Groupes abéliens finis

I.1) $\cdot\ xx^{-1} = e \in H$ donc xRx R est réflexive.

$\cdot\ xy^{-1} \in H \Rightarrow (xy^{-1})^{-1} \in H$
$xy^{-1} \in H \Rightarrow yx^{-1} \in H$ $\quad xRy \Rightarrow yRx$ R est symétrique.

$-\ xy^{-1} \in H \quad yz^{-1} \in H \Rightarrow xy^{-1}yz^{-1} \in H$
$xy^{-1} \in H \quad yz^{-1} \in H \Rightarrow xz^{-1} \in H$ $\quad xRy$ et $yRz \Rightarrow xRz$ R est transitive.

R est une relation d'équivalence (On aura compris que $xRy \overset{\text{def}}{\Leftrightarrow} xy^{-1} \in H$)

G/R l'ensemble des classe d'équivalence est donc une partition de G donc $|G| = \sum_{a \in G/R} |a|$ (1)

or classe $(y) = Hy = \{hy, h \in H\}$
Dans un groupe tout élément est régulier donc $h \to hy$ est est injective et $|\text{classe}(y)| = |H|$ (2)

Finalement, d'après (1) et (2) :

$$|G| = |H| \times |G/R|$$

et par conséquent $|H|$ divise $|G|$

I.2) $\langle a \rangle$ doit contenir $\{a^k, k \in \mathbb{N}\}$, or G est fini il existe donc $i < j$ $a^i = a^j$, sont après simplification puisque tout élément est régulier $a^{j-i} = e$.
Donc $n = \min\{p \in \mathbb{N}^*, a^p = e\}$ est bien défini
Montrons que $H = \{e, \ldots, a^{n-1}\}$ est un sous-groupe de G
D'après ce qui a été dit au début tout sous-groupe contenant a doit contenir H, on aura donc $H = \langle a \rangle$

- $H \neq \emptyset$ car $e \in H$
- $\forall x = a^k \in H$ $x^{-1} \in H$ car si $x = e$ $x^{-1} = e$ et si $x = a^k$ $1 \leq k \leq n-1$ alors $x^{-1} = x^{n-k} \in H$
- $\forall (x, y) \in H$ $xy \in H$ car $x = a^k$ $y = a^l$ $xy = a^{k+l} = \begin{cases} a^{k+l} & \text{si } k+l \leq n-1 \\ a^{k+l-n} & \text{si } k+l \geq n \end{cases}$

donc $xy \in H$.

I.3) + On vient de voir que l'ordre n de a est tel que $\langle a \rangle = \{e, \dots, a^{n-1}\}$. Or d'après la question I.1) $n = |\langle a \rangle|$ divise $|G|$. Donc l'ordre de a divise $|G|$

+ On suppose a d'ordre n et d diviseur de n. Soit $m = \frac{n}{d}$ dans $\mathbb{N}$ et $b = a^m$.
Or a bien $b^d = a^n = e$ et pour $1 \leq k < d$ $b^k \neq e$ car $b^k = a^{km}$ avec $1 \leq km < n$. Donc b est d'ordre d

II.1) Considérons $\varphi : H \times K \to G = H \oplus K$, $(x,y) \mapsto x+y$.

φ est défini, surjectif ; la structure de groupe commutatif de G garantit $\varphi((x,y)+(x',y')) = \varphi((x,y)) + \varphi((x',y'))$, donc φ est un morphisme.
Soit $(x,y) \in H \times K$ tel que $\varphi((x,y)) = 0$. On a $x+y=0$ donc $x = -y$ et $x \in H \cap K$, donc $x=0$ puis $y=0$.
$\ker \varphi = \{(0,0)\}$, donc φ est injectif.
Finalement φ est bien un isomorphisme de $H \times K$ sur G et φ^{-1} un isomorphisme de G sur $H \times K$

De plus si H' est isomorphe à H via $\varphi_H : H \to H'$ et K' isomorphe à K via $\varphi_K : K \to K'$, on vérifie aisément que $\Theta : H \times K \to H', K'$, $(x,y) \mapsto (\varphi_H(x), \varphi_K(y))$ est un isomorphisme de $H \times K$ sur $H' \times K'$

Par composition $\Theta \circ \varphi^{-1}$ est un isomorphisme de G sur $H' \times K'$

II.2) Soit x dans $H \cap K$, alors $m.x = 0$ et $n.x = 0$.

m et n sont premiers entre eux, d'après un résultat de Bézout il existe (u,v) dans $\mathbb{Z}^2$ tel que $u.m + v.n = 1$.

On en déduit $x = 1.x = u.(m.x) + v.(n.x) = u.0 + v.0 = 0$.

$\ker \varphi = \{(0,0)\}$ donc φ est injectif. (En effet $\varphi : H \times K \to H + K$, $(x,y) \mapsto x+y$ donc $\ker \varphi = \{(x,-x),\ x \in H \cap K\}$)

φ est surjectif par définition donc φ est un isomorphisme de $H \times K$ sur $H * K$.

II.3) Soit $H = \{n.\bar{x},\ \bar{x} \in \mathbb{Z}/n\mathbb{Z}\}$ $H = \{(nx).\bar{1},\ x \in \mathbb{Z}\}$

$H = \{x.(n.\bar{1}),\ x \in \mathbb{Z}\}$ $H = \langle n.\bar{1} \rangle$.

Or $\bar{1}$ est d'ordre mn, donc d'après I.3 $n.\bar{1}$ est d'ordre m. Par conséquent $H \simeq \mathbb{Z}/m\mathbb{Z}$, de même $K = \langle m.\bar{1} \rangle$ est d'ordre n et $K \simeq \mathbb{Z}/n\mathbb{Z}$

D'après la question précédente $H+K$ est isomorphe à $H \times K$ et en particulier est de cardinal mn.

Puisque $H+K \subset \mathbb{Z}/nm\mathbb{Z}$ qui est d'ordre mn on a donc $H+K = \mathbb{Z}/nm\mathbb{Z}$. On en déduit (par transitivité comme en II.1) que les groupes $\mathbb{Z}/nm\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ sont isomorphes.

II.4) Par définition l'ordre de x divise d ssi $d.x = 0$.

De plus $G_d = \ker f_d$ où $f_d : G \to G$, $x \mapsto d.x$ est un morphisme. Donc G_d est un sous-groupe de G.

II.5) L'existence d'un isomorphisme entre G_{nm} et $G_n \times G_m$ et $G_n + G_m$ se prouve comme en II-2), car on n'utilisait que la notion d'ordre d'un élément.

Il reste à prouver $G = G_n + G_m$. Ici nous ne disposons plus de l'argument de cardinal

Néanmoins, puisque m et n sont premiers entre eux il existe (u, v) dans $\mathbb{Z}^2$ tel que $1 = u.m + vn$

Pour tout x de G on a $x = u.(m.x) + v.(n.x) = (um).x + (vn).x$

or $\forall x \in G \quad mn.x = 0$ donc $n.((um).x) = nm.(u.x) = 0$

et $m.((vn).x) = 0$. Donc $(um).x \in G_n$ et $(vn).x \in G_m$.

Donc $x \in G \Rightarrow x \in G_n + G_m$ et on a bien $G = G_n + G_m$

II.6) Le résultat s'établit par récurrence sur D à l'aide de la proposition précédente.

En effet il est vrai pour $D = 1$.

Et s'il est vrai pour $D-1$, $D \geq 2$, alors il est vrai à l'ordre D car $\prod_{k=1}^{D} \uparrow_k^{mk} = \underbrace{\prod_{k=1}^{D-1} \uparrow_k^{mk}}_{m} \underbrace{\uparrow_D^{mD}}_{n}$ avec $m \wedge n = 1$.

donc $G \simeq G_m \times G_n$ et par hypothèse de récurrence

$$G_m \simeq \prod_{k=1}^{D-1} G_{\uparrow^{mk}}$$

(on utilise aussi que si G'_k est isomorphe à G''_k alors $G'_k \times G'''$ est isomorphe à $G'' \times G'''$, pour tout triplet de groupes.

III.1) Evident. Si x est un élément du sous groupe H, son ordre dans H est le même que son ordre dans G.

III.2) $\mathbb{Z}/p\mathbb{Z}$ est un corps car p est premier, donc tout élément non nul de $\mathbb{Z}/p\mathbb{Z}$ est inversible. (En effet $x = \bar{k}$ avec $1 \leq k \leq p-1$, donc $p \wedge k = 1$ (car p est premier) donc il existe (u,v) dans $\mathbb{Z}^2$ $uk + vp = 1$, puis $\bar{u}\bar{k} + \bar{v}\cdot\bar{0} = \bar{1}$, soit $\bar{u}\cdot\bar{k} = 1$.)

III.3) On a bien, pour des éléments quelconques de $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ et H, $\bar{m}\cdot(x+y) = m\cdot(x+y) = m\cdot x + m\cdot y = \bar{m}\cdot x + \bar{m}\cdot y$.
(Pq le $\cdot$ désigne ici deux lois externes différentes, le contexte permettant de savoir de laquelle on parle. Il faut prouver que $\bar{m}\cdot x$ est bien définie. Or si $\bar{m'} = \bar{m}$ il existe $u \in \mathbb{Z}$ $m' = m + up$ donc $m'\cdot x = m\cdot x + u\cdot(p\cdot x) = m\cdot x + 0 = m\cdot x$.)

On vérifie ensuite $\bar{m}\cdot(\bar{m'}\cdot x) = (\bar{m}\,\bar{m'})\cdot x$ $(= (mm')\cdot x)$
$(\bar{m} + \bar{m'})\cdot x = \bar{m}\cdot x + \bar{m'}\cdot x$.
$\bar{1}\cdot x = x$.

H est donc bien un $\mathbb{F}_p$ espace vectoriel. Comme H est fini il est nécessairement de dimension finie, notée d. Soit $(e_1, \dots, e_d)$ une base du $\mathbb{F}_p$-ev H. Alors

$$(\mathbb{F}_p)^d \longrightarrow H \qquad (\bar{m}_1, \dots, \bar{m}_d) \longmapsto \bar{m}_1 e_1 + \dots + \bar{m}_d e_d$$

est un isomorphisme d'espaces vectoriels. C'est en particulier un isomorphisme de groupes additifs

III 4) la définition de la loi externe comme cas itérations de la loi du groupe montre que H est un sous-espace vectoriel du $\mathbb{F}_p$-espace vectoriel G. Puisque G est de dimension finie. H possède donc un supplémentaire ~~K~~.
K est un $\mathbb{F}_p$-sev et c'est en particulier un sous-groupe de G et on a bien $G = H \oplus K$.

III 5) Soit $N = \max\{\text{ordre}(x), x \in G\}$. N est défini et atteint car G est fini. Donc $N = \text{ordre}(x_0)$ $x_0 \in G$, en particulier $\exists m \quad N = p^m$. Pour tout x de G $\text{ordre}(x) \leq N$
Mais $\text{ordre}(x) = p^k$ donc $k \leq m$ et $\text{ordre}(x)$ divise N.
Par conséquent $\forall x \in G \quad p^m \cdot x = 0$ ie. $p^m \cdot G = \{0\}$
et $p^{m-1} \cdot x_0 \neq 0$ donc $p^{m-1} \cdot G \neq \{0\}$ (Rq $G \neq \{0\}$ donc il existe dans G un élément d'ordre > 1, donc $m \geq 1$)

III 6) Si $\tau(G) = 0$, le résultat est vrai avec la convention $s = 0$.
Si $\tau(G) = 1$ $p \cdot G = \{0\}$ donc tout élément de G est d'ordre au plus p. G est isomorphe à $\left(\mathbb{Z}/p\mathbb{Z}\right)^d$. le résultat est vrai.

III 7) $p \cdot (x+y) = p \cdot x + p \cdot y$ donc φ est un morphisme de groupe.
$\forall y \in \text{Im}(\varphi) \quad \exists x \in G \quad y = p \cdot x$ donc $p^m \cdot y = p^{m+1} \cdot x = 0$
$\exists x_0 \in G \quad p^m \cdot x_0 \neq 0$ donc $p^{m-1} \cdot (p x_0) \neq 0 \quad \exists y_0 \in \text{Im}(\varphi) \quad p^{m-1} \cdot y_0 \neq 0$
Or a donc bien $\tau(\text{Im}\,\varphi) = m$

↖ licite car $m \geq 1$

III.8) $H = \{ \sum_{(n_1, \dots, n_D) \in \mathbb{Z}^D} n_i \cdot y_i \,,\ (n_1, \dots, n_D) \in \mathbb{Z}^D \}$

O2 $\forall j \quad p^{m_j} \cdot z_j = 0$, donc $\forall j \quad p^{m_j+1} \cdot y_j = 0 \quad (*)$

(car $\theta(p^{m_j+1} \cdot y_j) = \theta(p^{m_j} \varphi(y_j)) = p^{m_j} \theta(\varphi(y_j)) = p^{m_j} z_j = 0$
et θ est un isomorphisme.

Or a donc un morphisme surjectif de $\Pi \mathbb{Z} / p^{m_j+1}\mathbb{Z}$ vers H, noté ρ avec

$$\rho((\bar{n}_1, \dots, \bar{n}_D)) = n_1 \cdot y_1 + \dots + n_D y_D$$

- $(*)$ montre que ρ est bien défini ($\bar{n}_i = \bar{n}'_i \Rightarrow n_i \cdot y_i = n'_i \cdot y_i$)
- ρ est surjective (car d'après $(*)$ on peut se limiter à $n_i \in [0, p^{m_i+1} - 1]$

Il ne reste plus qu'à montrer que ρ est injectif.

Si $n_1 \cdot y_1 + \dots + n_D y_D = 0$

alors $\theta(\varphi(n_1 y_1 + \dots + n_D y_D)) = 0$

$$n_1 z_1 + \dots + n_D z_D = 0$$

donc $\forall i \quad p^{m_i} | n_i$ avec $m_i \geq 1$

donc $n_i = p^i n'_i$, puis

$$n'_1 \cdot p\, y_1 + \dots + n'_D p\, y_D = 0$$

soit $n'_1 \cdot z_1 + \dots + n'_D \cdot z_D = 0$ (en passant par l'isomorphisme θ)

donc $\forall i \quad p^{m_i} | n'_i$ et finalement

$\forall i \quad p^{m_i+1} | n_i$, c'est-à-dire $\bar{n}_i = \bar{0}$.

ce qui prouve l'injectivité de ρ.

III. 9) $\forall x \in \ker\varphi \quad p.x = 0$, donc $\tau(\ker\varphi) = 1$

d'après la question III. 4) il existe donc K', sous-groupe (contenu dans $\ker\varphi$) tel que $\ker\varphi = K \oplus K'$

III. 10) $K' \cap H \subset (K' \cap K \oplus \varphi) \cap H = K' \cap (\ker\varphi \cap H) = K' \cap K = \{0\}$

Soit x dans G, $y = \varphi(x) \in \mathrm{Im}\,\varphi$ donc il existe g dans H tel que $y = \varphi(g)$.

Or aura $\varphi(x - g) = 0$, c'est à dire $x - g \in \ker\varphi$

$x - g$ peut donc s'écrire $g_K + g_{K'}$ et finalement

$$x = (g + g_K) + g_{K'} \in H + K'$$

Donc $\underline{G = K' \oplus H}$

III 11) Or a $G \simeq H \times K'$, or H est isomorphe à $\prod_{i=1}^{s} \mathbb{Z}/p^{m_i}\mathbb{Z}$ et K' à $\prod_{j=1}^{d} \mathbb{Z}/p^{\alpha}\mathbb{Z}$, donc

G est bien isomorphe à $\prod_{i=1}^{s'} \mathbb{Z}/p^{m'_i}\mathbb{Z}$ $(s' = s + d)$

IV 1) D'après II. 6) si G est un groupe abélien fini il est isomorphe à $\prod H_k$ où H_k est un p_k-groupe

d'après III. 11) H_k est isomorphe à un produit de groupes cycliques. Par associativité du produit direct G est ~~est~~ isomorphe à un produit de groupes cycliques. (la réciproque est évidente)

V.1) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$

$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/35\mathbb{Z} \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$

V.2) l'application $\theta : \mathbb{Z}/n'\mathbb{Z} \to m.\mathbb{Z}/n\mathbb{Z}$

$\bar{x}' \to m.\bar{x} = \overline{mx}$

est bien définie, si $\bar{x}' = \bar{y}'$ $n' \mid x-y$ donc $n \mid m(x-y)$

c'est clairement un morphisme.

$\theta(\bar{x}') = \bar{0} \Leftrightarrow n \mid mx \Leftrightarrow n' \mid x \Leftrightarrow \bar{x}' = \bar{0}'$

θ est donc injective ; elle est surjective par construction

donc θ est un isomorphisme

V.3) Evident, par définition de la loi sur $G \times G'$

V.4) Soit G le membre de gauche et G' le membre de droite.

Raisonnons par recurrence sur $N = \sum_{i=1}^{r} \left(\sum_{j=1}^{s_i} m_{i,j} \right) + \sum_{i=1}^{r'} \left(\sum_{j=1}^{s'_i} m'_{i,j} \right)$

Si $N = 0$ le résultat est vrai (formellement)

On suppose le résultat vrai pour toute somme d'exposants strictement inférieure à N (≥ 1). Montrons que le résultat est vrai pour une somme d'exposants égale à N.

Par symétrie on peut supposer $r \geq 1$. (car $r = 0$ et $r' = 0 \Rightarrow N = 0$)

Soit $m = \min_{1 \leq j \leq s_1} m_{1,j}$ on peut supposer $m = m_{1,j}$ pour $j > s'_1$. avec $s'_1 < s_1$.

Puisque G est isomorphe à G' on a

$p_1^m . G$ isomorphe à $p_1^m . G'$

Or $p_1^m . \mathbb{Z}/p_1^{m_{1,j}}\mathbb{Z} = \{0\}$ si $j > s'_1$

$p_1^m \cdot \mathbb{Z}/p_1^{m_{i,j}}\mathbb{Z} \simeq \mathbb{Z}/p_1^{m_{i,j}-m}\mathbb{Z}$ si $j \leq D'_1$ d'après

la question précédente

$p_1^m \cdot \mathbb{Z}/p_i^{m_{i,0}}\mathbb{Z} \simeq \mathbb{Z}/p_i^{m_{i,0}}\mathbb{Z}$ si $i \geq 2$ (toujours

d'après la question précédente) et de même

$$\begin{cases} p_1^m \cdot \mathbb{Z}/p_i'^{m'_{i,0}}\mathbb{Z} \simeq \mathbb{Z}/p_i^{m'_{i,0}}\mathbb{Z} & \text{si } p'_i \neq p_1 \\ \simeq \mathbb{Z}/p_1^{m'_{i,0}-m}\mathbb{Z} & \text{si } p'_i = p_1 \text{ et } m'_{i,0} \geq m \\ \simeq \{0\} & \text{si } p'_i = p_1 \text{ et } m'_{i,0} < m \end{cases}$$

Dans le membre de gauche au moins deux des facteurs est réduit à $\{0\}$ et puisque $\{0\} \times G_1 \simeq G_1$ pour tout groupe G_1, on obtient une égalité de produit dont la somme des exposants est strictement inférieure à N. L'hypothèse de récurrence implique l'identité des décompositions.

On obtient donc * $\{p_i \neq p_1\} = \{p'_i \neq p_1\}$ et si

$p_i = p'_{i'} \neq p_1$ $D_i = D'_{i'}$ et $m_{i,j} = m'_{i',j}$ pour tout $j \leq D_i$

* On a aussi, si reste à gauche au moins un facteur $\mathbb{Z}/p_1^m\mathbb{Z}$

$\exists\, i'$ $p'_{i'} = p_1$ et ~~$\forall j$ $m_{i,j} > m$ $\Leftrightarrow$ $m'_{i',j} > m$~~

la collection des $m_{i,j}$ tels que $m_{1,j} > m$ est égale à la collection des $m'_{i',j'}$ tels que $m'_{i',j'} > m$.

Pour obtenir finalement qu'il existe autant de j tels que $m_{1,j} = m$ que de j' tels que $m'_{i,j'} = m$.

On remarque que les deux groupes doivent avoir même cardinal. Et le théorème de l'arithmétique montre que ces deux cardinaux doivent donc être divisible par la même puissance de p_1, qui est N_1

à gauche $\quad m \times \operatorname{card}\{j, m_{1,j} = m\} + \underbrace{\sum_{j, m_{1,j} > m} m_{1,j}}_{N_1}$

à droite $\quad m \times \operatorname{card}\{j', m'_{i,j'} = m\} + \underbrace{\sum_{j', m'_{i,j'} > m} m'_{i,j'}}_{N_2}$

Or on vient de prouver $N_1 = N_2$, donc

$$\operatorname{card}\{j, m_{1,j} = m\} = \operatorname{card}\{j', m'_{i,j'} = m\}$$ q.e.d.

V.5) On a donc $G \simeq \prod_{i=1}^{r} \left(\prod_{j=1}^{s_i} \mathbb{Z}/p_i^{m_{i,j}}\mathbb{Z} \right)$, on peut supposer la suite $(m_{i,j})_{1 \le j \le s_i}$ décroissante, quitte à la réordonner. On pose $n = \max s_i$ et on pose

$m_{i,j} = 0$ si $s_i < j \le n$.

On a alors

$$G \simeq \prod_{j=1}^{n} \left(\prod_{i=1}^{r} \left(\mathbb{Z}/p_i^{m_{i,n-j}}\mathbb{Z} \right) \right)$$

D'après II 6 (à l'envers)

$$G \simeq \prod_{j=1}^{n} \mathbb{Z}/d_j\mathbb{Z}$$

avec $d_j = \prod_{i=1}^{r} p_i^{m_{i,n-j}}$. Or a donc bien $d_j \mid d_{j+1}$ si $1 \le j < n$.

V.5.a) La démonstration de l'unicité de la décomposition se démontre comme en V 4 :

Si $G \neq \{0\}$ $d_1 \geq 1$ et $d_1 G \simeq \prod_{i=1}^{n} \frac{\mathbb{Z}}{\frac{d_i}{d_1}\mathbb{Z}} = \prod_{i=k}^{n} \frac{\mathbb{Z}}{\frac{d_i}{d_1}\mathbb{Z}}$

donc il y a unicité de $(\frac{d_k}{d_1}, \dots, \frac{d_n}{d_1})$ $(k-1 = \max\{i, d_i = d_1\})$

L'unicité de $(d_1, d_2, \dots, d_n)$ s'obtient en considérant ensuite le cardinal de G.

V 5.B) $\frac{\mathbb{Z}}{72\mathbb{Z}} \times \frac{\mathbb{Z}}{30\mathbb{Z}} \times \frac{\mathbb{Z}}{75\mathbb{Z}} \simeq \frac{\mathbb{Z}}{8\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{25\mathbb{Z}}$

$\frac{\mathbb{Z}}{72\mathbb{Z}} \times \frac{\mathbb{Z}}{30\mathbb{Z}} \times \frac{\mathbb{Z}}{75\mathbb{Z}} \simeq \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{8\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{25\mathbb{Z}}\right)$

$\simeq \left(\frac{\mathbb{Z}}{\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{8\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{25\mathbb{Z}}\right)$

$\simeq \left(\frac{\mathbb{Z}}{\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{8\mathbb{Z}} \times \frac{\mathbb{Z}}{9\mathbb{Z}} \times \frac{\mathbb{Z}}{25\mathbb{Z}}\right)$

$\frac{\mathbb{Z}}{72\mathbb{Z}} \times \frac{\mathbb{Z}}{30\mathbb{Z}} \times \frac{\mathbb{Z}}{75\mathbb{Z}} \simeq \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{30\mathbb{Z}} \times \frac{\mathbb{Z}}{1800\mathbb{Z}}$