Contrôle continu 1

Documents et calculatrices ne sont pas autorisés. Les exercices sont indépendants.

Exercice 1

Énoncer le théorème de Lagrange pour les groupes.

Exercice 2

On note $\mathbb{F}_7 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ le corps $\mathbb{Z}/7\mathbb{Z}$. Le groupe multiplicatif des éléments inversibles de ce corps est $\mathbb{F}_7^\times = \mathbb{F}_7 \setminus \{\overline{0}\}$. On note T le sous-ensemble de $M_3(\mathbb{F}_7)$ formé des matrices triangulaires supérieures inversibles, et I la matrice identité de $M_3(\mathbb{F}_7)$.

1. Montrer que pour tout $\alpha \in \mathbb{F}_7^\times$, $\alpha^6 = \overline{1}$.
2. Montrer que T est un sous-groupe de $GL_3(\mathbb{F}_7)$. Quel est son ordre ?
3. Soit $f : T \to \mathbb{F}_7^\times$ l'application qui à une matrice $A = (a_{i,j})_{1\leq i,j\leq 3}$ associe le coefficient $a_{1,1}$. Montrer que f est un morphisme surjectif de groupes.
4. Soit $K = \mathrm{Ker} f$ et $p : T \to T/K$ la projection canonique. Montrer qu'il existe une application g de l'ensemble quotient T/K dans $\mathbb{F}_7^\times$ telle que $f = g \circ p$.
5. Quel est le nombre d'antécédents d'un élément de $\mathbb{F}_7^\times$ par l'application g ?
6. Quel est l'ordre de K ?
7. Soit $A = (a_{i,j})_{1\leq i,j\leq 3} \in T$. En remarquant que la matrice $B = a_{1,1}^{-1}A$ est dans K, montrer que $A^{6^2\times 7^3} = I$.
8. Pour tout A dans T, on note $\overline{A}$ la classe de A dans T/K. Montrer qu'on peut définir de façon cohérente une loi de groupe sur T/K en posant $\overline{A} \times \overline{B} = \overline{AB}$ pour tous A et B dans T.
9. Soit S le sous-groupe de T formé des matrices de T de déterminant $\overline{1}$ et $p_1 : T \to T/S$ la projection canonique. Existe-t-il une application g_1 de l'ensemble quotient T/S vers $\mathbb{F}_7^\times$ telle que $f = g_1 \circ p_1$?
10. Soit H le sous-groupe de T formé des matrices de T dont tous les coefficients diagonaux sont égaux à $\overline{1}$ et $p_2 : T \to T/H$ la projection canonique. Montrer qu'il existe une application g_2 de l'ensemble quotient T/H vers $\mathbb{F}_7^\times$ telle que $f = g_2 \circ p_2$.
11. Soit $A \in T$. On note $\overline{A} = AK$ sa classe d'équivalence modulo K et $\tilde{A} = AH$ sa classe d'équivalence modulo H. Quels sont les cardinaux de $\overline{A}$ et $\tilde{A}$? Montrer que $\overline{A}$ est la réunion disjointe de classes d'équivalence modulo H.
12. Étant donné $\alpha \in \mathbb{F}_7^\times$, en déduire le cardinal de l'image réciproque $g_2^{-1}(\{\alpha\})$.

Un corrigé

1. Soit $\alpha \in \mathbb{F}_7^\times$. D'après le théorème de Lagrange, l'ordre de α divise l'ordre de $\mathbb{F}_7^\times$ qui est 6, donc $\alpha^6 = \overline{1}$.
2. On a $I \in T$ et $T \subset GL_3(\mathbb{F}_7)$. De plus, le produit de deux matrices triangulaires supérieures et l'inverse d'une matrice triangulaire supérieure sont encore des matrices triangulaires supérieures. Donc T est un sous-groupe de $GL_3(\mathbb{F}_7)$. Choisir une matrice de T revient à choisir indépendamment ses trois coefficients diagonaux dans $\mathbb{F}_7^\times$ (pour assurer l'inversibilité) et ses trois coefficients au-dessus de la diagonale dans $\mathbb{F}_7$. Donc $|T| = 6^3 \times 7^3$.
3. L'application f est bien définie. Quand on multiplie deux matrices triangulaires supérieures, les coefficients diagonaux du produit sont les produits terme à terme des coefficients diagonaux. Donc f est un morphisme de groupes.
   Si $\alpha \in \mathbb{F}_7^\times$, alors $\alpha I \in T$ et $\alpha = f(\alpha I)$. Donc f est surjective.
4. Comme f est un morphisme de groupes, la relation d'équivalence associée à f coïncide avec la relation d'équivalence associée au sous-groupe $K = \mathrm{Ker} f$. Le théorème de factorisation des applications fournit une application injective g de T/K dans $\mathbb{F}_7^\times$ telle que $f = g \circ p$.
5. De plus, g est surjective car f l'est. Ainsi, g est une bijection entre T/K et $\mathbb{F}_7^\times$. Chaque élément de $\mathbb{F}_7^\times$ a donc exactement un antécédent par g.
6. On peut déduire que $|K| = 6^2 \times 7^3$ de la question 2 et de la relation $|T| = |\mathrm{Ker} f| \times |\mathrm{Im} f| = |K| \times |\mathbb{F}_7^\times|$.
   Autre raisonnement plus direct : choisir une matrice de T dans $f^{-1}(\{\alpha\})$ revient à choisir indépendamment ses deux derniers coefficients diagonaux dans $\mathbb{F}_7^\times$ et ses trois coefficients au-dessus de la diagonale dans $\mathbb{F}_7$.
7. Soit $A = (a_{i,j})_{1 \leq i,j \leq 3} \in T$. Soit $B = a_{1,1}^{-1} A$. Alors le coefficient $(1,1)$ de B vaut $a_{1,1}^{-1} a_{1,1} = \overline{1}$. Donc $B \in K$. L'ordre de B divise l'ordre de K. Ainsi,
$$A^{6^2 \times 7^3} (a_{1,1} B)^{6^2 \times 7^3} = (a_{1,1}^6)^{6 \times 7^3} B^{6^2 \times 7^3} = \overline{1} I = I.$$
8. On commence par montrer la cohérence de la définition. Rappelons que la relation d'équivalence associée à K est aussi celle associée à f. Par conséquent, si A' et B' sont des matrices respectivement dans la même classe modulo K que A et B, alors $f(A') = f(A)$ et $f(B') = f(B)$. Comme f est un morphisme de groupes, $f(AB) = f(A)f(B) = f(A')f(B') = f(A'B')$, ainsi $\overline{AB} = \overline{A'B'}$, ce qui montre que $\overline{AB}$ ne dépend que des classes $\overline{A}$ et $\overline{B}$.
   La loi obtenue est interne par construction et hérite des propriétés de la multiplication dans T : elle est associative, $\overline{I}$ est élément neutre et $\overline{A}$ admet comme inverse $\overline{A^{-1}}$. Donc a bien défini une loi de groupe sur T/K.

9. Pour tout $\alpha \in \mathbb{F}_7^\times$, la matrice diagonale de diagonale $(\alpha, \alpha^{-1}, \overline{1})$ est dans S et a pour image α par f. Comme f n'est pas constante sur S, il ne peut pas exister d'application g_1 de T/S vers $\mathbb{F}_7^\times$ telle que $f = g_1 \circ p_1$.
10. Comme H est inclus dans $K = \mathrm{Ker} f$, le morphisme de groupes f est constant égal à $\overline{1}$ sur H donc il est constant plus généralement sur chaque classe modulo H. Donc il existe une application g_2 de l'ensemble quotient T/H vers $\mathbb{F}_7^\times$ telle que $f = g_2 \circ p_2$.
11. D'après le cours, les classes $\overline{A} = AK$ et $\tilde{A} = AH$ ont respectivement même cardinal que K et H, à savoir $6^2 \times 7^3$ et 7^3. Comme $I \in H \subset K$, on a

$$\forall B \in \overline{A}, \quad \{B\} \subset BH \subset BK = \overline{B} = \overline{A}.$$

Donc

$$\overline{A} = \bigcup_{B \in \overline{A}} \{B\} \subset \bigcup_{B \in \overline{A}} BH \subset \bigcup_{B \in \overline{A}} \overline{A} = \overline{A}.$$

Ainsi,

$$\overline{A} = \bigcup_{B \in \overline{A}} BH.$$

Donc A est une union de classes modulo H. Deux classes modulo H étant soit égales soit disjointes, on peut se ramener à une union disjointe de 6^2 classes modulo H (à cause des cardinaux) en supprimant les doublons.

12. Soit $\alpha \in \mathbb{F}_7^\times$. Soit $A \in T$. Alors $g_2(\tilde{A}) = g_2(p_2(A)) = f(A)$. Donc $\tilde{A} \in g_2^{-1}(\{\alpha\})$ si et seulement si $f(A) = \alpha$. Autrement dit, $g_2^{-1}(\{\alpha\})$ est l'ensemble des classes modulo H des matrices de $f^{-1}(\{\alpha\})$. Mais $f^{-1}(\{\alpha\})$ est une classe modulo K. Donc $g_2^{-1}(\{\alpha\})$ a exactement 6^2 éléments (qui sont des classes modulo H).

Remarques sur les copies :

1. Quand on sait que l'ordre d'un élément g dans un groupe $(G, \cdot)$ divise k, on en déduit directement que $g^k = 1_G$ sans qu'il y ait besoin de détailler plus.
2. Faire attention à l'ensemble dans lequel varient les objets. Une expression comme $f(a_{1,1})$ lorsque $A = (a_{i,j})_{1 \leq i,j \leq 3}$ n'a pas de sens.
3. Ne pas supposer implicitement que g existe quand on veut montrer son existence en vérifiant par exemple que f est constante sur chaque classe d'équivalence. L'unicité de g n'était pas demandée ici. Quand on affirme que f est surjective, il faut le prouver. Par ailleurs g est surjective car f l'est (vu en TD).
4. Comme f est un morphisme de groupes, la relation d'équivalence associée à $\mathrm{Ker} f$ est aussi la relation d'équivalence associée à f (vu en TD). Il faut le dire explicitement !
5. Beaucoup de réponses délirantes sur un dénombrement pourtant facile pour trouver le cardinal de T ou de K.