La composizione dei Gruppi finiti il cui grado è la quinta potenza di un numero primo.

(Di G. Bagnera, *a Palermo.)*

PREFAZIONE.

Cayley ha per il primo posta l'importante questione (*) di costruire tutti i possibili gruppi di un dato grado n.

Non bisogna, nemmeno lontanamente, sperare che il problema, enunciato in termini così generali, possa in qualche maniera essere abbordabile: delle ipotesi sono necessarie sopra l'intero n per servire di fondamento ad un ragionamento qualsiasi, e le ipotesi che hanno condotto in questi ultimi anni ai più rimarchevoli risultati si riferiscono al modo con cui l'intero n è composto con i suoi fattori primi.

Il sig. Netto ha dato (**) tutti i gruppi il cui grado è il prodotto di due soli numeri primi eguali o diseguali; il sig. Hölder ha, per la prima volta (***), dimostrato che tutti i gruppi il cui grado è il prodotto di tre numeri primi, eguali o diseguali, sono metaciclici (risolubili) (****); poi, in un lavoro posteriore (*****), lo stesso Autore ha dato la composizione dei

(*) Cayley's *Mathematical papers*, Vol. II, 125.

(**) Netto. *Substitutionentheorie und ihre Anwendung auf die Algebra*, 1882, pag. 133.

(***) Hölder. *Die einfachen Gruppen im ersten und zweiten Hundert der Ordnungszahlen.* Mathematische Annalen, Band 40, a. 1892.

(****) Nel presente lavoro mi servo delle denominazioni che, per i gruppi finiti, sono state adottate dal sig. H. Weber nel suo libro: *Lehrbuch der Algebra.*

(*****) Hölder. *Die Gruppen der Ordnungen* p^3, $p\,q^2$, $p\,q\,r$, p^4. Mathematische Annalen, Band 43, a. 1893.

gruppi di tale grado e quella di tutti i gruppi, il cui grado è la quarta potenza di un numero primo.

Seguendo lo stesso ordine d'idee, il sig. FROBENIUS ha osservato (*) che tutti i gruppi, il cui grado è il prodotto di quattro fattori primi, sono metaciclici, fatta eccezione per il grado $2^2 . 3 . 5 = 60$ dove si presenta il noto gruppo dell'icosaedro che è un gruppo semplice. Il sig. FROBENIUS è andato molto più in là: egli ha stabilito i due sorprendenti risultati generali che ogni gruppo, il cui grado è il prodotto di ν fattori primi tra cui ve ne siano $\nu - 1$ eguali, oppure il prodotto di ν fattori primi due a due diseguali, è necessariamente metaciclico, e, chi ha interesse di conoscere le ingegnose dimostrazioni di questi due teoremi, potrebbe leggerle nel libro del signor H. WEBER (**).

Il sig. HÖLDER, con molta fortuna, è ritornato sulla questione nell'anno 1895 (***) e, ponendo a fondamento l'ultimo dei due citati teoremi del sig. FROBENIUS, ha dato la composizione e la classificazione di tutti i possibili gruppi, il cui grado è il prodotto di quanti si vogliano fattori primi due a due diseguali; inoltre, nello stesso lavoro, ha stabilito il notevolissimo risultato che ogni gruppo di tale grado è necessariamente isomorfo ad un gruppo lineare di permutazioni.

Ma, dare la composizione e la classificazione di tutti i gruppi, il cui grado è il prodotto di quanti si vogliano fattori primi eguali, è un problema di ben altra portata. Su questo riguardo i risultati generali più importanti sono dovuti a SYLOW (****). Il sig. HÖLDER, nel citato lavoro del 1893, ha formato tutti i gruppi dei gradi p^3 e p^4, e, quasi contemporaneamente, è apparso un lavoro del sig. YOUNG (*****) il quale, in fondo, si è anche limitato a dare la composizione di tutti i gruppi dei gradi p^3 e p^4.

Io do, per la prima volta, la composizione di tutti i gruppi di grado p^5.

(*) FROBENIUS. *Ueber auflösbare Gruppen.* Sitzungsberichte der Berliner Akademie, a. 1893, I, pag. 337.

(**) H. WEBER. *Lehrbuch der Algebra.* Vol. II, pag. 129 e sg.

(***) HÖLDER. *Die Gruppen mit quadratfreier Ordnungszahl.* Göttinger Nachr., a. 1895.

(****) SYLOW. *Théorèmes sur les groupes de substitutions.* Mathematische Annalen, Band V.

(*****) YOUNG. *On the determination of Groups whose order is a power of a prime.* American Journal of Mathematics, Vol. XV, a. 1893.

È precisamente a partire dal valore $\nu = 5$ che il problema della composizione dei gruppi di grado p^ν mostra la sua vera faccia, giacchè, mentre qualunque sia il numero primo p esistono sempre:

un solo gruppo di grado p; due soli gruppi di grado p^2; cinque soli gruppi di grado p^3; soltanto quindici gruppi di grado p^4 tutte le volte che è $p > 2$; per i gruppi di grado p^5 accade invece che il loro numero dipende essenzialmente dal valore del numero primo p.

Il caso particolare di $p = 2$ è stato tentato dal sig. LEVAVASSEUR: egli dice (*) di aver trovato più di settantacinque gruppi di grado $2^5 = 32$ e di non avere ancora terminata la enumerazione; però, i risultati del sig. LEVAVASSEUR sono stati messi in dubbio dal sig. MILLER (**), il quale, sebbene giunga anch'egli a risultati non esatti, si accosta maggiormente al vero; giacchè, come appresso si vedrà, i gruppi di grado 32 sono soltanto in numero di cinquanta.

Nella prima parte di questo lavoro, dopo di avere stabilito nel § I il principio generale, che serve di fondamento alle successive ricerche, ritrovo anzitutto nel § II i gruppi di grado p^3 e p^4: ciò è stato necessario per potere, con uniformità di metodo, trattare i gruppi di grado p^5. Le differenze che si potrebbero osservare tra la tabella che sta alla fine del detto paragrafo ed i risultati dei sig. HÖLDER e YOUNG non hanno, e si comprende, niente di sostanziale: esse provengono dal fatto che io ho, qualche volta, scelto in modo diverso i tipi ridotti; però, nella maggior parte dei casi, per fare il confronto basta cambiare il nome agli elementi generatori.

Nel § III poi mi occupo della composizione dei gruppi di grado p^5, limitandomi al caso in cui questi posseggono più d'un divisore Abeliano d'indice p.

Nella seconda parte del lavoro, la quale comprende i §§ IV, V, VI e VII, è sviluppata l'analisi che riguarda gli altri casi, ed è data la classificazione completa di tutti i gruppi di grado p^5.

La classificazione, che ho adottata, a me basta per esser sicuro che nessun gruppo di grado p^5 mi sia sfuggito, e non mi curo di sapere se questa classificazione sia più o meno conveniente nel caso generale. D'altronde, giacchè in tal caso nulla o poco è conosciuto, una classificazione generale sarebbe cosa perfettamente arbitraria.

(*) *Comptes Rendus*, a. 1896, t. 122, pag. 182.
(**) *Comptes Rendus*, a. 1896, t. 122, pag. 370.

Quantunque io abbia fatto ogni sforzo per dare la massima omogeneità ai procedimenti, debbo confessare che, su questo punto, non ho potuto trionfare giacchè, ho dovuto spesso ricorrere ad artifizi ed a suddivisioni di ripiego anche nella ricerca dei gruppi appartenenti ad una medesima classe; ma, io dubito fortemente che questo fatto sia una necessità inerente alla natura del problema.

PARTE PRIMA.

§ I. Generalità.

1. Sia P un gruppo finito di grado n e Γ una classe di n elementi sopra la cui natura non si fa alcuna ipotesi. Io suppongo che, in un modo qualunque, si sia stabilita una corrispondenza S, univoca e reciproca, tra gli elementi del gruppo P e quelli della classe Γ e denoto con $S(e)$ l'elemento di Γ che corrisponde all'elemento e di P.

Essendo e' ed e'' due arbitrari elementi di P, si ponga *per definizione:*

$$S(e')\,S(e'') = S(e'\,e'');$$

allora, rispetto a questa legge di composizione, gli elementi di Γ costituiscono un gruppo $G = S(P)$ che si può pensare come il più generale gruppo oloedricamente isomorfo a P. Chiamerò brevemente il gruppo G una *rappresentazione* di P in Γ: cambiando la corrispondenza S cambia, in generale, la legge di composizione degli elementi di Γ e si ottiene un'altra rappresentazione di P in Γ.

Se T è una operazione che permuta gli elementi di Γ, l'operazione TS stabilisce una nuova corrispondenza tra gli elementi di P e gli elementi di Γ, e può accadere, in particolare, che le due corrispondenze S e TS definiscano la stessa legge di composizione negli elementi di Γ. Allora, l'operazione $S^{-1}TS$ fa corrispondere ad un elemento di P un elemento di P, in modo tale che al prodotto di due elementi corrisponde il prodotto dei due elementi corrispondenti. Esprimerò questo fatto dicendo che l'operazione $S^{-1}TS$ produce una trasformazione d'isomorfismo del gruppo P in sè.

È chiaro che tutte le possibili operazioni T, che corrispondono a trasformazioni d'isomorfismo del gruppo P in sè, costituiscono un gruppo divisore del gruppo simmetrico delle permutazioni di n cifre.

2. Siano:

$$E_1, E_2, \ldots, E_n, \tag{1}$$

elementi di Γ. Se, nella rappresentazione $G = S(P)$, il composto:

$$E_1^{\alpha_1} E_2^{\alpha_2} \dots E_\nu^{\alpha_\nu},$$

facendo percorrere ai numeri interi indipendenti $\alpha_1, \alpha_2, \dots, \alpha_\nu$ dati sistemi di numeri, fornisce tutti gli elementi di Γ, e ciascuno una sola volta, dirò che il gruppo G possiede la *base* (1) a ν dimensioni.

Denoti:

$$\Phi(E_1, E_2, \dots, E_\nu) = \Psi(E_1, E_2, \dots, E_\nu), \tag{2}$$

una relazione tra gli elementi (1), e si faccia subire agli elementi di Γ una qualunque operazione T. Allora si passa dalla rappresentazione $S(P)$ alla rappresentazione $T\,S(P)$ e viene perciò ad essere cambiata la legge di composizione degli elementi di Γ: dunque, la relazione (2), che sussiste nella rappresentazione $S(P)$, non si verifica, in generale, nella rappresentazione $T(G) = T\,S(P)$.

Epperò, una volta fissate alcune relazioni come la (2), io posso propormi il problema di cercare tutte le possibili operazioni T, che conservano le dette relazioni. Queste tali operazioni costituiscono un gruppo, il quale contiene, come divisore, il gruppo formato da tutte le operazioni T che corrispondono a trasformazioni d'isomorfismo del gruppo P in sè.

3. Io mi debbo occupare nel presente lavoro solamente di gruppi P_ν il cui grado è una potenza p^ν di un numero primo p: è quindi conveniente di fissare le idee al caso mio.

Se G_ν è una rappresentazione qualunque di un tale gruppo in Γ, è noto (*) che è possibile costruire una serie di composizione:

$$G_\nu, G_{\nu-1}, G_{\nu-2}, \dots, G_1, \tag{3}$$

tale che ogni termine della serie sia divisore normale di tutti i termini che lo precedono. L'ultimo termine G_1 della serie è allora un divisore normale di grado p del gruppo G_ν e quindi, l'elemento generatore E_1 di G_1 ha la nota (**) proprietà di essere invertibile con tutti gli elementi di G_ν.

(*) V. ad es. una mia Nota: *Sopra i divisori normali d'indice primo di un gruppo finito.* Rendiconti della R. Accademia dei Lincei. Vol. VII, 2.° sem., anno 1898.

(**) Se E è un elemento di G_ν di grado p^k, dalla relazione $E^{-1} E_1 E = E_1^\alpha$ si deduce $\alpha^{p^k} \equiv 1 \pmod p$ e quindi $\alpha \equiv 1 \pmod p$.

Gli elementi di G_ν, che godono la detta proprietà, formano evidentemente gruppo e questo gruppo, giacchè contiene G_1, non può coincidere col gruppo formato dall'elemento identico.

Ciò posto, chiamerò *divisore invertibile* di G_ν il massimo divisore *proprio* di G_ν tale che ogni suo elemento è invertibile con qualunque elemento del gruppo principale G_ν, e supporrò, cosa sempre possibile, che questo divisore faccia parte della serie di composizione (3).

Bisogna osservare che il divisore invertibile H di un gruppo G_ν è perfettamente determinato, tranne il caso in cui G_ν è un gruppo Abeliano: allora si può scegliere come gruppo H un divisore qualunque d'indice p di G_ν.

Se p^h è il grado di H, il numero:

$$\mu = \nu - h - 1,$$

è un numero invariantivo del gruppo G_ν e questo numero è, per quel che segue, della massima importanza.

Un gruppo G_ν, che ha il numero invariantivo μ, sarà denotato con G_ν^μ; così, ad es., i gruppi G_ν^0 sono gruppi Abeliani.

4. Nella Nota citata precedentemente, supponendo che un gruppo finito G possegga divisori normali d'indice primo p, ho chiamato *indipendenti* λ di tali divisori, quando la loro intersezione K ha in G l'indice p^λ, ed ho fatto vedere che, se λ è il numero totale dei divisori normali indipendenti d'indice p contenuti in G, questo possiede $\frac{p^\lambda - 1}{p-1}$, e non più, divisori normali d'indice p.

Inoltre ho dimostrato che il gruppo complementare $G|K$ è Abeliano ed ha tutti i suoi elementi di grado p; dunque, due arbitrari elementi del gruppo G sono invertibili rispetto a mod. K e le potenze p^{me} di tutti gli elementi di detto gruppo appartengono a K.

In un gruppo G_ν, di grado p^ν, ogni divisore d'indice p è normale, quindi si ha $\lambda \geq 1$, ed io dico che si ha $\lambda = 1$ solamente quando il gruppo G_ν è ciclico.

Siccome la proposizione si verifica per i gruppi di grado p^2, basta provare che, ammettendola vera per i gruppi di grado $p^{\nu-1}$, sussiste ancora per i gruppi di grado p^ν. Si chiami G_1 un divisore normale di grado p del gruppo G_ν: se questo gruppo ha un solo divisore d'indice p, anche il gruppo $G_\nu|G_1$ complementare di G_1, ha un solo divisore d'indice p, e giacchè detto gruppo complementare è di grado $p^{\nu-1}$, esso è ciclico per ipotesi. Sia dunque

E un elemento di G_ν di grado $p^{\nu-1}$ rispetto a mod. G_1 ed E_1 un elemento generatore di G_1. Se fosse $E^{p^{\nu-1}} = 1$, il gruppo G_ν, contrariamente all'ipotesi, ammetterebbe il divisore d'indice p generato dall'elemento E ed il divisore d'indice p generato dai due elementi E^p ed E_1. Dunque, l'elemento E è di grado p^ν e quindi G_ν è un gruppo ciclico.

Ciò posto, di ogni gruppo G_ν^μ io do anche il numero λ dei divisori indipendenti d'indice p che il detto gruppo possiede e convengo di denotare G_ν^μ con $G_\nu^{\mu\,\lambda}$ quando voglio mettere in evidenza il numero invariantivo λ.

È utile osservare che, se è $\mu > 0$, deve essere $2 \leq \lambda < \nu$: ciò risulta dalle cose ultimamente dette.

Inoltre si noti che, nell'ipotesi di $\mu > 0$, il gruppo G_ν H non è ciclico, e quindi esistono almeno due distinti divisori d'indice p di G_ν che contengono il gruppo H.

5. Ritornando alla serie (3), che io chiamo una serie *canonica* di composizione di G_ν, sia E_i $(i = 1, 2, \ldots, \nu)$ un elemento di G_i fuori di G_{i-1} e G_0 il gruppo formato dall'elemento identico: siano poi E'_i, E''_i, ... elementi qualunque di G_i.

Ciò posto, giacchè il gruppo G_i G_{i-1} è un divisore normale di grado p del gruppo G_ν G_{i-1}, risulta che l'elemento E_i è invertibile con ogni elemento del gruppo G_ν rispetto a mod. G_{i-1}; dunque, in particolare, supponendo $j > i$, si ha:

$$E_j^{-1} E_i E_j = E_i E'_{i-1}, \quad E_i^p = E''_{i-1}; \tag{4}$$

dove gli elementi E'_{i-1} ed E''_{i-1} appartengono, per quello che si è detto nel n.° precedente, al gruppo K intersezione dei divisori d'indice p del gruppo G_ν.

Data la serie di composizione (3) e, relativamente ad essa, definendo gli elementi:

$$E_\nu, \; E_{\nu-1}, \ldots, \; E_1,$$

nell'anzidetto modo, il composto:

$$E_\nu^{\alpha_\nu} E_{\nu-1}^{\alpha_{\nu-1}} \ldots E_1^{\alpha_1},$$

fornisce tutti gli elementi del gruppo G_ν, e ciascuno una sola volta, attribuendo agli interi α_ν, $\alpha_{\nu-1}, \ldots, \alpha_1$ valori scelti ad arbitrio nel sistema di numeri $0, 1, 2, \ldots, p-1$. Dunque, gli elementi E_ν, $E_{\nu-1}, \ldots, E_1$ costituiscono una base a ν dimensioni del gruppo G_ν e tra i detti elementi sussistono le relazioni (4). Una tale base la chiamerò una *base canonica* (*) di G_ν.

(*) L'esistenza di una base canonica per un gruppo di grado p^ν è stata, per la prima volta, dimostrata da SYLOW, l. c.

Quando si conosce una base canonica di G_ν è perfettamente individuata una serie canonica di composizione del gruppo G_ν; ma, in corrispondenza ad ognuna di dette serie, si possono definire più basi canoniche.

Sia:

$$\mathrm{E}_\nu, \mathrm{E}_{\nu-1}, \ldots, \mathrm{E}_1,$$

una base canonica di G_ν diversa dalla precedente. L'operazione che porta ogni elemento $\mathrm{E}_\nu^{\alpha_\nu} \mathrm{E}_{\nu-1}^{\alpha_{\nu-1}} \ldots \mathrm{E}_1^{\alpha_1}$ nell'elemento $E_\nu^{\alpha_\nu} E_{\nu-1}^{\alpha_{\nu-1}} \ldots E_1^{\alpha_1}$, e che rappresenterò con la notazione:

$$T = \begin{pmatrix} E_\nu, & E_{\nu-1}, & \ldots, & E_1 \\ \mathrm{E}_\nu, & \mathrm{E}_{\nu-1}, & \ldots, & \mathrm{E}_1 \end{pmatrix},$$

lascia inalterata la forma di tutte le relazioni (4), ma cambia, in generale, gli elementi E'_i ed E''_i che ivi figurano. Si può allora scegliere l'operazione T in modo che la rappresentazione $T(G_\nu)$ sia, da un dato punto di vista, più conveniente della rappresentazione G_ν.

Ma ciò che è ancora più importante è il fatto che, date due rappresentazioni dello stesso gruppo P_ν in Γ e scegliendo in ciascuna di esse una base canonica, si può passare dalla serie di relazioni (4) relativa alla prima rappresentazione alla serie di relazioni (4) relativa alla seconda rappresentazione mediante una operazione T appartenente al gruppo delle operazioni che portano una base canonica in una base canonica.

§ II. I Gruppi di grado p^3 e p^4.

6. Esistono soltanto tre gruppi G_3^0, i quali sono:

un gruppo $G_3^{0,1}$, che è il gruppo ciclico;

un gruppo $G_3^{0,2}$, che ha un elemento di grado p^2 ed un elemento di grado p il quale non è una potenza del primo;

un gruppo $G_3^{0,3}$, che ha tutti i suoi elementi di grado p.

Mettendo in evidenza, per ciascuno di questi tre gruppi, gl'invarianti del sig. Frobenius (*), scriverò:

$$G_3^{0,1}\{[p^3]\}, \qquad G_3^{0,2}\{[p^2][p]\}, \qquad G_3^{0,3}\{[p][p][p]\}.$$

(*) Frobenius u. Stickelberger. *Crelle's Journal*, Vol. LXXXVI, pp. 224-236.

7. I gruppi G_3 che non sono Abeliani sono gruppi $G_3^{1,2}$.

Se:

$$E_3,\ E_2,\ E_1,$$

è una base canonica di un tale gruppo, con le notazioni del paragrafo precedente si ha $G_1 = H = K$, e quindi è:

$$\left.\begin{aligned} &E_3^{-1} E_2 E_3 = E_2 E_1^{\alpha}, \qquad E_3^{-1} E_1 E_3 = E_1, \qquad E_2^{-1} E_1 E_2 = E_1; \\ &E_3^{p} = E_1^{\gamma}, \qquad E_2^{p} = E_1^{\beta}, \qquad E_1^{p} = 1; \end{aligned}\right\} \tag{1}$$

dove il numero α è primo con p. Allora, dati i due elementi E_3, E_2, si può definire l'elemento E_1 mediante la relazione:

$$E_3^{-1} E_2 E_3 = E_2 E_1, \tag{2}$$

e perciò, nelle relazioni (1), ritengo $\alpha \equiv 1 \pmod p$.

Io ho, in questo modo, dimostrato che, se esiste un gruppo P_3 rappresentato in Γ da un $G_3^{1,2}$, gli elementi E_3, E_2, E_1 di una base canonica del gruppo rappresentativo debbono soddisfare le (1). Bisogna pertanto provare che un tale gruppo P_3 effettivamente esiste.

Si considerino come elementi tutti i simboli:

$$e_3^{x}\, e_2^{y}\, e_1^{z}, \tag{3}$$

che si ottengono attribuendo agli esponenti x, y, z arbitrari valori interi, e si chiamino eguali due tali simboli quando si deducono l'uno dall'altro facendo variare ordinatamente i detti esponenti di $p\,k_3$, $p\,k_2$, h_1, purchè gl'interi h_1, k_2, k_3 soddisfino alla congruenza:

$$h_1 + \beta\, k_2 + \gamma\, k_3 \equiv 0 \pmod p.$$

Si ottengono così soltanto p^3 elementi distinti.

Così posto, se si assume come definizione del prodotto di due elementi la relazione:

$$(e_3^{x'} e_2^{y'} e_1^{z'})\,(e_3^{x''} e_2^{y''} e_1^{z''}) = e_3^{x'+x''} e_2^{y'+y''} e_1^{z'+z''+y'x''}, \tag{4}$$

riesce facile verificare che, essendo A, B, C elementi (3), sono soddisfatte le condizioni:

1.ª) se è $A = B$, è $A\,C = B\,C$ e $C\,A = C\,B$,

2.ª) se è $A\,C = B\,C$ oppure $C\,A = C\,B$, è $A = B$,

3.ª) in ogni caso, è $(A\,B)\,C = A\,(B\,C)$.

I simboli (3), rispetto alla legge di composizione (4), costituiscono dunque un gruppo P_3, di cui l'elemento unità è il simbolo $e^0{}_3\, e^0{}_2\, e^0{}_1$, e se si rappresenta detto gruppo in Γ facendo corrispondere agli elementi $e_3{}^1\, e_2{}^0\, e_1{}^0$, $e_3{}^0\, e_2{}^1\, e_1{}^0$, $e_3{}^0\, e_2{}^0\, e_1{}^1$ ordinatamente gli elementi E_3, E_2, E_1, questi costituiscono una base canonica di un gruppo $G_3{}^{\beta,\gamma}$ e soddisfano alle relazioni (1), le quali perciò, nel senso del sig. Dyck (*), definiscono sempre un gruppo $G_3{}^{\beta,\gamma}$ qualunque siano gl'interi β e γ.

8. Ma, giacchè non sono da considerarsi come gruppi distinti le diverse rappresentazioni di uno stesso gruppo, bisogna vedere come variano β e γ relativamente al gruppo delle operazioni:

$$T = \begin{pmatrix} E_3, & E_2, & E_1 \\ \mathbf{E}_3, & \mathbf{E}_2, & \mathbf{E}_1 \end{pmatrix},$$

che lasciano inalterata la (2).

Ponendo:

$$\mathbf{E}_2 \equiv E_3{}^u\, E_2{}^v, \qquad \mathbf{E}_2 \equiv E_3{}^r\, E_2{}^s, \qquad (\mathrm{mod}\ G_1), \tag{5}$$

affinchè la relazione (2) si conservi, bisogna prendere $\mathbf{E}_1 = E_1{}^{\Delta}$; quindi, per non contraddire alla definizione dell'elemento $\mathbf{E}_1$, deve essere il determinante $\Delta = u\,s - v\,r$ primo con p.

D'altra parte, io osservo che le operazioni T' appartenenti alla classe definita dalle relazioni:

$$\mathbf{E}_3 \equiv E_3, \qquad \mathbf{E}_2 \equiv E_2, \qquad (\mathrm{mod}\ G_1),$$

non alterano β e γ e costituiscono un divisore normale del gruppo delle operazioni T definito precedentemente; dunque, rispetto alla questione di cui mi sto occupando, posso ritenere eguale all'operazione identica ogni operazione di detta classe. In questa ipotesi, le (5) definiscono un'unica operazione che io rappresento con la notazione:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix}.$$

Ora, si osservi che la relazione (2) dà subito:

$$(E_3\, E_2)^n = E_3{}^n\, E_2{}^n\, E_1{}^{\binom{n}{2}}, \tag{6}$$

(*) W. Dyck. *Gruppentheoretische Studien.* Mathematische Annalen, Band XX, a. 1882.

e quindi, *se è* $p > 2$, si ha:

$$E_3^p = E_3^{up} E_2^{vp} = E_1^{\gamma u + \beta v}, \qquad E_2^p = E_3^{rp} E_2^{sp} = E_1^{\gamma r + \beta s}.$$

Dunque, se β_1 e γ_1 sono i nuovi valori di β e γ dopo avere eseguita la detta operazione, si trova:

$$\Delta\gamma_1 \equiv \gamma u + \beta v, \qquad \Delta\beta_1 \equiv \gamma r + \beta s, \qquad (\mathrm{mod}\, p).$$

Allora, se β e γ sono entrambi nulli (mod p), lo stesso accade per β_1 e γ_1 ed il gruppo $G_3^{1,2}$ ha tutti i suoi elementi di grado p; in caso contrario una almeno delle due operazioni:

$$\begin{vmatrix} \beta & -\gamma \\ 0 & 1 \end{vmatrix}, \qquad \begin{vmatrix} \beta & -\gamma \\ 1 & 0 \end{vmatrix},$$

ha il determinante primo con p, e questa porta β e γ ordinatamente nei resti 1 e 0 presi rispetto al modulo p.

In conclusione esistono, se è $p > 2$, due soli gruppi $G_3^{1,2}$ in corrispondenza alle due serie di formole:

$$\left.\begin{aligned} E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1; \\ E_3^p = 1, \quad E_2^p = E_1, \quad E_1^p = 1; \end{aligned}\right\} \qquad (7)$$

e, tralasciando di scrivere le relazioni che esprimono che l'elemento E_1 appartiene al divisore invertibile H, questi due gruppi sono perfettamente determinati dalle relazioni (7) insieme alla (2).

9. Il caso di $p = 2$ esige una breve analisi particolare. In questa ipotesi, tutte le possibili operazioni:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

formano un gruppo di grado sei che può essere generato dalle due operazioni:

$$\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}, \qquad \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix},$$

di secondo e terzo ordine rispettivamente.

Osservando che la (6) dà:

$$(E_3 E_2)^2 = E_3^2 E_2^2 E_1,$$

si vede che l'ipotesi di $E_2^2 = E_1$ ed $E_3^2 = E_1$ non è cambiata dalle dette due

operazioni; mentre qualunque altro caso si può ridurre a quello in cui è $E_2^2 = 1$ ed $E_3^2 = 1$.

Dunque, anche quando è $p = 2$, esistono due soli gruppi $G_3^{1,2}$ di grado $2^3 = 8$ definiti dalle due serie di formole:

$$E_3^2 = 1\,, \quad E_2^2 = 1\,, \quad E_1^2 = 1\,;$$

$$E_3^2 = E_1\,, \quad E_2^2 = E_1\,, \quad E_1^2 = 1\,,$$

e dalla relazione (2).

10. Passo ora ad occuparmi dei gruppi di grado p^4 cominciando a scrivere senz'altro i gruppi di tale grado che sono Abeliani.

Esistono soltanto cinque gruppi G_4^0 i quali sono:

un gruppo $G_4^{0,1}$, due gruppi $G_4^{0,2}$, un gruppo $G_4^{0,3}$ ed un gruppo $G_4^{0,4}$.

Mettendo in evidenza i rispettivi invarianti, rappresenterò i detti gruppi nel seguente modo:

$$G_4^{0,1} \,|\,[p^4]\,|\,, \quad G_4^{0,2} \,|\,[p^3]\,[p]\,|\,, \quad G_4^{0,2} \,|\,[p^2]\,[p^2]\,|\,,$$

$$G_4^{0,3} \,|\,[p^2]\,[p]\,[p]\,|\,, \quad G_4^{0,4} \,|\,[p]\,[p]\,[p]\,[p]\,|\,.$$

Il gruppo $G_4^{0,1}$ è il gruppo ciclico di grado p^4; il primo dei due gruppi $G_4^{0,2}$ ha p divisori $G_3^{0,1}$ ed un solo divisore $G_3^{0,2}$, mentre il secondo ha $p+1$ divisori $G_3^{0,2}$; il gruppo $G_4^{0,3}$ ha un solo divisore $G_3^{0,3}$ e $p^2 + p$ divisori $G_3^{0,2}$; finalmente, tutti i $\frac{p^4 - 1}{p - 1}$ divisori d'indice p del gruppo $G_4^{0,4}$ sono gruppi $G_3^{0,3}$.

11. I gruppi G_4 che non sono Abeliani sono gruppi G_4^1 oppure gruppi G_4^2: io comincio ad occuparmi dei primi.

Sia:

$$G_4^1\,, \quad G_3\,, \quad G_2\,, \quad G_1\,,$$

una serie canonica di composizione di un gruppo G_4^1 scelta in modo che si abbia $G_2 = H$.

Giacchè esistono (n.° 4) due divisori d'indice p di G_4^1 che contengono H, il gruppo K, o coincide con H oppure è un divisore proprio di H, secondo che G_4^1 è un $G_4^{1,2}$ od un $G_4^{1,3}$.

Ciò posto, se:

$$E_4\,, \quad E_3\,, \quad E_2\,, \quad E_1\,,$$

denota una base canonica relativa alla precedente serie di composizione, si ha:

$$E_4^{-1} E_3 E_4 = E_3 E_2'\,, \quad E_4^p = E_2''\,, \quad E_3^p = E_2'''\,, \quad E_2^p = E_1'\,, \quad E_1^p = 1. \qquad (8)$$

Trattandosi di un gruppo G_4^1, l'elemento E_3 non è invertibile con E_4, mentre il contrario accade per l'elemento E_3^p che appartiene ad H; quindi, dalla prima delle (8), risulta che E_2' è un elemento di grado p ed io posso ritenere $E_2' = E_1$. Allora, la prima delle formole (8) si può sostituire con:

$$E_4^{-1} E_3 E_4 = E_3 E_1 . \tag{9}$$

Se il gruppo $H = G_2$ è ciclico, E_2'' ed E_2''' sono potenze di E_2; quindi, scegliendo E_2 in modo che sia $E_2^p = E_1$, le ultime quattro delle relazioni (8) si possono, in questo caso, sostituire con:

$$E_4^p = E_2^a , \quad E_3^p = E_2^b , \quad E_2^p = E_1 , \quad E_1^p = 1. \tag{10}$$

Dopo ciò, si può subito dimostrare che le formole (9) e (10), insieme a quelle che esprimono che l'elemento E_2 appartiene ad H, definiscono, qualunque siano gl'interi α e β, un gruppo G_4^1.

Si considerino i simboli che si ottengono da:

$$e_4^x e_3^y e_2^z e_1^t ,$$

attribuendo ad x, y, z, t arbitrari valori interi, e si chiamino eguali due tali simboli quando si possono ottenere l'uno dall'altro facendo variare i detti interi ordinatamente di $p k_4$, $p k_3$, h_2, h_1, purchè sia:

$$\alpha k_4 + \beta k_3 + h_2 + p h_1 \equiv 0, \pmod{p^2}.$$

Dietro questa convenzione si ottengono solamente p^4 simboli distinti.

Ora, ponendo per definizione:

$$(e_4^{x'} e_3^{y'} e_2^{z'} e_1^{t'}) (e_4^{x''} e_3^{y''} e_2^{z''} e_1^{t''}) = e_4^{x'+x''} e_3^{y'+y''} e_2^{z'+z''} e_1^{t+t'+y'x''},$$

riesce facile verificare che, rispetto a questa legge di composizione i simboli $e_4^x e_3^y e_2^z e_1^t$ costituiscono un gruppo. Se si rappresenta questo gruppo in Γ facendo corrispondere ai simboli:

$$e_4^1 e_3^0 e_2^0 e_1^0, \quad e_4^0 e_3^1 e_2^0 e_1^0, \quad e_4^0 e_3^0 e_2^1 e_1^0, \quad e_4^0 e_3^0 e_2^0 e_1^1,$$

ordinatamente gli elementi E_4, E_3, E_2, E_1, questi costituiscono una base canonica di un gruppo G_4^1 e verificano le relazioni (9) e (10).

Si osservi che l'operazione:

$$\begin{pmatrix} E_4 & E_3 & E_2 & E_1 \\ E_4 E_2^{\lambda} & E_3 E_2^{\mu} & E_2 & E_1 \end{pmatrix},$$

cambia α e β rispettivamente in $\alpha + \lambda p$ e $\beta + \mu p$; quindi, se α e β sono multipli di p, si può supporre $\alpha = \beta = 0$.

Se uno dei due numeri α, β è primo con p, io suppongo che sia β primo con p giacchè, in caso contrario, scambio α in β mediante l'operazione:

$$\begin{pmatrix} E_4 & E_3 & E_2 & E_1 \\ E_3^{-1} & E_4^{-1} & E_2^{-1} & E_1^{-1} \end{pmatrix};$$

poi, eseguendo la trasformazione:

$$\begin{pmatrix} E_4 & E_3 & E_2 & E_1 \\ E_4^{\beta} & E_3 & E_2^{\beta} & E_1^{\beta} \end{pmatrix},$$

mi riduco al caso di $\beta = 1$. Ciò posto, cambiando l'elemento E_4 in $E_4 E_3^{-\alpha}$. si vede facilmente che si può sempre ritenere $\alpha = 0$.

Esistono perciò due soli gruppi G_4^4 che hanno il divisore invertibile ciclico e questi due gruppi sono definiti dalla (9) e dalle seguenti modificazioni delle (10):

$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = E_1$,	$E_1^p = 1$
$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = E_1$,	$E_1^p = 1$

Il primo di questi gruppi è un $G_4^{4,3}$ e fra tutti i suoi divisori d'indice p ve ne sono p^2 non Abeliani; il secondo gruppo è un $G_4^{4,2}$ e tutti i suoi $p+1$ divisori d'indice p sono Abeliani.

12. Si supponga ora che il gruppo $H = G_2$ non sia ciclico. Allora le ultime quattro delle relazioni (8) si scrivono:

$$E_4^p = E_2^{\alpha} E_1^{\beta}, \quad E_3^p = E_2^{\gamma} E_1^{\delta}, \quad E_2^p = 1, \quad E_1^p = 1. \tag{11}$$

Per dimostrare che le formole (9) e (11) definiscono, in ogni caso, un gruppo G_4^4, basta ripetere il ragionamento del n.° precedente, convenendo però, per andare d'accordo con le (11), di ritenere eguale al simbolo:

$$e_4^{x} e_3^{y} e_2^{z} e_1^{t},$$

ogni altro che da quello si ottiene facendo variare gli esponenti ordinatamente di $p k_4$, $p k_3$, h_2, h_1 in modo che siano soddisfatte le congruenze:

$$\left.\begin{aligned} \alpha k_4 + \gamma k_3 + h_2 &\equiv 0 \\ \beta k_4 + \delta k_3 + h_1 &\equiv 0 \end{aligned}\right\} \pmod{p}.$$

Se il gruppo G_4^4 è un $G_4^{4,2}$, almeno uno degl'interi α, γ deve essere primo con p ed io suppongo che sia γ primo con p. Allora si può definire l'ele-

mento E_2 mediante la relazione $E_3^p = E_2$; poi, chiamando E_4 l'elemento $E_4 E_3^{-\alpha}$ mi riduco al caso di $\alpha = 0$. Ciò posto, se non è β un multiplo di p, la trasformazione:

$$\begin{pmatrix} E_4 & E_3 & E_2 & E_1 \\ E_4 & E_3^\beta & E_2^\beta & E_1^\beta \end{pmatrix},$$

porta β in 1.

Esistono perciò due gruppi $G_4^{1,2}$ tali che il divisore invertibile abbia tutti i suoi elementi di grado p e questi due gruppi corrispondono alle seguenti modificazioni delle formole (11):

$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$
$E_4^p = E_1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$

Se il gruppo G_4^1 è un gruppo $G_4^{1,3}$, nelle (11) bisogna supporre $\alpha = \gamma = 0$, ed allora è necessario distinguere il caso di $p > 2$ dal caso di $p = 2$.

Nel primo caso, se è $\beta = \delta = 0$, il gruppo $G_4^{1,3}$ ha tutti i suoi elementi di grado p, e ciò risulta dalla formola:

$$(E_4 E_3)^n = E_4^n E_3^n E_1^{\binom{n}{2}}; \tag{12}$$

se invece uno dei due numeri β, δ è primo con p, io posso supporre che sia δ primo con p. Allora, facendo la trasformazione:

$$\begin{pmatrix} E_4 & E_3 & E_2 & E_1 \\ E_4^\delta & E_3 & E_2 & E_1^\delta \end{pmatrix},$$

mi riduco al caso di $\delta = 1$; poi, chiamando E_4 l'elemento $E_4 E_3^{-\beta}$ porto β in 0.

Esistono quindi, nel presente caso, due soli gruppi $G_4^{1,3}$ i quali sono definiti dalle formole:

$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_4^p = 1$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$

e dalla formola (9).

Nell'ipotesi di $p = 2$, tenendo presente la (12), si vede subito che il caso $E_4^2 = E_1$, $E_3^2 = E_1$ è irreduttibile, mentre qualunque altro caso si riduce a quello in cui è $E_4^2 = 1$, $E_3^2 = 1$.

Dunque, anche quando è $p = 2$, esistono due soli gruppi $G_4^{1,3}$ tali che il divisore invertibile non è ciclico e questi due gruppi corrispondono alle seguenti modificazioni delle formole (11):

$E_4^2 = 1$,	$E_3^2 = 1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_4^2 = E_1$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$

13. Ritornando alla distinzione fatta al principio del n.° 11, io mi voglio ora occupare dei gruppi G_4 che sono G_4^2 e comincio col dimostrare che un tale gruppo possiede sempre un divisore Abeliano d'indice p ed uno solo (*).

Sia:

$$G_4^2, \quad G_3, \quad G_2, \quad G_1,$$

una serie canonica di composizione di un gruppo G_4^2 e si considerino le classi distinte di elementi:

$$G_2, \quad E' G_2, \quad E'' G_2, \ldots$$

contenute in G_4^2. Ognuno degli elementi $E', E'', \ldots$ deve trasformare un elemento E_2 di G_2 nel prodotto di E_2 per una potenza di E_1; ora, giacchè gli elementi $E', E'', \ldots$ sono in numero di $p^2 - 1$, necessariamente esistono due tali elementi, per es. E', E'', che trasformano E_2 nel prodotto di E_2 per una stessa potenza di E_1; quindi l'elemento $E'^{-1} E''$, che non sta in G_2, è invertibile con E_2. Se chiamo E_3 il detto elemento, i tre elementi E_1, E_2, E_3, permutabili due a due, generano un gruppo Abeliano il cui grado non è minore, e non può essere maggiore di p^3.

Se il gruppo G_4^2 avesse due divisori Abeliani di grado p^3, la loro intersezione, che è di grado p^2, dovrebbe essere contenuta nel gruppo H il quale è attualmente di grado p: dunque la mia tesi è dimostrata.

Ciò posto, io dico che ogni gruppo G_4^2 è un gruppo $G_4^{2,2}$. Infatti, se fosse possibile un gruppo $G_4^{2,3}$, per un tal gruppo sarebbe $K = H = G_4$ e quindi sarebbe:

$$E_4^{-1} E_3 E_4 = E_3 E_1^{\alpha}, \quad E_4^{-1} E_2 E_4 = E_2 E_1^{\beta},$$

(*) Questo risultato è stato comunicato per lettera dal sig. HÖLDER al sig. MILLER. Cfr. MILLER. *Sur les groupes de substitutions.* Comptes Rendus, t. 122, a. 1896, pag. 371.

con β primo con p. Allora, scegliendo l'intero m in modo che sia $\beta m + \alpha \equiv 0 \pmod p$, l'elemento $E_3 E_2^m$ risulta permutabile con E_4 e quindi G_3 non sarebbe il solo divisore Abeliano d'indice p contenuto in $G_4^{2,3}$.

Le considerazioni che precedono mostrano che è possibile determinare una base canonica:

$$E_4, \quad E_3, \quad E_2, \quad E_1,$$

di un gruppo G_4^2 in modo tale che sia:

$$E_4^{-1} E_3 E_4 = E_3 E_2, \quad E_4^{-1} E_2 E_4 = E_2 E_1, \quad E_3^{-1} E_2 E_3 = E_2. \tag{13}$$

Dopo ciò si osservi che l'elemento E_4^p sta certamente in $K = G_2$; ma, giacchè il detto elemento è invertibile con E_4, esso sta in $G_1 = H$.

Inoltre *se è* $p > 2$, dalle (13) si ricava:

$$E_4^{-p} E_3 E_4^p = E_3 E_2^p,$$

e siccome E_4^p sta in H, deve essere $E_2^p = 1$; quindi l'elemento E_3^p, che risulta allora invertibile con E_4, sta in H. Si ha dunque:

$$E_4^p = E_1^\alpha, \quad E_3^p = E_1^\beta, \quad E_2^p = 1, \quad E_1^p = 1. \tag{14}$$

Le formole (13) e (14) definiscono sempre un gruppo $G_4^{2,2}$ tutte le volte che è $p > 2$.

Infatti, considero i simboli già precedentemente definiti:

$$e_4^x e_3^y e_2^z e_1^t,$$

e, come mi consigliano le (14), chiamo eguali due tali simboli quando si possono dedurre l'uno dall'altro facendo variare ordinatamente gli esponenti di $p k_4$, $p k_3$, $p k_2$, h_1, purchè sia:

$$\alpha k_4 + \beta k_3 + h_1 \equiv 0 \pmod p;$$

inoltre, per andare poi d'accordo con le (13), pongo per definizione:

$$(e_4^{x'} e_3^{y'} e_2^{z'} e^{t'}) \; (e_4^{x''} e_3^{y''} e_2^{z''} e_1^{t''}) = e_4^{x'''} e_3^{y'''} e_2^{z'''} e_1^{t'''},$$

essendo:

$$x''' = x' + x'', \quad y''' = y' + y'', \quad z''' = z' + z'' + y' x'',$$

$$t''' = t' + t'' + z' x'' + y' \binom{x''}{2}.$$

Poste queste definizioni e chiamando A, B, C tre qualunque elementi come $e_4^x e_3^y e_2^z e_1^t$, quando si vuole stabilire che tutte le volte che è $A = B$ è an-

che $A\,C = B\,C$, bisogna tenere conto della condizione $p > 2$; e supponendola verificata, le dette definizioni dànno origine ad un gruppo che è rappresentato in Γ con un $G_4^{2,2}$, e facendo corrispondere ai simboli:

$$e_4^{1}\,e_3^{0}\,e_2^{0}\,e_1^{0},\quad e_4^{0}\,e_3^{1}\,e_2^{0}\,e_1^{0},\quad e_4^{0}\,e_3^{0}\,e_2^{1}\,e_1^{0},\quad e_4^{0}\,e_3^{0}\,e_2^{0}\,e_1^{1},$$

ordinatamente gli elementi E_4, E_3, E_2, E_1, questi elementi verificano le relazioni (13) e (14).

14. Ponendo a fondamento le dette relazioni, la serie canonica:

$$G_4^{2,2},\quad G_3,\quad G_2,\quad G_1,$$

è perfettamente determinata nel senso che, se:

$$\mathbf{E}_4,\quad \mathbf{E}_3,\quad \mathbf{E}_2,\quad \mathbf{E}_1,$$

è un'altra base canonica di $G_4^{2,2}$, tale che l'operazione:

$$T = \begin{pmatrix} E_4, & E_3, & E_2, & E_1 \\ \mathbf{E}_4, & \mathbf{E}_3, & \mathbf{E}_2, & \mathbf{E}_1 \end{pmatrix}$$

non alteri la forma delle (13) e (14), la detta base definisce la stessa serie canonica.

Ponendo dunque, nella più generale maniera:

$$\mathbf{E}_4 \equiv E_4^{u}\,E_3^{v},\quad \mathbf{E}_3 \equiv E_3^{s},\quad (\mathrm{mod}\ G_2), \tag{15}$$

affinchè si conservino le formole (13) si deve scegliere $\mathbf{E}_2 \equiv E_2^{us}$ (mod G_1) ed $\mathbf{E}_1 = E_1^{u^2 s}$; allora, per non contraddire alla definizione di $\mathbf{E}_1$, bisogna supporre u ed s primi con p.

Se dopo avere definita in tal modo la nuova base $\mathbf{E}_4$, $\mathbf{E}_3$, $\mathbf{E}_2$, $\mathbf{E}_1$, si fa l'operazione che porta la detta base in E_4, E_3, E_2, E_1 e si chiamano α_1 e β_1 i valori trasformati di α e β, si trova facilmente:

$$u^2\,s\,\alpha_1 \equiv \alpha\,u + \beta\,v,\quad u^2\,\beta_1 \equiv \beta,\quad (\mathrm{mod}\ p),$$

purchè si supponga $p > 3$ e si osservi che, in virtù delle (13), si ha:

$$(E_4\,E_3)^n = E_4^{n}\,E_3^{n}\,E_2^{\binom{n}{2}}\,E_1^{\binom{n}{3}}.$$

Sia, in prima ipotesi, $\beta = 0$: allora, se non è $\alpha = 0$, scegliendo $u = 1$, $s = \alpha$, ottengo $\alpha_1 \equiv 1$ (mod p).

Sia, in seconda ipotesi, β primo con p: allora, posso scegliere v in modo che sia $\alpha_1 \equiv 0$ (mod p); inoltre, se β è un residuo quadratico di p, posso de-

terminare u in modo che sia $\beta_1 \equiv 1 \pmod p$; e se β non è residuo quadratico di p, essendo ε una qualunque radice primitiva di p, posso determinare u in modo che sia $\beta_1 \equiv \varepsilon \pmod p$.

Esistono dunque, se è $p > 3$, quattro gruppi $G_4^{\varepsilon,\varepsilon}$, i quali sono definiti dalle (13) e dalle seguenti modificazioni delle formule (14):

$$\begin{array}{|cccc|}
\hline
E_4^p = 1, & E_3^p = 1, & E_2^p = 1, & E_1^p = 1 \\
\hline
E_4^p = E_1, & E_3^p = 1, & E_2^p = 1, & E_1^p = 1 \\
\hline
E_4^p = 1, & E_3^p = E_1, & E_2^p = 1, & E_1^p = 1 \\
\hline
E_4^p = 1, & E_3^p = E_1^\varepsilon, & E_2^p = 1, & E_1^p = 1 \\
\hline
\end{array} \qquad (16)$$

Il divisore Abeliano G_3 dei primi due gruppi è un $G_3^{0,3}$ e quello degli ultimi due è un $G_3^{0,2}$.

15. Si supponga ora $p = 3$.

Giacchè due qualunque operazioni T appartenenti alla classe definita dalle congruenze (15) per dati valori di u, v, s, producono lo stesso effetto sopra i numeri α e β che figurano nelle formule (14), io ritengo eguali tutte le operazioni appartenenti alla detta classe e quest'unica operazione la rappresento col simbolo:

$$\begin{vmatrix} u & v \\ 0 & s \end{vmatrix}.$$

Tutte le possibili operazioni così definite costituiscono, nel presente caso, un gruppo di grado 12; ma, giacchè l'operazione:

$$\begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix},$$

non cambia α e β, io la posso ritenere eguale all'elemento identico del detto gruppo e quindi il grado di questo si riduce a 6. Il gruppo di grado 6, che qui si presenta, è isomorfo a quello di cui ho discorso nel n.° 9 e si può generare mediante le due operazioni:

$$\begin{vmatrix} 1 & 0 \\ 0 & 2 \end{vmatrix}, \qquad \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix},$$

che sono rispettivamente di secondo e terzo ordine.

La prima di queste operazioni cambia α in 2α e la seconda cambia α in $\alpha+\beta+1$; ma, nè l'una nè l'altra alterano β. Dunque, se β è 0 od 1, posso sempre supporre $\alpha=0$, e se è $\beta=2$, posso ridurre il caso di $\alpha=2$ al caso di $\alpha=1$.

Esistono quindi, anche quando è $p=3$, quattro gruppi $G_4^{2,2}$ i quali corrispondono alle seguenti modificazioni delle formole (14):

$$\begin{array}{|cccc|}\hline E_4^3=1, & E_3^3=1, & E_2^3=1, & E_1^3=1 \\ \hline E_4^3=1, & E_3^3=E_1, & E_2^3=1, & E_1^3=1 \\ \hline E_4^3=1, & E_3^3=E_1^2, & E_2^3=1, & E_1^3=1 \\ \hline E_4^3=E_1, & E_3^3=E_1^2, & E_2^3=1, & E_1^3=1 \\ \hline\end{array} \tag{17}$$

Soltanto per il primo di questi gruppi il divisore Abeliano G_3 è un $G_3^{0,3}$; per gli altri tre gruppi il detto divisore è un $G_3^{0,2}$.

16. Io considero finalmente il caso, finora escluso, di $p=2$, per il quale non sussistono le formole (14).

Le relazioni (13) dànno:

$$E_4^{-2}\,E_3\,E_4^2=E_3\,E_2^2\,E_1,$$

e siccome E_4^2 sta in H, deve essere $E_2^2=E_1$; allora, l'elemento E_3^2 che, a causa della prima delle dette relazioni, non risulta permutabile con E_4, è una potenza impari di E_2.

Le (14) debbono dunque essere sostituite con le formole:

$$E_4^2=E_1^\alpha,\quad E_3^2=E_2^\beta,\quad E_2^2=E_1,\quad E_1^2=1;$$

ed è facile vedere che, tutte le volte che β è impari, queste formole e le (13) definiscono un gruppo di grado $2^4=16$ che è un $G_4^{2,2}$.

Cambiando ora la base canonica e ponendo, nella maniera più generale,

$$\mathrm{E}_4=E_4\,E_3^\nu,\quad \mathrm{E}_3=E_3^\sigma,$$

la corrispondente operazione T non altera β ma cambia α in un numero α_1 tale che:

$$s\,\alpha_1\equiv\alpha+\frac{\beta+1}{2}\,\nu,\qquad (\mathrm{mod}\ 2).$$

Dunque, se è $\beta = 1$, si può sempre ritenere $\alpha = 0$, ma, se è $\beta = 3$, bisogna distinguere il caso di $\alpha = 0$ dal caso di $\alpha = 1$.

Esistono perciò tre gruppi di grado 16 che sono $G_4^{2,2}$, i quali sono definiti dalle formole:

$E_4^2 = 1,$	$E_3^2 = E_2,$	$E_2^2 = E_1,$	$E_1^2 = 1$
$E_4^2 = 1,$	$E_3^2 = E_2 E_1,$	$E_2^2 = E_1,$	$E_1^2 = 1$
$E_4^2 = E_1,$	$E_3^2 = E_2 E_1,$	$E_2^2 = E_1,$	$E_1^2 = 1$

insieme alle formole (13).

Per questi tre gruppi il divisore Abeliano G_3 è ciclico.

17 Io riepilogo brevemente i risultati ottenuti nel presente paragrafo.

Esistono soltanto *cinque* gruppi di grado p^3, dei quali: tre sono gruppi G_3^0 e gli altri due sono gruppi $G_3^{1,2}$.

Esistono soltanto *quattordici* gruppi di grado $2^4 = 16$, dei quali: cinque sono gruppi G_4^0, tre sono gruppi $G_4^{1,2}$, tre sono gruppi $G_4^{1,3}$ ed i rimanenti tre sono gruppi $G_4^{2,2}$.

Per tutti i valori del numero primo $p > 2$ esistono soltanto *quindici* gruppi di grado p^4, dei quali: cinque sono gruppi G_4^0, tre sono gruppi $G_4^{1,2}$, tre sono gruppi $G_4^{1,3}$ ed i rimanenti quattro sono gruppi $G_4^{2,2}$.

Le formole di composizione di tutti questi gruppi sono rappresentate nella seguente tabella:

Gruppi di grado p^3.

I. Gruppi G_3^0 | $[p^3]$, $[p^2]$ $[p]$, $[p]$ $[p]$ $[p]$ |.

II. Gruppi $G_3^{1,2}$ | $E_3^{-1} E_2 E_3 = E_2 E_1$, $H(E_1)$ |.

E_3^p	E_2^p	E_1^p	
1	1	1	$p \geq 2$
1	E_1	1	$p > 2$
E_1	E_1	1	$p = 2$

Gruppi di grado p^4.

I. Gruppi G_4^0 $\{[p^4], [p^3][p], [p^2][p^2], [p^2][p][p], [p][p][p][p]\}$.

II. Gruppi G_4^1 $\{E_4^{-1} E_3 E_4 = E_3 E_1,\ H(E_2, E_1)\}$.

	$p \geqq 2$	$p \geqq 2$	$p > 2$	$p \geqq 2$	$p \geqq 2$	$p > 2$	$p = 2$
E_4^p	1	1	E_1	1	1	1	E_1
E_3^p	E_2	E_2	E_2	1	1	E_1	E_1
E_2^p	E_1	1	1	E_1	1	1	1
E_1^p	1	1	1	1	1	1	1
	Gruppi $G_4^{1,2}$			Gruppi $G_4^{1,3}$			

III. Gruppi $G_4^2 = G_4^{2,2}$, $\{H(E_1)\}$.

$E_4^{-1} E_3 E_4 = E_3 E_2$, $E_4^{-1} E_2 E_4 = E_2 E_1$, $E_3^{-1} E_2 E_3 = E_2$

	$p \geqq 3$	$p > 3$	$p \geqq 3$	$p \geqq 3$	$p = 3$	$p = 2$	$p = 2$	$p = 2$
E_4^p	1	E_1	1	1	E_1	1	1	E_1
E_3^p	1	1	E_1	E_1^c	E_1^2	E_2	E_2^{-1}	E_2^{-1}
E_2^p	1	1	1	1	1	E_1	E_1	E_1
E_1^p	1	1	1	1	1	1	1	1

§ III. I Gruppi G_5^0 e G_5^1.

18. Esistono sette gruppi Abeliani di grado p^5, i quali sono: un gruppo $G_5^{0,1}$, due gruppi $G_5^{0,2}$, due gruppi $G_5^{0,3}$, un gruppo $G_5^{0,4}$ ed un gruppo $G_5^{0,5}$.

Mettendo in evidenza per ciascuno di questi sette gruppi gl'invarianti del sig. FROBENIUS, li rappresenterò nel seguente modo:

$$G_5^{0,1} \mid [p^5] \mid, \quad G_5^{0,4} \mid [p^2]\,[p]\,[p]\,[p] \mid, \quad G_5^{0,5} \mid [p]\,[p]\,[p]\,[p]\,[p] \mid,$$

$$G_5^{0,2} \mid [p^4]\,[p] \mid, \quad G_5^{0,2} \mid [p^3]\,[p^2] \mid, \quad G_5^{0,3} \mid [p^3]\,[p]\,[p] \mid, \quad G_5^{0,3} \mid [p^2]\,[p^2]\,[p] \mid.$$

Il gruppo $G_5^{0,1}$ è il gruppo ciclico di grado p^5; il gruppo $G_5^{0,4}$ possiede $\frac{p^4-1}{p-1} - 1$ divisori $G_4^{0,3}$ ed un solo divisore $G_4^{0,4}$, mentre tutti i divisori d'indice p del gruppo $G_5^{0,5}$ sono gruppi $G_4^{0,4}$. Il primo dei due gruppi $G_5^{0,2}$ ha un solo divisore $G_4^{0,2} \mid [p^3]\,[p] \mid$ e p divisori $G_4^{0,1}$, mentre il secondo dei detti due gruppi ha p divisori $G_4^{0,2} \mid [p^3]\,[p] \mid$ ed un solo divisore $G_4^{0,2} \mid [p^2]\,[p^2] \mid$.

Finalmente, il primo dei due gruppi $G_5^{0,3}$ ha un solo divisore $G_4^{0,3}$ e $p(p+1)$ divisori $G_4^{0,2} \mid [p^3]\,[p] \mid$, mentre tutti i divisori d'indice p del secondo dei detti due gruppi sono: $p+1$ gruppi $G_4^{0,3}$ e p^2 gruppi $G_4^{0,2} \mid [p^2]\,[p^2] \mid$.

Io mi limito a dimostrare soltanto quello che ho asserito relativamente al gruppo $[p^2]\,[p^2]\,[p]$.

Scegliendo in modo conveniente tre elementi E'', E', E dei gradi p^2, p^2, p rispettivamente, un arbitrario elemento di un tale gruppo si può rappresentare con:

$$E''^{\alpha} E'^{\beta} E^{\gamma},$$

dove α, β, γ sono tre interi presi ordinatamente rispetto ai moduli p^2, p^2, p.

I tre gruppi di grado p^4, costituiti rispettivamente dagli elementi dei seguenti tre tipi:

$$E''^{p\alpha} E'^{\beta} E^{\gamma}, \quad E''^{\alpha} E'^{p\beta} E^{\gamma}, \quad E''^{\alpha} E'^{\beta},$$

sono indipendenti, perchè s'intersecano secondo il gruppo K di grado p^2 costituito dagli elementi del tipo:

$$E''^{p\alpha} E'^{p\beta}.$$

Inoltre, un elemento qualunque del detto gruppo di grado p^2 è la p^{ma} potenza di un elemento del gruppo principale e quindi questo non può avere più di tre divisori indipendenti d'indice p: dunque il gruppo principale $[p^2]\,[p^2]\,[p]$ è un $G_5^{0,3}$.

Tutti gli elementi di grado p di questo gruppo formano il gruppo $G_3^{0,3}$ costituito dagli elementi del tipo:

$$E''^{p\gamma} E'^{p\beta} E^{\gamma}.$$

Dei divisori d'indice p del gruppo principale, quelli che contengono $G_3^{0,3}$ sono necessariamente gruppi $G_4^{0,3}$ e, pensando al gruppo complementare di $G_3^{0,3}$ nel detto gruppo principale, si vede subito che il loro numero è $p+1$.

Inoltre, ogni divisore $G_4^{0,3}$ del gruppo principale contiene evidentemente $G_3^{0,3}$: dunque il detto gruppo possiede $p+1$, e non più, divisori $G_4^{0,3}$.

Ciò posto, i rimanenti p^2 divisori d'indice p sono necessariamente gruppi $G_4^{0,2}\{[p^2][p^2]\}$.

19. I gruppi G_5^4 possono essere o gruppi $G_5^{4,2}$ o gruppi $G_5^{4,3}$, oppure gruppi $G_5^{4,4}$, ed io mostrerò che effettivamente esistono gruppi in ognuna di queste classi.

Sia:

$$G_5^4, \quad G_4, \quad G_3, \quad G_2, \quad G_1,$$

una serie canonica di un gruppo G_5^4 scelta in modo tale che sia $G_3 = H$, ed:

$$E_5, \quad E_4, \quad E_3, \quad E_2, \quad E_1,$$

una base canonica relativa alla detta serie.

Giacchè la potenza E_4^p sta in H, l'elemento E'_3, che figura nella relazione $E_5^{-1} E_4 E_5 = E_4 E'_3$, è di grado p ed io lo posso assumere come elemento E_4; quindi si ha:

$$E_5^{-1} E_4 E_5 = E_4 E_4. \tag{1}$$

Se il gruppo H è ciclico, scegliendo opportunamente l'elemento E_3, posso scrivere:

$$E_5^p = E_3^\alpha, \quad E_4^p = E_3^\beta, \quad E_3^p = E_2, \quad E_2^p = E_1, \quad E_1^p = 1; \tag{2}$$

e si può facilmente dimostrare che, qualunque siano gl'interi α e β, le formole (1) e (2) definiscono un gruppo G_5^4.

Ciò posto, si osservi che l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5 E_3^h, & E_4 E_3^k, & E_3, & E_2, & E_1 \end{pmatrix},$$

cambia α e β rispettivamente in $\alpha + hp$ e $\beta + kp$; dunque, se α e β sono multipli di p, si può supporre $\alpha = \beta = 0$.

Se uno dei due numeri α, β è primo con p, io suppongo che sia β primo con p giacchè, in caso contrario, scambio α in β mediante l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_4^{-1}, & E_5^{-1}, & E_3^{-1}, & E_2^{-1}, & E_1^{-1} \end{pmatrix};$$

poi, eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^{\beta}, & E_4, & E_3^{\beta}, & E_2^{\beta}, & E_1^{\beta} \end{pmatrix},$$

mi riduco al caso di $\beta = 1$. Dopo ciò, chiamando E_5 l'elemento $E_5 E_4^{-\alpha}$, si vede facilmente che è sempre lecito ritenere $\alpha = 0$

Esistono quindi due soli gruppi G_5^4, che hanno il divisore invertibile ciclico, i quali sono definiti dalla (1) e dalle formole:

$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = E_1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_3$,	$E_3^p = E_2$,	$E_2^p = E_1$,	$E_1^p = 1$

Il primo di questi gruppi è un $G_5^{4,3}$ e fra tutti i suoi divisori d'indice p, i quali s'intersecano in G_2, ve ne sono p^2 non Abeliani; il secondo gruppo è un $G_5^{4,2}$ e tutti i suoi $p+1$ divisori d'indice p sono Abeliani.

20. Si supponga ora che il gruppo $H = G_3$ sia un $G_3^{0,2}$.

In questo caso, scegliendo come gruppo G_2 l'unico divisore non ciclico di grado p^2 che possiede H, due ipotesi sono possibili rispetto all'elemento E_3^p, che è necessariamente di grado p: o questo elemento sta in G_1 oppure è fuori di G_1. Nella prima ipotesi posso supporre $E_3^p = E_1$, e nella seconda ipotesi pongo $E_3^p = E_2$: si hanno in corrispondenza ai due casi le due serie di formole:

$$E_5^p = E_3^{\alpha} E_2^{\beta}, \quad E_4^p = E_3^{\gamma} E_2^{\delta}, \quad E_3^p = E_1, \quad E_2^p = 1, \quad E_1^p = 1 \qquad (3)$$

$$E_5^p = E_3^{\alpha} E_1^{\beta}, \quad E_4^p = E_3^{\gamma} E_1^{\delta}, \quad E_3^p = E_2, \quad E_2^p = 1, \quad E_1^p = 1. \qquad (4)$$

Io dimostro ora che le (3) e la (1) definiscono sempre un gruppo G_5^4 qualunque siano gl'interi α, β, γ, δ, e in un modo perfettamente analogo si può dimostrare che anche le (4) e la (1) definiscono, in ogni caso, un gruppo G_5^4.

Si considerino i simboli che si ottengono da:

$$e_5^x e_4^y e_3^z e_2^t e_1^w,$$

attribuendo ad x, y, z, t, w arbitrari valori interi, e si chiamino eguali due tali simboli quando si ottengono l'uno dall'altro facendo variare i detti interi

ordinatamente di $p\,k_5$, $p\,k_4$, h_3, h_2, h_1, purchè sia:

$$\alpha\,k_5 + \gamma\,k_4 + h_3 + p\,h_1 \equiv 0, \pmod{p^5}$$

$$\beta\,k_5 + \delta\,k_4 + h_2 \equiv 0, \pmod{p}.$$

Dietro questa convenzione si ottengono soltanto p^5 simboli distinti.

Ora, ponendo per definizione:

$$(e_5^{x'} e_4^{y'} e_3^{z'} e_2^{t'} e_1^{w'})\,(e_5^{x''} e_4^{y''} e_3^{z''} e_2^{t''} e_1^{w''}) = e_5^{x'+x''} e_4^{y'+y''} e_3^{z'+z''} e_2^{u'+u''} e_1^{w'+w''+y'x''},$$

si può subito verificare che, rispetto a questa legge di composizione, i simboli considerati costituiscono un gruppo P_5. Se si rappresenta questo gruppo in Γ facendo corrispondere ai cinque elementi di P_5:

$$e_5^1\,e_4^0\,e_3^0\,e_2^0\,e_1^0, \quad e_5^0\,e_4^1\,e_3^0\,e_2^0\,e_1^0, \ldots, \quad e_5^0\,e_4^0\,e_3^0\,e_2^0\,e_1^1,$$

ordinatamente, i cinque elementi E_5, E_4, E_3, E_2, E_1 di Γ, questi elementi costituiscono una base canonica di un G_5^1 e verificano le relazioni (3) ed (1).

Io non ripeterò in seguito un simile ragionamento, che deve essere oramai familiare al lettore: mi limiterò solamente ad asserire, quando si presenta il caso, che una data serie di relazioni definiscono un gruppo di una data classe.

Riferendomi alle formole (3), se i numeri α e γ sono multipli di p, siccome la trasformazione:

$$\begin{pmatrix} E_5 & E_4 & E_3 & E_2 & E_1 \\ E_5\,E_3^h & E_4\,E_3^k & E_3 & E_2 & E_1 \end{pmatrix},$$

cambia i detti numeri rispettivamente in $\alpha + h\,p$ e $\gamma + k\,p$, posso supporre $\alpha = \gamma = 0$. Ciò posto, se uno dei due numeri β, δ è primo con p, ritengo, senza nuocere alla generalità, δ primo con p e pongo a definizione dell'elemento E_2 la relazione $E_4^p = E_2$; allora, cambiando $E_5\,E_4^{-\beta}$ in E_5, si vede facilmente che si può assumere $\beta = 0$. Ottengo quindi due gruppi G_5^1 definiti dalla (1) e dalle relazioni:

$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$

Il primo di questi gruppi è un $G_5^{1,3}$ ed il relativo gruppo K coincide con G_2, mentre il secondo è un $G_5^{1,4}$ ed il relativo gruppo K coincide con G_1.

Se uno dei due numeri α, γ è primo con p, posso supporre che sia γ primo con p: allora, facendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^\gamma, & E_4, & E_3^\gamma E_2^\delta, & E_2, & E_1^\gamma \end{pmatrix},$$

ottengo $E_4^p = E_3$. Ciò posto, chiamando E_5 l'elemento $E_5 E_4^{-\alpha}$, si vede facilmente che si può assumere $\alpha = 0$; allora, se è β primo con p, pongo a definizione dell'elemento E_2 la relazione $E_5^p = E_2$.

Ottengo quindi due nuovi gruppi G_5^4 definiti dalle (1) e dalle formole:

$E_5^p = E_2$,	$E_4^p = E_3$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_3$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$

Il primo di questi gruppi è un $G_5^{1,2}$ ed il relativo gruppo K coincide con H, mentre il secondo è un $G_5^{1,3}$ ed il relativo gruppo K coincide col gruppo ciclico generato dall'elemento E_3.

21. Riferendomi alle formole (4), siano, in prima ipotesi, α e γ multipli di p: in tale caso posso supporre come prima $\alpha = \gamma = 0$. Ciò posto, se uno dei due numeri β, δ è primo con p, io suppongo δ primo con p; poi, facendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^\delta, & E_4, & E_3, & E_2, & E_1^\delta \end{pmatrix},$$

mi riduco al caso di $\delta = 1$. Allora, *supponendo* $p > 2$ e chiamando E_5 l'elemento $E_5 E_4^{-\beta}$, posso supporre $\beta = 0$.

Ottengo perciò due gruppi i quali, nell'attuale ipotesi di $p > 2$, sono distinti, e questi gruppi sono definiti dalla (1) e dalle seguenti modificazioni delle formole (4):

$E_5^p = 1$,	$E_4^p = E_1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$

Entrambi questi gruppi appartengono alla classe dei gruppi $G_5^{1,3}$ ed i relativi gruppi K coincidono con G_2.

Se invece è $p=2$, si vede subito, pensando alla (1), che il caso di $E_5=E_1$, $E_4=E_1$ non è riducibile ad alcun altro caso, mentre poi tutti questi altri casi sono riducibili al caso di $E_5=1$, $E_4=1$.

Dunque ottengo due gruppi G_5^1 di grado $2^5=32$, i quali sono definiti dalle formole:

$E_5^2=E_1$,	$E_4^2=E_1$,	$E_3^2=E_2$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=1$,	$E_3^2=E_2$,	$E_2^2=1$,	$E_1^2=1$

insieme alla formula (1).

Entrambi questi gruppi sono gruppi $G_5^{1,3}$ e, in ognuno di essi, il divisore K coincide con G_2.

Sia, in seconda ipotesi, uno dei due numeri α, γ primo con p e precisamente si supponga γ primo con p. Allora, facendo la trasformazione:

$$\begin{pmatrix} E_5 & E_4 & E_3 & E_2 & E_1 \\ E_5 & E_4 & E_3^{\gamma} E_2^{\delta} & E_2^{\gamma} & E_1 \end{pmatrix},$$

ottengo $E_4^p=E_3$. Ciò posto, chiamando E_5 l'elemento $E_5 E_4^{-\alpha}$, posso ritenere $\alpha=0$; poi, se non è β multiplo di p, facendo la trasformazione:

$$\begin{pmatrix} E_5 & E_4 & E_3 & E_2 & E_1 \\ E_5 & E_4^{\beta} & E_3^{\beta} & E_2^{\beta} & E_1^{\beta} \end{pmatrix},$$

mi riduco al caso di $\beta=1$.

Ottengo perciò due gruppi G_5^1, che sono definiti dalla (1) e dalle formole:

$E_5^p=E_1$,	$E_4^p=E_3$,	$E_3^p=E_2$,	$E_2^p=1$,	$E_1^p=1$
$E_5^p=1$,	$E_4^p=E_3$,	$E_3^p=E_2$,	$E_2^p=1$,	$E_1^p=1$

Ognuno di questi due gruppi è un gruppo $G_5^{1,2}$ che ha il relativo divisore K coincidente con H.

22. Io abbandono ora l'ipotesi fatta al principio del n.° 20 e suppongo invece che il gruppo $H = G_3$ sia un $G_3^{0,3}$.

In questo caso si può porre nella più generale maniera:

$$E_5^p = E_3^\alpha E_2^\beta E_1^\lambda, \quad E_4^p = E_3^\gamma E_2^\delta E_1^\mu, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1, \quad (5)$$

e queste formole, insieme alla (1), definiscono sempre un gruppo G_5^1 qualunque siano gl'interi α, β, λ, γ, δ, μ.

Siano, in prima ipotesi, i quattro numeri α, β, γ, δ multipli di p. Allora, se uno dei due numeri λ, μ è primo con p, io suppongo μ primo con p; poi, mediante la traformazione:

$$\begin{pmatrix} E_5 & E_4 & E_3 & E_2 & E_1 \\ E_5^\mu & E_4 & E_3 & E_2 & E_1^\mu \end{pmatrix},$$

mi riduco al caso di $\mu = 1$. Ciò posto, se è $p > 2$, chiamando E_5 l'elemento $E_5 E_4^{-\lambda}$, si vede che è lecito ritenere $\lambda = 0$.

Si hanno quindi due gruppi G_5^1 in corrispondenza alle formole:

$E_5^p = 1$,	$E_4^p = E_1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Questi due gruppi appartengono alla classe dei gruppi $G_5^{1,4}$ e, per ognuno di essi, il gruppo K coincide con G_1.

Se è $p = 2$, si vede facilmente che il caso di $E_5^2 = E_1$, $E_4^2 = E_1$ si trasforma sempre in sè stesso mediante le operazioni T, che lasciano inalterata la (1) e la forma delle (5), mentre qualunque altro caso è riducibile a quello in cui è $E_5^2 = 1$, $E_4^2 = 1$.

Perciò si hanno due gruppi G_5^1 di grado 32 in corrispondenza alle due serie di formole:

$E_5^2 = E_1$,	$E_4^2 = E_1$,	$E_3^2 = 1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = 1$,	$E_3^2 = 1$,	$E_2^2 = 1$,	$E_1^2 = 1$

e questi due gruppi appartengono alla classe dei gruppi $G_5^{1,4}$.

Sia, in seconda ipotesi, uno dei numeri α, β, γ, δ primo con p. In tal caso, senza nuocere alla generalità, si può ritenere che uno dei due numeri γ, δ sia primo con p e quindi è lecito porre a definizione dell'elemento E_2 la relazione $E_4^p = E_2$; allora chiamando E_5 l'elemento $E_5 E_4^{-\beta}$, si vede che si può assumere $\beta = 0$. Ciò posto, se α è primo con p, pongo a definizione dell'elemento E_3 la relazione $E_5^p = E_3$; in caso contrario, bisogna distinguere l'ipotesi di λ primo con p da quella in cui è λ un multiplo di p; e, nella prima ipotesi, facendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5, & E_4^{\lambda}, & E_3, & E_2^{\lambda}, & E_1^{\lambda} \end{pmatrix},$$

mi riduco al caso di $\lambda = 1$.

Si hanno quindi tre gruppi G_5^{ι} che sono definiti dalla (1) e dalle seguenti modificazioni delle formole (5):

$E_5^p = E_3$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Il primo di questi gruppi è un $G_5^{1,2}$, mentre gli ultimi due appartengono alla classe dei gruppi $G_5^{1,3}$.

23. Riepilogando: qualunque sia il numero primo p, io ho trovato nel presente paragrafo *ventidue* gruppi di grado p^5.

Di questi ventidue gruppi, *sette* sono Abeliani e *quindici* sono gruppi G_5^1.

I quindici gruppi G_5^1 trovati sono tutti i possibili gruppi G_5^1 e sono: *cinque* gruppi $G_5^{1,2}$, *sette* gruppi $G_5^{1,3}$ e *tre* gruppi $G_5^{1,4}$.

I detti ventidue gruppi di grado p^5 sono brevemente rappresentati nella seguente tabella:

I. *Gruppi* G_5^0.

$$[p^5],\quad [p^2]\,[p]\,[p]\,[p],\quad [p]\,[p]\,[p]\,[p]\,[p],$$
$$[p^4]\,[p],\quad [p^3]\,[p^2],\quad [p^3]\,[p]\,[p],\quad [p^2]\,[p^2]\,[p].$$

II. *Gruppi* G_5^1.

$$E_5^{-1}\,E_4\,E_5 = E_4\,E_1\,,\ \{H(E_3,\ E_2,\ E_1)\}.$$

	E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
Gruppi $G_5^{1.2}$	1	E_3	E_2	E_1	1	$p \geqq 2$
	E_2	E_3	E_1	1	1	$p \geqq 2$
	E_1	E_3	E_2	1	1	$p \geqq 2$
	1	E_3	E_2	1	1	$p \geqq 2$
	E_3	E_2	1	1	1	$p \geqq 2$
Gruppi $G_5^{1.3}$	1	1	E_2	E_1	1	$p \geqq 2$
	1	E_2	E_1	1	1	$p \geqq 2$
	1	E_3	E_1	1	1	$p \geqq 2$
	1	E_1	E_2	1	1	$p > 2$
	1	1	E_2	1	1	$p \geqq 2$
	E_1	E_1	E_2	1	1	$p = 2$
	E_1	E_2	1	1	1	$p \geqq 2$
	1	E_2	1	1	1	$p \geqq 2$
Gruppi $G_5^{1.4}$	1	1	E_1	1	1	$p \geqq 2$
	1	E_1	1	1	1	$p > 2$
	1	1	1	1	1	$p \geqq 2$
	E_1	E_1	1	1	1	$p = 2$

La composizione dei Gruppi finiti il cui grado è la quinta potenza di un numero primo.

(Di G. Bagnera, *a Palermo.)*

PARTE SECONDA.

§ IV. I Gruppi G_5^2 che non posseggono alcun divisore Abeliano d'indice p.

24. I gruppi G_5^2 possono essere o gruppi $G_5^{2,2}$ o gruppi $G_5^{2,3}$ giacchè, come ora dimostrerò, non esistono gruppi $G_5^{2,4}$.

Infatti, supposta l'esistenza di un gruppo $G_5^{2,4}$, sia E un elemento di grado p generatore del gruppo K di $G_5^{2,4}$.

Siccome E appartiene certamente ad H, il gruppo complementare $G_5^{2,4} \mid H$, di grado p^3, è Abeliano ed ha tutti i suoi elementi di grado p. Essendo $E'H$, $E''H$, $E'''H$ tre elementi generatori del detto gruppo complementare, si ha:

$$E'^{-1}E''E' = E''E^{\alpha},\quad E'^{-1}E'''E' = E'''E^{\beta},\quad E''^{-1}E'''E'' = E'''E^{\gamma}. \qquad (1)$$

Giacchè il determinante:

$$\begin{vmatrix} 0 & \alpha & \beta \\ -\alpha & 0 & \gamma \\ -\beta & -\gamma & 0 \end{vmatrix}$$

è nullo identicamente, riesce possibile determinare tre numeri interi x, y, z, non tutti multipli di p, tali che sia:

$$\alpha y + \beta z \equiv 0,\quad -\alpha x + \gamma z \equiv 0,\quad -\beta x - \gamma y \equiv 0,\quad (\mathrm{mod}\, p).$$

Allora l'elemento $E'^{x}E''^{y}E'''^{z}$, che è fuori di H, risulta, in virtù delle (1), invertibile con ogni elemento di $G_5^{2,4}$ e ciò è assurdo.

Stabilito ciò, io passo ora a dimostrare che, se è $p > 2$, la potenza p^{ma} di un elemento qualunque di un gruppo G_5^2 appartiene al divisore invertibile H.

Sia, se è possibile, E un elemento di G_5^2 tale che E^p non appartenga ad H. Il gruppo di grado minimo, che contiene l'elemento E ed il divisore H, è Abeliano; quindi, non potendo coincidere con G_5^2, detto gruppo è un divisore G_4, d'indice p, di G_5^2.

Si chiami E' un elemento di G_5^2 fuori di G_4 e si ponga:

$$E'^{-1} E E' = E E'', \quad E'^{-1} E'' E' = E'' E'''. \tag{2}$$

L'elemento E'^p appartiene certamente ad H; altrimenti il gruppo di grado minimo che contiene E' ed H sarebbe un secondo divisore Abeliano di G_5^2; allora, l'intersezione di questi due divisori, che è di grado p^3, dovrebbe essere contenuta nel gruppo H che, in un gruppo G_5^2, è di grado p^2. L'elemento E'' appartiene al gruppo K intersezione di tutti i divisori d'indice p di G_5^2 e si può, in prima ipotesi, ammettere che E'' appartenga ad H. Allora dalla prima delle (2) si ricava:

$$E'^{-p} E E'^p = E E''^p, \quad E'^{-1} E^p E' = E^p E''^p;$$

quindi, giacchè E'^p sta in H, risulta $E''^p = 1$. L'elemento E^p è dunque invertibile con E' e perciò con ogni elemento di G_5^2, il che contraddice alla definizione di E.

Sia, in seconda ipotesi, E'' fuori di H e si pensi alla intersezione dei gruppi K ed H. Se K è di grado p^3, il gruppo G_5^2 è un $G_5^{2,2}$ e quindi (n.° 4) H è contenuto in K; se invece K è di grado p^2, il gruppo G_5^2 è un $G_5^{2,3}$ di cui K è divisore normale, e siccome detto divisore non coincide con H, esso contiene un sotto gruppo proprio di H. In ogni caso, si vede che la detta intersezione è un divisore d'indice p di K; quindi E''^p ed E''' sono elementi di questa intersezione e perciò di H.

Allora le formole (2) dànno:

$$E'^{-p} E E'^p = E E''^p E'''^{\binom{p}{2}}, \quad E'^{-1} E''^p E' = E''^p E'''^p,$$

e quindi deve essere $E'''^p = 1$, $E''^p = 1$, purchè si pensi che è $p > 2$.

Dopo ciò, tenendo presente la prima delle (2), si vede che E^p risulta invertibile con E' e con ogni elemento di G_5^2: dunque l'elemento E è assurdo.

25. Un gruppo G_5^2 o contiene uno, ma soltanto uno, oppure nessuno divisore Abeliano d'indice p, ed io voglio anzitutto mettermi in quest'ultima ipotesi.

Se:

$$G_5^2, \quad G_4^1, \quad G_3, \quad G_2, \quad G_1,$$

è una serie canonica di composizione di un tale gruppo scelta in modo che sia $G_2 = H$, ed

$$E_5, \quad E_4, \quad E_3, \quad E_2, \quad E_1,$$

è una base relativa alla detta serie, si ha:

$$E_5^{-1} E_4 E_5 = E_4 E_3', \quad E_5^{-1} E_3 E_5 = E_3 E_2', \quad E_4^{-1} E_3 E_4 = E_3 E_2''. \tag{3}$$

Giacchè E_3^p sta in H, dalle (3) risulta $E_2'^p = 1$, $E_2''^p = 1$; inoltre gli elementi E_2' ed E_2'' non possono appartenere ad uno stesso gruppo ciclico, perchè, se fosse ad es. $E_2'^\gamma = E_2''$, l'elemento $E_5^{-\gamma} E_4$, che non sta in G_3, risulterebbe permutabile con E_3 e quindi, contrariamente all'attuale ipotesi, il gruppo G_5^2 ammetterebbe un divisore Abeliano d'indice p. Dunque E_2' ed E_2'' sono due elementi di grado p capaci di generare il gruppo G_2.

Riguardo all'elemento E_3', dico che esso è fuori di G_2; giacchè, se fosse $E_3' = E_2'^\alpha E_2''^\beta$, i due elementi $E_5 E_3^\beta$, $E_4 E_3^{-\alpha}$, in virtù delle (3), risulterebbero invertibili e quindi il gruppo G_5^2 ammetterebbe il divisore Abeliano d'indice p generato dai detti due elementi e dagli elementi E_2', E_2''.

Il ragionamento precedente prova che, dati i due elementi E_5, E_4, si possono definire E_3, E_2, E_1 mediante le formole:

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_2, \quad E_4^{-1} E_3 E_4 = E_3 E_1. \tag{4}$$

Escludo subito il caso di $p = 2$, perchè mediante le (4) si può dimostrare che ogni gruppo G_5^2 di grado 32 ha necessariamente un divisore Abeliano d'indice 2.

Infatti, se un tale gruppo G_5^2 non ha un divisore Abeliano d'indice 2, debbono essere verificate le (4) e quindi deve essere:

$$E_5^{-2} E_4 E_5^2 = E_4 E_3^2 E_2;$$

allora, se E_5^2 sta in H, risulta $E_3^2 = E_2$. In questo caso, siccome le (4) dànno anche:

$$E_5^{-1} E_4^2 E_5 = E_4^2 E_3^2 E_1 = E_4^2 E_2 E_1,$$

l'elemento E_4^2 non sta in H e quindi, contrariamente all'ipotesi, il gruppo G_5^2 contiene il divisore Abeliano d'indice 2 generato dagli elementi E_4, E_2, E_1.

Supponendo dunque $p > 2$, dalle (4) facilmente si ricava:

$$E_5^{-p} E_4 E_5^p = E_4 E_3^p;$$

e siccome E_5^p sta (n.° 24) in H, risulta $E_3^p = 1$. Posso dunque scrivere:

$$E_5^p = E_2^\alpha E_1^\beta, \quad E_4^p = E_2^\gamma E_1^\delta, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1; \tag{5}$$

e, tenendo presente che E_2, E_1 appartengono al divisore invertibile H, si dimostra col solito procedimento che, nell'ipotesi di $p > 2$, qualunque siano gl'interi α, β, γ, δ, le formole (5) e (4) definiscono sempre un gruppo G_5^2. È poi evidente che tutti i gruppi G_5^2 così definiti sono gruppi della classe $G_5^{2,2}$.

26. Bisogna ora vedere come variano α, β, γ, δ relativamente al gruppo delle operazioni:

$$T = \begin{pmatrix} E_5 & E_4 & E_3 & E_2 & E_1 \\ \mathbf{E}_5 & \mathbf{E}_4 & \mathbf{E}_3 & \mathbf{E}_2 & \mathbf{E}_1 \end{pmatrix},$$

che lasciano inalterate le (4).

Ponendo:

$$\mathbf{E}_5 \equiv E_5^u E_4^v, \quad \mathbf{E}_4 \equiv E_5^r E_4^s, \quad (\mathrm{mod}\, G_3), \tag{6}$$

affinchè la prima delle (4) si conservi, bisogna prendere $\mathbf{E}_3 \equiv E_3^\Delta \ (\mathrm{mod}\, G_2)$; quindi, per non contraddire alla definizione di $\mathbf{E}_3$, deve essere il determinante $\Delta = us - vr$ primo con p; poi, affinchè si conservino le ultime due delle formole (4), deve essere:

$$\mathbf{E}_2 = E_2^{\Delta u} E_1^{\Delta v}, \quad \mathbf{E}_1 = E_2^{\Delta r} E_1^{\Delta s}.$$

D'altra parte, io osservo che le operazioni T appartenenti alla classe definita dalle relazioni:

$$\mathbf{E}_5 \equiv E_5, \quad \mathbf{E}_4 \equiv E_4, \quad (\mathrm{mod}\, G_3),$$

non alterano α, β, γ, δ, perchè allora, rammentando che è $p > 2$, le (4) dànno:

$$\mathbf{E}_5^p = E_5^p, \quad \mathbf{E}_4^p = E_4^p, \quad \mathbf{E}_2 = E_2, \quad \mathbf{E}_1 = E_1.$$

Inoltre le dette operazioni costituiscono evidentemente un gruppo, che è divisore normale del gruppo di tutte le operazioni T che conservano le (4); dunque, giacchè m'interessa studiare le variazioni di α, β, γ, δ, posso ritenere eguale all'operazione identica ogni operazione di detta classe. In questa

ipotesi le (6) definiscono un'unica operazione che io rappresenterò con la notazione:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix}.$$

Ora si osservi che le relazioni (4), dietro un facile calcolo, dànno:

$$(E_5^h E_4^k)^n = E_5^{nh} E_4^{nk} E_3^{\binom{n}{2}hk} E_2^{\lambda} E_1^{\mu}, \tag{7}$$

dove per brevità si è ritenuto:

$$\lambda = k\left\{h^2\binom{n}{3}+\binom{h}{2}\binom{n}{2}\right\}, \quad \mu = h\left\{2k^3\binom{n}{3}+k^2\binom{n}{2}+\binom{k}{2}\binom{n}{2}\right\}.$$

Dunque, *supponendo* $p>3$, in virtù delle (5) si ha:

$$(E_5^h E_4^k)^p = E_5^{ph} E_4^{pk} = E_2^{h\alpha+k\gamma} E_1^{h\beta+k\delta}.$$

Ciò posto, chiamando α_1, β_1, γ_1, δ_1 i valori che assumono rispettivamente α, β, γ, δ dopo avere eseguita la trasformazione:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

in seguito ad un breve calcolo si ha:

$$\left.\begin{aligned} \Delta^2\alpha_1 &\equiv (\alpha u+\gamma v)s-(\beta u+\delta v)r \\ \Delta^2\beta_1 &\equiv (\beta u+\delta v)u-(\alpha u+\gamma v)v \\ \Delta^2\gamma_1 &\equiv (\alpha r+\gamma s)s-(\beta r+\delta s)r \\ \Delta^2\delta_1 &\equiv (\beta r+\delta s)u-(\alpha r+\gamma s)v. \end{aligned}\right\} \pmod p \tag{8}$$

Dalle formole (8) risulta:

$$\Delta(\alpha_1+\delta_1)\equiv\alpha+\delta, \quad \Delta^2(\alpha_1\delta_1-\beta_1\gamma_1)\equiv\alpha\delta-\beta\gamma, \pmod p. \tag{9}$$

Io introduco il numero:

$$D=(\alpha+\delta)^2-4(\alpha\delta-\beta\gamma),$$

e distinguo i tre casi possibili:

$$\left(\frac{D}{p}\right)=+1, \quad \left(\frac{D}{p}\right)=-1, \quad \left(\frac{D}{p}\right)=0;$$

dove, secondo Legendre, il simbolo $\left(\frac{D}{p}\right)$ denota il resto di $D^{\frac{p-1}{2}}$, che è preso rispetto al numero primo p ed ha il minimo valore assoluto.

27. *Caso* $\left(\frac{D}{p}\right) = +1$.

Il minimo intero q, positivo o nullo, che verifica la congruenza:

$$D\,q - (\alpha + \delta)^2 \equiv 0, \pmod{p}, \tag{10}$$

in virtù delle (9) resta inalterato per tutte le possibili operazioni:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

e quindi è un numero invariantivo per il gruppo rappresentato dal $G_5^{2,2}$ definito dalle relazioni (4) e (5) del presente paragrafo.

Ciò posto, il discriminante D della congruenza quadratica:

$$\rho^2 - (\alpha + \delta)\,\rho + (\alpha\,\delta - \beta\,\gamma) \equiv 0, \pmod{p},$$

è, nel caso attuale, un numero quadrato rispetto a mod p, e perciò la detta congruenza è soddisfatta da due interi ρ_1, ρ_2, che sono distinti rispetto a questo modulo.

È possibile dunque determinare quattro numeri u, v, r, s che verifichino le congruenze:

$$\left.\begin{aligned} \rho_1 u &\equiv \alpha\,u + \gamma\,v \\ \rho_1 v &\equiv \beta\,u + \delta\,v \end{aligned}\right\}, \quad \left.\begin{aligned} \rho_2 r &\equiv \alpha\,r + \gamma\,s \\ \rho_2 s &\equiv \beta\,r + \delta\,s \end{aligned}\right\}, \pmod{p},$$

e tali che risulti il determinante $\Delta = u\,s - v\,r$ primo con p; allora, facendo la trasformazione:

$$\begin{vmatrix} u & v \\ v & s \end{vmatrix},$$

le (8) dànno:

$$\Delta\,\alpha_1 \equiv \rho_1, \quad \Delta\,\delta_1 \equiv \rho_2, \quad \beta_1 \equiv \gamma_1 \equiv 0, \pmod{p}.$$

In conclusione, per i gruppi considerati nel presente caso, le relazioni (5) possono essere sostituite dalle relazioni:

$$E_5^p = E_2^\alpha, \quad E_4^p = E_1^\delta, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1, \tag{11}$$

dove la differenza $\delta - \alpha$ non è divisibile per p.

Prendendo come formole iniziali le (11), mediante le (8) si vede che, eseguendo la trasformazione:

$$\begin{vmatrix} u & 0 \\ 0 & s \end{vmatrix},$$

non viene alterata la loro forma, ma i numeri α e δ acquistano uno stesso fattore arbitrario primo con p: si può dunque supporre:

$$\delta - \alpha \equiv 2, \pmod{p}.$$

Ciò posto, se la somma $\alpha + \delta$ non è divisibile per p, denotando con ε una radice primitiva di p, si può porre:

$$\alpha \equiv \varepsilon^m - 1, \quad \delta \equiv \varepsilon^m + 1, \pmod{p};$$

allora, sostituendo questi valori di α e δ nella (10), si ottiene:

$$q \equiv \varepsilon^{2m}, \pmod{p}. \tag{12}$$

Quando si cambia m in $m + \frac{p-1}{2}$, il numero q resta inalterato, ma α e δ si cambiano rispettivamente in $-\delta$ e $-\alpha$.

Giacchè la trasformazione:

$$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix},$$

produce lo stesso cambiamento, io debbo fare sul numero m solamente le ipotesi:

$$m = 0, 1, \ldots, \frac{p-3}{2}.$$

In corrispondenza a questi tali valori di m, si hanno $\frac{p-1}{2}$ gruppi $G_5^{2,2}$ definiti dalle formole:

$$E_5^p = E_2^{\varepsilon^m - 1}, \quad E_4^p = E_1^{\varepsilon^m + 1}, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1$$

e dalle formole (4).

Questi gruppi sono effettivamente distinti, perchè in virtù della (12) due qualunque di essi hanno i numeri invariantivi q diseguali.

Se la somma $\alpha + \delta$ è divisibile per p, il che equivale a supporre $q = 0$, si ha:

$$\alpha \equiv -1, \quad \delta \equiv 1, \pmod{p},$$

e quindi si ottiene un nuovo gruppo $G_5^{2,2}$ corrispondente alle formole:

$$E_5^p = E_2^{-1}, \quad E_4^p = E_1, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1$$

28. *Caso* $\left(\frac{D}{p}\right) = -1$.

Il numero q che soddisfa alla (10) è, anche in questo caso, invariantivo per il gruppo rappresentato dal $G_5^{2,2}$ definito dalle formole (4) e (5); però, se detto numero non è zero, esso è un non residuo quadratico di p.

Giacchè nelle attuali ipotesi, nessuno dei numeri β, γ può essere multiplo di p, è possibile determinare un intero v in modo che sia:

$$2\gamma v \equiv \delta - \alpha, \pmod{p};$$

allora, eseguendo la trasformazione:

$$\begin{vmatrix} 1 & v \\ 0 & 1 \end{vmatrix},$$

le (8) dànno $\alpha_1 \equiv \delta_1 \pmod{p}$.

Io suppongo dunque che i valori iniziali di α e δ, presi rapporto a mod p, abbiano uno stesso valore ρ e cerco tutte le trasformazioni:

$$\begin{vmatrix} u & v \\ v & s \end{vmatrix},$$

che lasciano sussistere questa ipotesi.

Ora, essendo $\alpha \equiv \delta \equiv \rho$, affinchè sia $\alpha_1 \equiv \delta_1 \equiv \rho_1$, è necessario e sufficiente che u, v, r, s verifichino la congruenza:

$$\beta u v - \gamma v s \equiv 0, \pmod{p}; \tag{13}$$

e ciò risulta subito dalle formole (8).

Supponendo soddisfatta la (13), le (8) si possono sostituire con le formole:

$$\Delta \rho_1 \equiv \rho, \quad \Delta^2 \beta_1 \equiv \beta u^2 - \gamma v^2, \quad \Delta^2 \gamma_1 \equiv \gamma s^2 - \beta r^2, \pmod{p}, \tag{14}$$

mediante le quali si verifica subito che è:

$$\Delta^2 \beta_1 \gamma_1 \equiv \beta \gamma, \pmod{p}.$$

Giacchè si ha ora $D = 4\beta\gamma$, i due numeri β e γ sono necessariamente uno residuo e l'altro non residuo quadratico rispetto a mod p, ed è indifferente attribuire una di queste proprietà all'uno od all'altro numero, perchè si può dimostrare che esiste una trasformazione la quale, senza alterare ρ, scambia β con γ.

Infatti, se -1 è un numero quadrato mod p, il che ha luogo soltanto quando $p-1$ è multiplo di 4, trovato un intero v tale che $v^2 \equiv -1 \pmod{p}$,

ottengo l'intento mediante la trasformazione:

$$\begin{vmatrix} 0 & v \\ r & 0 \end{vmatrix}.$$

Se invece $p-1$ non è divisibile per 4, si considerino i $\frac{p+1}{2}$ numeri che si ottengono da $1+v^2$ attribuendo a v i valori:

$$0,\ 1,\ldots,\ \frac{p-1}{2}.$$

I detti numeri risultano distinti rispetto a mod p, e perciò non possono essere tutti residui quadratici di p. Dunque, giacchè per ipotesi non è mai $1+v^2$ un multiplo di p, nella serie dei valori attribuiti a v ne esiste almeno uno per cui $1+v^2$ è un non quadrato (mod p).

Allora, fissato per v un tale valore, scelgo, il che riesce possibile, per u ed s una soluzione del sistema:

$$\left.\begin{aligned} \beta u - \gamma s &\equiv 0 \\ u s - v^2 &\equiv 1 \end{aligned}\right\} \pmod p,$$

e considero poi la trasformazione:

$$\begin{vmatrix} u & v \\ v & s \end{vmatrix}.$$

Questa trasformazione appartiene alla classe definita dalla formola (13) ed ha il determinante eguale ad 1 (mod p); inoltre, le (14) mostrano che essa scambia semplicemente i numeri β e γ.

Sia dunque β un residuo quadratico di p. Se si pone $v \equiv r \equiv 0 \pmod p$, la (13) è verificata e le (14) dànno:

$$u s \rho_1 \equiv \rho, \quad s^2 \beta_1 \equiv \beta, \quad \pmod p;$$

perciò, *se non è* ρ multiplo di p, si possono determinare s ed u in modo che sia:

$$\rho_1 \equiv 1, \quad \beta_1 \equiv 1, \quad \pmod p;$$

poi la (10) dà:

$$\gamma_1 q \equiv 1, \quad \pmod p.$$

Quindi, ponendo $\gamma_1 \equiv \varepsilon^{2m+1} \pmod p$, si ha:

$$q \equiv \varepsilon^{-2m-1}, \quad (\mathrm{mod}\, p). \tag{15}$$

In conclusione, ottengo $\frac{p-1}{2}$ gruppi $G_5^{2,2}$ che sono definiti dalle (4) e dalle formole che si ottengono da:

$$E_5^p = E_2 E_1, \quad E_4^p = E_2 E_1^{\varepsilon^{2m+1}}, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1$$

facendo successivamente:

$$m = 0,\ 1, \ldots, \frac{p-3}{2}.$$

Questi gruppi sono effettivamente distinti perchè, in virtù della (15), due qualunque di essi hanno i numeri invariantivi q diseguali.

Se invece il numero ρ è un multiplo di p, il che equivale a supporre $q = 0$, ponendo come prima $v \equiv r \equiv 0 \pmod p$, le (14) dànno:

$$s^2 \beta_1 \equiv \beta, \quad u^2 \gamma_1 \equiv \gamma, \quad (\mathrm{mod}\, p);$$

e perciò si possono determinare s ed u in modo che sia:

$$\beta_1 \equiv 1, \quad \gamma_1 \equiv \varepsilon, \quad (\mathrm{mod}\, p):$$

ottengo quindi un nuovo gruppo $G_5^{2,2}$ definito dalle formole:

$$E_5^p = E_1, \quad E_4^p = E_2^\varepsilon, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1$$

e dalle relazioni (4).

29. *Caso* $\left(\frac{D}{p}\right) = 0$.

Si ha allora $D \equiv 0 \pmod p$ e quindi la congruenza:

$$\rho^2 - (\alpha + \delta)\rho + (\alpha\delta - \beta\gamma) \equiv 0 \pmod p$$

è soddisfatta da un solo resto ρ di p.

Scegliendo come numeri u e v una soluzione propria del sistema:

$$\begin{matrix} \rho u \equiv \alpha u + \gamma v \\ \rho v \equiv \beta u + \delta v \end{matrix} \pmod p,$$

la seconda delle (8) dà $\beta_1 \equiv 0 \pmod p$; quindi direttamente dalle (9) si ricava $\Delta\alpha_1 \equiv \Delta\delta_1 \equiv \rho \pmod p$.

Assumendo dunque:

$$\beta \equiv 0, \quad \alpha \equiv \delta \equiv \rho, \quad (\mathrm{mod}\, p),$$

le (8) si scrivono:

$$\left.\begin{array}{ll} \Delta^2\alpha_1 \equiv \Delta\rho + \gamma v s, & \Delta^2\beta_1 \equiv -v^2\gamma \\ \Delta^2\delta_1 \equiv \Delta\rho - \gamma v s, & \Delta^2\gamma_1 \equiv \quad s^2\gamma \end{array}\right\} \pmod p.$$

Ciò posto, se γ è primo con p, volendo conservare le condizioni iniziali, bisogna supporre v nullo $(\mathrm{mod}\, p)$; indi si può determinare u in modo che sia $\gamma_1 \equiv 1 \pmod p$ ovvero $\gamma_1 \equiv \varepsilon \pmod p$. Allora, se ρ è un multiplo di p, si ha $\alpha_1 \equiv \delta_1 \equiv 0 \pmod p$, in caso contrario si possono scegliere r ed s in modo che sia $\alpha_1 \equiv \delta_1 \equiv 1 \pmod p$.

Se poi è γ un multiplo di p, si ha sempre $\beta_1 \equiv \gamma_1 \equiv 0 \pmod p$, ma è $\alpha_1 \equiv \delta_1 \equiv 0 \pmod p$, ovvero si può supporre $\alpha_1 \equiv \delta_1 \equiv 1 \pmod p$, secondo che è, ovvero non è, ρ un multiplo di p.

In conclusione, in corrispondenza all'ipotesi $\left(\frac{D}{p}\right) = 0$, si hanno soltanto *sei* gruppi, i quali sono definiti dalle (4) e dalle seguenti modificazioni delle formole (5):

$E_5^p = 1,$	$E_4^p = E_2,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = E_2,$	$E_4^p = E_2 E_1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = 1,$	$E_4^p = E_2^\varepsilon,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = E_2,$	$E_4^p = E_2^\varepsilon E_1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = 1,$	$E_4^p = 1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = E_2,$	$E_4^p = E_1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$

30. Finalmente io passo ad esaminare il caso di $p = 3$, che ho escluso verso la fine del n.° 26. Quando è $p = 3$ tutte le possibili operazioni:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

definite precedentemente costituiscono un gruppo di grado 48; però, osservando che l'operazione:

$$\begin{vmatrix} -1 & 0 \\ 0 & -1 \end{vmatrix}$$

lascia inalterati i quattro numeri α, β, γ, δ che figurano nelle (5), io non considero come distinte le due operazioni:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix}, \qquad \begin{vmatrix} -u & -v \\ -r & -s \end{vmatrix},$$

ed allora il grado del detto gruppo si riduce di metà. Il gruppo di grado 24, che così si ottiene, è isomorfo al gruppo dell'ottaedro (*): esso può essere generato mediante le tre operazioni:

$$U = \begin{vmatrix} -1 & 0 \\ 0 & 1 \end{vmatrix}, \qquad V = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}, \qquad W = \begin{vmatrix} 1 & 1 \\ -1 & 1 \end{vmatrix},$$

che sono ordinatamente di secondo, terzo e quarto ordine e che soddisfano alle relazioni:

$$V^2 W = W^3 V, \quad W^3 U = U W, \quad U V^2 = V U.$$

Si vede subito, tenendo presenti le formole (4) e (5), che la U non altera β e γ, ma cambia soltanto di segno α e δ.

Facendo uso della (7), si verifica facilmente che l'operazione V cambia la somma $\alpha + \delta$ in $\alpha + \delta + 1$ e quindi l'operazione V^2 cambia la detta somma in $\alpha + \delta + 2$; perciò non si lede la generalità ponendo:

$$\alpha + \delta \equiv 0, \pmod 3. \tag{16}$$

Ciò posto, servendosi della (7) e tenendo conto della congruenza (16), un breve calcolo mostra che l'operazione W produce sopra i numeri α, β, γ, δ la sostituzione congrua:

$$\left.\begin{aligned} \alpha_1 &\equiv \beta + \gamma, & \beta_1 &\equiv \alpha + \beta - \gamma + 1, \\ \delta_1 &\equiv -\beta - \gamma, & \gamma_1 &\equiv -\beta + \gamma - \delta - 1, \end{aligned}\right\} \pmod 3.$$

(*) Per convincersene, basta far corrispondere alle tre operazioni che sono denotate in seguito con U, V, W, ordinatamente le tre sostituzioni: (0 2), (0 1 2), (0 1 2 3).

Dunque le operazioni W ed U lasciano inalterata la (16) e lo stesso fa ogni operazione del gruppo di grado 8 da esse generato; mentre una qualunque delle rimanenti 16 operazioni, potendosi ottenere come prodotto di una operazione del detto gruppo di grado 8 per V, ovvero per V^2, non lascia sussistere la congruenza (16). In virtù di questa congruenza, relativamente ai valori di α e δ, si possono fare le seguenti tre ipotesi:

$$\alpha \equiv 0,\ \delta \equiv 0;\quad \alpha \equiv 1,\ \delta \equiv 2;\quad \alpha \equiv 2,\ \delta \equiv 1,\ \pmod 3;$$

poi a ciascuna di queste tre coppie si può associare una coppia qualunque di valori di β e γ: si ottengono così 27 quaterne di numeri $(\alpha\,\beta\,\gamma\,\delta)$ a ciascuna delle quali corrisponde un gruppo $G_5^{2,2}$ di grado $3^5 = 243$.

Però due quaterne, che si deducono l'una dall'altra mediante una operazione del precedente gruppo di grado 8, si debbono ritenere equivalenti in quanto che esse definiscono due gruppi isomorfi di grado 243.

Nella tabella che segue io scrivo tutte le 27 quaterne, mettendo in una stessa linea orizzontale le quaterne che sono equivalenti.

(1 0 1 2)	(1 1 1 2)	(2 2 0 1)	(2 2 2 1)	(2 0 1 1)	(2 1 1 1)	(1 2 0 2)	(1 2 2 2)
(1 0 2 2)	(2 0 2 1)	(2 1 0 1)	(1 1 0 2)				
(0 1 1 0)	(2 1 2 1)	(0 2 2 0)	(1 1 2 2)				
(0 0 1 0)	(1 0 0 2)	(0 2 0 0)	(2 0 0 1)				
(0 0 2 0)	(2 2 1 1)	(0 1 0 0)	(1 2 1 2)				
(0 0 0 0)	(0 1 2 0)						
(0 2 1 0)							

Si vede dunque che esistono soltanto *sette* gruppi $G_5^{2,2}$ di grado 243, che non posseggono alcun divisore Abeliano d'indice 3 e questi gruppi si posson fare corrispondere alle sette quaterne $(\alpha\,\beta\,\gamma\,\delta)$, che stanno nella prima linea verticale della precedente tabella.

Io scrivo le formole che, insieme alle (4), servono a definire i detti gruppi.

$E_5^3 = E_2$,	$E_4^3 = E_2 E_1^2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = E_2$,	$E_4^3 = E_2^2 E_1^2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = E_1$,	$E_4^3 = E_2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = 1$,	$E_4^3 = E_2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = 1$,	$E_4^3 = E_2^2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = 1$,	$E_4^3 = 1$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = E_1^2$,	$E_4^3 = E_2$,	$E_3^3 = 1$,	$E_2^3 = 1$,	$E_1^3 = 1$

31. Nel presente paragrafo io ho stabilito quanto segue.

Ogni gruppo $G_5^{2,2}$, che non possiede alcun divisore Abeliano d'indice p, è perfettamente definito dalle formole (4) e (5), purchè si tenga presente che E_2 ed E_1 appartengono al divisore invertibile H.

Non esistono di tali gruppi di grado $2^5 = 32$.

Esistono soltanto sette di tali gruppi di grado $3^5 = 243$.

Finalmente, quando il numero primo p supera 3, esistono $p + 7$, e non più, di tali gruppi, i quali, rispetto alle formole (4) e (5), si classificano nella seguente maniera.

Quando gl'interi α, β, γ, δ verificano la congruenza:

$$D = (\alpha + \delta)^2 - 4(\alpha\delta - \beta\gamma) \equiv 0, \pmod{p},$$

si ha uno dei sei gruppi trovati al n.° 29; in ogni altro caso, il minimo numero q positivo o nullo, che verifica la congruenza:

$$Dq - (\alpha + \delta)^2 \equiv 0, \pmod{p},$$

è un numero invariantivo per il gruppo definito dalla quaterna $(\alpha\beta\gamma\delta)$.

In corrispondenza ad ogni numero $q > 0$ si ha un solo gruppo; ma, per $q = 0$, si hanno due gruppi secondo che D è, ovvero non è, un residuo quadratico di p.

I diversi tipi di gruppi trovati nel presente paragrafo sono rappresentati nella seguente tabella.

I.

$$\{H(E_2,\ E_1)\},\ \{K(E_3,\ E_2,\ E_1)\}.$$

$$E_5^{-1}E_4E_5 = E_4E_3,\quad E_5^{-1}E_3E_5 = E_3E_2,\quad E_4^{-1}E_3E_4 = E_3E_1.$$

Gruppi $G_5^{2,2}$

E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
$E_2^{\varepsilon^{m}-1}$	$E_1^{\varepsilon^m+1}$	1	1	1	$\left(\frac{D}{p}\right)=+1$
E_2^{-1}	E_1	1	1	1	
E_2E_1	$E_2E_1^{\varepsilon^{2m+1}}$	1	1	1	$\left(\frac{D}{p}\right)=-1$
E_1	E_2^{ε}	1	1	1	
1	E_2	1	1	1	
E_2	E_2E_1	1	1	1	
1	E_2^{ε}	1	1	1	$\left(\frac{D}{p}\right)=0$
E_2	$E_2^{\varepsilon}E_1$	1	1	1	
1	1	1	1	1	
E_2	E_1	1	1	1	

$$m = 0,\ 1,\ \ldots,\ \frac{p-3}{2}\quad \{p>3\}$$

II.

Gruppi $G_5^{2,2}$ di grado 243

E_5^3	E_4^3	E_3^3	E_2^3	E_1^3
E_2	$E_2E_1^2$	1	1	1
E_2	$E_2^3E_1^2$	1	1	1
E_1	E_2	1	1	1
1	E_2	1	1	1
1	E_2^2	1	1	1
1	1	1	1	1
E_1^2	E_2	1	1	1

§ V. I Gruppi G_5^2 che posseggono un divisore Abeliano d'indice p.

32. Al principio del n.° 25 si è osservato che un gruppo G_5^2 può contenere uno oppure nessuno divisore Abeliano d'indice p. Io ho svolto nel paragrafo precedente l'analisi relativa alla seconda ipotesi ed ora mi propongo di svolgere in questo paragrafo l'analisi relativa alla prima.

Il divisore Abeliano G_4^0 contenuto per ipotesi in G_5^2, contiene evidentemente il divisore invertibile H, e quindi è possibile costruire una serie canonica di composizione:

$$G_5^2, \quad G_4^0, \quad G_3, \quad G_2, \quad G_1,$$

tale che sia $G_2 = H$.

Denotando con:

$$E_5, \quad E_4, \quad E_3, \quad E_2, \quad E_1,$$

una base relativa alla detta serie e scrivendo le formole:

$$E_5^{-1} E_4 E_5 = E_4 E'_3, \quad E_5^{-1} E_3 E_5 = E_3 E'_2, \quad E_4^{-1} E_3 E_4 = E_3,$$

l'elemento E'_3 può essere contenuto o non essere contenuto in H. Questi due casi si debbono distinguere accuratamente, perchè, in corrispondenza, si hanno due classi di gruppi G_5^2 ben diverse.

Comincio ad occuparmi del primo caso, il quale è equivalente all'ipotesi di ritenere il gruppo K coincidente col gruppo H, perchè, in virtù del ragionamento fatto al n.° 24, in tal caso, anche quando è $p = 2$, la potenza p^{ma} di un elemento qualunque di G_5^2 sta in H.

Dunque deve essere $E'^p_3 = 1$, $E'^p_2 = 1$; e siccome gli elementi E'_3, E'_2 non possono appartenere ad uno stesso gruppo ciclico (n.° 24), i detti elementi sono di grado p e possono generare il gruppo H.

Io posso dunque scrivere le formole:

$$\left.\begin{aligned} &E_5^{-1} E_4 E_5 = E_4 E_2, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_4^{-1} E_3 E_4 = E_3, \\ &E_5^p = E_2^\lambda E_1^\mu, \quad E_4^p = E_2^\alpha E_1^\beta, \quad E_3^p = E_2^\gamma E_1^\delta, \quad E_2^p = 1, \quad E_1^p = 1. \end{aligned}\right\} \quad (1)$$

Queste formole definiscono, qualunque siano gl'interi λ, μ, α, β, γ, δ, un gruppo G_5^2, e tutti i gruppi così definiti appartengono evidentemente alla classe dei gruppi $G_5^{2,3}$.

Si consideri una nuova base canonica:

$$\mathbf{F}_5, \quad \mathbf{F}_4, \quad \mathbf{F}_3, \quad \mathbf{F}_2, \quad \mathbf{F}_1,$$

tale che l'operazione T che porta questa nuova base nella primitiva non alteri le prime tre delle relazioni (1).

Ponendo:

$$\mathbf{E}_5 \equiv E_5, \quad \mathbf{E}_4 \equiv E_4^u E_3^v, \quad \mathbf{E}_3 \equiv E_4^r E_3^s, \quad (\text{mod } G_2), \tag{2}$$

si trova:

$$\mathbf{E}_2 \equiv E_2^u E_1^v, \quad \mathbf{E}_1 \equiv E_2^r E_1^s;$$

e giacchè $\mathbf{E}_2$ ed $\mathbf{E}_1$ sono due elementi generatori di H, deve supporsi il determinante $\Delta = u\,s - v\,r$ primo con p. Per la osservazione più volte fatta, considero come una sola operazione tutte le operazioni T appartenenti alla classe definita dalle (2), quando si attribuiscono ad u, v, r, s determinati resti di p, e quest'unica operazione la rappresento col simbolo:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix}.$$

Inoltre, se si cambia soltanto l'elemento $\mathbf{E}_5$ ponendo, nella maniera più generale,

$$\mathbf{E}_5 \equiv E_5^\sigma, \quad (\text{mod } G_4^0),$$

essendo σ primo con p, risulta subito dalle (1) che i quattro numeri α, β, γ, δ acquistano uno stesso fattore arbitrario primo con p: dunque le due quaterne $(\alpha, \beta, \gamma, \delta)$, $(\sigma\alpha, \sigma\beta, \sigma\gamma, \sigma\delta)$ debbono ritenersi equivalenti.

Ciò posto, eseguendo l'operazione:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

si trovano facilmente le relazioni:

$$\left.\begin{aligned} \Delta\,\alpha_1 &\equiv (\alpha u + \gamma v)\,s - (\beta u + \delta v)\,r \\ \Delta\,\beta_1 &\equiv (\beta u + \delta v)\,u - (\alpha u + \gamma v)\,v \\ \Delta\,\gamma_1 &\equiv (\alpha r + \gamma s)\,s - (\beta r + \delta s)\,r \\ \Delta\,\delta_1 &\equiv (\beta r + \delta s)\,u - (\alpha r + \gamma s)\,v \end{aligned}\right\} (\text{mod } p), \tag{3}$$

dalle quali risulta:

$$\alpha_1 + \delta_1 \equiv \alpha + \delta, \quad \alpha_1\delta_1 - \beta_1\gamma_1 \equiv \alpha\delta - \beta\gamma, \quad (\text{mod } p). \tag{4}$$

Allora, *supponendo* $p > 2$, introduco il numero:

$$D = (\alpha + \delta)^2 - 4(\alpha\delta - \beta\gamma),$$

e distinguo, come nel paragrafo precedente, i tre casi di:

$$\left(\frac{D}{p}\right) = +1, \quad \left(\frac{D}{p}\right) = -1, \quad \left(\frac{D}{p}\right) = 0.$$

33. Nei primi due casi, il minimo numero intero q, positivo o nullo, che verifica la congruenza:

$$D\,q - (\alpha + \delta)^2 \equiv 0, \pmod{p},$$

resta inalterato per tutte le possibili operazioni T, perchè, quando si moltiplicano i quattro numeri $\alpha, \beta, \gamma, \delta$ per uno stesso fattore σ primo con p, i numeri D ed $(\alpha + \delta)^2$ acquistano lo stesso fattore σ^2; quindi q ha carattere invariantivo per il gruppo rappresentato dal $G_5^{2,3}$ definito dalle relazioni (1) del presente paragrafo.

Quando è $\left(\frac{D}{p}\right) = +1$, la congruenza:

$$\rho^2 - (\alpha + \delta)\,\rho + (\alpha\,\delta - \beta\,\gamma) \equiv 0, \pmod{p},$$

è soddisfatta da due distinti resti di p; mentre quando è $\left(\frac{D}{p}\right) = -1$, non esiste alcun numero intero che verifichi la detta congruenza; allora, relativamente alla quaterna di numeri $\alpha, \beta, \gamma, \delta$, l'analisi procede in modo perfettamente analogo a quella dei n.i 27 e 28 del § IV e non è necessario ripeterla qui.

In riguardo ai numeri λ e μ io faccio la seguente osservazione.

Cambiando solamente l'elemento $\mathbf{E}_5$ che figura nelle (2), ponendo:

$$\mathbf{E}_5 \equiv E_5\,E_4^h\,E_3^k, \pmod{G_2},$$

i numeri $\alpha, \beta, \gamma, \delta$ restano inalterati, ma λ e μ si cambiano rispettivamente in due numeri λ_1 e μ_1 tali che:

$$\left.\begin{aligned} \lambda_1 &\equiv \lambda + \alpha\,h + \gamma\,k \\ \mu_1 &\equiv \mu + \beta\,h + \delta\,k \end{aligned}\right\} \pmod{p}. \tag{5}$$

Infatti, dalle formule (1) si ricava:

$$(E_5\,E_4^h\,E_3^k)^n = E_5^n\,E_4^{nh}\,E_3^{nk}\,E_2^{h\binom{n}{2}}\,E_1^{k\binom{n}{2}}, \tag{6}$$

e quindi, avendo supposto $p > 2$, si ha:

$$\mathbf{E}_5^p = E_5^p\,E_4^{ph}\,E_3^{pk}.$$

Ciò posto, quando il determinante $\alpha\delta - \beta\gamma$ è primo con p, cioè quando E_4^p ed E_3^p sono due elementi generatori del gruppo H, si possono determinare gl'interi h e k in modo che sia:

$$\lambda_1 \equiv \mu_1 \equiv 0, \pmod{p};$$

dunque, in tale ipotesi, è lecito supporre $E_5^p = 1$.

Fatte queste considerazioni, si vede che nel caso di $\left(\frac{D}{p}\right) = +1$, si hanno $\frac{p-1}{2}$ gruppi $G_5^{2,3}$ in corrispondenza alle seguenti modificazioni delle ultime cinque formole (1):

$$\boxed{E_5^p = 1, \quad E_4^p = E_2^{\varepsilon^m - 1}, \quad E_3^p = E_1^{\varepsilon^m + 1}, \quad E_2^p = 1, \quad E_1^p = 1} \tag{7}$$

essendo $m = 0, \ldots, \frac{p-3}{2}$.

Oltre ai detti $\frac{p-1}{2}$ gruppi, esistono ancora altri due particolari gruppi: il primo di questi si presenta quando il numero invariantivo q è nullo. In tal caso si ha un gruppo che corrisponde alle formole:

$$\boxed{E_5^p = 1, \quad E_4^p = E_2^{-1}, \quad E_3^p = E_1, \quad E_2^p = 1, \quad E_1^p = 1}$$

Il secondo gruppo particolare si presenta qualora si osservi che, nell'ipotesi di $m = 0$, non è sempre lecito supporre nelle (7) $E_5^p = 1$, perchè, nella detta ipotesi, E_4^p ed E_3^p non sono due elementi generatori di H. Ma essendo, nel caso attuale, $\alpha = \beta = \gamma = 0$ e $\delta = 2$, le (5) mostrano che si può sempre supporre $\mu = 0$; poi, se non è λ un multiplo di p, chiamando E_4 l'elemento E_4^λ, dalle (1) risulta che si può ritenere $\lambda = 1$. Ottengo così un nuovo gruppo $G_5^{2,3}$ corrispondente alle formole:

$$\boxed{E_5^p = E_2, \quad E_4^p = 1, \quad E_3^p = E_1, \quad E_2^p = 1, \quad E_1^p = 1}$$

Nel caso di $\left(\frac{D}{p}\right) = -1$ si hanno $\frac{p-1}{2}$ gruppi $G_5^{2,3}$ sostituendo le ultime cinque delle relazioni (1) con:

$$\boxed{E_5^p = 1, \quad E_4^p = E_2 E_1, \quad E_3^p = E_2 E_1^{\varepsilon^{2m+1}}, \quad E_2^p = 1, \quad E_1^p = 1}$$

e facendo poi successivamente:

$$m = 0, \ldots, \frac{p-3}{2};$$

inoltre, si ha un nuovo gruppo $G_5^{2,3}$ nell'ipotesi di $q = 0$ e questo gruppo corrisponde alle formole:

$$E_5^p = 1, \quad E_4^p = E_1, \quad E_3^p = E_2^\varepsilon, \quad E_2^p = 1, \quad E_1^p = 1$$

34. *Caso* $\left(\frac{D}{p}\right) = 0$.

Si ha allora $D \equiv 0 \pmod p$ e quindi la congruenza:

$$\rho^2 - (\alpha + \delta)\rho + (\alpha\delta - \beta\gamma) \equiv 0 \pmod p$$

è soddisfatta da un solo resto ρ di p; poi, ragionando come nel n.° 29, si vede che è lecito supporre:

$$\beta \equiv 0, \quad \alpha \equiv \delta \equiv \rho \pmod p$$

e quindi le formole (3) si scrivono:

$$\left.\begin{array}{llll} \Delta\alpha_1 \equiv \Delta\rho + \gamma v s, & \Delta\beta_1 \equiv -v^2\gamma \\ \Delta\delta_1 \equiv \Delta\rho - \gamma v s, & \Delta\gamma_1 \equiv & s^2\gamma \end{array}\right\} \pmod p.$$

Ciò posto, se γ è primo con p, volendo conservare le condizioni iniziali, bisogna supporre $v \equiv 0 \pmod p$; indi, se ρ è primo con p, scelgo gl'interi u ed s in modo che sia $\gamma_1 \equiv \rho \pmod p$, e se ρ è un multiplo di p, scelgo i detti interi in modo che sia $\gamma_1 \equiv 1 \pmod p$. Dunque, se è γ primo con p, giacchè α, β, γ, δ si possono moltiplicare per un fattore arbitrario (n.° 32), è lecito assumere:

$$\alpha = \delta = \gamma = 1, \quad \beta = 0,$$

ovvero:

$$\alpha = \delta = \beta = 0, \quad \gamma = 1.$$

Se invece γ è un multiplo di p, si vede subito che si può assumere:

$$\alpha = \delta = 1, \quad \beta = \gamma = 0,$$

ovvero:

$$\alpha = \delta = 0, \quad \beta = \gamma = 0.$$

Nel primo e nel terzo di questi quattro casi, per l'osservazione fatta nel n.° precedente, suppongo $\lambda = 0$, $\mu = 0$; ma il secondo e quarto caso si scindono ognuno in due dietro le considerazioni che seguono.

Quando è $\alpha = \delta = \beta = 0$ e $\gamma = 1$, le (5) mostrano che si può supporre $\lambda = 0$: allora, se μ è un multiplo di p, si ha $E_5^p = 1$; e se μ è primo con p, eseguendo l'operazione:

$$\begin{vmatrix} \mu & 0 \\ 0 & \mu \end{vmatrix},$$

α, β, γ, δ non si alterano e μ va nel resto 1 di p.

Quando è $\alpha = \beta = \gamma = \delta = 0$ ed uno dei due numeri λ, μ è primo con p, una delle due operazioni:

$$\begin{vmatrix} 1 & 0 \\ \lambda & \mu \end{vmatrix}, \qquad \begin{vmatrix} 0 & 1 \\ \lambda & \mu \end{vmatrix},$$

ha il determinante primo con p, e questa tale operazione dà $E_5^p = E_1$; se poi i numeri λ, μ sono entrambi multipli di p, allora è $E_5^p = 1$.

In conclusione, nel caso $\left(\frac{D}{p}\right) = 0$, si hanno *sei* gruppi $G_5^{2,3}$ i quali corrispondono alle seguenti modificazioni delle ultime cinque formole (1):

$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = E_2 E_1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = E_1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1$,	$E_4^p = 1$,	$E_3^p = E_2$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

35. Io prendo ora in esame il caso di $p = 2$ che fu escluso alla fine del n.° 32.

In questo caso, tutte le operazioni:

$$\begin{vmatrix} u & v \\ r & s \end{vmatrix},$$

costituiscono un gruppo di grado 6, che è isomorfo a quello che si è presentato nel n.° 9 del § II.

Le due operazioni:

$$U = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}, \qquad V = \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix},$$

generatrici del detto gruppo producono sopra i numeri $\alpha, \beta, \gamma, \delta$ le due sostituzioni congrue:

$$\left.\begin{array}{l} \alpha_1 \equiv \alpha + \gamma, \quad \beta_1 \equiv \alpha + \beta + \gamma + \delta, \quad \gamma_1 \equiv \gamma, \quad \delta_1 \equiv \gamma + \delta; \\ \alpha_1 \equiv \gamma + \delta, \quad \beta_1 \equiv \gamma, \quad \gamma_1 \equiv \alpha + \beta + \gamma + \delta, \quad \delta_1 \equiv \alpha + \gamma; \end{array}\right\} \pmod 2,$$

rispettivamente; e ciò si verifica subito mediante le (3).

Siccome ognuno dei numeri $\alpha, \beta, \gamma, \delta$ può ritenersi, indipendentemente, eguale a *0* od eguale ad *1*, si hanno 16 quaterne $(\alpha\beta\gamma\delta)$; però io assumo come equivalenti due tali quaterne che si deducono l'una dall'altra eseguendo una operazione composta con U e V.

Nella tabella che segue sono scritte tutte le 16 quaterne in modo che le quaterne equivalenti stanno in una stessa linea orizzontale.

(0 0 0 1)	(1 0 1 0)	(1 1 0 0)	(0 1 0 1)	(0 0 1 1)	(1 0 0 0)
(0 0 1 0)	(1 1 1 1)	(0 1 0 0)			
(0 1 1 0)	(1 1 0 1)	(1 0 1 1)			
(0 1 1 1)	(1 1 1 0)				
(1 0 0 1)					
(0 0 0 0)					

Allora io considero le sei quaterne che figurano nella prima verticale del precedente quadro e, per ognuna di esse, mi formo il gruppo $|\alpha\beta\gamma\delta|$ costituito da tutte operazioni:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ \mathbf{F}_5, & \mathbf{F}_4, & \mathbf{F}_3, & \mathbf{F}_2, & \mathbf{F}_1 \end{pmatrix},$$

che lasciano inalterata la quaterna $(\alpha\beta\gamma\delta)$.

Chiamando W una qualunque delle quattro operazioni definite dalle formole:

$$\mathbf{E}_5 \equiv E_5 E_4^h E_3^k, \quad \mathbf{E}_4 \equiv E_4, \quad \mathbf{E}_3 \equiv E_3, \quad (\text{mod } G_2),$$

è evidente che il gruppo generato dalle operazioni W e dalle operazioni U, V contiene tutte le possibili trasformazioni T.

Il detto gruppo è isomorfo al gruppo dell'ottaedro: alle quattro operazioni W corrispondono le quattro sostituzioni del gruppo quaternario normale.

Per rendere chiaro quel che segue, scrivo le relazioni:

$$(E_5 E_4)^2 = E_5^2 E_4^2 E_2, \quad (E_5 E_3)^2 = E_5^2 E_3^2 E_1,$$

che si possono, se più piace, ricavare dalla (6).

Ciò posto, il gruppo $\boxed{0001}$ è costituito dalle operazioni W: una qualunque di esse o lascia inalterati i numeri λ e μ oppure cambia soltanto λ in $\lambda + 1$; dunque, associando alla quaterna (0 0 0 1) una delle due coppie (0 0), (0 1) come coppia $(\lambda\,\mu)$, si ottengono in corrispondenza due gruppi $G_5^{2,3}$ distinti di grado 32.

Il gruppo $\boxed{0010}$ è generato dalle operazioni W e dall'operazione $U\,V$, e mediante le W si può portare la coppia $(\lambda\,\mu)$ in (0 0).

Il gruppo $\boxed{0110}$ è generato dalle operazioni W e dalla operazione $U\,V^2$: una qualunque W o non altera i numeri λ e μ oppure aumenta i detti numeri contemporaneamente di una unità; e la $U\,V^2$ scambia semplicemente λ con μ. Dunque, associando alla quaterna (0 1 1 0) o la coppia (0 0) oppure la coppia (0 1) si ottengono, in corrispondenza, due gruppi distinti $G_5^{2,3}$ di grado 32.

Il gruppo $\boxed{0111}$ è generato dalla operazione V e dalle W e mediante le W si può portare la coppia $(\lambda\,\mu)$ nella coppia (0 0).

Il gruppo $\boxed{1001}$ è il gruppo principale generato dalle W e dalle U, V: una qualunque delle W non altera λ e μ; l'operazione U cambia soltanto μ in $\mu + \lambda$ e l'operazione V cambia soltanto λ in $\lambda + \mu$. Dunque, associando alla quaterna (1 0 0 1) la coppia (0 0) oppure la coppia (0 1), si ottengono, in corrispondenza, due gruppi distinti $G_5^{2,3}$ di grado 32.

Finalmente, il gruppo $\boxed{0000}$ coincide anche col detto gruppo principale e mediante le W si può portare la coppia $(\lambda\,\mu)$ nella coppia (0 0).

La conclusione della precedente analisi è che, nelle attuali ipotesi, esistono *nove* gruppi $G_5^{2,3}$ di grado 32, e questi gruppi corrispondono alle seguenti modificazioni delle ultime cinque delle formole (1).

$E_5^2=1$,	$E_4^2=1$,	$E_3^2=E_1$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=E_1$,	$E_4^2=1$,	$E_3^2=E_1$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=1$,	$E_3^2=E_2$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=E_1$,	$E_3^2=E_2$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=E_1$,	$E_4^2=E_1$,	$E_3^2=E_2$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=E_1$,	$E_3^2=E_2E_1$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=E_2$,	$E_3^2=E_1$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=E_1$,	$E_4^2=E_2$,	$E_3^2=E_1$,	$E_2^2=1$,	$E_1^2=1$
$E_5^2=1$,	$E_4^2=1$,	$E_3^2=1$,	$E_2^2=1$,	$E_1^2=1$

36. Io ritorno all'ordine d'idee col quale ho incominciato il presente paragrafo e riscrivo le formole:

$$E_5^{-1}E_4E_5=E_4E'_3,\quad E_5^{-1}E_3E_5=E_3E'_2,\quad E_4^{-1}E_3E_4=E_3.$$

Ho già studiato in modo completo il caso in cui l'elemento E'_3 appartiene al gruppo H, ed ora voglio fare l'ipotesi che il detto elemento stia fuori di H.

La potenza E_3^p sta in H e quindi si ha $E'^p_2=1$; inoltre, giacchè non può E'_2 coincidere con l'elemento identico perchè E_3 è fuori di H, posso scrivere le relazioni:

$$E_5^{-1}E_4E_5=E_4E_3,\quad E_5^{-1}E_3E_5=E_3E_1,\quad E_4^{-1}E_3E_4=E_3. \tag{8}$$

Si supponga $p>2$: allora, siccome l'elemento E_4^p sta (n.° 24) in H, deve essere $E_3^p=1$.

Si ammetta, in prima ipotesi, il gruppo H ciclico: in tale caso, scegliendo E_2 in modo che sia $E_2^p=1$, ho:

$$E_5^p=E_2^\alpha,\quad E_4^p=E_2^\beta,\quad E_3^p=1,\quad E_2^p=E_1,\quad E_1^p=1; \tag{9}$$

e, purchè si rammenti che gli elementi E_2, E_1 stanno in H, queste formole, insieme alle (8), definiscono un gruppo G_5^2 qualunque siano gl'interi α e γ.

Se chiamo E_5 ed E_4 gli elementi $E_5 E_2^h$ ed $E_4 E_2^k$ rispettivamente, i numeri α e β si cambiano in $\alpha + p h$ e $\beta + p k$, e quindi i detti numeri si debbono intendere determinati a meno di multipli di p.

Ciò posto, avendosi una seconda base canonica:

$$\mathbf{F}_5, \quad \mathbf{F}_4, \quad \mathbf{F}_3, \quad \mathbf{F}_2, \quad \mathbf{F}_1,$$

definita nello stesso modo della prima, se, nella maniera più generale, si ha:

$$\mathbf{E}_5 \equiv E_5^u E_4^v, \quad \mathbf{E}_4 \equiv E_4^s, \quad (\mathrm{mod}\ G_3),$$

deve essere:

$$\mathbf{F}_3 \equiv E_3^{us}, \quad \mathbf{F}_2 \equiv E_2^{u^2 s}, \quad (\mathrm{mod}\ G_1),$$

ed il prodotto $u\,s$ deve necessariamente supporsi primo con p.

Intanto, dalle (8) si ricava:

$$(E_5 E_4)^n = E_5^n E_4^n E_3^{\binom{n}{2}} E_2^{\binom{n}{3}},$$

e perciò, *se è* $p > 3$, si ha:

$$(E_5 E_4)^p = E_5^p E_4^p.$$

Allora, sia p maggiore od eguale a 3, eseguendo l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ \mathbf{E}_5, & \mathbf{E}_4, & \mathbf{E}_3, & \mathbf{E}_2, & \mathbf{E}_1 \end{pmatrix},$$

si vede subito che α e β subiscono la sostituzione congrua:

$$\left.\begin{aligned} u^2 s\,\alpha_1 &\equiv \alpha u + \beta v \\ u^2 \beta_1 &\equiv \beta \end{aligned}\right\} \ (\mathrm{mod}\ p).$$

Dunque: se β è un multiplo di p, posso determinare u ed s in modo che α_1 sia o il resto 0 o il resto 1 di p; se invece β è primo con p, posso determinare u in modo che sia o $\beta_1 \equiv 1 \pmod p$ oppure $\beta_1 \equiv \varepsilon \pmod p$ e, in entrambi i casi, dispongo di v in modo che α_1 sia il resto 0 di p.

In conclusione, quando H è ciclico ed è $p > 2$, si hanno quattro gruppi G_5^2 in corrispondenza alle seguenti quattro serie di formole che sono modificazioni delle (9).

$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = E_1$,	$E_1^p = 1$
$E_5^p = E_2$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = E_1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = E_1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_2^\varepsilon$,	$E_3^p = 1$,	$E_2^p = E_1$,	$E_1^p = 1$

Il G_5^2 corrispondente alla prima serie di formole è un gruppo $G_5^{2,3}$, ed il relativo gruppo K è generato dagli elementi E_3, E_1; invece i tre gruppi corrispondenti alle ultime tre formole sono gruppi $G_5^{2,2}$ e, per ciascuno di essi, il gruppo K è generato dagli elementi E_3, E_2, E_1.

37. Si ammetta, in seconda ipotesi, che il gruppo H abbia tutti i suoi elementi di grado p.

In tale caso bisogna sostituire le (9) con le formole:

$$E_5^p = E_2^\alpha E_1^\beta, \quad E_4^p = E_2^\gamma E_1^\delta, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1, \qquad (10)$$

le quali, insieme alle (8), definiscono un gruppo G_5^2 qualunque siano gl'interi α, β, γ, δ.

Se il gruppo G_5^2 così definito è un $G_5^{2,2}$, uno almeno dei due numeri α, γ è primo con p.

Quando è γ primo con p, io pongo a definizione dell'elemento E_2 la relazione $E_4^p = E_2$. Allora, se v ed s sono interi ed il secondo è primo con p, eseguendo l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5 E_4^v, & E_4^s, & E_3^s E_1^s, & E_2^s, & E_1^s \end{pmatrix},$$

la quale non altera nè la detta relazione nè le formole (8), si vede subito che i numeri α, β si portano in due numeri α_1, β_1 tali che:

$$s\,\alpha_1 \equiv \alpha + v, \quad s\,\beta_1 \equiv \beta, \quad (\mathrm{mod}\, p > 3),$$

ovvero tali che:

$$s\,\alpha_1 \equiv \alpha + v, \quad s\,\beta_1 \equiv \beta + v, \quad (\mathrm{mod}\, p = 3).$$

Dunque, in entrambi i casi, disponendo opportunamente di v ed s si può portare la coppia $(\alpha\,\beta)$ o in $(0\,1)$ ovvero in $(0\,0)$.

Quando è γ un multiplo di p ma è α primo con p, io pongo a definizione dell'elemento E_2 la relazione $E_5^p = E_2$. Allora, se u è un intero primo con p, eseguendo l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^u, & E_4, & E_3^u E_1^{\binom{u}{2}}, & E_2^u, & E_1^{u^2} \end{pmatrix},$$

la quale non altera nè la detta relazione nè le formole (8), si ha:

$$u^2\,\delta_1 \equiv \delta, \quad (\mathrm{mod}\, p).$$

Dunque, disponendo convenientemente del numero intero u, si può portare δ in uno dei tre resti ε, 1, 0 relativi a p ed, evidentemente, uno qualunque di questi casi esclude gli altri due.

In conclusione, continuando a supporre $p > 2$, i gruppi $G_5^{2,2}$ definiti dalle relazioni (8) e (10) sono cinque e corrispondono alle seguenti modificazioni delle formole (10).

$E_5^p = E_1$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_2$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_2$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_2$,	$E_4^p = E_1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_2$,	$E_4^p = E_1^\varepsilon$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Se il gruppo definito dalle relazioni (8) e (10) è un $G_5^{2,3}$, i due numeri α, γ sono multipli di p; allora le dette relazioni mostrano che il gruppo $G_5^{2,3}$, così definito, si ottiene aggiungendo in modo ovvio l'elemento E_2 al gruppo $G_4^{2,2}$ generato dagli elementi E_5, E_4, E_3, E_1. Le formole di composizione dei gruppi $G_4^{2,2}$ sono le (16) del § II nel caso di $p > 3$ e le (17) dello stesso paragrafo nel caso di $p = 3$; quindi, riscrivendo le dette formole dopo avere osservato che gli elementi che vi figurano E_4, E_3, E_2 hanno ora, ordinatamente, i nomi E_5, E_4, E_3, ed aggiungendo la relazione $E_2^p = 1$, si ottengono tutte le modificazioni delle (10) che corrispondono a gruppi $G_5^{2,3}$ distinti.

Dunque, nelle attuali ipotesi, se è $p > 3$, si hanno quattro gruppi $G_5^{2,3}$ corrispondenti alle formole:

$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_1^\varepsilon$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

e se è $p = 3$, si hanno pure quattro gruppi $G_5^{2,3}$ corrispondenti alle

formole:

$E_5^3=1,$	$E_4^3=1,$	$E_3^3=1,$	$E_2^3=1,$	$E_1^3=1$
$E_5^3=1,$	$E_4^3=E_1,$	$E_3^3=1,$	$E_2^3=1,$	$E_1^3=1$
$E_5^3=1,$	$E_4^3=E_1^2,$	$E_3^3=1,$	$E_2^3=1,$	$E_1^3=1$
$E_5^3=E_1,$	$E_4^3=E_1^2,$	$E_3^3=1,$	$E_2^3=1,$	$E_1^3=1$

38. Mi rimane a considerare il caso di $p=2$ che ho escluso al principio del n.° 36.

Giacchè un gruppo G_5^2 non può avere che un solo divisore Abeliano d'indice p, risulta che, nella presente ipotesi di $p=2$, il quadrato dell'elemento E_5 che figura nelle relazioni (8) deve appartenere necessariamente al gruppo H. Intanto le dette relazioni dànno:

$$E_5^{-2}E_4E_5^2=E_4E_3^2E_1,$$

e perciò deve essere $E_3^2=E_1$. Allora la prima delle (8) mostra che la potenza E_4^2 è fuori di H e quindi essa coincide con uno dei quattro elementi:

$$E_3,\quad E_3E_2,\quad E_3E_1,\quad E_3E_2E_1.$$

Io suppongo che si avveri il primo od il secondo caso, perchè, se fosse altrimenti, assumerei come elemento E_4 l'elemento E_4E_3 e quindi come elemento E_3 l'elemento E_3E_1.

Ciò posto, si dimostra col solito procedimento che, aggiungendo alle (8) le relazioni:

$$E_5^2=E_2^\alpha E_1^\beta,\quad E_4^2=E_3,\quad E_3^2=E_1,\quad E_2^2=E_1^h,\quad E_1^2=1, \tag{11}$$

oppure le relazioni:

$$E_5^2=E_2^\alpha E_1^\beta,\quad E_4^2=E_3E_2,\quad E_3^2=E_1,\quad E_2^2=E_1^h,\quad E_1^2=1, \tag{12}$$

si definisce in ogni caso un gruppo G_5^2 di grado 32.

Essendo, in virtù delle (8),

$$(E_5E_4)^2=E_5^2E_4^2E_3,$$

si vede che, chiamando E_5 l'elemento E_5E_4, se hanno luogo le (11), gl'interi α e β si cambiano rispettivamente in α e $\beta+1$, e, se hanno luogo le (12), i detti interi si cambiano rispettivamente in $\alpha+1$ e $\beta+1$.

Dunque, nelle (11) io posso supporre che sia $E_5^2 = 1$ ovvero $E_5^2 = E_2$, ed è poi facile convincersi che questi due casi non si possono ridurre l'uno nell'altro qualunque sia h.

Nelle (12) posso supporre che sia $E_5^2 = 1$ ovvero $E_5^2 = E_1$, e questi due casi sono tra loro irreduttibili soltanto quando è $h = 0$; ma, se è $h = 1$, i detti casi si possono ridurre l'uno nell'altro chiamando E_5 l'elemento $E_5 E_2$.

In conclusione, nell'attuale ipotesi, si hanno *sette* gruppi G_5^2 di grado 32, i quali sono definiti dalle (8) insieme alle seguenti relazioni:

$E_5^2 = 1$,	$E_4^2 = E_3$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = E_3$,	$E_3^2 = E_1$,	$E_2^2 = E_1$,	$E_1^2 = 1$
$E_5^2 = E_2$,	$E_4^2 = E_3$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_5^2 = E_2$,	$E_4^2 = E_3$,	$E_3^2 = E_1$,	$E_2^2 = E_1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = E_3 E_2$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = E_3 E_2$,	$E_3^2 = E_1$,	$E_2^2 = E_1$,	$E_1^2 = 1$
$E_5^2 = E_1$,	$E_4^2 = E_3 E_2$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$

I due gruppi, che corrispondono alle prime due serie di formole, sono gruppi $G_5^{2,3}$; invece i cinque gruppi corrispondenti alle ultime cinque formole sono gruppi $G_5^{2,2}$.

39. Io riepilogo brevemente i risultati ottenuti nel presente paragrafo.

I gruppi G_5^2, che posseggono un divisore Abeliano d'indice p, si dividono in due categorie, secondo che il gruppo K coincide ovvero non coincide col gruppo H.

Nella prima categoria esistono $p + 8$, e non più, gruppi G_5^2 di grado p^5 con $p > 2$, e soltanto *nove* gruppi G_5^2 di grado 32.

Tutti i gruppi della prima categoria sono gruppi $G_5^{2,3}$.

Nella seconda categoria esistono soltanto *tredici* gruppi G_5^2 di grado p^5 con $p > 2$: di questi tredici gruppi, cinque sono gruppi $G_5^{2,3}$ ed i rimanenti otto sono gruppi $G_5^{2,2}$.

La detta seconda categoria contiene ancora *sette* gruppi G_5^2 di grado 32: di questi gruppi, due sono gruppi $G_5^{2,3}$ ed i rimanenti cinque sono gruppi $G_5^{2,2}$.

Tutti i gruppi che sono stati trovati in questo paragrafo sono rappresentati nelle seguenti tabelle.

I.

$$\{H(E_2, E_1)\}; \quad \{K = H\}.$$

$$E_5^{-1} E_4 E_5 = E_4 E_2, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_4^{-1} E_3 E_4 = E_3.$$

Gruppi $G_5^{2,3}$	E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
	1	$E_2^{\varepsilon m-1}$	$E_1^{\varepsilon m+1}$	1	1	$\left(\frac{D}{p}\right)=+1$
	1	E_2^{-1}	E_1	1	1	
	E_2	1	E_1	1	1	
	1	$E_2 E_1$	$E_2 E_1^{\varepsilon 2m+1}$	1	1	$\left(\frac{D}{p}\right)=-1$
	1	E_1	E_2^{ε}	1	1	
	1	E_2	E_1	1	1	
	1	E_2	$E_2 E_1$	1	1	
	1	1	E_2	1	1	$\left(\frac{D}{p}\right)=0$
	E_1	1	E_2	1	1	
	E_1	1	1	1	1	
	1	1	1	1	1	
	$m = 0, \ldots, \frac{p-3}{2}$ $\{p > 2\}$					

II.

Gruppi G_5^2 di grado 32.

$$\{H(E_2, E_1)\}; \quad \{K = H\}.$$

$$E_5^{-1} E_4 E_5 = E_4 E_2, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_4^{-1} E_3 E_4 = E_3.$$

	E_5^2	E_4^2	E_3^2	E_2^2	E_1^2
Gruppi $G_5^{2,3}$. $\{p = 2\}$.	1	1	E_1	1	1
	E_1	1	E_1	1	1
	1	1	E_2	1	1
	1	E_1	E_2	1	1
	E_1	E_1	E_2	1	1
	1	E_1	$E_2 E_1$	1	1
	1	E_2	E_1	1	1
	E_1	E_2	E_1	1	1
	1	1	1	1	1

$$\{H(E_2, E_1)\}; \quad \{K \neq H\}.$$

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_4^{-1} E_3 E_4 = E_3.$$

	E_5^2	E_4^2	E_3^2	E_2^2	E_1^2
$G_5^{2,3}$	1	E_3	E_1	1	1
	1	E_3	E_1	E_1	1
Gruppi $G_5^{2,2}$	E_2	E_3	E_1	1	1
	E_2	E_3	E_1	E_1	1
	1	$E_3 E_2$	E_1	1	1
	1	$E_3 E_2$	E_1	E_1	1
	E_1	$E_3 E_2$	E_1	1	1

III.

$$\{H(E_2, E_1)\}; \quad \{K = H\}.$$

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_4^{-1} E_3 E_4 = E_3.$$

	E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
Gruppi $G_5^{2,2}$ $\{p > 2\}$	1	1	1	E_1	1	$p \geqq 3$
	E_2	1	1	E_1	1	$p \geqq 3$
	1	E_2	1	E_1	1	$p \geqq 3$
	1	E_2^ε	1	E_1	1	$p \geqq 3$
	E_1	E_2	1	1	1	$p \geqq 3$
	1	E_2	1	1	1	$p \geqq 3$
	E_2	1	1	1	1	$p \geqq 3$
	E_2	E_1	1	1	1	$p \geq 3$
	E_2	E_1^ε	1	1	1	$p \geq 3$
Gruppi $G_5^{2,3}$	1	1	1	1	1	$p \geq 3$
	E_1	1	1	1	1	$p > 3$
	1	E_1	1	1	1	$p \geq 3$
	1	E_1^ε	1	1	1	$p \geq 3$
	E_1	E_1^2	1	1	1	$p = 3$

§ VI. I Gruppi $G_5^{3,2}$.

40. In un gruppo G_5^3 il divisore invertibile H è di grado p ed è quindi contenuto in ogni divisore normale di G_5^3. Nel presente paragrafo mi propongo di trovare tutti i gruppi G_5^3 che hanno due soli divisori indipendenti d'indice p: distinguerò questi gruppi in due categorie, ascrivendo alla prima categoria ogni gruppo $G_5^{3,2}$, che ammette un divisore Abeliano d'indice p, ed alla seconda categoria ogni gruppo $G_5^{3,2}$ che non possiede un tale divisore.

Se:

$$G_5^{3,2}, \quad G_4^0, \quad G_3, \quad G_2, \quad G_1,$$

è una serie canonica di composizione di un gruppo della prima categoria ed:

$$E_5, \quad E_4, \quad E_3, \quad E_2, \quad E_1,$$

è una base relativa alla detta serie si ha:

$$E_5^{-1} E_4 E_5 = E_4 E_3', \quad E_5^{-1} E_3 E_5 = E_3 E_2', \quad E_5^{-1} E_2 E_5 = E_2 E_1',$$
$$E_4^{-1} E_3 E_4 = E_3, \qquad E_4^{-1} E_2 E_4 = E_2, \qquad E_3^{-1} E_2 E_3 = E_2.$$

Qualsiasi elemento di G_4^0 che è invertibile con E_5 appartiene necessariamente ad H: infatti, un tale elemento risulta invertibile con ogni altro elemento di $G_5^{3,2}$.

Ciò posto, l'elemento E_1' che figura nelle formole precedenti è un elemento generatore E_1 del gruppo $G_1 = H$.

L'elemento E_2' è fuori di G_1, perchè, se fosse $E_2' = E_1^\alpha$, l'elemento $E_3 E_2^{-\alpha}$, che è fuori di H, risulterebbe invertibile con E_5. Suppongo dunque $E_2' = E_2$.

L'elemento E_3' è fuori di G_2, perchè, se fosse $E_3' = E_2^\alpha E_1^\beta$, l'elemento $E_4 E_3^{-\alpha} E_2^{-\beta}$, che è fuori di H, risulterebbe invertibile con E_5. Suppongo dunque $E_3' = E_3$.

Io posso ora scrivere le formole definitive:

$$\left.\begin{array}{lll} E_5^{-1} E_1 E_5 = E_4 E_3, & E_5^{-1} E_3 E_5 = E_3 E_2, & E_5^{-1} E_2 E_5 = E_2 E_1, \\ E_4^{-1} E_3 E_4 = E_3, & E_4^{-1} E_2 E_4 = E_2, & E_3^{-1} E_2 E_3 = E_2, \end{array}\right\} \quad (1)$$

le quali mostrano che il gruppo G_3 coincide necessariamente con K; inoltre, il ragionamento che ho fatto per stabilire le (1) prova che ogni gruppo G_5^3, che possiede un divisore Abeliano d'indice p, è certamente un gruppo $G_5^{3,2}$.

È importante osservare che la potenza E_5^p appartiene al gruppo G_3 ed è invertibile con E_5: dunque la detta potenza sta in H.

Dalle relazioni (1) si ricava:

$$E_5^{-n} E_4 E_5^n = E_4 E_3^n E_2^{\binom{n}{2}} E_1^{\binom{n}{3}}, \quad E_5^{-n} E_3 E_5^n = E_3 E_2^n E_1^{\binom{n}{2}};$$

quindi, *supposto* $p > 3$, per l'osservazione precedente deve essere:

$$E_2^p = 1, \quad E_3^p = 1.$$

Allora, siccome è:

$$E_5^{-1} E_4^p E_5 = E_4^p E_3^p,$$

l'elemento E_4^p risulta invertibile con E_5 e perciò sta in H.

Si hanno dunque le formole:

$$E_5^p = E_1^\alpha, \quad E_4^p = E_1^\beta, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1, \tag{2}$$

le quali, insieme alle (1) definiscono un gruppo $G_5^{3,2}$ qualunque siano gl'interi α, β purchè si tenga presente che E_1 appartiene ad H e che è $p > 3$.

Sia ora:

$$\mathbf{E}_5, \quad \mathbf{E}_4, \quad \mathbf{E}_3, \quad \mathbf{E}_2, \quad \mathbf{E}_1,$$

una seconda base canonica di $G_5^{3,2}$ definita come la prima. Ponendo, nel modo più generale,

$$\mathbf{E}_5 \equiv E_5^u E_4^v, \quad \mathbf{E}_4 \equiv E_4^s, \quad (\mathrm{mod}\ G_3),$$

si trova successivamente:

$$\mathbf{E}_3 \equiv E_3^{us} (\mathrm{mod}\ G_2), \quad \mathbf{E}_2 \equiv E_2^{u^2 s} (\mathrm{mod}\ G_1), \quad \mathbf{E}_1 \equiv E_1^{u^3 s},$$

e quindi il prodotto $u\,s$ deve supporsi primo con p.

Dopo ciò, pensando alle (1), dopo un breve calcolo si ha:

$$(E_5 E_4)^n = E_5^n E_4^n E_3^{\binom{n}{2}} E_2^{\binom{n}{3}} E_1^{\binom{n}{4}};$$

dunque, avendo supposto $p > 3$, risulta:

$$(E_5 E_4)^p = E_5^p E_4^p,$$

e quindi:

$$\mathbf{E}_5^p = E_5^{pu} E_4^{pv} = E_1^{\alpha u + \beta v}.$$

Si vede allora immediatamente che l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ \mathbf{E}_5, & \mathbf{E}_4, & \mathbf{E}_3, & \mathbf{E}_2, & \mathbf{E}_1 \end{pmatrix},$$

porta i numeri α e β nei numeri α_1 e β_1 tali che:

$$\left.\begin{aligned} u^3 s\,\alpha_1 &\equiv a\,u + \beta\,v\,, \\ u^3\,\beta_1 &\equiv \beta. \end{aligned}\right\} \pmod p.$$

Qui bisogna distinguere il caso in cui $p-1$ è primo con 3 dal caso in cui $p-1$ è un multiplo di 3. Nel primo caso, se non è β un multiplo di p, si può scegliere u in modo che sia $u^3 \equiv \beta \pmod p$: quindi β_1 si può portare o nel resto *1* oppure nel resto *0* di p; invece, nel secondo caso, il numero β_1 si può portare in uno dei quattro resti 0, 1, ε, ε^2 di p, ed una qualunque di queste quattro ipotesi esclude le altre tre. Inoltre si osservi che tutte le volte che è β primo con p, disponendo convenientemente di v, posso portare α_1 nel resto *0* di p; e se è β un multiplo di p, disponendo convenientemente di s posso portare α_1 in uno dei due resti 1, 0 di p.

In conclusione, se è $p-1$ primo con 3, esistono solamente tre gruppi $G_5^{3,2}$ che hanno ciascuno un divisore Abeliano d'indice p, e questi tre gruppi corrispondono alle seguenti modificazioni delle formole (2):

$E_5^p = 1\,,$	$E_4^p = 1\,,$	$E_3^p = 1\,,$	$E_2^p = 1\,,$	$E_1^p = 1$
$E_5^p = E_1\,,$	$E_4^p = 1\,,$	$E_3^p = 1\,,$	$E_2^p = 1\,,$	$E_1^p = 1$
$E_5^p = 1\,,$	$E_4^p = E_1\,,$	$E_3^p = 1\,,$	$E_2^p = 1\,,$	$E_1^p = 1$

Se poi $p-1$ è un multiplo di 3, oltre ai precedenti tre gruppi, si hanno ancora due nuovi gruppi $G_5^{3,2}$ che corrispondono alle seguenti modificazioni delle (2):

$E_5^p = 1\,,$	$E_4^p = E_1^{\varepsilon}\,,$	$E_3^p = 1\,,$	$E_2^p = 1\,,$	$E_1^p = 1$
$E_5^p = 1\,,$	$E_4^p = E_1^{\varepsilon^2}\,,$	$E_3^p = 1\,,$	$E_2^p = 1\,,$	$E_1^p = 1$

41. Supponendo ora $p = 3$, le (1) danno:

$$E_5^{-3} E_4 E_5^3 = E_4 E_3^3 E_2^3 E_1\,, \quad E_5^{-3} E_3 E_5^3 = E_3 E_2^3;$$

quindi, giacchè E_5^3 sta in H, si ha successivamente:

$$E_2^3 = 1\,, \quad E_3^3 = E_1^3.$$

Allora le formole (1) e la relazione:

$$E_5^{-1} E_4^3 E_5 = E_4^3 E_3^3 = E_4^3 E_1^2,$$

mostrano che l'elemento E_4 deve coincidere con un elemento di G_2 del tipo $E_2^2 E_1^\beta$.

Si hanno dunque le formole:

$$E_5^3 = E_1^\alpha, \quad E_4^3 = E_2^2 E_1^\beta, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1, \tag{3}$$

le quali, insieme alle (1), definiscono sempre un gruppo $G_5^{3,2}$ di grado 243.

Si osservi che l'operazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^2, & E_4, & E_3^2 E_2, & E_2 E_1, & E_1^2 \end{pmatrix},$$

lascia inalterate le (1) e cambia α e β rispettivamente in α e $2\beta + 2$: dunque si può ritenere o $\beta = 0$ oppure $\beta = 1$. Se è $\beta = 0$, osservando che è:

$$(E_5 E_4)^3 = E_5^3 E_4^2 E_3^3 E_2 = E_1^{\alpha+2},$$

si vede che, chiamando E_5 uno dei due elementi $E_5 E_4$, $E_5 E_4^2$, si può supporre $\alpha = 0$. Ma, se è $\beta = 1$, è facile verificare che, cambiando comunque la base canonica, in modo tale però che le (1) si conservino, i numeri α e β restano inalterati: dunque, se è $\beta = 1$, le tre ipotesi $\alpha = 0, 1, 2$ non si possono ridurre una in un'altra.

In conclusione, esistono soltanto quattro gruppi $G_5^{3,2}$ di grado 243 che posseggono ciascuno un divisore Abeliano di grado 81, e questi quattro gruppi sono definiti dalle (1) e dalle seguenti modificazioni delle formole (3):

$E_5^3 = 1$,	$E_4^3 = E_2^2$,	$E_3^3 = E_1^2$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = 1$,	$E_4^3 = E_2^2 E_1$,	$E_3^3 = E_1^2$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = E_1$,	$E_4^3 = E_2^2 E_1$,	$E_3^3 = E_1^2$,	$E_2^3 = 1$,	$E_1^3 = 1$
$E_5^3 = E_1^2$,	$E_4^3 = E_2^2 E_1$,	$E_3^3 = E_1^2$,	$E_2^3 = 1$,	$E_1^3 = 1$

42. Io suppongo finalmente $p = 2$.

Dalle (1) si ricava:

$$E_5^{-2} F_4 E_5^2 = E_4 E_3^2 E_2, \quad E_5^{-2} E_3 E_5^2 = E_3 E_2^2 E_1;$$

quindi, giacchè E_5^2 sta in H, si ha successivamente:

$$E_2^2 = E_1, \quad E_3^2 = E_2^{-1}.$$

Allora le formole (1) e la relazione:

$$E_5^{-1} E_4^2 E_5 = E_4^2 E_3^2 = E_4^2 E_2^{-1},$$

mostrano che l'elemento E_4^2 deve coincidere con un elemento di G_3 del tipo $E_3^{-1} E_1^{\beta}$.

Si hanno dunque le formole:

$$E_5^2 = E_1^{\alpha}, \quad E_4^2 = E_3^{-1} E_1^{\beta}, \quad E_3^2 = E_2^{-1}, \quad E_2^2 = E_1, \quad E_1^2 = 1, \qquad (4)$$

le quali, insieme alle (1) definiscono sempre un gruppo $G_5^{3,2}$ di grado 32.

Ciò posto, si verifica facilmente che, cambiando comunque la base canonica in modo tale però che le (1) si conservino, il numero β resta sempre inalterato ed il numero α o resta inalterato oppure si cambia in $\alpha + \beta$.

Dunque, se è $\beta = 0$, le due ipotesi $\alpha = 0$, 1 non si possono ridurre l'una nell'altra; ma, se è $\beta = 1$, si può sempre supporre $\alpha = 0$.

In conclusione, esistono soltanto tre gruppi $G_5^{3,2}$ di grado 32 che posseggono ciascuno un divisore Abeliano di grado 16, e questi tre gruppi sono definiti dalle formole (1) e dalle seguenti modificazioni delle (4):

$E_5^2 = 1$,	$E_4^2 = E_3^{-1}$,	$E_3^2 = E_2^{-1}$,	$E_2^2 = E_1$,	$E_1^2 = 1$
$E_5^2 = E_1$,	$E_4^2 = E_3^{-1}$,	$E_3^2 = E_2^{-1}$,	$E_2^2 = E_1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = E_3^{-1} E_1$,	$E_3^2 = E_2^{-1}$,	$E_2^2 = E_1$,	$E_1^2 = 1$

Ho già osservato che i gruppi G_5^3, che posseggono un divisore Abeliano d'indice p, sono necessariamente gruppi $G_5^{3,2}$; ma è ancora notevole il fatto che i rimanenti p divisori d'indice p sono gruppi $G_4^{2,2}$: ciò risulta dalle formole di composizione trovate nei tre ultimi numeri.

43. Si abbia ora un gruppo $G_5^{3,2}$ tale che in esso non sia contenuto alcuno divisore Abeliano d'indice p.

Sia G_2 un divisore normale di $G_5^{3,2}$ appartenente al gruppo K ed E_2 un elemento di G_2 fuori di H: ragionando come al n.° 13 del § II, si dimostra che esiste un elemento E_3, fuori di G_2, che è invertibile con E_2; poi, considerando il gruppo Abeliano G_3 generato dall'elemento E_3 e dagli elementi

di G_2, si dimostra ancora che esiste un elemento E_4 fuori di G_3, che è pure invertibile con E_2. Il gruppo G_4 generato dall'elemento E_4 e dagli elementi di G_3 è un G_4^1 che ha come divisore invertibile in gruppo G_2. Questo gruppo G_4^1 deve contenere il gruppo K di $G_5^{3,2}$ ed io pongo $K = G_3$; poi, denotando con E_1 un elemento generatore del gruppo $H = G_1$, considero la serie di composizione:

$$G_5^{3,2}, \quad G_4^1, \quad G_3, \quad G_2, \quad G_1.$$

Dopo ciò, ponendo:

$$E_4^{-1} E_3 E_4 = E_3 E_2'', \quad E_5^{-1} E_2 E_5 = E_2 E_1',$$

l'elemento E_2'' non è l'elemento identico perchè il gruppo G_4^1 non è Abeliano; inoltre, giacchè E_3^p sta in G_2, risulta $E''^p_2 = 1$. Ora, il gruppo ciclico generato dalle potenze di E_2'' è l'unico della sua specie contenuto in G_4^1, e siccome G_4^1 è divisore normale di $G_5^{3,2}$, il detto gruppo è anche divisore normale di $G_5^{3,2}$ e coincide quindi con G_1: si può dunque ritenere $E_2'' = E_1$.

Similmente, E_1' non è l'elemento identico altrimenti l'elemento E_2, che è fuori di H, risulterebbe permutabile anche con E_5 e quindi con ogni elemento di $G_5^{3,2}$: dunque si ha $E_1' = E_1^h$ essendo l'intero h primo con p.

Si hanno perciò le formole:

$$\left.\begin{array}{lll} E_5^{-1} E_4 E_5 = E_4 E_3', & E_5^{-1} E_3 E_5 = E_3 E_2', & E_5^{-1} E_2 E_5 = E_2 E_1^h, \\ E_4^{-1} E_3 E_4 = E_3 E_1, & E_4^{-2} E_2 E_4 = E_2, & E_3^{-1} E_2 E_3 = E_2, \end{array}\right\} \quad (5)$$

Io comincio coll'osservare che il gruppo K non può essere ciclico.

Infatti, giacchè il gruppo $G_5^{3,2}$ non contiene per ipotesi alcun divisore Abeliano d'indice p, la potenza E_5^p non è di grado superiore a p^2 e quindi sta in G_2. Allora l'elemento E_3' che figura nelle (5) non sta in G_2 perchè, in tale caso, i quattro elementi E_5, E_4, E_2, E_1 generano un gruppo di grado p^4 e questo gruppo non conterrebbe K. Ponendo dunque:

$$E_3' = E_3, \quad E_3^p = E_2,$$

dalle (5) risulta:

$$E_5^{-1} E_4^p E_5 = E_4^p E_3^p E_1^{\binom{p}{2}} = E_4^p E_2 E_1^{\binom{p}{2}};$$

ciò è assurdo giacchè, dovendo la potenza E_4^p appartenere a G_2, si ha:

$$E_5^{-1} E_4^p E_5 \equiv E_4^p, \pmod{G_1}.$$

44. Si ammetta, in prima ipotesi, che il gruppo Abeliano K abbia tutti i suoi elementi di grado p; in altri termini, che sia G_3 un gruppo $G_3^{0,3}$.

Supponendo allora $p > 3$, dalle (5) risulta:

$$E_5^{-p} E_4 E_5^p = E_4, \quad E_5^{-p} E_3 E_5^p = E_3, \quad E_5^{-p} E_2 E_5^p = E_2,$$
$$E_5^{-1} E_4^p E_5 = E_4^p, \quad E_4^{-p} E_3 E_4^p = E_3, \quad E_4^{-p} E_2 E_4^p = E_2;$$

quindi gli elementi E_5^p, E_4^p, i quali riescono invertibili con qualsiasi elemento di $G_5^{3,2}$, appartengono ad H.

Ciò posto, se E_3' potesse appartenere a G_2, i quattro elementi E_5, E_4, E_2, E_1 genererebbero un gruppo di grado p^4 il quale non conterrebbe K: dunque, si può porre $E_3' = E_3$. Similmente, se E_2' potesse appartenere a G_1, i quattro elementi E_5, E_4, E_3, E_1 genererebbero un gruppo di grado p^4 il quale non conterrebbe K: dunque si può porre $E_2' = E_2$.

Dopo quello che si è detto, si possono scrivere le formole:

$$\left.\begin{aligned} &E_5^{-1} E_4 E_5 = E_1 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_2, \quad E_5^{-1} E_2 E_5 = E_2 E_1^h, \\ &E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \qquad E_3^{-1} E_2 E_3 = E_2. \end{aligned}\right\} \quad (6)$$

$$E_5^p = E_1^\alpha, \quad E_4^p = E_1^\beta, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1. \quad (7)$$

Col solito ragionamento si prova che queste formole definiscono sempre un gruppo $G_5^{3,2}$, purchè si pensi che E_1 appartiene ad H e che è $p > 3$.

Inoltre si osservi che si può ritenere $h = 1$, perchè, se fosse altrimenti, eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5, & E_4^h, & E_3^h E_1^{\binom{h}{2}}, & E_2^h, & E_1^{h^2} \end{pmatrix},$$

la quale non altera la forma delle (6) e (7), si porta subito il numero h nel resto 1 di p.

Se:

$$\mathbf{E}_5, \quad \mathbf{E}_4, \quad \mathbf{E}_3, \quad \mathbf{E}_2, \quad \mathbf{E}_1,$$

è una seconda base canonica definita come la prima, si vede immediatamente sulle formole (6) e (7) che le trasformazioni definite dalle congruenze:

$$\mathbf{E}_5 \equiv E_5, \quad \mathbf{E}_4 \equiv E_4, \pmod{G_3},$$

non alterano gl'interi α, β, h; dunque io posso considerare come un'unica trasformazione tutte quelle definite da:

$$\mathbf{E}_5 \equiv E_5^u E_4^v, \quad \mathbf{E}_4 \equiv E_4^s, \pmod{G_3},$$

per dati valori degli interi u, v, s, i quali d'altronde debbono essere tali che il prodotto us risulti primo con p.

Gli elementi $\mathbf{E}_3$, $\mathbf{E}_2$, $\mathbf{E}_1$, che bisogna associare agli elementi $\mathbf{E}_5$, $\mathbf{E}_4$ ultimamente definiti, sono tali che:

$$\mathbf{E}_3 \equiv E_3^{us} \pmod{G_2}, \quad \mathbf{E}_2 \equiv E_2^{u^2 s} \pmod{G_1}, \quad \mathbf{E}_1 = E_1^{us^2};$$

quindi, dopo avere osservato che è:

$$(E_5 E_4)^n = E_5^n E_4^n E_3^{\binom{n}{2}} E_2^{\binom{n}{3}} E_1^{\binom{n}{4}},$$

e perciò, avendo supposto $p > 3$, che è:

$$(E_5 E_4)^p = E_5^p E_4^p,$$

si vede facilmente che la detta trasformazione fa subire agli interi α, β, h la sostituzione congrua:

$$s^2 u \alpha_1 \equiv \alpha u + \beta v, \quad s u \beta_1 \equiv \beta, \quad s h_1 \equiv u^2 h, \pmod{p}.$$

Avendo supposto $h = 1$, se si vuole che sia ancora $h_1 = 1$, bisogna prendere $s \equiv u^2 \pmod{p}$ e quindi si ha:

$$u^5 \alpha_1 \equiv u \alpha + v \beta, \quad u^3 \beta_1 \equiv \beta, \pmod{p}.$$

Osservo anzitutto che ogni volta che non è β un multiplo di p, si può determinare il numero v in modo che sia $\alpha_1 \equiv 0 \pmod{p}$.

Ciò posto, io distinguo i seguenti quattro casi possibili:

$$p \equiv -1, \quad p \equiv -5, \quad p \equiv 5, \quad p \equiv 1, \pmod{12}.$$

Nel primo caso, il numero $p - 1$ non è divisibile nè per 3 nè per 4 e quindi ogni numero è cubo $(\mathrm{mod}\, p)$ ed ogni numero quadrato $(\mathrm{mod}\, p)$ è un biquadrato $(\mathrm{mod}\, p)$.

Dunque, se β non è multiplo di p, si può determinare u in modo che β_1 sia il resto 1 di p: se invece è β un multiplo di p, tutte le volte che non è α un multiplo di p, si può determinare u in modo che sia o $\alpha_1 \equiv 1 \pmod{p}$ ovvero $\alpha_1 \equiv \varepsilon \pmod{p}$, secondo che α è della forma u^4 ovvero della forma εu^4 rispetto a $\mathrm{mod}\, p$.

Ottengo quindi quattro gruppi $G_5^{3,2}$, che corrispondono alle seguenti modificazioni delle (7):

$E_5^p = 1$,	$E_4^p = E_1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1^\varepsilon$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Nel secondo caso, $p-1$ è divisibile per *3* ma non per *4*, quindi ogni numero ha, rispetto a mod p, una delle forme:

$$u^3, \quad \varepsilon u^3, \quad \varepsilon^2 u^3;$$

allora, se β è della prima forma, si hanno i quattro gruppi trovati precedentemente, ma se β è della seconda o della terza forma, si hanno due nuovi gruppi $G_5^{3,2}$, i quali corrispondono alle seguenti modificazioni delle (7):

$E_5^p = 1$,	$E_4^p = E_1^\varepsilon$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = 1$,	$E_4^p = E_1^{\varepsilon^2}$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Nel terzo caso, $p-1$ è divisibile per *4* ma non per *3*, quindi ogni numero ha, rispetto a mod p, una delle forme:

$$u^4, \quad \varepsilon u^4, \quad \varepsilon^2 u^4, \quad \varepsilon^3 u^4.$$

I due ultimi gruppi trovati sono ora isomorfi al primo dei quattro gruppi che si riferiscono al primo caso; ma, oltre a questi, si hanno ancora due nuovi gruppi i quali si presentano quando è β un multiplo di p e che corrispondono alle seguenti modificazioni delle formole (7):

$E_5^p = E_1^{\varepsilon^2}$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_1^{\varepsilon^3}$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

Se si fosse nel secondo caso, questi due gruppi sarebbero isomorfi rispettivamente ai due ultimi gruppi che si riferiscono al primo caso.

Finalmente, nel quarto caso, $p-1$ è divisibile per *3* e per *4* e quindi gli *otto* gruppi scritti nei tre casi precedenti sono effettivamente distinti e sono tutti i possibili gruppi $G_5^{3,2}$ che rientrano nell'attuale caso.

45. Nell'ultimo numero ho supposto che il gruppo $G_5^{3,2}$ non abbia alcun divisore Abeliano d'indice p e che il gruppo K, intersezione dei $p+1$ divisori d'indice p di $G_5^{3,2}$ abbia tutti i suoi elementi di grado p.

In queste ipotesi, io posso dimostrare che non esistono gruppi $G_5^{3,2}$ di grado 243. Infatti, se è $p=3$, riferendomi alle formole (5), concludo come prima $E_3'=E_3$, $E_2'=E_2$, e quindi dovrebbero sussistere le formole (6). Allora da queste si ricava:

$$E_5^{-3} E_4 E_5^3 = E_4 E_3^3 E_2^3 E_1^h = E_4 E_1^h ;$$

perciò l'elemento E_5^3 è un elemento di K del tipo $E_3^{-h} E_2^\alpha E_1^\beta$. Questo elemento, essendo una potenza di E_5, dovrebbe essere invertibile con E_5 e ciò contraddice alle stesse formole (6).

Invece, se è $p=2$, esiste un gruppo di grado 32 ed uno solo, che soddisfa a tutte le attuali ipotesi. Allora l'elemento E_3' non può appartenere a G_1, perchè, se così fosse, il quadrato E_5^2, che appartiene a G_3, risulterebbe permutabile con E_4 e quindi dovrebbe essere contenuto in G_2, anzi in G_1, perchè il detto quadrato è invertibile con E_5: ciò non può essere a meno che non sia E_2' un elemento di G_1; ma, in tale caso, il gruppo definito dalle (5) e (7) sarebbe evidentemente un gruppo $G_5^{3,4}$.

Si ammetta dunque in primo luogo $E_3'=E_2$. Allora l'elemento E_5^2 non è invertibile con E_4 e quindi il detto elemento appartiene a G_3 ma non a G_2: dunque posso ritenere $E_5^2=E_3$ e conseguentemente $E_2'=1$. Inoltre, l'elemento E_4^2 risulta invertibile con E_5 e perciò sta in G_1; anzi io ritengo addirittura $E_4^2=1$, perchè, se fosse altrimenti, chiamerei E_4 l'elemento $E_4 E_3$.

Dopo ciò posso scrivere le formole:

$$E_5^{-1} E_4 E_5 = E_4 E_2 , \quad E_5^{-1} E_3 E_5 = E_3 , \quad E_5^{-1} E_2 E_5 = E_2 E_1 ,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1 , \quad E_4^{-1} E_2 E_4 = E_2 , \quad E_3^{-1} E_2 E_3 = E_2 ,$$
$$E_5^2 = E_3 , \quad E_4^2 = 1 , \quad E_3^2 = 1 , \quad E_2^2 = 1 , \quad E_1^2 = 1 ,$$

le quali definiscono effettivamente un gruppo $G_5^{3,2}$ di grado 32.

Questo gruppo ha tre divisori di grado 16, ciascuno dei quali è generato da uno dei tre elementi:

$$E_4 , \quad E_5 , \quad E_5 E_4 ,$$

e dagli elementi di $G_3=K$.

Mi resta ad esaminare il caso di $E_3' = E_3$: anche a questo caso corrisponde un gruppo di grado 32, che soddisfa alle attuali ipotesi; ma questo gruppo, è isomorfo al precedente e si ottiene scambiando nelle ultime formole E_5 con E_4 e, nello stesso tempo, E_3 con E_2.

È bene osservare che gli otto gruppi trovati nel numero precedente hanno un solo divisore G_4^1 e tutti gli altri p divisori d'indice p sono gruppi G_4^2; mentre, per l'unico gruppo di grado 32 ora trovato, accade che tutti i suoi divisori d'indice 2 sono gruppi G_4^1.

46. Si ammetta, in seconda ipotesi, che il gruppo K sia un $G_3^{0,2}$.

Allora il gruppo K possiede un solo divisore d'indice p tale che tutti i suoi elementi sono di grado p. Questo divisore è dunque normale in $G_5^{3,2}$ e si può assumere come gruppo G_2.

Se E_2 è un elemento di G_2 fuori di G_1, io mi costruisco come al n.° 43 il gruppo G_4^1 costituito da tutti gli elementi di $G_5^{3,2}$ che sono permutabili con E_2 e poi considero la serie canonica:

$$G_5^{3,2}, \quad G_4^1, \quad G_3^{0,2}, \quad G_2, \quad G_1,$$

ed una base:

$$E_5, \quad E_4, \quad E_3, \quad E_2, \quad E_1,$$

relativa alla detta serie.

Dopo ciò, ragionando come nel n.° 44, concludo che, se è $p > 2$, l'elemento E_3' che figura nelle (5) non può appartenere a G_2 e quindi posso porre $E_3' = E_3$.

L'elemento E_3 è nelle presenti ipotesi di grado p^2 e perciò la relazione:

$$E_5^{-1} E_4^p E_5 = E_4^p E_3^p,$$

mostra che la potenza E_4^p non è invertibile con E_5: dunque questa potenza è un elemento di G_2 fuori di G_1 e posso allora ritenere $E_4^p = E_2$. In tale caso la detta relazione si scrive:

$$E_5^{-1} E_2 E_5 = E_2 E_3^p,$$

e quindi deve necessariamente essere $E_3^p = E_1^h$.

Supponendo ora $p > 3$, le formole (5) mostrano che la potenza E_5^p non è invertibile con E_4 e quindi la detta potenza sta in G_3 ma non in G_2. Dunque il gruppo G_3 contiene elementi fuori di G_2 che sono invertibili con E_5 e per questo è necessario che l'elemento E_2' che figura nelle formole (5) appartenga a G_1.

Le considerazioni precedenti portano alle formole:

$$\left.\begin{array}{lll} E_5^{-1} E_4 E_5 = E_4 E_3\,, & E_5^{-1} E_3 E_5 = E_3 E_1^k\,, & E_5^{-1} E_2 E_5 = E_2 E_1^h\,, \\ E_4^{-1} E_3 E_4 = E_3 E_1\,, & E_4^{-1} E_2 E_4 = E_2\,, & E_3^{-1} E_2 E_3 = E_2\,, \end{array}\right\} \quad (8)$$

$$E_5^p = E_3^\alpha E_2^\beta E_1^\gamma\,, \quad E_4^p = E_2\,, \quad E_3^p = E_1^h\,, \quad E_2^p = 1\,, \quad E_1^p = 1\,, \quad (9)$$

le quali, come subito dimostrerò, non possono definire un gruppo $G_5^{3,2}$ se non quando è:

$$\alpha + h \equiv 0\,, \quad \beta \equiv k\,, \pmod p. \quad (10)$$

Infatti, trasformando la prima delle relazioni (9) mediante l'elemento E_4, si ha:

$$E_4^{-1} E_5^p E_4 = E_3^\alpha E_1^\alpha \cdot E_2^\beta E_1^\gamma = E_5^p E_1^\alpha\,,$$

donde si ricava:

$$E_5^{-p} E_4 E_5^p = E_4 E_1^{-\alpha}.$$

Ma dalla prima delle (8) e dalle altre si ha:

$$E_5^{-p} E_4 E_5^p = E_4 E_3^p = E_4 E_1^h;$$

dunque:

$$\alpha + h \equiv 0\,, \pmod p.$$

Inoltre, l'elemento E_5^p è invertibile con E_5 e quindi:

$$E_5^p = E_5^{-1} E_3^\alpha E_2^\beta E_1^\gamma E_5 = E_5^p E_1^{\alpha k} E_1^{\beta h}\,,$$

sicchè:

$$\alpha k + \beta h \equiv 0\,, \pmod p;$$

poi, da questa congruenza e dalla precedente segue:

$$\beta - k \equiv 0\,, \pmod p.$$

Ciò posto, eseguendo la trasformazione:

$$\begin{pmatrix} E_5\,, & E_4\,, & E_3\,, & E_2\,, & E_1 \\ E_5\,, & E_4^h\,, & E_3^h E_1^{\binom{h}{2}k}\,, & E_2^h\,, & E_1^{h^2} \end{pmatrix},$$

l'intero h nel resto 1 di p; ed eseguendo la trasformazione:

$$\begin{pmatrix} E_5\,, & E_4\,, & E_3\,, & E_2\,, & E_1 \\ E_5 E_4\,, & E_4\,, & E_3 E_1\,, & E_2\,, & E_1 \end{pmatrix},$$

i numeri k e β si cambiano in $k+1$ e $\beta+1$. Finalmente, eseguendo la tras-

formazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5 E_3, & E_4, & E_3 E_1^{-1}, & E_2, & E_1 \end{pmatrix},$$

si cambia soltanto γ in $\gamma + h$.

Supponendo dunque $h \equiv 1$, $k \equiv 0$, $\gamma \equiv 0 \pmod p$, le (10) dànno $\alpha \equiv -1$, $\beta \equiv 0 \pmod p$, e quindi non può, nella presente ipotesi, esistere che un solo gruppo $G_5^{3,2}$ corrispondente alle formole:

$$\left.\begin{aligned} &E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1, \\ &E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2, \\ &E_5^p = E_1^{-1}, \quad E_4^p = E_2, \quad E_3^p = E_1, \quad E_2^p = 1, \quad E_1^p = 1. \end{aligned}\right\} \quad (11)$$

D'altra parte è facile verificare che queste formole, se è $p > 3$, definiscono effettivamente un gruppo $G_5^{3,2}$ tale che il relativo gruppo K è un $G_3^{0,2}$.

I $p + 1$ divisori d'indice p del gruppo ora trovato sono gruppi G_4^1: uno solo di essi ha come divisore invertibile il gruppo G_2 e gli altri hanno il divisore invertibile ciclico.

47. *Caso di* $p = 3$.

Riferendomi sempre alle formole (5) si conclude, come nel numero precedente, $E_3' = E_3$, $E_4^3 = E_2$; poi, ammettendo l'ipotesi che E_2' appartenga a G_1, con un ragionamento identico a quello fatto nel detto numero, si trova un gruppo $G_5^{3,2}$ di grado 243, che è definito dalle formole (11) quando vi si suppone $p = 3$.

Ma oltre a questo gruppo, ne esiste un altro di grado 243, che si presenta quando si fa l'ipotesi che l'elemento E_2' non appartenga a G_1. In tale ipotesi io definisco l'elemento E_2 mediante la relazione:

$$E_5^{-1} E_3 E_5 = E_3 E_2,$$

ed osservo che allora il gruppo G_3 non contiene alcun elemento permutabile con E_5, fatta eccezione degli elementi di G_1: dunque la potenza E_5^3 appartiene a G_1.

Ciò posto, la relazione:

$$E_5^{-3} E_4 E_5^3 = E_4 E_3^3 E_2^3 E_1^h,$$

dà $E_3^3 = E_1^{2h}$; poi la relazione:

$$E_5^{-1} E_4^3 E_5 = E_4^3 E_3^3 = E_4^3 E_1^{2h},$$

mostra che la potenza E_4^p è un elemento di G_2 del tipo $E_2^2 E_1^f$.

Dietro le considerazioni che precedono hanno luogo le formole:

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_2, \quad E_5^{-1} E_2 E_5 = E_2 E_1^h,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2,$$
$$E_5^3 = E_1^\alpha, \quad E_4^3 = E_2^2 E_1^\beta, \quad E_3^3 = E_1^{2h}, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

Eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5, & E_4^2, & E_3^2 E_1, & E_2^2, & E_1 \end{pmatrix},$$

il numero h si cambia in $2h$ e quindi posso ritenere che sia $h = 1$.

Allora, chiamando E_5, E_4 rispettivamente gli elementi $E_5 E_3$, $E_4 E_3$, gl'interi α e β si possono fare aumentare, ciascuno in modo indipendente, di una unità.

Dunque, giacchè si può supporre $\alpha \equiv \beta \equiv 0 \pmod 3$, si ha soltanto un nuovo gruppo $G_5^{3,2}$ di grado 243, che si può ritenere definito dalle ultime formole quando ivi si fa $h = 1$, $\alpha = \beta = 0$.

48. *Caso di* $p = 2$.

Ragionando come nel n.° 45, si conclude che l'elemento E_3' che figura nelle formole (5) non può appartenere a G_1.

Se si ammette in primo luogo $E_3' = E_2$, il quadrato E_5^2 non risulta invertibile con E_4 e quindi esso è un elemento di G_3 fuori di G_2: posso perciò supporre $E_5^2 = E_3$ e conseguentemente $E_2' = 1$.

L'elemento E_4^2 risulta invertibile con E_5 e perciò sta in H; inoltre l'elemento E_3^2, che è pure invertibile con E_5, sta in H e, siccome E_3 è di grado 4 per ipotesi, risulta $E_3^2 = E_1$.

Dunque, supponendo $E_3' = E_2$, si hanno soltanto due possibili gruppi $G_5^{3,2}$ di grado 32 definiti dalle seguenti modificazioni delle (5):

$$E_5^{-1} E_4 E_5 = E_4 E_2, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2,$$

e dalle formole:

$$\begin{array}{|c|} \hline E_5^2 = E_3, \quad E_4^2 = E_1, \quad E_3^2 = E_1, \quad E_2^2 = 1, \quad E_1^2 = 1 \\ \hline E_5^2 = E_3, \quad E_4^2 = 1, \quad E_3^2 = E_1, \quad E_2^2 = 1, \quad E_1^2 = 1 \\ \hline \end{array} \tag{12}$$

Si può subito verificare che questi due gruppi realmente esistono e non sono isomorfi, perchè i corrispondenti gruppi G_4^1, i quali si sono presentati nel n.° 12 del § II, non sono isomorfi.

Nelle attuali ipotesi, non accade il fatto notato al n.° 45 cioè, non esiste un isomorfismo che porti l'elemento E_2 nell'elemento E_3; quindi io debbo continuare la mia analisi supponendo in secondo luogo $E_3' = E_3$.

Si osservi che gli elementi di grado 4 contenuti in G_3 hanno tutti lo stesso quadrato e quindi E_3^2 è invertibile con E_5 e con ogni elemento del gruppo principale: dunque deve essere E_2' un elemento di H ed $E_3^2 = E_1$.

Io posso ritenere $E_2' = 1$ giacchè, se fosse altrimenti, chiamerei E_5 l'elemento $E_5 E_4$; allora le (5) forniscono le relazioni:

$$E_5^{-1} E_4^2 E_5 = E_4^2 E_3^2 E_4, \quad E_5^{-2} E_4 E_5^2 = E_4 E_3^2,$$

le quali mostrano che l'elemento E_4^2 è invertibile con E_5 e perciò esso appartiene ad H, e che l'elemento E_5^2 non è invertibile con E_4 e perciò esso è un elemento di G_3 fuori di G_2.

Ponendo quindi:

$$E_5^2 = E_3 E_2^\beta E_1^\gamma,$$

giacchè E_5^2 è permutabile con E_5, deve essere $\beta \equiv 0 \pmod 2$ e si può ritenere anche $\gamma \equiv 0 \pmod 2$ perchè, in caso contrario, si chiamerebbe E_5 l'elemento $E_5 E_3$.

Dunque, quando è $E_3' = E_3$, si hanno soltanto due possibili gruppi G_5^{32} di grado 32 definiti dalle seguenti modificazioni delle (5):

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2,$$

e dalle formole (12).

In conclusione, esistono quattro, e non più, gruppi $G_5^{3,2}$ di grado 32 tali che i corrispondenti gruppi K sono gruppi $G_3^{0,2}$.

49. Io riassumo brevemente i risultati ottenuti nel presente paragrafo.

Esistono soltanto *otto* gruppi $G_5^{3,2}$ di grado 32 e soltanto *sei* gruppi G_5^{32} di grado 243.

Se poi è $p > 3$ bisogna distinguere i seguenti quattro casi:

$$p \equiv -1, \quad p \equiv 5, \quad p \equiv -5, \quad p \equiv 1, \pmod{12}.$$

Quando il numero primo p soddisfa alla prima congruenza, esistono solamente *otto* gruppi $G_5^{3,2}$, quando p soddisfa alla seconda congruenza esistono

solamente *dieci* gruppi $G_5^{3,2}$, quando p soddisfa alla terza congruenza esistono solamente *dodici* gruppi $G_5^{3,2}$; finalmente, quando il numero primo p soddisfa alla quarta congruenza esistono soltanto *quattordici* gruppi $G_5^{3,2}$.

Tutti i detti gruppi sono rappresentati nelle tre tabelle che seguono.

I.

Gruppi $G_5^{3,2}$ *di grado* 32.

$E_5^{-1}E_4E_5 = E_4E_3$, $E_5^{-1}E_3E_5 = E_3E_2$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_3$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.
$E_5^2 = 1$, $E_4^2 = E_3^{-1}$, $E_3^2 = E_2^{-1}$, $E_2^2 = E_1$, $E_1^2 = 1$.
$E_5^2 = E_1$, $E_4^2 = E_3^{-1}$, $E_3^2 = E_2^{-1}$, $E_2^2 = E_1$, $E_1^2 = 1$.
$E_5^2 = 1$, $E_4^2 = E_3^{-1}E_1$, $E_3^2 = E_2^{-1}$, $E_2^2 = E_1$, $E_1^2 = 1$.

$E_5^{-1}E_4E_5 = E_4E_2$, $E_5^{-1}E_3E_5 = E_3$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_3E_1$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.
$E_5^2 = E_3$, $E_4^2 = 1$, $E_3^2 = 1$, $E_2^2 = 1$, $E_1^2 = 1$.
$E_5^2 = E_3$, $E_4^2 = E_1$, $E_3^2 = E_1$, $E_2^2 = 1$, $E_1^2 = 1$.
$E_5^2 = E_3$, $E_4^2 = 1$, $E_3^2 = E_1$, $E_2^2 = 1$, $E_1^2 = 1$.

$E_5^{-1}E_4E_5 = E_4E_3$, $E_5^{-1}E_3E_5 = E_3$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_4E_1$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.
$E_5^2 = E_3$, $E_4^2 = E_1$, $E_3^2 = E_1$, $E_2^2 = 1$, $E_1^2 = 1$.
$E_5^2 = E_3$, $E_4^2 = 1$, $E_3^2 = E_1$, $E_2^2 = 1$, $E_1^2 = 1$.

II.

Gruppi $G_5^{3,2}$ *di grado* 243.

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_2, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2.$$

$$E_5^3 = 1, \quad E_4^3 = E_2^2, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

$$E_5^3 = 1, \quad E_4^3 = E_2^2 E_1, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

$$E_5^3 = E_1, \quad E_4^3 = E_2^2 E_1, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

$$E_5^3 = E_1^2, \quad E_4^3 = E_2^2 E_1, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2.$$

$$E_5^3 = E_1^1, \quad E_4^3 = E_2, \quad E_3^3 = E_1, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

$$E_5^{-1} E_4 E_5 = E_4 E_3, \quad E_5^{-1} E_3 E_5 = E_3 E_1, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2.$$

$$E_5^3 = 1, \quad E_4^3 = E_2^2, \quad E_3^3 = E_1^2, \quad E_2^3 = 1, \quad E_1^3 = 1.$$

III.

$E_5^{-1}E_4E_5 = E_4E_3$, $E_5^{-1}E_3E_5 = E_3E_2$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_3$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.	$G_5^{3.2}$	
$E_5^p = 1$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.	$p > 3$	
$E_5^p = E_1$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = 1$, $E_4^p = E_1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = 1$, $E_4^p = E_1^\varepsilon$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.	$p = 1 + 3m$	
$E_5^p = 1$, $E_4^p = E_1^{\varepsilon^2}$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		

$E_5^{-1}E_4E_5 = E_4E_3$, $E_5^{-1}E_3E_5 = E_3E_2$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_3E_1$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.	$G_5^{3.2}$	
$E_5^p = 1$, $E_4^p = E_1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.	$p > 3$	
$E_5^p = 1$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = E_1$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = E_1^\varepsilon$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = E_1^{\varepsilon^2}$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_4^p = 1$.	$p = 1 + 4m$	
$E_5^p = E_1^{\varepsilon^3}$, $E_4^p = 1$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		
$E_5^p = 1$, $E_4^p = E_1^\varepsilon$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.	$p = 1 + 3m$	
$E_5^p = 1$, $E_4^p = E_1^{\varepsilon^2}$, $E_3^p = 1$, $E_2^p = 1$, $E_1^p = 1$.		

$E_5^{-1}E_4E_5 = E_4E_3$, $E_5^{-1}E_3E_5 = E_3$, $E_5^{-1}E_2E_5 = E_2E_1$, $E_4^{-1}E_3E_4 = E_3E_1$, $E_4^{-1}E_2E_4 = E_2$, $E_3^{-1}E_2E_3 = E_2$.	$G_5^{3.2}$	
$E_5^p = E_1^{-1}$, $E_4^p = E_2$, $E_3^p = E_1$, $E_2^p = 1$, $E_1^p = 1$.	$p > 3$	

§ VII. I Gruppi $G_5^{3,3}$ e $G_5^{3\,4}$.

50. Il gruppo K intersezione di tutti i divisori d'indice p di un gruppo $G_5^{3,3}$ è di grado p^2. Sia E_1 un elemento generatore del divisore invertibile H di $G_5^{3,3}$ ed E_2 un elemento di K fuori di H; indi si consideri il gruppo G_4^1 costituito da tutti gli elementi di $G_5^{3,3}$ che sono permutabili con E_2.

Denotando con E_5 un elemento di $G_5^{3,2}$ fuori di G_4^1, per definizione, non è E_5 permutabile con E_2; però, io voglio dimostrare che esistono elementi di G_4^1, fuori di K, che sono permutabili con E_5.

Siano E_4 ed E_3 due elementi di G_4^1 tali che E_4 non appartenga al gruppo di grado p^3 generato dall'elemento E_3 e dagli elementi di K. Ponendo:

$$E_5^{-1} E_4 E_5 = E_4 E_2^{\alpha} E_1^{\beta}, \quad E_5^{-1} E_3 E_5 = E_3 E_2^{\gamma} E_1^{\delta},$$

uno almeno degli interi α, γ deve essere primo con p. Infatti, se α e γ sono due multipli di p, i tre elementi E_5^p, E_4^p, E_3^p risultano permutabili con ogni elemento di $G_5^{3,3}$ e quindi debbono appartenere ad H; inoltre, per la ragione detta al n.° 43 si può sempre ritenere:

$$E_4^{-1} E_3 E_4 = E_3 E_1^h,$$

essendo h primo con p: quindi gli elementi E_5, E_4, E_3, E_1 generano un gruppo di grado p^4 e questo gruppo, giacchè non contiene l'elemento E_2, non contiene K.

Ciò posto, l'elemento $E_4^{\gamma} E_3^{-\alpha}$ è fuori di K e si ha:

$$E_5^{-1} (E_4^{\gamma} E_3^{-\alpha}) E_5 = (E_4^{-\gamma} E_3^{\alpha}) E_1^{\alpha\delta-\beta\gamma}.$$

Ora, giacchè E_5 non è invertibile con E_2, ponendo:

$$E_5^{-1} E_2 E_5 = E_2 E_1,$$

risulta subito che l'elemento:

$$E_4^{-\gamma} E_3^{\alpha} E_2^{-(\alpha\delta-\beta\gamma)},$$

il quale non appartiene a K, è permutabile con E_5.

Io assumo un tale elemento come elemento E_3 e, scelto poi E_4 fuori del gruppo G_3 generato da E_3 e dagli elementi di K, definisco l'elemento E_2 mediante la relezione:

$$E_5^{-1} E_4 E_5 = E_4 E_2;$$

inoltre, posso ritenere che sia:

$$E_4^{-1} E_3 E_4 = E_3 E_1 ,$$

perchè, in caso contrario, chiamerei E_3 una conveniente potenza di E_3.

Ciò posto, gli elementi:

$$E_5 , \quad E_4 , \quad E_3 , \quad E_2 , \quad E_1 ,$$

definiti nella detta maniera costituiscono una base canonica di un gruppo $G_5^{3,3}$ e soddisfano alle relazioni:

$$\left.\begin{array}{lll} E_5^{-1} E_4 E_5 = E_4 E_2 , & E_5^{-1} E_3 E_5 = E_3 , & E_5^{-1} E_2 E_5 = E_2 E_1 , \\ E_4^{-1} E_3 E_4 = E_3 E_1 , & E_4^{-1} E_2 E_4 = E_2 , & E_3^{-1} E_2 E_3 = E_2 . \end{array}\right\} \quad (1)$$

51. L'elemento E_5^p appartiene a K ed è permutabile con E_5, quindi deve essere E_5^p un elemento di H. Intanto dalle (1) si ricava:

$$E_5^{-p} E_4 E_5^p = E_4 E_2^p E_1^{\binom{p}{2}};$$

dunque, *supponendo* $p > 2$, si ottiene $E_2^p = 1$.

Allora, le formole:

$$E_5^{\ 1} E_4^p E_5 = E_4^p E_2^p , \quad E_4^{-p} E_3 E_4^p = E_3 E_1^p ,$$

mostrano che la potenza E_4^p è invertibile con ogni elemento del gruppo principale e perciò la detta potenza sta in H. Similmente la potenza E_3^p è invertibile con ogni elemento del gruppo principale e perciò sta in H: dunque si hanno le relazioni:

$$E_5^p = E_1^\alpha , \quad E_4^p = E_1^\beta , \quad E_3^p = E_1^\gamma , \quad E_2^p = 1 , \quad E_1^p = 1 , \qquad (2)$$

le quali, insieme alle (1), definiscono sempre un gruppo $G_5^{3,3}$ purchè si tenga presente che è $p > 2$.

Essendo s un intero primo con p, si vede subito che eseguendo la trasformazione:

$$\begin{pmatrix} E_5 , & E_4 , & E_3 , & E_2 , & E_1 \\ E_5 E_3^\lambda , & E_4^s E_3^\mu , & E_3 , & E_2^s E_1^{-s\lambda} , & E_1^s \end{pmatrix}, \qquad (3)$$

la quale non altera la forma delle (1) e (2), i numeri α, β, γ subiscono la sostituzione:

$$s\,\alpha_1 \equiv \alpha + \lambda\,\gamma , \quad s\,\beta_1 \equiv s\,\beta + \mu\,\gamma , \quad s\,\gamma_1 \equiv \gamma \pmod p ;$$

quindi, se γ è primo con p, determinando convenientemente s, λ, μ, si può

supporre:

$$\alpha_1 = \beta_1 = 0, \quad \gamma_1 = 1.$$

Esiste allora un solo gruppo $G_5^{3,3}$ definito dalle relazioni (1) e dalle (2) modificate come segue:

$$E_5^p = 1, \quad E_4^p = 1, \quad E_3^p = E_1, \quad E_2^p = 1, \quad E_1^p = 1$$

Se il numero γ è un multiplo di p, bisogna distinguere il caso in cui è $p > 3$ dal caso in cui è $p = 3$.

Nel primo caso, se u è un intero primo con p, eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5^u E_4^v, & E_4, & E_3^{u^2} E_2^{-uv}, & E_2^u E_1^{\binom{u}{2}}, & E_1^{u^2} \end{pmatrix}, \tag{4}$$

la quale non altera la forma delle (1) e (2), si vede facilmente che α e β si portano rispettivamente in due numeri α_1 e β_1 tali che:

$$u^2 \alpha_1 \equiv u\alpha + v\beta, \quad u^2 \beta_1 \equiv \beta \pmod{p}.$$

Dunque, tutte le volte che è β primo con p, si può determinare u in modo che sia $\beta_1 \equiv 1 \pmod{p}$ oppure $\beta_1 \equiv \varepsilon \pmod{p}$; poi si determina v in modo che sia $\alpha_1 \equiv 0 \pmod{p}$. Se invece è β un multiplo di p, si può determinare u in modo da portare α_1 nel resto *1* ovvero nel resto *0* di p.

In conclusione, quando è $p > 3$, oltre all'ultimo gruppo trovato esistono altri quattro, e non più, gruppi $G_5^{3,3}$ i quali sono definiti dalle (1) e dalle seguenti modificazioni delle formole (2):

$E_5^p = 1,$	$E_4^p = E_1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = 1,$	$E_4^p = E_1^\varepsilon,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = E_1,$	$E_4^p = 1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$
$E_5^p = 1,$	$E_4^p = 1,$	$E_3^p = 1,$	$E_2^p = 1,$	$E_1^p = 1$

I cinque gruppi $G_5^{3,3}$ che ho trovato sono effettivamente distinti: infatti, assumendo come operazione identica ogni cambiamento della base canonica che lasci inalterati i tre numeri α, β, γ, è evidente che qualunque cambia-

mento della detta base, che conservi soltanto la forma delle (1) e (2), equivale al prodotto di una operazione del tipo (3) per una operazione del tipo (4).

52. *Caso di* $p = 3$.

Quando è $p = 3$ le formole (1) e (2) dànno:

$$(E_5^u E_4^v)^3 = E_5^{3u} E_4^{3v} E_1^{u^2 v},$$

e quindi, eseguendo la trasformazione (4) ed osservando che è $u^2 \equiv 1 \pmod 3$, si vede subito che i numeri α e β si portano rispettivamente in due numeri α_1 e β_1 tali che:

$$\alpha_1 \equiv u\alpha + (\beta + 1)v, \quad \beta_1 \equiv \beta \pmod 3.$$

Dunque, se β è 0 od 1, si può determinare v in modo che sia $\alpha_1 \equiv 0 \pmod 3$; ma se è $\beta = 2$, disponendo di u si può portare α_1 nel resto 1 oppure nel resto 0 di p.

Ottengo così quattro nuovi gruppi $G_5^{3,3}$ di grado 243, i quali sono definiti dalle (1) e dalle formole (2) modificate come segue:

$E_5^3 = 1,$	$E_4^3 = 1,$	$E_3^3 = 1,$	$E_2^3 = 1,$	$E_1^3 = 1$
$E_5^3 = 1,$	$E_4^3 = E_1,$	$E_3^3 = 1,$	$E_2^3 = 1,$	$E_1^3 = 1$
$E_5^3 = E_1,$	$E_4^3 = E_1^2,$	$E_3^3 = 1,$	$E_2^3 = 1,$	$E_1^3 = 1$
$E_5^3 = 1,$	$E_4^3 = E_1^2,$	$E_3^3 = 1,$	$E_2^3 = 1,$	$E_1^3 = 1$

53. *Caso di* $p = 2$.

Nel caso in cui è $p = 2$ le relazioni (2) non si verificano.

Però, siccome l'elemento E_5^2 sta in H, la relazione:

$$E_5^{-2} E_4 E_5^2 = E_4 E_2^2 E_1,$$

dà $E_2^2 = E_1$. Allora la formola:

$$E_5^{-1} E_4^2 E_5 = E_4^2 E_2^2 = E_4^2 E_1,$$

mostra che l'elemento E_4^2 non è invertibile con E_5 e quindi il detto elemento appartiene a K ma non ad H. L'elemento E_3^2 è invece permutabile con ogni elemento del gruppo principale e quindi sta in H.

Le (2) debbono perciò essere sostituite con le relazioni:

$$E_5^2 = E_1^\alpha, \quad E_4^2 = E_2 E_1^\beta, \quad E_3^2 = E_1^\gamma, \quad E_2^2 = E_1, \quad E_1^2 = 1, \qquad (5)$$

le quali, insieme alle (1), definiscono effettivamente un gruppo $G_5^{3,3}$ di grado 32 qualunque siano gl'interi α, β, γ.

Ciò posto, io posso sempre supporre $\gamma = 0$, perchè, in caso contrario, raggiungo lo scopo eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5 E_4, & E_4, & E_3 E_2, & E_2, & E_1 \end{pmatrix},$$

la quale non altera le (1).

Poi, eseguendo la trasformazione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5, & E_4 E_2, & E_3, & E_2, & E_1 \end{pmatrix},$$

si vede che il numero β si cambia in $\beta + 1$ e quindi posso supporre $\beta = 0$.

Si può d'altra parte verificare subito che tutti i cambiamenti della base canonica che lasciano inalterate le (1) e che conservano le ipotesi $\beta = \gamma = 0$, non alterano α.

Dunque, si hanno due gruppi distinti $G_5^{3,3}$ di grado 32, i quali sono definiti dalle (1) e dalle seguenti modificazioni delle formole (5):

$E_5^2 = 1,$	$E_4^2 = E_2,$	$E_3^2 = 1,$	$E_2^2 = E_1,$	$E_1^2 = 1$
$E_5^2 = E_1,$	$E_4^2 = E_2,$	$E_3^2 = 1,$	$E_2^2 = E_1,$	$E_1^2 = 1$

54. Io debbo in ultimo luogo ricercare i gruppi $G_5^{3,4}$ e, in questa ricerca, mi fonderò sul fatto che, tutte le volte che è $p > 2$, ogni gruppo $G_5^{3,4}$ contiene un divisore G_4^1 che ha tutti i suoi elementi di grado p.

Per stabilire ciò, si osservi anzitutto che, se E, E' sono due arbitrarî elementi di $G_5^{3,4}$ ed E_1 è un elemento generatore del gruppo $H = K$, si ha:

$$E^{-1} E' E = E' E_1^k,$$

donde si ricava:

$$(E E')^p = E^p E'^p E_1^{k\binom{p}{2}};$$

quindi, avendo supposto $p > 2$, risulta:

$$(E E')^p = E^p E'^p.$$

Sia ora E_2 un elemento di $G_5^{3,4}$ fuori del gruppo H ed E_3 un elemento fuori del gruppo generato dagli elementi E_2, E_1. Ponendo:

$$E_3^p = E_1^\alpha, \quad E_2^p = E_1^\beta,$$

se l'intero β è primo con p, l'elemento $E_3^{\beta} E_2^{\alpha}$, che non sta in H, è di grado p ed io lo assumo come elemento E_2.

Sia E_3 un elemento fuori del gruppo G_2 generato dagli elementi E_2, E_1 così definiti ed E_4 un elemento fuori del gruppo generato dagli elementi E_3, E_2, E_1. Ponendo:

$$E_4^p = E_1^{\alpha}, \quad E_3^p = E_1^{\beta},$$

se l'intero β è primo con p, l'elemento $E_4^{\beta} E_3^{-\alpha}$, che non sta in G_2, è di grado p ed io lo assumo come elemento E_3.

Sia E_4 un elemento fuori del gruppo G_3 generato dagli elementi E_3, E_2, E_1 così definiti, ed E_5 un elemento fuori del gruppo generato dagli elementi E_4, E_3, E_2, E_1. Ponendo:

$$E_5^p = E_1^{\alpha}, \quad E_4^p = E_1^{\beta},$$

se è β primo con p, l'elemento $E_5^{\beta} E_4^{-\alpha}$, che non sta in G_3, è di grado p ed io lo assumo come elemento E_4.

Il gruppo G_4 generato dagli elementi E_4, E_3, E_2, E_1 così definiti ha tutti i suoi elementi di grado p e possiede evidentemente tre divisori indipendenti d'indice p.

Il detto gruppo, per l'osservazione fatta al n.° 40 non può essere Abeliano; quindi, giacchè non esistono (n.° 13) gruppi $G_4^{2,3}$, il gruppo G_4 è un G_4^1.

Ciò posto, se G_2 è il divisore invertibile di G_4^1 ed E_5 è un elemento di $G_5^{3,4}$ fuori di G_4^1, si ha:

$$E_5^{-1} E_4 E_5 = E_4 E_1^{\lambda}, \quad E_5^{-1} E_3 E_5 = E_3 E_1^{\mu}, \quad E_5^{-1} E_2 E_5 = E_2 E_1^{h},$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_4^{-1} E_2 E_3 = E_2,$$
$$E_5^p = E_1^{\alpha}, \quad E_4^p = 1, \quad E_3^p = 1, \quad E_2^p = 1, \quad E_1^p = 1.$$

dove l'intero h è necessariamente primo con p, altrimenti l'elemento E_2 risulterebbe permutabile con ogni elemento del gruppo principale $G_5^{3,4}$.

Chiamando E_2 una conveniente potenza di E_2, io posso ritenere $h = 1$; poi, chiamando E_4, E_3 ordinatamente gli elementi $E_4 E_2^{-\lambda}$, $E_3 E_2^{-\mu}$, mi posso ridurre al caso di $\lambda = \mu = 0$.

Si hanno quindi le formole:

$$\left.\begin{aligned} &E_5^{-1} E_4 E_5 = E_4, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1, \\ &E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2. \end{aligned}\right\} \quad (6)$$

Se l'intero α è un multiplo di p, il gruppo principale ha tutti i suoi elementi di grado p. Se invece α è primo con p, eseguendo la trasforma-

zione:

$$\begin{pmatrix} E_5, & E_4, & E_3, & E_2, & E_1 \\ E_5, & E_4, & E_3^{\alpha}, & E_2^{\alpha}, & E_1^{\alpha} \end{pmatrix},$$

porto α nel resto 1 di p.

Dunque, se è $p > 2$, si hanno due soli gruppi $G_5^{3,4}$, i quali sono definiti dalle (6) e dalle formole:

$E_5^p = 1$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$
$E_5^p = E_4$,	$E_4^p = 1$,	$E_3^p = 1$,	$E_2^p = 1$,	$E_1^p = 1$

55. *Caso di* $p = 2$.

Quando è $p = 2$, chiamo E_2 un elemento di $G_5^{3,4}$ fuori del gruppo $H = K$ e chiamo E_3 un elemento permutabile con E_2 fuori del gruppo generato dagli elementi E_2, E_1. Se E_2 ed E_3 sono entrambi di grado 4, l'elemento $E_3 E_2$ è di grado 2 ed io lo assumo come elemento E_2. Poi si consideri il gruppo G_4^1 costituito da tutti quegli elementi del gruppo principale che sono invertibili col detto elemento E_2.

Allora, se E_3 è un elemento di G_4^1 fuori del gruppo generato da E_2, E_1, ed E_4 è un elemento di G_4^1 fuori del gruppo generato dagli elementi E_3, E_2, E_1; finalmente, se E_5 è un elemento del gruppo principale fuori di G_4^1, si hanno le formole:

$$E_5^{-1} E_4 E_5 = E_4 E_1^{\lambda}, \quad E_5^{-1} E_3 E_5 = E_3 E_1^{\mu}, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2,$$
$$E_5^2 = E_1^{\alpha}, \quad E_4^2 = E_1^{\beta}, \quad E_3^2 = E_1^{\gamma}, \quad E_2^2 = 1, \quad E_1^2 = 1,$$

le quali definiscono sempre un gruppo $G_5^{3,4}$ di grado 32.

Io posso supporre $\lambda = 0$ altrimenti chiamo E_4 l'elemento $E_4 E_2$ ed analogamente posso supporre $\mu = 0$; inoltre, se occorre, chiamando E_5 l'elemento $E_5 E_2$, posso ritenere $\alpha = 0$.

Si ritrovano quindi le formole (6) e le formole:

$$E_5^2 = 1, \quad E_4^2 = E_1^{\beta}, \quad E_3^2 = E_1^{\gamma}, \quad E_2^2 = 1, \quad E_1^2 = 1. \tag{7}$$

Se uno dei due numeri β, γ che vi figurano è zero, si può ritenere che sia $\gamma = 0$, perchè, in caso contrario, si scambierebbe E_4 con E_2; il che non altera le (6). Allora chiamando E_4 l'elemento $E_4 E_3$, si può ritenere anche $\beta = 0$.

Se invece β e γ hanno entrambi il valore *1*, è facile verificare che nessun cambiamento della base canonica che conservi la forma delle (6) e (7) altera β e γ.

Dunque, anche quando è $p = 2$, esistono due soli gruppi $G_5^{3,4}$ di grado 32, i quali sono definiti dalle (6) e dalle seguenti modificazioni delle formole (7):

$E_5^2 = 1$,	$E_4^2 = 1$,	$E_3^2 = 1$,	$E_2^2 = 1$,	$E_1^2 = 1$
$E_5^2 = 1$,	$E_4^2 = E_1$,	$E_3^2 = E_1$,	$E_2^2 = 1$,	$E_1^2 = 1$

56. Riepilogo brevemente i risultati ottenuti nel presente paragrafo.

Per tutti i valori del numero primo $p > 2$ esistono *cinque*, e non più, gruppi $G_5^{3,3}$; invece, quando è $p = 2$, esistono soltanto *due* gruppi $G_5^{3,3}$ di grado 32.

Qualunque sia il numero primo p esistono soltanto *due* gruppi $G_5^{3,4}$.

Tutti i gruppi che si sono presentati in questo paragrafo sono rappresentati nella seguente tabella:

I.

$$E_5^{-1} E_4 E_5 = E_4 E_2, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_1,$$
$$E_4^{-1} E_3 E_4 = E_3 E_1, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2.$$

	E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
Gruppi $G_5^{3,3}$	1	1	E_1	1	1	$p \geq 3$
	1	E_1	1	1	1	$p \geq 3$
	1	E_1^c	1	1	1	$p \geq 3$
	E_1	1	1	1	1	$p > 3$
	1	1	1	1	1	$p \geq 3$
	E_1	E_1^2	1	1	1	$p = 3$
	1	E_2	1	E_1	1	$p = 2$
	E_1	E_2	1	E_1	1	$p = 2$

II.

$$E_5^{-1} E_4 E_5 = E_4, \quad E_5^{-1} E_3 E_5 = E_3, \quad E_5^{-1} E_2 E_5 = E_2 E_4,$$
$$E_4^{-1} E_3 E_4 = E_3 E_4, \quad E_4^{-1} E_2 E_4 = E_2, \quad E_3^{-1} E_2 E_3 = E_2.$$

Gruppi $G_5^{3,4}$.	E_5^p	E_4^p	E_3^p	E_2^p	E_1^p	
	1	1	1	1	1	$p \geqq 2$
	E_1	1	1	1	1	$p > 2$
	1	E_1	E_1	1	1	$p = 2$

§ VIII. Conclusione.

57. Tutti i possibili gruppi di grado $2^5 = 32$ sono *cinquanta*. Di questi 50 gruppi, 22 tipi figurano nei quadri I e II alla fine del § III, altri 16 tipi nel quadro II alla fine del § V, altri 8 tipi nel quadro I alla fine del § VI e finalmente altri 4 tipi figurano nei quadri I e II alla fine del precedente paragrafo.

Tutti i possibili gruppi di grado $3^5 = 243$ sono *sessantasei*. Di questi 66 gruppi, 22 tipi figurano nei quadri I e II alla fine del § III, altri 7 tipi nel quadro II alla fine del § IV, altri 24 tipi nei quadri I e III alla fine del § V, altri 6 tipi nel quadro II alla fine del § VI e finalmente altri 7 tipi figurano nei quadri I e II alla fine del § VII.

Il numero di tutti i possibili gruppi di grado p^5, essendo $p > 3$, è uno dei quattro numeri:

$$2p + 65, \quad 2p + 67, \quad 2p + 69, \quad 2p + 71,$$

secondo che il numero primo p soddisfa, ordinatamente, ad una delle quattro congruenze:

$$p \equiv -1, \quad p \equiv 5, \quad p \equiv -5, \quad p \equiv 1 \pmod{12}.$$

Nei quadri I e II alla fine del § III figurano 22 tipi di gruppi di grado p^5, altri $p + 7$ tipi figurano nel quadro I alla fine del § IV, altri $p + 21$ tipi nei quadri I e III alla fine del § V ed altri 7 tipi nei quadri I e II alla

fine del § VII. Finalmente, nel quadro III alla fine del § VI figurano 8, 10, 12, 14 tipi di gruppi di grado p^5, secondo che il numero primo p soddisfa, ordinatamente, alla 1ª, 2ª, 3ª, 4ª delle precedenti congruenze.

Nella tabella che segue sono scritti i numeri dei diversi tipi di gruppi di grado p^5 contenuti in ciascuna classe $G_5^{\lambda,\mu}$ in corrispondenza alle varie forme del numero primo p.

	$p=2$	$p=3$	$p=12m-1$	$p=12m+5$	$p=12m-5$	$p=12m+1$
$G_5^{0,1}$	1	1	1	1	1	1
$G_5^{0,2}$	2	2	2	2	2	2
$G_5^{0,3}$	2	2	2	2	2	2
$G_5^{0,4}$	1	1	1	1	1	1
$G_5^{0,5}$	1	1	1	1	1	1
$G_5^{1,2}$	5	5	5	5	5	5
$G_5^{1,3}$	7	7	7	7	7	7
$G_5^{1,4}$	3	3	3	3	3	3
$G_5^{2,2}$	5	16	$p+16$	$p+16$	$p+16$	$p+16$
$G_5^{2,3}$	11	15	$p+12$	$p+12$	$p+12$	$p+12$
$G_5^{3,2}$	8	6	8	10	12	14
$G_5^{3,3}$	2	5	5	5	5	5
$G_5^{3,4}$	2	2	2	2	2	2

Palermo, Marzo 1898.