Contrôle continu 1

Question de cours : soient G un groupe et H un sous-groupe distingué de G. Montrer qu'on peut munir G/H d'une loi interne de sorte que la projection canonique $p : G \to G/H$ soit un morphisme de groupes.

I. Démonstration du théorème de Cauchy dans le cas d'un groupe abélien

Soit G un groupe abélien fini d'ordre $n \geq 2$. Soit p un diviseur premier de n. Le but de cette partie est de montrer que G possède au moins un élément d'ordre p.

Pour cela, on note $g_1, \ldots, g_n$ les éléments de G, et m le PPCM des ordres des éléments de G. Pour tout entier relatif a, on note $\overline{a}$ la classe de a dans $\mathbb{Z}/m\mathbb{Z}$.

1. Montrer qu'on définit de façon cohérente une application $f : (\mathbb{Z}/m\mathbb{Z})^n \to G$ par
$$\forall(\overline{a_1}, \ldots, \overline{a_n}) \in (\mathbb{Z}/m\mathbb{Z})^n, \quad f(\overline{a_1}, \ldots, \overline{a_n}) = g_1^{a_1} \cdots g_n^{a_n}.$$
2. Montrer que l'application f ainsi définie est un morphisme de groupes.
3. Montrer que f est surjective.
4. En déduire que $m^n = n|\mathrm{Ker} f|$.
5. En déduire que p divise m.
6. En déduire que G possède au moins un élément dont l'ordre est multiple de p.
7. En déduire que G possède au moins un élément d'ordre p.

II. Décomposition d'un groupe abélien fini

Soit G un groupe abélien fini d'ordre $n \geq 2$. Notons $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ la décomposition de n en facteurs premiers : $p_1, \ldots, p_r$ sont des nombres premiers deux-à-deux distincts et $\alpha_1, \ldots, \alpha_r$ sont des entiers strictement positifs. Pour tout $i \in [\![1, r]\!]$, on note q_i l'entier $n/p_i^{\alpha_i}$ et $H_i = \{x \in G : x^{p_i^{\alpha_i}} = 1_G\}$. Soit $\Phi : H_1 \times \cdots \times H_r \to G$ définie par
$$\forall(x_1, \ldots, x_r) \in H_1 \times \cdots \times H_r, \quad \Phi(x_1, \ldots, x_r) = x_1 \cdots x_r.$$

1. Si $x \in H_i$, quelles sont les valeurs possibles pour l'ordre de x ?
2. Montrer que H_i est un sous-groupe de G. Qu'en déduit-on sur $|H_i|$?
3. Montrer que $|H_i|$ divise $p_i^{\alpha_i}$ (utiliser le résultat de la partie I).
4. Montrer que Φ est un morphisme de groupes.
5. Montrer que Φ est surjective. Indication : le PGCD de $q_1, \ldots, q_r$ vaut 1, donc il existe $(a_1, \ldots, a_r) \in \mathbb{Z}^r$ tel que $a_1 q_1 + \cdots + a_r q_r = 1$.
6. Montrer que Φ est injective. Indication : prendre $(x_1, \ldots, x_r) \in \mathrm{Ker}\, \Phi$, et regarder l'ordre des éléments $x_i^{-1} = x_1 \cdots x_{i-1} x_{i+1} \cdots x_r$.
7. Ainsi, Φ est un isomorphisme de groupes. Montrer finalement que $|H_i| = p_i^{\alpha_i}$.

Première partie

1. Pour tout $g \in G$ et $a \in \mathbb{Z}$ l'élement g^a ne dépend que de la classe de a dans $\mathbb{Z}/m\mathbb{Z}$. En effet, si a et a' sont deux entiers ayant même classe dans $\mathbb{Z}/m\mathbb{Z}$, alors $a' - a$ est multiple de m qui est multiple de l'ordre de g, donc $g^{a'-a} = 1_G$ d'où $g^{a'} = g^a$. Ainsi, pour tout $(a_1, \dots, a_n) \in \mathbb{Z}$, le produit $g_1^{a_1} \cdots g_n^{a_n}$ ne dépend que des classes de $a_1, \dots, a_n$ dans $\mathbb{Z}/m\mathbb{Z}$.
2. Quels que soient $(\overline{a_1}, \dots, \overline{a_n})$ et $(\overline{b_1}, \dots, \overline{b_n}) \in (\mathbb{Z}/m\mathbb{Z})^n$,
$$\begin{aligned} f\big((\overline{a_1}, \dots, \overline{a_n}) + (\overline{b_1}, \dots, \overline{b_n})\big) &= f\big((\overline{a_1 + b_1}, \dots, \overline{a_n + b_n})\big) \\ &= g_1^{a_1+b_1} \cdots g_n^{a_n+b_n} \\ &= g_1^{a_1} \cdots g_n^{a_n} g_1^{b_1} \cdots g_n^{b_n} \text{ car } G \text{ est abélien} \\ &= f\big((\overline{a_1}, \dots, \overline{a_n})\big) f\big(\overline{b_1}, \dots, \overline{b_n})\big). \end{aligned}$$
   Donc f est un morphisme de groupes.
3. Pour tout $i \in [\![1, n]\!]$, $g_i = f(\overline{0}, \dots, \overline{0}, \overline{1}, \overline{0}, \dots, \overline{0})$, où le $\overline{1}$ est sur la i-ième composante. Donc $G \subset \mathrm{Im} f$, ce qui montre la surjectivité de f.
4. Le théorème de factorisation des morphismes de groupes assure que le groupe quotient $(\mathbb{Z}/m\mathbb{Z})^n/\mathrm{Ker} f$ est isomorphe à $\mathrm{Im} f = G$. En particulier, $m^n/|\mathrm{Ker} f| = [(\mathbb{Z}/m\mathbb{Z})^n : \mathrm{Ker} f] = |G| = n$, donc $m^n = n|\mathrm{Ker} f|$.
5. Comme p divise n qui divise m^n d'après la question précédente, p divise m^n. Comme p est premier, p divise m.
6. Comme m est le PPCM des ordres des éléments de G, et comme p apparaît dans la décomposition en facteurs premiers de m, il existe $g \in G$ tel que p apparaît dans la décomposition en facteurs premiers de l'ordre de g. Cet ordre $o(g)$ est donc multiple de p.
7. Posons $o(g) = pq$ avec $q \in \mathbb{Z}$. Alors g^q est d'ordre $o(g)/(o(g) \wedge q) = p$.

Deuxième partie

1. Si $x \in H_i$, alors $x^{p_i^{\alpha_i}} = 1_G$ donc l'ordre de x divise $p_i^{\alpha_i}$, donc l'ordre de x est une puissance de p_i comprise entre 1 et $p_i^{\alpha_i}$.
2. Comme G est abélien, l'application $f_i : x \mapsto x^{p_i^{\alpha_i}}$ est un morphisme de groupes. Comme H_i est le noyau de f_i, H_i est un sous-groupe de G. D'après le théorème de Lagrange, $|H_i|$ divise $|G|$.
3. Si H_i contient un élément d'ordre p premier, alors $p = p_i$. D'après la première partie, p_i est donc le seul nombre premier pouvant diviser $|H_i|$. Mais $|H_i|$ divise $|G| = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, donc $|H_i| = p_i^{\beta_i}$ avec $\beta_i \in [\![0, \alpha_i]\!]$.
4. Soient $(x_1, \dots, x_r)$ et $(y_1, \dots, y_r)$ dans $H_1 \times \cdots \times H_r$. Comme G est abélien,
$$\begin{aligned} \Phi((x_1, \dots, x_r)(y_1, \dots, y_r)) &= \Phi((x_1 y_1, \dots, x_r y_r)) = (x_1 y_1) \cdots (x_r y_r) \\ &= (x_1 \cdots x_r)(y_1 \cdots y_r) = \Phi(x_1, \dots, x_r)\Phi(y_1, \dots, y_r). \end{aligned}$$

Donc Φ est un morphisme de groupes.

5. Comme $q_1, \dots, q_r$ n'ont pas de diviseur premier commun, leur PGCD vaut 1, donc il existe $(a_1, \dots, a_r) \in \mathbb{Z}^r$ tel que $a_1 q_1 + \cdots + a_r q_r = 1$.
   Soit $y \in G$. Alors $y = y^{a_1 q_1} \cdots y^{a_r q_r}$. Mais pour tout $i \in [\![1, r]\!]$, $y^{a_i q_i} \in H_i$ puisque $(y^{a_i q_i})^{p_i^{\alpha_i}} = y^{a_i n} = (y^n)^{a_i} = 1_G$. Donc $y = \Phi((y^{a_1 q_1}, \dots, y^{a_r q_r})) \in \mathrm{Im}\Phi$, ce qui montre la surjectivité de Φ.
6. Soit $(x_1, \dots, x_r) \in \mathrm{Ker}\ \Phi$. Alors $x_1 \cdots x_r = 1_G$. Pour tout $i \in [\![1, r]\!]$, l'ordre de x_i^{-1}, égal à celui de x_i, divise $p_i^{\alpha_i}$ car $x_i \in H_i$. Mais $x_i^{-1} = x_1 \cdots x_{i-1} x_{i+1} \cdots x_r$. Comme les x_j pour $j \neq i$ commutent, $o(x_i^{-1})$ divise le produit des $o(x_j)$ pour $j \neq i$, qui divise q_i. Ainsi, $o(x_i) = 1$, d'où $x_i = 1_G$. Le noyau de Φ est réduit à $(\overline{1}, \dots, \overline{1})$, ce qui montre l'injectivité de Φ.
7. Comme Φ est un isomorphisme de groupes,

$$p_1^{\alpha_1} \cdots p_r^{\alpha_r} = |G| = |H_1 \cdots H_r| = p_1^{\beta_1} \cdots p_r^{\beta_r}.$$

   Par unicité de la décomposition de n en facteurs premiers, on a $\alpha_i = \beta_i$ pour tout $i \in [\![1, r]\!]$ d'où $|H_i| = p_i^{\alpha_i}$.