Université d'Aix–Marseille
L3 Structures Algébriques.

Examen partiel : Correction

Petits exercices

EXERCICE 1. Soit $x \in X$. On a $|G| = \text{Card(O(x))} \times |\text{G}_\text{x}|$ donc le cardinal d'une orbite divise $|G| = 33$. On a donc $\text{Card(O(x))} \in \{1, 3, 11, 33\}$. D'autre part, la formule des classes nous donne $\text{Card(X)} = \sum_{\omega \in \Omega} \text{Card}(\omega)$ où Ω est l'ensemble des orbites. Il existe donc $a, b, c, d \in \mathbb{N}$ tels que

$$\text{Card(X)} = 19 = 1 \times \text{a} + 3 \times \text{b} + 11 \times \text{c} + 33 \times \text{d}$$

. On a directement $\underline{d = 0}$ car $33 > 19$. On également $c \leq 1$. On distingue donc les deux cas

- $\underline{\text{si c=1}}$: on a $a + 3b = 8$ donc $b \leq 2$. On a donc
$$(a, b) \in \{(2, 2), (5, 1), (8, 0)\}$$
.
- $\underline{\text{si c=0}}$: on a $a + 3b = 19$ donc $b \leq 6$. On a donc
$$(a, b) \in \{(1, 6), (4, 5), (7, 4), (10, 3), (13, 2), (16, 1), (19, 0)\}$$
. Et on a d'autre part $a \neq 19$ car l'action est non-triviale.

On voit que dans tous les cas, $a \geq 1$, donc il y a au moins une orbite de cardinal 1, c'est à dire un point fixe. Les possibilités pour le nombre de points fixes sont : $\boxed{a \in \{1, 2, 4, 5, 7, 8, 10, 13, 16\}}$

EXERCICE 2. *Remarque préliminaire : Lorsqu'on se trouve dans un groupe, et qu'on parle de "produit" de deux éléments, c'est toujours la loi du groupe que l'on considère. Ici, l'ensemble des bijections de $\mathbb{R}$ est un groupe pour la loi de composition $\circ$. Ce n'est PAS un groupe pour la multiplication dans $\mathbb{R}$. Donc lorsqu'on parle d'ordre ou de "produit" de deux éléments dans cet exercice, c'est évidemment la composition qu'il faut utiliser et non pas la multiplication ...*

(1) Soit $a \in \mathbb{R}$. On a
$$\forall x \in \mathbb{R}, \sigma_a^2(a + x) = \sigma_a(\sigma_a(a + x)) = \sigma_a(a - x) = a - (-x) = a + x$$
On a donc $\sigma_a^2 = \text{Id}_\mathbb{R}$ qui est l'élément neutre de l'ensemble des bijections. Donc $\boxed{\sigma_a \text{ est d'ordre 2.}}$ D'autre part on a
$$\forall n \geq 1, \forall x \in \mathbb{R}, \tau_a^n(x) = na + x$$
Donc si $a \neq 0$ on a $\forall \tau_a^n \neq \text{Id}_\mathbb{R}$ donc $\boxed{\text{l'ordre de } \tau_a \text{ est infini}}$. Et si $a = 0$ alors $\tau_0 = \text{Id}$ est d'ordre 1.

(2) Soient $a, b \in \mathbb{R}$. Soit $x \in \mathbb{R}$.
$$\begin{aligned}\sigma_a(\sigma_b(x)) &= \sigma_a(\sigma_b(b + (x - b))) = \sigma_a(b - (x - b)) \\ &= \sigma_a(a + (2b - x - a)) = a - (2b - x - a) = x + (2a - 2b) \\ &= \tau_{2a-2b}(x)\end{aligned}$$
Donc $\boxed{\text{le produit } \sigma_a\sigma_b = \tau_{2a-2b} \text{ est une translation.}}$

(3) Supposons que σ_a et σ_b commutent, alors l'ordre de $\sigma_a\sigma_b$ est fini.
En effet $(\sigma_a\sigma_b)^2 = \sigma_a^2\sigma_b^2 = \text{Id}$. Or si $a \neq b$ on a $\sigma_a\sigma_b = \tau_{2a-2b}$ est d'ordre infini et on aboutit à une contradiction. Donc $\boxed{\text{en général, } \sigma_a \text{ et } \sigma_b \text{ ne commutent pas.}}$ (Mais les deux fonctions commutent dans le cas trivial où $\sigma_a = \sigma_b$.)

EXERCICE 3.

(1) Soit $x \in G$. Supposons que $o(x)$ est pair. Par le théorème de Lagrange, l'ordre d'un élément divise l'ordre du groupe. On a donc $o(x)$ divise $|G|$ et 2 divise $o(x)$ donc 2 divise $|G|$. On a une contradiction puisque $|G|$ est impair. En conclusion, $\boxed{o(x) \text{ est impair.}}$

(2) Soit $x \in G$. D'après la question précédente, on a $o(x) = 2l + 1$ avec $k \in \mathbb{Z}$. On a donc $x^{2l+1} = e$ d'où $x^{2l+2} = x$ et $x^{2l+2} = (x^{l+1})^2$. Donc en posant $y = x^{l+1}$, on en déduit $y^2 = x$. Donc $\boxed{\text{il existe } y \in G \text{ tel que } y^2 = x.}$

(3) Soit x d'ordre k et soit y tel que $y^2 = x$. Soit $m = o(y)$ l'ordre de y.
- On a $x^m = (y^2)^m = (y^m)^2 = e$, donc $\underline{k \text{ divise } m}$.
- D'autre part, on a $y^{2k} = (y^2)^k = x^k = e$. Donc m divise $2k$. Or l'ordre de y est impair et donc $\underline{m \text{ divise } k}$.

On en déduit que $m = k$ c'est à dire, $\boxed{y \text{ est d'ordre } k.}$

Remarque : il ne faut pas oublier de faire les deux étapes. il ne suffit pas de dire que $y^k = e$ pour montrer que l'ordre de y est k ...

(4) Soit x d'ordre $2k + 1$ et y tel que $y^2 = x$. Comme y est également d'ordre $2k + 1$ on a $y = yy^{2k+1} = y^{2k+2} = (y^2)^{k+1} = x^{k+1}$. Donc y est bien de la forme x^m, et m ne dépend que de x donc $\boxed{y \text{ est unique.}}$

Grands Exercices

EXERCICE 4.

(1) Soit G un groupe commutatif. Soit $k \in \mathbb{Z}$ et $x, y \in G$. On a $\Phi_k(xy) = (xy)^k$. Comme G est commutatif, on a $(xy)^k = x^k y^k$. Or $x^k y^k = \Phi(x)\Phi(y)$. Donc $\boxed{\Phi_k \text{ est un morphisme.}}$

Remarque : Cette question peut se montrer en une seule ligne de calcul, mais il faut utiliser l'hypothèse de commutativité au bon endroit. Si vous voulez montrer au correcteur que vous avez bien compris où était la petite subtilité, n'hésitez pas à réécrire "car G est commutatif" au moment où vous l'utilisez. Ca fait une petite différence pour vous, mais une grosse différence dans l'esprit du correcteur.

(2) Soit G un groupe d'ordre n. Soient $x, y \in G$.
- $\Phi_0(xy) = (xy)^0 = e = ee = x^0 y^0 = \Phi_0(x)\Phi_0(y)$
- $\Phi_1(xy) = (xy)^1 = xy = x^1 y^1 = \Phi_1(x)\Phi_1(y)$
- Dans un groupe d'ordre n on a $\forall g \in G, g^n = e$. Donc $\Phi_n(xy) = (xy)^n = e = ee = x^n y^n = \Phi_n(x)\Phi_n(y)$.

On a bien $\boxed{\Phi_0, \Phi_1 \text{ et } \Phi_n \text{ qui sont des morphismes.}}$

(3) On a montré que $\underline{\text{si } G \text{ est commutatif alors } \Phi_2 \text{ est un morphisme.}}$

$\underline{\text{Supposons que } \Phi_2 \text{ est un morphisme.}}$

Soit $x, y \in G$. On a

$$xy = (x^{-1}x)xy(yy^{-1}) = x^{-1}x^2y^2y^{-1} = x^{-1}\Phi_2(x)\Phi_2(y)y^{-1} = x^{-1}\Phi_2(xy)y^{-1} = x^{-1}xyxyy^{-1} = yx$$

On en déduit que $\underline{G \text{ est commutatif.}}$

(4) On a montré que $\underline{\text{si } G \text{ est commutatif alors } \Phi_{-1} \text{ est un morphisme.}}$

$\underline{\text{Supposons que } \Phi_{-1} \text{ est un morphisme.}}$

Soit $x, y \in G$. On a $(xy)^{-1} = \Phi_{-1}(xy) = \Phi_{-1}(x)\Phi_{-1}(y) = x^{-1}y^{-1} = (yx)^{-1}$, donc $xy = yx$.
On en déduit que $\underline{G \text{ est commutatif.}}$

(5) – $\star$ est associative : En effet, pour (a,b,c) , (a',b',c') et (a'',b'',c'') dans U_3, on a :

$$\begin{aligned}((a,b,c)\star(a',b',c'))\star(a'',b'',c'') &= (a+a',b+b,c+c'+b'a)\star(a'',b'',c'')\\ &= (a+a'+a'',b+b'+b'',(c+c'+b'a)+c''+b''(a+a'))\\ &= (a+(a'+a''),b+(b'+b''),c+(c'+c''+b''a')+(b'+b'')a)\\ &= (a,b,c)\star(a'+a'',b'+b'',c'+c''+b''a')\\ &= (a,b,c)\star((a',b',c')\star(a'',b'',c''))\end{aligned}$$

– $(0,0,0)$ est élément neutre. En effet, pour $(a,b,c)\in U_3$ on a :

$$(a,b,c)\star(0,0,0) = (a+0,b+0,c+0+0a) = (a,b,c) = (0,0,0)\star(a,b,c)$$

– tout élément admet un inverse. En effet, pour $(a,b,c)\in U_3$ on a :

$$(a,b,c)\star(-a,-b,ba-c) = (a+(-a),b+(-b),c+(ba-c)+(-b)a) = (0,0,0) = (-a,-b,ba-c)\star(a,b,c)$$

Remarque : le groupe n'est pas commutatif, il faut donc préciser que l'élément neutre est bien neutre à gauche ET à droite, et que l'inverse est bien à gauche ET à droite, même si vous ne réécrivez pas les calculs entièrement.

Remarque2 : Pour trouver l'element neutre ou l'inverse, vous pouvez "résoudre des équations". Mais attention, si vous raisonnez avec des implications, il faut vérifier à la fin que le triplet que vous obtenez à la fin du calcul est effectivement solution

(6) Soit $u=(a,b,c)\in U_3$. Alors $\Phi_3(u) = u\star u\star u = (a,b,c)\star(a+a,b+b,c+c+ba) = a+a+a,b+b+b,c+c+c+ba+ba+ba)$. Or on a $\forall x\in\mathbb{Z}/3\mathbb{Z}$, $x+x+x=0$. On en déduit que $\boxed{\Phi_3(a,b,c)=(0,0,0).}$

(7) Dans le groupe U_3, on a $\boxed{\Phi_3=\Phi_0 \text{ est un morphisme}}$, c'est le morphisme nul.
Or $\boxed{U_3 \text{ n'est pas commutatif}}$. En effet

$$(1,0,0)\star(0,1,0) = (1,1,1) \qquad (0,1,0)\star(1,0,0) = (1,1,0)$$

EXERCICE 5.

(1) Soit d un diviseur de n. Alors on peut écrire $n = d\times q$ avec $q\in\mathbb{N}$.
Alors $\boxed{x^q \text{ est un élément d'ordre } d \text{ dans } G}$. En effet
– D'après le théorème de Lagrange, $(x^q)^d = x^{qd} = x^n = e$ car G est d'ordre n. On en déduit l'ordre de x^q divise d.
– x est d'ordre n donc pour tout k, on a $(x^q)^k = e \Rightarrow n$ divise qk, c'est à dire qd divise qk donc d divise l'ordre de x^q.

(2) G est un groupe commutatif, donc tous les sous-groupes sont normaux. D'après le théorème de Lagrange on a $|G| = |G/H|\times|H|$. D'autre part p divise $|G|$, donc comme p est premier on a (p divise $|H|$) ou (p divise $|G/H|$).

(3) Supposons que p divise l'ordre de $\overline{x}$ dans G/H. On en déduit que si $\overline{x}^k = \overline{e}$ alors p divise k. C'est à dire que si $x^k\in H$ alors p divise k. En posant q l'ordre de x dans G, on a $x^q = e$ et $e\in H$ donc p divise q.
On considère alors le sous-groupe $\langle x\rangle$ qui cyclique et d'ordre divisible par p. En appliquant la question 1. on en déduit qu'$\boxed{\text{il existe un élément } y \text{ d'ordre } p \text{ dans } \langle x\rangle.}$

(4) Montrons le théorème de Cauchy par récurence sur n.
– si $n=1$, le théorème est trivialement vérifié.

– Supposons que pour tout groupe de cardinal inférieur à $n-1$, si p divise le cardinal du groupe alors il y a un élément d'ordre p.
Soit maintenant G d'ordre n et p qui divise n. Soit x un élément de G différent de l'élément neutre. On pose $H = \langle x \rangle$ est un sous-groupe de G non réduit à $\{e\}$, donc G/H est un groupe d'ordre inférieur à $n-1$. Alors d'après la question 2. le nombre p divise $|H|$ ou bien divise $|G/H|$. Si p divise $|H|$ la question 1. nous permet de conclure car H est cyclique. Si p divise $|G/H|$, on peut appliquer l'hypothèse de récurence au groupe G/H pour montrer qu'il existe un élément d'ordre p dans G/H. D'après la question 3. on en déduit qu'il existe un élément d'ordre p dans G.