Kui A on mittetühi hulk, siis tähistame $S(A)$ abil kõigi bijektiivsete teisenduste ehk substitutsioonide rühma hulgal A. Seda nimetame sümmeetriliseks rühmaks hulgal A. Kui $A = \{1, ..., n\}$, siis kirjutame $S(A)$ asemel S_n. Kõik paarissubsitutsioonid hulgal $\{1, ..., n\}$ moodustavad rühma S_n normaalse alamrühma, mida tähistame A_n.

Teoreem 1. *Kui $n = 3$ või $n \geq 5$, siis rühm A_n on lihtne.*

Definitsioon 1. Rühma G alamrühma H nimetatakse normaalseks, kui iga $a \in G$ ja $h \in H$ korral $a^{-1}ha \in H$.

Definitsioon 2. Rühma, millel ei ole mittetriviaalseid normaalseid alamrühmi, nimetatakse lihtsaks rühmaks.

Definitsioon 3. Olgu $M \neq \emptyset$ mistahes hulk. Subsitutsiooniks hulgal M nimetatakse hulga M mistahest üksühest pealekujutust.

Definitsioon 4. Substitutsiooni nimetatakse paarissubstitutsiooniks, kui mõlemad permutatsioonid tema esituses tabelina on ühesuguse paarsusega, see tähendab, inversioonide arv mõlemas esituses tabelina on sama paarsusega. Vastasel juhul nimetatakse subsitutsiooni paarituks substitutsiooniks.

Definitsioon 5. Lõpliku hulga teisendust, mis seisneb selle hulga kahe erineva elemendi ümbervahetamises, kusjuures ülejäänud elemendid jäävad paika nimetatakse transpositsiooniks.

Teoreem 2. *Iga substitutsioon vähemalt kaheelemendilisel hulgal on esitatav transpositsioonide korrutisena.*

Lause 3. *Tegurite arv substitutsiooni esituses transpositsioonide korrutisena on sama paarsusega kui substitutsioon ise.*

Definitsioon 6. Subsitsiooni nimetatakse tsükliks, kui ta paigutab teatud elemendid tsükliliselt ümber, ülejäänud elemendid jätab aga paigale. Tsüklit, mis viib elemendi i_1 elemendiks i_2, elmendi i_2 elemendiks i_3,...,elmendi i_k elemendiks i_1 tähistataikse $(i_1 i_2 ... i_k)$.

Mistahes substitutsiooni on võimalik esitada niinimetatud sõltumatute tsüklite korrutisena - tsüklite korrutisena, mille üleskirjutises ei ole ühiseid elemente. Paneme tähele, et transpositsioone võime vaadelda kui kahe elemendilise tsükleid.