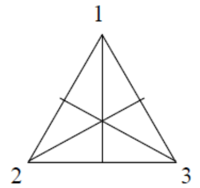
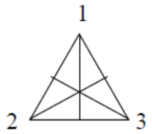
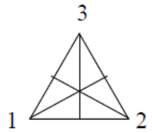
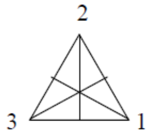
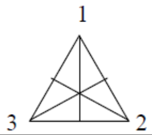
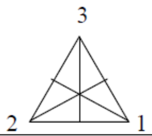
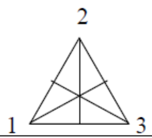
Simmetrie insiemistiche ed algebriche

Il gruppo simmetrico S_3 è isomorfo al gruppo delle simmetrie del triangolo equilatero:

Ogni simmetria (= movimento rigido) di un triangolo equilatero induce una permutazione dei vertici.

Precisiamo questa corrispondenza in una tabella:



Trasformazione	Triangolo trasformato	Permutazione dei vertici
Identità		id
Rotazione antioraria di $\frac{2\pi}{3}$ intorno al centro		$(1\ 2\ 3)$
Rotazione antioraria di $\frac{4\pi}{3}$ intorno al centro		$(1\ 3\ 2)$
Simmetria assiale rispetto all'asse del lato 23		$(2\ 3)$
Simmetria assiale rispetto all'asse del lato 13		$(1\ 3)$
Simmetria assiale rispetto all'asse del lato 12		$(1\ 2)$

L'aggettivo *simmetrico* diviene più difficile da giustificare geometricamente per i gruppi S_n con $n \geq 4$. Infatti, per questi valori di *n*, il gruppo delle simmetrie di un poligono regolare con *n* lati è isomorfo ad un sottogruppo proprio di S_n. Ad esempio, dato il quadrato i cui vertici siano numerati, in senso antiorario, con 1, 2, 3, 4, non esiste alcuna simmetria che induca su questi la permutazione che produce la sequenza 2, 1, 3, 4: infatti il quadrato di partenza non possiede un lato di vertici 1,3 e la distanza tra questi è pari alla lunghezza della diagonale. Questa esclusione è dovuta alla necessità di rispettare un vincolo determinato dalle posizioni reciproche dei punti sottoposti a permutazione. Per ottenere tutte le permutazioni, è sufficiente allora far cadere ogni ostacolo, non richiedendo agli *n* oggetti sottoposti a permutazione niente altro che essere, semplicemente, *n* cose *distinte*. In tal senso, S_n è il gruppo delle simmetrie di un qualsiasi insieme di cardinalità *n*, i cui elementi non siano soggetti ad alcuna condizione che debba essere preservata dalle trasformazioni considerate. In altri termini, tali elementi non costituiscono, nel loro complesso, alcuna particolare configurazione, non sono legati da alcuna relazione.

Ora ripensiamo alla visione geometrica proposta da Henri Poincaré, per il quale ogni elemento del gruppo è, contemporaneamente, una possibile *posizione* (iniziale o finale) ed un possibile *spostamento* (da una posizione ad un'altra). Secondo tale interpretazione, una *permutazione* è allora un modo per passare da una *permutazione* ad un'altra *permutazione*, dove il termine *permutazione* assume necessariamente due significati distinti: nel primo caso, indica una particolare disposizione degli n elementi, nel secondo caso, una trasformazione che modifica una disposizione formandone una nuova. In effetti, Evariste Galois usava una parola diversa per denotare questa trasformazione, che chiamava *sostituzione*. Il parallelo che si può tracciare con lo scritto di Poincaré assimila i *punti* alle *disposizioni* e gli *spostamenti* alle *sostituzioni*. Quindi, trasferendo a questo nuovo ambito "combinatorio" l'esempio della circonferenza generata dall'applicazione ad un punto P delle rotazioni intorno ad un distinto punto C, potremmo immaginare di applicare, ad una certa disposizione iniziale di 4 elementi *abcd*, tutte le "rotazioni" (quelle che si possono visualizzare come le simmetrie rotazionali di un insieme di quattro punti che suddividono una circonferenza in quattro archi uguali). L'insieme così ottenuto è formato dalle seguenti 4 disposizioni:

abcd
bcda
cdab
dabc

Questo, contemporaneamente, dovrebbe essere un gruppo di trasformazioni, avente ordine 4. I suoi elementi si possono così descrivere:

Permutazione identica

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

È facile vedere a quale dei due possibili modelli esso corrisponda.
Osserviamo infine che questa rappresentazione è indipendente dall'ordine in cui vengono elencate le disposizioni. Ed è proprio su questa proprietà che fa leva la "definizione" di (sotto)gruppo data da Galois.

Ma veniamo ora ad oggetti "algebrici" di cui i gruppi S_n ed i loro sottogruppi siano i gruppi delle simmetrie. Per fissare le idee, cominciamo fissando il valore di n: poniamo $n = 4$. Premettiamo che quanto esposto di seguito si estende ad ogni intero positivo n. Osserviamo che sono *invarianti* rispetto ad ogni permutazione di S_4 i seguenti polinomi a coefficienti interi nelle indeterminate x_1, x_2, x_3, x_4 :

$$
\begin{aligned}
s_1^{(4)} &= x_1 + x_2 + x_3 + x_4 \\
s_2^{(4)} &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\
s_3^{(4)} &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\
s_4^{(4)} &= x_1x_2x_3x_4
\end{aligned}
$$

Questi polinomi rivestono un ruolo particolare nella teoria delle equazioni algebriche, come indicato dalle cosiddette *formule di Viète*. Sia $f(x) = x^4 + \sum_{i=0}^{3} a_i x^i$ un polinomio monico di grado 4 a coefficienti complessi, e siano $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ le sue radici complesse (contate con le rispettive molteplicità). Allora, come conseguenza del Teorema di Ruffini,

$$f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)(x-\alpha_4).$$

Sviluppando il prodotto, si trovano le seguenti relazioni fra i coefficienti del polinomio e le sue radici:

$$
\begin{aligned}
a_3 &= -s_1^{(4)}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \\
a_2 &= s_2^{(4)}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \\
a_1 &= -s_3^{(4)}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \\
a_0 &= s_4^{(4)}(\alpha_1, \alpha_2, \alpha_3, \alpha_4)
\end{aligned}
$$

I coefficienti di $f(x)$ sono dunque espressioni polinomiali simmetriche (a coefficienti interi) delle radici di $f(x)$. Si prova che, in generale, ogni espressione polinomiale (o razionale) simmetrica delle radici è un'espressione polinomiale (o razionale) dei coefficienti.
Tra il Seicento e l'Ottocento diversi autori, tra cui

E. W. von Tschirnhaus (1683)
E. Bézout (1762-1765)
J.-L. Lagrange (1770-1771)
P. Ruffini (1799)
A. Cauchy (1815)
E. Galois (1831-1832)

hanno lavorato alla risoluzione delle equazioni algebriche intorno alla seguente idea (che ora illustriamo per le equazioni di quarto grado con 4 radici distinte): per risolvere l'equazione

$$f(x) = 0$$

si ricorre ad un'equazione ausiliaria $r(x) = 0,$ per la quale si conosce il metodo risolutivo, e le cui soluzioni sono espressioni polinomiali note delle soluzioni dell'equazione di partenza:

$$\beta_i = g_i(\alpha_1, \alpha_2, \alpha_3, \alpha_4).$$

Il problema è trasferito dunque alla ricerca delle radici β_i del polinomio $r(x)$. Una volta trovate queste, le radici α_i si ricavano invertendo le relazioni date sopra. Ora, attenzione: ad essere note sono soltanto le espressioni polinomiali $g_i(x_1,x_2,x_3,x_4)$. A partire da queste, in particolare, occorre costruire il polinomio $r(x)$. Naturalmente, non è pensabile ricavarlo a partire dalle radici β_i tramite la decomposizione suggerita dal Teorema di Ruffini, perché per conoscere β_i conoscendo g_i occorrerebbe avere già a disposizione le radici cercate $\alpha_1,\alpha_2,\alpha_3,\alpha_4$. L'ostacolo viene aggirato nel seguente modo. Si parte da un'unica espressione polinomiale $g(x_1,x_2,x_3,x_4)$, opportunamente scelta, e si definisce un nuovo polinomio

$$s(x)=\prod_{\sigma\in S_4}(x-\sigma g(\alpha_1,\alpha_2,\alpha_3,\alpha_4)),$$

i cui coefficienti, essendo espressioni polinomiali simmetriche nelle radici α_i, sono espressioni polinomiali nei coefficienti di $f(x)$. Quindi i coefficienti di $s(x)$ possono essere costruiti indipendentemente dalle radici di $f(x)$. A prima vista, il polinomio così ottenuto può sembrare tutt'altro che utile: ha infatti grado 24, molto maggiore del grado di $f(x)$. Solitamente, il metodo prevede di ricondurre il problema originario ad un problema di grado inferiore, nel caso specifico ci si riconduce ad un problema di terzo grado. In effetti, si può fare in modo che il polinomio $s(x)$ abbia esattamente 3 radici β_1,β_2,β_3 ognuna di molteplicità 8. Allora il polinomio $s(x)$ sarà l'ottava potenza di un polinomio di terzo grado, il vero *risolvente*:

$$r(x)=(x-\beta_1)(x-\beta_2)(x-\beta_3).$$

Precisamente, si prende

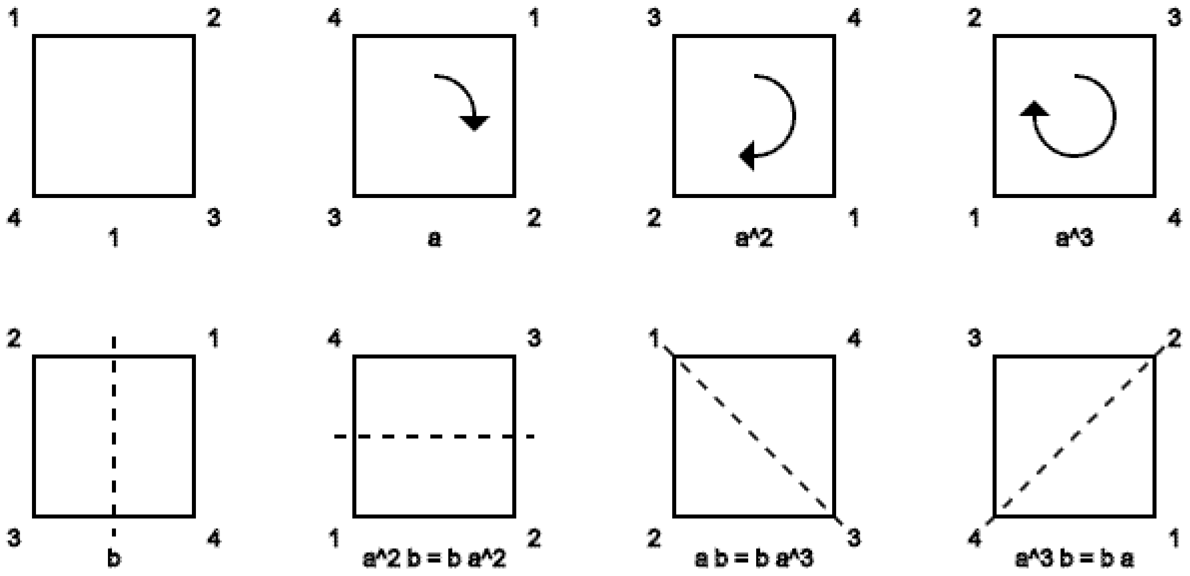
$$g=g_1(x_1,x_2,x_3,x_4)=x_1x_2+x_3x_4.$$

Applicando tutte le permutazioni di S_4 si ottengono complessivamente tre polinomi distinti. A quello assegnato si aggiungono i seguenti due:

$$g_2(x_1,x_2,x_3,x_4)=x_1x_3+x_2x_4$$
$$g_3(x_1,x_2,x_3,x_4)=x_1x_4+x_2x_3$$

Ciò corrisponde al fatto che il polinomio iniziale è lasciato fisso da esattamente 8 permutazioni: queste formano un sottogruppo di S_4 che costituisce il suo **gruppo di simmetria**. Si prova che altri due sottogruppi di ordine 8 sono i gruppi di simmetria degli altri due polinomi. Tali sottogruppi sono tutti isomorfi al **gruppo delle simmetrie di un quadrato**.

Ad esempio, si può osservare come il polinomio g_2 sia lasciato invariato da tutte e sole le permutazioni sotto la cui azione i due insiemi $\{1,3\}$ e $\{2,4\}$ vengono inviati in loro stessi oppure l'uno nell'altro. Questo è esattamente l'effetto prodotto da tutte e sole le simmetrie di un quadrato i cui vertici siano numerati con 1, 2, 3, 4 in senso orario, in modo che i due insiemi suindicati siano formati dai vertici delle due diagonali:



Il corrispondente sottogruppo del gruppo S_4 è formato dai seguenti elementi (letti, nella figura, orizzontalmente, da sinistra a destra):

$$\boldsymbol{id} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{3} & \mathbf{4} & \mathbf{1} & \mathbf{2} \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{2} & \mathbf{1} & \mathbf{4} & \mathbf{3} \end{pmatrix} \quad \begin{pmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} \\ \mathbf{4} & \mathbf{3} & \mathbf{2} & \mathbf{1} \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

In grassetto sono evidenziati gli elementi del gruppo delle simmetrie di un rettangolo che non sia un quadrato.

Il gruppo delle simmetrie del quadrato è detto ***gruppo diedrale D_4***. Non è abeliano. Inoltre, sei dei suoi elementi sono simmetrici di sé stessi (oltre all'identità, la rotazione di 180° e le quattro simmetrie assiali).