Devoir maison n°1, corrigé

Exercice 1. [Groupes monogènes, groupes cycliques]

(*a*) Soit G un groupe engendré par $x \in G$. Par hypothèse, $n \in \mathbf{Z} \mapsto x^n \in G$ est un morphisme surjectif, et son noyau est de la forme $n\mathbf{Z}$, $n \in \mathbf{N}$, d'où un isomorphisme $G \cong \mathbf{Z}$ dans le cas $n = 0$ et $G \cong \mathbf{Z}/n\mathbf{Z}$ pour $n > 0$.

(*b*) Le fait que les sous-groupes de $\mathbf{Z}$ soient de la forme $d\mathbf{Z}$ est bien connu, et ils sont bien monogènes. Maintenant, si H est un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$, alors $\pi^{-1}(H) = d\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}$, où $\pi : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ est la projection canonique. On en déduit que $H = d\mathbf{Z}/n\mathbf{Z}$, et comme $n\mathbf{Z} \subset d\mathbf{Z}$ on a que $d|n$. Par conséquent, $H \cong \mathbf{Z}/n'\mathbf{Z}$ avec $n' = n/d$, et H est bien monogène. Inversement, si $d|n$ et $n' = n/d$, $n'\mathbf{Z}/n\mathbf{Z}$ est un sous-groupe de $\mathbf{Z}/n\mathbf{Z}$ d'ordre d. Les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont donc exactement les $d\mathbf{Z}/n\mathbf{Z}$ avec $d|n$ (et ils sont bien monogènes).

(*c*) Cela suit du fait que les sous-groupes de $\mathbf{Z}/n\mathbf{Z}$ sont en bijection avec les sous-groupes de $\mathbf{Z}$ contenant $n\mathbf{Z}$ et donc avec les $d\mathbf{Z}$ où $d|n$. L'existence a été démontrée à la question précédente.

(*d*) Les générateurs de $\mathbf{Z}$ sont 1 et -1. Soit $n \geq 1$ et $u \in \{0, \ldots, n-1\}$ dont la classe modulo n est un générateur, alors il existe $a \in \mathbf{Z}$ tel que $au = 1 \mod n$. Autrement dit, $au = 1 + nk \in \mathbf{Z}$, ie u et n sont premiers entre eux. Inversement, par le théorème de Bézout, si u est premier à n, alors u engendre $\mathbf{Z}/n\mathbf{Z}$. Notons qu'un automorphisme de $\mathbf{Z}$ ou $\mathbf{Z}/n\mathbf{Z}$ est entièrement déterminé par l'image de 1, et que celle ci doit être un générateur. Ainsi $\mathrm{Aut}(\mathbf{Z}) = \{1, -1\}$ et $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) \subset (\mathbf{Z}/n\mathbf{Z})^\times$. Inversement, la multiplication par $u \in (\mathbf{Z}/n\mathbf{Z})^\times$ est un automorphisme. D'où $\mathrm{Aut}(\mathbf{Z}/n\mathbf{Z}) = (\mathbf{Z}/n\mathbf{Z})^\times$. On vérifie immédiatement que c'est un isomorphisme de groupes.

(*e*) On écrit $\mathbf{Z}/n\mathbf{Z}$ comme la réunion disjointe des E_d, où E_d est l'ensemble des éléments engendrant l'unique sous-groupe d'ordre d. Comme c'est un groupe cyclique d'ordre d, il est engendré par $\varphi(d)$ éléments, d'où le résultat.

(*f*) Soit $\psi(d)$ le nombre d'éléments d'ordre d. Par hypothèse, $\psi(d) \leq \varphi(d)$. Or $\sum_{d|n} \psi(d) = n = \sum_{d|n} \varphi(d)$, on en déduit donc que $\varphi(d) = \psi(d)$ pour tout $d|n$ et donc en particulier $\psi(n) = \varphi(n) \geq 1$, donc il existe au moins un élément d'ordre n et G est cyclique.

(*g*) Il suffit de vérifier que les hypothèses de la question précédente sont satisfaites. Soit $d|n = |G|$, et soit $H \subset G$ un sous-groupe cyclique d'ordre d. Alors pour tout $x \in H, x^d = 1$ et donc H est inclus dans l'ensemble des racines d-ièmes de l'unité, mais il y en a au plus d puisqu'on est dans un corps (commutatif), et donc il y a au plus un sous-groupe d'ordre d.

Exercice 2. [Formule de Burnside et applications]

(*a*) On calcule le cardinal de l'ensemble $\{(x, g) \in X \times G | gx = x\}$ de deux façons différentes selon qu'on compte d'abord par rapport à X ou par rapport à G. On obtient alors l'égalité $\sum_{x \in X} |\mathrm{Stab}(x)| = \sum_{g \in G} f(g)$. Ensuite, pour tout $x \in X$, dans la formule ci-dessus, l'orbite de $x \in X$ apporte au terme de gauche une contribution égale à $|\mathrm{Orb}(x)||\mathrm{Stab}(x)| = |G|$. En sommant sur le nombre d'orbites N, on voit donc que le terme de gauche est égal à $N|G|$, d'où la formule.

(*b*) Comme G agit transitivement sur X qui a au moins deux éléments, le terme de gauche de la formule de Burnside est 1, et $Card(X^1) > 1$. La moyenne des $Card(X^g)$ étant égale à 1, il y a donc au moins un $g \in G$ tel que $Card(X^g) = 0$.

(*c*) Soit H un sous-groupe strict de G. On fait agir G sur G/H par $k \cdot gH = (kg)H$. Cette action est transitive et $Card(G/H) \geq 2$ comme H est un sous-groupe strict. Il existe donc par la question précédente k agissant sans point fixe, ce qui signifie que k n'appartient à aucun des gHg^{-1}.

(*d*) Soit X l'ensemble de 3^6 colliers possibles. Chaque collier correspond aux sommets $S = (1, ..., 6)$ du polygone régulier à 6 cotés. On va faire agir le groupe de rotations R_6 engendré par la rotation τ sur l'angle $2\pi/6$ i.e $R_6 =< \tau >$. Un coloriage est donné par une application :

$$f : [\![1, ..., 6]\!] \to \{1, 2, 3\}$$

Soit $r \in R_6$ et $C = \{(1, f(1)), ..., (6, f(6))\}$ un collier coloré. La rotation r envoie alors bijectivement l'ensemble des sommets S sur lui-même i.e est une permutation de S : $r(i) = j$. On définit l'action de

R_6 sur L par : $R_6 \times X \to X$, $(r, C) \mapsto \{(1, \rho(1)), ...(6, \rho(6))\}$ où $\rho(k) = f(r^{-1}(k))$. Pour un k tel que $1 \leq k \leq 5$ soit d l'ordre de τ^k. Alors $d|6$ et τ^k est le produit de $6/d$ cycles disjointes de longueur d. Donc, $|X^{\tau^k}| = 3^{6/d}$. On obtient alors : $|X^e| = 3^6$, $|X^\tau| = |X^{\tau^5}| = 3^1$, $|X^{\tau^2}| = |X^{\tau^4}| = 3^2$, $|X^{\tau^3}| = 3^3$. D'après la formule de Burnside :

$$N = \frac{1}{6}(3^6 + 3^1 + 3^1 + 3^2 + 3^2 + 3^3) = 130.$$

Nous avons donc 130 colliers différents.
(e) Dans ce cas, le groupe qui agit sur X est D_6, $|D_6| = 12$. On ajoute donc à R_6 les réflexions de 2 types suivants :
a) Trois réflexions r_1, r_2, r_3, dont l'axe passe par milieux de 2 cotés symétriques par rapport à l'origine.
b) Trois réflexions ρ_1, ρ_2, ρ_3, dont l'axe passe par 2 perles symétriques.
Pour un r_i, il y a exactement $6/2 = 3$ perles de chaque coté de l'axe, donc $|X^{r_i}| = 3^3$. Pour un ρ_i, il'y a 2 perles de chaque coté de l'axe et il faut choisir la couleur de chaque perle sur l'axe. Par conséquent, $|X^{\rho_i}| = 3^2 \times 3^2$. D'après la formule de Burnside :

$$N = \frac{1}{12}(3^6 + 23^1 + 23^2 + 43^3 + 33^4) = 92.$$

Nous avons donc 92 colliers différents dans ce cas.

(f) Soit $P \in X$ un point de la sphère unité S^2 associé à un $g \in G$ (un *pôle*). G agit sur S^2 par rotations. Pour un $h \in G$ on a : $h\,g\,h^{-1}\,h(P) = hg(P) = h(P)$. Donc $h(P)$ est un pôle aussi i.e $h(P) \in X$. Donc, G agit sur X.

(e) D'après la formule de Burnside, le nombre N d'orbites d'action de G sur X est donné par :

$$N = \frac{1}{|G|}\sum_{g \in G} |X^g| = \frac{1}{|G|}(|X^e| + \sum_{g \neq e} |X^g|) = \frac{1}{|G|}(|X| + 2(|G| - 1)) = \frac{|X|}{|G|} + 2 - \frac{2}{|G|}.$$

Par conséquent, on a $2 \leq |X| \leq 2(|G| - 1)$ et donc :

$$2 \leq N \leq \frac{2(|G| - 1)}{|G|} + 2 - \frac{2}{|G|} = 4\left(1 - \frac{1}{|G|}\right) < 4$$

Nous avons alors $N = 2$ ou $N = 3$.
(h) Soit $N = 2$. Alors $2|G| = |X| + 2|G| - 2 \Rightarrow |X| = 2$. Dans ce cas, tous $g \in G$ admettent les mêmes pôles P et $-P$ i.e admettent le même axe de rotation. Le groupe G agit donc par rotations sur le plan orthogonal à cet axe et qui contient le centre de S^2. Un tel groupe fini est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ pour un $n \geq 1$.
(i) On considère le cas $N = 3$. Soient O_1, O_2, O_3 les 3 orbites avec $|O_1| \geq |O_2| \geq |O_3|$. Soit $m_i = |X^{x_i}|$, $1 \leq i \leq 3$. D'après la formule des classes : $|G| = m_i|O_i|$, $1 \leq i \leq 3 \Rightarrow m_1 \leq m_2 \leq m_3$. Soit $P \in O_1$, alors P est fixé par $e \in G$ et par une rotation non-triviale, donc $m_1 \geq 2$. On a : $3|G| = |X| + 2(|G| - 1) \Rightarrow |X| = |G| + 2$. On obtient alors :

$$|G| + 2 = |O_1| + |O_2| + |O_3| = \frac{|G|}{m_1} + \frac{|G|}{m_2} + \frac{|G|}{m_3} \Rightarrow \frac{1}{m_1} + \frac{1}{m_2} + \frac{1}{m_3} = 1 + \frac{2}{|G|} \Rightarrow \frac{3}{m_1} > 1 \Rightarrow m_1 = 2$$

Donc, $\frac{1}{m_2} + \frac{1}{m_3} = \frac{2}{|G|} + \frac{1}{2} \Rightarrow \frac{2}{m_2} > \frac{1}{2} \Rightarrow m_2 \in \{2, 3\}$. Si $m_2 = 3$, alors $\frac{1}{m_3} = \frac{2}{|G|} + \frac{1}{6} \Rightarrow m_3 \in \{3, 4, 5\}$. On obtient donc les cas suivants pour les triplets $(|O_1|, |O_2|, |O_3|)$ et $|G|$: $(2, 2, n)$, $|G| = 2n, n \geq 1$, $(2, 3, 3)$, $|G| = 12$, $(2, 3, 4)$, $|G| = 24$ et $(2, 3, 5)$, $|G| = 60$.

(j) Cas 1 : $(|O_1|, |O_2|, |O_3|, |G|) = (2, 2, n, 2n), n \geq 1$. Il s'agit du groupe diédral constitué des isométries qui laissent invariant le polygone régulier centré en l'origine à n côtés.
Cas 2 : $(|O_1|, |O_2|, |O_3|, |G|) = (2, 3, 3, 12)$. Il s'agit du groupe des isométries directes qui laissent invariant un tétraèdre régulier (isomorphe à A_4).
Cas 3 : $(|O_1|, |O_2|, |O_3|, |G|) = (2, 3, 4, 24)$. Dans ce cas, G est un groupe des isométries directes qui laissent invariant un cube (isomorphe à S_4).
Cas 4 : $(|O_1|, |O_2|, |O_3|, |G|) = (2, 3, 5, 60)$. G est un groupe des isométries directes qui laissent invariant un dodécaèdre (isomorphe à A_5).