Université de Bourgogne Année 2020-2021
Licence 2 Octobre

Correction du partiel de structures fondamentales

Rappelons que G est un groupe dont la loi est notée multiplicativement et dont l'élément neutre est noté e.

Exercice 1
1) Soit $x \in G$ un élément d'ordre n et soit $k \in \mathbb{N}^*$ tel que $x^k = e$. Par division euclidienne, il existe $q \in \mathbb{N}$ et $r \in [\![0; n-1]\!]$ tels que $k = nq + r$. On a alors (puisque $x^n = e$ et $x^k = e$)

$$x^r = (x^r)(x^n)^q = x^{r+nq} = x^k = e.$$

Or, par définition de l'ordre, n est le plus petit entier ≥ 1 tel que $x^n = e$. Mais r est un entier positif ou nul tel que $x^r = e$ et $r < n$ donc forcément, $r = 0$ et $k = nq$, ou dit autrement, n divise k.

2) Observons déjà que $(x^2)^n = x^{2n} = (x^n)^2 = e$ donc x^2 est d'ordre fini et d'ordre au plus n. Notons l l'ordre de x^2.
Si n est pair alors il existe $p \in \mathbb{N}^*$ tel que $n = 2p$. On a alors que $(x^2)^p = x^{2p} = x^n = e$. Donc l est au plus égale à $p = n/2$. Mais $(x^2)^l = x^{2l} = e$ donc d'après la définition de l'ordre de x, $2l$ est inférieur ou égale à n donc $l \leq n/2 = p$. On en déduit que $l = p$.
Maintenant, supposons que l est impair. On a que $(x^2)^l = x^{2l} = e$ donc d'après la question **1)**, n divise $2l$. Mais n est impaire donc n divise l. Or on a déjà vu que $1 \leq l \leq n$ donc $l = n$.

Exercice 2
1) Raisonons par récurrence. Pour $n = 0$, $(xy)^0 = e$ et $x^0y^0 = ee = e$ donc $(xy)^0 = x^0y^0$. Maintenant, supposons qu'il existe $n \in \mathbb{N}$ tel que $(xy)^n = x^ny^n$. On a alors que

$$(xy)^{n+1} = (xy)^n(xy) = x^ny^nxy.$$

Ici, la deuxième égalité vient de l'hypothèse de récurrence. Mais G est abélien donc $y^nx = xy^n$ ce qui implique que

$$x^ny^nxy = x^nxy^ny = x^{n+1}y^{n+1}.$$

On a donc bien par récurrence que pour tout $n \in \mathbb{N}$, $(xy)^n = x^ny^n$.

2) On a que $(x^q)^p = (x^p)^q = e$. Donc x^q est d'ordre fini et on note l son ordre. La précédente égalité donne que $l \leq p$. De plus, on a $(x^q)^l = x^{ql} = e$. Donc d'après l'exercice **1** p divise ql. Mais p est premier avec q donc p divise l. On en déduit que $l = p$.
L'ordre de $(xy)^q$ est aussi l car d'après la question **1)** $(xy)^q = x^qy^q = x^q$ car y est d'ordre q.

3) Déjà, observons que $(xy)^{pq} = x^{pq}y^{pq} = (x^p)^q(y^q)^p = e$. Donc xy est d'ordre fini et son ordre, qu'on note k, vérifie $k \leq pq$. Mais on sait que $(xy)^q$ est d'ordre p et puisque $((xy)^q)^k = ((xy)^k)^q = e$, l'exercice **1** implique que p divise k. De la même manière, en inversant les rôles de x et y, on obtient que q divise k. Or, p et q sont premiers entre eux donc pq divise $k \leq pq$, c-à-d $k = pq$.

Exercice 3
Soit $x, y \in G$ tels que $xH \cap yH \neq \varnothing$. Il existe donc un élément z dans cette intersection. Par définition de xH et yH, il existe $b \in H$ et $b' \in H$ tels que $z = xb = yb'$. On en déduit que $x = yb'b^{-1}$. Choisissons maintenant un élément a de xH. Toujours par définition de xH, il existe $c \in H$ tel que $a = xc$. En utilisant l'égalité précédente, on obtient $a = yb'b^{-1}c$. Or, H est un sous-groupe de G et $b, b', c \in H$ donc $b'b^{-1}c$ est aussi dans H. Donc $a = yb'b^{-1}c$ appartient à yH. Puisque a était arbitraire dans xH,

ceci montre que $xH \subset yH$. En inversant les rôles de x et y dans le raisonnement ci-dessus, on obtient aussi que $yH \subset xH$ et donc $xH = yH$.

Exercice 4
Soit H un sous-groupe de G tel que $H \neq G$. En particulier, il existe $x \in G \setminus H$. Notons F le sous-groupe engendré par $G \setminus H$. Rappelons qu'il s'agit d'un sous-groupe de G et que

$$G \setminus H \subset F.$$

On a donc que $G = H \cup F$. Or une union de deux sous-groupes n'est un sous-groupe que si l'un des deux est inclu dans l'autre (cf. TD). Le fait que G est un sous-groupe de G implique donc que $F \subset H$ ou $H \subset F$. Or, on a déjà fixé $x \in G \setminus H \subset F$ donc $F \not\subset H$. On a donc $H \subset F$. Mais vu qu'on savait déjà que $G \setminus H \subset F$, on a forcément $F = G$.

Exercice 5
Rappelons que $k \in \mathbb{N}^*$ et que a est un élément d'ordre k de G. L'objectif est de montrer que

$$H := \{a^n \mid n \in [\![0; k-1]\!]\}$$

est un sous-groupe de G. Déjà, observons que $0 \in [\![0; k-1]\!]$ (puisque $k \geq 1$) donc $a^0 \in H$ et H n'est pas vide. Maintenant, fixons $x, y \in H$. Par définition de H, il existe $n, m \in [\![0; k-1]\!]$ tels que $x = a^n$ et $y = a^m$. Donc $xy = (a^n)(a^m) = a^{n+m}$. Par division euclidienne, il existe $q \in \mathbb{N}$ et $r \in [\![0; k-1]\!]$ tels que $n + m = qk + r$ (il est facile de voir que $q = 0$ si $n + m < k$ et $q = 1$ sinon) ce qui implique que

$$xy = a^{n+m} = a^{qk+r} = (a^k)^q a^r = e^q a^r = a^r,$$

où la quatrième égalité vient du fait que a est d'ordre k. On a donc que $xy = a^r$ avec $r \in [\![0; k-1]\!]$ donc $xy \in H$. De la même manière, $x^{-1} = a^{-n}$ et il existe $q' \in \mathbb{Z}$, $r' \in [\![0; k-1]\!]$ tels que $-n = q'k + r'$ et donc $x^{-1} = a^{q'k+r'} = a^{r'}$, c-à-d $x^{-1} \in H$. Tout ceci montre que H est bien un sous-groupe de G.

Exercice 6
Supposons que $HF = FH$. Déjà (même sans l'hypothèse) HF est non-vide car $e \in H$ et $e \in F$ donc $ee = e \in HF$. Maintenat, fixons $x, y \in HF$. Par définition de cet ensemble, il existe $a_1, a_2 \in H$ et $b_1, b_2 \in F$ tels que $x = a_1 b_1$ et $y = a_2 b_2$. On a alors $xy = a_1 b_1 a_2 b_2$. Mais $b_1 a_2$ est dans FH donc notre hypothèse implique qu'il existe $a_3 \in H$ et $b_3 \in F$ tels que $b_1 a_2 = a_3 b_3$. Donc $xy = a_1 b_1 a_2 b_2 = a_1 a_3 b_3 b_2$. Mais H et F sont des sous-groupes donc $a_1 a_3 \in H$ et $b_3 b_2 \in F$ ce qui implique que $xy \in HF$.
De la même manière, $x^{-1} = (a_1 b_1)^{-1} = b_1^{-1} a_1^{-1}$. Mais F et H sont des sous-groupes donc $b_1^{-1} \in F$ et $a_1^{-1} \in H$ ce qui donne que $x^{-1} \in FH = HF$.
Tout cela implique que HF est un sous-groupe.

Inversement, supposons que HF est un sous-groupe de G. Si $z \in FH$ alors il existe $a \in H$ et $b \in F$ tels que $z = ba$. Puisque H est un sous-groupe, $a^{-1} \in H$ et de la même manière $b^{-1} \in F$. Donc $a^{-1} b^{-1} \in HF$. Mais puisque HF est un sous-groupe, $ba = (a^{-1} b^{-1})^{-1}$ est aussi dans HF. On a donc montrer que $FH \subset HF$. Pour l'autre inclusion, fixons $t \in HF$. Puisque HF est un sous-groupe, $t^{-1} \in HF$. Il existe donc $h \in H$ et $f \in F$ tels que $t^{-1} = hf$. Mais $t = (t^{-1})^{-1} = (hf)^{-1} = f^{-1} h^{-1}$. Avec les mêmes arguments que ci-dessus, on en déduit que $t \in FH$ et donc que $HF \subset FH$.