Groupes

Solution de l'exercice (??)

(a) Soient x, y deux éléments quelconques de G, il s'agit alors de monter que $xy = yx$ ce qui revient à prouver aussi que $xyx^{-1}y^{-1} = 1$. Or x (resp. y) étant d'ordre 2, on a $xx = 1 = x^{-1}x$ soit $x = x^{-1}$ (resp. $y = y^{-1}$). L'égalité cherchée revient s'écrit alors $xyxy = 1$ ce qui revient à montrer que xy est d'ordre 2 ce qui est vrai par hypothèse.

(b) Supposons, par récurrence, que si le cardinal de G est inférieur à r alors il est de la forme 2^n. La récurrence est clairement vérifiée pour $r = 1$ et $r = 2$, supposons la vraie jusqu'au rang r et traitons le cas de $r + 1$. Soit alors $g_1 \neq 1$ un élément de G qui engendre, par hypothèse, un sous-groupe d'ordre 2 qui est distingué car $gg_1g^{-1} = g_1$. On considère alors le groupe quotient $G/(g_1)$ qui est de cardinal $\frac{r}{2}$ et dont tous les éléments sont d'ordre 2; en effet $\bar{g}\bar{g} = \bar{g}g = \bar{1}$. Par récurrence on a donc $\frac{r}{2}$ qui est de la forme 2^n, d'o˘ le résultat.

(c) Soit $h \in H$ et soit $g \in G$, il s'agit de montrer que $ghg^{-1} \in H$. Or H étant d'indice 2, il existe $g_0 \notin H$ tel que G est la réunion disjointe de H et de g_0H. Il suffit alors de montrer que $g_0hg_0^{-1}$ ne s'écrit pas g_0h'. On raisonne par l'absurde ce qui donne $hg_0^{-1} = h'$ et donc $g_0 = h(h')^{-1}$ soit $g_0 \in H$ ce qui n'est pas.

Solution de l'exercice (??)

(a) On rappelle que dans un groupe fini G, tout élément est d'ordre un diviseur du cardinal de G ; en effet d'après le théorème de Lagrange (cf. (**??**)) le cardinal du groupe engendré par g, qui est égal à son ordre par définition, divise le cardinal de G. Ainsi si dans un groupe de cardinal 10 il n'y a avait aucun élément d'ordre 5, il n'y aurait aucun élément g d'ordre 10 car sinon g^2 serait d'ordre 5, de sorte que tout élément $g \neq 1$ serait d'ordre 2 ce qui contredit l'exercice précédent **??** car 10 n'est pas une puissance de 2.

(b) Soit alors g un élément d'ordre 5 de sorte que le sous-groupe H qu'il engendre est d'indice 2 et est donc distingué d'après le point (c) de l'exercice **??**. Soit alors $x \notin H$. Dans le groupe quotient G/H, on a $(\bar{x})^2 = 1$ de sorte que x^2 appartient à H. Si on avait $x_2 \neq 1$, x^2 serait alors d'ordre 5 et x serait d'ordre 10 et G serait cyclique et donc abélien.

(c) Supposons pour commencer que G est non commutatif. Soit $x \notin H$ de sorte que tout élément de G s'écrit de manière unique sous la forme g^kx^i avec $0 \leq k < 5$ et $i = 0, 1$. On considère alors l'application $f : G \longmapsto D_5$ qui envoie g^kx^i sur $r^k \circ s^i$ où r est la rotation d'angle $2\pi/5$ et s la réflexion d'axe

(Ox). Montrons que f est un morphisme de groupe, *i.e.* $f(g^k x^i g^{k'} x^{i'}) = r^k s^i r^{k'} s^{i'}$. Pour $i = 0$ ou $k' = 0$, le résultat découle de la définition. Dans le cas $i = i' = 1$, comme $(g^{k'} x)^2 = 1$ (resp. $(r^{k'} s)^2 = 1$), on a $g^k x g^{k'} x = g^{k-k'}$ (resp. $r^k s r^{k'} s = r^{k-k'}$), d'o˘ le résultat. Si $i' = 0$ on écrit $g^k x g^{k'}$ (resp. $r^k s r^{k'}$) sous la forme $g^k x g^{k'} x x$ (resp. $r^k s r^{k'} s s$) et on applique le calcul précédent.

On obtient ainsi un morphisme $G \longmapsto D_5$ qui est clairement injectif par définition, et qui réalise donc, vu l'égalité des cardinaux de G et D_5, un isomorphisme.

Si G est commutatif, on reprend le raisonnement de (b). Si $x^2 \neq 1$, x est d'ordre 10 et G est cyclique. Si $x^2 = 1$, x est alors d'ordre 2. Considérons alors $y = xg$ et soit n tel que $y^n = x^n g^n = 1$ soit $x^{-n} = x^n = g^n$. Si n était impair, on aurait $x \in H$ ce qui ne se peut pas car H ne contient pas d'éléments d'ordre 2. Ainsi n est pair et $g^n = 1$ soit 5 divise n et donc 10 divise n, de sorte que y est d'ordre 10, d'où le résultat.

Groupe symétrique

Solution de l'exercice (??) L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire,*i.e.*

$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$

de sorte que chaque classe est constitué de 5 éléments. On obtient alors $\binom{5}{5} frac5!5$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le mÍme raisonnement donne $\binom{4}{5}3!$ et de manière générale le nombre de r-cycles dans $\mathcal{S}_n$ est $(r \top n)(r-1)!$.

Solution de l'exercice (??)

(a) Soit c un p-cycle et soit $\bar{c}$ son image dans $\mathcal{S}_p/H$ qui n'est qu'un ensemble et n'est pas muni de structure de groupe car H n'est pas distingué. L'ensemble $\mathcal{S}_p/H$ étant de cardinal strictement inférieur à p, on en déduit qu'il existe $0 \leq i < j < p$ tel que $\bar{c^i} = \bar{c^j}$ de sorte qu'il existe $h \in H$ tel que $c^j = c^i h$ soit $c^{j-i} \in H$. Or p étant premier, il existe u et v tel que $u(j-i) + vp = 1$ de sorte que $c^{(j-i)u} = c \in H$.

(b) On calcule $(1\,3\,2\,4 \cdots p)^{-1} \circ (1\,2\,3 \cdots\, p) = (1\,3\,2)$ de sorte que pour un 3-cycle quelconque $(a\,b\,c)$ on a $(a\,b\,c) = (a\,b\,c\,i_1 \cdots i_{p-3})^{-1} \circ (a\,c\,b\,i_1 \cdots i_{p-3})$ où $\{i_1, \cdots, i_{p-3}\} = \{1, \cdots, n\} \backslash \{a, b, c\}$.

(c) Le groupe $\mathcal{A}_p$ étant engendré par les 3-cycles (exercice **??**) qui d'après la question précédente appartiennent à H, on en déduit que $\mathcal{A}_p \subset H \subset \mathcal{S}_p$

de sorte que $\frac{p!}{2}$ divise le cardinal de H qui est lui-même un diviseur de $p!$. Comme H est un sous-groupe strict de $\mathcal{S}_p$, on en déduit alors que H est de cardinal $\frac{p!}{2}$ et donc que $\mathcal{A}_p = H$.

(d) On applique ce qui précède au cas $p = 5$. Si H était un sous-groupe de $\mathcal{S}_5$ de cardinal 30 (resp. 40), il serait d'indice 4 (resp. 3) de sorte qu'il devrait contenir $\mathcal{A}_5$ ce qui ne se peut pas.

Solution de l'exercice (??)

(a) On part donc du fait que $\mathcal{S}_n$ est engendré par les transpositions $(i\ j)$. La technique est alors de montrer que toutes ces transpositions appartiennent au sous-groupe engendré par les éléments que l'on considère.

(i) On a $(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i)$; de plus si $2 \leq i_0 \leq n$, i_0 est laissé fixe par toutes les transpositions $(1\ i)$ pour $i \neq i_0$ de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(ii) Pour $1 \leq i < j-1 \leq n-1$, on a $(i\ j) = (j-1\ j) \circ (i\ j-1) \circ (j-1\ j)$, le résultat découle alors d'une récurrence simple sur $j - i$; soit $1 \leq i_0 < n$, l'intervalle $\{1, \cdots, i_0\}$ est laissé globalement stable par tous les éléments $(i, i+1)$ pour $i \neq i_0$, de sorte que $\mathcal{S}_n$ ne peut pas être engendré par un sous-ensemble strict de celui considéré.

(iii) On a $(i, i+1) = c_n^{i-1} \circ \tau \circ c_n^{-i+1}$; le résultat découle alors de (ii).

(b) Le résultat est clair pour $n = 3$. Pour $n \geq 4$, si $a \neq b$ et $b \neq c$ alors $(a\ b) \circ (b\ c) = (a\ b\ c)$; ainsi si a, b, c, d sont deux à deux distincts, $(a\ b) \circ (c\ d) = (a\ b\ c) \circ (b\ c\ d)$, d'où le résultat.

Solution de l'exercice (??). On a $\sigma = (1\ 2\ 3) \circ (2\ 4) \circ (1\ 3)$ qui est bien une décomposition en cycles mais pas à supports disjoints ; on vérifie sans peine que $\sigma = (3\ 2\ 4)$. De même $(1\ 2\ \cdots\ n-1) \circ (1\ n) = (1\ n\ 2\ \cdots\ n-1)$.

Solution de l'exercice (??)

(i) Si c est un cycle de longueur l: $c = (x_1\ x_2\ \cdots\ x_l)$ alors pour tout $\sigma \in \mathcal{S}_n$, σ^{-1} est le cycle de longueur l: $(\sigma(x_1)\ \sigma(x_2)\ \cdots\ \sigma(x_l))$. Ainsi si $s = c_1 \circ \cdots \circ c_r$ est la décomposition en cycles à supports disjoints de s alors $\sigma \circ s \circ \sigma^{-1} = (\sigma \circ c_1 \sigma^{-1}) \circ \cdots \circ (\sigma \circ c_r \circ \sigma^{-1})$ est celle de $\sigma \circ s \circ \sigma^{-1}$.

(ii) Si $\sigma = c_1 \circ \cdots \circ c_r$ est la décomposition en cycles à supports disjoints de σ, chaque cycle est d'ordre sa longueur et ces cycles commutent car leurs supports sont disjoints, de sorte que l'ordre de σ est le ppcm des longueurs des cycles c_i pour $1 \leq i \leq r$. En particulier dans $\mathcal{S}_5$, on trouve que l'ordre maximal d'un élément est 6.

(iii) Soit $x \in \{1, \cdots, n\}$ et cherchons quel est le cardinal de l'orbite de x

sous c^k :
$$(c^k)^i(x) = x \Longleftrightarrow n|ki \Longleftrightarrow \frac{n}{(n \wedge k)}|i$$
de sorte que l'orbite de x sous c^k est toujours de longueur $n/(n \wedge k)$. La décomposition en cycles à supports disjoints de c^k est donc constitué de $(n \wedge k)$ cycles de longueur $n/(n \wedge k)$.

Solution de l'exercice (??)

(i) On rappelle (cf. le théorème (**??**)) que pour $n \geq 5$, $\mathcal{A}_n$ est simple et que les sous-groupes distingués de $\mathcal{S}_n$ sont $\{1\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$. On considère l'action par translation à gauche de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$, ce qui donne un morphisme $\phi : \mathcal{S}_n \longmapsto \mathcal{S}(\mathcal{S}_n/H)$; son noyau qui est un sous-groupe distingué. Or si $\sigma \in \ker \phi$, on a $\overline{\sigma h} = \bar{h}$, soit $\sigma \in H$, de sorte que $\ker \phi \subset H$; or H étant d'indice n dans $\mathcal{S}_n$, $\ker \phi$ ne peut qu'être le sous-groupe trivial.

(ii) D'après (i) $\phi(H)$ est un sous-groupe de cardinal $(n-1)!$, laissant stable l'élément $\bar{Id}$, de sorte que $\phi(H)$ est inclus dans un sous-groupe de $\mathcal{S}(\mathcal{S}_n/H)$ est isomorphe à $\mathcal{S}_{n-1}$; par cardinalité on en déduit $H \simeq \mathcal{S}_{n-1}$.

(iii) On considère de même l'action par translation à gauche de $\mathcal{S}_n$ sur $\mathcal{S}_n/H$ ce qui donne un morphisme de groupe $\mathcal{S}_n \longmapsto \mathcal{S}_k$ qui pour des raisons évidente de cardinalité ($k < n$) ne peut être injectif ; or le noyau étant un sous-groupe distingué contenu dans H car stabilisant la classe de l'identité, on en déduit $\mathcal{A}_n \subset H$ et donc comme $k > 1$, $H = \mathcal{A}_n$.

Opération d'un groupe sur un ensemble

Solution de l'exercice (??)

(a) L'équation aux classes s'écrit :
$$n = a_1 + 3a_2 + 7a_3 + 21a_4 \tag{1}$$
où a_1 (resp. a_2, resp. a_3, resp. a_4) désigne le nombre de classes de cardinal 1 (resp. 3, resp. 7, resp. 21). Pour $n = 19$, a_4 est forcément nul, si par ailleurs on impose a_1 nul, l'équation (1) s'écrit $3a_2 + 7a_3 = 19$ ce qui impose $a_3 = 1$ et $a_2 = 4$, soit 5 orbites dont une de cardinal 7 et 4 de cardinal 3.

(b) Pour $n = 11$, a_4 est de même nul. Par ailleurs l'équation $3a_2 + 7a_3 = 11$ n'a pas de solutions entières de sorte que a_1 ne peut pas Ítre nul, *i.e.* il existe au moins un point fixe.

(c) D'après l'exercice (**??**) du chapitre 1, l'équation d'inconnues a et b, $pq - p - q = ap + bq$ n'a pas de solutions entières positives, d'où le résultat.

Trois polyèdres réguliers et leurs groupes.

Le tétraèdre régulier

(i) L'isobarycentre O du tétraèdre est invariant par tout éléments de $\mathcal{I}_T$ de sorte que l'application $vect : g \in \mathcal{I}_T \mapsto \vec{g} \in O(3)$ définie par $\vec{g}(\vec{v}) = O\vec{g(M)}$ où M est tel que $\vec{OM} = \vec{v}$ est un morphisme de groupe injectif.

(ii) Une application affine est déterminée par les images de 4 points non coplanaires. Tout élément de $\mathcal{I}_T$ permute les 4 sommets, de sorte que l'on a une injection $i : \mathcal{I}_T \longmapsto \mathcal{S}_4$.

(iii) Il suffit de vérifier que la transposition (12) est dans l'image de i ; en effet toute transposition est alors dans l'image et comme les transpositions engendrent $\mathcal{S}_4$, i sera alors un isomorphisme. La transposition (12) est l'image par i de la réflexion par rapport au plan médiateur du segment $[1, 2]$. Le sous-groupe $\mathcal{D}_T$ étant d'indice 2, il en est de mÍme de son image soit $\mathcal{D}_T \simeq \mathcal{A}_4$.

Le cube

(i) Comme dans l'exercice précédent, on a une injection $i : \mathcal{I}C \hookrightarrow \mathcal{S}_8$. L'indice $[\mathcal{I}_C : \mathcal{D}_T]$ est égal à 2 ou 1 selon que $\mathcal{I}_C$ contienne ou non une isométrie négative ; clairement la réflexion par rapport à un plan qui coupe le cube en deux selon le milieu de 4 arêtes parallèles appartient à $\mathcal{I}_C \backslash \mathcal{D}_C$ de sorte que $[\mathcal{I}_C : \mathcal{D}_C] = 2$.

(ii) On remarque que les grandes diagonales sont les plus grandes distances entre deux éléments du cubes et sont donc conservées par toute isométrie. On obtient ainsi un morphisme $f : \mathcal{I}_C \longmapsto \mathcal{S}_4$. Soit alors $g \in \ker f$. On vérifie aisément que $g = \pm Id$. Pour montrer la surjectivité, il suffit comme précédemment de montrer que la transposition (12) est obtenue. Notons $abcd$ les sommets de la face du dessus du cube et $a'b'c'd'$ les points de la face du dessous de sorte que les grandes diagonales soient aa', bb', cc' et dd'. La réflexion par rapport au plan contenant aa' et la direction orthogonale à la face du dessus, a pour image la transposition qui échange bb' et dd' et laisse fixe aa' et cc'. On obtient ainsi que f induit un isomorphisme de $\mathcal{D}_C$ sur $\mathcal{S}_4$.

(iii) La suite exacte

$$1 \longmapsto \mathcal{D}_C \longmapsto \mathcal{I}_C \longmapsto \mathbf{Z}/2\mathbf{Z} \longmapsto 1$$

est scindée, un relèvement étant donné par $\{\pm Id\}$ de sorte que $\mathcal{C}_C$ est isomorphe au produit direct de $\mathcal{S}_4 \times \mathbf{Z}$.

L'octaèdre

On remarque que le dual du dual d'un point (resp. d'un plan) est le même point (resp. plan). Ainsi le dual du cube est l'octaèdre. En outre toute isométrie préserve le produit scalaire, de sorte qu'une isométrie conservant une figure, conserve aussi la figure duale. On en déduit alors que le groupe de l'octaèdre est celui du cube.

Remarque : Le tétraèdre est autodual.

Problèmes

Solution du problème (??)

(1) Un élément x de G est dans $\ker \phi$, si et seulement si, pour tout $g \in G$, $xg \in gH$ ou de manière équivalente, $x \in gHg^{-1}$, d'où le résultat.

(2) On fait agir H sur $E = G/H$ par translation à gauche ; l'équation aux classes s'écrit $p = \sum_{x \in \mathcal{O}} |x|$, où $\mathcal{O}$ désigne l'ensemble des orbites. On sépare cette somme en deux en différenciant les orbites de cardinal 1 : $p = k + \sum_{x \in \mathcal{O}^1} [G : G_x]$, où $\mathcal{O}^1$ est l'ensemble des orbites de cardinal supérieur strictement à 1, et G_x est le stabilisateur d'un élément quelconque de l'orbite x ; G_x est un sous-groupe de G et d'après le théorème de Lagrange, $[G : G_x]$ est un diviseur de $|G|$ et est donc supérieur ou égal à p. Or on a $k \geq 1$ car H est stable sous l'action de H ; ainsi $\mathcal{O}^1$ est vide, soit toutes les orbites sont de cardinal 1, *i.e.* $H = H_1$ et donc H est distingué dans G.

(3) *cf.* l'exercice (**??**).

(4) Le raisonnement est strictement identique à celui de l'exercice (**??**) (a).

(5) même preuve que dans (**??**, (b)).

(6) cf. (**??**), (c).