Bollettino
Unione Matematica Italiana

Luigi Antonio Rosati

Sui gruppi ogni sottogruppo ciclico dei quali è caratteristico.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **11** (1956), n.4, p. 544–552.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1956_3_11_4_544_0>

Sui gruppi ogni sottogruppo ciclico dei quali è caratteristico.

Nota di LUIGI ANTONIO ROSATI (a Firenze)

Sunto. - *Si determina la struttura dei gruppi di torsione ogni sottogruppo ciclico dei quali è caratteristico, e si dà per un gruppo generico una condizione necessaria perchè ogni suo sottogruppo ciclico sia caratteristico. Si ritrova in particolare un risultato di* F. SZÁSZ.

1. Sia G un gruppo arbitrario rappresentato moltiplicativamente. Diremo che G ha la proprietà P se ogni suo sottogruppo ciclico è caratteristico. Esistono gruppi con proprietà P: tali sono per esempio tutti i gruppi ciclici. Il caso particolare che ogni sottogruppo ciclico di G sia una potenza di G, sia cioè il gruppo generato dalle potenze k-me degli elementi di G, è stato considerato da F. SZÁSZ [1] [2], che ha dimostrato che, in questo caso, G è ciclico. Noi in questo lavoro riusciamo a determinare la struttura dei gruppi di torsione con proprietà P e a dare per gli altri gruppi una condizione necessaria perchè abbiano la proprietà P. In particolare si ritrova più rapidamente il risultato di F. SZÁSZ.

2. Ricordiamo che un gruppo si dice *di torsione* se tutti i suoi elementi sono periodici, mentre si dice *senza torsione* se tutti i suoi elementi, eccettuata l'unità, sono aperiodici. Cominciamo col provare che

TEOREMA 1. - *Se* $\mathfrak{G}$ *è un gruppo abeliano di torsione ed ogni suo sottogruppo di ordine finito è ciclico, allora* $\mathfrak{G}$ *ha la proprietà* P.

Basterà far vedere che in G c'è al più un sottogruppo di un dato ordine n. Se ve ne fossero due, A e B, necessariamente ciclici, $A \bigcup B$ sarebbe ancora finito (essendo G abeliano, $A \bigcup B = AB$, il cui ordine è al massimo n^2), e quindi, per ipotesi, ciclico. Ma un gruppo ciclico ha al massimo un sottogruppo di un dato ordine, mentre $A \bigcup B$ conterrebbe A e B, ambedue d'ordine n. Onde l'assurdo.

Come immediata conseguenza si ricava il seguente

COROLLARIO. - *Il gruppo moltiplicativo di tutte le radici dell'unità positiva ha la proprietà* P.

Dimostriamo ora che

TEOREMA 2. - *Se* G *ha la proprietà* P. *allora* G *è abeliano.*

Ogni sottogruppo ciclico di G, essendo caratteristico, è anche normale, quindi ogni sottogruppo di G è normale e G è abeliano o hamiltoniano. Per assurdo supponiamo che G sia hamiltoniano; a_1 e a_2 siano due suoi elementi non permutabili ed inoltre sia $a_3 = a_1 a_2$. È noto che a_1 e a_2 generano un sottogruppo, Q, di G isomorfo al gruppo dei quaternioni e $G = QH$, dove H è un gruppo abeliano prodotto diretto di due gruppi, uno a elementi tutti bilateri, l'altro a elementi tutti di periodo dispari. Inoltre si sa che ogni elemento di Q è permutabile con qualsiasi elemento di H e che $Q \cap H$ è un sottogruppo d'ordine 2, costituente il centro di Q.

Risulta immediato verificare che in Q esiste un automorfismo, α, che cambia a_1 in a_2, a_2 in a_3, a_3 in a_1. Basterà allora prolungare tale automorfismo in G perchè sia dimostrato che G non può essere hamiltoniano. Con riferimento al teorema di G. ZAPPA « Sull'ampliamento degli automorfismi » [3], si assuma come sistema residuo di generatori di G rispetto a Q l'insieme degli elementi di H che non appartengono a Q e si faccia corrispondere ad ognuno di essi se stesso. Tenuto conto che $Q \cap H = |a_1^2| = |a_2^2| = |a_3^2|$, risultano soddisfatte le condizioni previste dal teorema di G. ZAPPA e, secondo il detto teorema, esiste un automorfismo di G che determina sugli elementi di Q la sostituzione determinata da α e che lascia inalterati gli elementi di H. Risulta dunque dimostrato quanto volevamo.

La dimostrazione fatta si può rendere più semplice se G è finito, oppure se si accetta fin da ora il postulato di ZERMELO, nei quali casi si sa che, se hamiltoniano, $G = Q \times L$, con Q isomorfo al gruppo dei quaternioni, ed L prodotto diretto di due gruppi, uno a elementi tutti bilateri, l'altro a elementi tutti di periodo dispari. In tal caso, detti a_1 e a_2 due elementi di periodo 4 di Q, che insieme generino Q, l'automorfismo di G che subordina in Q l'automorfismo $a_1 \rightarrow a_2 \rightarrow a_1 a_2$ e in L l'automorfismo identico, non muta in sè i sottogruppi $|a_1|$, $|a_2|$, $|a_1 a_2|$, onde G non gode della proprietà P. Resta quindi dimostrato che G è abeliano.

Diciamo ora *primario relativo al numero primo* p un gruppo abeliano tutti gli elementi del quale abbiano per ordine potenze di p. Diciamo poi *indecomponibile* un gruppo abeliano se non può essere rappresentato come prodotto diretto di sottogruppi nessuno dei quali sia identico. Indichiamo con $Z(p^n)$ un gruppo primario relativo al numero primo p ciclico di ordine p^n. Dimostriamo allora il

TEOREMA 3. - *Se* $\mathfrak{G}$ *ha la proprietà* P *ed è il prodotto diretto di un numero finito di gruppi ciclici allora* $\mathfrak{G}$ *è ciclico.*

Consideriamo prima il caso che G sia un gruppo di torsione e di conseguenza, nelle nostre ipotesi, finito. Siccome un gruppo di torsione finito è il prodotto di gruppi ciclici primari, potremo pensare che sia

$$G = Z(p_1^{n_1}) \times Z(p_2^{n_2}) \times \dots .$$

Se i numeri primi $p_1, p_2, \dots$ sono tutti differenti, allora G è un gruppo ciclico. Basterà dunque mostrare che non può essere ad esempio $p_1 = p_2 = p$. Siano g_1 e g_2 due generatori rispettivamente di $Z(p^{n_1})$ e di $Z(p^{n_2})$ e supponiamo $n_1 \geq n_2$. Nel generico elemento di $Z(p_1^{n_1})$, g_1^r, operiamo la sostituzione $g_1 \rightarrow g_1 g_2$, lasciando inalterati gli altri fattori diretti di G. Allora $g_1^r g_2^s \rightarrow g_1^r g_2^t$, con $t \equiv r + s \pmod{p^{n_2}}$. La trasformazione è dunque invertibile. Inoltre, avendosi $g_1^{r_1} g_2^{s_1} \rightarrow g_1^{r_1} g_2^{t_1}$, con $t_1 \equiv r_1 + s_1 \pmod{p^{n_2}}$, è anche $g_1^r g_2^s \cdot g_1^{r_1} g_2^{s_1} = g_1^{r_2} g_2^{s_2} \rightarrow g_1^{r_2} g_2^{t_2}$, con $r_2 \equiv r + r_1 \pmod{p^{n_1}}$, $s_2 \equiv s + s_1 \pmod{p^{n_2}}$, $t_2 \equiv r_2 + s_2 \equiv r + s + r_1 + s_1 \equiv t + t_1 \pmod{p^{n_2}}$. Quindi $g_1^{r_2} g_2^{t_2} = g_1^r g_2^t \cdot g_1^{r_1} g_2^{t_1}$. La trasformazione genera dunque un automorfismo in G per effetto del quale $| g_1 | \rightarrow | g_1 g_2 |$ contrariamente all'ipotesi fatta su G. G è dunque ciclico.

Se invece G è senza torsione, tenuto conto che due gruppi ciclici aperiodici sono isomorfi, si ricava ancora che G è ciclico. Infatti se fosse $G = A_1 \times A_2 \times \dots \times A_r$, con $A_1, A_2, \dots, A_r$ gruppi ciclici infiniti, detto a_i un generatore di A_i, la corrispondenza $a_1 \rightarrow a_2$, $a_2 \rightarrow a_1$, $a_i \rightarrow a_i$ $(i > 2)$ sarebbe un automorfismo di G, che non muta in sè il sottogruppo ciclico A_1. Basterà allora far vedere che G non può contenere insieme elementi periodici ed elementi aperiodici perchè il teorema sia dimostrato. Anzitutto, sarà $G = M \times N$, con M senza torsione ed N di torsione, e poichè M ed N devono anch'essi godere della proprietà P, M ed N devono essere, per quanto precede, uno ciclico infinito, l'altro ciclico finito. Detti dunque a un generatore di M e g, di periodo n, un generatore di N, per effetto della trasformazione $a \rightarrow ag$, $g \rightarrow g$ si ha $a^r g^s \rightarrow a^r g^r g^s = a^r g^t$ con $t \equiv r + s \pmod{n}$. La trasformazione è dunque invertibile. Analogamente $a^{r_1} g^{s_1} \rightarrow a^{r_1} g^{t_1}$ con $t_1 \equiv r_1 + s_1 \pmod{n}$. Inoltre $a^r g^s \cdot a^{r_1} g^{s_1} = a^{r+r_1} \cdot g^{s_2} \rightarrow a^{r+r_1} g^{t_2}$, essendo $s_2 \equiv s + s_1 \pmod{n}$, $t_2 \equiv r + r_1 + s_2 \equiv r + r_1 + s + s_1 \equiv t + t_1 \pmod{n}$. Quindi $a^r g^s \cdot a^{r_1} g^{s_1} \rightarrow a^r g^t \cdot a^{r_1} g^{t_1}$. La trasformazione genera dunque un automorfismo che porta $| a |$ in $| ag |$, onde l'assurdo.

Da questo teorema, siccome un gruppo abeliano finito è il prodotto diretto di gruppi ciclici, risulta il

COROLLARIO. – *Se* G *è finito ed ha la proprietà* P, *allora* G *è ciclico.*

Risulta ora immediato ricavare il risultato di F. SZASZ a proposito dei gruppi G tali che ogni loro sottogruppo ciclico è una potenza di G. Infatti, come osserva F. SZASZ, si vede subito che G, nelle ipotesi fatte, o è un gruppo finito oppure è un gruppo senza torsione. Infatti se G contiene un gruppo ciclico finito, di ordine n, per ipotesi uguale a una potenza, G^k, di G, allora di conseguenza G^{kn} è l'identità. L'insieme delle potenze differenti di G è dunque finito, di conseguenza è finito l'insieme dei gruppi ciclici di G che risulta finito. Per il teorema 3 (che in tal caso può dimostrarsi nel modo abbreviato) allora G è ciclico. Se invece G è senza torsione, allora, per essere abeliano, è isomorfo a qualunque sua potenza. Ma per ipotesi qualche potenza di G è un gruppo ciclico, quindi G è ciclico.

Si ammetta d'ora in poi il postulato di ZERMELO. In questa ipotesi si prova che un gruppo abeliano di torsione con (almeno) un elemento di periodo massimo è il prodotto diretto di gruppi ciclici [4] [5]. Il ragionamento fatto per provare il teorema 3 prova allora che

TEOREMA 4. – *Se* G *è un gruppo di torsione con (almeno) un elemento di periodo massimo ed ha la proprietà* P, *allora* G *è ciclico.*

Indichiamo ora con $Z(p^\infty)$ un gruppo isomorfo al gruppo moltiplicativo delle radici dell'unità positiva i cui indici sono potenze qualsiasi dell'intero primo p. Per il teorema 1, $Z(p^\infty)$ ha la proprietà P. Infatti ogni sottogruppo di $Z(p^\infty)$ di ordine finito è ciclico. D'altronde si sa che un gruppo di torsione indecomponibile è un gruppo ciclico primario o isomorfo, per un conveniente intero primo, a $Z(p^\infty)$ [4] [5]. Risulta allora evidente che

TEOREMA 5. – *Se* G *è un gruppo di torsione indecomponibile senza elementi di periodo massimo ed ha la proprietà* P, *allora* G *è isomorfo a* $Z(p^\infty)$, *essendo* p *un conveniente intero primo.*

Osserviamo ora che se G ha la proprietà P, due suoi fattori diretti indecomponibili non sono mai primari rispetto allo stesso numero primo. Infatti $Z(p^n) \times Z(p^m)$ non ha la proprietà P, come risulta dal teorema 3;

$Z(p^n) \times Z(q^m)$, $p \neq q$, è ciclico e quindi ha la proprietà P;

$Z(p^n) \times Z(q^\infty)$, $Z(p^\infty) \times Z(q^\infty)$, $p \neq q$, hanno la proprietà P ed ogni loro sottogruppo di ordine finito è ciclico;

$Z(p^\infty) \times Z(p^\infty)$, $Z(p^n) \times Z(p^\infty)$ non hanno la proprietà P. Il fatto è evidente per il primo dei due; per dimostrare che il secondo non ha la proprietà P, basterà supporre che $Z(p^\infty)$ sia il gruppo delle radici dell'unità positiva di indice uguale alle potenze del numero primo p e far vedere che, se a è un generatore di $Z(p^n)$ e b_{p^s} la radice dell'unità di indice p^s di argomento positivo minimo, esiste un automorfismo di $Z(p^n) \times Z(p^\infty)$ che muta a in ab_p e lascia fermo $Z(p^\infty)$. Infatti, per effetto della trasformazione indicata $a^\alpha b_{p^s}^\beta \rightarrow a^\alpha b_p^\alpha b_{p^s}^\beta = a^\alpha b_{p^s}^{p^{s-1}\alpha} b_{p^s}^\beta = a^\alpha b_{p^s}^{p^{s-1}\alpha+\beta}$. La trasformazione è dunque invertibile. Inoltre $a^{\alpha_1} b_{p^{s_1}}^{\beta_1} \rightarrow a^{\alpha_1} b_{p^{s_1}}^{p^{s_1-1}\alpha_1+\beta_1}$ e, se $s \geq s_1$ e γ è il resto di $\alpha + \alpha_1 \pmod{p^n}$, $a^\alpha b_{p^s}^\beta \cdot a^{\alpha_1} b_{p^{s_1}}^{\beta_1} = a^\gamma b_{p^s}^\beta b_{p^s}^{p^{s-s_1}\beta_1} \rightarrow$ $\rightarrow a^\gamma b_{p^s}^{\beta+p^{s-s_1}\beta_1+p^{s-1}\gamma}$. D'altra parte, siccome $p^{s-1}(\alpha + \alpha_1) \equiv p^{s-1}\gamma \pmod{p^s}$, si ha

$$b_{p^s}^{p^{s-1}\alpha+\beta} \cdot b_{p^{s_1}}^{p^{s_1-1}\alpha_1+\beta_1} = b_{p^s}^{p^{s-1}\alpha+\beta+p^{s-s_1}(p^{s_1-1}\alpha_1+\beta_1)} =$$

$$= b_{p^s}^{p^{s-1}(\alpha+\alpha_1)+p^{s-s_1}\beta_1+\beta} = b_{p^s}^{p^{s-1}\gamma+p^{s-s_1}\beta_1+\beta}.$$

È dunque dimostrata l'esistenza dell'automorfismo indicato.

Diciamo ora *divisibile* un gruppo abeliano G tale che per ogni x in G e ogni intero n esista un elemento y di G per cui $y^n = x$; in altre parole G è detto divisibile se $G = G^n$ per ogni intero n. Diciamo poi *ridotto* un gruppo abeliano che non abbia sottogruppi divisibili. Possiamo dimostrare che

TEOREMA 6. - *Se* G *è un gruppo di torsione ed ha la proprietà* P, *allora è il prodotto diretto di gruppi primari indecomponibili relativi a numeri primi tutti differenti ed è quindi isomorfo a un sottogruppo (proprio o improprio) del gruppo di tutte le radici dell'unità positiva. Precisamente, se* G *è ridotto, è il prodotto diretto di gruppi ciclici; se* G *è divisibile, è il prodotto diretto di gruppi del tipo* $Z(p^\infty)$; *contiene fattori diretti indecomponibili dei due tipi nel caso rimanente.*

Sia G ridotto e non si riduca alla sola identità; si sa allora che G ha un fattore diretto finito [4] [5] che per il corollario del teorema 3 risulta ciclico.

Quindi

$$G = Z(p_1^{n_1}) \times A$$

ed A è un gruppo ridotto di torsione. Supponiamo allora

$$G = R \times Z(p_1^{n_1}) \times Z(p_2^{n_2}) \times \dots ;$$

i numeri primi $p_1, p_2, \dots$ saranno tutti differenti e si potrà ulteriormente supporre che R, necessariamente ridotto, non contenga altri fattori diretti di tipo $Z(p^n)$. Allora R è necessariamente identico, perchè se non lo fosse, conterrebbe un fattore di tipo $Z(p^n)$. Quindi

$$G = Z(p_1^{n_1}) \times Z(p_2^{n_2}) \times \dots .$$

Sia G divisibile. È noto che un qualunque gruppo divisibile è il prodotto diretto di gruppi di tipo $Z(p^\infty)$ e di gruppi che, rappresentati additivamente, sono isomorfi al gruppo additivo dei numeri razionali [4] [5]. Siccome questi ultimi non sono gruppi di torsione, in questo caso

$$G = Z(p_1^\infty) \times Z(p_2^\infty) \times \dots ,$$

ed ancora i numeri primi $p_1, p_2, \dots$ sono tutti differenti.

Consideriamo il caso rimanente. Siccome due fattori diretti di G non sono mai primari rispetto allo stesso numero primo e poichè un sottogruppo divisibile di un gruppo abeliano è un fattore diretto [4] [5], si può supporre che G sia il prodotto di un gruppo ridotto e di uno divisibile. Quindi

$$G = Z(p_1^{n_1}) \times Z(p_2^{n_2}) \times \dots \times Z(q_1^\infty) \times Z(q_2^\infty) \times \dots ,$$

e due qualsiasi dei numeri primi $p_1, p_2, \dots, q_1, q_2, \dots$ non sono mai uguali. Tenuto conto che in tutti e tre i casi G risulta un sottogruppo di un gruppo isomorfo al gruppo di tutte le radici dell'unità, risulta completamente dimostrato il teorema.

Risulta dal teorema precedente il seguente

COROLLARIO. - *Se* $\mathfrak{G}$ *è un gruppo abeliano di torsione ed ogni suo sottogruppo di ordine finito è ciclico, allora* $\mathfrak{G}$ *è isomorfo a un sottogruppo del gruppo di tutte le radici dell'unità positiva.*

Infatti G, per il teorema 1, ha la proprietà P. Dal teorema precedente risulta allora l'asserto.

Dimostriamo il

TEOREMA 7. - *Se* $\mathfrak{G}$ *ha la proprietà* $\mathfrak{P}$ *o è un gruppo di torsione o è un gruppo indecomponibile senza torsione oppure è il prodotto diretto di un gruppo indecomponibile senza torsione per un gruppo di ordine due.*

Cominciamo col dimostrare che, se G ha la proprietà P e non è un gruppo di torsione, ammette soltanto due automorfismi, quello identico e quello che trasforma ogni elemento di G nel suo inverso. Poichè G, per ipotesi, non è di torsione, deve contenere almeno un elemento, a, aperiodico. Poichè G ha la proprietà P, un automorfismo di G deve mutare $|a|$ in sè, quindi a in sè o a in a^{-1}. Mostriamo che un automorfismo di G che muta a in sè, muta in sè ogni elemento di G; e se muta a nell'inverso, muta nell'inverso ogni elemento di G. Sia in primo luogo $\mathfrak{s}$ un automorfismo che muti a in sè, e sia b un altro elemento di G. Se b è periodico, ab è aperiodico, e si ha $(ab)^{\mathfrak{s}} = ab$ oppure $(ab)^{\mathfrak{s}} = (ab)^{-1}$. D'altra parte $(ab)^{\mathfrak{s}} = a^{\mathfrak{s}}b^{\mathfrak{s}} = ab^{\mathfrak{s}}$. Dovrà quindi aversi $ab^{\mathfrak{s}} = ab$, oppure $ab^{\mathfrak{s}} = a^{-1}b^{-1}$. Nel primo caso è $b^{\mathfrak{s}} = b$, nel secondo si avrebbe $ab^{\mathfrak{s}} = a^{-1}b^{-1}$, onde $a^{-2} = b \cdot b^{\mathfrak{s}}$; e poichè, per la proprietà P, è $b^{\mathfrak{s}} = b^{x}$, per un conveniente x si avrebbe $a^{-2} = b^{1+x}$, il che è assurdo, perchè a^{-2} è aperiodico e b^{1+x} periodico. Sia ora invece c un elemento aperiodico di G. Sarà $c^{\mathfrak{s}} = c$, oppure $c^{\mathfrak{s}} = c^{-1}$. Ma se fosse $c^{\mathfrak{s}} = c^{-1}$, si avrebbe $(ac)^{\mathfrak{s}} = ac^{-1}$, e allora, se ac è periodico, dovrebbe aversi, per quanto si è visto, $(ac)^{\mathfrak{s}} = ac$, onde $ac = ac^{-1}$, $c = c^{-1}$, e pertanto ancora $c^{\mathfrak{s}} = c$; mentre, se ac è aperiodico, si avrebbe $(ac)^{\mathfrak{s}} = ac$, e allora seguirebbe, come sopra, $c^{\mathfrak{s}} = c$, oppure si avrebbe $(ac)^{\mathfrak{s}} = a^{-1}c^{-1}$, e allora sarebbe $ac^{-1} = a^{-1}c^{-1}$, cioè $a = a^{-1}$, contro l'ipotesi che a sia aperiodico. Pertanto, se è $a^{\mathfrak{s}} = a$, è anche $b^{\mathfrak{s}} = b$, qualunque sia b in G.

Sia ora, invece, $\mathfrak{s}$ un automorfismo che muta a in a^{-1}, e sia b un altro elemento di G. Allora, se b è periodico, ab è aperiodico, e si ha $(ab)^{\mathfrak{s}} = a^{-1}b^{-1}$, perchè se fosse $(ab)^{\mathfrak{s}} = ab$, sarebbe $x^{\mathfrak{s}} = x$ per ogni x di G (per il caso precedente) onde anche $a^{\mathfrak{s}} = a$, contro l'ipotesi. Da $(ab)^{\mathfrak{s}} = a^{-1}b^{-1}$, $(ab)^{\mathfrak{s}} = a^{-1}b^{\mathfrak{s}}$ segue $b^{\mathfrak{s}} = b^{-1}$. Se poi b è aperiodico, deve essere $b^{\mathfrak{s}} = b^{-1}$, perchè se fosse $b^{\mathfrak{s}} = b$, per il caso precedente, sarebbe anche $a^{\mathfrak{s}} = a$, contro l'ipotesi.

Supponiamo allora G non di torsione, dotato della proprietà P, e decomponibile nel prodotto diretto $A \times B$ di due sottogruppi propri A e B. Possiamo definire un automorfismo φ di G che subordini in A l'automorfismo identico, e in B l'automorfismo che muti ogni elemento nel suo inverso. Per quanto abbiamo ora visto, φ dovrà in G stesso coincidere o con l'automorfismo identico, o con quello che muta ogni elemento nell'inverso. Affinchè ciò sia, occorre che in almeno uno dei fattori A e B l'automorfismo identico coincida con quello che muta ogni elemento nel proprio inverso; occorre quindi che in A, o in B, ogni elemento coincida col proprio inverso. Supponiamo ciò avvenga per A. Si ha allora

che anche A, come fattore diretto di G, ha la proprietà P, quindi, per il teorema 4, A è ciclico di ordine due. È subito visto che B non può essere decomponibile. Se lo fosse, tenuto conto del ragionamento precedente, dovrebbe contenere un fattore diretto C di ordine due e quindi isomorfo ad A e si avrebbe $G = A \times C \times D$ con D conveniente fattore diretto, onde si potrebbe definire in G un automorfismo che scambi i fattori diretti A e C di G, lasciando inalterati gli elementi di D, e ciò è assurdo, perchè per ipotesi G ha la proprietà P. Tenuto conto che un gruppo indecomponibile o è un gruppo di torsione o è un gruppo senza torsione [4] [5], risulta completamente dimostrato il teorema.

Chiamiamo *pienamente invariante* un sottogruppo di un gruppo G mutato in sè o in un suo sottogruppo da ogni endomorfismo di G. Sussiste il seguente

TEOREMA 8. - *Se ogni sottogruppo ciclico del gruppo* G *è pienamente invariante,* G *o è un gruppo indecomponibile senza torsione, o è un gruppo di torsione.*

Siccome un sottogruppo pienamente invariante è anche un sottogruppo caratteristico, tenuto conto del teorema 7, basterà dimostrare che G non può essere il prodotto diretto di un gruppo indecomponibile senza torsione per un gruppo di ordine due. Infatti, per assurdo, sia A un gruppo indecomponibile senza torsione e B un gruppo di ordine due e sia $G = A \times B$; se a e b sono due elementi qualsiasi rispettivamente di A e di B, la trasformazione $a \rightarrow a$, $b \rightarrow b^2$ è un endomorfismo. Infatti la trasformazione ad ogni elemento di G associa uno ed un solo elemento dello stesso gruppo; inoltre, se a_1 e b_1 sono altri due elementi rispettivamente di A e di B, si ha $a_1 \rightarrow a_1$, $b_1 \rightarrow b_1^2$ e $ab \cdot a_1 b_1 = aa_1 \cdot bb_1 \rightarrow aa_1 b^2 b_1^2 = ab^2 \cdot a_1 b_1^2$. Quindi la trasformazione conserva l'operazione di prodotto. D'altra parte se b è il generatore di B, per effetto di tale trasformazione $|ab| \rightarrow |a|$. Siccome $|a|$ non è un sottogruppo di $|ab|$ si ha l'assurdo e il teorema è dimostrato.

Dato il numero primo p si dicono *interi* p-*adici* le serie α della forma

$$\alpha = a_0 + a_1 p + \ldots + a_i p^i + \ldots = \sum_{i}^{1 \ldots \infty} a_i p^i,$$

essendo gli a_i interi razionali tali che $0 \leq a_i < p$. Rispetto all'operazione di addizione (che si effettua con la regola di addizione degli interi razionali scritti in base p) gli interi p-adici formano un gruppo. È noto che tale gruppo additivo è indecomponibile e senza torsione [5]. Dimostriamo che

TEOREMA 9. - *Il gruppo additivo indecomponibile senza torsione degli interi* p-*adici non ha la proprietà* P.

Cominciamo col far vedere che la trasformazione $\alpha \rightarrow (p+1)\alpha$ è un automorfismo.

$$(p+1)\alpha = p\alpha + \alpha = a_0 + b_1 p + \ldots + b_r p^r + \ldots ,$$

dove

$$b_1 = a_0 + a_1 - \varepsilon_1 p$$
$$b_2 = a_1 + a_2 + \varepsilon_1 - \varepsilon_2 p$$
$$\ldots\ldots$$

e $\varepsilon_0 = 0$; $\varepsilon_i = 0$, se $a_{i-1} + a_i + \varepsilon_{i-1} < p$; $\varepsilon_i = 1$, se $a_{i-1} + a_i + \varepsilon_{i-1} \geq p$ $(1 \leq i < \infty)$. Dalle precedenti relazioni si ha

$$a_1 = b_1 - a_0 + \varepsilon_1 p$$
$$a_2 = b_2 - a_1 - \varepsilon_1 + \varepsilon_2 p$$
$$\ldots\ldots$$

Da queste, fissati gli interi razionali non negativi $a_0, b_1, b_2, \ldots$, ciascuno minore di p, per la condizione $0 \leq a_i < p$, risultano univocamente determinati, insieme a $\varepsilon_1, \varepsilon_2, \ldots$, anche $a_1, a_2, \ldots$. La trasformazione è dunque invertibile. Inoltre, se $\beta \rightarrow (p+1)\beta$, allora $\alpha + \beta \rightarrow (p+1)(\alpha+\beta) = (p+1)\alpha + (p+1)\beta$. D'altra parte, siccome $M = \{1 + 0p + 0p^2 + \ldots\} \rightarrow N = \{1 + p + 0p^2 + 0p^3 + \ldots\}$, ed N è un sottogruppo proprio di M, il gruppo degli interi p-adici non ha la proprietà P, come volevamo dimostrare.

BIBLIOGRAFIA

[1] F. SZASZ, *On groups every cyclic subgroup of wich is a power of the group*, « Acta Math. Acad. Sci. Hungar », VI, (1955), pp. 475-477.

[2] F. SZASZ, *A characterization of the cyclic groups*, « Revue Math. pures et appl. » I, (1956) n. 2, pp. 13-16.

[3] G. ZAPPA, *Sull'ampliamento degli automorfismi*, « Rend. Sem. Mat. Univ. Roma », S. IV, v. 3, (1939) pp. 133-138.

[4] A. G. KUROSCH, *Gruppentheorie*, « Akademie Verlag Berlin », (1953).

[5] J. KAPLANSKY, *Infinite abelian groups*, University of Michigan press (1954).