Feuille TD 1 – Exercices Algèbre – Groupes – Corrigé partiel

1 Généralités

Exercice 1 — Morphismes ou non ?.
Soit G un groupe. Les applications suivantes de G dans G sont-elles toujours des morphismes ?

1. $f_a : x \mapsto ax$, avec $a \in G$ fixé ;
2. $f_n : x \mapsto x^n$ pour $n \in \mathbf{N}^*$;
3. $g : x \mapsto x^{-1}$.

Solution.

1. On remarque que si $a \neq e$, alors $f_a(e) = a \neq e$ et on a donc pas un morphisme de groupes. En revanche, si $a = e$, on a l'identité qui est bien un morphisme de groupes.
   Une autre façon de le voir est de constater qu'en général, pour $x, y \in G$, $a(xy) \neq (ax)(ay)$ (sauf si $a = e$).
2. Ici on a bien $f_n(e) = e$ mais de on n'a pas un morphisme en général si G n'est pas abélien car $(xy)^n \neq x^n y^n$.
3. Idem, non en général si G n'est pas abélien car $(xy)^{-1} = y^{-1}x^{-1} \neq x^{-1}y^{-1}$.

Exercice 2 — Groupes, intersections et réunions.

1. Montrer que l'intersection d'une famille quelconque de sous-groupes d'un groupe G est aussi un sous-groupe.
2. Soient A et B deux sous-groupes d'un même groupe G. Montrer que $A \cup B$ est un sous-groupe de G si, et seulement si, $A \subseteq B$ ou $B \subseteq A$.
3. Que se passe-t-il si l'on considère la réunion d'au moins trois sous-groupes ?

Solution.

1. Soient $(G_i)_{i\in I}$ une famille de sous-groupes de G. On a clairement que $e \in \bigcap_{i\in I} G_i$. Par ailleurs, pour tous $x, y \in \bigcap_{i\in I} G_i$, on a que pour tout $i \in I$, $x, y \in G_i$ qui est un sous-groupe de G. Par conséquent, pour tout $i \in I$, $x, y \in G_i$, $xy^{-1} \in G_i$ et $xy^{-1} \in \bigcap_{i\in I} G_i$ et on a gagné !
2. C'est clair si $B \subseteq A$ ou $A \subseteq B$. Réciproquement, supposons que $A \cup B$ soit un sous-groupe de G. Supposons par l'absurde que $B \not\subseteq A$ ou $A \not\subseteq B$. On dispose alors de $x \in A$, $x \notin B$ et de $y \in B$, $y \notin A$. Mais $x, y \in A \cup B$ qui est un groupe donc $xy \in A \cup B$. On a alors soit $xy \in A$ soit $xy \in B$ par définition. Si $xy \in A$, alors
$$y = x^{-1}(xy) \in A \quad \text{car} \quad x, xy \in A,$$
   ce qui est absurde. De même, si $xy \in B$, alors $x \in B$ et on aboutit à une contradiction. En conclusion, on a bien $B \subseteq A$ ou $A \subseteq B$.
3. Par exemple
$$\mathfrak{S}_3 = \mathfrak{A}_3 \cup \langle(12)\rangle \cup \langle(13)\rangle \cup \langle(23)\rangle \quad \text{ou} \quad (\mathbf{Z}/2\mathbf{Z})^2 = \langle(\overline{1},\overline{0})\rangle \cup \langle(\overline{0},\overline{1})\rangle \cup \langle(\overline{1},\overline{1})\rangle.$$
   En revanche, dans le cas d'un espace vectoriel E sur un corps k **infini**, on a bien que
$$E \neq F_1 \cup F_2 \cup \cdots \cup F_n$$
   pour tous $F_1, F_2, \ldots, F_n$ des sous-espaces vectoriels stricts de E. En effet, sinon on peut supposer que $E = F_1 \cup F_2 \cup \cdots \cup F_n$ et que $F_n \not\subseteq F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ (sinon il suffit de se débarrasser de F_n !). On peut alors choisir $x \in F_n \setminus F_1 \cup F_2 \cup \cdots \cup F_{n-1}$ et $y \notin F_n$. On a alors que pour tout $\lambda \in k$, $\lambda x + y \notin F_n$ et pour tout $i \leqslant n-1$, il existe au plus un $\lambda \in k$ tel que $\lambda x + y \in F_i$. En effet, si on dispose de $\lambda \neq \mu$ tels que $\lambda x + y$ et $\mu x + y$ sont dans F_i, alors $(\lambda - \mu)x \in F_i$ ce qui est absurde ! Mais comme $E = F_1 \cup F_2 \cup \cdots \cup F_n$, il existe au moins un $i \leqslant n-1$ tel que $\lambda x + y \in F_i$, ce qui vient contredire le caractère infini du corps k !

Exercice 3 — Botanique des groupes de petit cardinal. Décrire, à isomorphisme près, tous les groupes de cardinal $\leqslant 7$.

Solution. On a en fait la classification à isomorphisme près des groupes d'ordre $\leqslant 11$.

- Le seul groupe d'ordre 1 est le groupe trivial ;

- Si G est d'ordre p avec p premier alors nécessairement tout élément $g \in G$ distinct de l'identité est d'ordre p et engendre G si bien que[1] $G \cong \mathbf{Z}/p\mathbf{Z}$. Cela résout les cas $2, 3, 5, 7, 11$;
- Si G est d'ordre 4, on a que $G \cong \mathbf{Z}/4\mathbf{Z}$ si G contient un élément d'ordre 4 et sinon $G \cong (\mathbf{Z}/2\mathbf{Z})^2$ et G est engendré par toute paire d'éléments d'ordre 2 (qui commutent). En effet, l'ordre d'un élément non trivial de G divise 4 par Lagrange et vaut donc 2 ou 4. Si on a un élément d'ordre 4, alors G est cyclique et $G \cong \mathbf{Z}/4\mathbf{Z}$. Sinon, tout élément non trivial est d'ordre 2 et on peut faire appel à l'exercice 11 ou raisonner à la main. On doit avoir (puisque G est d'ordre 4) au moins un élément d'ordre 2, que nous pouvons appeler x. Puisque $x^2 = e$, $x^{-1} = x$ et donc on doit nécessairement avoir dans G un autre élément $y \neq x$ d'ordre 2. On a ainsi

$$\{e, x, y, xy\} \subseteq G \quad \text{et donc} \quad G = \{e, x, y, xy\}.$$

  Noter qu'ici on a utilisé que $xy \neq e, x, y$. On en déduit que $yx \in G$ et $yx \neq e, x, y$ donc $yx = xy$ et cela permet d'écrire la table de G. On reconnaît celle de $(\mathbf{Z}/2\mathbf{Z})^2$ si bien que $G \cong (\mathbf{Z}/2\mathbf{Z})^2$.
- Si G est d'ordre 6, on a que $G \cong \mathbf{Z}/6\mathbf{Z}$ si[2] G contient un élément d'ordre 6 (ou deux éléments d'ordre 2 et 3 respectivement qui commutent) et sinon[3] $G \cong \mathfrak{S}_3$ et G est engendré par un élément τ d'ordre 2 et un élément σ d'ordre 3 tels que $\tau\sigma\tau = \sigma^2$. En effet, l'ordre d'un élément non trivial de G vaut (par Lagrange) 2, 3 ou 6. Si on a un élément d'ordre 6, alors G est cyclique et $G \cong \mathbf{Z}/6\mathbf{Z}$. On peut donc supposer que tout élément non trivial est d'ordre 2 ou 3. On va montrer qu'il existe un élément d'ordre 2 et un élément d'ordre 3. En effet, si tous les éléments sont d'ordre 2, il vient qu'alors G est abélien[4] et contient au moins deux éléments d'ordre 2 distincts qui commutent. Le sous-groupe engendré par ces deux éléments est alors isomorphe à $(\mathbf{Z}/2\mathbf{Z})^2$ donc d'ordre 4, ce qui contredit le théorème de Lagrange. De même, si l'on avait que des éléments d'ordre 3, alors on disposerait d'au moins deux éléments x, y avec $y \neq x, x^2$ d'ordre 3 et

$$\{e, x, x^2, y, y^2, xy\} \subseteq G,$$

  où $xy \neq e, x, x^2, y, y^2$. On a alors que $xy^2 \neq e, x, x^2, y, y^2, xy$ et on aurait alors au moins 7 éléments dans G. On peut donc supposer que l'on dispose d'un élément τ d'ordre 2 et un élément σ d'ordre 3 et alors

$$\{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\} \subseteq G \quad \text{et donc} \quad G = \{e, \tau, \sigma, \sigma^2, \tau\sigma, \tau\sigma^2\}$$

  et où tous ces éléments sont deux à deux distincts. Alors, $\sigma\tau \in G$ et comme $\sigma\tau \neq \tau\sigma$, sinon le produit fournit un élément d'ordre[5] 6, on a nécessairement que $\tau\sigma\tau = \sigma^2$. Cela permet de dresser la table de multiplication du groupe G et on reconnaît celle de $\mathfrak{S}_3$ si bien que $G \cong \mathfrak{S}_3$.
- Si G est d'ordre 8, les exercices sur le groupe diédral et les quaternions ainsi le cours sur les produits semi-directs garantira que G est isomorphe soit à $(\mathbf{Z}/2\mathbf{Z})^3$, soit à $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, soit à $\mathbf{Z}/8\mathbf{Z}$, soit au groupe diédral $\mathbf{D}_4$ soit au groupe des quaternions $\mathbf{H}_8$.
- Si G est d'ordre $9 = 3^2$, le cours garantira que G est abélien et donc le théorème de structure des groupes abéliens de type fini garantit que $G \cong \mathbf{Z}/9\mathbf{Z}$ ou $G \cong (\mathbf{Z}/3\mathbf{Z})^2$;
- Si G est d'ordre $10 = 2 \times 5$ avec $2 \mid 5 - 1$, le cours sur le produit semi-direct garantira que G est soit abélien et isomorphe à $\mathbf{Z}/10\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z}$ soit isomorphe à l'unique produit semi-direct non trivial $\mathbf{Z}/2\mathbf{Z} \rtimes \mathbf{Z}/5\mathbf{Z}$ (qui est en fait isomorphe au groupe diédral[6] $\mathbf{D}_5$).

Pour aller plus loin, je vous renvoie aux feuilles de TD des annés précédentes[7] pour le cours d'Algèbre M1 MF, on peut classifier les groupes d'ordre p^2q avec p et q deux nombres premiers distincts ce qui traite le cas de 12 (qui peut également se traiter "à la main"), 13 est premier, 14 et 15 sont alors couverts par le cours sur le produit semi-direct ! On remarquera donc qu'il y a quelque chose qui semble se passer pour les

1. En effet, pour $x \in G \smallsetminus \{e\}$, $G = \{e, x, x^2, \ldots, x^{p-1}\}$. On pose alors l'application

$$\varphi : \left\{ \begin{array}{ccc} \mathbf{Z}/p\mathbf{Z} & \longrightarrow & G \\ \overline{k} & \longmapsto & x^k. \end{array} \right.$$

On vérifie comme toujours qu'une application définie sur un quotient est bien définie. Soient pour cela $\overline{k} = \overline{k'}$ pour $k, k' \in \mathbf{Z}$. Par définition, on a $k = k' + p\ell$ pour un certain entier ℓ. On a alors

$$x^k = x^{k'+p\ell} = x^{k'} \left(x^p\right)^\ell = x^{k'}$$

puisque $x^p = e$. L'application est donc bien définie et surjective vue la description de G plus haut. Comme $\#G = \#\left(\mathbf{Z}/p\mathbf{Z}\right) = p$, on a une bijection. Par ailleurs, il s'agit d'un morphisme de groupes puisque pour tous $\overline{k}, \overline{k'}$ dans $\mathbf{Z}/p\mathbf{Z}$ (attention ici que la loi de groupe sur $\mathbf{Z}/p\mathbf{Z}$ est **additive** tandis que celle sur G est **multiplicative**),

$$f\left(\overline{k} + \overline{k'}\right) = f\left(\overline{k+k'}\right) = x^{k+k'} = x^k x^{k'} = f\left(\overline{k}\right) f\left(\overline{k'}\right).$$

On a donc bien un isomorphisme et le résultat !

2. Noter que par théorème chinois, puisque 3 et 2 sont premiers entre eux, $G \cong \mathbf{Z}/6\mathbf{Z} \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

3. On a aussi que $G \cong \mathfrak{S}_3 \cong \mathbf{D}_3$ le groupe des isométries laissant invariant le triangle équilatéral formé des racines cubiques de l'unité et $\mathfrak{S}_3 \cong \mathbf{Z}/3\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$ est le seul produit semi-direct non trivial d'ordre 6.

4. En effet, pour tous $g, h \in G$, on a $(gh)^2 = e$ de sorte que $ghgh = e$ et en multipliant par h à droite il vient $ghg = h$ (car $h^2 = e$) et enfin en multipliant par g à droite on obtient $gh = hg$ (car $g^2 = e$).

5. En effet, $(\sigma\tau)^6 = \sigma^6\tau^6$ car G est abélien si $\sigma\tau = \tau\sigma$. Mais comme $\tau^2 = \sigma^3 = e$, on a $(\tau\sigma)^6 = e$. L'ordre de $\tau\sigma$ (qui est différent de e) vaut donc 2, 3 ou 6 mais $(\tau\sigma)^2 = \tau^2\sigma^2$ (toujours par caractère abélien de G) et donc $(\tau\sigma)^2 = \sigma^2 \neq e$ car $\tau^2 = e$ et σ est d'ordre 3. De même, $(\tau\sigma)^3 = \tau \neq e$ et l'ordre de $\tau\sigma$ est bien 6.

6. Voir l'exercice 5.

7. Disponibles sur la page web de David Harari.

groupes d'ordre 8 ou 12 (on a plus de travail et plus de classes d'isomorphismes). On peut aussi classifier [8] (à isomorphisme près) les groupes de cardinal $\leqslant 15$ on s'arrête à 15 pour une bonne raison, à savoir que le cardinal 16 est plus délicat et qu'on obtient beaucoup de classes d'isomorphismes (précisément 14). En fait, on peut voir que plus l'ordre du groupe possède de facteurs premiers de multiplicité grande, plus cela donne de la marge et donne lieu à de nombreuses classes d'isomorphismes. Pour une taille de cardinal donnée, l'ordre qui va maximiser ces critères est la puissance de 2. On peut par exemple l'illustrer par le fait que parmi tous les groupes d'ordre $\leqslant 2000$ (à isomorphisme près), $99,2\%$ sont d'ordre [9] $2^{10} = 1024$. En fait, on conjecture que presque tous les groupes finis sont des 2-groupes dans le sens où

$$\lim_{N\to+\infty} \frac{\#\left\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } \leqslant N\right\}}{\#\left\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leqslant N\right\}} = 1$$

et même

$$\lim_{N\to+\infty} \frac{\#\left\{\text{classes d'iso. de 2-groupes } G \text{ de cardinal } 2^{\left\lceil \frac{\log(N)}{\log(2)} \right\rceil}\right\}}{\#\left\{\text{classes d'iso. de groupes } G \text{ de cardinal } \leqslant N\right\}} = 1.$$

Exercice 4 — Groupe symétrique. Soit $\mathfrak{S}_n$ le groupe symétrique sur n lettres.

1. Quel est l'ordre maximal d'un élément de $\mathfrak{S}_3$? de $\mathfrak{S}_4$? de $\mathfrak{S}_5$? de $\mathfrak{S}_n$?
2. Donner le treillis [10] des sous-groupes de $\mathfrak{S}_3$, en précisant à chaque fois lesquels des sous-groupes sont distingués. Répéter l'exercice avec le groupe alterné $\mathfrak{A}_4$.
   Soient G un groupe et $K \subseteq H$ deux sous-groupes de G. On suppose que $K \lhd H$ et que $H \lhd G$. A-t-on $K \lhd G$? Démontrer que si K est caractéristique dans H et que H est caractéristique dans G, alors K est caractéristique dans G.
3. Une *partition d'un entier* n est une suite $0 < \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_r$ d'entiers tels que $\sum_{i=1}^{r} \lambda_i = n$. Montrer que les classes de conjugaison de $\mathfrak{S}_n$ sont en bijection avec les partitions de n.
4. Déterminer le centre de $\mathfrak{S}_n$.

Solution. Je vous renvoie pour des rappels sur le groupe symétrique et l'essentiel de ce qu'il faut connaître au premier chapitre du *Cours d'algèbre* de Daniel Perrin, un grand classique de l'agrégatif ou de l'agrégative !

1. Plusieurs façons de faire : décrire tous les éléments de $\mathfrak{S}_3$: $\mathrm{Id}, (12), (13), (23), (123), (132)$ ou alors en utilisant la décomposition de toute permutation en produit de cycles à supports disjoints dont l'ordre est alors le ppcm des longueurs des cycles [11] ou encore en utilisant le théorème de Lagrange et le fait que $\mathfrak{S}_3$ n'est pas cyclique car non abélien. Bref, on trouve 3 pour chacun des deux 3-cycles. De même, pour $\mathfrak{S}_4$, on trouve 4 atteint pour les six 4-cycles. Pour $\mathfrak{S}_5$, on obtient 6 pour chacun des 20 produits d'une transposition et d'un 3-cycle à supports disjoints. De manière générale, on voit que l'ordre maximal dans $\mathfrak{S}_n$ est donné par

   $$g(n) = \max_{\substack{0<\lambda_1\leqslant\cdots\leqslant\lambda_r \\ \lambda_1+\cdots+\lambda_r=n}} \mathrm{ppcm}(\lambda_1,\ldots,\lambda_r).$$

   On retrouve bien les résultats précédents puisqu'on a les partitions suivantes :

   $$3 = 1{+}1{+}1 = 1{+}2 = 3, \quad 4 = 1{+}1{+}1{+}1 = 2{+}2 = 1{+}3 = 4 \quad \text{et} \quad 5 = 1{+}1{+}1{+}1{+}1 = 1{+}1{+}1{+}2 = 1{+}1{+}3 = 1{+}4 = 2{+}3 = 5.$$

   On obtient par le théorème de Lagrange que $g(n) \mid n!$ et g est croissante. On a par exemple

n	3	4	5	6	7	8	9	10	11	12	13
g(n)	3	4	6	6	12	15	20	30	30	60	60

   Landau a démontré [12] en 1909 l'équivalent

   $$\log g(n) \underset{n\to+\infty}{\sim} \sqrt{n\log(n)}.$$

   ▶ **Compléments . –** C'est aussi un exercice intéressant de les dénombrer le nombre de partitions dont la décomposition en cycle à supports disjoints correspond à une partition $\boldsymbol{\lambda} = (\lambda_1,\ldots,\lambda_r)$ tel que $n = \lambda_1 + \cdots + \lambda_r$ vaut

   $$\frac{n!}{\prod_{j=1}^{n} a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}}$$

8. Voir à nouveau les feuilles de TD de l'an dernier.
9. Voir Besche, Eick et O'Brien, *The groups of order at most 2000*.
10. C'est-à-dire le graphe non orienté dont les sommets sont les sous-groupes de G et où une arête relie deux sous-groupes H_1 et H_2 si, et seulement si, $H_1 \subseteq H_2$ ou $H_2 \subseteq H_1$.
11. Car on vérifie immédiatement qu'un cycle de longueur ℓ est d'ordre ℓ et le fait que les cycles soient à support disjoints entraîne qu'ils commutent.
12. En utilisant des résultats d'arithmétique notamment sur la répartition des nombres premiers. Si l'article vous intéresse (et que vous lisez l'allemand), je peux vous transmettre l'article ! Vous trouverez une version en français ici.

où $a_j(\boldsymbol{\lambda})$ désigne le nombre de λ_k égaux à j. On peut faire pour cela agir G sur lui-même par conjugaison et on montre que le cardinal du stabilisateur de σ est donné par $\prod_{j=1}^{n} a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}$. En effet, pour envoyer σ sur lui-même par conjugaison, on procède cycle par cycle. Le premier cycle de longueur j est envoyé sur un autre cycle de longueur j. On a alors $a_j(\boldsymbol{\lambda})$ choix parmi tous les cycles de longueur j. Ensuite, on a j manières d'envoyer par conjugaison un j-cycle sur un autre j-cycle. Pour le second cycle de longueur j, il reste $a_j(\boldsymbol{\lambda})-1$ choix parmi tous les cycles de longueur j et toujours j manières d'envoyer par conjugaison un j-cycle sur un autre j-cycle. On obtient finalement un facteur $a_j(\boldsymbol{\lambda})! j^{a_j(\boldsymbol{\lambda})}$ et le produit apparaît lorsqu'on parcourt toutes les longueurs de cycles possibles.