

ANNALI DELLA SCUOLA NORMALE SUPERIORE DI PISA *Classe di Scienze*

ENNIO MATTIOLI

Sopra un'altra proprietà di gruppi abeliani finiti

Annali della Scuola Normale Superiore di Pisa, Classe di Scienze 3^e série, tome 5, n° 1-2 (1951), p. 121-141

http://www.numdam.org/item?id=ASNSP_1951_3_5_1-2_121_0

© Scuola Normale Superiore, Pisa, 1951, tous droits réservés.

L'accès aux archives de la revue « Annali della Scuola Normale Superiore di Pisa, Classe di Scienze » (<http://www.sns.it/it/edizioni/riviste/annaliscienze/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

SOPRA UN'ALTRA PROPRIETÀ DI GRUPPI ABELIANI FINITI

di ENNIO MATTIOLI (Pisa)

INTRODUZIONE

In una precedente memoria⁽¹⁾ ho dimostrato che se G è un gruppo abeliano finito di tipo $(1, \dots, 1)$ e di ordine p^n , se R_1, R_2, \dots, R_n sono gli elementi di una sua base ed n soddisfa alla condizione:

$$(1) \quad n = \frac{p^k - 1}{p - 1} \quad (k \text{ intero } \geq 2)$$

è possibile trovare in G un sottogruppo Γ di ordine p^{n-k} tale che la scomposizione di G secondo Γ ed i suoi laterali si presenta nella forma:

$$(2) \quad G = \Gamma + \Gamma R_1 \dots + \Gamma R_1^{p-1} + \Gamma R_2 + \dots + \Gamma R_n^{p-1}.$$

Ne deducevo un *teorema di ripartizione delle disposizioni con ripetizione*: se n soddisfa alla (1), con p numero primo, tra le p^n disposizioni con ripetizione di p oggetti della classe n è possibile sceglierne un insieme H di p^{n-k} tale che ogni altra disposizione differisca da una di quelle per un solo elemento.

Per ogni gruppo G si hanno più sottogruppi Γ soddisfacenti alla (2); essi sono isomorfi fra loro e si deducono l'uno dall'altro con una permutazione sugli indici delle generatrici e sugli esponenti. Verranno qui indicati con $\Gamma(G)$.

Nel presente lavoro do una generalizzazione di entrambi i teoremi. Sottolineo però che la generalizzazione del primo dimostra effettivamente

(¹) ENNIO MATTIOLI - *Sopra una particolare proprietà dei gruppi abeliani finiti* - Annali della Scuola Normale Superiore di Pisa, Serie III, Vol. III, Fasc. I-IV (1949).

una nuova proprietà dei gruppi G : nel senso che se la (2) dà di essi una scomposizione del 1° ordine, la nuova proprietà ne analizza, per così dire, la microstruttura, dando di G una scomposizione del 2° ordine, quando essa esista. Dimostrerò infatti che se k è pari il gruppo G può esprimersi come prodotto di N sottogruppi indipendenti G_1, G_2, \dots, G_N ($N = \frac{n}{p+1}$; G_i di tipo $(1, \dots, 1)$ e di ordine p^{p+1} per $i = 1, 2, \dots, N$) tali che il prodotto π dei sottogruppi $\Gamma(G_i)$ ($i = 1, 2, \dots, N$) ad essi relativi sta in $\Gamma(G)$; ed ogni laterale che si ottiene scomponendo $\Gamma(G)$ secondo π è il prodotto di N laterali derivati dalla scomposizione dei G_i secondo i corrispondenti $\Gamma(G_i)$. Da questo teorema dedurrò che il teorema di ripartizione delle disposizioni vale anche se nel suo enunciato, e quindi nella (1), si sostituisce al numero primo p il quadrato di un numero primo.

Poichè la comprensione del presente lavoro richiede la conoscenza del precedente (che sarà qui indicato con la locuzione l. c.) userò le stesse notazioni e rinverò senz'altro il lettore a tale memoria ogni volta che ciò potrà evitare ripetizioni.

1. I T -complessi.

Se a e b sono due elementi di G (dove G è un gruppo soddisfacente al 1° teorema dell'Introduzione), distinti fra loro e dall'identità, definiamo T -complesso l'insieme ordinato di $p+1$ elementi:

$$(3) \quad T = (a, b, a b, a^2 b, \dots, a^{p-1} b)$$

Gli elementi a e b , nell'ordine, si diranno generatori di T .
Indicheremo con

$$(4) \quad [T]_s \quad s = 1, 2, \dots, p+1$$

l'elemento di T che occupa il posto s . Per $s \geq 2$ è

$$(5) \quad [T]_s = a^{s-2} b.$$

Prodotto di due T -complessi è il T -complesso che ha per generatori i prodotti dei generatori corrispondenti: di conseguenza anche gli altri elementi del prodotto saranno il prodotto degli elementi corrispondenti dei fattori. La definizione si estende a più fattori e in particolare sarà:

$$(6) \quad T^\alpha = (a^\alpha, b^\alpha, a^\alpha b^\alpha, \dots, a^{(p-1)\alpha} b^\alpha) \quad 1 \leq \alpha \leq p-1$$

Sono di dimostrazione immediata le seguenti proprietà:

- 1) il prodotto dei T -complessi è commutativo e associativo
- 2) vale la relazione

$$(7) \quad [T^\alpha]_s = ([T]_s)^\alpha$$

3) per due T -complessi T e T' si ha:

$$(8) \quad [(T T')^\alpha]_s = [T^\alpha]_s \cdot [T'^\alpha]_s$$

Indicheremo d'ora in poi le prime $p - 1$ potenze di un elemento o di un T -complesso che la locuzione abbreviata: *le $p - 1$ potenze*.

Un T -complesso si dirà *primitivo* se i suoi generatori sono indipendenti, cioè se ogni relazione del tipo

$$(9) \quad a^\alpha = b^\beta$$

porta come conseguenza

$$\alpha \equiv \beta \equiv 0 \pmod{p}$$

Ciò equivale a dire, come si vede facilmente, che b non deve essere una potenza di a .

Per i T -complessi primitivi valgono i seguenti teoremi:

TEOREMA 1^o. — *Se T è primitivo le sue $p - 1$ potenze non contengono l'identità. E viceversa.*

Siano infatti a e b indipendenti e supponiamo per assurdo che per un certo α ed un certo s si abbia

$$(10) \quad [T^\alpha]_s = 1 \quad \begin{array}{l} 1 \leq \alpha \leq p - 1 \\ 1 \leq s \leq p + 1 \end{array}$$

La (10) in forma esplicita si scrive:

$$(11) \quad \begin{array}{ll} a^\alpha = 1 & \text{se } s = 1 \\ (a^{s-2} b)^\alpha = 1 & \text{se } s > 1 \end{array}$$

Entrambe le (11) portano come conseguenza

$$\alpha \equiv 0 \pmod{p}$$

contro l'ipotesi.

Se viceversa a e b non sono indipendenti, ma è:

$$(12) \quad a^\alpha = b^\beta \quad \text{con} \quad \alpha, \beta \equiv 1, \dots, p-1$$

detto s l'intero $\leq p+1$ tale che

$$(s-2)(p-\beta) \equiv \alpha \pmod{p}$$

risulta

$$[T^{(p-\beta)}]_s = 1.$$

TEOREMA 2°. — *Se T è primitivo le sue $p-1$ potenze contengono elementi tutti distinti. E viceversa.*

Se a e b sono indipendenti l'uguaglianza

$$(13) \quad [T^\alpha]_s = [T^{\alpha'}]_{s'}$$

o è assurda o è un'identità. Nella (13) abbiamo tralasciato di scrivere i limiti entro cui variano gli esponenti α, α' e gli indici s, s' ; ma tali limiti sono ovviamente 1 e $p-1$ per i primi, 1 e $p+1$ per i secondi. Ciò faremo anche in seguito quando non c'è possibilità di equivoco.

La (13) in forma esplicita equivale a:

$$\begin{aligned} a^\alpha &= a^{\alpha'} & \text{se} & \quad s = 1; s' = 1 \\ a^\alpha &= (a^{s'-2} b)^{\alpha'} & \text{se} & \quad s = 1; s' > 1 \\ (a^{s-2} b)^\alpha &= (a^{s'-2} b)^{\alpha'} & \text{se} & \quad s > 1; s' > 1 \\ (a^{s-2} b)^\alpha &= a^{\alpha'} & \text{se} & \quad s > 1; s' = 1 \end{aligned}$$

Dalla 1ª o 3ª di queste uguaglianze si deduce

$$\alpha = \alpha'; \quad s = s'$$

cioè la (13) è una identità; dalla 2ª o 4ª si deduce

$$\alpha' \equiv 0; \quad \alpha \equiv 0 \pmod{p}$$

che sono assurde per le limitazioni poste agli esponenti.

Se viceversa a e b non sono indipendenti, ma vale la (12) si ha:

$$[T^\alpha]_1 = [T^\beta]_2.$$

Combinando fra loro i Teoremi 1° e 2° si ottiene il:

TEOREMA 3°. — *Se gli elementi delle $p-1$ potenze di un T -complesso sono tutti distinti, fra essi non vi è l'identità. E viceversa.*

2. Sistema associato ad un T -complesso primitivo.

Sia ora p un numero primo > 2 . Il caso $p = 2$ sarà trattato al n° 4.

Consideriamo i resti (mod p) dei $\frac{p-1}{2}$ numeri

$$(14) \quad 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

e sia u un intero positivo $< p$ distinto da essi.

Dimostriamo che la congruenza

$$(15) \quad x^2 \equiv u \pmod{p}$$

è impossibile. Basterà limitarsi ai numeri $x \leq p-1$.

Se $x \leq \frac{p-1}{2}$ la cosa è evidente. Se invece

$$\frac{p-1}{2} < x \leq p-1$$

posto

$$x' = p - x$$

supponendo che x soddisfi la (15) si avrebbe

$$x'^2 \equiv x^2 \equiv u \pmod{p}$$

con $x' \leq \frac{p-1}{2}$, contro l'ipotesi fatta su u .

Sia ora T_{e1} un T -complesso primitivo⁽²⁾:

$$(16) \quad T_{e1} = (a, b, a b, \dots, a^{p-1} b)$$

Se u è un numero scelto nel modo detto sopra definiremo T -complesso coniugato di T_1 , e lo indicheremo con T_{e2} , il T -complesso avente come elementi generatori b ed a^u :

$$(17) \quad T_{e2} = (b, a^u, a^u b, \dots, a^u b^{p-1})$$

⁽²⁾ Nel presente numero il doppio indice a T_{e1} può apparire superfluo; ma è opportuno conservare l'indice e , che qui è fisso, per avere un simbolo adatto alle successive trattazioni.

Chiameremo poi *i*-esimo *T*-complesso associato a T_{e1} e lo indicheremo con T_{ei} ($i = 1, \dots, p + 1$) il *T*-complesso avente come elementi generatori ordinatamente l'*i*-esimo termine di T_{e1} e l'*i*-esimo termine di T_{e2} . Il primo associato di T_{e1} è T_{e1} stesso; il secondo associato è il suo coniugato T_{e2} .

Gli associati successivi al primo hanno per espressione generale, introducendo un simbolismo più comodo per gli indici:

$$(18) \quad T_{e,(r+2)} = (a^r b, a^u b^r, a^{r+u} b^{r+1}, \dots, a^{(p-1)r+u} b^{r+p-1})$$

$$r = 0, 1, \dots, p - 1.$$

Il termine generico dei T_{ei} , per $i > 1$, è:

$$(19) \quad \text{nel posto } 1: [T_{e,(r+2)}]_1 = a^r b \quad r = 0, \dots, p - 1$$

$$(20) \quad \text{nei posti successivi: } [T_{e,(r+2)}]_{s+2} = a^{sr+u} b^{r+s} \quad r, s = 0, \dots, p - 1$$

L'insieme dei T_{ei} forma il *sistema associato* a T_{e1} (corrispondente al valore fissato per u).

L'indice di associazione i varia tra 1 e $p + 1$ e tralascieremo di scrivere i limiti quando non vi sia possibilità di equivoci.

Dimostriamo il seguente:

TEOREMA. — *La matrice quadrata di ordine $p + 1$ avente come termini della riga i -esima gli elementi di T_{ei} ($i = 1, \dots, p + 1$) è simmetrica.*

Per i termini della prima riga la simmetria segue subito dalla definizione degli associati.

Per i rimanenti termini delle righe successive la simmetria segue dall'osservare che nella (20) scambiando fra loro a primo membro gli indici $r + 2$ ed $s + 2$ il secondo membro rimane inalterato.

Si ha perciò, in simboli:

$$(21) \quad [T_{ei}]_j = [T_{ej}]_i.$$

Dalla (21), tenendo presente la (7), segue pure:

$$(22) \quad [T_{ei}^a]_j = [T_{ej}^a]_i.$$

Infatti è:

$$[T_{ei}^a]_j = ([T_{ei}]_j)^a = ([T_{ej}]_i)^a = [T_{ej}^a]_i.$$

3. Teorema fondamentale.

I $p^2 - 1$ T complessi che si ottengono prendendo le $p - 1$ potenze di un sistema associato contengono, in uno stesso posto, $p^2 - 1$ elementi tutti distinti fra loro.

In simboli bisogna dimostrare che l'uguaglianza

$$(23) \quad [T_{ei}^\alpha]_j = [T_{e'i'}^{\alpha'}]_j$$

o è un'identità, cioè

$$(24) \quad i = i'; \quad \alpha = \alpha';$$

oppure, se si sa a priori che una almeno delle (24) non è vera, è assurda.

Osserviamo anzitutto che la (23) può scriversi, applicando a sinistra e a destra la proprietà (22):

$$(25) \quad [T_{ej}^\alpha]_i = [T_{e'j'}^{\alpha'}]_{i'}$$

e poichè la (25) esprime l'uguaglianza di due termini appartenenti alle $p - 1$ potenze dell'associato T_{ej} , il teorema fondamentale, tenendo conto del Teorema 2° del n° 1. potrà enunciarsi anche nella seguente forma:

I T -complessi associati a un T complesso primitivo sono tutti primitivi.

E dal Teorema 3° del n° 1 seguirà che fra i $p^2 - 1$ elementi tutti distinti, di cui si parla nel 1° enunciato del teorema fondamentale, non figura l'identità.

Dimostreremo dunque che è assurda la (25) quando non sia soddisfatta una almeno delle (24). Distingueremo i vari casi possibili.

I) Sia $j = 1$. La (25) o è un'identità o è assurda perchè per ipotesi T_{e1} è un T -complesso primitivo (Teorema 2° del n° 1).

II) Sia $j > 1$. Si hanno vari sottocasi secondo i valori di i e i' .

II a) Sia inoltre $i = i' = 1$. Applicando alla (25) la (22) si ricade nel caso I).

II b) Sia $i = 1$; $i' > 1$. (Il caso $i' = 1$; $i > 1$ non si distingue praticamente da questo).

La (25), indicando con $r + 2$ l'indice j ($r = 0, \dots, p - 1$) e con $s + 2$ l'indice i' ($s = 0, \dots, p - 1$), diventa

$$(26) \quad [T_{e,(r+2)}^\alpha]_1 = [T_{e,(r+2)}^{\alpha'}]_{s+2}$$

cioè, tenendo presenti le (19) e (20):

$$(26 \text{ bis}) \quad (a^r b)^\alpha = (a^{sr+u} b^{r+s})^{\alpha'}.$$

Sia ora $\bar{\alpha}$ il numero $< p$ per cui

$$(27) \quad \alpha' \bar{\alpha} \equiv 1 \pmod{p}$$

e β il resto (mod p) di $\alpha \bar{\alpha}$:

$$(28) \quad \beta \equiv \alpha \bar{\alpha} \pmod{p}$$

con

$$(29) \quad \beta < p.$$

Elevando ad $\bar{\alpha}$ ambo i membri della (26 bis) si ricava:

$$(30) \quad (\alpha^r b)^\beta = a^{sr+u} b^{r+s}$$

da cui, per l'indipendenza di a e b :

$$(31) \quad \left. \begin{array}{l} \beta \equiv r + s \\ r \beta \equiv s r + u \end{array} \right\} \pmod{p}$$

Le congruenze (31) sono incompatibili. Infatti se fosse $r = 0$ la seconda di esse darebbe:

$$(32) \quad u \equiv 0 \pmod{p};$$

mentre se fosse $r > 0$ eliminando β fra le (31) si ricaverebbe

$$(33) \quad r^2 \equiv u \pmod{p}.$$

Tanto la (32) che la (33) sono assurde.

Il c) Sia $i > 1$; $i' > 1$; $i \neq i'$.

Poniamo

$$j = r + 2; \quad i = s + 2; \quad i' = s' + 2$$

con

$$r, s \equiv 0, \dots, p-1; \quad s \neq s'.$$

La (25) si scrive allora:

$$(34) \quad [T_{e, (r+2)}^\alpha]_{s+2} = [T_{e, (r+2)}^{\alpha'}]_{s'+2}$$

cioè per la (20):

$$(34 \text{ bis}) \quad (a^{sr+u} b^{r+s})^\alpha = (a^{s'r+u} b^{r+s'})^{\alpha'}.$$

Introducendo i numeri $\bar{\alpha}$ e β dati dalle (27), (28), (29), ed elevando ad $\bar{\alpha}$ ambo i membri della (34 bis) si ricava :

$$(35) \quad (a^{sr+u} b^{r+s})^\beta = a^{s'r+u} b^{r+s'}$$

da cui, per l'indipendenza di a e b :

$$(36) \quad \left. \begin{aligned} \beta(r+s) &\equiv r+s' \\ \beta(sr+u) &\equiv s'r+u \end{aligned} \right\} \pmod{p}.$$

Le (36) sono incompatibili. Infatti se

$$(37) \quad r+s \equiv 0 \pmod{p}$$

per la 1^a delle (36) sarebbe pure

$$(38) \quad r+s' \equiv 0 \pmod{p}$$

e quindi

$$s = s'$$

contro l'ipotesi.

Se fosse :

$$(39) \quad sr+u \equiv 0 \pmod{p}$$

dalla seconda delle (36) si avrebbe pure :

$$(40) \quad s'r+u \equiv 0 \pmod{p}.$$

Ma la (39) e (40) avrebbero come conseguenza :

$$\text{per } r=0: \quad u=0$$

$$\text{per } r>0: \quad s=s'$$

entrambe contrarie all'ipotesi.

Supponiamo infine che sia :

$$(42) \quad \left. \begin{aligned} r+s &\not\equiv 0 \\ sr+u &\not\equiv 0 \end{aligned} \right\} \pmod{p}.$$

Allora eliminando β dalle (36) si ricava con facili passaggi :

$$(43) \quad r^2(s-s') \equiv u(s-s') \pmod{p}.$$

Dalla (43), essendo per ipotesi $s \neq s'$, si giunge di nuovo all'assurdo:

$$r^2 \equiv u \pmod{p}.$$

4. Sistema associato e teorema fondamentale per $p = 2$.

Nel caso $p = 2$ posto:

$$(44) \quad T_{e_1} = (a, b, a b)$$

con $a \neq b$, definiremo come associati di T_{e_1} i T -complessi:

$$(45) \quad T_{e_2} = (b, a b, a)$$

$$T_{e_3} = (a b, a, b)$$

Poichè ogni T -complesso possiede in questo caso soltanto la prima potenza, e per $a \neq b$ i tre T -complessi soprascritti sono primitivi, si verifica immediatamente che il sistema associato formato dalle (44) e (45) soddisfa alle condizioni di simmetria del n° 2, e ai due enunciati del teorema fondamentale del n° 3.

Nel seguito perciò non si farà più distinzione fra il caso $p > 2$ e il caso $p = 2$.

5. I B -complessi.

Se a e b sono due elementi di G distinti fra loro e dalla identità definiamo B -complesso l'insieme ordinato di $p - 1$ elementi:

$$(46) \quad B = (a b, a^2 b, \dots, a^{p-1} b)$$

Gli elementi a e b saranno detti generatori di B e se essi sono indipendenti il B -complesso sarà detto *primitivo*.

Ai B -complessi si estendono in modo ovvio le definizioni e le proprietà del prodotto date al n° 2 per i T -complessi. In particolare vale il

TEOREMA. — *Le $p - 1$ potenze di un B -complesso primitivo contengono $(p - 1)^2$ elementi tutti diversi fra loro e formati ciascuno di due generatori.*

La prima parte del teorema segue subito dall'osservare che i $(p - 1)^2$ elementi in questione appartengono anche alle $p - 1$ potenze di un T -complesso primitivo di generatori a e b , e perciò sono diversi fra loro.

La seconda parte segue dal fatto che :

$$[B^a]_s = (a^s b)^a = a^{sa} b^a$$

ed essendo α ed s compresi fra 1 e $p - 1$ non può essere nè $\alpha \equiv 0$, nè $s \alpha \equiv 0 \pmod{p}$.

6. La base ordinata e ripartita di $\theta(G)$.

Supporremo d'ora in poi che il numero k che compare nella (1) sia pari e ≥ 4 ; poniamo

$$(47) \quad k = 2h; \quad h \geq 2.$$

Il caso $h = 1$ non porterebbe a nuovi risultati.

Indichiamo con $\theta(G)$ l'insieme θ relativo al gruppo G (vedi l. c.); esso consta di

$$(48) \quad m = p^k - 1 - k(p - 1)$$

elementi costituiti di generatrici con indici $\leq k$.

Dimostriamo che è possibile costruire una base di $\theta(G)$, che diremo ordinata e ripartita, tale che i suoi elementi rappresentino ordinatamente i termini di h B -complessi primitivi e di l T -complessi primitivi, con

$$(49) \quad l = \frac{m - h(p - 1)^2}{p^2 - 1}.$$

Osserviamo subito che il numero totale di elementi contenuti in h B -complessi e in l T -complessi, ammesso che siano tutti distinti e tenendo conto della (49), è

$$\frac{m}{p - 1}$$

uguale cioè al numero di elementi necessari per formare una base di $\theta(G)$.

Suddividiamo le prime k generatrici di G in h coppie; la coppia generica di posto e sarà formata dalle generatrici:

$$(50) \quad R_{2e-1}, \quad R_{2e}. \quad (e = 1, \dots, h)$$

Indichiamo con B_e il B -complesso primitivo avente per generatori la coppia (50):

$$(51) \quad B_e = (R_{2e-1} R_{2e}, \dots, R_{2e-1}^{p-1} R_{2e})$$

Al variare di e si hanno dalla (51) h B -complessi.

Sia poi T_{e1} il T -complesso primitivo avente per generatori la coppia (50):

$$(52) \quad T_{e1} = (R_{2e-1}, R_{2e}, R_{2e-1} P_{2e}, \dots, R_{2e-1}^{p-1} R_{2e})$$

e sia T_{ei} l' i -esimo associato di T_{e1} .

Indichiamo con

$$(53) \quad k_1, k_2, \dots, k_f \quad 2 \leq f \leq h$$

una *combinazione semplice di classe f dei numeri $1, \dots, h$ ordinata per valori crescenti dei numeri che la compongono*.

Formiamo tutti i prodotti che si possono ricavare dall'espressione:

$$(54) \quad T = T_{k_1, 1} T_{k_2, i_2}^{\alpha_2}, \dots, T_{k_f, i_f}^{\alpha_f}$$

quando gli esponenti $\alpha_2, \dots, \alpha_f$ variano fra 1 e $p-1$ e gl'indici i_2, \dots, i_f fra 1 e $p+1$. Tali prodotti sono ancora dei T -complessi e per ogni combinazione (53) se ne ottengono

$$(p+1)^{f-1} (p-1)^{f-1} = (p^2-1)^{f-1}.$$

Perciò per ogni valore di f (compreso fra 2 ed h) facendo variare anche la combinazione dei primi indici, se ne avranno:

$$\binom{h}{f} (p^2-1)^{f-1};$$

in definitiva, al variare di f tra 2 ed h , si otterranno dalla (54)

$$(55) \quad \binom{h}{2} (p^2-1) + \binom{h}{3} (p^2-1)^2 + \dots + \binom{h}{h} (p^2-1)^{h-1}$$

prodotti distinti, differenti l'uno dall'altro per qualche indice o qualche esponente.

Il numero fornito dalla (55) ed il numero e dato dalla (49) sono uguali fra loro: si verifica infatti, con facili passaggi e tenendo conto delle (47) e (48), che entrambi, moltiplicati per (p^2-1) danno come risultato $m-h(p-1)^2$.

Ordiniamo gli h B -complessi (51) per valori crescenti dell'indice e . Ordiniamo con una legge qualunque gli l T -complessi (54) e poniamo i T -complessi di seguito ai B complessi.

Gli $\frac{m}{p-1}$ elementi contenuti negli h B -complessi e negli l T -complessi così riuniti costituiscono una base ordinata e ripartita di $\theta(G)$.

Per dimostrarlo occorrerà far vedere che gli m elementi che si ottengono dalle $p - 1$ potenze dei termini sopradetti:

A) stanno in $\theta(G)$

B) sono tutti distinti fra loro, e quindi essendo in numero di m esauriscono $\theta(G)$.

A) Abbiamo già visto al n° 5 che le $p - 1$ potenze di un B -complesso primitivo* contengono elementi formati da due generatori: perciò le $p - 1$ potenze dei B -complessi (51) danno elementi di $\theta(G)$.

I termini contenuti nelle $p - 1$ potenze dei T -complessi (52) possiedono almeno una generatrice (Teorema I del n° 1) perciò i prodotti (54) contengono almeno due diverse generatrici di G e quindi stanno in $\theta(G)$.

B) I termini delle $p - 1$ potenze dei B -complessi (51) sono tutti diversi fra loro: la cosa è evidente per B -complessi di indice diverso, e segue dal Teorema del n° 5 per le potenze di uno stesso B -complesso.

Detti termini sono inoltre tutti distinti dai termini ottenuti dalle $p - 1$ potenze dei T -complessi (54): perchè questi ultimi o contengono più di due generatrici di G o, se ne contengono due, queste appartengono a due diverse coppie (50).

Rimane da far vedere che sono tutti diversi i termini che si ottengono dalle $p - 1$ potenze dei T -complessi (54). Consideriamo due di tali termini

$$[T^\alpha]_s \text{ e } [T'^{\alpha'}]_{s'}$$

Se essi corrispondono a due diverse combinazioni k_1, \dots, k_f (diverse per la classe oppure di classe uguale, ma formate con numeri diversi) essi contengono differenti generatrici di G e sono perciò diversi fra loro. Se invece derivano dalla stessa combinazione k_1, \dots, k_f supponiamo che sia

$$(56) \quad \left[\left(T_{k_1,1}^{\alpha_1} T_{k_2,i_2}^{\alpha_2} \dots T_{k_f,i_f}^{\alpha_f} \right)^\alpha \right]_s = \left[\left(T_{k_1,1}^{\alpha'_1} T_{k_2,i'_2}^{\alpha'_2} \dots T_{k_f,i'_f}^{\alpha'_f} \right)^{\alpha'} \right]_{s'}$$

con le note limitazioni per gl'indici e gli esponenti, e dimostriamo che la (56) se non è assurda è una identità.

Per l'indipendenza delle generatrici di G che compaiono in $T_{k_1,1}, T_{k_2,1}, \dots, T_{k_f,1}$ la (56), tenendo conto della (8) si scinde nell'insieme di uguaglianze:

$$(57) \quad \left\{ \begin{array}{l} [T_{k_1,1}^\alpha]_s = [T_{k_1,1}^{\alpha'}]_{s'} \\ [T_{k_2,i_2}^{\alpha_2} T_{k_2,i'_2}^{\alpha'_2}]_s = [T_{k_2,i_2}^{\alpha'_2} T_{k_2,i'_2}^{\alpha'_2}]_{s'} \\ \dots \dots \dots \\ [T_{k_f,i_f}^{\alpha_f} T_{k_f,i'_f}^{\alpha'_f}]_s = [T_{k_f,i_f}^{\alpha'_f} T_{k_f,i'_f}^{\alpha'_f}]_{s'} \end{array} \right.$$

Dalla prima delle (57) essendo $T_{k_1,1}$ primitivo si deduce (Teorema 2° del n° 1) che, se si esclude l'assurdo, deve essere

$$(58) \quad \alpha = \alpha'; \quad s = s'.$$

Allora la seconda delle (57) diventa:

$$(59) \quad \left[T_{k_2, i_2}^{\alpha_2 \alpha} \right]_s = \left[T_{k_2, i_2'}^{\alpha_2' \alpha} \right]_s$$

e da questa, applicando al T -complesso $T_{k_2,1}$ il teorema fondamentale nella sua prima forma, si deduce:

$$\begin{aligned} \alpha_2 \alpha &= \alpha_2' \alpha; & i_2 &= i_2' \\ \text{cioè} & & & \\ (60) \quad \alpha_2 &= \alpha_2'; & i_2 &= i_2'. \end{aligned}$$

In modo perfettamente analogo si procede per le successive uguaglianze della (57) e si arriva alla conclusione che la (56) se non è assurda è un'identità.

7. Il sottogruppo composto $\Gamma(G)$.

Moltiplicando ordinatamente gli

$$\frac{n}{p-1} = n - k$$

elementi che costituiscono una base ordinata e ripartita di $\theta(G)$ per le generatrici di G di indice maggiore di k si ottiene la base di un sottogruppo $\Gamma(G)$ (vedi l. c.) che chiameremo *composto* e indicheremo semplicemente con Γ . Per esso vale il seguente:

TEOREMA. — *Il gruppo G si può scomporre nel prodotto di*

$$(61) \quad N = \frac{n}{p+1}$$

sottogruppi indipendenti

$$(62) \quad G_1, G_2, \dots, G_N$$

ciascuno di tipo $(1, \dots, 1)$ e di ordine p^{p+1} , tali che i sottogruppi

$$(63) \quad \Gamma(G_1), \Gamma(G_2), \dots, \Gamma(G_N)$$

ad essi relativi danno un prodotto π contenuto in Γ .

Suddividiamo le n generatrici di G in raggruppamenti di $p + 1$ generatrici secondo la legge che ora esporremo.

Dapprima formiamo h raggruppamenti prendendo per ciascuno le due generatrici di un B_e della formula (51) e di seguito le $p - 1$ generatrici che nella costruzione della base di Γ moltiplicano gli elementi del B_e medesimo. Il generico di tali raggruppamenti conterrà perciò le generatrici:

$$(64) \quad R_{2e-1}, R_{2e}, R_{k+(e-1)(p-1)+1}, R_{k+(e-1)(p-1)+2}, \dots, R_{k+e(p-1)} \quad e = 1, 2, \dots, h.$$

Indichiamo con G_e il sottogruppo da esse generato. I sottogruppi

$$G_1, \dots, G_h$$

fra loro indipendenti saranno detti sottogruppi di prima specie; essi contengono complessivamente le prime $h(p + 1)$ generatrici di G .

Con le rimanenti generatrici di G , ordinate per indice crescente, formiamo altri raggruppamenti di $p + 1$ generatrici e indichiamo con

$$G_{h+1}, \dots, G_N; \quad N = \frac{n}{p + 1}$$

i sottogruppi da essi generati (sottogruppi di seconda specie). Il generico G_j di tali sottogruppi avrà per generatrici:

$$(65) \quad R_{(j-1)(p+1)+1}, R_{(j-1)(p+1)+2}, \dots, R_{jp+1}.$$

Notiamo che nella formazione della base di Γ le generatrici (65) moltiplicavano ordinatamente gli elementi di un T -complesso del tipo (54) che sarà ora indicato brevemente con:

$$(66) \quad T_j = (a_j, b_j, a_j b_j, \dots, a_j^{p-1} b_j)$$

I sottogruppi di prima e seconda specie non si distinguono fra loro altro che per il diverso modo con cui abbiamo scelto le generatrici. Essi sono tutti indipendenti fra loro ed il loro prodotto coincide con G :

$$G = G_1 \cdot G_2 \dots G_N;$$

inoltre essendo di tipo $(1, \dots, 1)$ e di ordine p^{p+1} soddisfano alle condizioni del 1° Teorema dell'Introduzione (dalla (1) per $k = 2$ si ha $n = p + 1$) perciò sono scomponibili secondo la formula (2).

Dimostriamo che si può scegliere per ogni G_i ($i = 1, \dots, N$) un sottogruppo $\Gamma(G_i)$ appartenente a Γ .

Consideriamo dapprima i sottogruppi G_e di prima specie ($e = 1, \dots, h$). Il B -complesso B_e della (51) forma una base del $\theta(G_e)$; perciò moltiplicando gli elementi di B_e ordinatamente per le $p-1$ generatrici che nella (64) occupano i posti $3, \dots, p+1$ otteniamo un sottogruppo $\Gamma(G_e)$. Ma i prodotti così formati fanno parte anche della base di Γ perciò $\Gamma(G_e)$ sta in Γ .

Sia ora G_j ($j = h+1, \dots, N$) un sottogruppo di seconda specie e siano le (65) le sue generatrici. Per semplicità di notazioni indichiamo le (65) con:

$$(67) \quad \mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_{p+1}$$

e con

$$(68) \quad \alpha_1 = a_j \mathcal{R}_1, \quad \alpha_2 = b_j \mathcal{R}_2, \quad \alpha_3 = a_j b_j \mathcal{R}_3, \dots, \alpha_{p+1} = a_j^{p-1} b_j \mathcal{R}_{p+1}$$

i corrispondenti elementi della base di Γ . Nelle notazioni (67) e (68) l'indice j scompare, ma la dimostrazione vale inalterata per qualunque j compreso fra $h+1$ ed N .

I termini:

$$(69) \quad \mathcal{B}_1 = \mathcal{R}_1^{p-1} \mathcal{R}_2^{p-1}, \quad \mathcal{B}_2 = \mathcal{R}_1^{p-2} \mathcal{R}_2^{p-1}, \dots, \mathcal{B}_{p-1} = \mathcal{R}_1 \mathcal{R}_2^{p-1}$$

costituiscono, com'è facile verificare, una base di $\theta(G_j)$; perciò i prodotti:

$$(70) \quad \mathcal{B}_1 \mathcal{R}_3, \mathcal{B}_2 \mathcal{R}_4, \dots, \mathcal{B}_{p-1} \mathcal{R}_{p+1}$$

formano la base di un sottogruppo $\Gamma(G_j)$.

Dimostriamo che i termini della (70) si possono ottenere come prodotti di elementi α della (68): ne seguirà che la base di $\Gamma(G_j)$ è formata di elementi di Γ e quindi $\Gamma(G_j)$ sta in Γ .

Per il generico termine della successione (70), di posto s , si ha tenendo conto delle (69):

$$(71) \quad \mathcal{B}_s \mathcal{R}_{s+2} = \mathcal{R}_1^{p-s} \mathcal{R}_2^{p-1} \mathcal{R}_{s+2} \quad s = 1, \dots, p-1.$$

Ma per le (68) si ha pure:

$$(72) \quad \alpha_1^{p-s} \alpha_2^{p-1} \alpha_{s+2} = \mathcal{R}_1^{p-s} \mathcal{R}_2^{p-1} \mathcal{R}_{s+2} \quad s = 1, \dots, p-1$$

quindi

$$(73) \quad \mathcal{B}_s \mathcal{R}_{s+2} = \alpha_1^{p-s} \alpha_2^{p-1} \alpha_{s+2} \quad s = 1, \dots, p-1$$

cioè la base di $\Gamma(G_j)$ sta in Γ .

Posto ora

$$(74) \quad \pi = \Gamma(G_1) \cdot \Gamma(G_2) \dots \Gamma(G_N)$$

poichè i sottogruppi a secondo membro appartengono a Γ anche il loro prodotto π starà in Γ .

8. L'indice ed i laterali di π in Γ .

I sottogruppi $\Gamma(G_i)$ ($i = 1, \dots, N$) operando su generatrici diverse sono indipendenti fra loro. Avendo ciascuno ordine p^{p-1} il loro prodotto π avrà ordine:

$$(75) \quad p^{(p-1)N}.$$

D'altra parte l'ordine di Γ è p^{n-k} e posto

$$(76) \quad P = p^2$$

si ricava facilmente, tenendo conto delle (47) e (61), che l'indice di π in Γ è:

$$(77) \quad P^{N-h}.$$

Scomponiamo ogni gruppo G_i secondo $\Gamma(G_i)$ ed i suoi laterali in base alla (2) e indichiamo con

$$(78) \quad \Gamma_{i,r}$$

il laterale di posto r , con l'ipotesi $\Gamma_{i,1} = \Gamma(G_i)$.

Sarà cioè, per ogni $i = 1, \dots, N$, essendo P l'indice di $\Gamma(G_i)$ dentro G_i :

$$(79) \quad G_i = \Gamma_{i,1} + \Gamma_{i,2} + \dots + \Gamma_{i,P}.$$

Dimostriamo il seguente:

TEOREMA. — *I laterali di π , dentro Γ , possiedono una formula di scomposizione analoga alla (74) e che si ottiene da quella sostituendo nel primo membro il gruppo π con un suo laterale e nel secondo membro ogni singolo $\Gamma(G_i)$ con un rispettivo laterale (tale sostituzione essendo estesa a tutti o a parte i $\Gamma(G_i)$ del secondo membro).*

Se $\pi\gamma$ è un qualunque laterale di π (γ elemento di Γ esterno a π) dobbiamo dimostrare che:

$$(80) \quad \pi\gamma = \Gamma_{1,r_1} \cdot \Gamma_{2,r_2} \cdot \dots \cdot \Gamma_{N,r_N}$$

essendo

$$(81) \quad r_1, r_2, \dots, r_N$$

opportuni interi compresi fra 1 e P .

Scomponiamo γ nel prodotto di N elementi:

$$(82) \quad \gamma = \gamma_1 \cdot \gamma_2 \cdot \dots \cdot \gamma_N$$

con la condizione che γ_i stia in G_i ($i = 1, \dots, N$). Poichè i gruppi G_i sono fra loro indipendenti ed il loro prodotto coincide con G la scomposizione (82) è sempre possibile ed è unica; eventualmente qualche γ_i potrà ridursi all'identità.

Moltiplicando membro a membro la (74) e la (82) si ricava:

$$(83) \quad \pi \gamma = \Gamma(G_1) \gamma_1 \cdot \Gamma(G_2) \gamma_2 \cdot \dots \cdot \Gamma(G_N) \gamma_N.$$

D'altra parte moltiplicando ogni $\Gamma(G_i)$ per un elemento γ_i di G_i si ha un laterale di $\Gamma(G_i)$, eventualmente $\Gamma(G_i)$ stesso, perciò ponendo in generale

$$(84) \quad \Gamma(G_i) \gamma_i = \Gamma_{i,r_i} \quad \begin{array}{l} i = 1, \dots, N \\ r_i \equiv 1, \dots, P \end{array}$$

e sostituendo nella (83) si ha la (80).

9. La proprietà dei laterali di Γ .

Ogni laterale di Γ della scomposizione (2) si può ottenere da un altro laterale qualunque moltiplicandolo per una potenza di una sola generatrice.

Siano

$$(85) \quad L_1 = \Gamma R_i^\alpha \quad \text{ed} \quad L_2 = \Gamma R_j^\beta \quad \left(\begin{array}{l} i, j = 1, \dots, n \\ \alpha, \beta = 1, \dots, p-1 \end{array} \right)$$

due laterali di Γ , diversi fra loro.

Il termine:

$$R_i^{-\alpha} R_j^\beta$$

non potendo stare in Γ si troverà in uno dei laterali e potremo scrivere:

$$R_i^{-\alpha} R_j^\beta = \gamma R_m^\delta \quad \begin{array}{l} m \equiv 1, \dots, n \\ \delta \equiv 1, \dots, p-1 \end{array}$$

con γ elemento di Γ . Segue:

$$L_2 = \Gamma R_j^\beta = \Gamma \gamma R_i^\alpha R_m^\delta = L_1 R_m^\delta.$$

Dal teorema dimostrato si deduce che la scomposizione (2) del gruppo G è ancora valida se in luogo di Γ si sostituisce formalmente un laterale L , con l'unica differenza che L non è più un sottogruppo. Ma questa sostituzione ci dice che se invece di applicare alla disposizione fondamentale (vedi l. c. n° 2) le operazioni del sottogruppo Γ applichiamo quelle di un laterale L otteniamo ancora un insieme di disposizioni avente la stessa proprietà di H : e ciò perchè ogni operazione di G che non sta in L deve trovarsi in un « laterale » di L , cioè può ottenersi da un'operazione di L moltiplicandola per la potenza di una sola generatrice.

Dunque applicando alla disposizione fondamentale le operazioni di Γ e dei suoi laterali le p^n disposizioni con ripetizione vengono ripartite in p^k insiemi, ciascuno di p^{n-k} disposizioni, aventi la proprietà che considerato uno qualunque di essi, ogni disposizione ad esso esterna differisce da una disposizione dell'insieme per un solo elemento.

Di qui il nome di teorema di ripartizione delle disposizioni dato al teorema 2° dell'Introduzione.

10. Il teorema di ripartizione per il quadrato di un numero primo.

Se $P = p^2$ è il quadrato di un numero primo ed

$$(87) \quad N = \frac{P^h - 1}{P - 1} \quad (h \text{ intero } \geq 2)$$

fra le P^N disposizioni con ripetizione di P oggetti della classe N è possibile sceglierne un insieme H di P^{N-h} tali che ogni altra disposizione differisca da una di H per un solo elemento.

Siano dati P oggetti distinti. Indichiamo l' i -esimo oggetto ($i = 1, \dots, P$) col simbolo:

$$(88) \quad \Gamma_{1,i}, \Gamma_{2,i}, \dots, \Gamma_{N,i}$$

secondo che in una disposizione considerata esso occupi il posto $1, 2, \dots, N$. Ogni disposizione dei P oggetti sarà perciò rappresentata da una scrittura del tipo:

$$(89) \quad \Gamma_{1,r_1} \Gamma_{2,r_2} \dots \Gamma_{N,r_N}$$

dove l'accostamento dei simboli Γ_{i,r_i} non ha significato di prodotto ed r_1, r_2, \dots, r_N rappresenta una disposizione con ripetizione di classe N dei numeri $1, \dots, P$.

Consideriamo l'insieme H di tutte le disposizioni che si ottengono dalla formola (80) quando il primo membro di essa percorre tutti i laterali di π in Γ , intendendo soppressi nel secondo membro i simboli di moltiplicazione tra i fattori Γ_{i,r_i} che vi figurano. Dimostriamo che questo insieme è quello richiesto.

Intanto H contiene P^{N-h} disposizioni perchè tale è, per la (77), il numero dei laterali di π dentro Γ (in questo paragrafo quando si parla di laterali in genere si intende *comprendere fra essi il sottogruppo che li genera*).

Basta perciò far vedere che ogni altra disposizione differisce da una di H per un solo elemento. Sia

$$(90) \quad \Gamma_{1,i_1} \Gamma_{2,i_2} \dots \Gamma_{N,i_N}$$

una disposizione qualunque esterna ad H .

Consideriamo i laterali omonimi alla (90) e scegliamo da ciascuno di essi un elemento arbitrario diverso dall'identità. Sia

$$(91) \quad g = g_1 \cdot g_2 \dots g_N$$

il prodotto di tali elementi. Dimostriamo che g , che è un elemento di G , è esterno a Γ . Se infatti esso stesse in Γ moltiplicando membro a membro la (74) e la (91) si otterrebbe

$$(92) \quad \pi g = \Gamma_{1,i_1} \cdot \Gamma_{2,i_2} \dots \Gamma_{N,i_N}$$

ed essendo πg un laterale di π la disposizione (90) starebbe in H contro l'ipotesi.

Dunque g si troverà in un laterale di Γ e potremo porre in base alla (2)

$$(93) \quad g = \gamma \cdot K_s^\alpha \quad \begin{array}{l} \alpha \equiv 1, \dots, p-1 \\ s \equiv 1, \dots, n \end{array}$$

con γ elemento di Γ ed K_s^α certamente diverso dall'identità. Qui s è un numero fisso e non un indice variabile.

Sia G_s il sottogruppo che contiene R_s . Eseguiamo su γ la scomposizione indicata dalla (82) e sia

$$(94) \quad \gamma = \gamma_1 \cdot \gamma_2 \dots \gamma_N$$

con γ_i in G_i ($i = 1, \dots, N$); si noti che in generale γ_i non apparterrà al corrispondente $\Gamma(G_i)$.

Per l'indipendenza dei sottogruppi G_1, \dots, G_N dalle (94), (93) e (91) segue:

$$(95) \quad g_1 = \gamma_1, g_2 = \gamma_2, \dots, g_s = \gamma_s R_s^\alpha, \dots, g_N = \gamma_N$$

potendo s prendere i valori estremi 1 ed N .

Essendo per ipotesi g_s un elemento di I_{s,i_s} si ha:

$$(96) \quad \Gamma_{s,1} \cdot g_s = \Gamma_{s,i_s}.$$

Poniamo

$$(97) \quad \Gamma_{s,1} \cdot \gamma_s = \Gamma_{s,c_s}.$$

Dalle (97) e (96) tenendo presente la (95) si ricava:

$$(98) \quad \Gamma_{s,i_s} = \Gamma_{s,c_s} \cdot R_s^\alpha$$

cioè i laterali Γ_{s,i_s} e Γ_{s,c_s} , per quanto è stato detto al n° 9, sono diversi fra loro.

Moltiplichiamo infine membro a membro la (94) e la (74): tenendo conto delle (97) e (95) si arriva al risultato:

$$(99) \quad \pi \gamma = \Gamma_{1,i_1} \cdot \Gamma_{1,i_2} \dots \Gamma_{s,c_s} \dots \Gamma_{N,i_N}.$$

Ma il primo membro della (99) è un laterale di π perciò la disposizione ricavabile dal secondo membro *sta in* H . E la (90) differisce da essa soltanto per l'elemento di posto s che è Γ_{s,c_s} invece di Γ_{s,i_s} .

[Entrato in redazione il 1 6-1951]