Source : Oraux X-ENS – Francinou, Gianella, Nicolas

1. Équivalence $\operatorname{Ker} f = \operatorname{Ker} f^2 \iff \operatorname{Im} f = \operatorname{Im} f^2$

Énoncé

Soit G un groupe fini et f un morphisme de G dans G. Montrer que $\operatorname{Ker} f = \operatorname{Ker} f^2 \iff \operatorname{Im} f = \operatorname{Im} f^2$.

Solution

- On observe que l'on a $\operatorname{Ker} f \subset \operatorname{Ker} f^2$ et $\operatorname{Im} f^2 \subset \operatorname{Im} f$. Ces ensembles étant tous finis, on en déduit que $\operatorname{Ker} f = \operatorname{Ker} f^2$ équivaut à $\left|\operatorname{Ker} f\right| = \left|\operatorname{Ker} f^2\right|$ et $\operatorname{Im} f = \operatorname{Im} f^2$ à $\left|\operatorname{Im} f\right| = \left|\operatorname{Im} f^2\right|$. Il s'agit de démontrer que ces deux égalités de cardinaux sont équivalentes.
- Montrons que si $f : G \to G$ est un morphisme de groupes, alors $|G| = \left|\operatorname{Im} f\right| \times \left|\operatorname{Ker} f\right|$. Soit $\mathscr{R}$ la relation d'équivalence associée à f : $x \mathscr{R} y \iff f(x) = f(y)$. L'ensemble quotient $G/\mathscr{R}$ est équipotent à $\operatorname{Im} f$. Mais d'autre part, $f(x) = f(y)$ équivaut à $f(x^{-1}y) = 1$, puisque f est un morphisme et donc à $x^{-1}y \in \operatorname{Ker} f$. La classe $\overline{x}$ d'un élément x pour $\mathscr{R}$ est donc la classe à gauche modulo $\operatorname{Ker} f$: $\overline{x} = x \operatorname{Ker} f$. Ainsi, $\overline{x}$ est équipotent à $\operatorname{Ker} f$ (par la bijection $g \in \operatorname{Ker} f \longmapsto xg \in \overline{x}$). Les classes ont donc toutes même cardinal, celui de $\operatorname{Ker} f$. On en déduit que
$$|G| = |G/\mathscr{R}| \times \left|\operatorname{Ker} f\right| = \left|\operatorname{Im} f\right| \times \left|\operatorname{Ker} f\right|.$$

On a donc, pour tout morphisme f de G,
$$|G| = \left|\operatorname{Im} f\right| \times \left|\operatorname{Ker} f\right|.$$
On obtient de même
$$|G| = \left|\operatorname{Im} f^2\right| \times \left|\operatorname{Ker} f^2\right|.$$
Ces deux égalités impliquent l'équivalence entre $\left|\operatorname{Im} f\right| = \left|\operatorname{Im} f^2\right|$ et $\left|\operatorname{Ker} f\right| = \left|\operatorname{Ker} f^2\right|$, ce qui établit le résultat demandé.

2. Un cas particulier du lemme de Cauchy

Énoncé

Soit G un groupe de cardinal $2p$ avec p premier. Montrer que G contient un élément d'ordre p.

Solution

D'après le théorème de Lagrange, les éléments de G sont d'ordre $1, 2, p$ ou $2p$. Raisonnons par l'absurde et supposons qu'il n'y ait pas d'élément d'ordre p. Dans ces conditions, G n'est pas cyclique (car si x est un générateur de G, alors x^2 est d'ordre p) et si $x \in G$, x est d'ordre 1 (si x est l'élément neutre) ou 2. En particulier, $p \geqslant 3$ et pour tout $x \in G, x^2 = e$. On peut alors prouver le lemme suivant, intéressant en soi :

Lemme *Soit G un groupe tel que pour tout $x \in G, x^2 = e$. Alors G est abélien et $|G|$ est une puissance de 2.*

Démonstration du lemme

- Soit x et y dans G. Pour tout $z \in G$ on a $z^2 = e$, i.e. $z = z^{-1}$. On en déduit que
$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$$
et G est abélien.
- Montrons par récurrence sur $|G|$ que $|G|$ est une puissance de 2.

Il n'y a rien à vérifier si $|G| = 1$.

Supposons $|G| \geqslant 2$. On considère les sous-groupes de G distincts de G ; il en existe, $\{e\}$ par exemple. On en choisit un de cardinal maximal que l'on note H. D'après l'hypothèse de récurrence, $|H|$ est une puissance de 2. Soit $a \in G \setminus H$. Montrons que $H \cup aH$ est un sous-groupe de G ; en effet, il est égal au sous-groupe H' engendré par a et H :

- on a clairement $H \cup aH \subset H'$;
- réciproquement, a étant d'ordre 2, tout élément de H' s'écrit $a^\alpha h$, avec $\alpha \in \{0, 1\}$ et $h \in H$. D'où le résultat annoncé.

Les ensembles H et aH sont disjoints car sinon il existerait $h \in H$ qui s'écrirait ak avec $k \in H$ et on aurait $a = hk^{-1} \in H$, ce qui est exclu. On en déduit que $|H \cup aH| = 2|H|$. Par maximalité du cardinal de H, $H \cup aH = G$. En particulier, $|G| = 2|H|$ est une puissance de 2.

Le cardinal de notre groupe G devrait être une puissance de 2. Mais $|G| = 2p$, avec $p \geqslant 3$ et premier. C'est contradictoire et G possède donc un élément d'ordre p.

Un élégant argument d'algèbre linéaire permet de mieux saisir encore la structure de G lorsque pour tout $x \in G$, $x^2 = e$: G est alors naturellement muni d'une structure d'espace vectoriel sur $\mathbb{Z}/2\mathbb{Z}$, la loi externe étant définie par $0 \cdot x = e$ (neutre de G) et $1 \cdot x = x$ pour tout $x \in G$, et la loi de groupe étant bien entendu celle de G. La propriété vérifiée par G intervient dans l'axiome de distributivité $(1+1) \cdot x = 0 \cdot x = e$ et $(1 \cdot x)(1 \cdot x) = x^2 = e$. On laisse au lecteur le soin de vérifier les autres axiomes. Comme G est fini, il est de dimension finie en tant que $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel. Si on note n cette dimension, G est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^n$ en tant qu'espace vectoriel et a fortiori en tant que groupe.

3. Génération du groupe symétrique

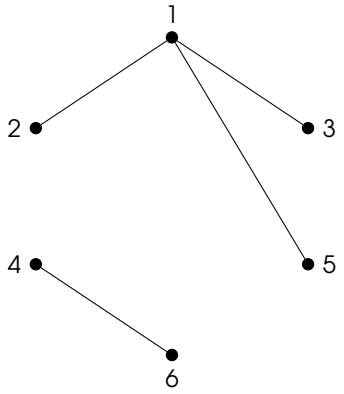
Énoncé

Soit $n \geqslant 2$. Quel est le nombre minimal de transpositions engendrant le groupe symétrique $\mathfrak{S}_n$?

Solution

On a classiquement que les transpositions $(1\ 2), \ldots, (1\ n)$ engendrent $\mathfrak{S}_n$. Ainsi, $n-1$ transpositions suffisent et intuitivement, il semble difficile de faire mieux, ce que semble confirmer l'étude des premières valeurs de n. En effet, pour $n=2$ il nous faut au moins une transposition (la seule !) et pour $n=3$, il nous en faut au moins 2 puisque une seule transposition engendre un sous-groupe à deux éléments.

Donnons-nous des transpositions $\tau_1, \ldots, \tau_k$, avec $k \leqslant n-2$. Pour visualiser le problème nous allons représenter les entiers de 1 à n par des points du plan. On fait en sorte que trois quelconques de ces points ne soient pas alignés. Si la transposition (a,b) apparaît dans la liste $\tau_1, \ldots, \tau_k$ on joint par un segment les points correspondant aux entiers a et b. On obtient ce qu'on appelle un graphe. Par exemple, pour $n=6, k=4, \tau_1=(1\ 2), \tau_2=(1\ 3), \tau_3=(1\ 5)$ et $\tau_4=(4\ 6)$, on obtient le graphe suivant :



Il est assez clair qu'une condition nécessaire pour que $\tau_1, \ldots, \tau_k$ engendrent $\mathfrak{S}_n$ est qu'on puisse passer de n'importe quel sommet $i \in \{1, \ldots, n\}$ à n'importe quel autre sommet $j \in \{1, \ldots, n\}$ en suivant les arêtes du graphe.

Un graphe vérifiant cette propriété est dit connexe.

Il est aisé de dessiner des graphes connexes sur un ensemble de cardinal n qui contiennent $n-1$ arêtes.

On peut par exemple choisir un sommet et le relier à tous les autres.

Mais il semble impossible d'y arriver avec seulement $n-2$ arêtes. On a effectivement le résultat suivant :

Lemme *Si un graphe G sur un ensemble E de cardinal $n \geqslant 2$ est connexe, alors il a au moins $n-1$ arêtes.*

Démonstration du lemme

On procède par récurrence sur n, le résultat étant clair pour $n=2$. Supposons le résultat prouvé au rang $n-1$. Soit $G=(S,A)$ un graphe à n sommets. Si x est un sommet de G on note $\deg(x)$ son degré c'est-à-dire le nombre d'arêtes qui arrivent en x. On a aisément

$$\sum_{x \in S} \deg(x) = 2|A|.$$

La connexité de G impose évidemment $\deg(x) \geqslant 1$ pour tout x. Deux cas se présentent :

- Pour tout $x, \deg(x) \geqslant 2$. Alors on a directement grâce à l'égalité ci-dessus $|A| \geqslant n$.
- Il existe un sommet x_0 de degré 1. Retirons ce sommet x_0 et l'unique arête qui y aboutit. On obtient un nouveau graphe $G'=(S',A')$ sur l'ensemble $S'=S \setminus \{x_0\}$ qui est encore connexe.
  Par hypothèse de récurrence, $|A'| \geqslant |S'|-1 = n-2$ et donc $|A| = |A'|+1 \geqslant n-1$.