1.9 Théorème chinois et applications

Recasage : 120, 122, 142.

Références : Exercices de mathématiques pour l'agrégation, Francinou-Gianella, Mathématiques pour l'agrégation : algèbre et géométrie, Rombaldi.

Théorème 1.7. *Soit A un anneau principal, et $a_1, \dots, a_n \in A$ premiers entre eux, alors :*

$$A/(a_1 \dots a_n) \cong A/(a_1) \times \cdots \times A/(a_n).$$

Démonstration. On va procéder par récurrence sur n. Pour $n = 1$, le résultat est immédiat. Pour $n = 2$, soient $a, b \in A$ premiers entre eux. Comme A est principal, d'après le théorème de Bezout, il existe $u, v \in A$ tels que $1 = au + bv$.
Pour $x \in A$, on note $\overline{x}$ la classe de x dans l'idéal (a), et $\tilde{x}$ la classe de x dans l'idéal (b). Considérons :

$$\phi : (\overline{x}, \tilde{y}) \in A/(a) \times A/(b) \mapsto (auy + bvx \mod (ab)) \in A/(ab).$$

Montrons que ϕ est correctement défini, c'est-à-dire que $\phi(\overline{x}, \tilde{y})$ ne dépend pas du choix des représentants. Soit $k, l \in A$, alors immédiatement :

$$auy + bvx \equiv am(y + lb) + bv(x + ka) \mod (ab),$$

et ϕ est correctement défini. De plus, ϕ est un morphisme d'anneaux :

— $\phi(\overline{1}, \tilde{1}) = au + bv \mod (ab) = 1 \mod (ab)$,

— soient $\overline{x}, \overline{x'} \in A/(a)$, soient $\tilde{y}, \tilde{y'} \in A/(b)$, on a modulo (ab) :

$$\begin{aligned}
\phi(\overline{x} + \overline{x'}, \tilde{y} + \tilde{y'}) &= au(\tilde{y} + \tilde{y'}) + bv(\overline{x} + \overline{x'}) = \phi(\overline{x}, \tilde{y}) + \phi(\overline{x'}, \tilde{y'}), \text{ et} \\
\phi(\overline{x}, \tilde{y})\phi(\overline{x'}, \tilde{y'}) &= (au\tilde{y} + bv\overline{x})(au\tilde{y'} + bv\overline{x'}) \\
&= (au)^2\tilde{y}\tilde{y'} + au\tilde{y}bv\overline{x'} + bv\overline{x}au\tilde{y'} + (bv)^2\overline{x}\overline{x'} \\
&= au(1 - bv)\tilde{y}\tilde{y'} + bv(1 - au)\overline{x}\overline{x'} \\
&= au\overline{x}\overline{x'} + bv\tilde{y}\tilde{y'} \\
&= \phi(\overline{x}\overline{x'}, \tilde{y}\tilde{y'}).
\end{aligned}$$

Montrons que ϕ est surjectif : soit $x \in A$, alors :

$$\phi(\overline{x}, \tilde{x}) \equiv aux + bvx \equiv (au + bv)x \equiv x \mod (ab),$$

et ceci prouve la surjectivité de ϕ.
Soit $(x, y) \in A^2$ tel que $auy + bvx \equiv 0 \mod (ab)$, alors ab divise $auy + bvx$. Comme a divise auy, a divise bvx. Or, la relation $au + bv = 1$ prouve que a et bv sont premiers entre eux. Le théorème de Gauss permet alors d'assurer que a divise x, i.e. $\overline{x} = 0$. De même, $\tilde{y} = 0$, donc ϕ est injectif.
Par conséquent, ϕ réalise un ismorphisme entre $A/(a) \times A/(b)$ et $A/(ab)$.

Supposons $n \geq 3$, et $a_1, \ldots, a_n$ premiers entre eux deux à deux. Par hypothèse de récurrence :

$$A/(a_1 \ldots a_{n-1}) \cong A/(a_1) \times \cdots \times A/(a_{n-1}).$$

Ainsi :

$$A/(a_1) \times \cdots \times A/(a_{n-1}) \times A/(a_n) \cong A/(a_1 \ldots a_{n-1}) \times A/(a_n) \cong A/(a_1 \ldots a_n).$$

En effet, le dernier isomorphisme résulte du cas $n = 2$, puisque a_n est premier avec le produit $a_1 \ldots a_n$. □

Application 1.3. *On considère le système d'équations diophantiennes :*

$$\begin{cases} k \equiv 2 \mod 4 \\ k \equiv 3 \mod 5 \\ k \equiv 1 \mod 9 \end{cases}$$

Alors, l'ensemble des solutions du système est de la forme $118 + 180n$, $n \in \mathbb{Z}$.

Démonstration. Comme $n_1 = 4$, $n_2 = 5$ et $n_3 = 9$ sont premiers entre eux deux à deux, ce système a des solutions données en déterminant des coefficients dans une relation de Bezout $u_1 m_1 + u_2 m_2 + u_3 m_3 = 1$, où $m_1 = n_2 n_3 = 45$, $m_2 = n_1 n_3 = 36$ et $m_3 = n_1 n_2 = 20$. Par l'associativité du pgcd, on a :

$$\begin{cases} (m_2, m_3) = 4 = (-1).36 + 2.20 \\ 1 = (m_1, (m_2, m_3)) = 1.45 + (-11).4 \\ 1 = 1.45 + 11.36 + (-22).20 \end{cases}$$

Ceci donne la solution particulière $k_0 = 2.45 + 33.36 - 22.20 = 838$, et la solution générale $k = 838 + 180q = 118 + 180q'$, avec $q' \in \mathbb{Z}$. □

Commentaires : Si le développement est trop court, on peut, en préambule, démontrer le théorème dans le cas où $A = \mathbb{Z}$.