Časopis pro pěstování matematiky a fysiky

Sophie Piccard

Sur les bases du groupe symétrique

Časopis pro pěstování matematiky a fysiky, Vol. 68 (1939), No. 1, 15--30

Persistent URL: http://dml.cz/dmlcz/121729

Sur les bases du groupe symétrique.

Sophie Piccard, Neuchâtel.

(Reçu le 27 octobre 1937.)

On voit sans peine que quel que soit le nombre entier $n \geqq 3$, le groupe symétrique G d'ordre $n!$ ne saurait être engendré par une seule de ses substitutions. Par contre, il existe des couples de substitutions de G qui permettent, par composition, d'engendrer ce groupe. Telles sont, p. ex., les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (1\ 2)$.[1])

Définitions. 1. Quel que soit le nombre entier $n \geqq 3$, nous dirons que deux substitutions S et T faisant partie du groupe symétrique G d'ordre $n!$ constituent une base de ce groupe si toute substitution du groupe G peut être obtenue en composant S et T. On voit immédiatement que quelle que soit la substitution R du groupe G, si deux substitutions S, T constituent une base de G, les deux substitutions RSR^{-1} et RTR^{-1} en constituent également une.[2])

2. Nous dirons que deux bases S, T et S_1, T_1 du groupe G sont distinctes si elles diffèrent au moins par une substitution.

3. Nous dirons que deux bases S, T et S_1, T_1 du groupe G sont indépendantes si quelle que soit la substitution R du groupe G, la base RSR^{-1}, RTR^{-1} est distincte de S_1, T_1 ou, ce qui revient au même, la base RS_1R^{-1}, RT_1R^{-1} est distincte de S, T.

Problème: Quel est le nombre total N des bases du groupe symétrique G d'ordre $n!$ $(n \geqq 3)$?

Le but de la présente note est de prouver que le nombre N est un multiple de $\frac{1}{2}n!$ et d'indiquer un système complet de bases du groupe G pour $n = 3, 4, 5$ et 6.

Proposition 1. Quel que soit le nombre entier $n \geqq 3$ et quelles que soient les deux substitutions S, T du groupe symétrique G

[1]) Pour simplifier l'écriture et sans nuire à la généralité des raisonnements qui suivent, nous désignerons généralement par les nombres $1, 2, \ldots, n$ les éléments d'une substitution de degré n.

[2]) Dans les formules donnant des substitutions composées, les substitutions successives de la composition sont toujours effectuées de droite à gauche.

d'ordre $n!$ qui constituent une base de ce groupe, il n'existe aucune substitution $R \neq 1$ du groupe G qui soit permutable aussi bien avec S qu'avec T.

Démonstration. Supposons le contraire et soit $R \neq 1$ une substitution de G, telle que l'on ait simultanément

$$\begin{aligned} RS &= SR \\ RT &= TR \end{aligned} \tag{1}$$

Comme S, T est une base de G, toute substitution Q de G s'obtient par composition de S et de T. Soit $Q = \varphi(S, T)$. On déduit alors sans peine par induction des relations (1) que l'on doit avoir $R\,\varphi(S, T) = \varphi(S, T)\,R$, c'est-à-dire, $RQ = QR$, quelle que soit la substitution Q de G. Or, cela n'est possible que si $R = 1$, contrairement à notre hypothèse sur R. Notre proposition est ainsi démontrée.

Proposition 2. Quelle que soit la base S, T du groupe symétrique G d'ordre $n!$ $(n \geqq 3)$, s'il existe une substitution R de G, telle que l'on a simultanément

$$\begin{aligned} RSR^{-1} &= T \\ RTR^{-1} &= S. \end{aligned} \tag{1}$$

la substitution R est du second ordre.

Démonstration: R ne saurait être $= 1$, puisque dans le cas contraire on aurait $S = T$ et, par suite, les deux substitutions S, T ne formeraient pas une base de G. Donc l'ordre de R est $\geqq 2$.

Des relations (1) on déduit immédiatement

$$\begin{aligned} R^2SR^{-2} &= RTR^{-1} = S \\ R^2TR^{-2} &= RSR^{-1} = T. \end{aligned}$$

Ainsi les deux substitutions S et T sont permutables avec la substitutions R^2. Or, en vertu de la proposition 1, cela n'est possible que si $R^2 = 1$. Donc l'ordre de R ne saurait être supérieur à 2. Et comme il n'est pas inférieur à 2, il est bien égal à 2, c. q. f. d.

Lemme 1. Quelle que soit la base S, T du groupe symétrique G d'ordre $n!$ $(n \geqq 3)$, s'il existe une substitution R de G, telle que

$$\begin{aligned} RSR^{-1} &= T \\ RTR^{-1} &= S, \end{aligned} \tag{1}$$

cette substitution R est unique.

Démonstration. En effet, supposons le contraire et soient R et R_1 deux substitutions distinctes du groupe G, telles que l'on ait (1) et

$$\begin{aligned} R_1SR_1^{-1} &= T \\ R_1TR_1^{-1} &= S. \end{aligned} \tag{2}$$

Puisque les deux substitutions S et T constituent une base de G, on ne saurait avoir ni $R = 1$, ni $R_1 = 1$.

De (1) et (2), on déduit:

$$RSR^{-1} = R_1SR_1^{-1} \text{ et } RTR^{-1} = R_1TR_1^{-1},$$

c'est-à-dire

$$R_1^{-1}RS = SR_1^{-1}R \text{ et } R_1^{-1}RT = TR_1^{-1}R.$$

Ainsi la substitution $R_1^{-1}R$ est permutable à la fois avec S et avec T. En vertu de la proposition 1, cela n'est possible que si $R_1^{-1}R = 1$, c. à. d. si $R_1 = R$. Notre lemme est donc démontré.

Lemme 2. Si S, T est une base du groupe symétrique G d'ordre $n!$ pour laquelle il existe une substitution R de G, telle que

$$\begin{aligned} RSR^{-1} &= T \\ RTR^{-1} &= S, \end{aligned} \tag{1}$$

quelle que soit la substitution P de G, il existe une substitution Q de G et une seule, telle que

$$\begin{aligned} PSP^{-1} &= QTQ^{-1} \\ PTP^{-1} &= QSQ^{-1}. \end{aligned} \tag{2}$$

Démonstration. Soit P une substitution quelconque du groupe G. De (1) on déduit immédiatement

$$\begin{aligned} PRSR^{-1}P^{-1} &= PTP^{-1} \\ PRTR^{-1}P^{-1} &= PSP^{-1}. \end{aligned}$$

Posons $PR = Q$.

On a donc

$$\begin{aligned} QSQ^{-1} &= PTP^{-1} \\ QTQ^{-1} &= PSP^{-1}. \end{aligned}$$

Il existe donc bien une substitution Q du groupe G, telle que les relations (2) soient satisfaites et il résulte immédiatement du lemme 1 que cette substitution est unique.

Lemme 3. Si S, T est une base du groupe symétrique G d'ordre $n!$ ($n \geq 3$), telle qu'il n'existe aucune substitution R de G pour laquelle on ait les relations:

$$\begin{aligned} RSR^{-1} &= T \\ RTR^{-1} &= S, \end{aligned}$$

quelle que soit la substitution P de G, il ne saurait exister une substitution Q de G, telle que l'on ait à la fois

$$\begin{aligned} PSP^{-1} &= QTQ^{-1} \\ PTP^{-1} &= QSQ^{-1}. \end{aligned} \tag{1}$$

Démonstration. Soit P une substitution quelconque de G et supposons, contrairement au lemme, qu'il existe une substitution Q de G, telle que les relations (1) aient lieu. On en déduit alors immédiatement:

$$\begin{aligned} Q^{-1}PSP^{-1}Q &= T \\ Q^{-1}PTP^{-1}Q &= S. \end{aligned}$$

Posons $R = Q^{-1}P$.

Il vient alors $$RSR^{-1} = T$$
$$RTR^{-1} = S.$$

Or, d'après nos hypothèses, il n'existe aucune substitution R de G qui vérifie ces deux relations. Nous sommes donc conduits à une contradiction et notre lemme est démontré.

Corollaire. Soit (1) $R_1, R_2, \ldots, R_{n!}$ une suite formée de toutes les substitutions du groupe symétrique G d'ordre $n!$, ces substitutions étant rangées dans un ordre quelconque. Soit S, T une base quelconque du groupe G. Posons $R_iSR_i^{-1} = S_i$, $R_iTR_i^{-1} = T_i$. quel que soit $i = 1, 2, \ldots, n!$. Je dis que la suite

$$(S_1, T_1), (S_2, T_2), \ldots, (S_{n!}, T_{n!}) \qquad (2)$$

contient soit $n!$ bases disctinctes, soit $\frac{1}{2}n!$ bases distinctes du groupe G.

En effet, s'il n'existe aucune substitution R_i de G, telle que $S_i = T$, $T_i = S$, il résulte du lemme 3 que tous les termes de la suite (2) sont distincts deux à deux. Cette suite contient donc dans le cas considéré $n!$ bases distinctes du groupe G.

S'il existe une substitution R_i de G, telle que $S_i = T$, $T_i = S$. en vertu du lemme 1, cette substitution R_i est unique et, en vertu du lemme 2, il existe alors pour toute substitution R_k de la suite (1) une substitution R_l et une seule de la suite (1), telle que $S_k = T_l$. $T_k = S_l$. La suite (2) contient donc dans ce cas $\frac{1}{2}n!$ bases distinctes.

Notre corollaire est donc bien établi.

Nous dirons que la base S_i, T_i est la transformée de S, T par la substitution R_i.

Proposition 3 (fondamentale). Quel que soit le nombre entier $n \geqq 3$, le nombre total N des bases distinctes du groupe symétrique G d'ordre $n!$ est un multiple de $\frac{1}{2}n!$.

Démonstration. Soit S, T une base quelconque de G.

Soit

$$(S_1, T_1), (S_2, T_2), \ldots, (S_{n!}, T_{n!}) \qquad (1)$$

la suite formée de toutes les transformées de la base S, T par les substitutions du groupe G. D'après notre corollaire, la suite (1) contient $n!$ ou $\frac{1}{2}n!$ bases distinctes du groupe G.

Soit à présent m un nombre entier quelconque $\geqq 1$ et supposons que nous avons déjà défini m bases indépendantes (voir définition 3) $(S^{(1)}, T^{(1)}) = (S, T)$, $(S^{(2)}, T^{(2)}), \ldots, (S^{(m)}, T^{(m)})$ du groupe G.

D'après ce qui précède, la suite

$$(S_1^{(i)}, T_1^{(i)}), (S_2^{(i)}, T_2^{(i)}), \ldots, (S_{n!}^{(i)}, T_{n!}^{(i)}) \qquad (i)$$

contient soit $n!$ soit $\frac{1}{2}n!$ bases distinctes de G, quel que soit $i = 1, 2, \ldots, m$ et l'on voit immédiatement que les suites

(1), (2), . . ., (m) sont disjointes deux à deux (c. à. d, qu'elles n'ont aucun élément commun).

Deux cas peuvent maintenant se présenter. Ou bien toute base du groupe G figure dans une des suites (i), ($i = 1, 2, \ldots, m$). Alors notre théorème est démontré. Ou bien il existe une base $S^{(m+1)}$, $T^{(m+1)}$ de G qui ne figure dans aucune de ces suites. Formons alors la suite

$$(S_1^{(m+1)}, T_1^{(m+1)}), (S_2^{(m+1)}, T_2^{(m+1)}), \ldots, (S_{n!}^{(m+1)}, T_{n!}^{(m+1)}). \quad (m+1)$$

D'après notre corollaire, cette suite contient $\frac{1}{2}n!$ ou $n!$ termes distincts. Je dis que la suite $(m+1)$ ne saurait contenir aucune base d'une suite (i), ($i = 1, 2, \ldots, m$). En effet, supposons le contraire et soit, p. ex.,

$$(S_j^{(m+1)}, T_j^{(m+1)}) = (S_k^{(i)}, T_k^{(i)}) \quad (1 \leqq j \leqq n!,\ 1 \leqq k \leqq n!).$$

On doit alors avoir

$$\text{soit a) } S_j^{(m+1)} = S_k^{(i)},\ T_j^{(m+1)} = T_k^{(i)};$$
$$\text{soit b) } S_j^{(m+1)} = T_k^{(i)},\ T_j^{(m+1)} = S_k^{(i)};$$

a) peut s'écrire

$$R_j S^{(m+1)} R_j^{-1} = R_k S^{(i)} R_k^{-1},\ R_j T^{(m+1)} R_j^{-1} = R_k T^{(i)} R_k^{-1}.$$

On en déduit

$$S^{(m+1)} = R_j^{-1} R_k S^{(i)} R_k^{-1} R_j,\ T^{(m+1)} = R_j^{-1} R_k T^{(i)} T_k^{-1} R_j.$$

Posons $R_j^{-1} R_k = Q$.

Nous voyons que $S^{(m+1)}$ est la transformée de $S^{(i)}$ par Q et que $T^{(m+1)}$ est la transformée de $T^{(i)}$ par Q. Donc les deux bases $S^{(i)}$, $T^{(i)}$ et $S^{(m+1)}$, $T^{(m+1)}$ ne sont pas indépendantes, contrairement à notre hypothèse. Dans le cas b), on trouve, par un raisonnement analogue, que $S^{(m+1)}$ est la transformée de $T^{(i)}$ par Q et que $T^{(m+1)}$ est la transformée de $S^{(i)}$ par Q, ce qui implique également une contradiction. Donc aucune base de la suite $(m+1)$ ne saurait appartenir à l'une des suites (i), ($i = 1, 2, \ldots, m$). Cela étant quel que soit le nombre entier $m \geqq 1$, il en découle que le nombre total N de bases du groupe symétrique G d'ordre $n!$ ($n \geqq 3$) est bien un multiple de $\frac{1}{2}n!$, c. q. f. d.

* * *

2. Il résulte de notre théorème fondamental que le nombre total N de bases du groupe symétrique G d'ordre $n!$ est un nombre de la forme

$$N = K \cdot \tfrac{1}{2}n!,$$

K désignant un nombre entier $\geqq 1$.

Nous dirons que M bases $(S^{(1)}, T^{(1)})$, $(S^{(2)}, T^{(2)})$, $(S^{(3)}, T^{(3)})$, ..., $(S^{(M)}, T^{(M)})$ de G forment un système complet de bases indépendantes si elles sont toutes indépendantes deux à deux et si

toute base de G s'obtient en transformant l'une des bases de ce système par une substitution déterminée de G.

Le nombre M est un invariant du groupe G.

Montrons que $M < K$, quel que soit $n \geqq 3$.

A cet effet, il suffit de montrer que quel que soit le nombre entier $n \geqq 3$, il existe au moins une base du groupe G, dont la suite des transformées au moyen de toutes les substitutions de G contient $n!$ bases distinctes de G. D'après ce qui précède, quelle que soit la base S, T du groupe G, dont l'ensemble des transformées au moyen de substitutions de G contient $\frac{1}{2}n!$ bases distinctes, les deux substitutions S et T sont semblables. Donc, toute base de G dont les deux substitutions ne sont pas semblables possède en tout cas $n!$ transformées distinctes au moyen de substitutions de G. Telle est, p. ex., la base $(1\ 2\ \ldots\ n)$, $(1\ 2)$.

On a donc bien $M < K$, quel que soit $n \geqq 3$, c. q. f. d.

D'autre part, il existe pour tout nombre entier $n \geqq 3$, des bases S, T du groupe symétrique G d'ordre $n!$, dont la suite des transformées au moyen de toutes les substitutions de G ne contient que $\frac{1}{2}n!$ bases de G. Quel que soit le nombre impair $n \geqq 3$, telle est, p. ex., la base $S = (1\ 2\ \ldots\ n-1)$, $T = (1\ 2\ \ldots\ n-2\ n)$.

En posant $R = (n-1\ n)$, on a alors $RSR^{-1} = T$, $RTR^{-1} = S$ et, en vertu des lemmes 1 et 2, il existe donc $\frac{1}{2}n!$ bases distinctes parmi toutes les transformées de la base S, T au moyen des substitutions de G.

Quel que soit le nombre pair n, la base $\begin{cases} S = (1\ 2\ 3\ \ldots\ n) \\ T = (2\ 1\ 3\ \ldots\ n) \end{cases}$ jouit de la propriété énoncée ci-dessus. En effet, pour $R = (1\ 2)$, on a $RSR^{-1} = T$, $RTR^{-1} = S$. Donc, en vertu des lemmes 1 et 2, la suite des transformées de la base S, T par toutes les substitutions de G contient $\frac{1}{2}n!$ bases distinctes.

Tout système complet de bases indépendantes du groupe symétrique G d'ordre $n!$ comprend donc nécessairement des bases de deux espèces: les unes possèdent $n!$ transformées au moyen de diverses substitutions de G, les autres n'en possèdent que $\frac{1}{2}n!$. Le nombre de bases de chacune de ces classes est, comme on voit sans peine, un invariant du groupe G. Soit M_1 le nombre total des bases de tout système complet de bases indépendantes, dont chacune possède $n!$ transformées au moyen de substitutions du groupe G et soit M_2 le nombre total de bases de tout système complet de bases indépendantes, dont chacune possède $\frac{1}{2}n!$ transformées au moyen de substitutions de G. On a $M = M_1 + M_2$ et $K = 2M_1 + M_2$.

Pour connaître toutes les bases du groupe symétrique G d'ordre $n!$, il suffit d'après ce qui précède, de connaître un système complet quelconque de bases indépendantes de ce groupe.

Nous avons calculé toutes les bases du groupe symétrique d'ordre $n!$ pour $n = 3, 4, 5$ et 6. Ensuite, nous avons cherché dans chacun de ces cas un système de bases indépendantes. Voici les résultats auxquels nous sommes parvenus:

Ordre du groupe symétrique G: $n!$	$\frac{1}{2}n!$	Nombre total des bases de G: N	$K = \frac{N}{\frac{1}{2}n!}$	$M = M_1 + M_2$	M_1	M_2
3! = 6	3	9	3	2	1	1
4! = 24	12	108	9	5	4	1
5! = 120	60	3.420	57	31	26	5
6! = 720	360	113.760	316	162	154	8

Notations: Nous affecterons d'un indice inférieur $\frac{1}{2}$ les deux substitutions de toute base du groupe symétrique d'ordre $n!$ dont le nombre de transformées au moyen de substitutions de ce groupe est égal à $\frac{1}{2}n!$. Les bases dont les deux substitutions ne sont affectées d'aucun indice possèdent chacune $n!$ transformées au moyen de substitutions du groupe. Le cycle (1 2 3 4) sera désigné par IV; de même, V = (1 2 3 4 5), VI = (1 2 3 4 5 6), $\text{IV}_{\frac{1}{2}} = (1\ 2\ 3\ 4)_{\frac{1}{2}}$ etc.

Système de bases indépendantes du groupe symétrique d'ordre 3!

$(1\ 2)_{\frac{1}{2}}$, $(2\ 3)_{\frac{1}{2}}$; (1 2 3), (1 2).

Système de bases indép. du groupe symétr. d'ordre 4!

(1 2 3), (3 4); IV, (1 2); IV, (1 2 3); IV, (1 3 2); $\text{IV}_{\frac{1}{2}}$, $(1\ 3\ 2\ 4)_{\frac{1}{2}}$

Système de bases indép. du groupe symétr. s'ordre 5!

IV, (4 5)
IV, (1 2 5)
IV, (1 5 2)
IV, (1 3 5)
IV, (2 3) (4 5)
$\text{IV}_{\frac{1}{2}}$, $(1\ 2\ 3\ 5)_{\frac{1}{2}}$
$\text{IV}_{\frac{1}{2}}$, $(1\ 5\ 3\ 2)_{\frac{1}{2}}$
IV, (1 2 3) (4 5)
IV, (1 3 2) (4 5)
IV, (1 2) (3 4 5)
IV, (1 2) (3 5 4)
IV, (1 3) (2 4 5)
(1 2 3) (4 5), (3 4)
(1 2 3) (4 5), (1 2 4)
(1 2 3) (4 5), (1 4 2)
(1 2 3) (4 5), (1 4 5)
(1 2 3) (4 5), (1 2) (3 4)
(1 2 3) (4 5), (1 4) (2 5)
$(1\ 2\ 3)\ (4\ 5)_{\frac{1}{2}}$, $(1\ 2\ 4)\ (3\ 5)_{\frac{1}{2}}$
$(1\ 2\ 3)\ (4\ 5)_{\frac{1}{2}}$, $(1\ 4\ 2)\ (3\ 5)_{\frac{1}{2}}$
$(1\ 2\ 3)\ (4\ 5)_{\frac{1}{2}}$, $(1\ 4\ 5)\ (2\ 3)_{\frac{1}{2}}$
V, (1 2)
V, (1 3)
V, (1 2 3 4)
V, (1 4 3 2)
V, (1 3 2 4)
V, (1 4 2 3)
V, (1 2 3) (4 5)
V, (1 3 2) (4 5)
V, (1 3 5) (2 4)
V, (1 5 3) (2 4)

Système de bases indép. du groupe symétr. d'ordre 6!

IV, (4 5 6)
IV, (1 3 5 6)
IV, (1 2 5) (3 6)
IV, (1 5 2) (3 6)
IV, (1 2 5) (4 6)
IV, (1 5 2) (4 6)
IV, (1 3 5) (4 6)
IV, (1 5 3) (4 6)
IV, (1 2) (3 5 6)
IV, (1 2) (4 5 6)
IV, (1 3) (2 5 6)
IV, (1 2) (3 4 5 6)
IV, (1 2) (3 6 5 4)
IV, (1 2) (3 5 4 6)
IV, (1 3) (2 4 5 6)
IV, (1 5) (2 3 4 6)
IV, (1 5) (2 6 4 3)
IV, (1 5) (2 3 6 4)
IV, (1 5) (2 4 6 3)
IV, (1 5) (2 4 3 6)
IV, (1 5) (2 6 3 4)
(1 2 3) (4 5), (1 4 6)
(1 2 3) (4 5), (1 6 4)
(1 2 3) (4 5), (1 4) (2 6)
(1 2 3) (4 5), (1 4) (5 6)
(1 2 3) (4 5), (1 6) (3 4)
(1 2 3) (4 5), (1 2) (3 4 6)
(1 2 3) (4 5), (1 2) (3 6 4)
(1 2 3) (4 5), (1 4) (2 3 6)
(1 2 3) (4 5), (1 4) (2 6 3)
(1 2 3) (4 5), (1 4) (2 5 6)
(1 2 3) $(4\ 5)_{\frac{1}{2}}$, (1 4) $(2\ 6\ 5)_{\frac{1}{2}}$
(1 2 3) $(4\ 5)_{\frac{1}{2}}$, (1 4) $(3\ 5\ 6)_{\frac{1}{2}}$
(1 2 3) $(4\ 5)_{\frac{1}{2}}$, (1 6) $(2\ 3\ 4)_{\frac{1}{2}}$
(1 2 3) $(4\ 5)_{\frac{1}{2}}$, (1 6) $(2\ 4\ 3)_{\frac{1}{2}}$
(1 2 3) (4 5), (1 2) (3 4) (5 6)
(1 2 3) (4 5), (1 2 4) (3 5 6)
(1 2 3) (4 5), (1 4 2) (3 6 5)
(1 2 3) (4 5), (1 4 5) (2 3 6)
(1 2 3) (4 5), (1 5 4) (2 6 3)
(1 2 3) (4 5), (1 4 6) (2 3 5)
(1 2 3) (4 5), (1 6 4) (2 5 3)
V, (5 6)
V, (1 2 6 3)
V, (1 3 6 2)
V, (1 3 2 6)
V, (1 6 2 3)
V, (1 3 4 6)
V, (1 6 4 3)
V, (1 4 3 6)
V, (1 6 3 4)
V, (1 2 3) (4 6)
V, (1 3 2) (4 6)
V, (1 2 3) (5 6)
V, (1 3 2) (5 6)
V, (1 2 4) (3 6)
V, (1 4 2) (3 6)
V, (1 2 4) (5 6)
V, (1 4 2) (5 6)
V, (1 2 6) (3 4)
V, (1 6 2) (3 4)
V, (1 2 6) (3 5)
V, (1 6 2) (3 5)
V, (1 2 6) (4 5)
V, (1 6 2) (4 5)
V, (1 3 6) (2 4)
V, (1 6 3) (2 4)
V, (1 3 6) (2 5)
V, (1 6 3) (2 5)
V, (1 3 6) (4 5)
V, (1 6 3) (4 5)
V, (1 2) (3 4) (5 6)
IV (5 6), (1 2) (3 4 5)
IV (5 6), (1 2) (3 5 4)
IV (5 6), (1 2) (3 5 6)
IV (5 6), (1 2) (4 5 6)
IV (5 6), (1 3) (2 5 6)
IV (5 6), (1 5) (2 3 4)
IV (5 6), (1 5) (2 4 3)
IV (5 6), (1 5) (2 3 6)
IV (5 6), (1 5) (2 6 3)
IV (5 6), (1 5) (3 4 6)
IV (5 6), (1 5) (3 6 4)
VI, (1 2)
VI, (1 2 3)

VI. (1 3 2)
VI. (1 2 4)
VI. (1 4 2)
VI. (1 2 5)
VI. (1 5 2)
VI. (1 2) (3 5)
VI. (1 2) (3 6)
VI. (1 2) (4 6)
VI. (1 2 3 4)
VI. (1 4 3 2)
VI. (1 2 4 3)
VI. (1 3 4 2)
VI. (1 4 3 5)
VI. (1 5 3 4)
VI. (1 4 5 3)
VI. (1 3 5 4)
VI. (1 4 6 3)
VI. (1 2) (3 4 5)
VI. (1 2) (3 5 4)
VI. (1 2) (3 4 6)
VI. (1 2) (3 6 4)
VI. (1 2) (3 5 6)
VI. (1 2) (3 6 5)
VI. (1 2) (4 5 6)
VI. (1 2) (4 6 5)
VI. (1 3) (2 4 5)
VI. (1 3) (2 5 4)
VI. (1 3) (2 5 6)
VI. (1 3) (2 6 5)
VI. (1 3) (4 5 6)
VI. (1 3) (4 6 5)
VI. (1 4) (2 3 5)
VI. (1 4) (2 5 3)
VI. (1 4) (2 3 6)
VI. (1 4) (2 6 3)
VI. (1 2 3 4 5)
VI. (1 5 4 3 2)
VI. (1 2 3 5 4)
VI. (1 4 5 3 2)

VI. (1 2 4 3 5)
VI. (1 5 3 4 2)
VI. (1 2 5 4 3)
VI. (1 3 4 5 2)
VI. (1 2 5 3 4)
VI. (1 4 3 5 2)
VI. (1 3 2 4 5)
VI. (1 5 4 2 3)
VI. (1 3 2 5 4)
VI. (1 4 5 2 3)
VI. (1 3 4 2 5)
VI. (1 5 2 4 3)
VI. (1 3 5 2 4)
VI. (1 4 2 5 3)
VI. (1 4 2 3 5)
VI. (1 5 3 2 4)
VI. (1 2) (3 4 6 5)
VI. (1 2) (3 5 6 4)
VI. (1 2) (3 5 4 6)
VI. (1 2) (3 6 4 5)
VI. (1 3) (2 4 5 6)
VI. (1 3) (2 6 5 4)
VI. (1 3) (2 4 6 5)
VI. (1 3) (2 5 6 4)
VI. (1 3) (2 5 4 6)
VI. (1 3) (2 6 4 5)
VI. (1 4) (2 5 3 6)
VI. (1 2 4) (3 6 5)
VI. (1 2 5) (3 6 4)
VI. (1 3 2 5 6 4)
VI. (1 3 5 6 2 4)
VI. (1 4 2 6 5 3)
VI. (1 4 5 6 2 3)
VI. (1 5 6 3 2 4)
$VI_{\frac{1}{2}}$, $(1\ 2\ 6\ 5\ 4\ 3)_{\frac{1}{2}}$
$VI_{\frac{1}{2}}$, $(1\ 3\ 4\ 5\ 6\ 2)_{\frac{1}{2}}$
$VI_{\frac{1}{2}}$, $(1\ 3\ 2\ 6\ 5\ 4)_{\frac{1}{2}}$
$VI_{\frac{1}{2}}$, $(1\ 4\ 3\ 2\ 6\ 5)_{\frac{1}{2}}$

3. Voici encore quelques considérations générales au sujet des systèmes complets de bases indépendantes du groupe symétrique G.

Proposition 4. Quelle que soit la substitution R du groupe symétrique G d'ordre $n!$, les transformées au moyen de R de

deux bases indépendantes quelconques de G sont aussi deux bases indépendantes de G.

Démonstration. Soient S, T et S_1, T_1 deux bases indépendantes de G et soit R une substitution quelconque de G. Il s'agit de montrer que les deux bases

$$S' = RSR^{-1},\quad T' = RTR^{-1}$$

et

$$S'_1 = RS_1R^{-1},\quad T'_1 = RT_1R^{-1}$$

sont indépendantes. En effet, supposons le contraire et soit R_1 une substitution de G, telle que l'on ait, par exemple,

$$R_1S'R_1^{-1} = S'_1,\quad R_1T'R_1^{-1} = T'_1.$$

On a donc

$$R_1RSR^{-1}R_1^{-1} = RS_1R^{-1},\quad R_1RTR^{-1}R_1^{-1} = RT_1R^{-1}.$$

D'où l'on déduit

$$R^{-1}R_1RSR^{-1}R_1^{-1}R = S_1,\quad R^{-1}R_1RTR^{-1}R_1^{-1}R = T_1.$$

Il en découle que S_1 est la transformée de S par la substitution $R^{-1}R_1R$ et que T_1 est la transformée de T par $R^{-1}R_1R$. Les bases S, T et S_1, T_1 ne sont donc pas indépendantes, contrairement à notre hypothèse.

Par un raisonnement tout à fait analogue, on est également conduit à une contradiction en supposant qu'il existe une substitution R_1 de G, telle que

$$R_1S'R_1^{-1} = T'_1,\quad R_1T'R_1^{-1} = S'_1.$$

Les bases S', T' et S'_1, T'_1 sont donc bien indépendantes, c. q. f. d.

Corollaire. Il résulte immédiatement de la proposition 4 que, quelle que soit la substitution S de G et quel que soit le système complet $\mathfrak{S}$ de bases indépendantes de G, si l'on transforme toutes les bases de $\mathfrak{S}$ par S, on obtient également un système complet de bases indépendantes de G.

Soit encore G le groupe symétrique d'ordre $n!$

Nous dirons que deux systèmes complets de bases indépendantes de G

$$B_1,\ B_2,\ \ldots,\ B_M$$
$$B'_1, B'_2, \ldots, B'_M$$

sont distincts s'il existe au moins une base du premier système qui ne figure pas dans le second et vice versa.

Quelle que soit la base B de G et quelle que soit la substitution R de G, nous désignerons dans ce qui suit par B^R la base de G que l'on obtient en transformant les deux substitutions de B par la substitution R.

D'après les lemmes 2 et 3, si B est une base de G qui possède $n!$ transformées au moyen de substitutions de G et si R et R' sont deux substitutions distinctes quelconques de G, on a $B^R \neq B^{R'}$. Par contre, si B est une base de G possédant $\frac{1}{2}n!$ transformées au moyen de substitutions de G, il existe pour toute substitution R de G une substitution R' de G et une seule, telle que $B^R = B^{R'}$.

Soit

$$B_1, B_2, \ldots, B_M \tag{1}$$

un système complet de bases indépendantes de G.

Quelle que soit la substitution R de G, nous savons que le système

$$B_1^R, B_2^R, \ldots, B_M^R \tag{2}$$

constitue également un système complet de bases indépendantes de G. Nous dirons que le système (2) est le transformé de (1) par R.

Montrons que quel que soit le système (1), ses $n!$ transformés au moyen des diverses substitutions de G sont tous distincts. En effet, supposons le contraire et soient R et R' deux substitutions distinctes de G, telles que les deux systèmes (2) et

$$B_1^{R'}, B_2^{R'}, \ldots, B_M^{R'} \tag{3}$$

soient identiques.

Soit $B_i = (S_i, T_i)$ une base du système (1) qui possède $n!$ transformées au moyen de substitutions de G. Si les deux systèmes (1) et (3) sont identiques, il doit exister une base $B_j = (S_j, T_j)$ du système (1), distincte de B_i et telle que $B_i^R = B_j^{R'}$, c. à. d. telle que

$$\text{soit } \begin{cases} RS_iR^{-1} = R'S_jR'^{-1} \\ RT_iR^{-1} = R'T_jR'^{-1}, \end{cases} \qquad \text{soit } \begin{cases} RS_iR^{-1} = R'T_jR'^{-1} \\ RT_iR^{-1} = R'S_jR'^{-1}. \end{cases}$$

Dans le premier cas, on a $S_j = R'^{-1}RS_iR^{-1}R'$, $T_j = R'^{-1}RT_iR^{-1}R'$. Dans le second cas, on a $T_j = R'^{-1}RS_iR^{-1}R'$, $S_j = R'^{-1}RT_iR^{-1}R'$. Dans les deux cas, les bases B_i et B_j ne sont pas indépendantes, ce qui est contradictoire puisqu'elles font toutes deux partie d'un même système complet de bases indépendantes.

Les systèmes (2) et (3) sont donc nécessairement distincts et par suite tout système complet de bases indépendantes possède bien $n!$ transformés distincts au moyen de substitutions de G.

Mais les divers transformés du système (1) au moyen de substitutions de G ne sont pas tous disjoints. En effet, soit $B_k = (S_k, T_k)$ une base du système (1) qui possède $\frac{1}{2}n!$ transformées au moyen de substitutions de G. Il existe alors comme nous savons une substitution R du second ordre faisant partie de G et telle que $RS_kR^{-1} = T_k$, $RT_kR^{-1} = S_k$. Le système complet de bases indépendantes que l'on obtient en transformant le système (1)

au moyen de la substitution R possède alors au moins une base commune B_k avec le système (1). Il peut fort bien exister des transformés du système (1) qui ont en commun avec le système (1) plus d'une base, tout en étant distincts de (1). Cela résulte du fait que pour n suffisamment grand, le groupe symétrique G d'ordre $n!$ peut posséder plusieurs bases indépendantes ayant chacune $\frac{1}{2}n!$ transformées au moyen de substitutions de G et qui sont transformées en elles mêmes par une même substitution du second ordre de G.

Exemple: Soit $n = 7$. On vérifie aisément que les deux couples de substitutions $S = (1\,2\,3\,4)$, $T = (4\,5\,6\,7)$ et $S' = (1\,4)\,(2\,5\,3)$, $T' = (1\,7\,6)\,(4\,5)$ sont des bases du groupe symétrique G d'ordre $7!$ Chacune de ces bases possède $\frac{1}{2}7!$ transformées au moyen de substitutions de G. Ces deux bases sont évidemment indépendantes, puisque les substitutions de l'une de ces bases ne sont pas semblables à celles de l'autre.

Posons $R=(1\,5)\,(2\,6)\,(3\,7)$. On a $\begin{cases} RSR^{-1}=T \\ RTR^{-1}=S \end{cases}$ et $\begin{cases} RS'R^{-1}=T' \\ RT'R^{-1}=S'. \end{cases}$

Si donc nous considérons un système complet de bases indépendantes de G comprenant les deux bases S, T et S', T', le transformé de ce système par la substitution R est un nouveau système complet de bases indépendantes de G qui a en tout cas deux bases communes avec le précédent, tout en étant distinct de ce système.

Il résulte également de ce qui précède que quel que soit le système complet de bases indépendantes (1) du groupe G, si deux systèmes complets de bases indépendantes que l'on obtient du système (1) en le transformant au moyen de deux substitutions différentes R et R' de G ne sont pas disjoints, ils n'ont en commun que des bases possédant $\frac{1}{2}n!$ transformées au moyen de substitutions de G.

4. Il résulte sans peine de la proposition 2 que pour connaître toutes les bases du groupe symétrique G d'ordre $n!$ $(n \geqq 3)$ qui possèdent $\frac{1}{2}n!$ transformées au moyen de substitutions de G, il suffit de connaître toutes les bases de G dont l'une des substitutions est du second ordre.

En effet, soit S, T une base de G qui possède en tout $\frac{1}{2}n!$ transformées distinctes au moyen de substitutions de G. Il existe alors nécessairement, d'après ce qui précède, une substitution R du groupe G, telle que

$$(*) \quad \begin{cases} RSR^{-1} = T \\ RTR^{-1} = S \end{cases}$$

et, d'après la proposition 2, la substitution R est du second ordre. Les deux relations (*) sont donc équivalentes à la seule relation (**) $RSR = T$. Comme S, T est une base de G et que T s'obtient

en composant S et R, on voit immédiatement que S, R est également une base de G. Ainsi, à toute base de G qui possède $\frac{1}{2}n!$ transformées au moyen de substitutions de ce groupe correspond une base S, R de G, dont l'une des substitutions R est du second ordre et telle que les trois substitutions S, R, T vérifient la relation (**). On voit donc bien que si l'on connaît toutes les bases de G dont l'une des substitutions est du second ordre, on peut déterminer toutes les bases de G, dont le nombre des transformées au moyen de substitutions de G est égal à $\frac{1}{2}n!$.

Si une base S, T de G possède en tout $\frac{1}{2}n!$ transformées au moyen de substitutions de G, les deux substitutions S et T sont semblables. Mais il peut aussi exister des bases de G, formées de deux substitutions semblables et qui possèdent $n!$ transformées au moyen de substitutions de G. En effet, soit, p. ex., n un nombre pair quelconque $\geqq 4$ et soit $S=(1\,2\,3\,4\,\ldots\,n)$, $T=(2\,3\,1\,4\,5\,\ldots\,n)$. Ces deux substitutions circulaires constituent une base de G. Or, on vérifie aisément qu'il n'existe aucune substitution R de G, telle que $RSR^{-1}=T$, $RTR^{-1}=S$.

Comme nous l'établirons ailleurs, quel que soit le nombre entier $n>3$, deux substitutions du second ordre ne sauraient constituer une base du groupe symétrique G d'ordre $n!$ Donc, quel que soit l'entier $n>3$, toute base de G dont l'une des substitutions est du second ordre est formée de deux substitutions qui ne sauraient être semblables et par suite une telle base possède $n!$ transformées différentes au moyen de substitutions de G. Par conséquent, si $n>3$, quelle que soit la base S, T de G, possédant $\frac{1}{2}n!$ transformées au moyen de substitutions de G, si R désigne la substitution du second ordre faisant partie de G et telle que $RSR=T$, les deux bases S, R et S, T sont indépendantes.

Montrons que quelles que soient les bases indépendantes S, T et S_1, T_1 du groupe symétrique G d'ordre $n!$ ($n>3$), possédant chacune $\frac{1}{2}n!$ transformées au moyen de substitutions de G, si R et R_1 désignent les deux substitutions du second ordre de G, telles que $RSR=T$, $R_1S_1R_1=T_1$, alors S, R et S_1, R_1 sont deux bases indépendantes de G. En effet, comme nous savons, chacun de ces couples de substitutions est une base de G et comme les deux substitutions R et R_1 sont du second ordre, n étant supposé >3, aucune des substitutions S, S_1 n'est semblable ni à R ni à R_1.

Supposons que les bases S, R et S_1, R_1 ne sont pas indépendantes. Il existe alors une substitution U de G, telle que l'on a

$$USU^{-1}=S_1,\quad URU^{-1}=R_1.$$

On en déduit

$$T_1=R_1S_1R_1=URU^{-1}USU^{-1}URU^{-1}=URSRU^{-1}=UTU^{-1}.$$

Ainsi S_1 est la transformée de S par U et T_1 est la transformée

de T par U. Donc les deux bases S, T et S_1, T_1 ne sont pas indépendantes, contrairement à notre hypothèse. Notre supposition est donc erronnée et les bases S, R et S_1, R_1 sont bien indépendantes, c. q. f. d.

Nous en concluons que quel que soit le nombre entier $n > 3$, à tout système de M_2 bases indépendantes de G, possédant chacune $\frac{1}{2}n!$ transformées au moyen de substitutions de G, correspondent M_2 bases indépendantes de G formées chacune de deux substitutions dont l'une est du second ordre, chacune de ces bases ayant $n!$ transformées au moyen de substitutions de G.

On en déduit immédiatement que le nombre total m de bases indépendantes de G, dont chacune contient une substitution du second ordre, est $\geqq M_2$.

Je dis que quel que soit le nombre entier $n > 3$, on a $m > M_2$. En effet, quel que soit le nombre entier $n > 3$, il existe des bases S, R de G, dont l'une des substitutions S est de classe paire et l'autre R est du second ordre. Telles sont, par exemple, pour n impair, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $R = (1\ 2)$, et, pour n pair, les deux substitutions $S = (1\ 2\ \ldots\ n-1)$, $R = (n-1\ n)$. La substitution $T = RSR$ est alors aussi de classe paire et, par suite, les deux substitutions S et T ne sauraient constituer une base de G.

Or, une telle base S, R est indépendante de toute base S_1, R_1 de G, dont l'une des substitutions R_1 est du second ordre et telle que les deux substitutions S_1 et $T_1 = R_1S_1R_1$ constituent également une base de G. En effet, quelle que soit la base S_1, R_1 jouissant des propriétés énumérées ci-dessus, si cette base n'était pas indépendante de S, T, il devrait exister une substitution U de G, telle que $US_1U^{-1} = S$, $UR_1U^{-1} = R$.

Posons $$T = RSR.$$

On aurait alors

$$T = UR_1U^{-1}US_1U^{-1}UR_1U^{-1} = UR_1S_1R_1U^{-1} = UT_1U^{-1}.$$

S serait donc la transformée de S_1 par U et T — la transformée de T_1 par U. Or, comme par hypothèse S_1, T_1 est une base de G, il en serait de même de S, T, contrairement à notre supposition. Les bases S, R et S_1, R_1 sont donc bien indépendantes.

On a donc bien $m > M_2$, quel que soit $n > 3$, c. q. f. d.

Des considérations ci-dessus il résulte que le nombre total M de bases indépendantes du groupe symétrique G d'ordre $n!$ ($n > 3$) est $\geqq m + M_2$, et comme $M_1 \geqq m > M_2$ et $M = M_1 + M_2$, on a $M > 2M_2$.

Lorsque le degré n du groupe G augmente, les deux nombres M_1 et M_2 augmentent aussi, mais il n'existe pas de relation simple entre les trois nombres n, M_1 et M_2.

Le tableau suivant indique, dans le cas de $n = 3, 4, 5$ et 6, pour chaque base S, T de G, faisant partie du système complet de bases indépendantes indiqué plus haut et possédant $\frac{1}{2}n!$ transformées au moyen de substitutions de G, la substitution de second ordre R, telle que $T = RSR$.

	S	T	R
$n = 3$	(1 2)	(2 3)	(1 3)
$n = 4$	(1 2 3 4)	(1 3 2 4)	(2 3)
$n = 5$	(1 2 3 4)	(1 2 3 5)	(4 5)
	(1 2 3 4)	(1 5 3 2)	(1 3) (4 5)
	(1 2 3) (4 5)	(1 2 4) (3 5)	(3 4)
	(1 2 3) (4 5)	(1 4 2) (3 5)	(1 2) (3 4)
	(1 2 3) (4 5)	(1 4 5) (2 3)	(2 4) (3 5)
$n = 6$	(1 2 3) (4 5)	(1 4) (2 6 5)	(1 5) (3 6)
	(1 2 3) (4 5)	(1 4) (3 5 6)	(1 5) (2 6)
	(1 2 3) (4 5)	(1 6) (2 3 4)	(1 4) (5 6)
	(1 2 3) (4 5)	(1 6) (2 4 3)	(1 4) (2 3) (5 6)
	(1 2 3 4 5 6)	(2 1 3 4 5 6)	(1 2)
	(1 2 3 4 5 6)	(2 6 5 4 3 1)	(3 6) (4 5)
	(1 2 3 4 5 6)	(2 6 5 4 1 3)	(2 3) (4 6)
	(1 2 3 4 5 6)	(2 6 5 1 4 3)	(2 4) (5 6)

Remarque. Nous avons vu qu'en dehors de la substitution identique, il n'existe aucune substitution du groupe symétrique G d'ordre $n!$ qui soit permutable avec les deux substitutions S et T d'une base de G. On peut se demander si tout couple de substitutions de G qui ne sont simultanément permutables avec aucune substitution $\neq 1$ de G constitue une base de ce groupe? La réponse à cette question est négative, comme le montre l'exemple suivant:

Soit $n = 5$, $S = (1\ 2\ 3\ 4\ 5)$, $T = (2\ 3\ 5\ 4)$.

Ces deux substitutions appartiennent au groupe métacyclique d'ordre 20. Donc elles ne sauraient constituer une base ni du groupe symétrique ni du groupe alternant de degré 5. Or, je dis qu'il n'existe aucune substitution $\neq 1$ du groupe symétrique d'ordre 5! qui soit permutable aussi bien avec S qu'avec T. En effet, comme on le prouve aisément, les seules substitutions permutables avec S sont les diverses itérées de S. Ce sont, notamment, les substitutions (1 2 3 4 5), (1 3 5 2 4), (1 4 2 5 3), (1 5 4 3 2) et 1, et les transformées de T par les quatre premières de ces substitutions sont: (3 4 1 5), (4 5 2 1), (5 1 3 2) et (1 2 4 3). Aucune de ces substitutions n'est égale à T, ce qui démontre notre assertion.

5. D'une façon générale, étant donné un groupe quelconque de substitutions G, nous appellerons base de ce groupe tout système

formé d'un nombre déterminé k de substitutions de G qui permettent, par composition, d'engendrer ce groupe, alors qu'aucun système formé d'un nombre inférieur à k de substitutions de G ne permet d'engendrer ce groupe.

Envisageons, en particulier, le groupe alternant G_1 de degré n. Il est d'ordre $\frac{1}{2}n!$

Si $n = 3$, une seule substitution permet d'engendrer G_1. Par contre, si $n > 3$, le groupe G ne saurait être engendré par une seule de ses substitutions. Mais on démontre aisément que quel que soit le nombre entier $n > 3$, il existe des couples de substitutions de G qui constituent des bases de ce groupe. Telles sont, par exemple, lorsque n est impair, les deux substitutions $S = (1\ 2\ \ldots\ n)$, $T = (1\ 2\ 3)$, et, lorsque n est pair, les deux substitutions $S = (1\ 2\ 3)$, $T = (2\ 3\ \ldots\ n)$.

On démontre, par un raisonnement tout à fait analogue à celui que nous avons fait pour le groupe symétrique, que, quel que soit le nombre entier $n > 3$ et quelle que soit la base S, T du groupe alternant G_1 de degré n, il n'existe aucune substitution $\neq 1$ de G_1 qui soit permutable aussi bien avec S qu'avec T et il existe au plus une substitution R de G_1, telle que $RSR^{-1} = T$ et $RTR^{-1} = S$. Lorsqu'une telle substitution R existe, elle est nécessairement du second ordre. *Le nombre total N_1 de bases du groupe G_1 est un multiple de $\frac{1}{4}n!$*

Parmi les autres sous-groupes remarquables du groupe symétrique G d'ordre $n!$ qui possèdent, quel que soit l'entier $n > 4$, une base formée de deux substitutions, citons le groupe métacyclique.

Mais il existe, aussi, comme on sait, pour n suffisamment grand, des sous-groupes de G qui ne sauraient être engendrés par deux substitutions. Comme il découle de la théorie des groupes abéliens de substitutions, il existe pour tout nombre entier $m > 2$ donné d'avance, de tels groupes dont une base se compose de m substitutions.

*

O basích symetrické grupy.

(Obsah předešlého článku.)

Budiž G symetrická grupa řádu $n!$ ($n \geqq 3$); basí této grupy nazýváme každou dvojici jejích prvků, jež vytvořuje celou grupu G. Tyto base (jejichž počet je násobkem čísla $\frac{1}{2}n!$) jsou studovány v této práci; připojena je tabulka, udávající úplný systém nezávislých basí pro $n = 3, 4, 5, 6$.