Devoir à la maison n°1

Un corrigé

Quizz. Voici certaines affirmations *fausses* relevées dans les copies. A vous de comprendre pourquoi elles ne sont pas correctes en donnant un contre-exemple ; à vous de voir si, en mettant des hypothèses supplémentaires, elles peuvent devenir correctes.

- Soit G un groupe. L'application

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & x^7 \end{array}$$

  est un morphisme de groupes.
- Soit G un groupe d'ordre n. Alors il existe un élément de G d'ordre n.
- Soit G un groupe d'ordre n et d divisant n. Alors il existe un sous-groupe de G d'ordre d.
- Soit G un groupe possédant un 2-Sylow P d'ordre 8. Alors P contient le neutre et 7 éléments d'ordre 8.
- Soit G un groupe possédant n 2-Sylow d'ordre 8. Alors ces sous-groupes donnent $n \times (8-1)+1$ éléments distincts de G.
- Par contre, l'affirmation suivante est vraie : Soit G un groupe ayant n p-Sylow d'ordre p, où p est premier. Alors ces sous-groupes donnent $n \times (p-1)+1$ éléments distincts de G.

Exercice 1. Raisonnons par l'absurde. Supposons qu'il existe un groupe G simple d'ordre $56 = 2^3 \times 7$. Dénombrons les 7-sous-groupes de Sylow de G en utilisant les théorèmes de Sylow.

Les 7-Sylow sont d'ordre 7, il y en a n_7, avec $n_7 \mid 8$ et $n_7 \equiv 1 \mod 7$. Donc n_7 vaut 1 ou 8. Si $n_7 = 1$, alors l'unique 7-Sylow est distingué dans G par le deuxième théorème de Sylow. Comme G est simple, ses seuls sous-groupes distingués sont $\{1\}$ et G. Cela donne une contradiction car le 7-Sylow est de cardinal 7. On a donc $n_7 = 8$.

Dénombrons maintenant les éléments de G en fonction de leur ordre. Les 7-Sylow sont d'ordre 7. Soient H et K deux 7-Sylow. D'après le théorème de Lagrange, l'ordre de $H \cap K$ divise l'ordre de H, donc $|H \cap K| = 1$ ou 7. Cela signifie que deux 7-Sylow distincts sont d'intersection $\{1\}$.

Les éléments non neutre des 7-Sylow sont donc distincts, et d'ordre 7 (car leur ordre divise 7) : il y en $6 \times 8 = 48$. Dans G, il reste $56 - 48 = 8$ éléments d'ordre différent de 7. D'après le théorème de Lagrange, un 2-Sylow possède 8 éléments d'ordre 1, 2, 4 ou 8. Il reste donc juste assez d'éléments pour avoir un unique 2-Sylow. Il est distingué dans G d'après le deuxième théorème de Sylow. Ceci est impossible car G est simple. Donc il n'existe aucun groupe simple d'ordre 56.

Remarque : une autre façon de voir que les éléments non neutre des 7-Sylow sont distincts. Les 7-Sylow sont d'ordre premier 7 donc cycliques. C'est un résultat classique (feuille 1, exercice 2) qu'un groupe cyclique d'ordre *premier* p est engendré par n'importe lequel de ses éléments différents du neutre (ce qui revient à dire que tout élément différent du neutre est d'ordre p).

Exercice 2. Soit G un groupe cyclique d'ordre n. Notons x un générateur de G ; il est d'ordre n.

1) Soit H un sous-groupe de G. On peut supposer $H \neq \{e\}$. On considère l'ensemble $\{k \geq 1 \mid x^k \in H - \{e\}\}$. C'est un ensemble non vide de $\mathbb{N}$. Il admet un plus petit élément qu'on note d. Démontrons que H est le sous-groupe engendré par x^d.

Soit x^k un élément de H, avec $k \geq 0$. La division euclidienne de k par d donne $k = qd+r$ avec $0 \leq r < d$. Alors on a $x^k = (x^d)^q x^r$. Or, x^d appartient à H par définition de d, donc $x^r \in H$. Par minimalité de d, on a donc $r = 0$, d'où $x^k = (x^q)^d$. On obtient ainsi $H \subset \langle x^d \rangle$. Enfin, comme $x^d \in H$, on a l'autre inclusion $\langle x^d \rangle \subset H$. D'où $H = \langle x^d \rangle$, ce qui montre que H est cyclique.

2) Soit d divisant n. Soit H le sous-groupe engendré par $x^{n/d}$. On vérifie que $x^{n/d}$ est d'ordre d. Donc il existe un sous-groupe H de G d'ordre d.

Soit K un sous-groupe de G d'ordre d. Montrons qu'il coïncide avec H. Soit y un élément de K. Comme G est cyclique, il existe $k \in \mathbb{Z}$ tel que $y = x^k$. D'après le théorème de Lagrange, $y^d = x^{kd} = 1$. Donc n divise kd, donc $\frac{n}{d}$ divise k. Ceci montre que $y \in \langle x^{n/d} \rangle$, donc $K \subset H$. Comme H et K ont même cardinal d, on a donc $H = K$.

Finalement, il existe un unique sous-groupe de G d'ordre d.

Le nombre d'éléments de G d'ordre d est le nombre de générateurs de l'unique sous-groupe H d'ordre d. Rappelons que H est cyclique ; notons z un générateur qui est d'ordre d. Un élément z^k de H est d'ordre $\frac{d}{\mathrm{pgcd}(d,k)}$ (feuille 1, exercice 5). Il est d'ordre d si et seulement si d et k sont premiers entre eux. En notant φ la fonction indicatrice d'Euler, il y a $\varphi(d) = \{1 \leq k \leq d \mid \mathrm{pgcd}(d,k) = 1\}$ valeurs possibles pour un tel k. Il y a donc $\varphi(d)$ éléments de G d'ordre d.

Exercice 3. On calcule $|C|$ en «fixant» g puis en «fixant» x.

- On a $C = \bigsqcup_{g \in G} \{x \in X \mid gx = x\} = \bigsqcup_{g \in G} N(g)$. Donc $|C| = \sum_{g \in G} |N(g)|$.
- On a également $C = \bigsqcup_{x \in X} \{g \in G \mid gx = x\} = \bigsqcup_{x \in X} G_x$, où G_x désigne le stabilisateur de x pour l'action de G. Donc $|C| = \sum_{x \in X} |G_x|$. D'après la première formule des classes, c'est aussi :

$$|C| = \sum_{x \in X} |G|/|\mathcal{O}(x)| = |G| \sum_{x \in X} 1/|\mathcal{O}(x)|.$$

  Soient Ω un système de représentants des orbites. Puisque les orbites forment une partition de X, on a

$$\sum_{x \in X} 1/|\mathcal{O}(x)| = \sum_{o \in \Omega} \sum_{x \in o} 1/|o| = \sum_{o \in \Omega} 1 = |\Omega|.$$

  Donc $|C| = n|G|$ où n désigne le nombre d'orbites de l'action.

En comparant les résultats, on obtient la formule suivante, appelée « formule de Burnside » :

$$n = |\Omega| = \frac{1}{|G|} \sum_{g \in G} |N(g)|.$$

Exercice 4. 1) Soit X l'ensemble des colliers avant identification et G le groupe engendré par une rotation d'ordre n. L'ensemble des colliers après identification est l'ensemble des orbites de X sous l'action de G. D'après l'exercice 3, il y en a donc :

$$m = \frac{1}{|G|} \sum_{g \in G} |N(g)| = \frac{1}{n} \sum_{g \in G} |N(g)|.$$

Pour tout élément g de G, il s'agit maintenant de calculer $|N(g)| = |\{x \in X \mid gx = x\}|$.

Soit d l'ordre de g (c'est un diviseur de n par le théorème de Lagrange). Soit $H = \{1, g, \ldots, g^{d-1}\}$ le sous-groupe de G engendré par g. Alors un collier x appartient à $N(g)$ si et seulement si pour tout $k \geq 1$, $g^k x = x$ (dans un sens c'est trivial ; dans l'autre sens, cela se démontre par récurrence sur k). On a donc $N(g) = N(H)$.

Numérotons de 1 à n les emplacements possibles des perles et faisons agir H sur $\{1, \ldots, n\}$. On obtient ainsi une partition de $\{1, \ldots, n\}$ en orbites pour cette action. Un collier x appartient à $N(H)$ si et seulement si toutes les perles de x situées dans la même orbite ont la même couleur (réfléchissez-y ou faites un dessin). Maintenant, calculons de combien de façons on peut colorier les orbites.

Il y a c couleurs possibles. L'orbite de n'importe quel élément de $\{1, \ldots, n\}$ est de cardinal d. De plus, les orbites forment une partition de $\{1, \ldots, n\}$. Donc il y a $\frac{n}{d}$ orbites et $c^{n/d}$ façons différentes de colorier les orbites. Remarque : on peut également dénombrer les orbites en utilisant la formule de l'exercice 3 dans le cas de l'action de H sur $\{1, \ldots, n\}$.

Le nombre de colliers après identification est donc :

$$m = \frac{1}{n} \sum_{d|n} \sum_{g \in G \text{ d'ordre } d} |N(g)| = \frac{1}{n} \sum_{d|n} \sum_{g \in G \text{ d'ordre } d} c^{n/d}$$

Puis on utilise le résultat de l'exercice 2 pour compter le nombre d'éléments d'ordre d :

$$m = \frac{1}{n} \sum_{d|n} \varphi(d) c^{\frac{n}{d}}.$$

2) Le groupe qu'on fait agir sur X est le groupe engendré par une rotation d'ordre n et une symétrie axiale dans le plan c'est-à-dire le groupe diédral D_n, d'ordre $2n$. La formule de l'exercice 3 donne :

$$m = \frac{1}{2n} \sum_{g \in D_n} |N(g)|.$$

On a déjà calculé $|N(g)|$ dans le cas où g est une rotation. Calculons $|N(s)|$ dans le cas où s est une symétrie de D_n. Comme précédemment, on fait agir le sous-groupe H engendré par s sur le polygone régulier à n côtés formé par les emplacements possibles des perles et on dénombre les orbites de cette action.

- *Cas où n est impair* : alors toute symétrie du groupe diédral a son axe qui passe par un seul sommet du polygone. Les sommets qui ne sont pas sur l'axe s'apparient en des orbites à 2 éléments ; il y a $\frac{n-1}{2}$ orbites de ce type. Il reste une autre orbite, celle du sommet qui est sur l'axe de la symétrie. Au total, on obtient $\frac{n+1}{2}$ orbites. Comme il y a c couleurs, cela donne $c^{(n+1)/2}$ façons de colorier les orbites. Enfin, il y a n symétries dans le groupe diédral D_n. Donc le nombre de colliers est :

$$m = \frac{1}{2n}\left(\sum_{d|n} \varphi(d) c^{\frac{n}{d}} + n c^{\frac{n+1}{2}}\right).$$

- *Cas où n est pair* : on a deux type de symétries, celles dont l'axe passe par deux sommets et celles dont l'axe ne passe par aucun sommet du polygone.

  Pour les premières, les sommets qui ne sont pas sur l'axe donnent $\frac{n-2}{2}$ orbites à 2 éléments, et les autres une orbite à 2 éléments. On obtient ainsi $\frac{n+2}{2}$ orbites. Enfin, il y a $\frac{n}{2}$ symétries de ce type dans D_n puisque cela revient à choisir l'axe de la symétrie. On a donc $\frac{n}{2}c^{(n+2)/2}$ façons de colorier les orbites.

  Pour les deuxièmes, les sommets s'apparient en $\frac{n}{2}$ orbites à 2 éléments. Il y a $\frac{n}{2}$ symétries de ce type, puisque D_n compte n symétries. On a donc $\frac{n}{2}c^{n/2}$ façons de colorier les orbites.

  Au total, le nombre de colliers est :

$$m = \frac{1}{2n}\left(\sum_{d|n} \varphi(d) c^{\frac{n}{d}} + \frac{n}{2} c^{\frac{n+2}{2}} + \frac{n}{2} c^{\frac{n}{2}}\right).$$