La théorie des groupes au secours de la combinatoire

Xavier Caruso

Janvier 2009

Résumé

Le but de cette note est de montrer comment la théorie des groupes permet de résoudre — de façon peut-être un peu inattendue — un exercice issu d'une olympiade iranienne. Durant la solution, on essaie en outre d'expliquer *un peu* les idées essentielles qui permettent de transposer le problème en une question de théorie des groupes et les méthodes générales que l'on peut utiliser pour résoudre cette dernière.

Énoncé

On dispose d'une infinité de jetons que l'on va répartir sur un cercle selon certaines règles. Chaaue jeton a une face est peinte en rouge et l'autre face peinte en bleu. On commence par placer deux jetons, la face rouge étant visible. On s'autorise maintenant à faire les deux manipulations suivantes :

- ☞ si A et B désignent deux jetons côté à côté sur le cercle, on s'autorise à retourner A et B à condition de placer un jeton, face rouge visible, entre A et B ;
- ☞ si un jeton X dont on voit la face rouge est placé entre deux jetons A et B distincts, on s'autorise à retourner A et B à condition de retirer X.

Pour quels entiers n est-il possible d'obtenir, en itérant un certain nombre (fini) de fois les deux transformations précédentes, une configuration avec exactement n jetons, chacun montrant sa face rouge.

Solution

Pour simplifier les notations (et les dessins que nous n'allons pas faire), nous allons représenter les configurations à l'aide de mots écrits sur l'alphabet $\{\mathtt{R}, \mathtt{B}\}$: lorsque l'on a une configuration, on se fixe une origine, et on écrit le mot obtenu en parcourant le cercle dans le sens trigonométrique depuis cette origine, et en ajoutant la lettre $\mathtt{R}$ (resp. la lettre $\mathtt{B}$) lorsque l'on croise un jeton face rouge visible (resp. face bleue visible). On prendra garde au fait que le mot obtenu de cette façon peut dépendre du choix de l'origine ; ainsi si l'on souhaite réellement représenter les configurations, on est amené à identifier deux mots lorsque l'un se déduit de l'autre en déplaçant sa première lettre à la fin. Au niveau des mots, les transformations autorisées sont les suivantes

$$\mathtt{RR} \leftrightarrow \mathtt{BRB} \quad ; \quad \mathtt{RB} \leftrightarrow \mathtt{BRR} \quad ; \quad \mathtt{BR} \leftrightarrow \mathtt{RRB} \quad ; \quad \mathtt{BB} \leftrightarrow \mathtt{RRR} \tag{1}$$

où la notation signifie que l'on a le droit de remplacer n'importe où dans le mot la suite de lettres qui apparaît à gauche du signe $\leftrightarrow$ et par celle qui apparaît à droite, et vice et versa. On écrira dans la suite $x \sim y$ si le mot x peut s'obtenir à partir de y en un nombre fini d'étapes, soit en utilisant les remplacements précédents, soit en déplaçant la première lettre à la fin. On notera également $\mathtt{R}^n$ (resp. $\mathtt{B}^n$) pour signifier une suite de n lettres toutes égales à $\mathtt{R}$ (resp. à $\mathtt{B}$). La question revient donc à chercher les entiers n pour lesquels $\mathtt{R}^n \sim \mathtt{R}^2$.

Nous allons montrer dans un premier temps que tous les entiers $n \geqslant 2$ qui ne sont pas multiples de 3 conviennent. Il est déjà clair que $n = 1$ ne peut convenir car les manipulations autorisées laissent toujours au moins deux jetons. Maintenant, si k et ℓ sont deux entiers, on remarque que

$$\mathtt{BR}^k\mathtt{BR}^\ell = \mathtt{BR}^k(\mathtt{BR})\mathtt{R}^{\ell-1} \sim \mathtt{BR}^k(\mathtt{RRB})\mathtt{R}^{\ell-1} = \mathtt{BR}^{k+2}\mathtt{BR}^{\ell-1}$$

d'où on obtient par une récurrence immédiate $\mathtt{BR}^k\mathtt{BR}^\ell \sim \mathtt{BR}^{k+2\ell}\mathtt{B}$. On en déduit que

$$\mathtt{R}^k = (\mathtt{RR})\mathtt{R}^{k-2} \sim \mathtt{BRBR}^{k-2} \sim \mathtt{BR}^{2k-3}\mathtt{B} \sim \mathtt{R}^{2k-3}(\mathtt{BB}) \sim \mathtt{R}^{2k-3}(\mathtt{RRR}) = \mathtt{R}^{2k}$$

pour tout entier $k \geqslant 2$ et que

$$\mathtt{R}^{2k} = \mathtt{R}^{2k-2}(\mathtt{RR}) \sim \mathtt{R}^{2k-2}(\mathtt{BRB}) \sim \mathtt{BR}^{2k-2}\mathtt{BR} \sim \mathtt{BBR}^k \sim \mathtt{R}^{k+3}$$

pour tout entier $k \geqslant 1$. En particulier si $k \geqslant 2$, on a $\mathtt{R}^k \sim \mathtt{R}^{k+3}$, d'où on déduit que tous les entiers n congrus à 2 modulo 3 conviennent. En outre, de $\mathtt{R}^k \sim \mathtt{R}^{2k}$, on déduit $\mathtt{R}^2 \sim \mathtt{R}^4$, et donc en réutilisant la propriété précédente, on trouve que tous les entiers n supérieurs ou égaux à 4 et congrus à 1 modulo 3 conviennent. La conjonction des deux précédents résultats est bien ce que l'on voulait obtenir.

La réciproque est plus délicate et va nous conduire à utiliser la théorie des groupes. Les mots qui apparaissaient précédemment sont, par définition, des éléments du groupe libre L engendré par les deux générateurs $\mathtt{R}$ et $\mathtt{B}$. Les relations de réécriture (1) nous amènent à considérer le quotient de L par les relations[1] $\mathtt{RR} = \mathtt{BRB}$, $\mathtt{RB} = \mathtt{BRR}$, $\mathtt{BR} = \mathtt{RRB}$ et $\mathtt{BB} = \mathtt{RRR}$: on obtient comme ceci un groupe G muni d'un morphisme surjectif $L \to G$. Dans la suite nous noterons $\bar{x}$ l'image dans G d'un élément $x \in L$. On a le lemme suivant, très facile :

Lemme 1. *Si deux mots x et y (que l'on voit comme des éléments de L) définissent des configurations qui se déduisent l'une de l'autre par une suite d'opérations licites, alors leurs images dans G sont conjuguées (*i.e. *il existe $g \in G$ tel que $\bar{x} = g\bar{y}g^{-1}$).*

Démonstration. Il suffit de montrer que si $x \sim y$, alors $\bar{x}$ et $\bar{y}$ sont conjugués dans G. C'est clair si x se déduit de y par application d'une loi de réécriture puisqu'alors par définition du quotient, on a même $\bar{x} = \bar{y}$. Si, au contraire, x s'obtient à partir de y en déplaçant sa première lettre à la fin, on a la relation $x = g^{-1}yg$ où g désigne la première lettre de y ; x et y sont donc déjà conjugués dans L, ce qui assure qu'il en est de même de leurs images dans G. On conclut par récurrence. □

Pour la question qui nous intéresse, le lemme précédent nous dit qu'il suffit de montrer que $\bar{\mathtt{R}}^2$ et $\bar{\mathtt{R}}^{3k}$ (où k est un entier) ne sont pas conjugués dans G. Tester la conjugaison — ou plutôt démontrer la non-conjugaison — dans un groupe défini par générateurs et relations (comme c'est le cas de G) est en général un problème difficile. La méthode traditionnelle pour le résoudre est de considérer un morphisme φ vers un groupe « concret » dans lequel on sait tester si deux éléments sont conjugués : si l'on arrive à faire cela et que par chance $\varphi(x)$ et $\varphi(y)$ ne sont pas conjugués dans le groupe concret, alors x et y ne pouvaient être conjugués dans le groupe défini par générateurs et relations. Choisir le groupe concret adéquat et le morphisme φ peut, dans certaines situations, se révéler être un exercice périlleux. On peut en tout cas commencer par essayer des groupes commutatifs simples (par exemple $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{R}$ ou $\mathbb{C}$), la conjugaison étant alors équivalente à l'égalité. Si cela ne fonctionne pas, on peut continuer avec les groupes de permutations ou les groupes usuels de matrices. Dans les deux cas, les éléments sont certainement représentés de façon suffisamment concrètes pour pouvoir faire des calculs avec, et on dispose de méthodes efficaces pour tester la conjugaison : la décomposition en cycle et la théorie de la réduction donne des réponses satisfaisantes respectivement dans le cas des groupes de permutations et des groupes de matrices. Revenons à notre exercice. Un morphisme de G dans un groupe X correspond à la donnée des images R et B de $\bar{\mathtt{R}}$ et $\bar{\mathtt{B}}$ respectivement, celles-ci devant être abstreintes à vérifier les relations

$$R^2 = BRB \quad ; \quad RB = BR^2 \quad ; \quad BR = R^2B \quad ; \quad B^2 = R^3. \tag{2}$$

Pour le problème qui nous intéresse, il ne va pas être suffisant de choisir X commutatif. En effet, avec un tel choix, R et B commuteraient et les relations ci-dessous entrainement alors directement

[1] Quotienter par la relation $x = y$ signifie quotienter par le plus petit sous-groupe distingué contenant l'élément xy^{-1}.

$R = e_X$ (où e_X est le neutre de X) ; les images par φ de $\bar{\mathtt{R}}^2$ et $\bar{\mathtt{R}}^{3k}$ vaudraient alors toutes deux e_X et seraient donc conjugués, ce qui ne permettrait pas de conclure. On en vient donc à chercher X parmi les groupes de permutations ou les groupes de matrices usuels ; autrement dit, on cherche désormais à résoudre à résoudre le système 2 dans un tel groupe.

Commençons par regarder le cas des permutations. Un peu de tatonnement[2] montre que (2) a déjà une solution intéressante dans $\mathfrak{S}_3$: il suffit de choisir pour R un 3-cycle et pour B une transposition (la vérification est laissée au lecteur). On construit comme ceci un morphisme $\varphi : G \to \mathfrak{S}_3$ en envoyant $\bar{\mathtt{R}}$ sur R et $\bar{\mathtt{B}}$ sur B. L'image par φ de $\bar{\mathtt{R}}^2$ est encore un 3-cycle, tandis que celle de $\bar{\mathtt{R}}^{3k}$ est l'identité, et il est évident que ces deux permutations ne sont pas conjuguées (la seule permutation conjuguée à l'identité est l'identité elle-même). Ainsi, en remontant les étapes, on a montré que l'on ne peut pas obtenir une configuration avec exactement $3k$ jetons, chacun montrant sa face rouge.

Si l'on n'aime pas les permutations, on aurait pu également trouver un morphisme vers un groupe de matrices puisque le système (2) a aussi une solution dans $\mathrm{GL}_2(\mathbb{C})$ à savoir[4]

$$R = \begin{pmatrix} j & 0 \\ 0 & j^2 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

où $j = -\frac{1}{2} + i\frac{\sqrt{2}}{2}$ est une racine primitive cubique de l'unité. On construit comme ceci un morphisme $\varphi : G \to \mathrm{GL}_2(\mathbb{C})$ et on conclut comme précédemment.

Finalement, les entiers n pour lesquels la réponse à la question de l'énoncé est affirmative sont exactement les entiers $\geqslant 2$ qui ne sont pas des multiples de 3.

[2]Si l'on pense[3] à imposer en plus la relation $R^3 = e$ (où e est le neutre, c'est-à-dire ici la permutation identité), trouver la solution que l'on propose n'est en fait pas si délicat. En effet, le système se simplifie alors en $R^3 = B^2 = I$ et $R^2 = BRB = BRB^{-1}$, et on cherche donc une permutation d'ordre 3 (c'est-à-dire un 3-cycle) conjuguée à son carré par une transposition. L'exemple que l'on a donné est alors le premier auquel on peut penser.

[3]Là encore, étant donné ce qui a été fait pour le sens direct et étant donné ce que l'on veut démontrer, cette idée ne semble pas complètement parachutée.

[4]Là encore, trouver cette solution n'est pas très difficile si l'on pense à nouveau à imposer la condition supplémentaire $R^3 = I$.