Bollettino
Unione Matematica Italiana

Gaetano Villari

Sui commutatori del gruppo modulare.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **13** (1958), n.2, p. 196–201.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1958_3_13_2_196_0>

Sui commutatori del gruppo modulare.

Nota di GAETANO VILLARI (a Firenze)

Sunto. - *Si dimostra che per* $p > 3$ (p *numero primo*) *gli elementi del gruppo modulare* G_p *sono tutti commutatori.*

Summary. - *It is shown that for* $p > 3$ (p *prime number*) *the elements of the modular group* G_p *are all commutators.*

1. Sia G un gruppo, ed indichi G' il suo derivato. Non sempre accade, come è noto. che ogni elemento di G' sia un commutatore di G, o, in altre parole, che il prodotto di un numero qualunque di commutatori sia sempre un commutatore; è perciò naturale domandarsi come possano riconoscersi quei gruppi che godono della proprietà sopra indicata.

In particolare, se il gruppo G è perfetto ($G \equiv G'$), si tratta di stabilire se ogni elemento di G è un commutatore (1).

Criteri di carattere generale, atti ad accertare o ad escludere per un generico gruppo la proprietà in oggetto, non sembra siano stati finora segnalati; è stato invece studiato direttamente in alcuni casi il comportamento di singoli gruppi.

Ad esempio è stato provato (2) che nel gruppo finito simmetrico Σ_n ogni elemento del gruppo alterno è un commutatore, e per $n \geq 5$ ogni elemento del gruppo alterno risulta commutatore di elementi del gruppo stesso. Pertanto, sia nel gruppo simmetrico che. per $n \geq 5$, nel gruppo alterno, il prodotto di due o più commutatori è ancora un commutatore. Altrettanto avviene, come subito si vede. anche per $n < 5$.

In questa Nota mi propongo di studiare il comportamento del gruppo modulare G_p, ove p è un numero primo, e di provare una proprietà analoga a quella più sopra segnalata per i gruppi simmetrico ed alterno. Precisamente verrà dimostrato che, per $p > 3$, ogni elemento di G_p è un commutatore, e che anche per $p = 2, 3$, come direttamente si verifica, il prodotto di commutatori è sempre un commutatore.

(1) Cfr. H. HILTON, *An introduction to the theory of groups of finite order*, Oxford Press, 1908; (Appendix, n. 3).

(2) Cfr. O. ORE, *Some remarks on commutators*, Proc. Am. Math. Soc., 2 (1951), 307-314. Cfr. anche N. ITO, *A theorem on the alternating group* U_n ($n \geq 5$), Math. Jap., 2 (1949), 59-60.

2. Sia $p > 3$ un numero primo, ed indichiamo con G_p il relativo gruppo modulare G_p [3], cioè l'insieme delle $p(p+1)(p-1)/2$ sostituzioni sopra i $p+1$ simboli

$$\infty,\ 0,\ 1,\ \ldots,\ p-1,$$

definite dalla legge

$$x' \equiv \frac{\alpha x + \beta}{\gamma x + \delta}, \qquad \alpha\delta - \beta\gamma \equiv 1 \pmod{p}. \tag{1}$$

Indichiamo con $S(a,\ b,\ \infty)$, $b \not\equiv 0 \pmod{p}$, la sostituzione $\begin{pmatrix} b & a \\ 0 & 1/b \end{pmatrix}$ appartenente a G_p [4].

Fissato il valore di b e facendo assumere ad a i valori

$$0,\ 1,\ \ldots,\ p-1, \tag{2}$$

si ottengono allora p sostituzioni che lasciano fermo il simbolo ∞ e sono tra loro tutte distinte. Infatti le sostituzioni $S(a_1,\ b,\ \infty)$, $S(a_2,\ b,\ \infty)$, $a_1 \not\equiv a_2 \pmod{p}$, portano rispettivamente lo zero in ba_1, ba_2, e non possono coincidere.

Osserviamo ancora che, fissato in (2) il valore di a, si ha $S(a,\ p-b,\ \infty) = S(p-a,\ b,\ \infty)$, e pertanto tali simboli, quando a percorre l'insieme (2), rappresentano le medesime sostituzioni.

Inversamente, supponiamo che le sostituzioni $S(a_1,\ b_1,\ \infty)$, $S(a_2,\ b_2,\ \infty)$ coincidano, che cioè si abbia per la (1)

$$b_1\ (b_1\ x + a_1) \equiv b_2\ (b_2\ x + a_2) \pmod{p};$$

facendo allora $x = 0,\ 1$ si ottiene rispettivamente

$$a_1\ b_1 \equiv a_2\ b_2,\ b_2^2 - b_1^2 = (b_2 - b_1)(b_2 + b_1) \equiv 0, \pmod{p},$$

e poichè non può aversi $b_2 - b_1 \equiv 0$, dovrà essere $b_2 = p - b_1$.

Pertanto, facendo assumere ad a i valori (2), e a b i valori

$$1,\ 2,\ \ldots,\ \frac{p-1}{2}, \tag{3}$$

[3] Cfr. L. BIANCHI, *Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois*, Pisa (1900), pp. 90 e sgg.

[4] I numeri α, β, γ, δ si considerano presi rispettò al modulo p; col simbolo a/b si indica il numero intero soluzione della congruenza $bx \equiv a \pmod{p}$.

col simbolo $S(a, b, \infty)$ si rappresentano $p(p-1)/2$ sostituzioni distinte del gruppo G_p, ciascuna delle quali lascia fermo il simbolo ∞.

Indichiamo ancora con $S(a, b, c)$, $b \equiv\!\equiv 0 \pmod{p}$, la sostituzione $\begin{pmatrix} a & -1/b - ac \\ b & -bc \end{pmatrix}$ appartenente a G_p.

Con considerazioni analoghe alle precedenti si vede che, fissati b e c e facendo assumere ad a i valori (2), si ottengono p sostituzioni che portano c in ∞ e sono tra loro tutte distinte.

Si ha pure $S(a, p-b, c) = S(p-a, b, c)$, e pertanto tali simboli, quando a percorre l'insieme (2), rappresentano le medesime sostituzioni. Inversamente, supponendo $S(a_1, b_1, c) = S(a_2, b_2, c)$, discende $b_2 = p - b_1$.

Dunque, fissato c e facendo assumere ad a e b rispettivamente i valori (2) e (3), si ottengono $p(p-1)/2$ sostituzioni distinte di G_p che portano il simbolo c in ∞.

Da ciascuna di queste poi, facendo variare c nell'insieme (2), si ottengono p sostituzioni tutte distinte tra loro e dalle precedenti, e perciò in totale $p^2(p-1)/2$ sostituzioni esprimibili col simbolo $S(a, b, c)$.

Tali sostituzioni risultano distinte da quelle precedentemente espresse col simbolo $S(a, b, \infty)$, e poichè il loro numero complessivo è $p(p+1)(p-1)/2$, che è l'ordine di G_p, possiamo concludere:

Le sostituzioni del gruppo modulare G_p *sono tutte e sole quelle che si esprimono con i simboli*

$$(4) \qquad S(a, b, \infty) \equiv \begin{pmatrix} b & b \\ 0 & 1/b \end{pmatrix}, \qquad \begin{cases} a = 0, 1, \ldots, p-1, \\ b = 1, 2, \ldots, (p-1)/2; \end{cases}$$

$$(5) \qquad S(a, b, c) = \begin{pmatrix} a & -1/b - ac \\ b & -bc \end{pmatrix}, \qquad \begin{cases} a, c = 0, 1, \ldots, p-1, \\ b = 1, 2, \ldots, (p-1)/2. \end{cases}$$

3. Facendo uso di note relazioni sul prodotto di due sostituzioni lineari, facilmente si provano per i simboli (4) e (5) le seguenti identità:

$$(6) \qquad S^{-1}(a, b, c) = \begin{pmatrix} bc & -1/b - ac \\ b & -b\ a/b \end{pmatrix} = S(bc, b, a/b),$$

$$(7) \qquad S^{-1}(a, b, \infty) = \begin{pmatrix} 1/b & -a \\ 0 & b \end{pmatrix} = S(-a, 1/b, \infty).$$

Si ha pure

$$S(a, b, c)S(\alpha, \beta, \gamma) = \begin{pmatrix} \alpha(a - b\gamma) - \dfrac{b}{\beta} & -\dfrac{\alpha}{b} + \dfrac{bc}{\beta} - \alpha c(a - b\gamma) \\ \beta(a - b\gamma) & -\dfrac{\beta}{b} - \beta c(a - b\gamma) \end{pmatrix},$$

e pertanto, ponendo $D = a - b\gamma$:

$$S(a,\ b,\ c)S(\alpha,\ \beta,\ \gamma) = S\left(\frac{\alpha}{b} - \frac{bc}{\beta},\ \frac{b}{\beta},\ \infty\right) \qquad \text{se } D \equiv 0 \pmod{p}; \tag{8}$$

$$S(a,\ b,\ c)S(\alpha,\ \beta,\ \gamma) = S\left(\alpha D - \frac{b}{\beta},\ \beta D,\ c + \frac{1}{bD}\right) \qquad \text{se } D \not\equiv 0 \pmod{p}. \tag{9}$$

Analogamente si ottiene

$$S(a,\ b,\ c)S(\alpha,\ \beta,\ \infty) = S\left(a\beta + \alpha b,\ \frac{b}{\beta},\ c\right), \tag{10}$$

$$S(\alpha,\ \beta,\ \infty)S(a,\ b.\ c) = S\left(a\beta,\ b\beta,\ \frac{c - \alpha\beta}{\beta^2}\right), \tag{11}$$

$$S(a,\ b,\ \infty)S(\alpha,\ \beta,\ \infty) = S\left(a\beta + \frac{\alpha}{b},\ b\beta,\ \infty\right). \tag{12}$$

Indichiamo adesso col simbolo $[S,\ S']$ il commutatore della coppia di sostituzioni $S,\ S'$, ed esaminiamo i commutatori del sottogruppo $\bar{G}_p$ di G_p formato dalle sostituzioni (4) che lasciano fermo il simbolo ∞.

Tenendo conto delle (7) e (12) si ha

$$[S(a,\ b,\infty),\ S(\alpha,\ \beta,\ \infty)] = S\left(-a, \frac{1}{b}, \infty\right) \cdot S\left(-\alpha, \frac{1}{\beta}, \infty\right) \cdot$$
$$\cdot\ S(a,\ b,\infty) \cdot S(\alpha,\ \beta,\infty) = S(K,\ 1,\infty),$$

avendo posto $K = \frac{a}{b} - ab + \frac{\alpha}{b^2\beta} - \alpha b^2\beta$; pertanto i commutatori del gruppo (4) sono sostituzioni della forma $S(a,\ 1,\ \infty)$, $a = 0,\ 1,\ \ldots,\ p-1$.

Inversamente ogni sostituzione del tipo indicato può pensarsi come commutatore di elementi di $\bar{G}_p$, dato che per es. si ha:

$$\left[S(0,\ 2,\ \infty),\ S\left(-\frac{2}{3}a,\ \frac{1}{2}.\ \infty\right)\right] = S(a,\ 1,\ \infty).$$

I commutatori di G_p sono quindi tutte e sole le sostituzioni $S(a,\ 1.\ \infty)(a = 0,\ 1,\ \ldots,\ p-1)$; e poichè il prodotto di due tali sostituzioni è ancora dello stesso tipo, il derivato di $\bar{G}_p$ risulta composto, esclusivamente, di commutatori. Ciò vale ovviamente, per

simmetria, anche per gli altri sottogruppi di G formati dalle sostituzioni che lasciano fisso un dato elemento.

4. Per quanto precede, ogni sostituzione del tipo $S(a, 1, \infty)$ si può considerare come commutatore di elementi di G_p, e mostreremo adesso come ciò sia vero anche per tutti gli altri elementi di G_p.

Per le sostituzioni del tipo $S(0, b, \infty)$ si ha infatti, tenendo conto delle (6), (8) e (9):

$$\left[S\left(\frac{2+b}{1-b}, -\frac{1+2b}{1-b}, -\frac{b(2+b)}{1+2b}\right), S\left(\frac{1+2b}{1-b}, -\frac{1+2b}{b(1-b)}, -1\right)\right] =$$

$$= S\left(\frac{b(2+b)}{1-b}, -\frac{1+2b}{1-b}, -\frac{2+b}{1+2b}\right) S\left(\frac{1+2b}{b(1-b)}, -\frac{1+2b}{b(1-b)}, -b\right)$$

$$S\left(\frac{2+b}{1-b}, -\frac{1+2b}{1-b}, -\frac{b(2+b)}{1+2b}\right) S\left(\frac{1+2b}{1-b}, -\frac{1+2b}{b(1-b)}, -1\right) =$$

$$= S\left(\frac{1+b+b^2}{1-b}, -\frac{1+2b}{1-b}, -\frac{1+b+b^2}{b(1+2b)}\right) S\left(\frac{1+b+b^2}{1-b}, -\frac{1+2b}{b(1-b)}, -\frac{1+b+b^2}{1+2b}\right) = S(0, b, \infty).$$

La precedente identità perde significato per $b \equiv 1$, ma per tale valore è stata dimostrata al n. 3, e pertanto è vera sempre [5].

Infine, se $a \not\equiv 0 \pmod{p}$, si ha

$$\left[S\left(2, -\frac{3(b+1)}{a}, \frac{ab}{3(b+1)}\right), S\left(-2, -\frac{3(b+1)}{ab}, -\frac{a}{3(b+1)}\right)\right] =$$

$$= S\left(-b, -\frac{3(b+1)}{a}, -\frac{2a}{3(b+1)}\right) \cdot S\left(\frac{1}{b}, -\frac{3(b+1)}{ab}, \frac{2ab}{3(b+1)}\right) \cdot$$

$$\cdot S\left(2, -\frac{3(b+1)}{a}, \frac{ab}{3(b+1)}\right) \cdot S\left(-2, -\frac{3(b+1)}{ab}, -\frac{a}{3(b+1)}\right) =$$

$$= S\left(1-b, -\frac{3(b+1)}{a}, -\frac{a(2b+1)}{3b(b+1)}\right) S\left(-b-2, -\frac{3(b+1)}{ab}, \frac{a(b-1)}{3(b+1)}\right) = S(a, b, \infty)\ [6].$$

[5] Le espressioni che figurano nella identità perdono significato anche quando $b = (p-1)/2$, ma ricordando che $S(0, (p-1)/2, \infty) = S(0, (p+1)/2, \infty)$, può sempre pensarsi che sia $b \neq (p-1)/2$.

[6] Può escludersi il valore $b \equiv -1$, dato che, per ottenere tutte le sostituzioni distinte del tipo indicato, b varia nell'insieme (3).

Pertanto tutte le sostituzioni della classe (4) risultano commutatori di elementi di G_p.

Rimane da verificare la proprietà per le sostituzioni della classe (5).

Ma anche in tal caso, tenendo conto delle (6), (7), (9), (10), si ha

$$\left[S\left(\frac{4bc-1}{2},\ 2b,\ \frac{4bc-a-6}{3b}\right)S\left(\frac{a+5-4bc}{2b},\ 2,\ \infty\right)\right]=$$

$$=S\left(\frac{8bc-2a-12}{3},\ 2b,\ c-\frac{1}{4b}\right)S\left(\frac{4bc-a-5}{2b},\ \frac{1}{2},\ \infty\right)\cdot$$

$$S\left(\frac{4bc-1}{2},\ 2b,\ \frac{4bc-a-6}{3b}\right)S\left(\frac{a+5-4bc}{2b},\ 2\ \ \infty\right)=$$

$$=S\left(\frac{16bc-4a-21}{3},\ 4b,\ c-\frac{1}{4b}\right)S\left(a+4,\ b,\ \frac{4bc-a-6}{3b}\right)=S(a,\ b,\ c).$$

Possiamo dunque concludere: *Ogni sostituzione del gruppo* G_p $(p>3)$ *è un commutatore, e pertanto il prodotto di un numero qualsiasi di commutatori è sempre un commutatore.*

5. Per $p=2,\ 3$, pur non valendo la proprietà che ogni elemento del gruppo è un commutatore, si verifica immediatamente come già si è detto al n. 1, che il gruppo derivato è composto esclusivamente di commutatori.

Basta osservare che G_2 coincide col gruppo totale sopra gli elementi ∞, 0, 1, e G_3 col gruppo alterno sopra gli elementi ∞, 0, 1, 2.

Si può ancora notare che la proprietà dimostrata per i gruppi modulari consente di affermarne una analoga per i corrispondenti gruppi lineari, formati cioè dalle sostituzioni $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ con $\alpha\delta-\beta\gamma\equiv 0$ (mod. p).

Infatti il derivato del gruppo lineare ($p>3$) coincide col gruppo modulare, e poichè ogni elemento di questo è commutatore del gruppo modulare, e quindi anche del gruppo lineare, ne viene che *il prodotto di commutatori del gruppo lineare è sempre un commutatore.*