Esercizio: Provare che, se G è un gruppo finito, allora in G esiste un elemento distinto dall'elemento neutro che è simmetrico di sé stesso se e solo se G ha ordine pari.

<u>Svolgimento:</u> Adotteremo la notazione moltiplicativa. Supponiamo dapprima che nessun elemento di G distinto da 1 sia simmetrico (inverso) di sé stesso. Definiamo su G la seguente relazione binaria: per ogni $x, y \in G$ porremo $x \sim y$ se $y \in \{x,\ x^{-1}\}$.
Questa relazione è di equivalenza. Infatti:

- per ogni $x \in G$ si ha evidentemente $x \sim x$;
- se $x, y \in G$ sono tali che $x \sim y$, allora $x = y$, oppure x e y sono l'uno l'inverso dell'altro, e in entrambi i casi $x \in \{y,\ y^{-1}\}$, quindi $y \sim x$.
- se $x, y, z \in G$ sono tali che $x \sim y$, $y \sim z$, allora, se $y = x$, evidentemente $x \sim z$, altrimenti $y = x^{-1}$, e dunque, se $z = y$, si avrà che $z = x^{-1}$, altrimenti, se $z = y^{-1}$, si avrà che $z = x$, e in entrambi i casi sarà $x \sim z$.

Indicata con $[x]$ la classe di equivalenza di ogni $x \in G$, si ha che

- $[x]$ ha un solo elemento se e solo se x è inverso di sé stesso (e ciò vale, per ipotesi, solo per l'elemento neutro 1);
- altrimenti, $[x]$ ha due elementi.

Detto s il numero delle classi di equivalenza del secondo tipo, tenendo conto del fatto che le classi di equivalenza formano una partizione di G, seguirà allora che

$$|G| = 2s + 1,$$

e dunque l'ordine di G è dispari.

Viceversa, supponiamo ora che almeno un elemento di G distinto dall'elemento neutro, diciamo x, sia inverso di sé stesso. Posto $n = |G|$, sia $G = \{a_1, \dots, a_n\}$. Per cancellabilità si ha che gli elementi $xa_1, \dots, xa_n$ sono a due a due distinti, ossia sono tutti gli elementi di G. Dunque, per ogni indice j esiste un indice i tale che $xa_i = a_j$. Identificheremo questa uguaglianza con il doppio indice (i, j). Al variare di i, si ottengono n uguaglianze siffatte. Si noti che in ogni caso si ha $i \neq j$, in quanto $x \neq 1$. Si osservi ora che $xa_j = x(xa_i) = (xx)a_i = 1a_i = a_i$, essendo per ipotesi x inverso di sé stesso. Dunque, per ogni uguaglianza di doppio indice (i, j), ve n'è una di doppio indice (j, i), distinta dalla precedente. Da ciò si deduce che le n uguaglianze si possono raggruppare due a due, e ne consegue che n è pari.