Exercice

Soient G_1 et G_2 deux groupes, H_1 un sous-groupe distingué de G_1 et H_2 un sous-groupe distingué de G_2. On note f l'application de $G_1 \times G_2$ dans $G_1/H_1 \times G_2/H_2$ définie par $f(x_1, x_2) = (x_1H_1, x_2H_2)$.

1. Montrer que f est un morphisme de groupes.
2. Déterminer l'image et le noyau de f.
3. En déduire que $H_1 \times H_2$ est un sous-groupe distingué de $G_1 \times G_2$ et en déduire un isomorphisme de groupes entre $(G_1 \times G_2)/(H_1 \times H_2)$ et un groupe qu'on précisera.

Problème

On fixe un nombre premier p et un entier $\alpha \geq 2$. On admet que le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Le but du problème est d'en déduire la structure du groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

Pour tout entier x, on note $\dot{x}$ la classe de x dans $\mathbb{Z}/p\mathbb{Z}$ et $\overline{x}$ la classe de x dans $\mathbb{Z}/p^\alpha\mathbb{Z}$.

1. **Cas où $p = 2$**
   (a) Déterminer $(\mathbb{Z}/4\mathbb{Z})^\times$. Ce groupe est-il cyclique ?
   (b) Montrer que $\overline{-1}$ et $\overline{5}$ sont dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
   (c) Quel est l'ordre de $\overline{-1}$ dans le groupe multiplicatif $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$?
   (d) Montrer par récurrence que pour tout $k \in \mathbb{N}$, il existe un entier λ_k **impair** tel que $5^{2^k} = 1 + \lambda_k 2^{k+2}$.
   (e) En déduire l'ordre de $\overline{5}$ dans le groupe multiplicatif $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.
   (f) Soit $\psi : \mathbb{Z}^2 \to (\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ le morphisme de groupes défini par $\psi(a, b) = \overline{-1}^a\overline{5}^b$. Montrer que Ker $\psi = 2\mathbb{Z} \times 2^{\alpha-2}\mathbb{Z}$ et déterminer Im ψ.
   Indication : montrer que pour tout $b \in \mathbb{Z}$, $5^b \not\equiv -1 \mod 2^\alpha$.
   (g) En déduire que $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$.
2. **Cas où p est impair**
   On choisit un entier g_p tel que $\dot{g_p}$ est d'ordre $p-1$ dans le groupe multiplicatif $(\mathbb{Z}/p\mathbb{Z})^\times$, grâce au fait que ce groupe est cyclique d'ordre $p-1$.
   (a) Montrer que $\overline{g_p}$ appartient au groupe multiplicatif $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ et que son ordre dans ce groupe est un multiple de $p-1$.
   (b) Montrer que $\overline{1+p} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.
   (c) Montrer par récurrence que pour tout $k \in \mathbb{N}$, il existe un entier λ_k tel que $\lambda_k \equiv 1 \mod p$ et $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$.
   Indication : $\binom{p}{1} = p$ et $\binom{p}{2} = \frac{p(p-1)}{2}$ est multiple de p.
   (d) En déduire que l'ordre de $\overline{1+p}$ dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est $p^{\alpha-1}$.
   (e) Montrer que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ admet un élément d'ordre $p^{\alpha-1}(p-1)$, et en déduire que $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times \simeq \mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Un corrigé

Exercice

1. Soient (x_1, x_2) et (y_1, y_2) dans $G_1 \times G_2$. Par définition de la multiplication dans un groupe produit et dans un groupe quotient,

$$\begin{aligned} f\big((x_1, x_2) \times (y_1, y_2)\big) = f((x_1y_1, x_2y_2)) &= (x_1y_1H_1, x_2y_2H_2) \\ &= (x_1H_1, x_2H_2) \times (y_1H_1, y_2H_2) \\ &= f((x_1, x_2)) \times f((y_1, y_2)). \end{aligned}$$

   Donc f est un morphisme de groupes.

2. Par définition de G_1/H_1 et G_2/H_2, tout élément de $G_1/H_1 \times G_2/H_2$ est de la forme (x_1H_1, x_2H_2) avec $(x_1, x_2) \in G_1 \times G_2$. Donc f est surjective.
   Pour tout $(x_1, x_2) \in G_1 \times G_2$,

$$(x_1, x_2) \in \text{Ker } f \iff (x_1H_1, x_2H_2) = (H_1, H_2) \iff (x_1 \in H_1 \text{ et } x_2 \in H_2).$$

   Donc $\text{Ker} f = H_1 \times H_2$.

3. Comme $H_1 \times H_2$ est le noyau d'un morphisme issu de $G_1 \times G_2$, c'est un sous-groupe distingué de $G_1 \times G_2$. Le théorème de factorisation des morphismes de groupes fournit donc un isomorphisme de groupes $\overline{f}$ de $(G_1 \times G_2)/(H_1 \times H_2) = (G_1 \times G_2)/\text{Ker } f$ vers $\text{Im} f = (G_1/H_1 \times G_2/H_2)$ tel que $f = \overline{f} \circ p$, où p est la projection canonique de $G_1 \times G_2$ sur $(G_1 \times G_2)/(H_1 \times H_2)$.

Problème

1. (a) Le groupe $(\mathbb{Z}/4\mathbb{Z})^\times$ a deux éléments : les classes de 1 (élément neutre) et de 3. Il est donc cyclique engendré par la classe de 3.

   (b) Comme -1 et 5 sont impairs, ils sont premiers avec 2^α. Donc $\overline{-1}$ et $\overline{5}$ sont dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$.

   (c) On a $\overline{-1} \neq \overline{1}$ puisque 2^α ne divise pas $2 = 1 - (-1)$, car $\alpha \geq 2$. Or $\overline{-1}^2 = \overline{1}$ Donc l'ordre de $\overline{-1}$ dans le groupe multiplicatif $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ est 2.

   (d) On a $5^{2^0} = 5^1 = 1 + \lambda_0 2^2$ avec $\lambda_0 = 1$.
   Soit $k \in \mathbb{N}$. Supposons que $5^{2^k} = 1 + \lambda_k 2^{k+2}$ avec λ_k entier impair. Alors

$$5^{2^{k+1}} = (1 + \lambda_k 2^{k+2})^2 = 1 + \lambda_k 2^{k+3} + \lambda_k^2 2^{2k+4} = 1 + \lambda_{k+1} 2^{k+3},$$

   avec $\lambda_{k+1} = \lambda_k + \lambda_k^2 2^{k+1}$ impair.
   Par récurrence, la propriété est vraie pour tout $n \in \mathbb{N}$.

(e) D'après la question précédente, $\overline{5}^{2^{\alpha-2}} = \overline{1}$. L'ordre de $\overline{5}$ dans le groupe multiplicatif $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ divise $2^{\alpha-2}$. Pour voir que c'est $2^{\alpha-2}$, il suffit de montrer qu'il ne divise pas $2^{\alpha-3}$ si $\alpha \geq 3$.
Si $\alpha \geq 3$, alors $\lambda_{\alpha-3} = 1 + 2\mu$ avec $\mu \in \mathbb{Z}$ et $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + \mu 2^\alpha$, donc $\overline{5}^{2^{\alpha-3}} = \overline{1 + 2^{\alpha-1}} \neq \overline{1}$, d'où le résultat.

(f) Pour tout $b \in \mathbb{Z}$, $5^b \equiv 1 \not\equiv -1 \mod 4$. *A fortriori* $5^b \not\equiv -1 \mod 2^\alpha$. Donc $\overline{5}^b \neq \overline{-1}$. Pour tout $(a, b) \in \mathbb{Z}^2$, comme $\overline{-1}^a = \pm\overline{1}$, on a donc

$$\begin{aligned} \psi(a,b) = \overline{1} &\iff \overline{5}^b = \overline{-1}^a \\ &\iff \left(\overline{-1}^a = \overline{1} \text{ et } \overline{5}^b = \overline{1} \right) \\ &\iff \left(2|a \text{ et } 2^{\alpha-2}|b \right). \end{aligned}$$

Ainsi, $\mathrm{Ker}\ \psi = 2\mathbb{Z} \times 2^{\alpha-2}\mathbb{Z}$.

Par ailleurs, $\mathrm{Im}\ \psi$ est un sous-groupe de $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ contenant le sous-groupe engendré par $\overline{5}$, strictement puisqu'il contient $\overline{-1}$. Son ordre divise donc $|(\mathbb{Z}/2^\alpha\mathbb{Z})^\times| = 2^{\alpha-1}$ et est strictement supérieur à l'ordre de $\overline{5}$, qui est $2^{\alpha-2}$. Ainsi, $\mathrm{Im}\ \psi$ est d'ordre $2^{\alpha-1}$, donc est $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$ tout entier.

(g) D'après le théorème de factorisation des morphismes de groupes, $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times = \mathrm{Im}\psi$ est isomorphe à $\mathbb{Z}^2/\mathrm{Ker}\psi = \mathbb{Z}^2/(2\mathbb{Z} \times 2^{\alpha-2}\mathbb{Z})$, donc à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-2}\mathbb{Z}$ d'après l'exercice précédent.

2. (a) Comme g_p est premier avec p, il est premier avec p^α, donc $\overline{g_p} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Notons m l'ordre de $\overline{g_p}$ dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. Comme $\overline{g_p}^m = 1$, l'entier g_p^m est congru à 1 modulo p^α donc modulo p, i.e. $\dot{g_p}^m = \dot{1}$. Donc m est multiple de l'ordre de $\dot{g_p}$ dans le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$, qui est $p - 1$.

(b) Comme $1 + p$ n'est pas multiple du nombre premier p, il est premier avec p^α. Donc $\overline{1+p} \in (\mathbb{Z}/p^\alpha\mathbb{Z})^\times$.

(c) $(1+p)^{p^0} = (1+p)^1 = 1 + \lambda_0 p$ avec $\lambda_0 = 1 \equiv 1 \mod p$.
Soit $k \in \mathbb{N}$. Supposons que $(1+p)^{p^k} = 1 + \lambda_k p^{k+1}$ avec $\lambda_k \equiv 1 \mod p$. Alors

$$\begin{aligned} (1+p)^{p^{k+1}} &= (1 + \lambda_k p^{k+1})^p = \sum_{i=0}^{p} \binom{p}{i} (\lambda_k p^{k+1})^i \\ &= 1 + p\lambda_k p^{k+1} + \frac{p(p-1)}{2}(\lambda_k p^{k+1})^2 + \sum_{i=3}^{p} \binom{p}{i} (\lambda_k p^{k+1})^i. \end{aligned}$$

Donc $(1+p)^{p^{k+1}} = 1 + \lambda_{k+1} p^{k+2}$ avec

$$\lambda_{k+1} = \lambda_k + \frac{p(p-1)}{2}\lambda_k^2 p^k + \sum_{i=3}^{p} \binom{p}{i} \lambda_k^i p^{(i-1)k+i-2} \equiv \lambda_k \equiv 1 \mod p.$$

Par récurrence, la propriété est donc vraie pour tout $k \in \mathbb{N}$.

(d) D'après la question précédente, $\lambda_{\alpha-2} = 1 + p\mu$ avec $\mu \in \mathbb{N}$ et

$$(1+p)^{p^{\alpha-2}} = 1 + p^{\alpha-1} + \mu p^\alpha \equiv 1 + p^{\alpha-1} \mod p^\alpha,$$
$$(1+p)^{p^{\alpha-1}} = 1 + \lambda_{\alpha-1} p^\alpha \equiv 1 \mod p^\alpha.$$

Donc

$$\overline{1+p}^{p^{\alpha-2}} = \overline{1+p^{\alpha-1}} \neq \overline{1} \text{ et } \overline{1+p}^{p^{\alpha-1}} = \overline{1}.$$

L'ordre de $\overline{1+p}$ dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ divise $p^{\alpha-1}$ mais ne divise pas $p^{\alpha-2}$, il vaut donc $p^{\alpha-1}$.

(e) Notons q l'entier $m/(p-1)$. Dans le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$, $\overline{g_p}$ est d'ordre m donc $\overline{g_p}^q$ est d'ordre $m/(m \wedge q) = m/q = p-1$. Or $\overline{1+p}$ est d'ordre p^α. Comme ces éléments commutent et sont d'ordre premiers entre eux, leur produit est d'ordre $p^\alpha(p-1)$. Comme le groupe $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$ est d'ordre $p^\alpha(p-1)$, il est donc cyclique et isomorphe à $\mathbb{Z}/p^{\alpha-1}(p-1)\mathbb{Z}$.

Remarques sur les copies

Si le groupe n'est pas supposé abélien, la notation + pour la loi est à proscrire.
Ne pas redémontrer les résultats du cours, sauf si c'est demandé. Exemples : si $H \triangleleft G$, alors G/H possède une structure de groupe telle que la projection canonique de G sur G/H est un morphisme de groupes ; pour que la classe d'un entier k soit inversible dans l'anneau $\mathbb{Z}/n\mathbb{Z}$, il faut et il suffit que $k \wedge n = 1$.
L'expression logique $P \implies Q$ ne signifie pas que P et Q soient vraies. Il faut savoir si l'on fait des déductions, si l'on procède par implications, si l'on procède par équivalences.
Des implications dans un seul sens ne suffisent pas à démontrer une égalité d'ensembles.
Confusion entre les entiers et leurs classes modulo 2^α. On prend le PGCD d'entiers relatifs et non de classes.
Pour voir que $\overline{-1}$ est dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, il suffit de dire que -1 est premier avec 2^α (ses seuls diviseurs sont -1 et 1). Se ramener à $2^\alpha - 1$ complique inutilement les choses.
Pour dire que $\overline{-1}$ est d'ordre 2 dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, il faut aussi penser à dire que $\overline{-1} \neq \overline{1}$, ce qui requiert l'hypothèse $\alpha \geq 2$.
Les récurrences doivent être rédigées correctement lorsqu'elles constituent la principale difficulté. Le pas de récurrence commence par « Soit $k \in \mathbb{N}$ tel que la propriété est vraie au rang k », avant d'en déduire la propriété au rang $k+1$.
$5^{2^{k+1}} = 5^{2^k \times 2}$ est égal à $(5^{2^k})^2$ et non à $5^{2^k} \times 5^2$...
Des raisonnements faux en arithmétique, ou sur l'ordre d'un élément. Pour dire que $\overline{5}$ est d'ordre $2^{\alpha-2}$ dans $(\mathbb{Z}/2^\alpha\mathbb{Z})^\times$, il faut non seulement dire que $\overline{5}^{2^{\alpha-2}} = \overline{1}$ mais aussi vérifier que si $\alpha \geq 3$, alors $\overline{5}^{2^{\alpha-3}} \neq \overline{1}$; ainsi l'ordre de $\overline{5}$ divise $2^{\alpha-2}$ mais pas $2^{\alpha-3}$.
Le groupe $(\mathbb{Z}/p\mathbb{Z})^\times$ n'est pas inclus dans $(\mathbb{Z}/p^\alpha\mathbb{Z})^\times$. On peut trouver un morphisme injectif du premier dans le second, mais cela demande une preuve.