Examen "Groupes"

Corrigé

1. Considérons les deux éléments suivants du groupe symétrique S_9 :

$$\sigma_1 = (1\,2)(3\,4\,5)(6\,7\,8\,9) \quad \text{et} \quad \sigma_2 = (1\,2\,3\,4)(5\,6\,7)(8\,9).$$

Justifier pourquoi σ_1 et σ_2 sont conjugués, puis exhiber une permutation $\omega \in S_9$ telle que $\sigma_2 = \omega\sigma_1\omega^{-1}$. Quel est le cardinal (une expression sous forme de produit d'entiers me suffit) de la classe de conjugaison de σ_1 dans S_9 ?

Solution. (**2 points**)
Les décompositions canoniques des permutations σ_1 et σ_2 font intervenir des cycles de mêmes longueurs (2,3 et 4), ces deux permutations sont donc conjuguées. En écrivant

$$\sigma_1 = (1\,2)(3\,4\,5)(6\,7\,8\,9)$$
$$\sigma_2 = (8\,9)(5\,6\,7)(1\,2\,3\,4)$$

on trouve (parmi de nombreux choix possibles)

$$\omega = (1\,8\,3\,5\,7\,2\,9\,4\,6)$$

Le cardinal de la classe de conjugaison s'obtient en calculant le nombre de permutations de S_9 de type 2,3,4 :

- $(9.8)/2 = 9.4$ *choix pour la transposition;*
- $2.(7.6.5)/6 = 7.5.2$ *choix pour le 3-cycle;*
- *6 choix pour le 4-cycle*

Soit finalement $9.8.7.6.5$ *choix possibles.*

2. Soit $G = (\mathbb{Z}/7\mathbb{Z})^*$ le groupe multiplicatif des éléments inversibles de l'anneau $\mathbb{Z}/7\mathbb{Z}$. Rappeler les résultats du cours qui permettent de prédire *a priori* d'une part que G est cyclique, et d'autre part le nombre d'éléments dans G qui peuvent être choisis comme générateur. Expliciter ensuite la liste des éléments $g \in G$ tel que $G = \langle g \rangle$.

Solution. (**2 points**)
On sait que le groupe multiplicatif d'un corps fini est cyclique (plus généralement, tout sous-groupe fini de K^* où K est un corps est cyclique). Ici on a donc affaire à un groupe cyclique d'ordre 6, c'est-à-dire isomorphe à $\mathbb{Z}/6\mathbb{Z}$, et ce dernier groupe admet deux générateurs possibles, $\bar{1}$ et $\bar{5}$, qui sont les seuls entiers entre 1 et 6 premiers avec 6.

Pour revenir au groupe $G = (\mathbb{Z}/7\mathbb{Z})^*$, on voit que

- $\bar{1}$ *est d'ordre 1;*
- $-\bar{1}$ *est d'ordre 2;*
- $\bar{2}$ *est d'ordre 3;*
- $\bar{3}$ *est d'ordre 6;*
- $-\bar{2}$ *est d'ordre 6;*
- $-\bar{3}$ *est d'ordre 3;*

Les deux générateurs attendus sont donc $-\bar{2}$ et $\bar{3}$.

3. Dans les groupes suivants, donner un exemple d'élément d'ordre 4 s'il en existe, ou sinon donner un argument pour justifier qu'il n'y en a pas :

   (a) Le groupe linéaire $\mathrm{GL}_2(\mathbb{R})$;

   (b) Le groupe alterné A_8;

(c) Le groupe $\mathrm{Isom}^+(T) \subset \mathrm{SO}_3(\mathbb{R})$ des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T.

(d) Un groupe d'ordre 16 quelconque (ici il s'agit de décider si *tout* groupe d'ordre 16 admet un élément d'ordre 4).

SOLUTION. (**2 points**)

(a) La rotation d'angle $\pi/2$, est un exemple, sa matrice est $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

(b) $(1234)(5678)$ *ou* $(1234)(56)$ *sont des exemples.*

(c) Le groupe $\mathrm{Isom}^+(T)$ *ne contient pas d'éléments d'ordre 4 : il contient 12 éléments dont huit d'ordre 3, trois d'ordre 2, et l'identité. On pouvait aussi dire que* $\mathrm{Isom}^+(T)$ *est isomorphe à A_4, et que A_4 ne contient pas d'éléments d'ordre 4 (les 4-cycles ne sont pas de signature 1).*

(d) Le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est un groupe d'ordre 16 qui ne contient que des éléments d'ordre 2 à part le neutre.

4. Montrer que le groupe $\mathrm{Isom}(C)$ des isométries de $\mathbb{R}^3$ préservant un cube C peut s'écrire comme un produit direct de deux sous-groupes isomorphes respectivement à S_4 et $\mathbb{Z}/2\mathbb{Z}$. Montrer ensuite que $\mathrm{Isom}(C)$ peut s'écrire comme un produit semi-direct (mais non direct) de deux sous-groupes isomorphes eux aussi à S_4 et $\mathbb{Z}/2\mathbb{Z}$.

SOLUTION. (**2 points**)
Le groupe $\mathrm{Isom}^+(C)$ *des rotations préservant un cube est isomorphe à S_4 : en numérotant D_1, D_2, D_3, D_4 les diagonales du cube, cet isomorphisme envoie $R \in \mathrm{Isom}^+(C)$ sur $\sigma \in S_4$ de façon a ce que $R(D_i) = D_{\sigma(i)}$. De plus* $\mathrm{Isom}^+(C)$ *est distingué dans* $\mathrm{Isom}(C)$ *comme noyau du morphisme déterminant.*

Prenons S_O la symétrie centrale (par rapport au centre de gravité du cube). Il s'agit d'un élément de $\mathrm{Isom}(C) \smallsetminus \mathrm{Isom}^+(C)$ *qui commute avec tout élément de* $\mathrm{Isom}(C)$*, ainsi* $\mathrm{Isom}(C)$ *est le produit direct de* $\mathrm{Isom}^+(C) \simeq S_4$ *et de $\langle S_O \rangle \simeq \mathbb{Z}/2\mathbb{Z}$.*

Prenons maintenant S une symétrie orthogonale préservant le cube (par rapport à un plan parallèle à deux faces opposées). Alors $\mathrm{Isom}(C)$ *est le produit semi-direct de* $\mathrm{Isom}^+(C) \simeq S_4$ *et de $\langle S_O \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Ce n'est pas un produit direct car $\langle S_O \rangle$ n'est pas distingué dans* $\mathrm{Isom}(C)$.

5. Notons $G = \mathrm{Isom}^+(T)$ le groupe des rotations de $\mathbb{R}^3$ préservant un tétraèdre régulier T. Décrire géométriquement les éléments d'ordre 3 dans G, en déduire leur nombre, puis justifier (toujours géométriquement, c'est-à-dire, sans utiliser l'isomorphisme $\mathrm{Isom}^+(T) \simeq A_4$) qu'il existe deux éléments d'ordre 3 non conjugués dans G.

SOLUTION. (**2 points**)
Les éléments d'ordre 3 dans $\mathrm{Isom}^+(T)$ *sont les rotations d'angle $\pm 2\pi/3$ et d'axe passant par un sommet et le milieu de la face opposée. Comme il y a 4 tels axes, on compte en tout 8 rotations d'ordre 3. De plus les axes sont munis d'une orientation intrinsèque (disons de la face vers le sommet), qui est préservée par conjugaison par une rotation, ainsi on en déduit qu'une rotation d'angle $2\pi/3$ n'est pas conjuguée à la rotation d'angle $-2\pi/3$ et de même axe.*

NB: on pouvait aussi dire qu'il est impossible d'avoir une classe de conjugaison de cardinal 8 dans un groupe d'ordre 12, puisque le premier nombre est censé diviser le second.

6. Donner la liste des groupes abéliens d'ordre 36 à isomorphisme près, et justifier que la liste est complète en énonçant précisément le théorème de classification que vous utilisez.

SOLUTION. (**2 points**)
Tout groupe abélien fini admet une unique écriture comme produit de groupes cycliques d'ordre des puissances de nombres premiers. Comme $36 = 2^2.3^2$, on obtient 4 possibilités qui sont

$$\mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/3, \quad \mathbb{Z}/4 \times \mathbb{Z}/3 \times \mathbb{Z}/3, \quad \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/9, \quad \mathbb{Z}/4 \times \mathbb{Z}/9$$

On pouvait aussi utiliser que tout groupe abélien fini admet une unique écriture comme produit de groupes cycliques d'ordre $a_i \geq 2$, avec a_{i+1} divisant a_i pour tout i. On obtenait alors la liste (équivalente à la précédente, s'en persuader à l'aire du théorème des restes chinois !):

$$\mathbb{Z}/6 \times \mathbb{Z}/6, \quad \mathbb{Z}/12 \times \mathbb{Z}/3, \quad \mathbb{Z}/18 \times \mathbb{Z}/2, \quad \mathbb{Z}/36.$$

7. Montrer de façon élémentaire (aucun argument sophistiqué au-delà du théorème de Lagrange) que tout groupe d'ordre 6 non cyclique est isomorphe au groupe symétrique S_3.

   SOLUTION. (**2 points**)
   Soit G un groupe d'ordre 6 non cyclique, et $g \in G$ distinct de l'élément neutre. Par Lagrange, et comme on suppose G non cyclique, l'ordre de g est 2 ou 3. G ne peut pas contenir deux éléments a, b d'ordre 2 tel que le produit ab soit aussi d'ordre 2, car alors $\{1, a, b, ab\}$ serait un sous-groupe, contradiction avec Lagrange. Donc G contient au moins un élément d'ordre 3, et comme les éléments d'ordre 3 arrivent par paire g, g^{-1}, il y en a au plus 4 dans G. Bilan : G contient un élément τ d'ordre 2, et un élément γ d'ordre 3. On a $G = \langle \tau, \gamma \rangle$, par Lagrange à nouveau. Les éléments τ et γ ne commutent pas, sinon $\tau\gamma$ serait d'ordre $\mathrm{PPCM}(2,3) = 6$ et on a exclu ce cas. Donc $\gamma\tau\gamma^{-1}$ est d'ordre 2 et distinct de τ, donc il y a exactement 2 éléments d'ordre 3 dans G qui sont τ et τ^{-1} (plus la place pour deux autres...). Finalement $\sigma\tau\sigma = \tau^{-1}$ (seul élément d'ordre 3 distinct de τ), et cette identité permet de reconstruire entièrement la table de G, qui coïncide donc avec celle de S_3, via l'isomorphisme $\phi(\tau) = (12)$ et $\phi(\gamma) = (123)$.

8. Montrer que le groupe symétrique S_3 est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(S_3)$.

   SOLUTION. (**2 points**)
   L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de S_3 dans $\mathrm{Aut}(S_3)$, car le centre de S_3 est trivial.

   De plus $\phi \in \mathrm{Aut}(S_3)$ est déterminé par l'image des générateurs (12) et (13). Il y a au plus six choix possibles (choisir deux parmi les trois éléments d'ordre 2 de S_3), donc en comparant les cardinaux on obtient que le morphisme ci-dessus est un isomorphisme.

9. Soit p premier et $a \geq 1$. En utilisant une action de groupe que l'on précisera, montrer que tout groupe G d'ordre p^a admet un élément central (c'est-à-dire commutant avec tout élément de G) d'ordre p.

   SOLUTION. (**2 points**)
   On fait agir G sur lui-même par conjugaison. Les orbites sont ou bien de cardinal 1 (pour chaque élément du centre), ou bien de cardinal une puissance de p non égale à 1. En écrivant G comme une union d'orbites, on a donc $|Z(G)| \equiv 0 \mod p$, ce qui interdit à $Z(G)$ d'être trivial. Maintenant soit $g \in Z(G) \smallsetminus \{1\}$, donc g est d'ordre p^b pour un certain $1 \leq b \leq a$. Alors $g^{p^{b-1}}$ est central et d'ordre p, comme attendu.

10. Montrer qu'il n'existe qu'un seul groupe d'ordre 35 à isomorphisme près.

    SOLUTION. (**2 points**)
    Soit G un groupe d'ordre $35 = 5.7$. Par le théorème de Sylow, le nombre de 7-Sylow divise 5 et est congru à 1 modulo 7 : il y a donc un unique 7-Sylow S_7. De même le nombre de 5-Sylow divise 7 et est congru à 5 modulo 1 : de nouveau on conclut qu'il y a un unique 5-Sylow S_5 dans G. En particulier les groupes S_5, S_7 snt distingués dans G. Par ailleurs le théorème de Lagrange permet d'affirmer :

    - *Les sous-groupes S_5 et S_7 sont cycliques;*
    - *Les sous-groupes S_5 et S_7 sont d'intersection triviale;*
    - *Les sous-groupes S_5 et S_7 engendrent G : le sous-groupe $\langle S_5, S_7 \rangle$ est d'ordre un multiple de 5 et de 7, donc égal à 35;*

    On conclut que G est le produit direct des groupes cycliques S_5 et S_7, par le théorème des reste chinois G est donc isomorphe à $\mathbb{Z}/35$.