ATTI

DELLA

REALE ACCADEMIA DEI LINCEI

ANNO CCXCV.

1898

SERIE QUINTA

RENDICONTI

Classe di scienze fisiche, matematiche e naturali.

VOLUME VII.

1° SEMESTRE

ROMA

TIPOGRAFIA DELLA R. ACCADEMIA DEI LINCEI

PROPRIETÀ DEL CAV. V. SALVIUCCI

1898

Matematica. — *Sopra i divisori normali d'indice primo di un gruppo finito.* Nota del dott. G. Bagnera, presentata dal Socio Luigi Bianchi.

1. In alcune questioni che mi sono proposto, riguardanti la composizione dei gruppi finiti, ho avuto spesso bisogno di sapere il numero dei divisori normali di un dato indice primo p, contenuti in un gruppo finito G, nell'ipotesi che il gruppo G possegga divisori normali di detto indice.

Se r è il numero di tali divisori, io ho dimostrato che esso è della forma

$$\frac{p^r - 1}{p - 1};$$

inoltre, ho fatto vedere che il gruppo G è allora isomorfo, almeno meriedricamente, ad un gruppo commutativo di grado p^r che ha tutti gl'invarianti eguali a p.

Questi risultati mi sembrano non privi d'interesse perchè, in alcuni casi importanti, sono di grande ausilio nella trattazione del difficilissimo problema enunciato dal Cayley (1), quello, cioè, di trovare tutti i possibili gruppi di un dato grado n; sicchè, non credo inutile esporre qui l'analisi di cui mi son servito per stabilirli, tanto più che essa è molto semplice per chi è familiare con la teoria dei gruppi finiti.

2. Sia G un tale gruppo il quale possegga r divisori normali distinti di indice primo p: $G_1, G_2, \ldots, G_r$. Dico che la loro intersezione ha, in G, un indice che è un divisore di p^r. Infatti, G_1 e G_2 sono due divisori normali massimi distinti di G e quindi, come è noto (2), la loro intersezione $[G_1, G_2]$ ha, in G_1, lo stesso indice che G_2 ha in G, cioè p; dunque, $[G_1, G_2]$ ha, in G, l'indice p^2. Se i gruppi $G_3, G_4, \ldots G_r$ ammettono il divisore $[G_1, G_2]$, allora, l'intersezione $[G_1, G_2, G_3, \ldots, G_r]$ coincide con $[G_1, G_2]$; diversamente, uno di essi, G_3, non avrà detto divisore. In questo caso, $[G_1, G_2]$ e $[G_1, G_3]$ sono due divisori normali distinti di G_1, d'indice p, quindi la loro intersezione $[G_1, G_2, G_3]$ ha l'indice p in $[G_1, G_2]$ e l'indice p^3 in G. Se i gruppi $G_4, \ldots, G_r$ ammettono il divisore $[G_1, G_2, G_3]$, allora l'intersezione $[G_1, G_2, G_3, \ldots, G_r]$ coincide con $[G_1, G_2, G_3]$; diversamente, uno di essi, G_4, non avrà detto divisore. In questo caso, $[G_1, G_2, G_3]$ e $[G_1, G_2, G_4]$

(1) Nell'American Journal of Mathematics, vol. I, pag. 50.

(2) H. Weber, Lehrbuch der Algebra, vol. II, pag. 22.

sono due divisori normali distinti di $[G_1, G_2]$ d'indice p, quindi la loro intersezione $[G_1, G_2, G_3, G_4]$ ha l'indice p in $[G_1, G_2, G_3]$ e l'indice p^4 in G.

Continuando a ragionare in questo modo, si conclude che l'indice di $[G_1, G_2, \ldots, G_r]$, in G, è p^λ, essendo $1 \leq \lambda \leq r$; inoltre, se $\lambda < r$, l'intersezione dei divisori $G_1, G_2, \ldots G_r$ coincide con l'intersezione di λ di essi convenientemente scelti.

Ciò posto, chiamo i divisori $G_1, G_2, \ldots, G_r$ *indipendenti* se è $\lambda = r$, in altri termini, se la loro intersezione ha, nel gruppo principale G, precisamente l'indice p^r.

Due divisori normali distinti, d'indice p, sono sempre indipendenti. Se più divisori normali d'indice p, $G_1, G_2, \ldots, G_r$, sono indipendenti, una parte qualunque di essi sono indipendenti. Infatti, se, essendo $s < r$, l'indice di $[G_1, G_2, \ldots, G_s]$, in G, non è p^s, si possono scegliere $\lambda < s$ divisori, $G_1, G_2, \ldots, G_\lambda$, in modo che

$$[G_1, G_2, \ldots, G_\lambda] = [G_1, G_2, \ldots, G_s];$$

allora, essendo

$$[G_1, G_2, \ldots, G_\lambda, G_{s+1}, \ldots, G_r] = [G_1, G_2, \ldots, G_s, G_{s+1}, \ldots, G_r],$$

l'indice di $[G_1, G_2, \ldots, G_r]$, in G, sarà un divisore di $p^{r+\lambda-s}$ e quindi inferiore a p^r.

3. Chiamo, per brevità, T l'intersezione di r divisori normali indipendenti, $G_1, G_2, \ldots, G_r$, d'indice p rispetto ad un gruppo finito G. Dico che il gruppo complementare a T, in G, che è di grado p^r e che denoto, secondo l'uso, col simbolo G/T, ha tutti i suoi elementi di grado p.

Se a è un elemento qualunque di G non contenuto nel divisore normale T, aT sarà un elemento di G/T diverso dall'elemento unitario T, e giacchè si ha

$$(a\mathrm{T})^p = a^p\mathrm{T},$$

basta far vedere che a^p appartiene a T. Ora, a^p appartiene a ciascuno dei gruppi $G_1, G_2, \ldots, G_r$, perchè $aG_1, aG_2, \ldots, aG_r$ sono elementi dei rispettivi gruppi complementari in G, i quali gruppi hanno il grado comune p; dunque, a^p appartiene a

$$\mathrm{T} = [G_1, G_2, \ldots, G_r].$$

Dippiù, il gruppo G/T è commutativo (Abeliano). Ciò è vero per $r = 1$ ed $r = 2$, perchè ogni gruppo di grado p o di grado p^2 [1] è commutativo; quindi, suppongo che il fatto si verifichi quando il numero dei divisori normali indipendenti d'indice p è inferiore ad r e dimostro che si verifica ancora allorchè detto numero è r.

[1] Netto, *Substitutionentheorie und ihre Anwendung auf die Algebra*, 1882, pag. 133.

I gruppi $[G_1, G_2], [G_1, G_3], \ldots, [G_1, G_r]$ sono $r-1$ divisori normali di G_1 d'indice p e sono indipendenti, perchè la loro intersezione T ha in G_1 l'indice p^{r-1}; dunque, il gruppo G_1/T, che è un divisore normale d'indice p di G/T, è commutativo per ipotesi. Il gruppo

$$N = [G_2, G_3, \ldots, G_r],$$

che è d'indice p^{r-1} in G, non è contenuto in G_1, perchè $G_1, G_2, \ldots, G_r$ sono, per ipotesi, indipendenti e quindi G_1/T non contiene il gruppo ciclico, di grado p, N/T.

Ciò posto, dato un elemento qualunque E di G/T, si può, in una maniera sola, scegliere un elemento A di N/T ed un elemento B di G_1/T in modo che sia

$$E = A.B;$$

dunque, per dimostrare che il gruppo G/T è commutativo, basta provare che ogni elemento A di N/T è permutabile con ogni elemento B di G_1/T. Ora, giacchè N/T è un divisore normale ciclico di G/T, si deve avere

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

donde

$$B^{-p}AB^{p} = A^{\alpha^{p}},$$

ed essendo B un elemento di grado p, sarà

$$\alpha^{p} - 1 \equiv 0 \pmod{p}.$$

D'altronde, per il teorema di Fermat, è

$$\alpha^{p} - \alpha \equiv 0 \pmod{p};$$

quindi,

$$\alpha \equiv 1 \pmod{p}$$

e conseguentemente

$$AB = BA.$$

4. Se r è il massimo numero di divisori normali indipendenti d'indice p che possiede il gruppo G, allora qualsiasi divisore normale di G di tale indice contiene T, ed il rispettivo gruppo complementare di T, in detto divisore, è un sottogruppo di G/T di grado p^{r-1}; dunque, il numero dei divisori normali d'indice p di G è lo stesso del numero dei divisori di grado p^{r-1} di G/T.

M'interessa quindi sapere, più generalmente, il numero dei divisori di grado p^{λ} di un gruppo Abeliano di grado p^{r} che ha tutti i suoi invarianti eguali a p.

Io considero un elemento E diverso dall'unità di un tale gruppo e penso al gruppo ciclico di grado p formato dalle potenze di E; poi, prendendo un altro elemento E_1 fuori di detto gruppo ciclico, penso al gruppo formato dalle potenze di E_1; .... e così continuo fino ad esaurire i $p^r - 1$ elementi, diversi dall'unità, contenuti nel gruppo dato. Dal momento che ognuno di detti gruppi ciclici contiene soltanto $p - 1$ di tali elementi, concludo che il numero dei divisori di grado p è

$$\nu_1 = \frac{p^r - 1}{p - 1}.$$

Per trovare il numero ν_2 dei divisori di grado p^2 considero tutti quelli che hanno uno stesso divisore di grado p, il cui numero è quello dei sottogruppi di grado p che possiede il gruppo complementare di detto divisore, cioè $\frac{p^{r-1} - 1}{p - 1}$: ottengo così $\frac{p^r - 1}{p - 1} \cdot \frac{p^{r-1} - 1}{p - 1}$ divisori di grado p^2; ma ognuno, giacchè ha $\frac{p^2 - 1}{p - 1}$ divisori di grado p, viene ad essere contato precisamente $\frac{p^2 - 1}{p - 1}$ volte; quindi,

$$\nu_2 = \frac{(p^r - 1)(p^{r-1} - 1)}{(p - 1)(p^2 - 1)}.$$

Il ragionamento porta subito alla formola

$$\nu_\lambda = \frac{(p^r - 1)(p^{r-1} - 1) \dots (p^{r-\lambda+1} - 1)}{(p - 1)(p^2 - 1) \dots (p^\lambda - 1)},$$

dove, ponendo $\lambda = r - 1$, si ottiene il numero

$$\nu_{r-1} = \frac{p^r - 1}{p - 1},$$

il quale coincide, per quello che si è detto, col numero ν dei divisori normali d'indice p di G.

5. Termino col fare un'applicazione dei risultati precedenti alla composizione di un gruppo P, il cui grado è una potenza p^k di un numero primo p. Per un teorema dovuto a Sylow [1], un tale gruppo ha certamente dei divisori d'indice p, e si può ancora asserire che qualunque divisore di detto indice è normale [2].

Ciò posto, sia G un divisore normale di P, e si pensino tutti i ν divisori del gruppo G, che hanno l'indice p rispetto a questo gruppo: essi,

[1] H. Weber, Lehrbuch der Algebra, vol. II, pag. 122.
[2] H. Weber, l. c., pag. 128.

come si è detto, sono normali in G, ed io aggiungo che ne esiste almeno uno che è normale anche in P. Infatti, se G_1 è un divisore di G d'indice p, che non è normale in P, il numero dei suoi trasformati distinti è uguale all'indice, in P, del gruppo formato dagli elementi di P invertibili con G_1, e, siccome questo gruppo non coincide con P, detto numero è un multiplo di p. Allora, tutti i trasformati di G_1, non possono esaurire i r divisori di G considerati, perchè, da quello che ho già stabilito, risulta che

$$r \equiv 1 \pmod{p};$$

quindi, esisterà almeno un divisore di G, d'indice p, che non è un trasformato di G_1 in P. Se questo nuovo divisore non è normale in P, tutti i suoi trasformati distinti, il cui numero è multiplo di p, non esauriscono ancora i r divisori di G considerati; e continuando in tale modo, debbo necessariamente essere arrestato dalla presenza di un divisore d'indice p in G e normale in P.

Sia ora P_1 un divisore d'indice p del gruppo P. Tra i divisori di P_1, d'indice p, ve ne sono di quelli che sono normali in P e sia P_2 uno di questi; poi, tra i divisori di P_2, d'indice p, ve ne sono di quelli che sono normali in P e sia P_3 uno di questi;.... così procedendo, si vede che è possibile costruire una *serie di composizione* del gruppo P:

$$P, P_1, P_2, P_3, \ldots, P_{k-1}$$

tale che, ogni gruppo della serie, è divisore normale di tutti quelli che lo precedono.

Io chiamo, brevemente, una tale serie una *serie canonica di composizione* e mi riservo di ritornare fra breve su questo argomento.

Fisica. — *Sulla diffusione dei raggi Röntgen.* Nota dei dottori R. Malagoli e C. Bonacini, presentata dal Socio Blaserna.

Questa Nota sarà pubblicata nel prossimo fascicolo.

Fisica terrestre — *Sulla velocità di propagazione del terremoto d'Aidin* (Asia M.) *del 19 agosto 1895.* Nota di G. Agamennone, presentata dal Socio P. Tacchini.

L'interesse che presenta lo studio della velocità, con cui si propagano le onde sismiche, va crescendo ogni dì più, a causa delle importanti questioni sulla costituzione interna del nostro globo che si riattaccano a tale studio. Oggi più che mai simili ricerche sono feconde in risultati, grazie ai moderni strumenti ben superiori agli antichi, vuoi per una più esatta determinazione