Série 7

David Wiedemann

30 octobre 2020

1

Supposons que $(m, n) = 1$.
On utilise la propriété du produit universelle pour construire un morphisme entre ${}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}}$.
Soit l'application α définie par

$$\alpha : k \in {}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}} \mapsto [k]_n \in {}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$$

De même on définit l'application β par

$$\beta : k \in {}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}} \mapsto [k]_m \in {}^{\mathbb{Z}}\!/\!_{m\mathbb{Z}}$$

où $[.]_m$ est la classe de congruence modulo m d' un élément.

Vérifions que ces applications sont linéaires.
On vérifie facilement que α et β sont des morphismes, en effet

$$\alpha(0) = 0$$

car 0 est congru à 0 modulo n.
Soit $a, b \in {}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}}$, alors

$$\alpha(a + b) = [a + b]_n = [a]_n + [b]_n$$

où la dernière égalité suit directement de la définition de classe d'équivalence modulo n.
On vérifie de la même manière que β est linéaire.
Par la propriété du produit universel, il existe donc un morphisme ϕ de ${}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}}$ vers ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{m\mathbb{Z}}$.

De plus, on sait que $\mathrm{pr}_n \circ \phi = \alpha$ et $\mathrm{pr}_m \circ \phi = \beta$ où pr_n est la projection sur ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}}$ et pr_m la projection sur ${}^{\mathbb{Z}}\!/\!_{m\mathbb{Z}}$.

Vérifions que ϕ est un isomorphisme.
Car

$$\left|{}^{\mathbb{Z}}\!/\!_{nm\mathbb{Z}}\right| = \left|{}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}} \times {}^{\mathbb{Z}}\!/\!_{m\mathbb{Z}}\right|$$

Il suffit, par l'exercice 1 de la série 5, de vérifier que ϕ est injective.

Supposons que $\phi(k) = (0,0)$ et montrons que ceci implique $k = 0$.
Si $\phi(k) = (0,0)$, alors $\alpha(k) = 0$ et $\beta(0)$. Donc $[k]_n = 0$ et $[k]_m = 0$, donc k est un multiple de n et de m. Car n et m sont premiers entre eux, ceci implique qu'il existe a tel que $k = anm$, donc $k = 0$.

Supposons maintenant que $(n,m) \neq 1$.
Supposons par l'absurde qu'il existe un isomorphisme ϕ entre $\mathbb{Z}/_{nm\mathbb{Z}}$ et $\mathbb{Z}/_{n\mathbb{Z}} \times \mathbb{Z}/_{m\mathbb{Z}}$. On sait que les isomorphismes préservent les ordres des éléments, on a donc en particulier

$$o(1) = nm.$$

Ce qui implique

$$o(\phi(1)) = nm$$

Or, posons que $(n,m) = a$, alors $a|nm$ et donc $\frac{nm}{a}$ est un entier.
Car $\frac{nm}{a}$ est un multiple de n, on trouve que pour tout $k \in \mathbb{Z}/_{n\mathbb{Z}}$

$$\frac{nm}{a} \cdot [k] = [0]$$

et de même, $\forall k \in \mathbb{Z}/_{m\mathbb{Z}}$

$$\frac{nm}{a} \cdot [k] = [0]$$

Donc l'ordre de $\phi(1)$ est borné par $\frac{nm}{a}$ ce qui est une contradiction au fait que ϕ est bijective.
Donc, il ne peut pas y avoir d'isomorphismes si $(n,m) \neq 1$.

2

Théorème 1. *Soit A un groupe, et $B \simeq C$ deux groupes isomorphes, alors*

$$A \times B \simeq A \times C$$

Démonstration. On sait qu'il existe un isomorphisme ϕ entre B et C, on peut donc construire un isomorphisme ainsi

$$A \times B \mapsto A \times C$$
$$(a,b) \mapsto (a, \phi(b))$$

La vérification que cette application est un isomorphisme est immédiate car ϕ est un isomorphisme. $\square$

On procède par récurrence sur r.
On sait que le cas $r = 2$ est vrai par la partie 1. (Le cas $r = 1$ est trivialement vrai)
Supposons donc vrai pour r et montrons pour $r + 1$.
On sait que $(n_r, n_i) = 1$ et $(n_{r+1}, n_i) = 1$ pour tout $0 < i < r$. On en déduit que $(n_r \cdot n_{r+1}, n_i) = 1$. Ceci suit directement de la décomposition en nombre premiers, en effet n_{r+1} et n_r ne partagent pas de facteurs avec les n_i et donc $n_r \cdot n_{r+1}$ non plus.
En posant donc que $n_r \cdot n_{r+1} = p$, on trouve

$$\begin{aligned}
\mathbb{Z}/(n_1 \dots n_{r+1})\mathbb{Z} \simeq \mathbb{Z}/(n_1 \dots n_{r-1}p)\mathbb{Z} &\simeq \prod_{i=1}^{r-1} \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} && (1)\\
&\simeq \prod_{i=1}^{r-1} \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}/n_r n_{r+1}\mathbb{Z} && (2)\\
&\simeq \prod_{i=1}^{r-1} \mathbb{Z}/n_i\mathbb{Z} \times \mathbb{Z}/n_r\mathbb{Z} \times \mathbb{Z}/n_{r+1}\mathbb{Z} && (3)\\
&\simeq \prod_{i=1}^{r+1} \mathbb{Z}/n_i\mathbb{Z} && (4)
\end{aligned}$$

où l'égalité (1) suit de l'hypothèse de récurrence, et l'égalité (3) suit du théorème 1.
La forme de l'isomorphisme ci-dessus est donné par la généralisation de l'isomorphisme donné en 1 à plusieurs entiers, c'est à dire

$$k \in \mathbb{Z}/(n_1 \dots n_r)\mathbb{Z} \mapsto ([k]_{n_1}, \dots [k]_{n_r})$$