Devoir Maison n^{o}2

Exercice 1

Soit G un groupe et X un ensemble. On note $S(X)$ l'ensemble des permutations de X. Soit $\phi\colon G \to S(X)$ un morphisme de groupes.

1. Montrer que $g.x = \phi(g)(x)$ définit une action du groupe G sur X.

   — pour tout $x \in X$, $1 \cdot x = \phi(1)(x) = \mathrm{Id}(x) = x$.
   — pour tout $x \in X$, et $g, h \in H$ on a

$$\begin{aligned} g \cdot (h \cdot x) &= g \cdot \phi(h)(x) \\ &= [\phi(g) \circ \phi(h)](x) = \phi(gh)(x) \\ &= (gh) \cdot x \end{aligned}$$

   Donc $g \cdot x = \phi(g)(x)$ définit bien une action de groupe.

2. On considère l'action de G sur lui-même par translation à gauche.
   — Expliciter $\phi\colon G \to S(G)$ dans ce cas.

   Pour tout $x \in X = G$, $\phi(g)(x) = gx$.

   — Montrer que cette action est fidèle.

   Soit $g \in G$. Si pour tout $x \in G$, $g \cdot x = gx = x$, alors évidemment $g = 1$. L'action est donc fidèle.

3. On suppose que $|G| = n$.
   — Montrer que $S(G)$ est isomorphe à S_n.

   Soit $f\colon G \to \{1, ..., n\}$ une bijection. Alors

$$\Psi\colon \begin{cases} S(G) & \to S_n \\ \sigma & \mapsto f \circ \sigma \circ f^{-1} \end{cases}.$$

   est un morphisme de groupes (exo facile). En définissant :

$$\Phi\colon \begin{cases} S_n & \to S(G) \\ \sigma & \mapsto f^{-1} \circ \sigma \circ \end{cases}$$

   on vérifie facilement que $\Phi \circ \Psi = \mathrm{Id}_{S(G)}$ et $\Psi \circ \Phi = \mathrm{Id}_{S_n}$, donc Ψ est bijective et donc un isomorphisme.

   — Montrer que G est isomorphe à un sous-groupe de S_n.

   Le morphisme $\phi\colon G \to S(G)$ défini à la question 2), est un morphisme injectif de groupes (car l'action est fidèle). La composée $\Psi \circ \phi$ est donc un morphisme injectif de G dans S_n. Donc G est isomorphe au sous-groupe $\mathrm{Im}(\Psi \circ \phi)$ de S_n.

Exercice 2

On note par A_4 l'ensemble des éléments du groupe de permutations S_4 de signature 1.

1. Faire la liste des éléments de A_4 et donner leurs ordres.

   — Id est d'ordre 1
   — les produits de 2 transpositions de supports disjoints (12)(34), (13)(24) et (14)(23) sont d'ordre 2.
   — les cycles (123), (132), (124), (142), (134), (143), (234), et (243) sont d'ordre 3.
   On a bien fait le tour : en effet, il y a là 12 éléments, or $\#(A_4) = \#(S_4)/2 = 4!/2 = 12$.

2. Soit H l'ensemble formé de l'identité, et des permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

Montrer que H est un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et est distingué dans A_4.

Pour simplifier, posons $\sigma_1 = (12)(34)$, $\sigma_2 = (13)(24)$ et $\sigma_3 = (14)(23)$. On vérifie facilement que $H = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_3\}$ est un groupe et que

$$\Phi\colon \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \to H \\ (0,0) & \mapsto \mathrm{Id} \\ (1,0) & \mapsto \sigma_1 \\ (0,1) & \mapsto \sigma_2 \\ (1,1) & \mapsto \sigma_3 \end{cases}$$

est un isomorphisme de groupes.
Montrons maintenant que H est distingué dans A_4. Remarquons que $H \setminus \{\mathrm{Id}\}$ est l'ensemble des permutations de la forme $(ab)(cd)$ où $\{a,b,c,d\} = \{1,2,3,4\}$. Soit $\sigma_i = (ab)(cd)$ une telle permutation. Pour toute permutation σ, $\sigma\sigma_i\sigma^{-1} = (\sigma(a)\sigma(b))(\sigma(c))(\sigma(d))$ et comme σ est une bijection de $\{1,2,3,4\}$, on a bien encore un élément de $H \setminus \{\mathrm{Id}\}$.

3. Montrer que les sous-groupes propres de H ne sont pas distingués dans A_4.

D'après le théorème de Lagrange, les sous-groupes de H sont de cardinal $1, 2$ ou 4. Les sous-groupes non-triviaux sont donc de cardinal 2. Ces sous-groupes de cardinal 2 sont les $\langle \sigma_i \rangle$, pour $i = 1,2,3$. Ils sont donc de la forme $\{\mathrm{Id}, \sigma_i = (ab)(cd)\}$, où $\{a,b,c,d\} = \{1,2,3,4\}$. Or si $\sigma = (bcd)$, d'après le cours $\sigma\sigma_i\sigma^{-1} = (a\sigma(b))(\sigma(c)\sigma(d)) \notin \{\mathrm{Id}, \sigma_i(ab)(cd)\}$. Donc $\langle \sigma_i \rangle$ n'est pas distingué dans A_4

4. Montrer que tout sous-groupe d'indice 2 d'un groupe G est distingué.

Si H est d'indice 2, alors le quotient à droite G/H ainsi que le quotient à gauche $H \setminus G$ sont de cardinal 2. Donc, si $x \in G \setminus H$, on a $G/H = \{H, xH\}$ et $H \setminus G = \{H, Hx\}$. Or ce sont deux partitions de G donc $xH = Hx$. Si $x \in G$, l'égalité $xH = Hx$ est triviale. Donc H est distingué dans G.

5. Déduire des questions précédentes que A_4 n'a pas de sous-groupe d'ordre 6 (on pourra raisonner par l'absurde et remarquer qu'une intersection de sous-groupes distingués est distinguée).

Supposons par l'absurde que A_4 a un sous-groupe K d'ordre 6. D'après le théorème de Lagrange, le cardinal de $K \cap H$ divise ceux de K et H, donc vaut 1 ou 2. On exclut $K \cap H = \{1\}$ car alors $|KH| = |K|.|H|$ (Cf. DS) ce qui est absurde ! Donc $K \cap H$ est un sous-groupe d'ordre 2 dans H.
D'après les questions 2 et 4, H et K sont distingués dans A_4, donc leur intersection l'est aussi, ce qui contredit la question 3.

6. Déterminer tous les sous-groupes de A_4. Lesquels sont distingués ?

D'après le théorème de Lagrange et la question précédente, les ordres possibles des sous-groupes de A_4 sont $1, 2, 3, 4, 12$.
— Passons rapidement sur les groupes triviaux $\{1\}$ et A_4 qui sont distingués.
— Les ordres $2, 3$ sont premiers, donc les groupes de ces ordres sont monogènes. Or on a fait en première question la liste des éléments d'ordre 2 et 3.
  — Les groupes d'ordre 2 sont donc les $\langle \sigma_i \rangle$, pour $i = 1,2,3$. On a vu qu'ils n'étaient pas distingués/.
  — Les groupes d'ordres 3 sont $\langle (123) \rangle$, $\langle (124) \rangle$, $\langle (134) \rangle$, $\langle (234) \rangle$. Ces groupes ne sont pas distingués dans A_4, même genre d'argument qu'en 3. De fait, on envoie facilement tout groupe sur un autre en conjuguant par une permutation bien choisie.

— Soit K un groupe d'ordre 4. Ce groupe ne peut être cyclique puisqu'il n'y a pas d'élément d'ordre 4 dans A_4. Donc les ordres de ses éléments autres que Id sont 2. Or il n'y a que 3 él'ements d'ordre 2 : les σ_i. On en déduit que $K = H$ est l'unique groupe d'ordre 4.
On a déjà montré que H est distingué.

Exercice 3 Soit $n \geq 2$ un entier.

1. Montrer que les transpositions sont conjuguées dans S_n : pour toute paire de transpositions $\tau_1, \tau_2 \in S_n$, il existe une permutation $\sigma \in S_n$ telle que

$$\tau_2 = \sigma\tau_1\sigma^{-1}$$

Soient deux transpositions $\tau_1 = (ab)$ et $\tau_2 = (cd)$. Soit σ une permutation qui envoie a sur c et b sur d. Alors $\sigma\tau_1\sigma^{-1} = (\sigma(a)\sigma(b)) = \tau_2$.

2. En déduire que le seul morphisme de groupes non-trivial de S_n dans $(\mathbb{C}^*, \times)$ est la signature.

Soit $\phi\colon S_n \to \mathbb{C}^*$ un morphisme de groupes. Alors pour toutes transpositions τ_1, τ_2 il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$, donc

$$\phi(\tau_2) = \phi(\sigma)^{-1}\phi(\tau_1)\phi(\sigma) = \phi(\tau_1)$$

par commutativité de $\mathbb{C}^*$. Donc toutes les transpositions ont la même image.

Or, si τ est une transposition, $[\phi(\tau)]^2 = \phi(\tau^2) = \phi(\text{Id}) = 1$ donc $\phi(\tau) = \pm 1$. Donc il y a deux cas de figures :
— toutes les transpositions sont envoyées sur 1, et comme les transpositions engendrent S_n, ϕ est identiquement égal à 1,
— toutes les transpositions sont envoyées sur -1, et comme les transpositions engendrent S_n, $\text{Im}(\phi) \subset \langle -1 \rangle = \{-1, 1\}$. D'après le cours, ce morphisme est donc la signature.

3. Conclure que le seul sous-groupe de S_n d'indice 2 est le groupe A_n des permutations de signature 1. (On pourra utiliser la question 4 de l'exercice précédent)

Soit H un sous-groupe de S_n d'indice 2. Alors H est distingué dans S_n d'après la question 4 de l'exercice 2. Donc S_n/H est un groupe de cardinal 2 et donc isomorphe à $\{-1, 1\}$. La surjection canonique $s\colon S_n \to S_n/H$ nous donne donc un morphisme non trivial de S_n vers $\{-1, 1\}$. C'est la signature d'après la question précédente. Son noyau H est donc A_n. Le seul sous-groupe de S_n d'indice 2 est donc le groupe A_n.

Exercice 4 Soit G un groupe fini et p un facteur premier de $|G|$.

1. Montrer que le sous-ensemble de G^p

$$\Sigma = \{(x_1, ..., x_p) \in G^p / x_1 ... x_p = 1_G\}.$$

est en bijection avec G^{p-1}.

Remarquons que

$$\Sigma = \{(x_2x_3...x_p)^{-1}, x_2, ..., x_p)/x_2, ..., x_p \in G\}.$$

Donc clairement Σ est en bijection avec G^{p-1}.

2. On note "n mod p" le reste de la division euclidienne de n par p. Montrer que l'application

$$\phi\colon \begin{cases} \mathbb{Z}/p\mathbb{Z} \times \Sigma & \to \Sigma \\ \left(\bar{k}, (x_1, ..., x_p)\right) & \mapsto \bar{k} \cdot (x_1, ..., x_p) = \left(x_{1+k \text{ mod } p}, ..., x_{p+k \text{ mod } p}\right) \end{cases}$$

est bien définie est que c'est une action du groupe $\mathbb{Z}/p\mathbb{Z}$ sur l'ensemble Σ.

Si $k, k' \in \mathbb{Z}$ sont tels que $\bar{k} = \bar{k}'$ dans $\mathbb{Z}/p\mathbb{Z}$, alors $k \bmod p = k' \bmod p$. Donc l'application ci-dessus est bien définie.
De plus, $\bar{0} \cdot (x_1, ..., x_p) = (x_1, ..., x_p)$ et pour tous $k, k' \in \mathbb{Z}$,

$$\begin{aligned} \bar{k}' \cdot (\bar{k} \cdot (x_1, ..., x_p)) &= \left(x_{1+k+k' \text{ mod } p}, ..., x_{p+k+k' \text{ mod } p}\right) \\ &= k \bar{+} k' \cdot (\bar{k} \cdot (x_1, ..., x_p)) \\ &= (\bar{k} + \bar{k}') \cdot (\bar{k} \cdot (x_1, ..., x_p)) \end{aligned}$$

On a donc bien une action de groupes.

3. Montrer que le stabilisateur de $(x_1, ..., x_p)$ est $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x_1 = x_2 = ... = x_p$.

Si le $(x_1, ..., x_p)$ est $\mathbb{Z}/p\mathbb{Z}$, alors en particulier $\bar{1}$ y est et donc $x_1 = x_2$, $x_2 = x_3$, ... $x_{p-1} = x_p$. Réciproquement, si $x_1 = x_2 = ... = x_p$, $\bar{k} \cdot (x_1, ..., x_p) = (x_1, ..., x_p)$ pour tout k.

Donc le stabilisateur de $(x_1, ..., x_p)$ est $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $x_1 = x_2 = ... = x_p$.

4. En appliquant l'équation aux classes, en déduire que G contient au moins un élément d'ordre p.

On applique l'équation aux classes :

$$|G|^{p-1} = |\Sigma| = \sum_{O \in \{Orbites\}} |\mathrm{O}|$$

Comme p divise $|G|$ et $p \geq 2$, p divise $|G|^{p-1}$. Par ailleurs, le cardinal de l'orbite d'un point $x = (x_1, ..., x_p)$ divise $|\mathbb{Z}/p\mathbb{Z}|$, donc vaut p ou 1. Donc, le nombre d'orbites de cardinal 1 divise p.

Or, on sait qu'il y a une orbite de cardinal 1 dans Σ : celle de $(1, ..., 1)$. Il y en a donc au moins p. En particulier, il existe $x = (x_1, ..., x_p) \in \Sigma \setminus \{(1, ..., 1)\}$ dont l'orbite est de cardinal 1. On a alors $x_1 = x_2 = ... = x_p$, d'après la question 3.

On a donc trouvé un elément $x_1 \neq 1$ tel que $x_1 ... x_p = x_1^p = 1$. Comme p premier, on a donc un élément d'ordre p.

CQFD