}$與巡回羣$\mathfrak{H}$一致也.

2.° $h=3$時.

以此值代入於(1),

(2) $$g+2=\nu+\nu'+\nu''.$$

由是爲決定ν, ν', ν''之值計,乃取

$$n\leqq n'\leqq n'',\quad \text{隨之}\quad \nu\geqq\nu'\geqq\nu''.$$

此時非 $n=2$ 不可. 蓋若 $n\geqq 3$, 則 $\nu\leqq\frac{g}{3}$, 因之

$$\nu+\nu'+\nu''\leqq g,$$

而與(2)矛盾故也. 其次以

(3)　　$$g=n\nu=2\nu$$

代入(2), 則

(4)　　$$\nu+2=\nu'+\nu''.$$

(i) 若取 $n'=2$, 則 $\nu'=\nu$, 而由(4)得 $\nu''=2$. 卽此時

$$\begin{cases} n=n'=2, & n''=\frac{g}{2} \\ \nu=\nu'=\frac{g}{2}, & \nu''=2 \end{cases}$$

也.

(ii) 若取 $n'=3$, 則由(3)及(4),

(5)　　$$\frac{g}{2}+2=\frac{g}{3}+\nu'',$$

卽　　$$\nu''=\frac{g}{6}+2.$$

故　　$\nu''>\frac{g}{6}$, 因之 $n''<6$.

於是　　$n''=3, 4, 5.$

因之　　$\nu''=\frac{g}{3}, \frac{g}{4}, \frac{g}{5}.$

以此之值代入(5)以定 g, 則分別得

$$g=12, 24, 60.$$

將上三款綜記之則如次:

$$\begin{cases} n=2, & n'=3, & n''=3, & g=12, \\ \nu=6, & \nu'=4, & \nu''=4; \end{cases}$$

$$\begin{cases} n=2, & n'=3, & n''=4, & g=24, \\ \nu=12, & \nu'=8. & \nu''=6; \end{cases}$$

$$\begin{cases} n=2, & n'=3, & n''=5, & g=60, \\ \nu=30, & \nu'=20, & \nu''=12. \end{cases}$$

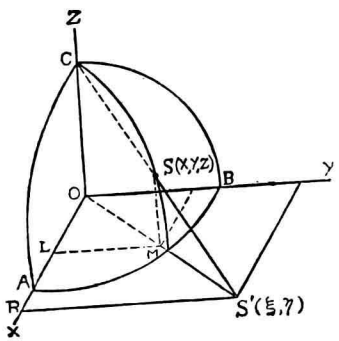
最後則$n'\geqq 4$者不得有也. 蓋此時$\nu'\leqq\frac{g}{4}$, 因之

$$\nu'+\nu''\leqq\frac{g}{4}+\frac{g}{4}=\frac{g}{2}=\nu,$$

是與(4)相反故耳. 以故分數變換之有限羣不過上所得之五種. 與是五種相當之羣之存在,則如下所述, 對於Cayley氏變換與以幾何學的意義,得由之而自明也.

154. 立體平畫射影.

試取以O爲原點之直角坐標軸OX, OY, OZ, 而以O爲中心作一單位球. 球面上取一點S, 由球與OZ軸之交點C, 將S射影於XY平面上. 由此方法, 球面上之點均可映於XY平面上也. 遂呼之曰**立體平畫射影**.



以點S之坐標爲(X, Y, Z),

其射影S′之坐標爲(ξ, η), 則

$$\frac{Z}{1}=\frac{MS}{OC}=\frac{MS'}{OS'}=\frac{LR}{OR}=\frac{\xi-X}{\xi}.$$

故　　$X=\xi(1-Z).$

同樣　　$Y=\eta(1-Z).$

換書之爲

(1)　　$$\xi=\frac{X}{1-Z},\ \eta=\frac{Y}{1-Z}.$$

或將此就X, Y, Z而解之, 因$X^2+Y^2+Z^2=1$, 遂得

(2)　　$$X=\frac{2\xi}{\xi^2+\eta^2+1},\quad Y=\frac{2\eta}{\xi^2+\eta^2+1},\quad Z=\frac{\xi^2+\eta^2-1}{\xi^2+\eta^2+1}.$$

(1)卽(2), 乃示由C點射影時, 球面上之點與其射影之坐標間之關係者也.

由此射影, 則圓映爲圓. 蓋因平面

(3)　　$$lX+mY+nZ+h=0$$

上之點(X, Y, Z)之射影, 由(2)非滿足方程式

$$l\left(\frac{2\xi}{\xi^2+\eta^2+1}\right)+m\left(\frac{2\eta}{\xi^2+\eta^2+1}\right)+n\left(\frac{\xi^2+\eta^2-1}{\xi^2+\eta^2+1}\right)+h=0$$

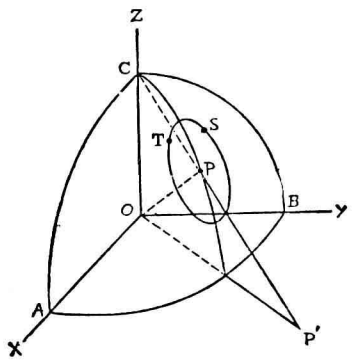
不可. 將此換書之, 則爲

(4)　　$$2l\xi+2m\eta+n(\xi^2+\eta^2-1)+h(\xi^2+\eta^2+1)=0.$$

是卽圓也. 特別若$n+h=0$, 則爲直線. 平面(3)與球之交圓, 便宜上呼之曰圓(3)焉.

其次垂直於平面(3)之直線之方向餘弦之比爲$l:m:n$

故若取 $l^2+m^2+n^2=1$, 則垂直於此平面之直徑之兩端 P, Q 之坐標爲 $(l, m, n), (-l, -m, -n)$. 此點名曰圓(3)之**極**. 以極 P, Q 之射影爲 P′, Q′, 則其坐標由(1)分別爲



$$(5)\qquad \left(\frac{l}{1-n}, \frac{m}{1-n}\right),$$

$$\left(\frac{-l}{1+n}, \frac{-m}{1+n}\right).$$

以含球之直徑 PQ 者之平面爲

$$(6)\qquad l'X+m'Y+n'Z=0,$$

則

$$(7)\qquad ll'+mm'+nn'=0.$$

此平面與球之交圓, 卽以 P, Q 爲兩極時之子午線, 由前述乃射影於圓

$$(8)\qquad 2l'\xi+2m'\eta+n'(\xi^2+\eta^2-1)=0.$$

而此圓通過 P′ 及 Q′ 也. 反之, 在 XY 平面上過二點 P′, Q′ 之圓, 皆爲子午線(以 P, Q 爲兩極者)之射影. 蓋若於 XY 平面上任意取一點 U′, 而以直線 CU′ 與球之交點爲 U. 於是圓 P′U′Q′ 爲過 U 之子午線 PUQ 之射影, 明已

且圓(4)與圓(8)爲直交. 此則用(7)之關係而易得證明者. 一般球面上兩圓之交角, 由此射影而不變. 蓋由(2),

$$dX=\frac{2(1-\xi^2+\eta^2)d\xi-4\xi\eta d\eta}{(\xi^2+\eta^2+1)^2},$$

$$dY=\frac{2(1+\xi^2-\eta^2)d\eta-4\xi\eta d\xi}{(\xi^2+\eta^2+1)^2},$$

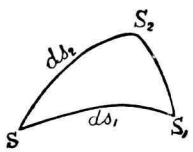
$$dZ=\frac{4(\xi d\xi+\eta d\eta)}{(\xi^2+\eta^2+1)^2},$$

$$\therefore\quad dX^2+dY^2+dZ^2=\frac{4(d\xi^2+d\eta^2)}{(\xi^2+\eta^2+1)^2}.$$

即若將球面上之線分素表以 ds, 平面 XY 上之線分素表以 $d\sigma$, 則得

$$ds^2=\frac{4d\sigma^2}{(\xi^2+\eta^2+1)^2} \tag{9}$$

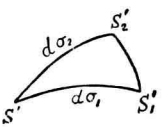
也. 因之於球面上取線分素所作之三角形 SS_1S_2, 而以其在 XY 平面上之射影爲 $S'S'_1S'_2$, 則得



$$\frac{SS_1}{SS_2}=\frac{ds_1}{ds_2}=\frac{d\sigma_1}{d\sigma_2}=\frac{S'S_1'}{S'S_2'};$$

同樣,

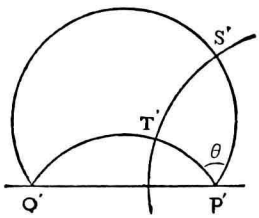
$$\frac{S_1S_2}{S_1S}=\frac{S_1'S_2'}{S_1'S'}.$$



故兩三角形 SS_1S_2 及 $S'S'_1S'_2$ 相似, 因之角 S_1SS_2 等於角 $S_1'S'S_2'$ 也.

最後於第二圖以直徑 PQ 爲軸將球轉角 θ. 此之結果, 乃以球面上之點 S 爲移於 T 者. 於是子午線 PSQ 之射影 P′S′Q′ 與子午線 PTQ 之射影 P′T′Q′ 於 P′, Q′ 相交, 其交角由上述爲 θ 也. 更 S 若在以 P 爲極之圓 (3) 上時, T 亦非在同圓上不可, 因之兩點之射影 S′, T′ 共在圓 (4) 上. 然圓 (4) 如上述乃與子午線 (以 P, Q 爲極者) 之射影直交. 即關於

P′, Q′ 之 Apollonius 氏圓也. 故由上之迴轉, S 之射影 S′ 得移達之點 T′, 乃爲過 S′ 之 Apollonius 氏圓(關於 P′, Q′ 者)與過 P′, Q′ 而對圓 P′S′Q′ 成 θ 角者之圓之交點也.



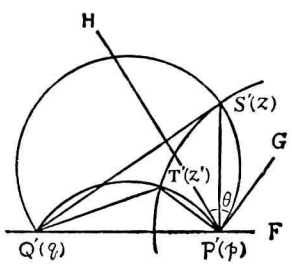
155. Cayley 氏變換之幾何學的意義.

於前節之射影以 XY 平面作爲 Gauss 氏複素數平面, 而 XY 平面上之點 (ξ, η) 以之爲表示複素數 $\xi+\eta i$ 者而定之. 乃以點 P′, Q′ 所表之複素數爲 p, q, 則由前節(5), 得

$$(1)\qquad p=\frac{l+mi}{1-n},\quad q=-\frac{l+mi}{1+n}\qquad (l^2+m^2+n^2=1).$$

次以 S′, T′ 所表之複素數爲 z, z' 而觀其兩數間之關係. 因 S′, T′ 在同一之 Apollonius 圓上之故,

$$\frac{\text{線分 P′T′}}{\text{線分 Q′T′}}=\frac{\text{線分 P′S}}{\text{線分 Q′S′}}.$$



故

$$(2)\qquad \frac{|z'-p|}{|z'-q|}=\frac{|z-p|}{|z-q|}.$$

又於 P′ 點引兩圓之切線 P′G, P′H, 則

$$\angle P'S'Q'=\angle FP'G,\ \angle P'T'Q'=\angle FP'H=\angle FP'G+\theta.$$

故
$$\angle P'T'Q'=\angle P'S'Q'+\theta.$$

然
$$\angle P'S'Q'=\angle FP'S'-\angle FQ'S'$$

$$=(z-p\text{ 之偏角})-(z-q\text{ 之偏角})=\frac{z-p}{z-q}\text{ 之偏角.}$$

同樣

$$\angle \mathrm{P'T'Q'}=\frac{z'-p}{z'-q}\text{ 之偏角.}$$

故

$$\frac{z'-p}{z'-q}\text{ 之偏角}=\frac{z-p}{z-q}\text{ 之偏角}+\theta.$$

由此與(2)得

$$\frac{z'-p}{z'-q}=e^{\theta i}\frac{z-p}{z-q}. \tag{3}$$

此卽所求之關係也.

爲將z與z'之關係(3)換書起見,乃以之就z'而解之,則有:

$$z'=\frac{(p-qe^{\theta i})z+pq(e^{\theta i}-1)}{(1-e^{\theta i})z+(pe^{\theta i}-q)}.$$

右邊之分母子以$qe^{\frac{\theta i}{2}}$除之,而以(1)之值代入p, q,則

$$z'=\frac{\left(\cos\frac{\theta}{2}-in\sin\frac{\theta}{2}\right)z+\left(m\sin\frac{\theta}{2}-il\sin\frac{\theta}{2}\right)}{-\left(m\sin\frac{\theta}{2}+il\sin\frac{\theta}{2}\right)z+\left(\cos\frac{\theta}{2}+in\sin\frac{\theta}{2}\right)}. \tag{4}$$

於是令

$$\cos\frac{\theta}{2}=d,\ -n\sin\frac{\theta}{2}=a,\ m\sin\frac{\theta}{2}=c,\ l\sin\frac{\theta}{2}=b, \tag{5}$$

則(4)遂爲

$$z'=\frac{(d+ai)z+(c-bi)}{-(c+bi)z+(d-ai)}. \tag{6}$$

而此之行列式爲

$$d^2+a^2+b^2+c^2=\cos^2\frac{\theta}{2}+\sin^2\frac{\theta}{2}(l^2+m^2+n^2)=1$$

甚明. 卽謂(6)爲Cayley氏變換也. 由此是觀,其伴於軸PQ周圍之迴轉(迴轉角θ)所生S′之移動,乃與對z行以Cayley氏變換(6)者相當焉.

反之,Cayley氏變換(6)爲已知時,則用(5)而將其換書之,遂成(3)形. 故由上述,可知此變換乃表球之迴轉者甚明. 變換(6)視爲表球之迴轉者時,則名之曰**Cayley氏之公式**.

注意. 以λ_1, λ_2 $(\lambda_1 \neq \lambda_2)$爲變換

$$x'=\alpha x+\beta y,\quad y'=\gamma x+\delta y\quad (\alpha\delta-\beta\gamma=1)$$

之指標根,而以與是相應之分數變換

$$z'=\frac{\alpha z+\beta}{\gamma z+\delta} \tag{7}$$

之極爲p, q,則分數變換得換書如次:

$$\frac{z'-p}{z'-q}=\frac{\lambda_2}{\lambda_1}\cdot\frac{z-p}{z-q}. \tag{8}$$

特別若$q=\infty$,則有次形:

$$z'-p=\frac{\lambda_2}{\lambda_1}(z-p)$$

又變換若爲橢圓的,則由第151節(5), $\frac{\lambda_2}{\lambda_1}=e^{\theta i}$. 此時在Gauss氏平面上,$z$由(7)卽(8)所移之點$z'$,乃爲過$z$之Apollonius氏圓與過$p$及$q$而對圓$pzq$成$\theta$角者之圓之交點也.

156. 分數變換羣與球之迴轉羣.

試先就Cayley氏變換之積與其各個所表示之迴轉之

積*之關係一論. 將前兩節所述球之迴轉(軸PQ, 角θ). 卽

$$\frac{z'-p}{z'-q}=e^{\theta i}\frac{z-p}{z-q} \tag{1}$$

行之之後更於直徑P_1Q_1之周迴轉一角θ_1,其結果則以之爲球面上之點T移至U者. 而P_1, Q_1, T, U之射影(射影之中心C)分別以之爲P'_1, Q'_1, T', U'. XY平面與Gauss氏平面之關係,與前節同樣而定,而此諸射影所表之複素數分別以爲p_1, q_1, z', z'', 則

$$\frac{z''-p_1}{z''-q_1}=e^{\theta_1 i}\frac{z'-p_1}{z'-q_1} \tag{2}$$

由此與(1)消去z',則得z與z''之關係. 此關係卽表示上之二迴轉續行之結果者也. 又於(2)之z',以(1)之z'代入之,則其所得者,不外右乘(1)於變換(2)者而已(參照第150節). 故於上之兩迴轉,以其以PQ爲軸者名曰甲,P_1Q_1爲軸者名曰乙,則甲乙兩運動續行之結果,得以左乘(2)於變換(1)之積表之也. 於是對於以直徑爲軸之一迴轉,以其表此之變換之逆相與對應,則對二迴轉之積,乃有與其各個對應之積相與對應焉. 是則球之迴轉所作之羣與Cayley氏分數變換所作之羣爲同型矣. 然Cayley形變換皆表迴轉者(參照前節);而分數變換有限羣,又得導之爲Cayley形變換所作之羣(第152節第二定理). 故第153節所得五種羣之

*與第16, 17兩節同樣,其二運動續行之結果,呼曰兩運動之積焉.

存否，得由其各個之相當者能實現之於球之迴轉羣與否而定也.

1°. 一定軸周圍之迴轉$\left(\text{迴轉角}\frac{2\pi}{g}\right)$作一$g$元巡回羣.

2°. 試將內接於球之大圓之正$\frac{g}{2}$角形考之，則球之迴轉能使其於運動前後占有同一空間者作一g元多角羣(參照第16節). 此羣乃與第153節2°(i)者相當者也.

3°. 試就球之內接正四面體而論之，則若此在運動前後仍占同一空間者之球之迴轉，乃作一四面體羣(參照第17節). 此羣爲與第153節2°(ii)之第一羣相當者. 至其餘二羣則分別與八面體羣，二十面體羣相當焉(參照第17, 21, 60諸節). 綜合上述，得次

定理. 分數變換有限羣爲巡回羣，多角羣，四面體羣，八面體羣及二十面體羣之五種.

系. Cayley形母式所作之有限羣，若不含母式$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$時，屬於上之五種；反之，若含$\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$時，則由約羣$\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}\right\}$之商屬於上之五種.

蓋因Cayley形相似母式僅爲$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $\begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}$故(參照第149節共線變換羣).

第 五 篇

羣 母 式. 羣 指 標

第二十五章 母式之階級

157. 一般母式.

將 mn 個文字 a_{ij} $(i=1, 2, \cdots\cdots, m;\ j=1, 2, \cdots\cdots, n)$ 概括一處,排之爲 m 行而各行則由 n 個文字而成者:

$$(1) \qquad \begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m1} & a_{m2} & \cdots\cdots & a_{mn} \end{pmatrix}$$

名之曰 m **行** n **列之母式**,或單曰 $m-n$ **母式**. 特別在 $m=n$ 時,則名之曰 m **次之正方母式**,或單曰 m **次母式**.* 其作母式之各文字 a_{ij} 則無論上二者之爲何,皆稱曰母式之**項**. 母式 (1) 略記之爲

$$(a_{ij}) \qquad \begin{cases} i=1, 2, \cdots\cdots, m, \\ j=1, 2, \cdots\cdots, n. \end{cases}$$

---

*參照第 109 節.

由 $m-n$ 母式(1)及 $n-p$ 母式

(2) $\qquad (b_{ij})\quad (i=1, 2, \cdots\cdots, n;\ j=1, 2, \cdots\cdots, p),$

以

$$c_{ij}=a_{i1}b_{1j}+a_{i2}b_{2j}+\cdots\cdots+a_{in}b_{nj}$$
$$(i=1, 2, \cdots\cdots, m;\ j=1, 2, \cdots\cdots, p)$$

之關係,得作一 $m-p$ 母式:

(3)
$$\begin{pmatrix} c_{11} & c_{12} & \cdots\cdots & c_{1p} \\ c_{21} & c_{22} & \cdots\cdots & c_{2p} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ c_{m1} & c_{m2} & \cdots\cdots & c_{mp} \end{pmatrix}$$

此名曰右乘(2)於母式(1)之積. 又二母式之和,與第109節中者得全然同樣定義之. 但此時兩母式之行數列數非分別相等不可.

若

A 爲 $m-n$ 母式 $\quad A=(a_{ij})\quad \begin{cases} i=1, 2, \cdots\cdots, m \\ j=1, 2, \cdots\cdots, n, \end{cases}$

B 爲 $m-p$ 母式 $\quad B=(b_{ij})\quad \begin{cases} i=1, 2, \cdots\cdots, m \\ j=1, 2, \cdots\cdots, p, \end{cases}$

C 爲 $l-n$ 母式 $\quad C=(c_{ij})\quad \begin{cases} i=1, 2, \cdots\cdots, l \\ j=1, 2, \cdots\cdots, n, \end{cases}$

D 爲 $l-p$ 母式 $\quad D=(d_{ij})\quad \begin{cases} i=1, 2, \cdots\cdots, l \\ j=1, 2, \cdots\cdots, p, \end{cases}$

則以此等之項所作之母式:

$$\begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} & b_{11} & b_{12} & \cdots\cdots & b_{1p} \\ \cdots\cdots & & & & & & & \cdots\cdots \\ a_{m1} & a_{m2} & \cdots\cdots & a_{mn} & b_{m1} & b_{m2} & \cdots\cdots & b_{mp} \\ c_{11} & c_{12} & \cdots\cdots & c_{1n} & d_{11} & d_{12} & \cdots\cdots & d_{1p} \\ \cdots\cdots & & & & & & & \\ c_{l1} & c_{l2} & \cdots\cdots & c_{ln} & d_{l1} & d_{l2} & \cdots\cdots & d_{lp} \end{pmatrix}$$

爲簡便計，乃以 $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ 表之.

定理. 若 A, P 爲 m 次正方母式, D, S 爲 n 次正方母式, B, Q 爲 $m-n$ 母式, C, R 爲 $n-m$ 母式, 則

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} P & Q \\ R & S \end{pmatrix}=\begin{pmatrix} AP+BR & AQ+BS \\ CP+DR & CQ+DS \end{pmatrix}.$$

其次各項爲零之母式，名曰**零母式**，而以 0 表之. 在上定理之母式 $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ 中，若 B=0, C=0 時，則名之曰母式 A, D **之直乘積**. 對此乃有次

系.
$$\begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & S \end{pmatrix}=\begin{pmatrix} AP & 0 \\ 0 & DS \end{pmatrix}.$$

此定理及系幷不限於 A, D 爲正方母式時，只要 A 之列數與 P 之行數一致，D 之列數與 S 之行數一致，便常成立也.

注意. 主母式與逆母式之定義，雖於第 109 節已示，但爲後之便宜計特再言之. 令

$$e_{ij}=\begin{cases}1 & (i=j)\\ 0 & (i\neq j)\end{cases}$$

時,則正方母式(e_{ij})曰主母式;兩正方母式之積AA′等於主母式時,則A′稱曰A之逆而以A^{-1}表之. 又於正方母式$(\lambda_i e_{ij})$,雖$\lambda_1, \lambda_2, \cdots\cdots$之中有若干個爲零,然仍與第109節同樣呼之曰倍乘母式. 此外則在本篇中,均以e_{ij}爲表如上之值者.

158. 母式之生成.

今取第115節所論之n次母式.

(1) $$G_{rs\lambda}=(g_{ij\lambda}) \quad (i,j=1,2,\cdots\cdots,n).$$

但 (2) $$g_{rs\lambda}=\lambda \quad (r\neq s),$$

(3) $$g_{11\lambda}=g_{22\lambda}=\cdots\cdots=g_{nn\lambda}=1,$$

而對他之i,j之值,則

(4) $$g_{ij\lambda}=0 \quad (i\neq j).$$

本篇與第三篇之相異處,在對λ得與以任意數值之一點. 此時亦與第115節所示者同樣.

(5) $$\begin{cases}G_{rs\lambda}\,G_{rs\mu}=G_{rs(\lambda+\mu)},\\ (G_{rs\lambda})^{-1}=G_{r,s,-\lambda},\\ (G_{rs\lambda})^{x}=G_{r,s,x\lambda}.\end{cases}$$

又與該節之公式(7)乃至(10)相當者亦成立, 卽若$A=(a_{ij})$爲$m-n$母式,則

$$(6)\quad AG_{rs\lambda}=\begin{pmatrix} a_{11}\ a_{12}\cdots\cdots a_{1s}+\lambda a_{1r}\ a_{1,s+1}\cdots\cdots a_{1n} \\ a_{21}\ a_{22}\cdots\cdots a_{2s}+\lambda a_{2r}\ a_{2,s+1}\cdots\cdots a_{2n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}\ a_{m2}\cdots\cdots a_{ms}+\lambda a_{mr}\ a_{m,s+1}\cdots\cdots a_{mn} \end{pmatrix}$$

次若以 $G_{rs\lambda}$ 爲 m 次，則

$$(7)\quad G_{rs\lambda}A=\begin{pmatrix} a_{11} & a_{12} & \cdots\cdots \\ a_{21} & a_{22} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{r1}+\lambda a_{s1} & a_{r2}+\lambda a_{s2} & \cdots\cdots \\ a_{r+1,1} & a_{r+1,2} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \end{pmatrix}$$

且於 $m-n$ 母式 $A=(a_{ij})$，當 $a_{11}\neq 0$ 時，若能定 λ_s 之值使適合

$$(8)\qquad a_{1s}+\lambda_s a_{11}=0\quad (s=2,3,\cdots\cdots,n),$$

則由 (6) 得

$$(9)\quad AG_{12\lambda_2}G_{13\lambda_3}\cdots\cdots G_{1n\lambda_n}=\begin{pmatrix} a_{11} & 0 & 0\cdots\cdots 0 \\ a_{21} & a'_{22} & a'_{23}\cdots\cdots a'_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots\cdots \\ a_{m1} & a'_{m2} & a'_{m3}\cdots\cdots a'_{mn} \end{pmatrix}$$

此之左邊以 A' 示之．其次對於滿足

$$(10)\qquad a_{r1}+\mu_r a_{11}=0\quad (r=2,3,\cdots\cdots,m)$$

者之 μ_r 之值,則由(7)得

$$(11)\quad G_{m1\mu_m}\cdots\cdots G_{31\mu_3}G_{21\mu_2}A'=\begin{pmatrix} a_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & a''_{22} & a''_{23} & \cdots\cdots & a''_{2n} \\ 0 & a''_{32} & a''_{33} & \cdots\cdots & a''_{3n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 & a''_{m2} & a''_{m3} & \cdots\cdots & a''_{mn} \end{pmatrix}$$

茲名之曰 A''.

於母式 A,當 $a_{11}=0$ 時,若

$$a_{12},\ a_{13},\ \cdots\cdots,\ a_{1n}$$

$$a_{21},\ a_{31},\ \cdots\cdots,\ a_{m1}$$

皆爲零,則 A 乃有 A'' 之形已. 反之,若其中有不爲零者在時,如 $a_{1t}\neq 0$,則由(6)得

$$AG_{t11}=\left\{\begin{matrix} a_{1t}\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \end{matrix}\right\},$$

又 $a_{t1}\neq 0$ 時,則由(7)得

$$G_{1t1}A=\left\{\begin{matrix} a_{t2}\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots \end{matrix}\right\},$$

總之無論二者之爲何,積之第一項不爲零也. 若將上記之方法適用於此積,則遂成 A'' 之形. 於是對於任意之 $m-n$ 母式 A,得使

$$\mathrm{PAQ}=\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & b_{22} & b_{23} & \cdots\cdots & b_{2n} \\ 0 & b_{32} & b_{33} & \cdots\cdots & b_{3n} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & b_{m2} & b_{m3} & \cdots\cdots & b_{mn} \end{pmatrix}$$

而定母式P, Q也. 但P爲表m次特殊母式$G_{rs\mu}$之積，而Q爲表n次特殊母式$G_{rs\lambda}$之積者. 復次令

$$\begin{pmatrix} b_{22} & b_{23} & \cdots\cdots & b_{2n} \\ b_{32} & b_{33} & \cdots\cdots & b_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ b_{m2} & b_{m3} & \cdots\cdots & b_{mn} \end{pmatrix}=\mathrm{B},$$

則能定母式R, S能使滿足

$$\mathrm{RBS}=\begin{pmatrix} c_{22} & 0 \\ 0 & \mathrm{C} \end{pmatrix},\quad \mathrm{C}=(c_{ij}),\quad \begin{cases} i=3, \cdots\cdots, m, \\ j=3, \cdots\cdots, n. \end{cases}$$

但R爲$(m-1)$次，S爲$(n-1)$次之特殊母式之積. 而由前節系，則得

$$\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{R} \end{pmatrix}\begin{pmatrix} b_{11} & 0 \\ 0 & \mathrm{B} \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & \mathrm{S} \end{pmatrix}=\begin{pmatrix} b_{11} & 0 \\ 0 & \mathrm{RBS} \end{pmatrix}=\begin{pmatrix} b_{11} & 0 & 0 \\ 0 & c_{22} & 0 \\ 0 & 0 & \mathrm{C} \end{pmatrix}.$$

更得上之手續反覆之，遂得

$$\mathrm{TAU}=\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & c_{22} & 0 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & \mathrm{K} \end{pmatrix}$$

但 T 爲示 m 次, U 爲 n 次之特殊母式之積; 而 K, 則 $m=n$ 時爲示一次母式, $m<n$ 時, 爲 1 行 $(n-m+1)$ 列母式, $m>n$ 時爲 $(m-n+1)$ 行 1 列母式者.

$m<n$ 時, 令 $\mathrm{K}=(k_{mm}, k_{m,m+1}, k_{m,m+2}, \cdots\cdots)$, 則由 (6) 得

$$\mathrm{TAU}\cdot \mathrm{G}_{m,m+1,\lambda_1}\mathrm{G}_{m,m+2,\lambda_2}\cdots\cdots=\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & c_{22} & 0 & \cdots\cdots & 0 \\ \cdots\cdots & & & & \\ 0 & 0 & 0 & \cdots\cdots & \mathrm{K}' \end{pmatrix}$$

但 $\mathrm{K}'=(k_{mm}, k_{m,m+1}+\lambda_1 k_{mm}, k_{m,m+2}+\lambda_2 k_{mm}, \cdots\cdots)$. 於是當 $k_{mm}\neq 0$ 時, 則得定 $\lambda_1, \lambda_2, \cdots\cdots$ 使 K' 之第二項以下皆爲零者. $k_{mm}=0$ 時, 若 $k_{m,m+1}, k_{m,m+2}, \cdots\cdots$ 之中有不爲零者如 $k_{m,m+t}$, 則由 (6) 得

$$\mathrm{TAU}\cdot \mathrm{G}_{m+t,m,1}=\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots & 0 \\ 0 & c_{22} & 0 & \cdots\cdots & 0 \\ \cdots\cdots & & & & \\ 0 & 0 & 0 & \cdots\cdots & \mathrm{K}_1 \end{pmatrix}$$

但 K_1 之第一項不爲零. 而於此, 上之方法可以適用.

須次 $m>n$ 時, 乃適用 (7). 夫如是, 無論 $m\gtreqless n$ 之爲何, 均得選擇一 m 次之特殊母式之積 V, 及 n 次特殊母式之積 W, 能使滿足

$$(12)\quad \mathrm{VAW}=\mathrm{J},\ \mathrm{J}=\begin{pmatrix} b_{11} & 0 & 0 & \cdots\cdots \\ 0 & c_{22} & 0 & \cdots\cdots \\ 0 & 0 & d_{33} & \cdots\cdots \\ \cdots\cdots & & & \end{pmatrix}$$

也．因之得定

定理．設A爲$m-n$母式，則能選擇一m次母式V及一n次母式W，其行列式不爲零，且能滿足

$$VAW=J,\ J=(\xi_i e_{ij})\quad \begin{cases} i=1,2,\cdots\cdots,m, \\ j=1,2,\cdots\cdots,n, \end{cases}$$

者．

定理．$m-n$母式得以XJY之形表之．但X爲表m次特殊母式$G_{rs\mu}$之積，Y爲n次特殊母式$G_{rs\lambda}$之積，而J爲表$m-n$母式$(\xi_i e_{ij})$者．

蓋若於上式(12)之兩邊以V^{-1}，W^{-1}左右乘之，則得

$$A=V^{-1}JW^{-1},$$

而由(5)，則特殊母式之逆又爲特殊母式故也．

系．n次正方母式，得以特殊母式$G_{rs\lambda}$及倍乘母式之積表之．

蓋若於(12)，A爲正方母式時，J爲倍乘母式故也．

又於(12)，因V，W之行列式爲1，故A爲正方母式時，$|A|=|J|$．* 因之若$|A|=0$，則J之倍乘數中其爲零者不得不存在也．

例．試取母式$\begin{pmatrix} 2 & 10 & -2 \\ 6 & 31 & -7 \\ -4 & -16 & -2 \end{pmatrix}$，而就之以行上之計算．

---

*一般正方母式A之行列式乃以$|A|$表之．

先由(8)以定 λ_2, λ_3, 則有

$$10+2\lambda_2=0,\ -2+2\lambda_3=0,\ \text{即}\ \lambda_2=-5,\ \lambda_3=1.$$

與是相應者,乃有

$$G_{1,2,-5}=\begin{pmatrix}1&-5&0\\0&1&0\\0&0&1\end{pmatrix},\ G_{131}=\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix},\ G_{1,2,-5}\,G_{131}=\begin{pmatrix}1&-5&1\\0&1&0\\0&0&1\end{pmatrix}.$$

次由(10)以定 μ_2, μ_3, 得

$$6+2\mu_2=0,\ -4+2\mu_3=0,\ \text{即}\ \mu_2=-3,\ \mu_3=2.$$

其相應者有

$$G_{2,1,-3}=\begin{pmatrix}1&0&0\\-3&1&0\\0&0&1\end{pmatrix},\ G_{312}=\begin{pmatrix}1&0&0\\0&1&0\\2&0&1\end{pmatrix},\ G_{312}G_{2,1,-3}=\begin{pmatrix}1&0&0\\-3&1&0\\2&0&1\end{pmatrix}.$$

而
$$\begin{pmatrix}1&0&0\\-3&1&0\\2&0&1\end{pmatrix}\begin{pmatrix}2&10&-2\\6&31&-7\\-4&-16&-2\end{pmatrix}\begin{pmatrix}1&-5&1\\0&1&0\\0&0&1\end{pmatrix}$$

$$=\begin{pmatrix}1&0&0\\-3&1&0\\2&0&1\end{pmatrix}\begin{pmatrix}2&0&0\\6&1&-1\\-4&4&-6\end{pmatrix}=\begin{pmatrix}2&0&0\\0&1&-1\\0&4&-6\end{pmatrix}.$$

其次
$$\begin{pmatrix}1&0\\-4&1\end{pmatrix}\begin{pmatrix}1&-1\\4&-6\end{pmatrix}\begin{pmatrix}1&1\\0&1\end{pmatrix}=\begin{pmatrix}1&0\\-4&1\end{pmatrix}\begin{pmatrix}1&0\\4&-2\end{pmatrix}=\begin{pmatrix}1&0\\0&-2\end{pmatrix}.$$

因之
$$\begin{pmatrix}1&0&0\\0&1&0\\0&-4&1\end{pmatrix}\begin{pmatrix}2&0&0\\0&1&-1\\0&4&-6\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}2&0&0\\0&1&0\\0&0&-2\end{pmatrix},$$

然
$$\begin{pmatrix}1&0&0\\0&1&0\\0&-4&1\end{pmatrix}\begin{pmatrix}1&0&0\\-3&1&0\\2&0&1\end{pmatrix}=\begin{pmatrix}1&0&0\\-3&1&0\\14&-4&1\end{pmatrix},$$

$$\begin{pmatrix}1&-5&1\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&0&0\\0&1&1\\0&0&1\end{pmatrix}=\begin{pmatrix}1&-5&-4\\0&1&1\\0&0&1\end{pmatrix}.$$

故　$$\begin{pmatrix} 1 & 0 & 0 \\ -3 & 1 & 0 \\ 14 & -4 & 1 \end{pmatrix}\begin{pmatrix} 2 & 10 & -2 \\ 6 & 31 & -7 \\ -4 & -16 & -2 \end{pmatrix}\begin{pmatrix} 1 & -5 & -4 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

此卽與(12)相當之結果也．又左邊之第一及第三因子，由上之計算自明，乃分別爲

$$G_{3,2,-4}\,G_{312}\,G_{2,1,-3},\quad G_{1,2,-5}\,G_{131}\,G_{231}.$$

故由上式得

$$\begin{pmatrix} 2 & 10 & -2 \\ 6 & 31 & -7 \\ -4 & -16 & -2 \end{pmatrix}=G^{-1}_{2,1\,-3}\,G^{-1}_{312}\,G^{-1}_{3,2,-4}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}G^{-1}_{231}\,G^{-1}_{131}\,G^{-1}_{1,2,-5}$$

$$=G_{213}\,G_{3,1,-2}\,G_{324}\begin{pmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}G_{2,3,-1}\,G_{1,3,-1}\,G_{125}.$$

159. 母式之階級.

試取 m 行 n 列之母式:

$$A=\begin{pmatrix} a_{11} & a_{12} & \cdots\cdots & a_{1n} \\ a_{21} & a_{22} & \cdots\cdots & a_{2n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ a_{m1} & a_{m2} & \cdots\cdots & a_{mn} \end{pmatrix}.$$

由此除去若干行若干列，其所得之行列式* 中，其不爲零者之最高次數爲 r 時，則母式 A 曰 r 階，而 r 曰 A 之階級數或簡曰階數．如於 3−4 母式

---

*名此曰母式 A 之小行列式.

$$\begin{pmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 2 & 1 \\ 1 & 3 & 2 & 2 \end{pmatrix},$$

由此所得之三次行列式

$$\begin{vmatrix} 1 & 2 & 0 \\ 0 & 1 & 2 \\ 1 & 3 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 1 \\ 0 & 1 & 1 \\ 1 & 3 & 2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 0 & 1 \\ 0 & 2 & 1 \\ 1 & 2 & 2 \end{vmatrix}, \quad \begin{vmatrix} 2 & 0 & 1 \\ 1 & 2 & 1 \\ 3 & 2 & 2 \end{vmatrix}$$

雖皆爲零，然二次行列式中之不爲零者如 $\begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix}$ 尙存在也. 故此母式爲二階. 又於 n 次倍乘母式，其不爲零之倍乘數有 r 個時，則其母式爲 r 階.

定理. 凡母式，雖對之以行列式不爲零之正方母式左乘之或右乘之，於其階級不生變動.

證明. 設 P 爲 $m-n$ 母式. 若 P 之小行列式中其 $(n-l)$ 次者皆爲零，則由前節 (6)，就積 $PG_{rs\lambda}$ 言，亦復同樣. 故

$$P \text{ 之階數} \geqq PG_{rs\lambda} \text{ 之階數}.$$

然 $$P=(PG_{rs\lambda})G_{r,s,-\lambda} \quad [\text{由前節 (5)}].$$

因之與前同樣，

$$PG_{rs\lambda} \text{ 之階數} \geqq P \text{ 之階數}.$$

故 $PG_{rs\lambda}$ 之階數與 P 之階數一致. 於是若以 X 爲特殊母式 $G_{rs\lambda}$ 之積，則 PX 與 P 爲同階級.

次令 $$PX=(q_{ij}) \begin{cases} i=1,2,\cdots\cdots,m, \\ j=1,2,\cdots\cdots,n, \end{cases}$$

而以 n 次倍乘母式 $J=(\xi_i e_{ij})$ 右乘之，則得

$$\mathrm{PXJ}=(q_{ij}\xi_j)\begin{cases}i=1,2,\cdots\cdots,m,\\ j=1,2,\cdots\cdots,n.\end{cases}$$

故若$\xi_1,\xi_2,\cdots\cdots,\xi_n$之任何個皆不爲零時，則PXJ之階級與PX因之與P不得不同一也．更以Y爲特殊母式$G_{rs\lambda}$之積，則由上述，PXJY之階數與PXJ之階數一致．然行列式不爲零之正方母式，由前節系，得書之爲XJY($|J|\neq 0$)之形．故於P雖以行列式不爲零之n次母式右乘之，其階級亦不變也．又在左乘時，用前節(7)得同樣證明之．

系．正方母式，雖以行列式不爲零之母式變其形，對其階級不生變動．

定理．設P爲r階之母式，則於其左右以行列式不爲零之適當的正方母式A，B乘之，可得

$$\mathrm{APB}=\begin{pmatrix}\mathrm{E}_r & 0\\ 0 & 0\end{pmatrix}.$$

但E_r爲示r次之主母式者．

就本定理之特別情形者，再加以一言之說明．卽P爲r次之正方母式時，上式之右邊爲E_r；而P爲r行n列或m行r列時，則右邊分別爲$(\mathrm{E}_r\ 0)$或$\begin{pmatrix}\mathrm{E}_r\\ 0\end{pmatrix}$．

證明．設P爲$m-n$母式．由前節第一定理，於P之左右以適當的正方母式(行列式不爲零者)V，W乘之，則得

$$(1)\qquad \mathrm{VPW}=\mathrm{J},\ \mathrm{J}=(\xi_i e_{ij})\begin{cases}i=1,2,\cdots\cdots,m,\\ j=1,2,\cdots\cdots,n,\end{cases}$$

而由前定理, J非與P同爲r階不可. 爲此之故, 則$\xi_1, \xi_2, \cdots\cdots$之中$r$個不爲零甚明.

今定c_{ij}之值, 令

$$c_{st}=c_{ts}=1 \quad (s, t\leqq m, n),$$

$$c_{ss}=c_{tt}=0,\ c_{ii}=1 \quad (i\neq s, t),$$

而其有他之添數者皆爲零, 乃以之作m次及n次之正方母式:

$$\mathrm{C}=(c_{ij})\ (i, j=1, 2, \cdots\cdots, m);\ \mathrm{D}=(c_{ij}) \quad (i, j=1, 2, \cdots\cdots, n).$$

再以之乘於J之左右而令

$$\mathrm{CJD}=(\eta_{ij}) \quad \begin{cases} i=1, 2, \cdots\cdots, m, \\ j=1, 2, \cdots\cdots, n, \end{cases}$$

則

$$\eta_{ij}=\sum_{k, l} c_{ik}\,\xi_k\,e_{kl}\,c_{lj} \quad \begin{cases} k=1, 2, \cdots\cdots, m, \\ l=1, 2, \cdots\cdots, n. \end{cases}$$

由是

$$\eta_{sj}=c_{st}\,\xi_t\,c_{tj}=\begin{cases} \xi_t & (j=s), \\ 0 & (j\neq s); \end{cases}$$

$$\eta_{tj}=c_{ts}\,\xi_s\,c_{sj}=\begin{cases} \xi_s & (j=t), \\ 0 & (j\neq t). \end{cases}$$

而$i\neq s, t$時,

$$\eta_{ij}=c_{ii}\,\xi_i\,c_{ij}=\xi_i\,e_{ij}.$$

故J之左右分別以C, D乘之, 則ξ_s與ξ_t得以交換.* 於是將

---

* 以(c_{ij})將正方母式變形, 則其第s行與第t行得以交換, 同時第s列與第t列亦然.

此反覆行之，則能使

$$HJK=\begin{pmatrix}M_r & 0\\ 0 & 0\end{pmatrix} \tag{2}$$

而求得 m 次母式 H 及 n 次母式 K 也．但 M_r 爲示行列式不爲零之 r 次倍乘母式者．於(2)之兩邊，以正方母式

$$\begin{pmatrix}M_r^{-1} & 0\\ 0 & E_{n-r}\end{pmatrix}\quad (E_{n-r}\text{ 爲 }(n-r)\text{ 次之主母式})$$

右乘之，則有

$$HJK\begin{pmatrix}M_r^{-1} & 0\\ 0 & E_{n-r}\end{pmatrix}=\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix},$$

由此與(1)，遂得

$$HV\cdot P\cdot WK\begin{pmatrix}M_r^{-1} & 0\\ 0 & E_{n-r}\end{pmatrix}=\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix}.$$

注意． 今後 m 次之主母式概以 E_m 示之．

第二十六章　羣母式

160．羣母式．

設 $\mathfrak{G}$ 爲 g 元羣，其元素爲

$$G_0, G_1, \cdots\cdots, G_{g-1}. \tag{1}$$

若對此諸元素，分別有同次數之正方母式

$$(G_0), (G_1), \cdots\cdots, (G_{g-1}) \tag{2}$$

相與對應，* 而

---

*(2)之母式中，其相等者許其存在．

(3) $$(G_i)(G_j)=(G_i\,G_j)$$

時，則此一組之母式(2)稱曰羣 $\mathfrak{G}$ 之**母式表示**. 但 $(G_i\,G_j)$ 乃示對應於積 G_iG_j 之母式者. 卽 $G_iG_j=G_k$ 時，$(G_i\,G_j)$ 則表示 (G_k) 者也.

如第144節之例，卽四元數羣之二次母式表示也. 又

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}\sqrt{-1}&0&0\\0&-\sqrt{-1}&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&-\sqrt{-1}&0\\-\sqrt{-1}&0&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&1&0\\-1&0&0\\0&0&0\end{pmatrix},$$

$$\begin{pmatrix}-1&0&0\\0&-1&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}-\sqrt{-1}&0&0\\0&\sqrt{-1}&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&\sqrt{-1}&0\\\sqrt{-1}&0&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&-1&0\\1&0&0\\0&0&0\end{pmatrix}$$

亦表示同羣者. 母式之行列式在前例雖皆爲1，而在後例則均爲零. 又與羣之主元素相對應者，於前例爲主母式 $\begin{pmatrix}1&0\\0&1\end{pmatrix}$，於後例則爲 $\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix}$. 此後者非主母式也(第157節注意參照).

次以由 $\mathfrak{G}$ 之表示(2)與 g 個獨立變數

(4) $$x_{G_0},\ x_{G_1},\ \cdots\cdots,\ x_{G_{g-1}}$$

所作之母式

(5) $$X=(G_0)x_{G_0}+(G_1)x_{G_1}+\cdots\cdots+(G_{g-1})x_{G_{g-1}}$$
$$=\sum_R(R)x_R \qquad (R=G_0,\ G_1,\ \cdots\cdots,\ G_{g-1}),$$

名曰相應於表示(2)之**羣母式**. 而表示(2)之母式之次數

---

*正方母式(A)之行列式亦以 |A| 表之.

爲 n 時，則曰羣母式爲 n 次.

若 E 爲 $\mathfrak{G}$ 之主元素，則

$$(\mathrm{E})\mathrm{X}=\sum_{\mathrm{R}}(\mathrm{E})(\mathrm{R})x_{\mathrm{R}}=\sum_{\mathrm{R}}(\mathrm{R})x_{\mathrm{R}}=\mathbf{X},$$

因之得

$$|\mathrm{E}|\cdot|\mathrm{X}|=|\mathrm{X}|.$$

故若 $|\mathrm{E}|=0$，則 $|\mathrm{X}|$ 恆等的爲零. 反之，若 $|\mathrm{X}|$ 恆等的爲零時，則須 $|\mathrm{E}|=0$. 蓋於 (5) 以 $x_{\mathrm{E}}=1$ 而他之變數悉以爲零時，則 $\mathrm{X}=(\mathrm{E})$ 故也.

由上，若 $|\mathrm{X}|$ 不爲零，則 $|\mathrm{E}|\neq 0$，而此時 (E) 又不得不爲主母式. 蓋因 (E)(E)=(E) 之故，若以 (e_{ij}) 爲主母式，$(\mathrm{E})=(a_{ij})$，則

$$(a_{ij})(a_{ij})=(a_{ij})=(a_{ij})(e_{ij})\quad (i, j=1, 2, \cdots\cdots, n).$$

$$\therefore\ (a_{ij})\{(a_{ij})-(e_{ij})\}=0.$$

由是

$$\sum_{s=1}^{n}a_{is}(a_{sj}-e_{sj})=0\quad (i=1, 2, \cdots\cdots, n).$$

然

$$|a_{ij}|\neq 0.$$

故

$$a_{sj}-e_{sj}=0\quad (s, j=1, 2, \cdots\cdots, n).$$

卽

$$(\mathrm{E})=(e_{ij}).$$

又 $|\mathrm{X}|\neq 0$ 時，(2) 之母式之行列式，任何個皆不得爲零. 蓋若以 R 之巡回率爲 r，則 $(\mathrm{R})^r=(\mathrm{E})$，因之 $|\mathrm{R}|^r=|\mathrm{E}|=1$ 故也.

定理. 若以 $\mathrm{X}=(x_{ij})$ 爲與羣 $\mathfrak{G}(\mathrm{G}_0, \mathrm{G}_1, \cdots\cdots, \mathrm{G}_{g-1})$ 之母式表示相應之羣母式，則 X 乃有次之性質:

(i) x_{ij} 爲 $x_{G_0}, x_{G_1}, \cdots\cdots, x_{G_{g-1}}$ 之一次函數.

(ii) 同 $y_{G_0}, y_{G_1}, \cdots\cdots, y_{G_{g-1}}$ 爲他之獨立變數,而令

$$z_R = \sum_S x_S\, y_{S^{-1}R}^{*} \quad (R, S = G_0, G_1, \cdots\cdots, G_{g-1});$$

又將於 X 中以 y_R, z_R 代其變數 x_R 者分別示以 Y, Z, 則得

$$XY = Z.$$

反之,若母式 X 有上之二性質時,則此母式爲 $\mathfrak{G}$ 之羣母式.

證明. 設 X 爲相應於(2)之羣母式. 則其有(i)之性質者,由(5)自明. 其次

$$Y = \sum_R (R)\, y_R = \sum_R (S^{-1}R)\, y_{S^{-1}R}$$

$$XY = \{\sum_S (S)\, x_S\}\{\sum_R (S^{-1}R)\, y_{S^{-1}R}$$

$$= \sum_{S,R} (S)(S^{-1}R)\, x_S\, y_{S^{-1}R} = \sum_{S,R} (R)\, x_S\, y_{S^{-1}R}$$

$$= \sum_R (R) \sum_S x_S\, y_{S^{-1}R} = \sum_R (R)\, z_R = Z.$$

爲逆之證明計,乃以母式 (x_{ij}) 爲具備上條件(i)及(ii)者. 對 $\mathfrak{G}$ 之一元素 R, 令 $x_R = 1$, 而其他之變數皆令爲零,由是若以自 (x_{ij}) 所生之母式爲 (R), 則與 $\mathfrak{G}$ 之各元素相應,遂得母式

---

* $AB = C$ 時, y_{AB} 以 y_C 表之.

(6)　　$(G_0), (G_1), \cdots\cdots, (G_{g-1})$.

而由條件 (i),

$$(x_{ij})=\sum_{R}(R)\,x_R \quad (R=G_0, G_1, \cdots\cdots, G_{g-1});$$

再由條件 (ii),

$$\sum_{R}(R)\,x_R\cdot\sum_{S}(S)\,y_S=\sum_{U}(U)\,z_U,$$

但

$$z_U=\sum_{R}x_R\,y_R{}^{-1}{}_U.$$

於是，在變數 x, y 中，令 $x_R=y_S=1$，其他皆爲零，則上式之左邊爲 $(R)(S)$. 此時自其右邊而觀，若以

$$RS=T, \text{ 卽 } R^{-1}T=S,$$

則變數 z 之中 $z_T=1$，其他皆爲零. 因之 $RS=T$ 時，

$$(R)(S)=(T).$$

故 (6) 表示 $\mathfrak{G}$，隨之 $\sum_{R}(R)x_R$ 卽 (x_{ij}) 爲羣母式也.

系. 設 X_1, X_2 分別爲 r 次，s 次之正方母式，U 爲 $s-r$ 母式. 若 $X=\begin{pmatrix}X_1 & 0\\ U & X_2\end{pmatrix}$ 爲屬於一羣之羣母式，則 X_1, X_2 亦爲屬於同羣之羣母式.

證明. 設屬於羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之羣母式

$$X=\sum_{R}(R)x_R \quad (R=G_0, G_1, \cdots\cdots, G_{g-1})$$

爲具有 $\begin{pmatrix}X_1 & 0\\ U & X_2\end{pmatrix}$ 之形者. 而於 X, X_1, X_2, U，其變數 x_R 代以

y_R 者，分別以 Y, Y_1, Y_2, V 示之；其代以 z_R 者分別以 Z, Z_1, Z_2, W 示之．於是由第157節定理

$$XY=\begin{pmatrix}X_1 & 0\\ U & X_2\end{pmatrix}\begin{pmatrix}Y_1 & 0\\ V & Y_2\end{pmatrix}=\begin{pmatrix}X_1Y_1 & 0\\ UY_1+X_2V & X_2Y_2\end{pmatrix},$$

然因 X 爲羣母式之故，由上定理，

$$XY=Z=\begin{pmatrix}Z_1 & 0\\ W & Z_2\end{pmatrix}\quad (z_R=\sum_S x_S y_S{}^{-1}{}_R).$$

故

$$X_1Y_1=Z_1,\ X_2Y_2=Z_2\quad (z_R=\sum_S x_S y_S{}^{-1}{}_R).$$

因之由上定理，X_1, X_2, 共爲屬於 $\mathfrak{G}$ 之羣母式也．

161. 羣母式之同值，簡約．

凡母式，其所有之項皆常數者，曰**常數母式**．以 n 次之常數母式 A（行列式不爲零者）將屬於羣 $\mathfrak{G}$ 之 n 次羣母式 X 變形時，則由此所得之 $A^{-1}XA$ 亦爲屬於 $\mathfrak{G}$ 之羣母式．蓋若以

$$X=\sum_R (R)x_R,$$

則

$$A^{-1}XA=\sum_R \{A^{-1}(R)A\}x_R;$$

而 $(R)(S)=(T)$ 時，則

$$A^{-1}(R)A\cdot A^{-1}(S)A=A^{-1}(T)A$$

故也．後者之羣母式 $A^{-1}XA$ 名曰**與 X 同值**．就羣母式之同值言，得次之簡單定理：

(i) 羣母式 X′ 若與 X 同值，則 X 與 X′ 同值．

(ii) 兩個羣母式若與第三者同值，則兩者互同值．

(iii) 一個羣母式與其行及列施以同一置換者同值.

蓋若以第159節第二定理之證明中所用之母式(c_{ij})而變其形，則羣母式之第s行與第t行交換，同時第s列與第t列亦交換故也.

(iv) 同值之羣母式，其行列式相等，階數亦一致. (參照第159節第一定理之系.)

復次，若一羣母式X與$\begin{pmatrix} X_1 & 0 \\ U & X_2 \end{pmatrix}$形者同值時，則X名曰**可約的**. 但$X_1, X_2$，皆示正方母式者. 此時$X_1, X_2$由前節系亦爲羣母式. 非可約的羣母式名曰**既約的**. 羣之母式表示，隨其相應之羣母式爲既約或可約的，卽名曰既約或可約的.

定理. 羣母式$X'=\begin{pmatrix} X_1 & 0 \\ U & X_2 \end{pmatrix}$與羣母式$X''=\begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$爲同值. 但$X_1, X_2$爲正方母式.

證明. 若X_1, X_2之次數分別爲r, s，而

$$(1) \qquad X'=\sum_{R}(R)x_R \quad (R=G_0, G_1, \cdots\cdots, G_{g-1}),$$

則得置

$$(2) \qquad (R)=\begin{pmatrix} A_R & 0 \\ C_R & D_R \end{pmatrix} \quad (R=G_0, G_1, \cdots\cdots, G_{g-1}).$$

但A_R, D_R分別爲r次，s次之正方母式，C_R爲$s-r$母式. 茲取正方常數母式

$$P=\begin{pmatrix} E_r & 0 \\ F & E_s \end{pmatrix}.$$

但 E_r, E_s 分別爲 r 次, s 次之主母式, F 則其項未定之 $s-r$ 母式. 若對羣之各元素 R, 能示得以定一 P, 使有

$$(3) \qquad (R)P = P\begin{pmatrix} A_R & 0 \\ 0 & D_R \end{pmatrix}$$

者, 則得

$$P^{-1}X'P = \sum_R \{P^{-1}(R)P\}x_R = \sum_R \begin{pmatrix} A_R & 0 \\ 0 & D_R \end{pmatrix} x_R = \begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix},$$

而定理之爲眞可知也. 今計算(3)之左右兩邊,

$$(R)P = \begin{pmatrix} A_R & 0 \\ C_R & D_R \end{pmatrix}\begin{pmatrix} E_r & 0 \\ F & E_s \end{pmatrix} = \begin{pmatrix} A_R & 0 \\ C_R+D_RF & D_R \end{pmatrix},$$

$$P\begin{pmatrix} A_R & 0 \\ 0 & D_R \end{pmatrix} = \begin{pmatrix} E_r & 0 \\ F & E_s \end{pmatrix}\begin{pmatrix} A_R & 0 \\ 0 & D_R \end{pmatrix} = \begin{pmatrix} A_R & 0 \\ FA_R & D_R \end{pmatrix}.$$

故對羣之各元素 R, 若得定如

$$(4) \qquad C_R + D_RF = FA_R$$

者之 F, 則爲已足.

且對羣之二元素 R, S, 既有 (R)(S)=(RS), 故由(2)得次關係:

$$(5) \qquad A_RA_S = A_{RS}, \quad D_RD_S = D_{RS}.$$

$$(6) \qquad C_RA_S + D_RC_S = C_{RS}.$$

於(6)之兩邊以 A_S^{-1} 右乘之, 再就 S 而加之, 則

$$\sum_S C_RA_SA_S^{-1} + \sum_S D_RC_SA_S^{-1} = \sum_S C_{RS}A_S^{-1}$$

$$(S = G_0, G_1, \cdots\cdots, G_{g-1}).$$

由是而用(5), 則

(7)　$$gC_RA_E+D_R\cdot gF'=\sum_S C_{RS}A_S^{-1}$$

但　$$F'=\frac{1}{g}\sum_S C_SA_S^{-1},$$

而 E 爲羣之主元素. 於(7)之右邊，其 S 代以 $R^{-1}S$，因之 S^{-1} 代以 $S^{-1}R$，則

$$\sum_S C_{RS}A_S^{-1}=\sum_S C_SA_S^{-1}{}_R=\sum_S C_SA_S^{-1}A_R=gF'A_R.$$

故(7)爲

(8)　$$C_RA_E+D_RF'=F'A_R.$$

X_1 之行列式若不爲零，則如前節所述，$A_E=E_r$. 故若取 $F=F'$，則(4)之得滿足，由(8)而自明也. $|X_1|=0$ 時，若取

(9)　$$F=F'-D_EC_E,$$

則(4)遂告滿足. 示之如次：

試於(6)令 $S=E$，則

(10)　$$C_RA_E+D_RC_E=C_R.$$

右乘 A_S 於此之兩邊，則由(5)，

$$C_RA_S+D_RC_EA_S=C_RA_S.$$

$$\therefore\quad D_RC_EA_S=0\quad (R, S=G_0, G_1, \cdots\cdots, G_{g-1}).$$

故　$$FA_R=F'A_R-D_EC_EA_R=F'A_R.$$

自他方言，由(9)及(5)，

$$\begin{aligned}C_R+D_RF&=C_R+D_RF'-D_RC_E\\&=C_RA_E+D_RF' &&[\text{由 (10)}]\\&=F'A_R &&[\text{由 (8)}].\end{aligned}$$

由此與前式,則由(9)所定之F得滿足(4)可知也.

系1. 可約羣母式與$\begin{pmatrix} X_1 & 0 \\ 0 & X_2 \end{pmatrix}$形者同值. 但$X_1, X_2$爲正方母式.

系2. 設(E)爲n次r階$(r<n)$之正方母式. 若$(E)^2=(E)$時,用適當的母式以變其形,則其遂成爲$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$.

證明. 由第159節第二定理,則如

$$X(E)Y=\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \qquad [\,|X|\neq 0, |Y|\neq 0]$$

者之n次母式X, Y得以選定. 然$(E)^2=(E)$. 故

$$X(E)Y\cdot Y^{-1}(E)Y=\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}. \tag{11}$$

次令 $Y^{-1}(E)Y=\begin{pmatrix} P & Q \\ R & S \end{pmatrix}$ $\begin{bmatrix} P\text{爲}r\text{次}, S\text{爲}(n-r)\text{次} \\ \text{之正方母式} \end{bmatrix}$,

而計算其左邊

$$X(E)Y\cdot Y^{-1}(E)Y=\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} P & Q \\ R & S \end{pmatrix}=\begin{pmatrix} P & Q \\ 0 & 0 \end{pmatrix}.$$

將此與(11)之左邊比較,

$$P=E_r, \quad Q=0.$$

故 $$Y^{-1}(E)Y=\begin{pmatrix} E_r & 0 \\ R & S \end{pmatrix}.$$

然(E)之階級爲r. 故$S=0$爲必要. 卽

$$Y^{-1}(E)Y=\begin{pmatrix} E_r & 0 \\ R & 0 \end{pmatrix}.$$

自他面言，因$(E)^2=(E)$，故(E)表主元素羣，因之$\begin{pmatrix}E_r & 0\\ R & 0\end{pmatrix}x_E$爲羣母式．於是由本定理，此羣母式非與$\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix}x_E$同值不可．即得本系．

定理．屬於羣$\mathfrak{G}$之n次r階$(r<n)$之羣母式與$\begin{pmatrix}X_1 & 0\\ 0 & 0\end{pmatrix}$形之羣母式同值．但$X_1$爲示行列式非零之$r$次羣母式者．

證明．令

$$X=\sum_R(R)x_R \qquad (R=G_0, G_1, \cdots\cdots, G_{g-1}),$$

而(E)爲與$\mathfrak{G}$之主元素E相對應之母式．$|X|=0$時，則$|E|=0$(前節)．今以(E)之階數爲r，則由適當的選擇母式D，乃有

$$D^{-1}(E)D=\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix}. \tag{12}$$

但E_r爲r次之主母式．以是D變X之形，以其所得爲X'，即若令

$$D^{-1}XD=X', \tag{13}$$

則由(12)得

$$\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix}X'\begin{pmatrix}E_r & 0\\ 0 & 0\end{pmatrix}=D^{-1}(E)D\cdot D^{-1}XD\cdot D^{-1}(E)D$$
$$=D^{-1}(E)X(E)D=D^{-1}XD=X'. \tag{14}$$

又爲自他方面以計算其左邊計，乃令

$$X'=\begin{pmatrix}X_1 & U\\ V & W\end{pmatrix}.$$

但 X_1, W 分別爲 r 次, $n-r$ 次之正方母式; U 爲 r 行 $n-r$ 列, V 爲 $n-r$ 行 r 列之母式. 於是

$$\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} X_1 & U \\ V & W \end{pmatrix}\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} X_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

故由 (13) 及 (14),

$$D^{-1}XD=X'=\begin{pmatrix} X_1 & 0 \\ 0 & 0 \end{pmatrix}.$$

於此令 $x_E=1$, 其他變數皆爲零, 則由 (12) 得 $(X_1)=E_r$. 故 $|X_1|\neq 0$, 因之 X' 之階數爲 r. 最後, 因 X' 爲羣母式故, 由前節系, X_1 亦羣母式也. 故定理云云.

系. 羣母式之階數, 與羣之主元素相應母式之指標等.

證明. (12) 式右邊之指標根, 其 $(n-r)$ 個爲零, 其他皆爲 1. 故由第 147 節第一定理, (E) 之指標根亦復同樣. 故 (E) 之指標與 r 等 (參照第 147 節第一定理之系).

注意. 由本定理, 則既約羣母式之行列式不爲零. 因之與主元素相應之母式爲主母式.

例. 試取一三次亞巡回羣 (卽三次對稱羣)

$$S^3=1,\quad T^2=1,\quad ST=TS^2,$$

(參照第 101 節), 對此之 S, T, 1 分別使母式

$$(S)=\begin{pmatrix} \omega & -\omega & \omega \\ 0 & \omega^2 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix},\quad (T)=\begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 1 & -1 & 1 \end{pmatrix},\quad (E)=\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

相與對應．於是由計算自明，乃得

$$(S)^3=(E),\ (T)^2=(E),\ (S)(T)=(T)(S)^2,$$

$$(S)(E)=(E)(S)=(S),\ (T)(E)=(E)(T)=(T),\ (E)(E)=(E).$$

故其以(S)及(T)之積所作之六個母式

$$(E)=\begin{pmatrix}1&-1&1\\0&1&0\\0&1&0\end{pmatrix},\quad (S)=\begin{pmatrix}\omega&-\omega&\omega\\0&\omega^2&0\\0&\omega^2&0\end{pmatrix},\quad (S)^2=\begin{pmatrix}\omega^2&-\omega^2&\omega^2\\0&\omega&0\\0&\omega&0\end{pmatrix},$$

$$(T)=\begin{pmatrix}0&1&0\\1&-1&1\\1&-1&1\end{pmatrix},\ (T)(S)=\begin{pmatrix}0&\omega^2&0\\\omega&-\omega&\omega\\\omega&-\omega&\omega\end{pmatrix},\ (T)(S)^2=\begin{pmatrix}0&\omega&0\\\omega^2&-\omega^2&\omega^2\\\omega^2&-\omega^2&\omega^2\end{pmatrix}$$

乃表三次亞巡回羣；而其中與主元素對應者，(E)也．(E)之階級爲2．是故與上表示相應之羣母式，由本節之定理及系，不得不與$\begin{pmatrix}X_1&0\\0&0\end{pmatrix}$形者($X_1$爲二次母式)同值．實際計算以示之，乃以

$$\begin{pmatrix}1&0&-1\\0&1&0\\0&1&1\end{pmatrix}\left\{\text{其逆爲}\begin{pmatrix}1&-1&1\\0&1&0\\0&-1&1\end{pmatrix}\right\}$$

將上之母式變形，則分別得

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}\omega&0&0\\0&\omega^2&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}\omega^2&0&0\\0&\omega&0\\0&0&0\end{pmatrix},$$

$$\begin{pmatrix}0&1&0\\1&0&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&\omega^2&0\\\omega&0&0\\0&0&0\end{pmatrix},\ \begin{pmatrix}0&\omega&0\\\omega^2&0&0\\0&0&0\end{pmatrix},$$

其與是相應之羣母式之階級之爲2，明也．

定理．*n次r階之羣母式X，與次形之母式同值；*

$$\begin{pmatrix} X_1 & 0 & \cdots\cdots & 0 & 0 \\ 0 & X_2 & \cdots\cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & X_m & 0 \\ 0 & 0 & \cdots\cdots & 0 & N_{n-r} \end{pmatrix}$$

但 $X_1, X_2, \cdots\cdots, X_m$ 爲既約羣母式，N_{n-r} 爲 $(n-r)$ 次之零母式.

證明. 由本節第二定理，X 與 $\begin{pmatrix} X_1 & 0 \\ 0 & N_{n-r} \end{pmatrix}$ 同值. 但式中 X_1 爲 r 次羣母式，其行列式不爲零者. X_1 若爲既約，則定理自告成立. 反之，X_1 若爲可約的，則由第一定理系 1，得選一常數母式 P 能使

$$P^{-1}X_1P=\begin{pmatrix} X_{11} & 0 \\ 0 & X_{12} \end{pmatrix} \quad (X_{11}, X_{12} \text{ 爲正方母式}).$$

由是

$$\begin{pmatrix} P & 0 \\ 0 & E_{n-r} \end{pmatrix}^{-1}\begin{pmatrix} X_1 & 0 \\ 0 & N_{n-r} \end{pmatrix}\begin{pmatrix} P & 0 \\ 0 & E_{n-r} \end{pmatrix}=\begin{pmatrix} P^{-1}X_1P & 0 \\ 0 & N_{n-r} \end{pmatrix}=\begin{pmatrix} X_{11} & 0 & 0 \\ 0 & X_{12} & 0 \\ 0 & 0 & N_{n-r} \end{pmatrix}.$$

X_{11} 或 X_{12} 如爲可約的，則更以同樣之方法反覆之即可得本定理.

定理中之 $X_1, X_2, \cdots\cdots, X_m$ 名曰屬於羣母式 X 之既約羣母式. 此 m 個中有互爲同值者時，則其得以同一者置換之. 其互不同值者以爲

$$X_1, X_2, \cdots\cdots, X_l, \tag{15}$$

而與是同值者分別有

(16)　　$r_1, r_2, \cdots\cdots, r_l$

個時，此 r_i 名曰 X_i 之指數，將(16)之指數概括一處，則名之曰羣母式 X 之指數.

$|X| \neq 0$ 時，X 及 X_i 之行列式* 分別以 Φ, Φ_i 示之，則

(17)　　$\Phi = \Phi_1^{r_1}\Phi_2^{r_2}\cdots\cdots\Phi_l^{r_l}.$

而 $\Phi_1, \Phi_2, \cdots\cdots$，如第 163 節所證明，不得分解爲因數，故名之曰 Φ 之素因數.

又 X 之次數若爲 n，既約羣母式之次數分別爲 $f_1, f_2, \cdots\cdots, f_l$，則

(18)　　$n = r_1f_1 + r_2f_2 + \cdots\cdots + r_lf_l$

甚明.

162. 既約羣母式.

定理. 設 X, X′ 分別爲 f 次，f' 次之既約羣母式(屬於同一羣者). f 行 f' 列之常數母式 P 滿足等式 $XP = PX'$ 時，則 $P = 0$ 或 $|P| \neq 0$. 而在後者，則 X 與 X′ 同值.

證明. 設 $P \neq 0$，P 之階級爲 $r\ (>0)$. 而令 $f - r = s, f' - r = t$. 茲選擇二正方母式 A 及 B ($|A|, |B| \neq 0$) 使能滿足

(1)　　$APB = Q, \quad Q = \begin{pmatrix} E_r & N_{rt} \\ N_{sr} & N_{st} \end{pmatrix}$

者(第 159 節第二定理). 但 N_{kl} 爲 k 行 l 列之零母式. 次於

---

*羣母式之行列式單呼曰羣行列式.

等式 $XP=PX'$ 之兩邊分別以 A, B 左右乘, 則得

$$AXA^{-1}\cdot APB=APB\cdot B^{-1}X'B.$$

於是令

$$AXA^{-1}=X_1,\quad B^{-1}X'B=X'_1,$$

則得

$$X_1Q=QX'_1. \tag{2}$$

由假設, X, X' 爲既約, 故 X_1 及 X_1' 亦非爲既約不可. 更以 X_1, X'_1 書於次形:

$$X_1=\begin{pmatrix}X_{rr} & X_{rs}\\ X_{sr} & X_{ss}\end{pmatrix},\quad X'_1=\begin{pmatrix}X'_{rr} & X'_{rt}\\ X'_{tr} & X'_{tt}\end{pmatrix},\quad \left[\begin{matrix}X_{kl},\ X'_{kl}\ \text{爲}\\ k-l\ \text{母式}\end{matrix}\right],$$

而計算 (2) 之兩邊, 則

$$X_1Q=\begin{pmatrix}X_{rr} & X_{rs}\\ X_{sr} & X_{ss}\end{pmatrix}\begin{pmatrix}E_r & N_{rt}\\ N_{sr} & N_{st}\end{pmatrix}=\begin{pmatrix}X_{rr} & N_{rt}\\ X_{sr} & N_{st}\end{pmatrix},$$

$$QX'_1=\begin{pmatrix}E_r & N_{rt}\\ N_{sr} & N_{st}\end{pmatrix}\begin{pmatrix}X'_{rr} & X'_{rt}\\ X'_{tr} & X'_{tt}\end{pmatrix}=\begin{pmatrix}X'_{rr} & X'_{rt}\\ N_{sr} & N_{st}\end{pmatrix}.$$

爲此二者之相等計, 則

$$X_{sr}=0,\quad X'_{rt}=0$$

爲必要. 卽

$$X_1=\begin{pmatrix}X_{rr} & X_{rs}\\ N_{sr} & X_{ss}\end{pmatrix},\quad X_1'=\begin{pmatrix}X'_{rr} & N_{rt}\\ X'_{tr} & X'_{tt}\end{pmatrix}.$$

由此是觀, 若 $t\neq 0$, 則 X'_1 爲可約的, 與假設反也. 故不得不 $t=0$, 卽 $r=f'$. 又 $s>0$ 時, X_1 爲可約的. 蓋由前節定理 (iii), X_1 與 $\begin{pmatrix}X''_{ss} & N_{sr}\\ X''_{rs} & X''_{rr}\end{pmatrix}$ 形者同值故. 是則 $s=0$, 卽 $r=f$ 爲必要也. 夫如是, $P\neq 0$ 時, 則

$$f=f'=r\ (\mathrm{P}\text{之階數}).$$

故P爲正方母式，而其行列式不爲零.

定理. X爲f次之既約羣母式時，則與X交換可能之常數母式乃有$a\mathrm{E}_f$形. 但a爲常數.

證明. 設f次正方母式$\mathrm{P}=(p_{ij})$與X爲交換可能. 乃取x之方程式

$$|\mathrm{P}-x\mathrm{E}_f|=0$$

即

$$|p_{ij}-xe_{ij}|=0 \qquad (i,j=1,2,\cdots\cdots,f)$$

之根a，則母式$\mathrm{P}-a\mathrm{E}_f$之行列式爲零. 而對此母式，由假設則有

$$\mathrm{X}(\mathrm{P}-a\mathrm{E}_f)=\mathrm{P}-a\mathrm{E}_f)\mathrm{X}.$$

故由前定理，

$$\mathrm{P}-a\mathrm{E}_f=0,\ \text{即}\ \mathrm{P}=a\mathrm{E}_f.$$

系. 凡屬於Abel氏羣之既約羣母式之次數皆爲1. (即母式Abel氏羣，若以適當的母式變其形，則其皆爲倍乘母式).

證明. 設$\mathrm{X}=\sum_{\mathrm{R}}(\mathrm{R})x_{\mathrm{R}}$爲一個屬於Abel氏羣之既約羣母式，其次數爲$f$. 對於羣之任意一元素S，

$$(\mathrm{S})\mathrm{X}=\sum_{\mathrm{R}}(\mathrm{S})(\mathrm{R})x_{\mathrm{R}}=\sum_{\mathrm{R}}(\mathrm{R})(\mathrm{S})x_{\mathrm{R}}=\mathrm{X}(\mathrm{S}).$$

故

$$(\mathrm{S})=a_{\mathrm{S}}\mathrm{E}_f \quad (a_{\mathrm{S}}\text{爲常數}).$$

因之若$f>1$，則X爲可約的，是不合理.

定理. 設 $X=(x_{ij})$ 爲屬於 g 元羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之 f 次既約羣母式，而

$$x_{ij}=\sum_R a_{ij}^R x_R \quad (R=G_0, G_1, \cdots\cdots, G_{g-1}).$$

於是

$$(I) \qquad \sum_R a_{ij}^{R^{-1}} a_{kl}^R = \frac{g}{f} e_{il} e_{kj} \quad (i, j, k, l=1, 2, \cdots\cdots, f).$$

次以 $X'=(x'_{ij})$ 爲與 X 不同值之 f' 次既約羣母式，而

$$x'_{ij}=\sum_R b_{ij}^R x_R \quad (R=G_0, G_1, \cdots\cdots, G_{g-1}),$$

則生次之關係:

$$(II) \qquad \sum_R a_{ij}^{R^{-1}} b_{kl}^R = 0 \quad \begin{pmatrix} i, j=1, 2, \cdots\cdots, f \\ k, l=1, 2, \cdots\cdots, f' \end{pmatrix}.$$

證明. 茲將母式 (a_{ij}^R), (b_{ij}^R) 分別示以 A_R, B_R. 於是對於 $\mathfrak{G}$ 之二元素 R, S, 則

$$(3) \qquad A_R A_S = A_{RS}, \quad B_R B_S = B_{RS}.$$

乃取一有任意常數項者之 f 次正方母式 $U=(u_{ij})$, 而令

$$(4) \qquad \sum_R A_{R^{-1}} U A_R = V,$$

則對 $\mathfrak{G}$ 之任意元素 S,

$$(5) \qquad A_S V A_{S^{-1}} = \sum_R A_{SR^{-1}} U A_{RS^{-1}} = V.$$

蓋因 $G_0S^{-1}, G_1S^{-1}, \cdots\cdots, G_{g-1}S^{-1}$ 與 $G_0, G_1, \cdots\cdots, G_{g-1}$ 一致，而 SR^{-1} 爲 RS^{-1} 之逆故.

然由(3)

$$A_{g-1}A_S=A_E=E_f \quad (\text{參照前節注意}).$$

故於(5)之兩邊以A_S右乘之，則

$$A_SV=VA_S \quad (S=G_0, G_1, \cdots\cdots, G_{g-1}).$$

因之V與X爲交換可能．故

$$V=vE_f.$$

(前定理)．然V爲由(4)得以決定者，故其項爲u_{ij}之一次齊次式．於是若令

$$v=\sum_{j,k} c_{jk}u_{jk} \quad (j,k=1,2,\cdots\cdots,f),$$

則由(4)(比較兩邊之i行l列之項)，

$$\sum_R\sum_{j,k} a_{ij}^{R^{-1}}u_{jk}a_{kl}^R=(\sum_{j,k} c_{jk}u_{jk})e_{il}.$$

於此令$u_{jk}=1$，他之u皆爲零，則

$$(6) \qquad \sum_R a_{ij}^{R^{-1}}a_{kl}^R=e_{il}c_{jk}.$$

更於此令$l=i$而就$i=1,2,\cdots\cdots,f$以加之，則

$$\sum_R\sum_i a_{ij}^{R^{-1}}a_{ki}^R=\sum_i e_{ii}c_{jk}.$$

此右邊等於fc_{jk}，左邊爲

$$\sum_R\sum_i a_{ki}^Ra_{ij}^{R^{-1}}=ge_{kj} \quad [\because A_RA_{R^{-1}}=E_f].$$

故

$$ge_{kj}=fc_{jk}.$$

將此值代入(6)之右邊，即得公式(I).

爲證明公式(II)計,乃以U爲f行f'列,而令

$$\sum_{R} A_{R-1} U B_R = V$$

於是於此之兩邊以A_S, B_{S-1}左右乘之,則與前同樣知$XV = VX'$也. 然X, X'非同值. 故由前前定理,$V=0$爲必要. 因之由上式,

$$\sum_{R} \sum_{j,k} a_{ij}^{R^{-1}} u_{jk} b_{kl}^{R} = 0.$$

於此令$u_{jk}=1$,他之u皆爲零,則得公式(II).

系. 用定理中之記號,則

(III) $$\sum_{R} a_{ij}^{SR^{-1}} a_{kl}^{TR} = \frac{g}{f} a_{il}^{S} a_{kj}^{T},$$

(IV) $$\sum_{R} a_{ij}^{SR^{-1}} a_{kl}^{R} = \frac{g}{f} a_{il}^{S} e_{kj},$$

(V) $$\sum_{R} a_{ij}^{SR^{-1}} b_{kl}^{TR} = 0.$$

證明. 於公式(I),其i, k分別以r, s置換,又以a_{ir}^{S} a_{ks}^{T}乘其兩邊,而就$r, s=1, 2, \cdots\cdots, f$加之,則

$$\sum_{R} \sum_{r} a_{ir}^{S} a_{rj}^{R^{-1}} \sum_{s} a_{ks}^{T} a_{sl}^{R} = \frac{g}{f} \sum_{r} a_{ir}^{S} e_{rl} \sum_{s} a_{ks}^{T} e_{sj}.$$

然 $$\left(\sum_{r} a_{ir}^{S} a_{rj}^{R^{-1}}\right) = A_S A_R^{-1} = A_{SR^{-1}} = \left(a_{ij}^{SR^{-1}}\right),$$

而 $$\left(\sum_{s} a_{ks}^{T} a_{sl}^{R}\right) = A_T A_R = A_{TR} = \left(a_{kl}^{TR}\right),$$

故　$$\sum_{\mathrm{R}} a_{ij}^{\mathrm{SR}^{-1}} a_{kl}^{\mathrm{TR}} = \frac{g}{f} a_{il}^{\mathrm{S}} a_{kj}^{\mathrm{T}}.$$

是卽(III)也．於此令 T=E(主元素)則因 $\left(a_{kj}^{\mathrm{E}}\right)=\mathrm{E}_f=(e_{kj})$ 之故，遂得(IV).

用同樣之方法由(II)可以得(V).

163. 定理. 設 $\mathrm{X}=(x_{ij})$, $\mathrm{X}'=(x'_{ij})$, …… 爲屬於一個羣 $\mathfrak{G}$ 之既約羣母式，且其非互爲同值者．於是其作此諸羣母式之項皆爲一次的獨立.

在證明定理之先，試先就一次的獨立之意義說明之．對於 n 個變數之一次整函數 $\mathrm{L}_1, \mathrm{L}_2, \cdots\cdots, \mathrm{L}_m$，滿足方程式

$$a_1\mathrm{L}_1+a_2\mathrm{L}_2+\cdots\cdots+a_m\mathrm{L}_m=0$$

者之常數 $a_1, a_1, \cdots\cdots, a_m$ 之值，僅

$$a_1=a_2=\cdots\cdots=a_m=0$$

時，則上之 m 個一次函數，名曰**一次的獨立**．此時若函數皆爲齊次的，則 m 不得大於 n 甚明.

證明. 以 X, X' …… 之次數分別爲 $f, f', \cdots\cdots$；而對於常數 $c_{ij}, c'_{kl}, \cdots\cdots$，則方程式

$$\sum_{i,j} c_{ij}x_{ij}+\sum_{k,l} c'_{kl}x'_{kl}+\cdots\cdots=0 \qquad \begin{cases} i, j=1, 2, \cdots\cdots, f \\ k, l=1, 2, \cdots\cdots, f' \\ \cdots\cdots\cdots\cdots \end{cases}$$

爲成立者．又 $a_{ij}^{\mathrm{R}}, b_{kl}^{\mathrm{R}}, \cdots\cdots$ 爲有與前定理同樣之意義.

於是由上之等式，

$$\sum_{i,j} c_{ij} a_{ij}^{\mathrm{R}} + \sum_{k,l} c'_{kl} b_{kl}^{\mathrm{R}} + \cdots\cdots = 0.$$

於此以 $a_{st}^{\mathrm{R}^{-1}}$ 乘之，再就 $\mathrm{R} = \mathrm{G}_0, \mathrm{G}_1, \cdots\cdots, \mathrm{G}_{g-1}$ 以加之，得

$$\sum_{i,j} c_{ij} \sum_{\mathrm{R}} a_{st}^{\mathrm{R}^{-1}} a_{ij}^{\mathrm{R}} + \sum_{k,l} c'_{kl} \sum_{\mathrm{R}} a_{st}^{\mathrm{R}^{-1}} b_{kl}^{\mathrm{R}} + \cdots\cdots = 0.$$

適用公式 (I), (II), 得

$$\frac{g}{f} \sum_{i,j} c_{ij} e_{sj} e_{it} = 0.$$

$$\therefore \quad c_{ts} = 0 \qquad (s, t = 1, 2, \cdots\cdots, f).$$

又以 $b_{st}^{\mathrm{R}^{-1}}$ 乘初之方程式，而就 R 以加之，則同樣得

$$c'_{ts} = 0 \qquad (s, t = 1, 2, \cdots\cdots, f').$$

他之係數準此. 故 X, X′, …… 之項皆爲一次的獨立.

系. 設 $\mathrm{X}_1, \mathrm{X}_2, \cdots\cdots, \mathrm{X}_l$ 爲屬於羣母式 $\mathrm{X}\ (|\mathrm{X}| \neq 0)$ 之既約羣母式中之非相互同值者，其各個之次數分別爲 $f_1, f_2, \cdots\cdots, f_l$，則於 X 其一次的獨立項之個數爲 $f_1^2 + f_2^2 + \cdots\cdots + f_l^2$.

證明. X 若爲既約羣母式之直乘積時，則由本定理自明. 否則，示其互爲同直之羣母式乃有同數之一次的獨立項爲已足也. 於 n 次羣母式 $\mathrm{X} = (x_{ij})$ 其一次的獨立項爲有 v 個，且以 $x_1, x_2, \cdots\cdots, x_v$ 示之，則 X 之各項非得表之爲此各個之一次函數不可. 卽

$$x_{ij} = a_{ij}^{(1)} x_1 + a_{ij}^{(2)} x_2 + \cdots\cdots + a_{ij}^{(v)} x_v \quad (i, j = 1, 2, \cdots\cdots, n).$$

但 $a_{ij}^{(s)}$ 爲常數. 茲以他之羣母式 $\mathrm{X}' = (x'_{ij})$ 爲與 X 同值，則

x'_{ij} 爲X之項之一次函數. 故其爲 $x_1, x_1, \cdots\cdots, x_v$ 之一次函數，得表爲

$$x'_{ij}=b_{ij}^{(1)}x_1+b_{ij}^{(2)}x_2+\cdots\cdots+b_{ij}^{(v)}x_v \quad (i, j=1, 2, \cdots\cdots, n).$$

因之X′之一次的獨立項不得多於 v 個. 反之，因X與X′同值，故X之一次的獨立項不能較X′者爲多. 是則X′中一次的獨立項之個數爲 v 也.

定理. 若 $r_1, r_2, \cdots\cdots, r_l$ 爲羣母式 $X(|X|\neq 0)$ 之指數，則在與X交換可能之母式中，其一次的獨立者有 $r_1^2+r_2^2+\cdots\cdots+r_1^2$ 個.

母式之一次的獨立之意義與一次函數者全然同樣.

證明. 將X變形爲既約羣母式之直乘積. 即

$$K^{-1}XK=\begin{pmatrix} X_1 & 0 & \cdots\cdots & 0 \\ 0 & X_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & X_m \end{pmatrix}$$

當此變形時，乃取K，使

$$(1) \qquad \begin{cases} X_1=X_2=\cdots\cdots=X_{r_1} \\ X_{r_1+1}=X_{r_1+2}=\cdots\cdots=X_{r_1+r_2} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

而 $X_1, X_{r_1+1}, \cdots\cdots$ 非同值者. 再以P爲與X交換可能之母式，

則 $K^{-1}PK$ 與 $K^{-1}XK$ 爲交換可能. 令 $K^{-1}PK=Q$, 而將其書於次形:

$$Q=\begin{pmatrix} Q_{11} & Q_{12} & \cdots\cdots & Q_{1m} \\ Q_{21} & Q_{22} & \cdots\cdots & Q_{2m} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ Q_{m1} & Q_{m2} & \cdots\cdots & Q_{mm} \end{pmatrix}$$

但 Q_{ii} 爲與 X_i 同次數之正方母式, Q_{ij} 爲行數等於 X_i, 列數等於 X_j 者之母式. 因 Q 與 $K^{-1}XK$ 爲交換可能, 故由第 157 節定理,

$$X_iQ_{ij}=Q_{ij}X_j \quad (i,j=1,2,\cdots\cdots). \tag{2}$$

對於 $i,j=1,2,\cdots\cdots,r_1$, 由 (1) 則 $X_i=X_j$. 故由前節第二定理,

$$Q_{ij}=q_{ij}F_1 \quad (i,j=1,2,\cdots\cdots,r_1). \tag{3}$$

但 F_1 爲與 X_1 同次數之主母式, q_{ij} 爲常數.

$i=1,2,\cdots\cdots,r_1$; $j=r_1+1,r_2+2,\cdots\cdots,r_1+r_2$ 時, 則如上述, X_i 與 X_j 非同值. 故由前節第一定理, $Q_{ij}=0$. 同樣,

$$\begin{cases} Q_{ij}=q_{ij}F_2 \quad (i,j=r_1+1,r_1+2\cdots\cdots,r_1+r_2), \\ Q_{ij}=q_{ij}F_3 \quad (i,j=r_1+r_2+1,\cdots\cdots,r_1+r_2+r_3), \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases} \tag{3}$$

但 $F_2,F_3,\cdots\cdots$ 分別爲與 $X_{r_1+1}, X_{r_1+r_2+1},\cdots\cdots$ 同次數之主母式, q_{ij} 爲常數. 而他之 Q_{ij} 則須悉爲零母式. 卽

$$Q=\begin{pmatrix} Q_{11} \cdots\cdots Q_{1r_1} & 0 \cdots\cdots 0 & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ Q_{r_1 1} \cdots\cdots Q_{r_1 r_1} & 0 \cdots\cdots 0 & \cdots\cdots \\ 0 \cdots\cdots 0 & Q_{r_1+1,r_1+1} \cdots\cdots Q_{r_1+1,r_1+r_2} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ 0 \cdots\cdots 0 & Q_{r_1+r_2,r_1+1} \cdots\cdots Q_{r_1+r_2,r_1+r_2} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \end{pmatrix}$$

但 Q_{ij} 以(3)與之．反之，對於 q_{ij} 之任意之值，此Q之與 $K^{-1}XK$ 爲交換可能，由上之計算自明，因之於Q，以其係數之一 q_{ij} 爲1，他之係數爲零，而以是所得者示以 S_{ij}，則得

$$Q=\sum_{i,j} q_{ij} S_{ij} \begin{cases} i,j=1,2,\cdots\cdots,r_1 \\ i,j=r_1+1,\cdots\cdots,r_1+r_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots. \end{cases}$$

即Q得表之爲 $r_1^2+r_2^2+\cdots\cdots$ 個母式 S_{ij} 之一次式者也．而此諸 S_{ij} 之爲一次的獨立者甚明．然 $K^{-1}PK=Q$．故

$$P=\sum_{i,j} q_{ij} K S_{ij} K^{-1}.$$

但 S_{ij} 既爲一次的獨立，故 $KS_{ij}K^{-1}$ 亦復同樣．故定理云云．

系．在與本定理中羣母式X且與凡母式P之與X交換可能者爲交換可能之母式中，其一次的獨立者爲 l 個．

證明．採用本定理之記號，而以

$$Q'=\sum_{i,j} q'_{ij}S_{ij} \quad \begin{cases} i,j=1,2,\cdots\cdots,r_1 \\ i,j=r_1+1,\cdots\cdots,r_1+r_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

爲與Q交換可能者. (但Q中係數q_{ij},則以爲取任意之值者.) 於是以

$$QQ'=\sum_{i,j}(\sum_{s} q_{is}q'_{sj})S_{ij}, \quad Q'Q=\sum_{i,j}(\sum_{t} q'_{it}q_{tj})S_{ij}$$

之故,

$$\sum_{s} q_{is}q'_{sj}=\sum_{t} q'_{it}q_{tj} \quad \begin{cases} i,j,s,t=1,2,\cdots\cdots,r_1 \\ i,j,s,t=r_1+1,\cdots\cdots,r_1+r_2 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}.$$

茲以其一係數$q_{ij}(1\leqq i\leqq r_1)$爲1,他之係數皆爲零,則由上式,

$$q'_{jj}=0 \quad (i\neq j).$$

又以其一係數$q_{1j}(1<j\leqq r_1)$爲1,他之係數爲零,則由上式得

$$q'_{ij}=q'_{11} \quad (j=1,2,\cdots\cdots,r_1).$$

就他之係數言,同樣得

$$q'_{ij}=0\,(i\neq j),\ q'_{ij}=q'_{r_1+1,r_1+1} \quad (j=r_1+1,\cdots\cdots,r_1+r_2),$$

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

故

$$Q'=q'_{11}\sum_{i} S_{ii}+q'_{r_1+1,r_1+1}\sum_{j} S_{jj}+\cdots\cdots$$

$$(i=1,2,\cdots\cdots,r_1;\ j=r_1+1,\cdots\cdots,r_1+r_2;\ \cdots\cdots).$$

卽Q'得表之爲l個母式$\sum_{i} S_{ii}, \sum_{j} S_{jj}, \cdots\cdots$之一次式;而此諸母式之爲一次的獨立甚明. 故在與$K^{-1}XK$且與任意之Q交

換可能者之母式中，其一次的獨立者有 l 個也．故本系云云．

定理．既約羣母式之行列式不得分解爲因數．

證明．設 $X=(x_{ij})$ 爲屬於羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之 f 次既約羣母式．於是 x_{ij} 爲變數 x_R $(R=G_0, G_1, \cdots\cdots, G_{g-1})$ 之一次函數，而 f^2 個之 x_{ij}，由本節第一定理，爲一次的獨立．故吾人能使 x_{ij} 取任意所與之值而以定變數 x_R 之值也．即 $X=(x_{ij})$ 之各項得視爲獨立變數焉．因之行列式 $|x_{ij}|$ 不得表之爲 x_{ij} $(i, j=1, 2, \cdots\cdots, f)$ 之有理函數之積．而於他方，因 f^2 不能大於 g (f^2 個之項 x_{ij} 係一次的獨立故)，故變數 x_R 得表爲 x_{ij} 之一次函數．故若行列式 $|X|$ 得分解爲因數，即 $|X|=\Phi_1\Phi_2$，則因 Φ_1 及 Φ_2 之變數 x_R 得以 x_{ij} 表之之故，兩因子遂成爲 x_{ij} 之整函數．是與上述矛盾也．故云云．

164．同值之條件．

定理．行列式不爲零之兩羣母式若同值，則其行列式相等；反之，行列式相等時，則兩羣母式同值．

證明．同值羣母式之行列式相等甚明(第 161 節 iv)．至其逆之成立，則分次之二段論之．

1°．設 $X=(x_{ij})$，$X'=(x'_{kl})$ 爲屬於羣 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 之 f 次及 f' 次之既約羣母式．X 與 X′ 不同值時，則 x_{ij} 及 x'_{kl} 爲一次的獨立(前節第一定理)．故得定變數 x_R $(R=G_0, G_1, \cdots\cdots, G_{g-1})$ 之值而使

$$x_{ij}=e_{ij} \qquad (i, j=1, 2, \cdots\cdots, f),$$

$$x'_{kl}=0 \qquad (k, l=1, 2, \cdots\cdots, f')$$

也. 對此則

$$|X|=1, \quad |X'|=0$$

焉. 是故 X 與 X′ 非爲同值時,則兩者之行列式不得相等. 因之行列式若相等時,則兩者不得不爲同值.

2°. 設羣母式爲可約的,其屬於前者之既約羣母式爲 $X_1, X_2, \cdots\cdots, X_m$, 屬於後者者爲 $X'_1, X'_2, \cdots\cdots, X'_n$. 於是

$$|X|=|X_1|\cdot|X_2|\cdots\cdots|X_m|, \quad |X'|=|X'_1|\cdot|X'_2|\cdots\cdots|X'_n|.$$

故 $|X|=|X'|$ 時,

$$|X_1|\cdot|X_2|\cdots\cdots|X_m|=|X'_1|\cdot|X'_2|\cdots\cdots|X'_n|.$$

然由前節第三定理,$|X_i|, |X'_j|$ 任何個皆不能分解. 故其與 $|X_1|$ 等者不得不存在於右邊因數之中. 以之爲 $|X'_1|$, 則由 1°, X_1 與 X'_1 爲同值. 卽

$$P_1^{-1}X_1P_1=X'_1 \quad (P_1 \text{ 爲常數母式}, |P_1|\neq 0).$$

其次以 $|X_1|$ 除前式之兩邊,

$$|X_2|\cdots\cdots|X_m|=|X'_2|\cdots\cdots|X'_n|.$$

乃如前令右邊因子之與 $|X_2|$ 等者爲 $|X'_2|$, 則

$$P_2^{-1}X_2P_2=X'_2 \quad (P_2 \text{ 爲常數母式}, |P_2|\neq 0).$$

更以 $|X_2|$ 除前式之兩邊,而將同樣之方法反覆之,則知 X, X′ 中之既約羣母式之個數相等,而

$$P_m^{-1}X_mP_m=X'_m.$$

由上之結果,遂得

$$\begin{pmatrix} P_1 & 0 & \cdots\cdots & 0 \\ 0 & P_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & P_m \end{pmatrix}^{-1} \begin{pmatrix} X_1 & 0 & \cdots\cdots & 0 \\ 0 & X_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & X_m \end{pmatrix} \begin{pmatrix} P_1 & 0 & \cdots\cdots & 0 \\ 0 & P_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & P_m \end{pmatrix}$$

$$= \begin{pmatrix} P_1^{-1}X_1P_1 & 0 & \cdots\cdots & 0 \\ 0 & P_2^{-1}X_2P_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & P_m^{-1}X_mP_m \end{pmatrix} = \begin{pmatrix} X'_1 & 0 & \cdots\cdots & 0 \\ 0 & X'_2 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots\cdots & X'_m \end{pmatrix}$$

然 $\begin{pmatrix} X_1 & 0 & \cdots\cdots \\ 0 & X_2 & \cdots\cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$ 及 $\begin{pmatrix} X'_1 & 0 & \cdots\cdots \\ 0 & X'_2 & \cdots\cdots \\ \cdots & \cdots & \cdots \end{pmatrix}$ 分別與 X, X′ 同值. 故 $|X| = |X'|$ 時，則 X 與 X′ 爲同值.

165. 正羣母式，既約羣母式系.

設 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 爲 g 元羣，試就與之相應之 g 次母式

(1)　　$X = (x_{P^{-1}Q})$　$(P, Q = G_0, G_1, \cdots\cdots, G_{g-1})$

$$= \begin{pmatrix} x_{G_0^{-1}G_0} & x_{G_0^{-1}G_1} & \cdots\cdots & x_{G_0^{-1}G_{g-1}} \\ x_{G_1^{-1}G_0} & x_{G_1^{-1}G_1} & \cdots\cdots & x_{G_1^{-1}G_{g-1}} \\ \cdots & \cdots & \cdots & \cdots \\ x_{G_{g-1}^{-1}G_0} & x_{G_{g-1}^{-1}G_1} & \cdots\cdots & x_{G_{g-1}^{-1}G_{g-1}} \end{pmatrix}$$

論之. 但 x_R $(R = G_0, G_1, \cdots\cdots, G_{g-1})$ 爲示獨立變數者. 於此

令

$$x_E=1 \quad (E\text{爲}\mathfrak{G}\text{之主元素}),$$

而他之變數悉爲零,則 $X=E_g$. 故上之母式之行列式不爲零. 其次

$$XY=(x_{P^{-1}Q})(y_{P^{-1}Q})=(\sum_S x_{P^{-1}S}y_{S^{-1}Q}).$$

然

$$\sum_S x_{P^{-1}S}y_{S^{-1}Q}=\sum_S x_{P^{-1}S}y_{S^{-1}P\cdot P^{-1}Q}=\sum_S x_S y_{S^{-1}\cdot P^{-1}Q}.$$

故若令

$$z_R=\sum_S x_S y_{S^{-1}R}, \quad Z=(z_{P^{-1}Q}),$$

則 $XY=Z$. 因之 X 爲屬於$\mathfrak{G}$之羣母式(第 160 節定理),而名之曰**正羣母式**.

乃以 $X_0, X_1, \cdots\cdots, X_{k-1}$ 爲在屬於正羣母式 X 之既約羣母式中之不爲同值者,而以其次數分別爲 $f_0, f_1, \cdots\cdots, f_{k-1}$,指數爲 $e_0, e_1, \cdots\cdots, e_{k-1}$,則由第 161 節 (18),

$$(2) \qquad e_0f_0+e_1f_1+\cdots\cdots+e_{k-1}f_{k-1}=g.$$

又因 X 有 g 個之一次的獨立項 x_R $(R=G_0, G_1, \cdots\cdots, G_{g-1})$,故由第 163 節第一定理系,

$$(2) \qquad f_0^2+f_1^2+=\cdots+f^2_{k-1}=g.$$

其次試求與 X 交換可能之母式. 若以之爲

$$Y=(y_{P,Q}) \quad (P, Q=G_0, G_1, \cdots\cdots G_{g-1}),$$

則因

$$(y_{P,Q})\,(x_{P^{-1}Q})=(x_{P^{-1}Q})\,(y_{P,Q}),$$

故

$$\sum_S y_{P,S}x_{S^{-1}Q}=\sum_T x_{P^{-1}T}y_{T,Q}.$$

於此而令Q=E (𝔊之主元素)，且將右邊換書之，則得

$$\sum_{S} y_{P,S}x_S^{-1}=\sum_{T} x_T^{-1}y_{PT^{-1},E}.$$

再於此令$x_Q^{-1}=1$，他之變數爲零，則得

$$y_{P,Q}=y_{PQ^{-1}},_E.$$

故將$y_{R,E}$表以y_R，則得

$$(4)\qquad Y=(y_{PQ^{-1}})\quad (P,Q=G_0,G_1,\cdots\cdots,G_{g-1})$$

$$=\begin{pmatrix} y_{G_0G_0^{-1}} & y_{G_0G_1^{-1}} & \cdots\cdots & y_{G_0G_{g-1}^{-1}} \\ y_{G_1G_0^{-1}} & y_{G_1G_1^{-1}} & \cdots\cdots & y_{G_1G_{g-1}^{-1}} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ y_{G_{g-1}G_0^{-1}} & y_{G_{g-1}G_1^{-1}} & \cdots\cdots & y_{G_{g-1}G_{g-1}^{-1}} \end{pmatrix}$$

而對y_R ($R=G_0,G_1,\cdots\cdots,G_{g-1}$) 之任意一值，Y與X爲交換可能者，則由上之計算自明.

又因母式Y含有g個之項y_R之得取任意值者，故由第163節第二定理，則

$$(5)\qquad e^2{}_0+e^2{}_1+\cdots\cdots+e^2{}_{k-1}=g$$

爲必要. 更由此與(2)，(3)，卽得

$$(e_0-f_0)^2+(e_1-f_1)^2+\cdots\cdots+(e_{k-1}-f_{k-1})^2=0.$$

故$e_i=f_i$ ($i=0,1,2,\cdots\cdots,k-1$). 卽

定理. 屬於正羣母式者之既約羣母式之指數與其次數一致.

定理. 在屬於正羣母式之既約羣母式中,其不爲同值者之數,與羣之共軛元素系之數等.

證明. 試取母式

$$Z=(z_{P,Q}) \quad (P, Q=G_0, G_1, \cdots\cdots, G_{g-1}).$$

若此與上之正羣母式 X 爲交換可能,則由上述,

$$z_{P,Q}=z_{PQ^{-1}, E}.$$

又若 Z 與 Y 爲交換可能,則同樣

$$z_{P,Q}=z_{Q^{-1}P, E}.$$

故 Z 與 X 及 Y 爲交換可能時,

$$z_{P,Q}=z_{PQ^{-1}}=z_{Q^{-1}P}.$$

但 z_R 爲表 $z_{R,E}$ 者. 於是以 QP 置換 P, 則得

$$z_{QPQ^{-1}}=z_P.$$

即在 Z 之項 z_R $(R=G_0, G_1, \cdots\cdots, G_{g-1})$ 中,其添數共軛者,得取相等之值者也. 故 Z 之項內,其得取任意之值者之個數,與 $\mathfrak{G}$ 之共軛元素系之數等. 因之由第 163 節第二定理系,得本定理.

定理. 既約羣母式與屬於正羣母式者之一爲同值.

證明. 茲假定上述之羣 $\mathfrak{G}$, 含有與 $X_0, X_1, \cdots\cdots, X_{k-1}$ 之任何個皆不同值之既約羣母式 X_k, 則此諸羣母式中之 $f_0^2+\cdots\cdots+f^2_{k-1}+f^2_k$ 個之項皆爲一次的獨立(第 163 節第一

定理). 而由(3),

$$f^2{}_0+\cdots\cdots+f^2{}_{k-1}+f^2{}_k=g+f^2{}_k.$$

然羣母式之各項，乃 g 個之變數 x_R 之一次函數，因之一次的獨立項不得多於 g 個. 故 X_k 之存在爲矛盾. 卽不同值之羣母式之個數爲 k. 故定理云云.

由上二定理，卽得次

定理. 屬於同一羣而不爲同值之既約羣母式之數，與羣中之共軛元素系之數等.

將上記之 $X_0, X_1, \cdots\cdots, X_{k-1}$ 卽屬於羣 $\mathfrak{G}$ 之既約羣母式中之不同值者之全部括爲一組，而名之曰屬於羣 $\mathfrak{G}$ 之**既約羣母式系**. 此諸既約羣母式之行列式分別表以 $\Phi_0, \Phi_1, \cdots\cdots, \Phi_{k-1}$，則一羣母式 X' 之行列式(不爲零者)，由第161節末所述，得分解如次之素因數:

$$|X'|=\Phi_0^{r_0}\Phi_1^{r_1}\cdots\cdots\Phi_{k-1}^{r_{k-1}}.$$

但其與 X_i 同值者不含於 X' 時，則 $r_i=0$. 爲在 $r_i=0$ 時亦得適用起見，乃將第161節末之定義擴張，遂以

$$r_0,\ r_1,\ \cdots\cdots,\ r_{k-1}$$

爲一組而名之曰羣母式 X' 之**指數**. 由是，則前節定理，得換言之如次. 卽:

行列式不爲零者之羣母式之同值非同值，以其指數之一致與否而定.

羣母式X之行列式爲零時,乃以之變形爲行列式不爲零之羣母式$\overline{\mathrm{X}}$與零母式N之直乘積$\begin{pmatrix}\overline{\mathrm{X}} & 0\\ 0 & \mathrm{N}\end{pmatrix}$(第161節第一定理),而以$\overline{\mathrm{X}}$之指數定X之指數之義. 於是由X之指數,則$\overline{\mathrm{X}}$亦定. 嚴格以言之,卽謂與$\overline{\mathrm{X}}$同值之羣母式之組得定也. 而由X之次數,N可定. 故指數相等而次數一致之羣母式爲同值焉.

例. 試取三次亞巡回羣(三次對稱羣)

$$S^3=1,\ T^2=1,\ ST=TS^2.$$

其與此羣之元素

$$1,\ S,\ S^2,\ T,\ TS,\ TS^2$$

相對應之變數分別以爲

$$x_0,\ x_1,\ x_2,\ x_3,\ x_4,\ x_5,$$

則此羣之正羣母式得以

$$\mathrm{X}=\begin{pmatrix} x_0 & x_1 & x_2 & x_3 & x_4 & x_5\\ x_2 & x_0 & x_1 & x_4 & x_5 & x_3\\ x_1 & x_2 & x_0 & x_5 & x_3 & x_4\\ x_3 & x_4 & x_5 & x_0 & x_1 & x_2\\ x_4 & x_5 & x_3 & x_2 & x_0 & x_1\\ x_5 & x_3 & x_4 & x_1 & x_2 & x_0 \end{pmatrix}$$

與之. 將此用母式

$$K=\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & \omega & 0 & 0 & \omega^2 \\ 1 & 1 & \omega^2 & 0 & 0 & \omega \\ 1 & -1 & 0 & 1 & 1 & 0 \\ 1 & -1 & 0 & \omega^2 & \omega & 0 \\ 1 & -1 & 0 & \omega & \omega^2 & 0 \end{pmatrix} \quad \left[\omega=\frac{-1+\sqrt{-3}}{2}\right]$$

變其形，則得

$$K^{-1}XK=\begin{pmatrix} X_0 & 0 & 0 & 0 & 0 & 0 \\ 0 & X_1 & 0 & 0 & 0 & 0 \\ 0 & 0 & X_{21} & X_{22} & 0 & 0 \\ 0 & 0 & X_{23} & X_{24} & 0 & 0 \\ 0 & 0 & 0 & 0 & X_{21} & X_{22} \\ 0 & 0 & 0 & 0 & X_{23} & X_{24} \end{pmatrix}$$

但

$$X_0=x_0+x_1+x_2+x_3+x_4+x_5,$$

$$X_1=x_0+x_1+x_2-x_3-x_4-x_5,$$

$$X_{21}=x_0+\omega x_1+\omega^2 x_2,$$

$$X_{22}=x_3+\omega^2 x_4+\omega x_5,$$

$$X_{23}=x_3+\omega x_4+\omega^2 x_5,$$

$$X_{24}=x_0+\omega^2 x_1+\omega x_2.$$

而

$$(X_0)=(1)x_0+(1)x_1+(1)x_2+(1)x_3+(1)x_4+(1)x_5,$$

$$(X_1)=(1)x_0+(1)x_1+(1)x_2+(-1)x_3+(-1)x_4+(-1)x_5,$$

$$\begin{pmatrix} X_{21} & X_{22} \\ X_{23} & X_{24} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} x_0 + \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} x_1 + \begin{pmatrix} \omega^2 & 0 \\ 0 & \omega \end{pmatrix} x_2$$
$$+ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} x_3 + \begin{pmatrix} 0 & \omega^2 \\ \omega & 0 \end{pmatrix} x_4 + \begin{pmatrix} 0 & \omega \\ \omega^2 & 0 \end{pmatrix} x_5$$

則作既約羣母式系. 此最後者之爲既約系,因三次亞巡回羣乃由三共軛元素系而成,故由本節之兩定理自明也.

注意. 對於羣之各元素使一次主母式卽(1)相與對應,則羣由之而表示甚明. 此名曰**主表示**. 而與之相應之羣母式爲$(\sum_{R} x_R)$. 此名曰**主羣母式**. 如上例之(X_0)卽主羣母式也.

第二十七章 羣指標

166. 羣指標.

令

$$(1) \qquad (G_0), (G_1), \cdots\cdots, (G_{g-1})$$

爲羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之母式表示. 母式$(R)$之指標若以$\chi(R)$表之,則伴上表示乃得$g$個之數:

$$(2) \qquad \chi(G_0), \chi(G_1), \cdots\cdots, \chi(G_{g-1}).$$

以之爲一組,而名之曰表示(1)或羣母式

$$(3) \qquad X = \sum_{R} (R) x_R \qquad (R = G_0, G_1, \cdots\cdots, G_{g-1})$$

之相應之**羣指標**.* 例如取三次亞巡回羣,其與第161節例

---

*$\chi(G_i)$名曰元素G_i之指標(屬於表示(1)者).

所揭之表示相應之羣指標爲 $\chi(1)=2, \chi(S)=-1, \chi(S^2)=-1, \chi(T)=0, \chi(TS)=0, \chi(TS^2)=0$; 又其與正羣母式相當者，則由前節例自明爲

$$\chi(1)=6, \chi(S)=0, \chi(S^2)=0, \chi(T)=0, \chi(TS)=0, \chi(TS^2)=0.$$

一般，與 g 元羣之正羣母式相應之羣指標爲

$$g, 0, 0, \cdots\cdots, 0 \quad (\chi(1)=g).$$

蓋因正羣母式中其主對角線上之各項爲 x_E (E 爲主元素) 故.

以二羣指標言，當同一元素之指標一致時，則兩者曰相等. 如與同值羣母式相應之羣指標爲相等是. 蓋因母式雖以任何母式變其形其指標不變故也(第 147 節第一定理之系).

羣母式 $X=\sum_R(R)x_R$ 爲 n 次 f 階時，由第 161 節第二定理，能選擇一常數母式 (A) 使

$$(A)^{-1}X(A)=\begin{pmatrix} X' & 0 \\ 0 & N_{n-f} \end{pmatrix}$$

也. 但 X' 爲行列式不爲零之 f 次羣母式，N_{n-f} 爲 $(n-f)$ 次零母式. 故母式 (R) 之指標根中，有 $n-f$ 個爲零，其他不爲零者(參照第 147 節第一定理). 以後者爲 $\omega_1, \omega_2, \cdots\cdots, \omega_f$，則

$$\chi(R)=\omega_1+\omega_2+\cdots\cdots+\omega_f$$

(參照第 147 節第一定理系之證明). 觀乎此值，則由第 147 節第三定理，

$$\chi(R^m)=\omega_1{}^m+\omega_2{}^m+\cdots\cdots+\omega_f{}^m.$$

然元素R之巡回率爲m時，由第161節第二定理系之證明中所述，$\omega_1{}^m=\omega_2{}^m=\cdots\cdots=\omega_f{}^m=1$爲必要也．即謂此時$\omega_i$爲1之$m$乘根焉．特別對於主元素*E，則

$$\chi(E)=f.$$

又由上述自明

$$\chi(R^{-1})=\omega_1{}^{-1}+\omega_2{}^{-1}+\cdots\cdots+\omega_f{}^{-1},$$

即$\chi(R)$與$\chi(R^{-1})$爲共軛複素數也．

更因母式之指標與變形無關係，故若以R及S爲一羣之二元素，則

$$(VI)\qquad \chi(S^{-1}RS)=\chi(R).$$

即在一個表示中，其屬於同一共軛系之元素乃有同一之指標者也．於此公式若以SR置換R則得

$$(VI')\qquad \chi(RS)=\chi(SR).$$

如就上例之三次亞巡回羣之指標而觀，無論在任何表示，皆得

$$\chi(T^{-1}ST)=\chi(S^2)=\chi(S),\ \chi(ST)=\chi(TS^2)=\chi(TS).$$

注意．若將羣之表示(1)之母式(G_i)之各項，以其共軛複素數置換之，而以其所得者示以$(\overline{G_i})$，則

$$(\overline{G_0}),\ (\overline{G_1}),\ \cdots\cdots,\ (\overline{G_{g-1}})$$

*今後羣之主元素概以E表之．

又作羣之表示，明已．而其與是相應之指標則與相應於(1)之指標(2)分別共軛也．

167．單指標及其相關之公式．

在羣指標中其與既約表示相應者曰**單指標**，不然者曰**複指標**．而既約表示之次數爲f時，則與之相應之單指標曰f**次**．

如三次亞巡回羣之單指標，由第165節之例可知爲次之三．卽：

$$1,\quad 1,\quad 1,\quad 1,\quad 1,\quad 1,\quad [\text{與}(X_0)\text{相應者}],$$

$$1,\quad 1,\quad 1,\quad -1,\quad -1,\quad -1,\quad [\text{與}(X_1)\text{相應者}],$$

$$2,\quad -1,\quad -1,\quad 0,\quad 0,\quad 0,\quad \left[\text{與}\begin{pmatrix} X_{21} & X_{22} \\ X_{23} & X_{24}\end{pmatrix}\text{相應者}\right].$$

茲以羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之既約**羣母式系**爲

$$X_0, X_1, \cdots\cdots, X_{k-1},$$

其次數分別爲

$$f_0, f_1, \cdots\cdots, f_{k-1},$$

而與此諸羣母式相應之單指標分別爲

$$\chi_0, \chi_1, \cdots\cdots, \chi_{k-1}.$$

於是因$|X_k| \neq 0$之故，由前節末所述，

$$(1)\qquad \chi_\kappa(E)=f_\kappa \quad (\kappa=0, 1, 2, \cdots\cdots, k-1).$$

次以前節之羣母式X'之指數爲$r_0, r_1, \cdots\cdots, r_{k-1}$，則由第161節第三定理，$X'$乃與$r_0$個之$X_0$，$r_1$個之$X_1$，……，$r_{k-1}$個之

X_{k-1}之直乘積同值. 故若以相應於X′之羣指標示以χ', 則

$$\chi'(R)=r_0\chi_0(R)+r_1\chi_1(R)+\cdots\cdots+r_{k-1}\chi_{k-1}(R).$$

因之對於前節所述之n次r階之羣母式X, 則得

$$(2)\quad \chi(R)=r_0\chi_0(R)+r_1\chi_1(R)+\cdots\cdots+r_{k-1}\chi_{k-1}(R).$$

特別當X爲正羣母式時, 則由第165節第一定理, $r_\kappa=f_\kappa$, 由前節, $\chi(E)=g$, $\chi(R)=0$ $(R\neq E)$. 故若以ε_R, 當$R=E$時爲表1, $R\neq E$時爲表0者, 則由(2)得次之公式:

$$(\mathrm{VII})\quad f_0\chi_0(R)+f_1\chi_1(R)+\cdots\cdots+f_{k-1}\chi_{k-1}(R)=g\,\varepsilon_R.$$

更就單指標間之關係而觀,令

$$X_\kappa=\sum_R(a_{ij}^R)\,x_R,\quad X_\lambda=\sum_R(b_{ij}^R)\,x_R\quad (R=G_0, G_1, \cdots\cdots, G_{g-1}),$$

則

$$\chi_\kappa(R)=\sum_i a_{ii}^R,\quad \chi_\lambda(R)=\sum b_{jj}^R.$$

然由第162節公式(IV),

$$\sum_R a_{ii}^{SR^{-1}}a_{jj}^R=\frac{g}{f_\kappa}a_{ij}^S e_{ji}\quad (R=G_0, G_1, \cdots\cdots, G_{g-1}).$$

將此就i, j而加之, 則由上式,

$$(\mathrm{VIII})\qquad \sum_R\chi_\kappa(SR^{-1})\chi_\kappa(R)=\frac{g}{f_\kappa}\chi_\kappa(S).$$

於此令$S=E$(主元素), 則因$\chi_\kappa(E)=f_\kappa$之故, 遂得

$$(\mathrm{IX})\qquad \sum_R\chi_\kappa(R^{-1})\chi_\kappa(R)=g.$$

次將第162節公式(III)

$$\sum_{R} a_{ij}^{SR^{-1}} a_{ji}^{TR} = \frac{g}{f_\kappa} a_{ii}^{S} a_{jj}^{T}$$

就 j 相加，則

$$\sum_{R} a_{ii}^{SR^{-1}TR} = \frac{g}{f_\kappa} a_{ii}^{S} \sum_{j} a_{jj}^{T};$$

更以此就 i 加之，則得

$$\sum_{R} \chi_\kappa(SR^{-1}TR) = \frac{g}{f_\kappa} \chi_\kappa(S)\chi_\kappa(T).$$

換書之，則爲

$$(X) \qquad \chi_\kappa(S)\chi_\kappa(T) = \frac{f_\kappa}{g} \sum_{R} \chi_\kappa(SR^{-1}TR).$$

又用公式(V)與上同樣，得

$$(XI) \qquad \sum_{R} \chi_\kappa(SR^{-1})\chi_\lambda(R) = 0 \quad (\kappa \neq \lambda),$$

$$(XII) \qquad \sum_{R} \chi_\kappa(R^{-1})\chi_\lambda(R) = 0 \quad (\kappa \neq \lambda).$$

將公式(X)之兩邊就 κ 加之，更適用(VII)，則

$$\sum_{\kappa=0}^{k-1} \chi_\kappa(S)\chi_\kappa(T) = \sum_{R} \varepsilon_{SR^{-1}TR}.$$

若適合 $SR^{-1}TR = E$，即 $S = R^{-1}T^{-1}R$ 之元素 R 不存在於 $\mathfrak{G}$ 時，換言之，即 S 與 T^{-1} **不共軛時，則上式之右邊爲零.** 故此時

$$(XIII) \qquad \sum_{\kappa} \chi_\kappa(S)\chi_\kappa(T) = 0 \quad (\kappa = 0, 1, 2, \cdots\cdots, k-1).$$

反之，若 S 與 T^{-1} 屬於同一共軛元素系，而此共軛系由 g_S 個之元素而成時，則滿足 $S = R^{-1}T^{-1}R$ 之元素 R 在 $\mathfrak{G}$ 中有 g/g_S

個存在(第29節定理). 故此時得

$$\sum_{\kappa}\chi_{\kappa}(S)\chi_{\kappa}(T)=\frac{g}{g_S}.$$

然若令 $S=U^{-1}T^{-1}U$, 則由公式(VI),

$$\chi_{\kappa}(T)=\chi_{\kappa}(US^{-1}U^{-1})=\chi_{\kappa}(S^{-1}).$$

故

$$(XIV)\qquad \sum_{\kappa}\chi_{\kappa}(S)\chi_{\kappa}(S^{-1})=\frac{g}{g_S}\quad(\kappa=0,1,2,\cdots\cdots,k-1).$$

今以 $\mathfrak{C}_0,\mathfrak{C}_1,\cdots\cdots,\mathfrak{C}_{k-1}$ 爲 $\mathfrak{G}$ 中共軛元素系(參照第165節第四定理),而以在與既約羣母式 X_{κ} 相應之羣指標中之 $\mathfrak{C}_{\tau}$ 之一元素之指標爲 $\chi_{\kappa}^{(\tau)}$, 則由公式(VI), $\mathfrak{C}_{\tau}$ 之元素皆有此指標也. 故與 X_{κ} 相應之羣指標,其各元素之指標不必全行記出,而得以屬於各共軛之指標

$$(3)\qquad \chi_{\kappa}^{(0)},\ \chi_{\kappa}^{(1)},\ \cdots\cdots,\ \chi_{\kappa}^{(k-1)}$$

與之焉. $\chi_{\kappa}^{(\tau)}$, 便宜上遂呼曰共軛系 $\mathfrak{C}_{\tau}$ 之指標(與 X_{κ} 相應者). 又屬於 $\mathfrak{C}_{\tau}$ 之元素之逆作一共軛系. 此系之指標以 $\overline{\chi}_{\kappa}^{(\tau)}$ 表之,而屬於 $\mathfrak{C}_{\tau}$ 之元素之個數以爲 g_{τ}, 則公式(IX)換書之,遂爲

$$(IX')\qquad \sum_{\tau}g_{\tau}\chi_{\kappa}^{(\tau)}\overline{\chi}_{\kappa}^{(\tau)}=g\quad(\tau=0,1,2,\cdots\cdots,k-1).$$

次將公式(X)換書之,乃以 $\mathfrak{C}_{\tau}$ 之元素 T 之正常化羣爲 $\mathfrak{T}$, 則其元數爲 g/g_{τ}. 將 $\mathfrak{G}$ 就 $\mathfrak{T}$ 分爲傍系,而以之爲

$$\mathfrak{G}=\mathfrak{T}Q_0+\mathfrak{T}Q_1+\cdots\cdots+\mathfrak{T}Q_{\nu-1}\qquad(\nu=g_{\tau}),$$

則當元素 R 屬於 $\mathfrak{T}Q_i$ 時,

$$\chi_\kappa(SR^{-1}TR)=\chi_\kappa(SQ_i^{-1}TQ_i).$$

故

$$\sum_R \chi_\kappa(SR^{-1}TR)=\frac{g}{g_\tau}\sum_{i=0}^{\nu-1}\chi_\kappa(SQ_i^{-1}TQ_i).$$

因之，若以 S 所屬之共軛系爲 $\mathfrak{C}_\sigma$，則(X)得換書如次：

$$(X')\quad g_\tau\chi_\kappa^{(\sigma)}\chi_\kappa^{(\tau)}=f_\kappa\sum_i\chi_\kappa(SQ_i^{-1}TQ_i)\quad(i=0,1,2,\cdots\cdots,\nu-1)$$

$$=f_\kappa\sum_i\chi_\kappa(ST_i).$$

但 $T_0, T_1, \cdots\cdots$ 爲表 $\mathfrak{C}_\tau$ 之元素者.

復次在既約羣母式 X_λ 之相應之羣指標中，其共軛系 $\mathfrak{C}_\tau$ 之指標以爲 $X_\lambda^{(\tau)}$，則公式(XII)得換書如次：

$$(XII')\qquad \sum_\tau g_\tau\overline{\chi}_\kappa^{(\tau)}\chi_\lambda^{(\tau)}=0\quad(\kappa\neq\lambda)$$

$$(\tau=0,1,2,\cdots\cdots,k-1).$$

又(XIII)及(XIV)分別得表之如下：

$$(XIII')\qquad \sum_\kappa\chi_\kappa^{(\sigma)}\overline{\chi}_\kappa^{(\tau)}=0\quad(\sigma\neq\tau).$$

$$(XIV')\qquad \sum_\kappa\chi_\kappa^{(\tau)}\overline{\chi}_\kappa^{(\tau)}=\frac{g}{g_\tau}\quad(\kappa=0,1,2,\cdots\cdots,k-1).$$

又對以單指標所作之行列式，則由最後兩式得

$$(4)\quad|\chi_\kappa^{(\tau)}|\neq0,\ |\overline{\chi}_\kappa^{(\tau)}|\neq0,\quad(\kappa,\tau=0,1,2,\cdots\cdots,k-1).$$

蓋因

$$|\chi_\kappa^{(\tau)}|\cdot|\overline{\chi}_\kappa^{(\tau)}|=\left|\sum_\kappa\chi_\kappa^{(\sigma)}\overline{\chi}_\kappa^{(\tau)}\right|\quad(\sigma,\tau=0,1,2,\cdots\cdots,k-1)$$

$$=\left|\frac{g}{g_\tau}e_{\sigma\tau}\right|=\frac{g^k}{g_0g_1\cdots\cdots g_{k-1}}$$

故也.

注意. 與主羣母式 $\sum_{R} x_R$ 相應之指標爲 $1, 1, \cdots\cdots, 1$. 名之曰**主羣指標**. 於公式(XIII), 若取主羣指標以爲 χ_κ, 則 χ_λ 非主羣指標時, 爰得

$$\sum_{R} \chi_\lambda(R) = 0.$$

168. 定理. 既約羣母式之次數爲羣之元數之約數.

證明. 將公式(VIII)換書之, 則

$$\sum_{R} \chi_\kappa(SR^{-1})\, \chi_\kappa(R) = \frac{g}{f_\kappa} \sum_{R} \chi_\kappa(R)\, \varepsilon_{SR^{-1}}.$$

$$\therefore \quad \sum_{R} \chi_\kappa(R) \left\{ \frac{g}{f_\kappa} \varepsilon_{SR^{-1}} - \chi_\kappa(SR^{-1}) \right\} = 0.$$

於是令 $S = G_0, G_1, \cdots\cdots, G_{g-1}$, 則得關於

$$\chi_\kappa(G_0), \chi_\kappa(G_1), \cdots\cdots, \chi_\kappa(G_{g-1})$$

之一次齊次方程式. 然 $\chi_\kappa(E) = f_\kappa \neq 0$. 故此聯立方程式之行列式須爲

$$\left| \frac{g}{f_\kappa} \varepsilon_{SR^{-1}} - \chi_\kappa(SR^{-1}) \right| = 0 \quad (S, R = G_0, G_1, \cdots\cdots, G_{g-1}).$$

即 $\frac{g}{f_\kappa}$ 爲 g 次方程式

$$| x\varepsilon_{SR^{-1}} - \chi_\kappa(SR^{-1}) | = 0$$

之根也. 然指標爲1之冪根之和, 因之, 此方程式之係數爲代數的整數. 故此根 $\frac{g}{f_\kappa}$ 亦非爲代數的整數不可. 自他方

言，$\frac{g}{f_\kappa}$ 爲有理數．因之，$\frac{g}{f_\kappa}$ 不得不爲有理整數也.*

定理．兩個羣母式，當其次數一致而指標相等時，且只限於此時爲同值.

證明．以羣母式 X 之次數爲 n，其指數爲 $r_0, r_1, \cdots\cdots, r_{k-1}$．於是與 X 相應之羣指標得以前節 (2) 與之．此之兩邊乘以 $\chi_\kappa(R^{-1})$ 再就 R 而加之，則由 (IX) 及 (XII)，得

$$\sum_R \chi(R)\chi_\kappa(R^{-1}) = g r_\kappa \quad (\kappa = 0, 1, 2, \cdots\cdots, k-1).$$

然單指標乃與羣相應而定者．故由上式觀，X 之指數由其指標 χ 而定．因之指標相等之羣母式，其指數一致也．於是由第 165 節末所述，遂得本定理.

系．行列式不爲零之羣母式，只在其指標相等時而且唯此時爲同值.

定理．若 χ 爲與 f 次既約羣母式相應之單指標．則 $g_R\chi(R)/f$ 爲代數的整數．但 g_R 爲示與 R 共軛元素之個數者.

證明．若 $\mathfrak{C}_\tau, g_\tau$ 爲有前節中同一之意義者，而在 f 次既約羣母式 X 相應之單指標中，其共軛系 $\mathfrak{C}_\tau$ 之指標示以 $\chi^{(\tau)}$，則由公式 (X′) 得

---

* $a_1, a_2, a_3\cdots\cdots, a_n$ 爲代數的整數時，則方程式 $x^n + a_1x^{n-1} + \cdots\cdots + a_n = 0$ 之根亦爲代數的整數，又代數的整數，同時又爲有理數者，則此爲有理整數．是二者之證明姑皆從略.

$$(1)\qquad g_\tau\chi^{(\sigma)}\chi^{(\tau)}=f\sum_i\chi(\mathrm{ST}_i)\quad(i=0,1,2,\cdots\cdots,g_\tau-1).$$

但 $\mathrm{T}_0,\mathrm{T}_1,\cdots\cdots$ 爲 $\mathfrak{C}_\tau$ 之元素. 次以 $\mathrm{S}_0,\mathrm{S}_1,\cdots\cdots$ 爲 S 所屬之共軛系 $\mathfrak{C}_\sigma$ 之元素, 則由上式

$$g_\tau\chi^{(\sigma)}\chi^{(\tau)}=f\sum_i\chi(\mathrm{S}_j\mathrm{T}_i)\quad(j=0,1,2,\cdots\cdots,g_\sigma-1).$$

將此等加之, 則得

$$g_\sigma g_\tau\chi^{(\sigma)}\chi^{(\tau)}=f\sum_{i,j}\chi(\mathrm{S}_j\mathrm{T}_i)\begin{cases}i=0,1,2,\cdots\cdots,g_\tau-1,\\ j=0,1,2,\cdots\cdots,g_\sigma-1.\end{cases}$$

在 $g_\sigma g_\tau$ 個元素 $\mathrm{S}_j\mathrm{T}_i$ 之中, 以其屬於共軛系 $\mathfrak{C}_\rho$ 者之個數爲 $g_{\sigma\tau\rho}$, 則

$$\sum_{i,j}\chi(\mathrm{S}_j\mathrm{T}_i)=\sum_\rho g_{\sigma\tau\rho}\chi^{(\rho)}\quad(\rho=0,1,2,\cdots\cdots,k-1).$$

故

$$g_\sigma g_\tau\chi^{(\sigma)}\chi^{(\tau)}=f\sum_\rho g_{\sigma\tau\rho}\chi^{(\rho)}.$$

於是令

$$(2)\qquad \frac{g_{\sigma\tau\rho}}{g_\rho}=a_{\sigma\tau\rho},$$

則換書之, 得

$$(3)\qquad \frac{g_\sigma\chi^{(\sigma)}}{f}\cdot\frac{g_\tau\chi^{(\tau)}}{f}=\sum_\rho a_{\sigma\tau\rho}\frac{g_\rho\chi^{(\rho)}}{f}\quad(\rho=0,1,2,\cdots\cdots,k-1).$$

此卽(1)之所換書者也.

若已知 $a_{\sigma\tau\rho}$ 之值而解(3), 則如次. 以任意之數 a_σ 乘(3)之兩邊而就 σ 以相加, 則得

$$\xi\frac{g_\tau\chi^{(\tau)}}{f}=\sum_{\rho,\sigma}a_\sigma a_{\sigma\tau\rho}\frac{g_\rho\chi^{(\rho)}}{f},$$

但

$$\xi=\sum_\sigma a_\sigma\frac{g_\sigma\chi^{(\sigma)}}{f}\quad(\sigma=0,1,2,\cdots\cdots,k-1).$$

將上式換書之，得

$$\sum_{\rho}\left(\sum_{\sigma}a_{\sigma}a_{\sigma\tau\rho}-\xi e_{\tau\rho}\right)\frac{g_{\rho}\chi^{(\rho)}}{f}=0 \quad (\tau=0,1,2,\cdots\cdots,k-1).$$

由此以消去 $g_{\rho}\chi^{(\rho)}/f$，則

$$(4) \qquad \left|\sum_{\sigma}a_{\sigma}a_{\sigma\tau\rho}-\xi e_{\tau\rho}\right|=0 \quad (\tau,\rho=0,1,2,\cdots\cdots,k-1).$$

解之，即得 ξ，於是令 $a_0, a_1, \cdots\cdots, a_{k-1}$ 順次爲1，他爲零，則得 $g_{\rho}\chi^{(\rho)}/f$ $(\rho=0,1,2,\cdots\cdots,k-1)$. (因此方程式之次數爲 k，故恰得 k 組之單指標.)

然 $a_{\sigma\tau\rho}$ 如下所說乃爲整數. 故 $a_0, a_1, \cdots\cdots, a_{k-1}$ 爲整數時，(4) 之根 ξ 爲代數的整數. 因之 $g_{\rho}\chi^{(\rho)}/f$ 爲代數的整數. 即得本定理.

茲以共軛系 $\mathfrak{C}_{\rho}$ 之元素爲

$$\mathrm{R},\ \mathrm{P}_1^{-1}\mathrm{R}\mathrm{P}_1,\ \cdots\cdots,\ \mathrm{P}_{\mu-1}^{-1}\mathrm{R}\mathrm{P}_{\mu-1} \quad (\mu=g_{\rho}),$$

而以對於 $\mathfrak{C}_{\sigma}$ 之元素 S，$\mathfrak{C}_{\tau}$ 之元素 T，其

$$\mathrm{S}\mathrm{T}=\mathrm{R}$$

之解法爲 $(\mathrm{S}', \mathrm{T}')$, $(\mathrm{S}'', \mathrm{T}'')$, ……，則 $(\mathrm{P}_i^{-1}\mathrm{S}'\mathrm{P}_i, \mathrm{P}_i^{-1}\mathrm{T}'\mathrm{P}_i)$, $(\mathrm{P}_i^{-1}\mathrm{S}''\mathrm{P}_i, \mathrm{P}_i^{-1}\mathrm{T}''\mathrm{P}_i)$, …… 之任何個皆爲 $\mathrm{S}\mathrm{T}=\mathrm{P}_i^{-1}\mathrm{R}\mathrm{P}_i$ 之解法也. 而 $(\mathrm{S}', \mathrm{T}')$ 與 $(\mathrm{S}'', \mathrm{T}'')$ 相異時，則 $(\mathrm{P}_i^{-1}\mathrm{S}'\mathrm{P}_i, \mathrm{P}_i^{-1}\mathrm{T}'\mathrm{P}_i)$ 之與 $(\mathrm{P}_i^{-1}\mathrm{S}''\mathrm{P}_i, \mathrm{P}_i^{-1}\mathrm{T}''\mathrm{P}_i)$ 亦互異自明. 故 $g_{\sigma\tau\rho}$ 爲 g_{ρ} 之合數. 即 $a_{\sigma\tau\rho}$ 爲整數也.

169. 決定單指標之方程式.

一羣之單指標，既以之爲相應於既約羣母式者而定

其義,且由之而導出與之相關之若干公式矣. 在此諸公式之中其能表示單指標之特性者,換言之,即離開母式表示而充分得定單指標之義者,實爲(VI), IX),(X)之三焉. 即次

定理. 對於羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之元素R,一數$\chi(R)$相與對應,而其間有次之關係:

$$\text{(i)} \qquad \chi(S^{-1}TS)=\chi(T),$$

$$\text{(ii)} \qquad g\chi(S)\chi(T)=f\sum_{R}\chi(SR^{-1}TR) \quad f>0$$

$$(R=G_0, G_1, \cdots\cdots, G_{g-1}),$$

$$\text{(iii)} \qquad g=\sum_{R}\chi(R)\chi(R^{-1}) \quad (R=G_0, G_1, \cdots\cdots, G_{g-1})$$

成立時,則單指標得以

$$\chi(G_0), \chi(G_1), \cdots\cdots, \chi(G_{g-1})$$

與之.

證明. 先於(ii)令T=E(主元素),則對$\mathfrak{G}$之任意元素S,

$$g\chi(S)\chi(E)=fg\chi(S).$$

然由(iii), $\chi(R)$ $[R=G_0, G_1, G_2, \cdots\cdots, G_{g-1}]$之中有不爲零者存在. 故由上式得

$$\chi(E)=f.$$

次以單指標$\chi_\kappa(T^{-1})$乘(ii)之兩邊而就T以相加,則

$$g\chi(S)\sum_{T}\chi(T)\chi_\kappa(T^{-1})=f\sum_{T,R}\chi(SR^{-1}TR)\chi_\kappa(T^{-1})$$

$$(T, R=G_0, G_1, \cdots\cdots, G_{g-1}).$$

然由公式(VI), $\chi_\kappa(T^{-1})=\chi_\kappa(R^{-1}T^{-1}R)$. 故

$$\sum_T \chi(SR^{-1}TR)\chi_\kappa(T^{-1})=\sum_T \chi(SR^{-1}TR)\chi_\kappa(R^{-1}T^{-1}R)=\sum_T \chi(ST)\chi_\kappa(T^{-1}).$$

因之前式遂爲

$$g\chi(S)\sum_T \chi(T)\chi_\kappa(T^{-1})=fg\sum_T \chi(ST)\chi_\kappa(T^{-1}).$$

乃以 fg 除之，得

$$(1)\qquad \frac{\chi(S)}{f}\sum_T \chi(T)\chi_\kappa(T^{-1})=\sum_T \chi(ST)\chi_\kappa(T^{-1}).$$

次以 $\chi(T^{-1})$ 乘公式(X)之兩邊，而就 T 以相加且用(i)，則與上同樣，

$$(2)\qquad \frac{\chi_\kappa(S)}{f_\kappa}\sum_T \chi_\kappa(T)\chi(T^{-1})=\sum_T \chi_\kappa(ST)\chi(T^{-1}).$$

但

$$\chi_\kappa(E)=f_\kappa.$$

於此右邊以 TS 置換 T^{-1}，則得

$$\sum_T \chi_\kappa(ST)\chi(T^{-1})=\sum_T \chi_\kappa(T^{-1})\chi(TS)=\sum_T \chi_\kappa(T^{-1})\chi(ST)$$

[由(i)].

故由(1), (2),

$$\left\{\frac{\chi(S)}{f}-\frac{\chi_\kappa(S)}{f_\kappa}\right\}\sum_T \chi(T)\chi_\kappa(T^{-1})=0.$$

然如後所示，能使左邊之第二因子不爲零而得選擇適當的單指標 χ_κ 也. 故對此單指標則

$$\frac{\chi(S)}{f}=\frac{\chi_\kappa(S)}{f_\kappa}$$

爲必要. 更由是，則有

$$\sum_{S}\frac{\chi(S)\chi(S^{-1})}{f^2}=\sum_{S}\frac{\chi_\kappa(S)\chi_\lambda(S^{-1})}{f_\kappa^2}\quad(S=G_0, G_1, \cdots\cdots, G_{g-1}).$$

於是適用(iii)及公式(IX),

$$f^2=f_\kappa^2.$$

然f, f_κ共爲正數. 故

$$f=f_\kappa, \text{ 因之 } \chi(S)=\chi_\kappa(S).$$

卽χ與單指標χ_κ一致也.

最後請就$\sum_{T}\chi(T)\chi_\kappa(T^{-1})$不爲零者之單指標$\chi_\kappa$爲存在之點一示. 與前前節同樣,以$\mathfrak{G}$之共軛元素系爲$\mathfrak{C}_0, \mathfrak{C}_1, \cdots\cdots, \mathfrak{C}_{k-1}$,而$\mathfrak{C}_\tau$爲由$g_\tau$個元素而成,則由(i),對於同一共軛系中之元素,以同一數χ相與對應;又由(VI),則屬於同一共軛系之元素乃有同一之指標. 故若以與$\mathfrak{C}_\tau$之元素相應之數爲$\chi^{(\tau)}$,其指標爲$\chi_\kappa^{(\tau)}$則得

$$\sum_{T}\chi(T)\chi_\kappa(T^{-1})=\sum_{\tau=0}^{k-1}g_\tau\chi^{(\tau)}\overline{\chi}_\kappa^{(\tau)}.$$

然如前前節末之所示,

$$|\overline{\chi}_\kappa^{(\tau)}|\neq 0\quad(\kappa, \tau=0, 1, 2, \cdots\cdots, k-1).$$

故若以對所有之單指標皆爲有

$$\sum_{\tau=0}^{k-1}g_\tau\chi^{(\tau)}\overline{\chi}_\kappa^{(\tau)}=0\qquad(\kappa=0, 1, 2, \cdots\cdots, k-1)$$

者,則非得

$$g_\tau\chi^{(\tau)}=0\qquad(\tau=0, 1, 2, \cdots\cdots, k-1)$$

卽

$$\chi(T)=0\qquad(T=G_0, G_1, \cdots\cdots, G_{g-1})$$

不可也. 然此與條件(iii)矛盾. 因之如

$$\sum_{T}\chi(T)\chi_{\kappa}(T^{-1})\neq 0$$

者之單指標必定存在.

系. Abel氏羣之單指標,得以次之關係:

$$\chi(S)\chi(T)=\chi(ST),\ \chi(E)=1$$

決定.

證明. 在Abel氏羣, 因 $S^{-1}TS=T$ 之故, 定理之(i)式不需要也. 而(ii)式則爲

(3) $g\chi(S)\chi(T)=fg\chi(ST)$, 卽 $\chi(S)\chi(T)=f\chi(ST)$.

於是令 $T=S^{-1}$, 再就S而加之, 則得

$$\sum_{S}\chi(S)\chi(S^{-1})=fg\chi(E).$$

故(iii)式爲

(4) $$1=f\chi(E).$$

本式與(3)卽決定Abel氏羣之單指標者也. 更於(3)令 $S=T=E$, 則 $\{\chi(E)\}^2=f\chi(E)$, 由此與(4)得

(5) $$f=1,\quad \chi(E)=1.$$

因之(3)爲

(6) $$\chi(S)\chi(T)=\chi(ST).$$

反之, 由此式與 $\chi(E)=1$ 卽能導出(3)與(4)甚明. 故系云云.

Abel氏羣之一元素S之巡回率爲 n 時,

$$\{\chi(S)\}^n=\chi(S^n)=\chi(E)=1.$$

故 $\chi(S)$ 爲 1 之 n 乘根. 此則由 Abel 氏羣之既約羣母式皆爲一次的亦自明也(參照第162節第二定理之系),

例. 設 $[A_1, A_2, \cdots\cdots, A_m]$ 爲 Abel 氏羣之底,其各母元素之巡回率分別爲 $a_1, a_2, \cdots\cdots, a_m$. 以 ω_i 爲 1 之 a_i 乘原根,乃取

$$1, \omega_i, \omega^2{}_i, \cdots\cdots, \omega_i{}^{a_i-1}$$

中之任意一個 η_i 而對羣之元素 $A_1{}^{\alpha_1}A_2{}^{\alpha_2}\cdots\cdots A_m{}^{\alpha_m}$ 使 $\eta_1{}^{\alpha_1}\eta_2{}^{\alpha_2}\cdots\cdots\eta_m{}^{\alpha_m}$ 相與對應,則此諸數得滿足本系之二條件. 因此諸數卽得與吾人以羣指標者也. 然此等羣指標之取法有 $a_1a_2\cdots\cdots a_m$ 種. 故由之遂得羣之全部之羣指標焉.

170. 求單指標之例.

Frobenius 氏定羣指標之義時,皆以前節之方程式 (i), (ii), (iii) 而爲之者也. 是中 (i) 乃示屬於同一共軛系之元素之指標爲相等者. 故若以 $\mathfrak{C}_\tau$, g_τ, $\chi^{(\tau)}$ 爲其有前節中同一之意義者時,則如第167節所述,羣之單指標得以

$$\chi^{(0)}, \chi^{(1)}, \cdots\cdots, \chi^{(k-1)} \quad [k \text{ 爲共軛元素之個數}]$$

與之. 且如同節所述, (iii) 與 (ii) 分別得換書如 (IX'), (X') 形,卽

$$(1) \qquad g=\sum_\tau g_\tau \chi^{(\tau)}\overline{\chi}^{(\tau)} \qquad (\tau=0, 1, 2, \cdots\cdots, k-1),$$

$$(2) \qquad g_\tau \chi^{(\sigma)}\chi^{(\tau)}=f\sum_i \chi(ST_i) \quad (i=0, 1, 2, \cdots\cdots, g_\tau-1).$$

但 S 屬於共軛系 $\mathfrak{C}_\sigma$; $T_0, T_1, \cdots\cdots$ 爲 $\mathfrak{C}_\tau$ 之元素. 由 Frobenius 氏定義直接以求單指標,則由此兩方程式爲便利.

例 1. 四角羣.

羣	共軛系	g_τ	指　標
1	$\mathfrak{C}_0$	1	$\chi^{(0)}=f$
$(ac)(bd)=\mathrm{P}^2$	$\mathfrak{C}_1$	1	$\chi^{(1)}=\overline{\chi}^{(1)}$
$(ab)(cd)=\mathrm{QP}$, $(ad)(bc)=\mathrm{QP}^3$	$\mathfrak{C}_2$	2	$\chi^{(2)}=\overline{\chi}^{(2)}$
$(abcd)=\mathrm{P}$, $(adcb)=\mathrm{P}^3$	$\mathfrak{C}_3$	2	$\chi^{(3)}=\overline{\chi}^{(3)}$
$(bd)=\mathrm{Q}$, $(ac)=\mathrm{QP}^2$	$\mathfrak{C}_4$	2	$\chi^{(4)}=\overline{\chi}^{(4)}$

先由(2)乃得次式:

(i)　$\chi^{(1)}\chi^{(1)}=f\chi(\mathrm{P}^2\mathrm{P}^2)=f\chi(1)=f^2$,

(ii)　$2\chi^{(2)}\chi^{(2)}=f\{\chi(\mathrm{QPQP})+\chi(\mathrm{QPQP}^3)\}$

$=f\{\chi(1)+\chi(\mathrm{P}^2)\}=f\{f+\chi^{(1)}\}$,

(iii)　$2\chi^{(3)}\chi^{(3)}=f\{\chi(\mathrm{PP})+\chi(\mathrm{PP}^3)\}$

$=f\{\chi(\mathrm{P}^2)+\chi(1)\}=f\{f+\chi^{(1)}\}$,

(iv)　$2\chi^{(4)}\chi^{(4)}=f\{\chi(\mathrm{QQ})+\chi(\mathrm{QQP}^2)\}$

$=f\{\chi(1)+\chi(\mathrm{P}^2)\}=f\{f+\chi^{(1)}\}$,

(v)　$2\chi^{(2)}\chi^{(3)}=f\{\chi(\mathrm{QPP})+\chi(\mathrm{QPP}^3)\}$

$=f\{\chi(\mathrm{QP}^2)+\chi(\mathrm{Q})\}=2f\chi^{(4)}$.

次因 $\overline{\chi}^{(\tau)}=\chi^{(\tau)}$, 故用(i)乃至(iv), 而由(1), 則

(vi)　$8=2f^2+3f(f+\chi^{(1)})$.

且由(i), $\chi^{(1)}=\pm f$. $\chi^{(1)}=-f$ 時, 由(ii), (iii), (iv), 得

$$\chi^{(2)}=\chi^{(3)}=\chi^{(4)}=0.$$

而由 (vi), $f=2$. 又 $\chi^{(1)}=f$ 時, 由 (vi), $f=1$, 而由 (ii), (iii), (iv),

$$(\chi^{(2)})^2=(\chi^{(3)})^2=(\chi^{(4)})^2=1.$$

於是參酌(v), 遂得次之結果:

f	$\chi^{(0)}$	$\chi^{(1)}$	$\chi^{(2)}$	$\chi^{(3)}$	$\chi^{(4)}$
1	1	1	1	1	1
1	1	1	1	−1	−1
1	1	1	−1	1	−1
1	1	1	−1	−1	1
2	2	−2	0	0	0

例 2. 四面體羣(四次交代羣*).

羣	共軛系	g_τ	指標
1	$\mathfrak{C}_0$	1	$\chi^{(0)}=f$
$(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$	$\mathfrak{C}_1$	3	$\chi^{(1)}=\overline{\chi}^{(1)}$
(bcd), (acb), (cad), (dab)	$\mathfrak{C}_2$	4	$\chi^{(2)}=\overline{\chi}^{(3)}$
(bdc), (abc), (cda), (dba)	$\mathfrak{C}_3$	4	$\chi^{(3)}=\overline{\chi}^{(2)}$

* 參照第 30 節例.

(i)　$3\chi^{(1)}\chi^{(1)}=f\{\chi(1)+\chi[(ad)(bc)]+\chi[(ac)(bd)]\}$

$=f\{f+2\chi^{(1)}\}$,

(ii)　$4\chi^{(2)}\chi^{(2)}=f\{\chi[(bdc)]+\chi[(cda)]+\chi[(dba)]+\chi[(abc)]\}$

$=4f\chi^{(3)}$,

(iii)　$4\chi^{(3)}\chi^{(3)}=4f\chi^{(2)}$,

(iv)　$4\chi^{(2)}\chi^{(3)}=f\{\chi(1)+\chi[(ab)(cd)]+\chi[(ac)(bd)]$

$+\chi[(ad)(bc)]\}$

$=f\{f+3\chi^{(1)}\}$,

(v)　$12=f^2+3\chi^{(1)}\chi^{(1)}+4\chi^{(2)}\chi^{(3)}+4\chi^{(3)}\chi^{(2)}$

$=4f^2+8f\chi^{(1)}$.

將 (i) 就 $\chi^{(1)}$ 解之，得 $\chi^{(1)}=f,-\frac{f}{3}$. $\chi^{(1)}=f$ 時，以之代入 (v) 得 $f=1$. 因之 (ii), (iii), (iv) 爲

$$\chi^{(2)}\chi^{(2)}=\chi^{(3)},\ \chi^{(3)}\chi^{(3)}=\chi^{(2)},\ \chi^{(2)}\chi^{(3)}=1.$$

解之得

$$(\chi^{(2)},\chi^{(3)})=(1,1),\ \left(\frac{-1+\sqrt{-3}}{2},\ \frac{-1-\sqrt{-3}}{2}\right),$$

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

復次 $\chi^{(1)}=-\frac{f}{3}$ 時，將此值代入 (v) 得 $f=3$，又代入 (iv) 則 $\chi^{(2)}\chi^{(3)}=0$. 然由 (ii), (iii), $\chi^{(2)}$, $\chi^{(3)}$ 之一個爲零時，則他方亦須爲零. 故 $\chi^{(2)}=\chi^{(3)}=0$. 上之結果以表示之則如次：

f	$\chi^{(0)}$	$\chi^{(1)}$	$\chi^{(2)}$	$\chi^{(3)}$
1	1	1	1	1
1	1	1	$\frac{-1+\sqrt{-3}}{2}$	$\frac{-1-\sqrt{-3}}{2}$
1	1	1	$\frac{-1-\sqrt{-3}}{2}$	$\frac{-1+\sqrt{-3}}{2}$
3	3	−1	0	0

例 3. 二十面體羣(五次交代羣).

茲取五文字 0, 1, 2, 3, 4 之交代羣. 此中巡回率 3 之元素作一共軛系. 蓋因五次交代羣爲三重可遷之故,置換(012)得變形爲任意之三項巡回置換故也. 又巡回率 2 之元素亦作一共軛系. 此則因二十面體羣中之 2 元約羣作一共軛系故(參照第 60 節). 再次,則巡回率 5 之元素得分爲兩個共軛系. 良由如第 60 節所述 5 元約羣作一共軛系,而於 5 元約羣 $\{(01234)\}$, 雖

$$[(14)(23)]^{-1}(01234)[(14)(23)]=(01234)^4,$$

然將 (01234) 變形爲 $(01234)^2$ 或 $(01234)^3$ 者, 如第 100 節所述, 乃奇數置換 (1243) 或 (1342), 是不含於交代羣者也. 故巡回率 5 之元素得分爲與 (01234) 共軛者及與此之自乘共軛者之二組焉.

又屬於二十面體羣之元素之巡回率爲 2, 3 及 5. 故由

上記遂得次表：

共軛系	共軛系之代表	g_τ	指標
$\mathfrak{C}_0$	1	1	$\chi^{(0)}=f$
$\mathfrak{C}_1$	(01)(23)	15	$\chi^{(1)}=\overline{\chi}^{(1)}$
$\mathfrak{C}_2$	(012)	20	$\chi^{(2)}=\overline{\chi}^{(2)}$
$\mathfrak{C}_3$	(01234)	12	$\chi^{(3)}=\overline{\chi}^{(3)}$
$\mathfrak{C}_4$	(02413)	12	$\chi^{(4)}=\overline{\chi}^{(4)}$

由此以求單指標，則如次表：

f	$\chi^{(0)}$	$\chi^{(1)}$	$\chi^{(2)}$	$\chi^{(3)}$	$\chi^{(4)}$
1	1	1	1	1	1
3	3	−1	0	$\frac{1+\sqrt{5}}{2}$	$\frac{1-\sqrt{5}}{2}$
3	3	−1	0	$\frac{1-\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$
4	4	0	1	−1	−1
5	5	−1	−1	0	0

171. 商之羣指標. 以

(1)　　$(G_0), (G_1), \cdots\cdots, (G_{g-1})$

爲羣$\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$之母式表示. 此表示之次數若爲$n$, 階數爲$f$, 則如第161節第二定理之證明中所示, 對於如

$$D^{-1}(E)D=\begin{pmatrix} E_f & 0 \\ 0 & N_{n-f} \end{pmatrix} \quad \begin{bmatrix} E\text{爲羣之主元素,} \\ E_f\text{爲}f\text{次主母式} \end{bmatrix}$$

者之母式D, 則

$$D^{-1}(R)D=\begin{pmatrix} R_f & 0 \\ 0 & N_{n-f} \end{pmatrix} \quad [R\text{爲}(1)\text{之一母式}]$$

因之若將表示(1)相應之羣指標示以χ, 則

$$\chi(E)=f,\ \chi(R)=\omega_1+\omega_2+\cdots\cdots+\omega_f.$$

但ω_i爲母式R_f之指標根, 因之卽1之冪根(參照第166節). 故若

$$\chi(R)=\chi(E),$$

則

$$\omega_1=\omega_2=\cdots\cdots=\omega_f=1$$

爲必要也.* 因之由第162節第二定理系得選f次母式K而使

$$K^{-1}R_fK=E_f.$$

與是相應, 乃有

$$\begin{pmatrix} K & 0 \\ 0 & N_{n-f} \end{pmatrix}^{-1} D^{-1}(R)\, D\begin{pmatrix} K & 0 \\ 0 & N_{n-f} \end{pmatrix}=\begin{pmatrix} E_f & 0 \\ 0 & N_{n-f} \end{pmatrix},$$

---

*若以$\omega_1+\omega_2+\cdots\cdots+\omega_f=f$, 則$|\omega_1+\omega_2+\cdots\cdots+\omega_f|=f$.

若ω_1與和$\omega_2+\cdots\cdots+\omega_f$之偏角相異時, 則

$|\omega_1+\omega_2+\cdots\cdots+\omega_f|<|\omega_1|+|\omega_2+\cdots\cdots+\omega_f|\leqq|\omega_1|+|\omega_2|+\cdots\cdots+|\omega_f|=f$,

是與假設反也. 故兩者之偏角須相等. 然偏角相等之二數之和欲爲正之實數, 則偏角不得不爲零. 故$\omega_1=1$. 因之$\omega_2+\cdots\cdots+\omega_f=f-1$. 由是同樣得$\omega_2=1, \cdots\cdots, \omega_f=1$焉.

$$\begin{pmatrix} K & 0 \\ 0 & N_{n-f} \end{pmatrix}^{-1} D^{-1}(E)\, D \begin{pmatrix} K & 0 \\ 0 & N_{n-f} \end{pmatrix} = \begin{pmatrix} E_f & 0 \\ 0 & N_{n-f} \end{pmatrix}.$$

由此兩式遂得

$$(R)=(E).$$

反之 $(R)=(E)$ 時，則 $\chi(R)=\chi(E)$ 甚明.

今在羣之元素中以適合 $\chi(R)=\chi(E)$ 者爲

$$H_0, H_1, \cdots\cdots, H_{h-1} \qquad (H_0=E), \tag{2}$$

則表此諸元素之母式（(1) 的）

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

由上述皆與 (E) 等；又凡等於 (E) 者則均含於此中. 故此諸母式成羣，而此羣卽表示 (1) 之主元素羣也. 因之 (2) 乃作 $\mathfrak{G}$ 之正常約羣焉（參照第 43 節）. 此約羣名曰 $\mathfrak{H}$，而就之分 $\mathfrak{G}$ 爲傍系，而以其爲

$$\mathfrak{G}=\mathfrak{H}S_0+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{\nu-1},$$

則得

$$(H_rS_i)=(H_r)(S_i)=(E)(S_i)=(S_i). \tag{3}$$

因之

$$\chi(H_rS_i)=\chi(S_i) \quad \begin{cases} r=0, 1, 2, \cdots\cdots, h-1, \\ i=0, 1, 2, \cdots\cdots, \nu-1. \end{cases}$$

於是得次

定理. 若 χ 爲與羣之一表示相應之羣指標時，則滿足 $\chi(R)=\chi(E)$ 者之羣之元素 R 相集，乃作一正常約羣. 而對關於此正常約羣而相合同之二元素 R 及 S，則 $\chi(R)=\chi(S)$.

復次於上若 $S_iS_j \equiv S_k \pmod{\mathfrak{H}}$, 卽 $S_iS_j = H_sS_k$, 則由 (3),

$$(S_i)(S_j) = (S_iS_j) = (H_sS_k) = (S_k).$$

故母式

$$(4) \qquad (S_0), (S_1), \cdots\cdots, (S_{\nu-1})$$

表示商

$$\frac{\mathfrak{G}}{\mathfrak{H}}: \quad S_0, S_1, \cdots\cdots, S_{\nu-1} \pmod{\mathfrak{H}}$$

者也. 而與 (4) 相應之羣指標 ($\mathfrak{G}/\mathfrak{H}$ 者) 爲

$$\chi(S_0), \chi(S_1), \cdots\cdots, \chi(S_{\nu-1}).$$

因之得

定理. 對羣指標 χ, 以其滿足 $\chi(R) = \chi(E)$ 者之元素之集合爲 $\mathfrak{H}$, 則其羣指標屬於商 $\mathfrak{G}/\mathfrak{H}$.

爲討論此定理之逆計, 乃以 (2) 爲羣 $\mathfrak{G}$ 之正常約羣, 以 (4) 爲商 $\mathfrak{G}/\mathfrak{H}$ 之母式表示, 卽 $S_iS_j \equiv S_k \pmod{\mathfrak{H}}$ 時 $(S_i)(S_j) = (S_k)$ 者. 茲對 $\mathfrak{H}$ 之任意元素 H, 令

$$(5) \qquad (HS_i) = (S_i) \qquad (i = 0, 1, 2, \cdots\cdots, \nu-1),$$

將此母式與 $\mathfrak{G}$ 之元素 HS_i 相應, 則因

$$H_rS_i \cdot H_sS_j = H_tS_k \text{ 卽 } S_iS_j \equiv S_k \pmod{\mathfrak{H}}$$

時,

$$(H_rS_i)(H_sS_j) = (S_i)(S_j) = (S_k) = (H_tS_k),$$

故 g 個之母式

$$(6) \qquad (H_rS_i) \begin{cases} r = 0, 1, 2, \cdots\cdots, h-1, \\ i = 0, 1, 2, \cdots\cdots, \nu-1 \end{cases}$$

表示 $\mathfrak{G}$ 也．而與是相應之 $\mathfrak{G}$ 之羣指標，則爲

$$\chi(\mathrm{H}_r\mathrm{S}_i)\quad\begin{cases}r=0,\,1,\,2,\,\cdots\cdots,\,h-1,\\ i=0,\,1,\,2,\,\cdots\cdots,\,\nu-1.\end{cases}$$

在此諸數之中，其

$$\chi(\mathrm{S}_0),\ \chi(\mathrm{S}_1),\ \cdots\cdots,\ \chi(\mathrm{S}_{\nu-1})$$

分別爲母式(4)之指標．卽此乃與吾人以表示(4)相應之 $\mathfrak{G}/\mathfrak{H}$ 之羣指標者也．爰得

定理．商 $\mathfrak{G}/\mathfrak{H}$ 之羣指標屬於 $\mathfrak{G}$ 之羣指標．

茲欲使 $\mathfrak{G}/\mathfrak{H}$ 之羣指標與 $\mathfrak{G}$ 之羣指標更爲明瞭起見，乃令

$$(7)\quad x_{\mathfrak{H}\mathrm{S}_i}=x_{\mathrm{H}_0\mathrm{S}_i}+x_{\mathrm{H}_1\mathrm{S}_i}+\cdots\cdots+x_{\mathrm{H}_{h-1}\mathrm{S}_i}\quad(i=0,\,1,\,2,\,\cdots\cdots,\,\nu-1).$$

於是則其與 $\mathfrak{G}$ 之表示(6)相應之羣母式，由(5)，爲

$$(8)\qquad \sum_i(\mathrm{S}_i)\,x_{\mathfrak{H}\mathrm{S}_i}\qquad(i=0,\,1,\,2,\,\cdots\cdots,\,\nu-1).$$

此卽不外乎在與表示(4)相應之商 $\mathfrak{G}/\mathfrak{H}$ 之羣母式

$$(9)\qquad \Sigma(\mathrm{S}_i)x_{\mathrm{S}_i}\quad(i=0,\,1,\,2,\,\cdots\cdots,\,\nu-1)$$

中以 $x_{\mathfrak{H}\mathrm{S}_i}$ 代其變數 x_{S_i} 者而已也．因之若(9)爲可約的，則(8)亦然．又於 $x_{\mathfrak{H}\mathrm{S}_i}$ $(i=0,\,1,\,2,\,\cdots\cdots,\,\nu-1)$ 令 x_{S_i} 以外之變數皆爲零，則(8)成(9)．故若(8)爲可約的，則(9)亦爾．以故(8)與(9)或共爲旣約，或共爲可約焉．

例．試取四面體羣(前節例2)以爲 $\mathfrak{G}$，而取 $\mathfrak{H}=\mathfrak{C}_0+\mathfrak{C}_1$，

則

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}(bcd)+\mathfrak{H}(bdc).$$

故由該例之表卽知$\mathfrak{G}/\mathfrak{H}$之羣指標爲

$$\begin{array}{ccc} 1 & 1 & 1 \\ 1 & \dfrac{-1+\sqrt{-3}}{2} & \dfrac{-1-\sqrt{-3}}{2} \\ 1 & \dfrac{-1-\sqrt{-3}}{2} & \dfrac{-1+\sqrt{-3}}{2}. \end{array}$$

又若羣之單指標爲已知時,則由本節定理,所有之正常約羣皆可求得. 如四角羣(前節例1)之正常約羣(除主元素羣及羣自身)由該例之表觀之,知爲

$$\mathfrak{C}_0+\mathfrak{C}_1+\mathfrak{C}_2 \quad \text{卽} \quad 1, P^2, QP, QP^3;$$

$$\mathfrak{C}_0+\mathfrak{C}_1 \quad \text{卽} \quad 1, P^2$$

之二. 又就二十面體羣之羣指標而觀,在前節例3之表中,其指標與$\chi^{(0)}$等者,僅存於第一行之

$$\chi^{(0)}=\chi^{(1)}=\chi^{(2)}=\chi^{(3)}=\chi^{(4)}=1;$$

而與是相應之正常約羣則爲$\mathfrak{C}_0+\mathfrak{C}_1+\mathfrak{C}_2+\mathfrak{C}_3+\mathfrak{C}_4$,卽羣自身,故二十面體羣爲單純的.

最後就一次之羣指標一言. 上記之母式(4),由(3)自明,不外乎自$\mathfrak{G}$之表示(1)之母式中取出其互異者而已也. 故母式(1)作一與$\mathfrak{G}/\mathfrak{H}$爲單純同態之羣焉. 特別,當此表示爲一次時,則母式(1)爲Abel氏羣,因之$\mathfrak{G}/\mathfrak{H}$亦復同樣. 故此時$\mathfrak{H}$非含$\mathfrak{G}$之換位羣不可(第42節第二定理). 於是,羣

除主羣母式$\sum_{R} x_R$以外，含有一次羣母式時，則換位羣爲眞約羣，因之其羣爲複合的也．如就四次交代羣之羣指標之表（前節例2）而觀，其一次者除屬於$\sum_{R} x_R$者外有二組．且無論其爲何，皆$\chi^{(0)}=\chi^{(1)}=1$，因之滿足$\chi(R)=1$者之元素爲屬於$\mathfrak{C}_0, \mathfrak{C}_1$者，卽

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

是．此四元素所作之羣，由上述含有換位羣．是與第42節所例示者一致也．

第二十八章　羣指標之應用

172. $p^\alpha q^\beta$元羣之可解性．

設R爲g元羣$\mathfrak{G}$之一元素，μ爲對R之巡回率m互素之任意整數，則冪R^μ之正常化羣與R之正常化羣一致.* 故R所屬之共軛系由g_ρ個之元素而成時，則就R^μ所屬之共軛系言，亦復如是．因之於f次之單指標χ，其$\frac{g_\rho \chi(R^\mu)}{f}$爲代數的整數也（第168節第三定理）．以故相乘積

$$\left(\frac{g_\rho}{f}\right)^{\varphi(m)} \prod_{\mu} \chi(R^\mu)$$

---

*蓋因$A^{-1}RA=R$時，$A^{-1}R^\mu A=R^\mu$．反之，$A^{-1}R^\mu A=R^\mu$時，則$A^{-1}R^{\mu x}A=R^{\mu x}$．因之若取滿足$\mu x\equiv 1 \pmod{m}$之$x$，則得$A^{-1}RA=R$．故與R爲交換可能之元素之集合，卽R之正常化羣乃與R^μ之正常化羣一致也．

亦代數的整數. 但μ爲在$0, 1, 2, \cdots\cdots m-1$中對於$m$互素之全部之值[其個數爲$\varphi(m)$]. 然自他方言,

$$\chi(\mathrm{R})=\omega_1+\omega_2+\cdots\cdots+\omega_f, \quad \chi(\mathrm{R}^\mu)=\omega_1{}^\mu+\omega_2{}^\mu+\cdots\cdots+\omega_f{}^\mu.$$

但$\omega_1, \omega_2, \cdots\cdots, \omega_f$爲1之$m$乘根, 卽1之$m$乘原根$\omega$之冪. 故$\prod_\mu \chi(\mathrm{R}^\mu)$雖以$\omega^\lambda$(1之$m$乘原根之任意者)置換$\omega$, 而其值不變. 故其不得不爲有理數.* 然$\chi(\mathrm{R}^\mu)$乃代數的整數. 故$\prod_\mu \chi(\mathrm{R}^\mu)$非爲有理整數不可. 由是$\left(\frac{g_\rho}{f}\right)^{\varphi(m)}\prod_\mu \chi(\mathrm{R}^\mu)$既爲有理數, 而同時如上所述又爲代數的整數, 是則須爲有理整數也. 以故若特別g_ρ對f互素時, 則$\prod_\mu \chi(\mathrm{R}^\mu)$定得以$f^{\varphi(m)}$整除. 因之

$$\prod_\mu \left|\frac{\chi(\mathrm{R}^\mu)}{f}\right| = \left|\frac{\prod_\mu \chi(\mathrm{R}^\mu)}{f^{\varphi(m)}}\right| = \text{有理整數}.$$

然 $$|\chi(\mathrm{R}^\mu)| \leqq |\omega_1{}^\mu| + |\omega_2{}^\mu| + \cdots\cdots + |\omega_f{}^\mu| = f.$$

故爲前式之成立計, 則須

$$|\chi(\mathrm{R}^\mu)| = 0 \text{ 或 } f;$$

而爲後者計, 則

$$\omega_1=\omega_2=\cdots\cdots=\omega_f$$

爲必要.† 卽在與單指標χ相應之旣約表示中, 其表元素R者之母式(R)之指標根皆相等也.

---

*證明從略, 參考代數學自明.

†此之證明與第171節中之腳註同.

更就此母式(R)而觀，若以適當的母式K變其形，則成爲相似母式(指標根相等故)．即

$$K^{-1}(R)K=\omega_1 E_f.$$

由是　　$$(R)=K\cdot\omega_1 E_f\cdot K^{-1}=\omega_1 E_f.$$

即(R)爲相似母式也。因之得次之結果.

定理．若某一個共軛系之元素數對一個既約表示之次數互素時，則與此表示相應之該共軛系之指標或爲零；或於此表示中其表該共軛系之元素者之母式，任何個皆爲相似的.

原來相似母式與任意之母式爲交換可能．故本定理之後部生起時，則該既約表示遂含自己共軛母式，因之羣當然不得爲單純的．Burnside氏考查$p^\alpha q^\beta$元羣之單複時，乃利用此點而得次之結果.

定理．p,q爲互異之素數時，則$p^\alpha q^\beta$元羣爲複合的，因之爲可解的.

證明．將$p^\alpha q^\beta$元羣$\mathfrak{G}$之元素分爲共軛系，而以之爲$\mathfrak{G}_0$，$\mathfrak{G}_1$，……，$\mathfrak{G}_{k-1}$；其各個所含之元素之數則以爲g_0,g_1，……，g_{k-1}．於是

$$g_0+g_1+\cdots\cdots+g_{k-1}=p^\alpha q^\beta,$$

而g_p爲$p^\alpha q^\beta$之約數．若以$\mathfrak{G}_0$爲由主元素而成者，則$g_0=1$，因之

$$1+g_1+\cdots\cdots+g_{k-1}\equiv 0 \pmod{q}.$$

故在g_1，……，g_{k-1}之中其對q互素者非存在不可也．以之

爲 g_1, 卽 $g_1=p^\gamma$. $\gamma=0$ 時, $g_1=1$, 因之 $\mathfrak{C}_1$ 之元素爲自己共軛. 故此時羣爲複合的. 於是吾人僅就 $\gamma>0$ 者論之.

次以 $X_0, X_1, \cdots\cdots, X_{k-1}$ 爲 $\mathfrak{G}$ 之既約羣母式系, 其次數分別爲 $f_0, f_1, \cdots\cdots, f_{k-1}$. 於是

$$f^2{}_0+f^2{}_1+\cdots\cdots+f^2{}_{k-1}=p^\alpha q^\beta \quad \text{(參照第 165 節)},$$

而 f_σ 爲 $p^\alpha q^\beta$ 之約數 (第 168 節第一定理). 以 X_0 爲 $\mathfrak{G}$ 之主羣母式 (參照第 165 節注意), 則 $f_0=1$, 因之

$$1+f^2{}_1+\cdots\cdots+f^2{}_{k-1}\equiv 0 \pmod{p}.$$

故在 $f_1, \cdots\cdots, f_{k-1}$ 之中, 其對 p 互素者非存在不可. 以之爲 $f_1, \cdots\cdots, f_l$, 卽

$$f_1=q^{\delta_1}, \cdots\cdots, f_l=q^{\delta_l},$$

而

$$f_{l+1}=pf'_{l+1}, \cdots\cdots, f_{k-1}=pf'_{k-1}.$$

$\delta_1, \cdots\cdots, \delta_l$ 中有等於零者時, 如 $\delta_1=0$, 則 $f_1=1$, 於是, 羣除主羣母式以外含有一次之羣母式, 因之由前節末所述爲複合的. 以故僅就 $\delta_1, \cdots\cdots, \delta_l$ 皆大於零者而論之焉.

與既約羣母式 X_σ 相應之羣指標示以 χ_σ, 其中共軛系 $\mathfrak{C}_1$ 之元素之指標示以 $\chi_\sigma{}^{(1)}$, 則

$$\sum_{\sigma=0}^{k-1} f_\sigma \chi_\sigma{}^{(1)}=1+q^{\delta_1}\chi_1{}^{(1)}+\cdots+q^{\delta_l}\chi_l{}^{(1)}+p\left(f'_{l+1}x_{l+1}^{(1)}+\cdots+f'_{k-1}\chi_{k-1}^{(1)}\right).$$

故若 $\chi_1{}^{(1)}, \cdots\cdots, \chi_l{}^{(1)}$ 皆爲零, 則

$$\sum_\sigma f_\sigma \chi_\sigma{}^{(1)}=1+p\mathrm{N} \quad (\mathrm{N} \text{ 爲代數的整數}).$$

然由 (XIII),

$$\sum_{\sigma} f_\sigma \chi_\sigma^{(1)} = \sum_{\sigma} \chi_\sigma^{(0)} \chi_\sigma^{(1)} = 0.$$

故非

$$1+p\mathrm{N}=0$$

不可．是不合理．蓋此時分數$\frac{1}{p}$等於代數的整數$-\mathrm{N}$故．因之指標$\chi_1^{(1)}, \cdots\cdots, \chi_l^{(1)}$之中必有不爲零者在也．以其一爲$\chi_1^{(1)}$，則因其次數$f_1$對$g_1$互素之故，由前定理，則羣不得不爲複合的焉．

173. 羣之指標與約羣之指標之關係．

設

$$\mathfrak{H}: \quad \mathrm{H}_0, \mathrm{H}_1, \cdots\cdots, \mathrm{H}_{h-1}$$

爲g元羣$\mathfrak{G}$之約羣，而

$$(1) \qquad \mathfrak{G}=\mathfrak{H}\mathrm{S}_0+\mathfrak{H}\mathrm{S}_1+\cdots\cdots+\mathfrak{H}\mathrm{S}_{n-1} \quad (\mathrm{S}_0=\mathrm{E}=1).$$

於是$\mathfrak{G}$之正羣母式得以次形與之：

$$(2) \qquad \begin{pmatrix} \mathrm{X}_{00} & \mathrm{X}_{01} & \cdots\cdots & \mathrm{X}_{0,\,n-1} \\ \mathrm{X}_{10} & \mathrm{X}_{11} & \cdots\cdots & \mathrm{X}_{1,\,n-1} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \mathrm{X}_{n-1,\,0} & \mathrm{X}_{n-1,\,1} & \cdots\cdots & \mathrm{X}_{n-1,\,n-1} \end{pmatrix}$$

但

$$\mathrm{X}_{ij}=(x_{\mathrm{A}-1\mathrm{B}}) \quad \begin{cases} \mathrm{A}=\mathrm{H}_0\mathrm{S}_i, \mathrm{H}_1\mathrm{S}_i, \cdots\cdots, \mathrm{H}_{h-1}\mathrm{S}_i, \\ \mathrm{B}=\mathrm{H}_0\mathrm{S}_j, \mathrm{H}_1\mathrm{S}_j, \cdots\cdots, \mathrm{H}_{h-1}\mathrm{S}_j. \end{cases}$$

然由(1)

$$\mathfrak{G}=\mathrm{S}_0^{-1}\mathfrak{H}+\mathrm{S}_1^{-1}\mathfrak{H}+\cdots\cdots+\mathrm{S}_{n-1}^{-1}\mathfrak{H}.$$

故於變數x_R之中以其R不屬於$\mathfrak{H}$者悉以爲零，則得

$$\mathrm{X}_{0i}=0, \quad \mathrm{X}_{i0}=0 \qquad (i=1, 2, \cdots\cdots, n-1).$$

因之上之正羣母式(2)之行列式遂等於

$$|X_{00}|\cdot|X_{ij}| \qquad (i,j=1,2,\cdots\cdots,n-1).$$

此中 X_{00} 之爲 $\mathfrak{H}$ 之正羣母式甚明.

今將 $\mathfrak{G}$ 及 $\mathfrak{H}$ 之正羣母式之行列式分別示以 $\Theta(x)$, $H(x)$, 且以之分解爲素因數:

$$\Theta(x)=\prod_{\kappa}\Phi_{\kappa}^{f_\kappa} \qquad (\kappa=0,1,2,\cdots\cdots,k-1),$$

(3)

$$H(x)=\prod_{\lambda}\Psi_{\lambda}^{e_\lambda} \qquad (\lambda=0,1,2,\cdots\cdots,l-1).*$$

但 Φ_0 及 Ψ_0 乃分別爲表主羣母式之行列式者, 因之 $f_0=e_0=1$. 然對不屬於 $\mathfrak{H}$ 之元素 R 令 $x_R=0$, 則如上述, $H(x)$ 遂爲 $\Theta(x)$ 之約數. 故此時

$$\Phi_\kappa=\prod_{\lambda}\Psi_{\lambda}^{r_{\lambda\kappa}} \qquad (\lambda=0,1,2,\cdots\cdots,l-1). \tag{4}$$

特別, $\Phi_0=\Psi_0$. 故

$$r_{00}=1, \quad r_{\lambda 0}=0 \qquad (\lambda=0,1,2,\cdots\cdots,l-1). \tag{5}$$

且於行列式不爲零之 m 次羣母式 (x_{ij}), 以 x_E+u 代其 x_E, 則得 $(x_{ij}+ue_{ij})$, (因如第160節所述, 在行列式不爲零之羣母式 $(x_{ij})=\Sigma(R)x_R$ 中, (E) 爲主母式故也.) 而此之行列式之展開中 u^{m-1} 之係數爲

$$\sum_{i=1}^{m}x_{ii}=\sum_{R}x(R)x_R.$$

---

*k 及 l 乃分別爲 $\mathfrak{G}$ 及 $\mathfrak{H}$ 中共軛元素系之個數.

但 X 爲示屬於 (x_{ij}) 之羣指標者．故若以與 Φ_κ 相應之 $\mathfrak{G}$ 之羣指標爲 χ_κ，又以與 Ψ_λ 相應之 $\mathfrak{H}$ 之羣指標爲 Ψ_λ，而於(4)以 x_E+u 代其 x_E 而比較其兩邊之 $u^{l_\kappa-1}$ 之係數，則得

$$\sum_P \chi_\kappa(P)\,x_P=\sum_{P\lambda}\sum r_{\lambda\kappa}\,\Psi_\lambda(P)\,x_P \qquad (P=H_0, H_1, \cdots\cdots, H_{h-1}).$$

因之對 $\mathfrak{H}$ 之元素 P，

$$(6)\quad \chi_\kappa(P)=\sum_\lambda r_{\lambda\kappa}\psi_\lambda(P) \qquad \begin{cases}\kappa=0, 1, 2, \cdots\cdots, k-1,\\ \lambda=0, 1, 2, \cdots\cdots, l-1.\end{cases}$$

自他方言，由關於單指標之公式(IX)，(XII)，

$$(7)\quad \sum_P \psi_\lambda(P)\psi_\lambda(P^{-1})=h,\ \sum_P \psi_\lambda(P)\psi_\nu(P^{-1})=0 \quad [\lambda\neq\nu]$$

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

故由(6)，

$$(8)\quad \sum_P \chi_\kappa(P)\chi_\mu(P^{-1})=\sum_{P\lambda,\nu}\sum r_{\lambda\kappa}\psi_\lambda(P)r_{\nu\mu}\psi_\nu(P^{-1})$$

$$=h\sum_\lambda r_{\lambda\kappa}r_{\lambda\mu} \qquad \begin{cases}\lambda=0, 1, 2, \cdots\cdots, l-1,\\ \kappa,\mu=0, 1, 2, \cdots\cdots, k-1.\end{cases}$$

於是令 $\mu=\kappa$，再就 κ 以加之，且適用公式(XIV)，則得

$$\sum_P \frac{g}{g_P}=h\sum_{\lambda,\kappa} r_{\lambda\kappa}^2 \qquad (P=H_0, H_1, \cdots\cdots, H_{h-1})$$

但 g_P 爲示 P 所屬共軛系($\mathfrak{G}$ 的)之元素數者．今將 $\mathfrak{G}$ 中第 ρ 共軛系之元素數示以 g_ρ，而將此系之元素中其屬於 $\mathfrak{H}$ 者之個數示以 h_ρ，則

$$\sum_P \frac{g}{g_P}=\sum_\rho \frac{gh_\rho}{g_\rho} \qquad (\rho=0, 1, 2, \cdots\cdots, k-1)$$

甚明. 以此代入前式, 則得

$$(9)\qquad \sum_{\lambda,\kappa} r_{\lambda\kappa}^{2}=\sum_{\rho}\frac{gh_\rho}{hg_\rho}\begin{cases}\lambda=0,\ 1,\ 2,\ \cdots\cdots,\ l-1,\\ \kappa=0,\ 1,\ 2,\ \cdots\cdots,\ k-1,\\ \rho=0,\ 1,\ 2,\ \cdots\cdots,\ k-1.\end{cases}$$

此卽(4)之右邊中之指數間之關係也.

次由(6)及(7),

$$(10)\qquad \sum_{\mathrm{P}}\psi_\lambda(\mathrm{P}^{-1})\chi_\kappa(\mathrm{P})=hr_{\lambda\kappa}\qquad(\mathrm{P}=\mathrm{H}_0,\ \mathrm{H}_1,\ \cdots\cdots,\ \mathrm{H}_{h-1}).$$

故對$\mathfrak{G}$之元素R,

$$h\sum_{\kappa} r_{\lambda\kappa}\chi_\kappa(\mathrm{R})=\sum_{\mathrm{P}}\psi_\lambda(\mathrm{P})\{\sum_{\kappa}\chi_\kappa(\mathrm{P}^{-1})\chi_\kappa(\mathrm{R})\}\quad(\kappa=0,\ 1,\ 2,\ \cdots\cdots,\ k-1).$$

然P若與R於$\mathfrak{G}$非爲共軛時, 則由公式(XIII), $\sum_{\kappa}\chi_\kappa(\mathrm{P}^{-1})\chi_\kappa(\mathrm{R})$等於零; 反之, P及R於$\mathfrak{G}$爲屬於同一共軛系時, 則由公式(XIV), 此值爲g/g_{R}. 故上式爲

$$(11)\qquad \sum_{\kappa} r_{\lambda\kappa}\chi_\kappa(\mathrm{R})=\frac{g}{hg_{\mathrm{R}}}\sum_{\mathrm{P}}\psi_\lambda(\mathrm{P}).$$

但右邊之加法, 乃就R所屬共軛系($\mathfrak{G}$的)之元素中之屬於$\mathfrak{H}$者而行之者也. 對於不屬於$\mathfrak{H}$之元素S, 若令$\psi_\lambda(\mathrm{S})=0$, 則(11)之右邊, 就$\mathfrak{G}$中與R共軛全部之元素加之可.

於(6)及(11), 令P=R=E, 則得

$$f_\kappa=\sum_{\lambda} r_{\lambda\kappa}e_\lambda\qquad(\lambda=0,\ 1,\ 2,\ \cdots\cdots,\ l-1),$$

$$(12)$$

$$\sum_{\kappa} r_{\lambda\kappa}f_\kappa=\frac{g}{h}e_\lambda\qquad(\kappa=0,\ 1,\ 2,\ \cdots\cdots,\ k-1).$$

次令 $r_{0\kappa}=r_\kappa$，則由 (10) 及 (11)，

$$\sum_{\mathrm{P}}\chi_\kappa(\mathrm{P})=hr_\kappa \qquad (\mathrm{P}=\mathrm{H}_0, \mathrm{H}_1, \cdots\cdots, \mathrm{H}_{k-1}),$$

$$\sum_{\kappa} r_\kappa\chi_\kappa(\mathrm{R})=\frac{gh_{\mathrm{R}}}{hg_{\mathrm{R}}} \qquad (\kappa=0, 1, 2, \cdots\cdots, k-1).$$

但 h_{R} 爲在 $\mathfrak{G}$ 中與 R 共軛之元素內之屬於 $\mathfrak{H}$ 者之個數.

若 R 爲屬於 $\mathfrak{G}$ 之第 ρ 共軛系者，則此兩式分別得換書爲次形:

$$(13)\qquad \sum_{\rho}h_\rho\chi_\kappa(\rho)=hr_\kappa \qquad (\rho=0, 1, 2, \cdots\cdots, k-1),$$

$$(14)\qquad \sum_{\kappa} r_\kappa\chi_\kappa(\rho)=\frac{gh_\rho}{hg_\rho} \qquad (\kappa=0, 1, 2, \cdots\cdots, k-1).$$

後式中其左邊乃代數的整數，故 $\frac{gh_\rho}{hg_\rho}$ 爲有理整數.

Frobenius 氏曾用 (14) 以定對稱羣之羣指標,* 更進以求交代羣之指標矣.† 又如次節所述，則對 n 次 $n-1$ 級可遷羣之考察，利用本節之諸公式，可得重要之結果也.‡

由羣之性質直接以明 $\frac{gh_\rho}{hg_\rho}$ 之所有之意義，則以 R 與上同樣爲第 ρ 共軛系之元素，而以 $\mathfrak{G}$ 中 g 個之元素變其形，則其結果，得第 ρ 共軛系中 g_ρ 個之元素，而各元素均出現

---

* Berliner Sitzungsberichte, 1900 (516—534).

† 同 上, 1901 (303—315).

‡ 同 上, 1901 (1216—1230).

g/g_ρ 回焉. 然第 ρ 共軛系之元素中其屬於 $\mathfrak{H}$ 者有 h_ρ 個. 故如

$$G^{-1}RG=\mathfrak{H}\text{之元素}$$

者之元素 G (𝔊的) 之數爲 $\frac{g}{g_\rho}h_\rho$. 此集合以 $\mathfrak{A}$ 示之. 若 A 爲 $\mathfrak{A}$ 中任意一元素, 則對 $\mathfrak{H}$ 之元素 H,

$$(AH)^{-1}R(AH)=H^{-1}A^{-1}RAH=H^{-1}\ (\mathfrak{H}\text{之元素})\ H=\mathfrak{H}\text{之元素}.$$

因之傍系 A$\mathfrak{H}$ 之元素皆屬於 $\mathfrak{A}$. 於是由(1)就 $\mathfrak{H}$ 將 𝔊 分爲傍系, 而以之爲

$$\mathfrak{G}=S_0^{-1}\mathfrak{H}+S_1^{-1}\mathfrak{H}+\cdots\cdots+S_{n-1}^{-1}\mathfrak{H}.$$

在 $S_0^{-1}, S_1^{-1}, \cdots\cdots, S_{n-1}^{-1}$ 之中其屬於 $\mathfrak{A}$ 者之個數若爲 m, 則與之相應之 m 個傍系乃形成 $\mathfrak{A}$ 焉. 故 $\mathfrak{A}$ 之元素之數爲 mh. 卽

$$\frac{g}{g_\rho}h_\rho=mh,\ \text{或}\ \frac{gh_\rho}{hg_\rho}=m. \tag{15}$$

更就 m 而論之, S_i^{-1} 屬於 $\mathfrak{A}$ 時,

$$S_iRS_i^{-1}=H,\ \text{卽}\ RS_i^{-1}=S_i^{-1}H\quad [H\text{爲}\mathfrak{H}\text{之元素}].$$

故

$$RS_i^{-1}\mathfrak{H}=S_i^{-1}\mathfrak{H}.$$

反之, 此時 S_i^{-1} 之屬於 $\mathfrak{A}$ 甚明. 因之 m 爲表示滿足上式之傍系之數者也.

特別, 將此結果應用於 n 文字 $\alpha, \alpha_1, \cdots\cdots, \alpha_{n-1}$ 之可遷羣時, 乃取文字 α 不動者之約羣以爲 $\mathfrak{H}$, 而以 S_i 爲置換 α 於 α_i 之置換, 則 $S_i^{-1}\mathfrak{H}$ 之置換, 乃置換 α_i 於 α 也. 故 $RS_i^{-1}\mathfrak{H}=S_i^{-1}\mathfrak{H}$

時，RS_i^{-1} 亦復同樣，因之 $RS_i^{-1}S_i(=R)$ 不使 a_i 移動．反之，R 不使 a_i 動時，則 $RS_i^{-1}\mathfrak{H}=S_i^{-1}\mathfrak{H}$．因之在關於 $\mathfrak{H}$ 之傍系之中，其屬於 $\mathfrak{A}$ 者之數 m 乃與由 R 而不動者之文字之數相等．故若對 R 而不動之文字之數示以 $\nu(R)$，則由 (15) 得

$$\nu(R)=\frac{gh_R}{hg_R}. \tag{16}$$

174．n 次 $n-1$ 級可遷羣．

於 n 次可遷羣，若其恰使 c 個文字不動之置換雖存在，然使多於 c 個之文字不動者僅爲不動置換時，則此羣名曰 $n-c$ 級．* 特別，在不動置換以外之置換能使 n 個文字全動或 $n-1$ 個文字動時，則其羣曰 $n-1$ 級．如 p 次亞巡回羣乃爲 $p-1$ 級者也．

試以 $\mathfrak{G}$ 爲 n 文字 $a, a_1, \cdots\cdots, a_{n-1}$ 之 $n-1$ 級可遷羣，$\mathfrak{H}$ 爲不使 a 動者之約羣，而

$$\mathfrak{G}=\mathfrak{H}+\mathfrak{H}S_1+\cdots\cdots+\mathfrak{H}S_{n-1}.$$

但 S_i 爲示置換 a 於 a_i 之置換者．因 $\mathfrak{G}$ 爲 $n-1$ 級，故 $\mathfrak{H}$ 非爲僅由 $n-1$ 次之正置換而成立者不可．故其元數 h 須爲 $n-1$ 之約數（第 72 節系）．因之 h 對 n 互素．其次，$\mathfrak{H}$ 之共軛約羣

$$\mathfrak{H},\ S_1^{-1}\mathfrak{H}S_1,\ \cdots\cdots,\ S_{n-1}^{-1}\mathfrak{H}S_{n-1} \tag{1}$$

乃分別不使 $a, a_1, \cdots\cdots, a_{n-1}$ 動者．而 $\mathfrak{G}$ 又係 $n-1$ 級，故此諸約羣除不動置換以外無有共通之置換．因之含於此諸約

*對稱羣爲 2 級，交代羣爲 3 級．又 n 次正置換羣則爲 n 級．

羣中之置換之總數爲$n(h-1)+1$. 是卽含有不動文字之置換之總數也. 以故其使全部文字皆動之置換之數爲$nh-\{n(h-1)+1\}=n-1$焉.

然使全部文字皆動之置換乃n次正置換也. 何以故? 蓋若以其一爲

$$R=(a a'\cdots\cdots)(\beta\beta'\cdots\cdots)\cdots\cdots,$$

而巡回因子之項數分別爲$a, b, \cdots\cdots$時, 苟$a<b$, 則

$$R^a=(\beta\beta'\cdots\cdots)^a\cdots\cdots\neq 1,$$

而R^a不能使a個之文字移動故耳. 由是, R之巡回率遂爲n之約數. 卽$R^n=E$. 自他方言, h對n互素. 故對置換H之使唯一個文字不動者, 則$H^n\neq E$. 於是$\mathfrak{G}$之置換得分爲滿足$R^n=E$者與不滿足者之二種. 前者由不動置換及其使全部文字皆動者之置換而成, 其數爲n個; 而後者則由不使一文字動者之置換而成者也.

若$\mathfrak{H}$之二元素P, Q於$\mathfrak{G}$爲共軛, 卽$G^{-1}PG=Q$(G爲$\mathfrak{G}$之元素), 則以共軛約羣(1)無有共通之置換(非不動的)之故, G不得使a動, 隨之屬於$\mathfrak{H}$也. 故P, Q於$\mathfrak{H}$亦共軛焉. 因之於$\mathfrak{H}$之羣指標ψ_λ, 乃有$\psi_\lambda(P)=\psi_\lambda(Q)$. 於是若對$n$次$n-1$級可遷羣$\mathfrak{G}$及其約羣$\mathfrak{H}$適用前節之公式, 則(11)得如次:

$$(2)\qquad \sum_\kappa \tau_{\lambda\kappa}\chi_\kappa(R)=\frac{gh_R}{hg_R}\psi_\lambda(P)\quad(\kappa=0, 1, 2, \cdots\cdots, k-1).$$

但P爲示與R共軛者之$\mathfrak{H}$之元素.

且於$\mathfrak{G}$其與P($\mathfrak{H}$之元素)交換可能之置換有g/g_P個；而此諸置換又非全部屬於$\mathfrak{H}$不可．此則由共軛約羣系(1)無有共通之元素而自明也．然$\mathfrak{H}$之元素中於$\mathfrak{G}$與P共軛者有h_P個，而此諸個如上述則於$\mathfrak{H}$亦共軛．故於$\mathfrak{H}$其與P交換可能之置換之數爲h/h_P．因之P爲$\mathfrak{H}$之元素時，則

$$\frac{g}{g_P}=\frac{h}{h_P},\quad 即\ \frac{gh_P}{hg_P}=1.$$

其次若R能使n個文字皆動時，則與之共軛者不得存在於$\mathfrak{H}$．故$h_R=0$．因之$\frac{gh_R}{hg_R}=0$．又$\frac{gh_E}{hg_E}=\frac{g}{h}=n$自明．將此所得之值代入(2)，遂得次之關係：

$$(3)\qquad \sum_{\kappa}\tau_{\lambda\kappa}\chi_{\kappa}(R)=\begin{cases}\psi_{\lambda}(P) & [R^n\neq E],\\ ne_{\lambda} & [R=E],\\ 0 & [R\neq E,\ R^n=E].\end{cases}$$

但P爲與R共軛之$\mathfrak{H}$之元素．

特別在R屬於$\mathfrak{H}$時，上式遂爲

$$(4)\qquad \sum_{\kappa}\tau_{\lambda\kappa}\chi_{\kappa}(P)=\begin{cases}\psi_{\lambda}(P) & [P\neq E],\\ ne_{\lambda} & [P=E].\end{cases}$$

次以前節(6)代入此之左邊，則得

$$\sum_{\kappa,\mu}\tau_{\lambda\kappa}\tau_{\mu\kappa}\psi_{\mu}(P)=\begin{cases}\psi_{\lambda}(P) & [P\neq E],\\ ne_{\lambda} & [P=E].\end{cases}$$

於是令

$$(5)\qquad \sum_{\kappa=0}^{k-1} r_{\lambda\kappa} r_{\mu\kappa} = s_{\lambda\mu} = s_{\mu\lambda} \qquad (\lambda, \mu = 0, 1, 2, \cdots\cdots, l-1),$$

則得

$$(6)\qquad \sum_{\mu} s_{\lambda\mu}\psi_{\mu}(\mathrm{P}) = \begin{cases} \psi_{\lambda}(\mathrm{P}) & [\mathrm{P} \neq \mathrm{E}] \\ n e_{\lambda} & [\mathrm{P} = \mathrm{E}] \end{cases} \qquad (\mu = 0, 1, 2, \cdots\cdots, l-1).$$

但 P 爲 $\mathfrak{G}$ 之元素. 然由關於單指標之公式(IX),(XIII),

$$\sum_{\mu} e_{\mu}\psi_{\mu}(\mathrm{P}) = \sum_{\mu} \psi_{\mu}(\mathrm{E})\psi_{\mu}(\mathrm{P}) = \begin{cases} 0 & [\mathrm{P} \neq \mathrm{E}], \\ h & [\mathrm{P} = \mathrm{E}], \end{cases} \qquad (\mu = 0, 1, 2, \cdots\cdots, l-1).$$

用此而將(6)換書之,則得

$$\sum_{\mu} s_{\lambda\mu}\psi_{\mu}(\mathrm{P}) = \psi_{\lambda}(\mathrm{P}) + \frac{n-1}{h} e_{\lambda} \sum e_{\mu}\psi_{\mu}(\mathrm{P}).$$

此式不問 P 爲不動置換與否,只要其屬於 $\mathfrak{G}$ 時,常告成立. 更將其換書之,則得

$$\sum_{\mu} \left\{ s_{\lambda\mu} - \frac{n-1}{h} e_{\lambda} e_{\mu} - e_{\lambda\mu} \right\} \psi_{\mu}(\mathrm{P}) = 0.$$

$$(\mu = 0, 1, 2, \cdots\cdots, l-1).$$

但

$$e_{\lambda\mu} = \begin{cases} 0 & (\lambda \neq \mu), \\ 1 & (\lambda = \mu). \end{cases}$$

然 $\mathfrak{G}$ 之單指標 $\psi_0, \psi_1, \cdots\cdots, \psi_{l-1}$ 乃一次的獨立者,即

$$|\psi_{\lambda}^{(\mu)}| \neq 0 \quad (\lambda, \mu = 0, 1, 2, \cdots\cdots, l-1)$$

(第 167 節末). 故由前式,則

$$s_{\lambda\mu} - \frac{n-1}{h} e_{\lambda} e_{\mu} - e_{\lambda\mu} = 0 \quad (\lambda, \mu = 0, 1, 2, \cdots\cdots, l-1)$$

爲必要也．將此移項得

$$(7)\qquad s_{\lambda\mu}=e_{\lambda\mu}+\frac{n-1}{h}e_\lambda e_\mu \quad (\lambda,\mu=0,1,2,\cdots\cdots,l-1).$$

自他方面言，

$$\Sigma(r_{\lambda\kappa}-e_\lambda r_\kappa)^2=s_{\lambda\lambda}-2e_\lambda s_{\lambda 0}+e_\lambda{}^2 s_{00} \quad (\kappa=0,1,2,\cdots\cdots,k-1).$$

以(7)之值代入此右邊，則$\lambda>0$時，此和遂等於

$$1+\frac{n-1}{h}e_\lambda{}^2-2e_\lambda\frac{n-1}{h}e_\lambda+e_\lambda{}^2\left(1+\frac{n-1}{h}\right)=1+e_\lambda{}^2.$$

又$r_{00}=1$，$r_{\lambda 0}=0$［前節(5)］，因之

$$(8)\qquad r_{\lambda 0}-e_\lambda r_0=-e_\lambda \quad (\lambda>0).$$

故

$$\sum_{\kappa=1}^{k-1}(r_{\lambda\kappa}-e_\lambda r_\kappa)^2=1 \qquad (\lambda=1,2,\cdots\cdots,l-1).$$

因之，在$k-1$個之整數

$$r_{\lambda\kappa}-e_\lambda r_\kappa \qquad (\kappa=1,2,\cdots\cdots,k-1)$$

之中，其一個等於±1，而其他皆爲零．復次若λ，μ不爲零且互異時，則與上同樣，可知

$$\sum_{\kappa=1}^{k-1}(r_{\lambda\kappa}-e_\lambda r_\kappa)(r_{\mu\kappa}-e_\mu r_\kappa)=0.$$

故若對$\kappa=\alpha$有$r_{\lambda\alpha}-e_\lambda r_\alpha=\pm1$，而對$\kappa=\beta$有$r_{\mu\beta}-e_\mu r_\beta=\pm1$，則$\alpha$與$\beta$不得不相異．因之於$\Theta(x)$之分解，若將其素因數之順序適當定之，則得使

$$(9)\qquad r_{\lambda\lambda}-e_\lambda r_\lambda=\pm1 \qquad (\lambda=1,2,\cdots\cdots,l-1),$$

$$(10)\qquad r_{\lambda\kappa}-e_\lambda r_\kappa=0\ [\lambda\neq\kappa]\qquad(\kappa=1,2,\cdots\cdots,k-1)$$

也. 由此關係與(8), 當 $\lambda>0$ 時,

$$\sum_{\kappa=0}^{k-1}(r_{\lambda\kappa}-e_\lambda r_\kappa)\chi_\kappa(\mathrm{R})=\pm\chi_\lambda(\mathrm{R})-e_\lambda\chi_0(\mathrm{R})=\pm\chi_\lambda(\mathrm{R})-e_\lambda.$$

然以(3)計算此左邊, 則以 $\psi_0(\mathrm{P})=1$ 之故, 遂得

$$\sum_\kappa(r_{\lambda\kappa}-e_\lambda r_\kappa)\chi_\kappa(\mathrm{R})=\begin{cases}\psi_\lambda(\mathrm{P})-e_\lambda & [\mathrm{R}^n\neq\mathrm{E}],\\ 0 & [\mathrm{R}^n=\mathrm{E}].\end{cases}$$

故 $\lambda>0$ 時,

$$(11)\qquad \pm\chi_\lambda(\mathrm{R})-e_\lambda=\begin{cases}\psi_\lambda(\mathrm{P})-e_\lambda & [\mathrm{R}^n\neq\mathrm{E}],\\ 0 & [\mathrm{R}^n=\mathrm{E}].\end{cases}$$

特別當 $\mathrm{R}=\mathrm{E}$ 時,

$$\pm\chi_\lambda(\mathrm{E})-e_\lambda=0,\ \text{卽}\ \pm f_\lambda=e_\lambda.$$

然素因數之次數 f_λ, e_λ 共爲正. 故(11)僅對正符號而始成立. 因之

$$(12)\qquad \chi_\lambda(\mathrm{R})=\begin{cases}\psi_\lambda(\mathrm{P}) & [\mathrm{R}^n\neq\mathrm{E}],\\ e_\lambda=f_\lambda & [\mathrm{R}^n=\mathrm{E}],\end{cases}\qquad(\lambda>0).$$

但 P 爲與 R 共軛之 $\mathfrak{S}$ 之元素.

在不適合 $\mathrm{R}^n=\mathrm{E}$ 者之元素($\mathfrak{S}$的)中, 對於 $\lambda=1,2,\cdots\cdots,l-1$ 全部之值, 其如 $\psi_\lambda(\mathrm{P})=e_\lambda$ 者之元素 P, 決不能存在. 蓋因 $\mathrm{P}^n\neq\mathrm{E}$ 時, P 已如前述爲不使一文字動者. 若假定 P 屬於 $\mathfrak{S}$, 而 $\psi_\lambda(\mathrm{P})=e_\lambda$ $(\lambda=1,2,\cdots\cdots,l-1)$, 則有

$$\sum_\lambda\psi_\lambda(\mathrm{E})\psi_\lambda(\mathrm{P})=\sum_\lambda e^2{}_\lambda=h\neq0\quad(\lambda=0,1,2,\cdots\cdots,l-1)$$

是生出違反單指標公式(XIII)之結果爲不合理故也．於是其滿足$l-1$個方程式

$$\chi_\lambda(R)=f_\lambda \qquad (\lambda=1, 2, \cdots\cdots, l-1)$$

之元素，由(12)知僅爲適合$R^n=E$者．而此諸元素，由第171節第一定理乃作一正常約羣．然滿足$R^n=E$之元素，如前述，爲不動置換與使全文字皆動者之置換(其數有$n-1$個)之二種．因之得次

定理．於n次$n-1$級可遷羣，其不動置換與全文字皆動之置換相集成一正常約羣．而此約羣爲n次正置換羣．(Frobenius 氏)

本定理中之正常約羣乃特性的也．蓋因在羣之自己同態中其滿足$R^n=E$之元素仍與同樣之元素對應故(參照第103節)．又由本定理，n次$n-1$級可遷羣之爲n元羣之全形或其約羣可知(參照第98, 101節)．於是此羣在二重可遷時，則爲第99節之所述者也．

175. 屬於可遷羣之羣母式．

茲於一置換

$$S=\begin{pmatrix} a_1 & a_2 & \cdots\cdots \\ b_1 & b_2 & \cdots\cdots \end{pmatrix},$$

使變數$\xi_{a_1}, \xi_{a_2}, \cdots\cdots$之變換

$$S': \quad \xi'_{a_1}=\xi_{b_1},\ \xi'_{a_2}=\xi_{b_2}, \cdots\cdots$$

相與對應．如與$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$對應者爲

$$\xi'_1=\xi_2,\ \xi'_2=\xi_1,\ \xi'_3=\xi_4,\ \xi'_4=\xi_3$$

是. 就變換 S′ 之係數之母式而觀, $b_i=a_j$ 時, 其第 i 橫行, 僅其第 j 項爲 1, 而他項皆爲零也. 乃名之曰屬於 S 之母式. 如屬於上例之置換者, 則爲

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

更取與S同文字上所行之置換

$$\mathrm{T}=\begin{pmatrix} b_1 & b_2 & \cdots\cdots \\ c_1 & c_2 & \cdots\cdots \end{pmatrix},$$

則與之相應之變換爲

$$\mathrm{T}':\quad \xi'_{b_1}=\xi_{c_1},\ \xi'_{b_2}=\xi_{c_2},\cdots\cdots;$$

而對兩置換之積

$$\mathrm{ST}=\begin{pmatrix} a_1 & a_2 & \cdots\cdots \\ c_1 & c_2 & \cdots\cdots \end{pmatrix}$$

者, 則爲

$$\xi'_{a_1}=\xi_{c_1},\ \xi'_{a_2}=\xi_{c_2},\cdots\cdots.$$

而此與 S′ 及 T′ 之積相等甚明. 於是若以 S′, T′ 及積 S′T′ 之母式分別以 (S), (T), 及 (ST) 表之, 則得 (S)(T)=(ST). 因之 n 次置換羣爲已知時, 則與之爲單純同態之變換羣或 n 次母式羣, 得以上記之方法而作出之也. 此則名曰屬於置換羣之變換羣或母式羣焉. 如屬於三次對稱羣

1, (123), (132), (23), (31), (12)

之母式羣，則爲

$$\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\ \begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\ \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix},\ \begin{pmatrix}1&0&0\\0&0&1\\0&1&0\end{pmatrix},\ \begin{pmatrix}0&0&1\\0&1&0\\1&0&0\end{pmatrix},\ \begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}.$$

復以 $\mathfrak{H}(\mathrm{H}_0, \mathrm{H}_1, \cdots\cdots, \mathrm{H}_{h-1})$ 爲 g 元羣 $\mathfrak{G}$ 之約羣，而

$$\mathfrak{G}=\mathfrak{H}\mathrm{S}_0+\mathfrak{H}\mathrm{S}_1+\cdots\cdots+\mathfrak{H}\mathrm{S}_{n-1}\quad(\mathrm{S}_0=1).$$

試取 g 個之獨立變數

$$x_{\mathrm{H}_\alpha \mathrm{S}_i}\quad\begin{cases}\alpha=0,1,2,\cdots\cdots,h-1,\\ i=0,1,2,\cdots\cdots,n-1,\end{cases}$$

而令

$$(1)\qquad\begin{cases}x_{\mathfrak{H}}=x_{\mathrm{H}_0}+x_{\mathrm{H}_1}+\cdots\cdots+x_{\mathrm{H}_{h-1}}\\ x_{\mathrm{A}\mathfrak{H}\mathrm{B}}=x_{\mathrm{AH}_0\mathrm{B}}+x_{\mathrm{AH}_1\mathrm{B}}+\cdots\cdots+x_{\mathrm{AH}_{h-1}\mathrm{B}},\end{cases}$$

再由之以作 n 次母式

$$(2)\qquad \mathrm{X}=(x_{\mathrm{S}_i^{-1}\mathfrak{H}\mathrm{S}_j})\quad(i,j=0,1,2,\cdots\cdots,n-1)$$

$$=\begin{pmatrix}x_{\mathfrak{H}} & x_{\mathfrak{H}\mathrm{S}_1} & \cdots\cdots & x_{\mathfrak{H}\mathrm{S}_{n-1}}\\ x_{\mathrm{S}_1^{-1}\mathfrak{H}} & x_{\mathrm{S}_1^{-1}\mathfrak{H}\mathrm{S}_1} & \cdots\cdots & x_{\mathrm{S}_1^{-1}\mathfrak{H}\mathrm{S}_{n-1}}\\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots\\ x_{\mathrm{S}_{n-1}^{-1}\mathfrak{H}} & x_{\mathrm{S}_{n-1}^{-1}\mathfrak{H}\mathrm{S}_1} & \cdots\cdots & x_{\mathrm{S}_{n-1}^{-1}\mathfrak{H}\mathrm{S}_{n-1}}\end{pmatrix}$$

於是以 $x_{\mathrm{R}}=1$，他之變數悉爲零，其所生之母式示以 (R)，則得

$$(3)\qquad \mathrm{X}=\sum_{\mathrm{R}}(\mathrm{R})x_{\mathrm{R}}.$$

他方面令 $\mathrm{S}_i\mathrm{R}=\mathrm{HS}_j$（H 爲 $\mathfrak{H}$ 之元素），則在 $\mathfrak{G}$ 之元素

$$S_i^{-1}H_\alpha S_\beta \begin{cases} \alpha=0,1,2,\cdots\cdots,h-1 \\ \beta=0,1,2,\cdots\cdots,n-1 \end{cases}$$

中其等於R者僅唯一之$S_i^{-1}HS_j$. 故$x_R=1$, 他之變數爲零時, 則X之第$(i+1)$橫行, 其第$(j+1)$項$x_{S_i^{-1}\mathfrak{H}S_j}$爲1, 他之項皆爲零也. 然

$$S_i^{-1}\mathfrak{H}S_j=S_i^{-1}\mathfrak{H}S_iR, \text{ 因之 } \mathfrak{H}S_j=\mathfrak{H}S_iR.$$

故(R)爲屬於傍系之置換

$$\begin{pmatrix} \mathfrak{H} & \mathfrak{H}S_1 & \cdots\cdots & \mathfrak{H}S_{n-1} \\ \mathfrak{H}R & \mathfrak{H}S_1R & \cdots\cdots & \mathfrak{H}S_{n-1}R \end{pmatrix}$$

之母式. 因之X爲屬於$\mathfrak{G}$之傍系置換表示(就$\mathfrak{H}$而生者)之羣母式.

特別取主元素羣爲$\mathfrak{H}$, 則得

$$\mathfrak{G}=S_0+S_1+\cdots\cdots+S_{n-1} \quad (n=g),$$

$$X=(x_{S_i^{-1}S_j}) \quad (i,j=0,1,2,\cdots\cdots,n-1),$$

而關於$\mathfrak{H}$之傍系置換表示則爲正置換表示. 卽正羣母式爲屬於正置換表示者也.

其次取羣母式X之行列式, 則

$$|X| = |x_{S_i^{-1}\mathfrak{H}S_j}| \quad (i,j=0,1,2,\cdots\cdots,n-1)$$

$$= \begin{vmatrix} \sum_{i=0}^{n-1} x_{\mathfrak{H}S_i} & x_{\mathfrak{H}S_1} & \cdots\cdots \\ \sum_{i=0}^{n-1} x_{S_1^{-1}\mathfrak{H}S_i} & x_{S_1^{-1}\mathfrak{H}S_1} & \cdots\cdots \\ \cdots\cdots\cdots\cdots\cdots\cdots & & \end{vmatrix}$$

然

$$\sum_i x_{\mathfrak{H}\mathfrak{S}_i}=\sum_i x_{\mathfrak{S}_1^{-1}\mathfrak{H}\mathfrak{S}_i}=\cdots\cdots=\sum_{\mathrm{R}} x_{\mathrm{R}}.$$

但此最後之和乃就$\mathfrak{G}$之全部元素而取之者．故若令

$$\Phi_0(x)=\sum_{\mathrm{R}} x_{\mathrm{R}}.$$

則得

$$|\,\mathrm{X}\,|=\Phi_0(x)\cdot \mathrm{D}(x).$$

但

$$\mathrm{D}(x)=\begin{vmatrix} 1 & x_{\mathfrak{H}\mathfrak{S}_1} & \cdots\cdots \\ 1 & x_{\mathfrak{S}_1^{-1}\mathfrak{H}\mathfrak{S}_1} & \cdots\cdots \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \end{vmatrix}.$$

對所有之變數，雖以$x_{\mathrm{R}}+u$代x_{R}，行列式$\mathrm{D}(x)$仍不變甚明，然$\Phi_0(x)$由此置換而變其值．故$\mathrm{D}(x)$不得以$\Phi_0(x)$整除．因之$|\,\mathrm{X}\,|$雖得以$\Phi_0(x)$整除，而以其自乘則否．故$|\,\mathrm{X}\,|$分解爲素因數，則爲

$$(4)\quad |\,\mathrm{X}\,|=\Phi_0(x)[\Phi_1(x)]^{a_1}[\Phi_2(x)]^{a_2}\cdots\cdots[\Phi_{m-1}(x)]^{a_{m-1}}$$

但$\Phi_0,\Phi_1,\cdots\cdots,\Phi_{m-1}$爲示互異之既約羣母式之行列式者．

$\mathfrak{G}$爲n文字$\alpha,\alpha_1,\cdots\cdots,\alpha_{n-1}$之可遷羣時，選其一文字$\alpha$不動者之約羣以爲$\mathfrak{H}$，則關於$\mathfrak{H}$之傍系置換表示與$\mathfrak{G}$爲同值．即傍系置換表示者，不外於$\mathfrak{G}$以傍系$\mathfrak{H},\mathfrak{H}\mathrm{S}_1,\cdots\cdots,\mathfrak{H}\mathrm{S}_{n-1}$分別代其文字$\alpha,\alpha_1,\cdots\cdots,\alpha_{n-1}$者而已也（第76節）．因之此時母式(R)屬於$\mathfrak{G}$之置換R，而羣母式X則屬於可遷羣$\mathfrak{G}$焉．

176. 可遷羣之置換與羣指標之關係.

設 $\mathfrak{G}(G_0, G_1, \cdots\cdots, G_{g-1})$ 爲 n 次可遷羣, X 爲其羣母式 X 之指標, χ_μ 爲與素因數 Φ_μ 相應之單指標, 則由前節(4)得*

$$(1) \qquad \boldsymbol{\chi}(R)=1+\sum_\mu a_\mu \chi_\mu(R) \quad (\mu=1, 2, \cdots\cdots, m-1).$$

他方面就屬於 $\mathfrak{G}$ 之置換

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

者之母式(R)而觀, 其第 i 行第 i 項, 若 $\beta_{i-1}=\alpha_{i-1}$ 雖爲 1, 然若 $\beta_{i-1}\neq\alpha_{i-1}$ 則爲零. 故(R)之指標, 乃表其由置換 R 而不動之文字之數者. 於是若以對 R 而不動之文字之數示以 $\nu(R)$, 則由(1)得

$$(2) \qquad \nu(R)=1+\sum_\mu a_\mu \chi_\mu(R) \quad (\mu=1, 2, \cdots\cdots, m-1).$$

今於 $\mathfrak{G}$ 之置換中以其恰爲 r 個文字不動者之個數示以 N_r, 則

$$\sum_R \nu(R)=\sum_{r=0}^{n} rN_r=\sum_{r=1}^{n} rN_r \quad (R=G_0, G_1, \cdots\cdots, G_{g-1}).$$

然

$$\sum_R \chi_\mu(R)=0 \qquad [\text{第 167 節注意}].$$

因之

$$\sum_R\left\{1+\sum_\mu a_\mu \chi_\mu(R)\right\}=g+\sum_\mu a_\mu \sum_R \chi_\mu(R)=g.$$

---

*與導出第 173 節 (6) 者同樣, 以 x_E+u 代其 x_E, 而比較 (4) 之兩邊中 u^{n-1} 之係數卽得本式.

故由(2),

$$(3)\qquad g=\sum_{r=1}^{n} r\mathrm{N}_r=\sum_{\mathrm{R}}\left\{1+\sum_{\mu}a_\mu\chi_\mu(\mathrm{R})\right\}.$$

此開始之部分與第71節之定理一致.

又 $\nu(\mathrm{R})=\nu(\mathrm{R}^{-1})$ 自明，因之

$$\sum_{\mathrm{R}}\nu(\mathrm{R})\nu(\mathrm{R}^{-1})=\sum_{r=1}^{n} r^2\mathrm{N}_r$$

然

$$\sum_{\mathrm{R}}\left\{1+\sum_{\mu}a_\mu\chi_\mu(\mathrm{R})\right\}\left\{1+\sum_{\lambda}a_\lambda\chi_\lambda(\mathrm{R}^{-1})\right\}$$

$$=\sum_{\mathrm{R}}\left\{1+\sum_{\mu}a_\mu\chi_\mu(\mathrm{R})+\sum_{\lambda}a_\lambda\chi_\lambda(\mathrm{R}^{-1})+\sum_{\mu,\lambda}a_\mu a_\lambda\chi_\mu(\mathrm{R})\chi_\lambda(\mathrm{R}^{-1})\right\}$$

$$=g+\sum_{\mu,\lambda}a_\mu a_\lambda\sum_{\mathrm{R}}\chi_\mu(\mathrm{R})\chi_\lambda(\mathrm{R}^{-1})$$

$$=g+g\sum_{\mu}a^2\mu \qquad [\text{由公式 (IX), (XII)}].$$

故由(2)得

$$(4)\qquad \left(1+\sum_{\mu=1}^{m-1}a^2\mu\right)g=\sum_{r=1}^{n} r^2\mathrm{N}_r$$

$$=\sum_{\mathrm{R}}\left\{1+\sum_{\mu}a_\mu\chi_\mu(\mathrm{R})\right\}\left\{1+\sum_{\mu}a_\mu\chi_\mu(\mathrm{R}^{-1})\right\}.$$

最後就 $\sum_{\mu}a^2\mu$ 之意義一討論之. 以一個定文字不動之約羣 $\mathfrak{H}$ 視爲 $n-1$ 次之置換羣時，乃以文字爲分成 t 個可遷系，而在 $\mathfrak{H}$ 中其不動文字恰爲 r 個者之置換之數以爲 N'_r，則由第71節定理，

$$(5)\qquad t\cdot\frac{g}{n}=\sum r\mathrm{N}_r' \qquad (r=1, 2, \cdots\cdots, n-1).$$

然由同節所述,

$$N_r' = \frac{(r+1)\,N_{r+1}}{n}.$$

以此代入上式,得

$$tg = \Sigma r(r+1)N_{r+1} \qquad (r=1, 2, \cdots\cdots, n-1).$$

於此兩邊加以(3)之開始部分,得

$$(1+t)g = \sum_r r^2 N_r \qquad (r=1, 2, \cdots\cdots, n).$$

以之與(4)比較得

$$(6) \qquad \sum_\mu a^2{}_\mu = t \quad (\mu=1, 2, \cdots\cdots, m-1).$$

爰得次

定理. 在屬於可遷羣$\mathfrak{G}$之羣母式X之行列式之素因數分解

$$|X| = \Phi_0 \Phi_1^{a_1} \Phi_2^{a_2} \cdots\cdots \Phi_{m-1}^{a_{m-1}}$$

中,其$a^2{}_1+a^2{}_2+\cdots\cdots+a^2{}_{m-1}$乃表一個定文字不動之約羣中之可遷系之數.

特別在$\mathfrak{G}$爲二重可遷時,$\mathfrak{H}$爲可遷的. 故$\sum_\mu a^2{}_\mu = 1$,因之$|X| = \Phi_0\Phi_1$,而與Φ_1相應之指標由(2)爲$\nu(R)-1$. 若$\mathfrak{G}$之次數爲n時,則Φ_1爲$n-1$次甚明. 遂得次

系. n次二重可遷羣乃有$n-1$次之單指標.

如第170節所示之四次及五次之交代羣分別有三次及四次之單指標者是.

注意 1. 本節(5)卽第71節之定理，與將屬於非遷羣之羣母式之行列式分解爲素因數以得(3)者同樣得以導出之.*

注意 2. $\mathfrak{G}$爲正置換羣時，$\mathfrak{H}=1, n-1$個文字得分爲$n-1$個之可遷系. 因之由定理遂得

$$1+a^2_1+a^2_2+\cdots\cdots+a^2_{m-1}=n.$$

此卽第165節(5)也.

177. 含n次巡回置換之n次可遷羣.

試取n次巡回置換

$$\mathrm{P}=(0, 1, 2, \cdots\cdots, n-1),$$

其屬於此之母式爲

$$(\mathrm{P})=\begin{pmatrix} 0 & 1 & 0 & \cdots\cdots & 0 \\ 0 & 0 & 1 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots\cdots & 1 \\ 1 & 0 & 0 & \cdots\cdots & 0 \end{pmatrix}$$

$$=(e_{i,j-1}) \qquad (i, j=1, 2, \cdots\cdots, n).$$

但$e_{i0}=e_{in}$. 而其指標行列式爲

$$(1) \qquad |(\mathrm{P})-(\mathrm{E})u|=(-1)^n(u^n-1).$$

---

*欲窺其詳請參閱著者之論文 On Transitive Groups viewed from Group-characteristics, Mem. Col. Sci. and Eng. Kyoto Imp. Univ. V (1913), pp. 297–300.

因之(P)之指標根爲

$$(2) \qquad 1, \omega, \omega^2, \cdots\cdots, \omega^{n-1}.$$

但 ω 爲示1之 n 乘原根者. 然由第162節第二定理系,其以P變形爲倍乘母式者之母式乃得存在. 以其一爲 $(a_{ij})^{-1}$, 則

$$(a_{ij})(\mathrm{P})(a_{ij})^{-1}=(\omega^{\rho_i}e_{ij}) \qquad (i, j=1, 2, \cdots\cdots, n).$$

但 $\rho_1, \rho_2, \cdots\cdots, \rho_n$ 爲將 $0, 1, 2, \cdots\cdots, n-1$ 自某個次序而取之者. 將此式換書之,則得

$$(a_{ij})(e_{i,j-1})=(\omega^{\rho_i}e_{ij})(a_{ij}) \qquad (i, j=1, 2, \cdots\cdots, n).$$

由是

$$\sum_k a_{ik}e_{k,j-1}=\sum_k \omega^{\rho_i}e_{ik}a_{kj} \qquad (k=1, 2, \cdots\cdots, n).$$

故

$$a_{i,j-1}=\omega^{\rho_i}a_{ij} \qquad (a_{i0}=a_{in}).$$

由是

$$a_{ij}=a_{in}\omega^{-\rho_i j}.$$

卽謂母式 (a_{ij}) 得如次也:

$$(3) \quad (a_{ij})=(a_{in}\omega^{-\rho_i j})=(a_{in}e_{ij})(\omega^{-\rho_i j}) \quad (i, j=1, 2, \cdots\cdots, n).$$

若 n 次一重可遷羣 $\mathfrak{G}$ 含有置換P時,其屬於 $\mathfrak{G}$ 之羣母式X之行列式所分解之素因數以爲

$$|\mathrm{X}|=\Phi_0\Phi_1^{a_1}\Phi_2^{a_2}\cdots\cdots\Phi_{m-1}^{a_{m-1}},$$

則 $a_1=a_2=\cdots\cdots=a_{m-1}=1$ 爲必要也. 蓋若令 $x_{\mathrm{E}}=-u$, $x_{\mathrm{P}}=1$, 而他之變數皆爲零,則上式爲

$$|(\mathrm{P})-(\mathrm{E})u|=\Phi_0\Phi_1^{a_1}\Phi_2^{a_2}\cdots\cdots\Phi_{m-1}^{a_{m-1}}.$$

然(1)之左邊無有等根. 故此右邊之指數不得不皆爲1故耳.

復次其以Φ_μ爲行列式之既約羣母式以爲X_μ，而X_0，X_1，……，X_{m-1}之直乘積表以$(X_0, X_1, \cdots\cdots, X_{m-1})$，則由上述，如

$$AXA^{-1}=(X_0, X_1, \cdots\cdots, X_{m-1})$$

者之常數母式A定然存在(第161節)．於X_μ其與P對應之母式爲(P_μ)時，則得選上之母式A使(P_μ)[$\mu=1, 2, \cdots\cdots, m-1$]爲倍乘的者自明．而若是之A，由上述非得有(3)形不可．卽

$$A=(a_{in}e_{ij})(\omega^{-\rho_i j}) \quad (i, j=1, 2, \cdots\cdots, n).$$

由是

$$(4)\quad (\omega^{-\rho_i j})X(\omega^{-\rho_i j})^{-1}=(a_{in}e_{ij})^{-1}(X_0, X_1, \cdots\cdots, X_{m-1})(a_{in}e_{ij})$$
$$=(X_0, X'_1, \cdots\cdots, X'_{m-1}).$$

但X'_μ爲與X_μ同值之羣母式．爰有

定理．含n次巡回置換之n次可遷羣$\mathfrak{G}$，其所屬之羣母式X，由一以1之n乘根爲項之母式，得將其變形爲既約羣母式之直乘積．而屬於X之既約羣母式之指數則皆爲1.

今特就n爲奇素數p時以明此定理之應用．設$\mathfrak{G}$爲p次一重可遷羣，其屬於此之羣母式以爲X，則由上定理，

$$(5)\qquad |X|=\Phi_0\Phi_1\Phi_2\cdots\cdots\Phi_{m-1};$$

而由前節定理則$m>2$．於(5)其與Φ_μ相應之羣指標以爲χ_μ，則p次巡回置換P之指標爲

(6) $$\chi_0(P)=1,$$

(7) $$\begin{cases} \chi_1(P)=\omega^{d_{11}}+\omega^{d_{12}}+\cdots\cdots, \\ \chi_2(P)=\omega^{d_{21}}+\omega^{d_{22}}+\cdots\cdots, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots. \end{cases}$$

但 ω 爲 1 之 p 乘原根. 且如前所述, 母式(P)之指標根乃互異者, 故(7)右邊之項亦互異, 而其與 1 相等者不存在也. 由是則在其項中其等於 ω 者必存在焉. 以之爲 $\omega^{d_{11}}$, 卽 $d_{11}=1$. 自他面觀, $|X|$ 之係數乃有理整數, 而由上定理, Φ_μ 之係數爲 ω 之有理式(此之係數爲有理數). 故於 Φ_μ 若以他之 p 乘原根 $\bar{\omega}$ 代其 ω, 而令由是所得者爲 $\bar{\Phi}_\mu$, 則由此之代入, 由(5)遂得

$$|X|=\Phi_0\bar{\Phi}_1\bar{\Phi}_2\cdots\cdots\bar{\Phi}_{m-1}.$$

然 Φ_μ 乃不可分解的, 且其中 x_E 之最高冪之係數爲 1. 故 $\bar{\Phi}_\mu$ 非與 $\Phi_1, \Phi_2, \cdots\cdots, \Phi_{m-1}$ 中之某一個相等不可. 因之, 若其與 $\bar{\Phi}_1$ 相應之羣指標表以 $\bar{\chi}_1$, 則

$$\bar{\chi}_1(P)=\bar{\omega}^{d_{11}}+\bar{\omega}^{d_{12}}+\cdots\cdots \qquad (d_{11}=1),$$

而此又必與(7)中之某一個等也. 然對有理整數 $c_1, c_2, \cdots\cdots, c_{p-1}$, 欲使

$$c_1\omega+c_2\omega^2+\cdots\cdots+c_{p-1}\omega^{p-1}=0,$$

則 $c_1=c_2=\cdots\cdots=c_{p-1}=0$ 爲必要. 故 $\chi_\lambda(P)$ 之項中其等於 $\bar{\omega}$ 者不存在時, 則 $\chi_\lambda(P)$ 不得與 $\bar{\chi}_1(P)$ 等. 於是在(7)之指標中其等於 $\bar{\chi}_1(P)$ 者僅限於含 $\bar{\omega}$ 者也. 然此由前所述只有一個.

故若以之爲 $\bar{\omega}=\omega^{d_{\mu 1}}$，則 $\bar{\chi}_1(\mathrm{P})=\chi_\mu(\mathrm{P})$. 卽

$$(8)\quad \chi_\mu(\mathrm{P})=\omega^{d_{\mu 1}d_{11}}+\omega^{d_{\mu 1}d_{12}}+\cdots\cdots \quad (\mu=1,2,\cdots\cdots,m-1).$$

因之 $\Phi_1=\Phi_\mu$ 爲必要. 由此是觀，則 $\Phi_1,\Phi_2,\cdots\cdots,\Phi_{m-1}$ 之次數悉爲同一. 將此以 f 示之，而比較 (5) 之兩邊之次數，則得

$$(9)\qquad p=1+(m-1)f, \text{ 或 } (m-1)f=p-1.$$

$\mathfrak{G}$ 之元素 Q 之巡回率爲 q 時，則 Q 之指標 $\chi_1(\mathrm{Q}),\chi_2(\mathrm{Q}),\cdots\cdots,\chi_{m-1}(\mathrm{Q})$ 任何個皆爲 1 之 q 乘根之和. 然 $\Phi_1,\Phi_2,\cdots\cdots,\Phi_{m-1}$ 之係數，如上所述，皆爲 1 之 p 乘根 ω 之有理式(此之係數爲有理數). 故若 q 對 p 互素，則 $\chi_1(\mathrm{Q}),\chi_2(\mathrm{Q}),\cdots\cdots,\chi_{m-1}(\mathrm{Q})$ 不得不悉爲有理數也.* 因之，此諸個雖以 $\bar{\omega}$ 代其 ω，而其值不變. 但自他方言，若 ω 代以 $\omega^{d_{\mu 1}}$，則如上述，Φ_1 遂爲 Φ_μ，其結果，$\chi_1(\mathrm{Q})$ 則成爲 $\chi_\mu(\mathrm{Q})$. 故

$$(10)\qquad \chi_1(\mathrm{Q})=\chi_2(\mathrm{Q})=\cdots\cdots=\chi_{m-1}(\mathrm{Q})$$

爲必要也.

由他方面以觀，$\mathfrak{G}$ 之元素，因 $\mathfrak{G}$ 之次數爲素數 p 之故，其置換之巡回率或爲 p 或對 p 互素. 若以與 p 元巡回約羣 $\{\mathrm{P}\}$ 共軛者之個數爲 N，則屬於此諸約羣而其巡回率爲 p 者之元素有 $(p-1)\mathrm{N}$ 個. 然 $\mathfrak{G}$ 之元數爲 ph $[h\not\equiv 0(\mathrm{mod}.\ p)]$ 甚明. 故由 Sylow 氏定理，巡回率 p 之元素得以此諸個而盡. 且以 $\mathfrak{G}$ 之元數觀，其巡回率對 p 互素之置換，乃屬於一個

*證明從略，讓諸代數學.

定文字不動者之約羣中;反之,其屬於此約羣之置換之巡回率,對 p 卽爲互素,明也.

茲用上所得結果,以計算關於單指標之公式(第167節)

$$(11)\qquad \sum_{R}\chi_\mu(R)=0,\quad \sum_{R}\chi_\mu(R)\chi_\lambda(R^{-1})=0$$

$$(\lambda,\mu=1,2,\cdots\cdots,m-1;\ \lambda\neq\mu)$$

之左邊. 此時以 $\mathfrak{G}$ 之置換分爲不動置換,巡回率爲 p 者,以及巡回率對 p 互素者之三組而分別以 E, S, Q 示之. 於是

$$\sum_{R}\chi_\mu(R)=\chi_\mu(E)+\sum_{s}\chi_\mu(S)+\sum_{Q}\chi_\mu(Q)$$

$$=f+N\sum_{s}\chi_\mu(P^s)+\sum_{Q}\chi_1(Q)\quad(s=1,2,\cdots\cdots,p-1).$$

然由(8),*

$$\sum\chi_\mu(P^s)=\sum(\omega^{sd_{\mu1}d_{11}}+\omega^{sd_{\mu1}d_{12}}+\cdots\cdots+\omega^{sd_{\mu1}d_{1f}})=-f.$$

故(11)之第一式換書之遂爲

$$(12)\qquad (1-N)f+\sum_{Q}\chi_1(Q)=0.$$

其次

$$\sum_{R}\chi_\mu(R)\chi_\lambda(R^{-1})=\chi_\mu(E)\chi_\lambda(E)+\sum_{s}\chi_\mu(S)\chi_\lambda(S^{-1})+\sum_{Q}\chi_\mu(Q)\chi_\lambda(Q^{-1})$$

$$=f^2+N\sum_{s}\chi_\mu(P^s)\chi_\lambda(P^{-s})+\sum_{Q}\{\chi_1(Q)\}^2\quad(s=1,2,\cdots\cdots,p-1).$$

---

*對此計算以及後之計算(13),皆利用(7)之右邊無有共通項以及 $\omega+\omega^2+\cdots\cdots+\omega^{p-1}=-1$ 之兩點者.

然

$$\chi_\mu(P^s)\chi_\lambda(P^{-s})=\sum_{\alpha,\beta}\omega^{s(d_{\mu 1}d_{1\alpha}-d_{\lambda 1}d_{1\beta})}\quad(\alpha,\beta=1,2,\cdots\cdots,f).$$

且因(7)之右邊無共通項，

$$d_{\mu 1}d_{1\alpha}-d_{\lambda 1}d_{1\beta}\not\equiv 0\pmod{p}.$$

故

$$\sum_s\chi_\mu(P^s)\chi_\lambda(P^{-s})=-f^2. \tag{13}$$

於是(11)之第二式如次：

$$(1-N)f^2+\sum_Q\{\chi_1(Q)\}^2=0. \tag{14}$$

復次，以$(m-1)f$乘(12)，由此所得，減去(14)之乘以$(m-1)$者，再適用(9)，則得

$$\sum_Q\{(p-1)-(m-1)\chi_1(Q)\}\chi_1(Q)=0.$$

然由前節(2)及本節(10)，

$$\nu(Q)=1+\sum_\mu\chi_\mu(Q)=1+(m-1)\chi_1(Q). \tag{15}$$

以此代入上式，

$$\sum_Q\{p-\nu(Q)\}\chi_1(Q)=0. \tag{16}$$

此中$p-\nu(Q)>0$甚明，又由前所述，$\chi_1(Q)$爲有理整數，故由(15)，則$\chi_1(Q)\not\equiv 0$爲必要．因之，爲(16)之成立計則對所有之Q，非

$$\chi_1(Q)=0,\text{ 隨之 }\nu(Q)=1$$

不可也．此卽示屬於一個定文字不動者之約羣之置換(非不動置換)乃爲使唯一個文字不動者而已也．卽$\mathfrak{S}$爲

$p-1$級焉. 因之,由第174節之定理及第100節之定義得次

定理. 凡次數爲奇素數者之一重可遷羣爲亞巡回羣之約羣. (Burnside.)

由此定理可知一重可遷羣任何個皆複合的. 且此在次數爲p之冪時亦克成立. 卽p^m次一重可遷羣含有p^m次之巡回置換時,則此羣爲複合的也.*

---

*請參閱 Burnside, Theory of Groups (2nd ed.) p. 343,及著者之 On Transitive Groups viewed from Group-characteristics, Mem. Col. Sci. & Eng. Kyoto Imp. Uni. V. (1913), p. 313.

索　引

一　畫

二　畫

三　畫

四　畫

五 畫

六 畫

七 畫

八 畫

九　畫

十 畫

十一畫

十二畫

十 三 畫

十九畫

二十二畫