I (sotto)gruppi secondo Galois

Supponiamo che siano date le seguenti permutazioni, mediante le quali si voglia rappresentare un gruppo:

abcd
bcda
cdab

Si intende, con questa scrittura, l'insieme delle sostituzioni che portano dalla prima permutazione a ciascuna delle altre. Ivi è compresa anche quella che porta dalla prima alla prima, ossia la sostituzione identica.
Chiamiamo S la sostituzione che porta dalla prima alla seconda permutazione. La possiamo descrivere, astrattamente, con le seguenti assegnazioni:

1° elemento-→2° elemento
2° elemento-→3° elemento
3° elemento-→4° elemento
4°elemento-→1° elemento

Chiamiamo T la sostituzione che porta dalla prima alla terza permutazione. La possiamo descrivere, astrattamente, con le seguenti assegnazioni:

1° elemento-→3° elemento
2° elemento-→4° elemento
3° elemento-→1° elemento
4°elemento-→2° elemento

Supponiamo adesso di cambiare rappresentazione, cominciando dalla permutazione *bcda*, che prendiamo come riferimento per descrivere le sostituzioni. Allora il "gruppo" dovrebbe poter essere rappresentato anche da

bcda
cdab
abcd

e dunque dovrebbe comprendere anche la sostituzione di passaggio dalla prima permutazione alla seconda. E questa si ottiene tornando da *bcda* a *abcd* mediante S^{-1} e poi andando da *abcd* a *cdab* mediante T. Ossia, il nostro gruppo deve possedere, tra i suoi elementi, anche la composizione $T \circ S^{-1}$.
Alla luce della caratterizzazione dei sottogruppi, si conclude che la

seguente condizione (vedi il file Nota storica_2.pdf) indicata da Evariste Galois per individuare i (sotto)gruppi di permutazioni ci restituisce esattamente la nozione a noi nota:

Siccome si tratta sempre di questioni in cui la disposizione originale delle lettere non influisce in alcun modo sui gruppi che considereremo, bisognerà avere le stesse sostituzioni, qualunque sia la permutazione di partenza. Quindi, se in un siffatto gruppo ci sono le sostituzioni S *e* T*, sicuramente vi sarà anche la sostituzione* ST.

Ricordiamo, a questo proposito, che, in un **gruppo finito**, i sottogruppi sono tutti e soli i sottoinsiemi non vuoti e chiusi rispetto all'operazione del gruppo (nel caso in esame, la composizione).