

Groupe symétrique

Dans ce chapitre, n désigne un entier naturel non nul.

I. Généralités

Définition. On appelle groupe symétrique d'ordre n et on note \mathcal{S}_n le groupe des permutation de l'ensemble $\llbracket 1, n \rrbracket$. Les éléments de \mathcal{S}_n sont appelés permutations.

Proposition. Le groupe \mathcal{S}_n est de cardinal $n!$

Soit σ une permutation de \mathcal{S}_n . On la notera

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

Définition. On appelle support d'une permutation $\sigma \in \mathcal{S}_n$ l'ensemble

$$\{k \in \llbracket 1, n \rrbracket, \sigma(k) \neq k\}$$

Remarque : le support de la permutation Id est l'ensemble vide.

Définition. Soit $k \geq 2$. On dit qu'une permutation σ est un k -cycle s'il existe k entiers distincts a_1, \dots, a_k entre 1 et n tels que

$$\begin{cases} \forall p \in \llbracket 1, k-1 \rrbracket, & \sigma(a_p) = a_{p+1} \\ & \sigma(a_k) = a_1 \\ \forall p \in \llbracket 1, n \rrbracket \setminus \{a_1, \dots, a_k\}, & \sigma(p) = p \end{cases}$$

On note $\sigma = (a_1, \dots, a_k)$.

Un 2-cycle est appelé une transposition.

Remarque : les notations $(1, 2)$ et $(2, 1)$ représentent deux écritures possibles de la même transposition qui échange 1 et 2.

Remarque : le groupe \mathcal{S}_n n'est pas commutatif dès que $n \geq 3$.

En effet, $(1, 2, 3)(1, 2) = (1, 2, 3) \neq (2, 3) = (1, 2)(1, 2, 3)$.

Proposition. Deux permutations à support disjoints commutent.

Proposition. Soit (G, \star) un groupe de cardinal fini N et $g \in G$.

Il existe un unique $p \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z} : g^k = e\} = p\mathbb{Z}$. Cet entier p est appelé ordre de g .

On a en particulier que $p = \text{Min}\{k \in \mathbb{N}^* : g^k = e\}$

Corollaire. Soit $\sigma \in \mathcal{S}_n$

Il existe un unique $p \in \mathbb{N}^*$ tel que $\{k \in \mathbb{Z} : \sigma^k = Id\} = p\mathbb{Z}$. Cet entier p est appelé ordre de σ .

On a en particulier que $p = \text{Min}\{k \in \mathbb{N}^* : \sigma^k = e\}$

Proposition. Un k -cycle est d'ordre k .

II. Décomposition canonique d'une permutation

Théorème. (*admis*)

Soit $\sigma \in \mathcal{S}_n$ une permutation, alors σ s'écrit comme un produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près.

Proposition. Soit (a_1, a_2, \dots, a_k) un cycle. On a :

$$(a_1, a_2, \dots, a_k) = (a_1, a_2)(a_2, a_3)\dots(a_{k-1}, a_k) = (a_1, a_k)(a_1, a_{k-1})\dots(a_1, a_2).$$

Proposition. Toute permutation peut s'écrire comme un produit de transpositions. On dit que les transpositions engendrent le groupe symétrique \mathcal{S}_n .

Remarque : Attention, la décomposition d'une permutation en produit de transpositions n'est pas unique et les transpositions ne sont pas à support disjoints. C'est une différence importante avec la décomposition en cycles à support disjoints.

III. Signature, groupe alterné

Théorème. (*admis*) Il existe un unique morphisme de groupes non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$. On l'appelle signature et on le note ε .

Proposition. Toute transposition est de signature -1 .

Corollaire. La signature d'un k -cycle est égale à $(-1)^{k-1}$.

Définition. Le noyau de ε est un sous-groupe de \mathcal{S}_n appelé groupe alterné et noté \mathcal{A}_n .

Exemple. $\mathcal{A}_1 = \{Id\}$, $\mathcal{A}_2 = \{Id\}$ et $\mathcal{A}_3 = \{Id, (1, 2, 3), (1, 3, 2)\}$. Le groupe \mathcal{A}_3 est abélien. Pour $n > 3$, le groupe \mathcal{A}_n n'est pas commutatif car $(1, 2, 3)(1, 2, 4) \neq (1, 2, 4)(1, 2, 3)$.

Proposition. Soit τ une transposition de \mathcal{S}_n . L'application $\phi : \mathcal{S}_n \rightarrow \mathcal{S}_n$, $\sigma \mapsto \tau\sigma$ est involutive et donc bijective. Comme $\phi(\mathcal{A}_n) = \mathcal{S}_n \setminus \mathcal{A}_n$, on en déduit que

$$\#\mathcal{A}_n = \frac{\#\mathcal{S}_n}{2} = \frac{n!}{2}.$$

IV. Compléments

Définition. Soit $\sigma \in \mathcal{S}_n$ et $k \in \llbracket 1, n \rrbracket$. On appelle orbite de k sous l'action de σ l'ensemble

$$\mathcal{O}_\sigma(k) = \{\sigma^p(k), p \in \mathbb{N}\}$$

Exemple. L'orbite de 1 par la transposition $(1, 2)$ est l'ensemble $\{1, 2\}$ alors que l'orbite de 3 par la même transposition est le singleton $\{3\}$.

Proposition. Soit $\sigma \in \mathcal{S}_n$. La relation \mathcal{R} définie sur $\llbracket 1, n \rrbracket$ par

$$\forall(k, k') \in \llbracket 1, n \rrbracket^2, \quad k \mathcal{R} k' \Leftrightarrow k' \in \mathcal{O}_\sigma(k)$$

est une relation d'équivalence.

La classe d'un entier k pour cette relation est son orbite sous l'action de σ .

Les orbites sous l'action de σ forment donc une partition de $\llbracket 1, n \rrbracket$.

Démonstration. Pour tout entier $k \in \llbracket 1, n \rrbracket$, on a $\sigma^0(k) = k$, donc $k \in \mathcal{O}(k)$ et la relation \mathcal{R} est réflexive. Supposons que pour un certain entier p , on ait $k' = \sigma^p(k)$. Alors en composant par σ^{r-p} , où r est l'ordre de σ , on obtient

$$\sigma^{r-p}(k') = \sigma^r(k) = k$$

Donc $k \in \mathcal{O}(k')$ et la relation \mathcal{R} est symétrique. On suppose maintenant que l'on a, pour un certain couple d'entiers (p, q) ,

$$k' = \sigma^p(k) \quad \text{et} \quad k'' = \sigma^q(k')$$

Alors on en déduit $k'' = \sigma^{p+q}(k)$, puis $k'' \in \mathcal{O}(k)$ et la relation \mathcal{R} est transitive. C'est donc une relation d'équivalence sur l'ensemble $\llbracket 1, n \rrbracket$.

De plus, la classe d'un entier k est l'ensemble des éléments de l'orbite de k . L'ensemble des orbites forme donc une partition de $\llbracket 1, n \rrbracket$. \square

Proposition. Soit $\sigma \in \mathcal{S}_n$ et $k \in \llbracket 1, n \rrbracket$.

Si l'on note r le cardinal de $\mathcal{O}_\sigma(k)$, alors $\mathcal{O}_\sigma(k) = \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-1}(k)\}$ et $\sigma^r(k) = k$.

Démonstration. Par définition de $\mathcal{O}_\sigma(k)$, on a déjà $\{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-1}(k)\} \subset \mathcal{O}_\sigma(k)$. Il reste à prouver que $\{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-1}(k)\}$ est de cardinal r pour conclure.

Supposons par l'absurde qu'il ne le soit pas.

Il existe alors $(i, j) \in \llbracket 0, r-1 \rrbracket^2$ tel que $i < j$ et $\sigma^i(k) = \sigma^j(k)$. Comme σ est injective, on en déduit que $\sigma^{j-i}(k) = k$ puis que $\mathcal{O}_\sigma(k) \subset \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{j-i-1}(k)\}$. Ainsi, $\mathcal{O}_\sigma(k)$ est de cardinal inférieur ou égal à $j-i$. Comme $j-i \leq r-1-i \leq r-1$, on aboutit à une absurdité. Donc $\mathcal{O}_\sigma(k) = \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-1}(k)\}$.

Par définition, $\sigma^r(k) \in \mathcal{O}_\sigma(k)$ donc il existe $i \in \llbracket 0, r-1 \rrbracket$ tel que $\sigma^r(k) = \sigma^i(k)$. On a donc $\mathcal{O}_\sigma(k) \subset \{k, \sigma(k), \sigma^2(k), \dots, \sigma^{r-i-1}(k)\}$ et donc, pour des raisons de cardinal $r \leq r-i$ puis $i = 0$. \square

Corollaire. Si σ est une permutation telle qu'il n'existe qu'une orbite non réduite à un élément, alors σ est un cycle et réciproquement.

Démonstration. On remarque que si σ est le cycle (a_1, \dots, a_k) , alors l'orbite de a_1 est la seule orbite non réduite à un élément. Réciproquement, soit σ une permutation telle qu'il n'existe qu'une orbite non réduite à un élément et a un élément de cette orbite. Soit k le plus petit entier non nul tel que $\sigma^k(a) = a$. Elle s'écrit alors

$$\mathcal{O} = \{a, \sigma(a), \dots, \sigma^{k-1}(a)\}$$

où les $(\sigma^i(a))_{i \in \llbracket 0, k-1 \rrbracket}$ sont distincts. Ainsi, $\sigma = (a, \sigma(a), \dots, \sigma^{k-1}(a))$. \square

Proposition. Soit $\sigma \in \mathcal{S}_n$ et \mathcal{O} une orbite sous l'action de σ . L'orbite \mathcal{O} est stable par σ .

Démonstration. On considère un élément $k \in \mathcal{O}$, alors \mathcal{O} est l'orbite de k , ce qui implique $\sigma(k) \in \mathcal{O}$. On en déduit que \mathcal{O} est stable par σ , ce qui autorise à définir la restriction $\sigma|_{\mathcal{O}}$.

On note r le cardinal de \mathcal{O} et on définit la suite a_p par récurrence de la manière suivante : $a_1 = k$ et, pour tout entier $p > 1$, $a_p = \sigma(a_{p-1})$. On remarque alors que les entiers $(a_p)_{p \in \llbracket 1, r \rrbracket}$ sont distincts et que

$$\mathcal{O} = \{a_1, \dots, a_r\}$$

Finalement, $\sigma|_{\mathcal{O}}$ est le cycle (a_1, \dots, a_r) . \square

Théorème. (admis)

Soit $\sigma \in \mathcal{S}_n$ une permutation, alors σ s'écrit comme un produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près.

Démonstration.

Existence :

Notons N le nombre d'orbites non réduites à un point et $\mathcal{O}_\sigma(k_1), \dots, \mathcal{O}_\sigma(k_N)$ les N orbites distinctes et r_1, \dots, r_N leurs cardinaux respectifs.

Pour tout $i \in \llbracket 1, n \rrbracket$, on note $c_i = (k_i, \sigma(k_i), \sigma^2(k_i), \dots, \sigma^{r_i-1}(k_i))$.

D'après la propriété précédente, pour tout $i \in \llbracket 1, n \rrbracket$, c_i est un cycle (car les entiers $k_i, \sigma(k_i), \dots, \sigma^{r_i-1}(k_i)$ sont distincts), de support $\mathcal{O}_\sigma(k_i)$ et σ et c_i coïncident sur $\mathcal{O}_\sigma(k_i)$.

Comme les orbites $\mathcal{O}_\sigma(k_1), \dots, \mathcal{O}_\sigma(k_N)$ sont des classes d'équivalences distinctes, elles sont disjointes deux à deux donc les cycles c_1, \dots, c_r sont à supports disjoints.

Ils commutent donc et $c_1 \circ \dots \circ c_r$ coïncide avec σ sur $\bigcup_{i=1}^r \mathcal{O}_\sigma(k_i)$.

Enfin, les entiers appartenant à $\llbracket 1, n \rrbracket \setminus \bigcup_{i=1}^r \mathcal{O}_\sigma(k_i)$ sont invariants par σ et par $c_1 \circ \dots \circ c_r$.

Ainsi, $\sigma = c_1 \circ \dots \circ c_r$; σ s'écrit donc comme un produit de cycles à support disjoints.

Unicité à l'ordre près : Supposons que l'on dispose d'une autre décomposition

$$\sigma = \tau_1 \circ \dots \circ \tau_m$$

où les τ_i sont des cycles à support disjoints. Les orbites non triviales de σ sont alors les supports des τ_i , ce qui montre que $m = r$.

Quitte à ré-ordonner, on a donc pour tout $i \in \llbracket 1, r \rrbracket$, $\text{Supp } \tau_i = \text{Supp } c_i$; on notera \mathcal{O}_i ce support commun.

Comme les permutations τ_1, \dots, τ_r sont à support disjoints, pour tout $i \in \mathcal{O}_i$, \mathcal{O}_i est invariant par les τ_j avec $j \neq i$. Comme \mathcal{O}_i est stable par σ , on en déduit que

$$\forall i \in \llbracket 1, r \rrbracket, \forall \ell \in \llbracket 1, n \rrbracket, \sigma(k) = \tau_i(k)$$

Mais, les cycles c_1, \dots, c_r étant à supports disjoints, on a aussi

$$\forall i \in \llbracket 1, r \rrbracket, \forall \ell \in \llbracket 1, n \rrbracket, \sigma(k) = c_i(k)$$

Donc, pour tout $i \in \llbracket 1, r \rrbracket$, les permutation τ_i et c_i coïncident sur leur support, ce qui implique leur égalité et achève la preuve de l'unicité. \square

Proposition. Soit $\sigma \in \mathcal{S}_n$ une permutation qui s'écrit de deux façons différentes comme produit de transposition

$$\sigma = \tau_1 \tau_2 \dots \tau_p = \tau'_1 \tau'_2 \dots \tau'_q$$

alors les entiers p et q ont la même parité.

Démonstration. Par l'absurde, on suppose que p et q n'ont pas la même parité. Alors $p + q$ est impair et on a

$$Id = \tau_1 \tau_2 \dots \tau_p \tau'_q \dots \tau'_2 \tau'_1$$

On a donc décomposé Id en un nombre impair de permutation, ce qui est impossible d'après le lemme qui suit. On en déduit que p et q ont la même parité. \square

Lemme. Soit r un entier naturel. Il n'existe de pas de décomposition de Id en un produit de $2r + 1$ transpositions.

Démonstration. On démontre le résultat par récurrence sur r . Pour $r = 0$, la proposition est vraie. On la suppose donc vraie au rang $r - 1$ pour un certain entier naturel r et on écrit

$$Id = \tau_1 \dots \tau_{2r}(ij)$$

En comparant les supports des transpositions (ij) et τ_{2r} , on a alors quatre possibilités :

- Si $\tau_{2r} = (ij)$, alors on a $Id = \tau_1 \dots \tau_{2r-1}$, ce qui est impossible par hypothèse de récurrence.
- Si $i \in \text{Supp}(\tau_{2r})$, mais $j \notin \text{Supp}(\tau_{2r})$, alors $\tau_{2r} = (ik)$ avec $k \neq j$ et on peut écrire

$$Id = \tau_1 \dots \tau_{2r-1}(ik)(ij) = \tau_1 \dots \tau_{2r-1}(ij)(jk)$$

et on remarque que, dans ce cas, $i \notin \text{Supp}(jk)$.

— Si $j \in \text{Supp}(\tau_{2r})$, mais $i \notin \text{Supp}(\tau_{2r})$, alors $\tau_{2r} = (jk)$ avec $k \neq j$ et on peut écrire

$$Id = \tau_1 \dots \tau_{2r-1}(jk)(ij) = \tau_1 \dots \tau_{2r-1}(ik)(jk)$$

et on remarque que, dans ce cas, $i \notin \text{Supp}(jk)$.

— Si $i \notin \text{Supp}(\tau_{2r})$ et $j \notin \text{Supp}(\tau_{2r})$, alors les transpositions (i, j) et τ_{2r} sont a support disjoints donc elles commutent. On écrit alors

$$Id = \tau_1 \dots \tau_{2r-1}(ij)\tau_{2r}$$

Dans ce cas aussi, on a $i \notin \text{Supp}(\tau_{2r})$.

Finalement, on peut écrire

$$Id = \tau_1 \dots \tau_{2n-1}(ik)\tau'_{2r+1} \quad \text{avec} \quad i \notin \text{Supp}(\tau'_{2r+1})$$

En répétant l'algorithme précédent, on a deux éventualités :

- Soit on s'arrête car on fait apparaître deux transpositions identique et on applique l'hypothèse de récurrence
- Soit on peut écrire

$$Id = (ik')\tau'_2 \dots \tau'_{2r+1} \quad \text{avec} \quad i \notin \bigcup_{p=2}^{2r+1} \text{Supp}(\tau'_p)$$

ce qui est absurde puisque i n'est pas un point fixe de la permutation de droite.

On a donc montré que l'identité ne peut s'écrire comme produit d'un nombre impair de transpositions. \square

Définition. On dit que deux permutations σ_1 et σ_2 sont conjuguées s'il existe une permutation τ telle que

$$\sigma_2 = \tau\sigma_1\tau^{-1}$$

Proposition. La relation \mathcal{R} définie sur \mathcal{S}_n par

$$\forall (\sigma_1, \sigma_2) \in \mathcal{S}_n^2, \quad \sigma_1 \mathcal{R} \sigma_2 \quad \text{si} \quad \exists \tau \in \mathcal{S}_n \quad \sigma_2 = \tau\sigma_1\tau^{-1}$$

est une relation d'équivalence.

Démonstration. Montrons que la relation \mathcal{R} est une relation d'équivalence. Soit $\sigma \in \mathcal{S}_n$. Si on prend $\tau = Id$, on a $\sigma \mathcal{R} \sigma$ et la relation \mathcal{R} est réflexive. On suppose maintenant qu'il existe $\tau \in \mathcal{S}_n$ telle que

$$\sigma_2 = \tau\sigma_1\tau^{-1}$$

Alors on a aussi

$$\sigma_1 = \tau^{-1}\sigma_2\tau$$

ce qui montre que la relation \mathcal{R} est symétrique. Enfin, si on a

$$\sigma_2 = \tau\sigma_1\tau^{-1} \quad \text{et} \quad \sigma_3 = \tau'\sigma_2\tau'^{-1}$$

alors on a

$$\sigma_3 = \tau'\tau\sigma_1\tau\tau'^{-1} = (\tau'\tau)\sigma_1(\tau'\tau)^{-1}$$

ce qui montre la transitivité. Finalement, la conjugaison est une relation d'équivalence sur \mathcal{S}_n . \square

La proposition suivante permet de décrire les classe d'équivalence pour la relation de conjugaison (on les appelle classe de conjugaison).

Proposition. Deux transpositions quelconques sont conjuguées dans \mathcal{S}_n . Plus généralement, pour tout entier $1 \leq k \leq n$, deux k -cycles sont conjugués dans \mathcal{S}_n

Démonstration. Soit k un entier naturel compris entre 1 et n et (a_1, \dots, a_k) et (b_1, \dots, b_k) , deux k -cycles. On considère la permutation τ définie par

$$\tau = \begin{pmatrix} a_1 & a_2 & \dots & a_k \\ b_1 & b_2 & \dots & b_k \end{pmatrix}$$

alors on a

$$(b_1, \dots, b_k) = \tau(a_1, \dots, a_k)\tau^{-1}$$

ce qui montre que deux k -cycles sont conjugués. \square

Corollaire. *Deux permutations quelconques sont donc conjuguées si et seulement si elles admettent, dans leur décomposition canonique, le même nombre de k -cycle pour tout entier k entre 2 et n .*

Théorème. (admis) *Il existe un unique morphisme de groupes non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$. On l'appelle signature et on le note ε .*

Démonstration. Prouvons l'existence d'un unique morphisme de groupes non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$.

Unicité :

Soit ϕ un morphisme non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$. Soient $\sigma = (i, j)$ et $\sigma' = (i', j')$ deux transpositions.

Pour toute permutation τ , on a $\tau\sigma\tau^{-1} = (\tau(i), \tau(j))$. Ainsi, il existe une permutation τ telle que $\tau\sigma\tau^{-1} = \sigma'$. En particulier,

$$\phi(\sigma') = \phi(\tau')\phi(\sigma)\phi(\tau^{-1}) = \phi(\sigma)$$

Donc ϕ est constant sur les transpositions.

Si ϕ est constant à 1 sur toutes les transpositions alors, comme les transpositions engendrent \mathcal{S}_n , on en déduit que ϕ est trivial.

Par conséquent, ϕ est constant à -1 sur toutes les transpositions. Par suite, ϕ est nécessairement l'application qui à tout produit de r transposition associe $(-1)^r$.

Existence :

On note $E = \mathcal{P}_2(\llbracket 1, n \rrbracket)$, l'ensemble des parties de $\llbracket 1, n \rrbracket$ à deux éléments et on considère l'application

$$\varepsilon : \mathcal{S}_n \rightarrow \{-1, 1\}, \sigma \mapsto \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i, j\} \in E} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Commençons par vérifier que ε est bien définie. Soit $\sigma \in \mathcal{S}_n$ alors l'application

$$E \rightarrow E, \{i, j\} \mapsto \{\sigma(i), \sigma(j)\}$$

est une bijection donc

$$\prod_{1 \leq i < j \leq n} |\sigma(j) - \sigma(i)| = \prod_{1 \leq i < j \leq n} |j - i|$$

et $\varepsilon(\sigma) \in \{-1, 1\}$.

Soit $\tau = (i, j)$ une transposition avec $i < j$ alors

$$\varepsilon(\tau) = \frac{\tau(j) - \tau(i)}{j - i} \prod_{k \in \llbracket 1, n \rrbracket \setminus \{i, j\}} \frac{\tau(k) - \tau(i)}{k - i} \frac{\tau(j) - \tau(j)}{j - k} \prod_{\{i', j'\} \in E \setminus \{\{i, j\}\}} \frac{\tau(j') - \tau(i')}{j' - i'}$$

donc $\varepsilon(\tau) = -1$.

Il reste à montrer que ε est un morphisme. Pour cela, on considère deux permutations σ et τ .

On a

$$\begin{aligned} \prod_{i < j} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} &= \prod_{\{i,j\} \in E} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \prod_{\{i,j\} \in E} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{\{i,j\} \in E} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \prod_{\{i,j\} \in E} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{\{i,j\} \in E} \frac{\tau(j) - \tau(i)}{j - i} \end{aligned}$$

car l'application τ est bijective. On a donc montré que l'application ε est un morphisme de groupe non trivial de \mathcal{S}_n dans $(\{-1, 1\}, \times)$.

On peut aussi démontrer l'existence en posant

$$\varepsilon : \mathcal{S}_n \rightarrow \{-1, 1\}, \sigma \mapsto (-1)^r \text{ où } r \text{ est le nombre de transpositions apparaissant dans une écriture de } \sigma.$$

Cette définition a un sens car on a montré que si $\tau_1 \tau_2 \dots \tau_p = \tau'_1 \tau'_2 \dots \tau'_q$ avec $\tau_1, \tau_2, \dots, \tau_p, \tau'_1, \tau'_2, \dots, \tau'_q$ des transpositions, alors les entiers p et q ont la même parité.

Enfin, ε est alors trivialement un morphisme de groupes non trivial. \square