Université Joseph Fourier	2012-2013
Licence 3	Parcours A

Algèbre

Contrôle continu du 24/09/2012

Les quatre exercices sont indépendants.
Prévoir deux copies distinctes, une pour les exercices 1 et 2, une pour les exercices 3 et 4.
Le barème est donné à titre indicatif. Il sera tenu compte de la présentation et de la rédaction.

Exercice 1 (Le groupe symétrique $\mathcal{S}_n$ est engendré par deux éléments). [Environ 7 à 8 points]

Soit $\mathcal{S}_n$ le groupe symétrique sur $\{1, \dots, n\}$, c'est-à-dire le groupe des bijections de $\{1, \dots, n\}$ sur $\{1, \dots, n\}$. Pour i et j distincts dans $\{1, \dots, n\}$, on note $(i\ j)$ la transposition qui échange i et j. On note $\tau = (1\ 2)$ et γ le cycle $(1\ 2\ \dots n-1\ n)$, défini par $\gamma(x) = x + 1$ pour $1 \leqslant x \leqslant n - 1$ et $\gamma(n) = 1$. Soit H le sous-groupe de $\mathcal{S}_n$ engendré par τ et γ.

1. Montrer que si deux éléments a et b de $\{1, \dots, n\}$ sont congrus modulo n (on rappelle que cela signifie que $a - b \in n\mathbb{Z}$ et on note $a \equiv b\ [n]$), ils sont égaux.
2. Montrer que pour tout $k \in \mathbb{N}^*$ et $x \in \{1, \dots, n\}$, $\gamma^k(x) \equiv x + k\ [n]$ (on pourra raisonner par récurrence sur k).
3. En déduire $\gamma^k(x)$ pour $k \in \{1, \dots, n-1\}$ et $x \in \{1, \dots, n\}$ (on distinguera deux cas suivant la valeur de $x + k$). Que vaut γ^n ?
4. Montrer que pour tout $\sigma \in \mathcal{S}_n$, pour i et j distincts dans $\{1, \dots, n\}$, $\sigma \circ (i\ j) \circ \sigma^{-1} = (\sigma(i)\ \sigma(j))$.
5. Montrer que H contient toutes les transpositions de la forme $(i\ i+1)$ pour $1 \leqslant i \leqslant n-1$ (utiliser les questions précédentes).
6. En déduire que H contient toutes les transpositions de la forme $(1\ i)$ pour $2 \leqslant i \leqslant n$ (on pourra raisonner par récurrence sur i).
7. En déduire que H contient toutes les transpositions, et reconnaître le groupe H.

Exercice 2 (Parties stables finies d'un groupe). [Environ 3 à 4 points]

Soit $(G, \cdot)$ un groupe de neutre 1_G. Soit S une partie finie non-vide de G, stable par $\cdot$.

1. Montrer que pour tout $x \in S$ et $n \in \mathbb{N}^*$, $x^n \in S$.
2. Soit $x \in S$. Montrer qu'il existe $n \in \mathbb{N}^*$ tel que $x^n = 1_G$ et que $x^{-1} \in S$. Indication : montrer que l'application $n \mapsto x^n$ de $\mathbb{N}^*$ dans S ne peut pas être injective.
3. En déduire que S est un sous-groupe de G.

Exercice 3 (Un sous-groupe de $\mathbb{Z}^2$). [Environ 3 à 4 points]

Soit H le sous-groupe de $\mathbb{Z}^2$ engendré par $u = (1, 2)$ et $v = (2, 1)$.

1. Montrer que H est l'ensemble des couples $(a, b) \in \mathbb{Z}^2$ tels que 3 divise $a + b$.
2. Est-ce que H est un sous-groupe monogène de $\mathbb{Z}^2$?

Exercice 4 (Inverses et éléments simplifiables, à gauche et à droite). [Environ 5 à 6 points]

Soient A un ensemble non vide, et $\star : A \times A \to A$ une loi interne associative. Dans les questions 1 à 3, on suppose que $(A, \star)$ possède un élément neutre qu'on notera e_A. Lorsque deux éléments a, b de A vérifient $a \star b = e_A$, on dit que a est l'inverse à gauche de b, et b est l'inverse à droite de a.

1. Soient a, b, c dans A. On suppose que a est un inverse à gauche de b et que c est un inverse à droite de b. Montrer que $a = c$.
2. En déduire que si tous les éléments de A admettent un inverse à droite, cet inverse à droite est aussi un inverse à gauche. Qu'en déduit-on alors pour $(A, \star)$?
3. Dans cette question, on suppose que A est fini et que tout élément de A est simplifiable à gauche, c'est-à-dire que, pour tous a, b, c dans A,

$$a \star b = a \star c \Rightarrow b = c.$$

   Montrer que $(A, \star)$ est un groupe. Indication : on pourra considérer les applications $\tau_a : x \mapsto a \star x$ de A dans A.
4. Dans cette question, on suppose que A est fini et que tout élément de A est simplifiable à gauche et à droite : on a donc aussi, pour tous a, b, c dans A,

$$b \star a = c \star a \Rightarrow b = c,$$

   mais on ne suppose plus l'existence de e_A. Montrer que $(A, \star)$ est un groupe. Indication : on pourra fixer $a \in E$, montrer l'existence d'éléments $e, e' \in A$ tel que $e \star a = a = a \star e'$, et montrer que pour tout $y \in A$, $e \star y = y$ etc..

Remarques sur le contrôle

Exercice 1

1. Question souvent faite correctement, mais pas toujours.

2. Presque tous les étudiants ont fait comme si $\gamma(x) = x + 1$ pour tout $x \in [1, n]$! Dans la preuve par récurrence de la congruence $\gamma^k(x) \equiv x + k\ [n]$, il fallait donc distinguer deux cas pour démontrer la formule pour $k = 1$. Très peu l'ont fait. Par ailleurs, ce n'est pas parce que deux entiers sont congrus modulo n que leurs images par une application le sont !

3. Très peu voient que pour k et x dans $[1, n]$, $\gamma^k(x) = x + k$ ou $x + k - n$ suivant que $2 \leqslant x + k \leqslant n$ ou $n + 1 \leqslant x + k \leqslant 2n$. Il faut préciser qu'on utilise la questions 1, après avoir démontré les inégalités qui permettent de l'utiliser.

4. Pour montrer que $\sigma \circ (i\ j) \circ \sigma^{-1} = (\sigma(i)\ \sigma(j))$, on compare simplement les images d'un élément quelconque x. Il y a trois cas sont à distinguer : si $x = \sigma(i)$, si $x = \sigma(j)$, et si x n'est ni $\sigma(i)$ ni $\sigma(j)$.

5, 6 et 7. Des formules parfois fantaisistes, alors qu'il suffisait d'utiliser la formule vue à la question 4. Noter que le produit de deux transpositions n'est jamais une transposition.

7. Très peu pensent à dire que les transpositions engendrent $\mathcal{S}_n$.

Exercice 2

1. Quand une question très simple du début nécessite une récurrence, il faut la faire proprement.

2. Comme S est fini et $\mathbb{N}^*$ infini, une application de $\mathbb{N}^*$ dans S n'est jamais injective. Attention, une application de $\mathbb{N}^*$ dans S n'a pas de noyau, même si c'est un morphisme pour de $(\mathbb{N}^*, +)$ dans $(S, \cdot)$ puisque $\mathbb{N}^*$ n'est pas un groupe (pour S on ne sait pas encore). Il faut refaire le raisonnement simple consistant à dire que si deux entiers $i < j$ vérifient $x^i = x^j$ alors $x^{j-i} = 1_G$. On a alors trouvé un entier $n \geqslant 1$ tel que $x^n = 1_G$ (cet entier dépend de x). Pour montrer que $x^{-1} = x^{n-1}$ est dans S, il faut traiter à part le cas où $n = 1$.

3. L'hypothèse que S est non vide doit servir. Une partie non-vide de G stable par produit et par inverse est un sous-groupe de G. Si l'on veut montrer que 1_G est dans S à l'aide de la question 2, on doit mentionner que S est non vide, ce qui autorise à prendre un élément dedans.

Exercice 3

1. On a $H = \{mu + nv\ ;\ m \in \mathbb{Z}, n \in Z\}$ parce que $\mathbb{Z}^2$ est commutatif. Pour montrer l'inclusion $A \subset H$ (où $A = \{(a, b) \in \mathbb{Z}^2 : 3 \text{ divise } a + b\}$), il suffit de résoudre un système d'équations approprié.

2. Assez bien traité, mais souvent avec peu de rigueur.

Exercice 4

1. Dans ce genre de question, il est important de préciser les propriétés utilisées (et comment).

2. Dans la question précédente, l'existence de deux inverses était supposée, ce n'est plus le cas ici.

3. Assez bien traité.

4. On peut suivre l'indication (en utilisant la bijection τ_a pour montrer l'existence de e', l'autre bijection pour montrer l'existence de e, puis $e * y = y$ car tout y s'écrit sous la forme $y = a \star z$ avec $z \in A$.) Sinon, on peut aussi remarquer que $e \star a = a$ implique que $d \star e \star a = d \star a$ puis simplifer à droite par a.