Système de congruences

Référence : CVA p167 et J. Calais Elt de théorie des groupes (Dunod)

Leçons :

Théorème 1 : Soient $m, n \in \mathbb{Z}$. On note $\delta = pgcd(m,n)$ et $\mu = ppcm(m,n)$.
On considère $\tilde{\varphi}$ le morphisme d'anneaux :

$$\tilde{\varphi} : \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Alors il existe un morphisme $\varphi : \mathbb{Z}/\mu\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ injectif et un autre $\psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$ surjectif tel que $\operatorname{Im}\varphi = \operatorname{Ker}\psi$.

Application 2 :

(i) $(S)\begin{cases} x \equiv 2 \ [21] \\ x \equiv 11 \ [35] \end{cases}$ n'admet pas de solutions

(ii) Soit $a, b \in \mathbb{Z}$ tq $a \equiv b \ [\delta]$. Posons $u_0 = \frac{1}{\delta}(avn + bum)$ où $um + vn = \delta$
Alors, $\mathcal{S} = x_0 + \mu\mathbb{Z}$.

Théorème 0 : (Propriété universelle du groupe quotient)
Soient G un groupe, $H \lhd G$, $f : G \longrightarrow G'$ tq $H \subset \operatorname{Ker} f$. Alors il existe un unique morphisme $\varphi : G/H \longrightarrow G'$ tel que $\varphi \circ \pi = f$.

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ & \searrow^{f} & \downarrow \varphi \\ & & \operatorname{Im} f \end{array}$$

Preuve 0 :

Considérons $\varphi : G/H \longrightarrow G'$, $\bar{x} \longmapsto f(x)$

φ est bien définie : si $\bar{x} = \bar{x}'$ dans G/H alors $x x'^{-1} \in H$ et comme $H \subset \operatorname{Ker} f$:

$$f(x x'^{-1}) = e' \Rightarrow f(x) = f(x').$$

φ est un morphisme : $\varphi(\bar{x}\bar{y}) = \varphi(\overline{xy}) = f(xy) = f(x)f(y) = \varphi(\bar{x})\varphi(\bar{y})$

et $\varphi(\bar{x}) = \varphi(\pi(x)) = f(x)$.

φ est unique supposons que $\varphi' : G/H \longrightarrow G'$ tel que $\varphi' \circ \pi = f$

alors $\forall \bar{x} \in G/H, \varphi(\bar{x}) = f(x) = \varphi'(\bar{x})$ donc $\varphi = \varphi'$. ∎

Preuve 1

(i) $\ker \varphi = \{ a \in \mathbb{Z},\ m \mid a \text{ et } n \mid a \} = \mu\mathbb{Z}$. ~~(De plus, φ est surjectif).~~

~~Par le 1er thm d'isomorphisme on a :~~

$$\frac{\mathbb{Z}}{\ker \tilde{\varphi}} = \frac{\mathbb{Z}}{\mu\mathbb{Z}} \simeq \nu_m \tilde{\varphi}$$

~~Et~~ Par passage au quotient, on a un morphisme $\varphi : \mathbb{Z}/\mu\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ injectif.

(ii) ~~Posons $G = \mathbb{Z}/m\mathbb{Z}$ et $G' = \mathbb{Z}/\delta\mathbb{Z}$.~~ Posons $G = \mathbb{Z}$ et $G' = \mathbb{Z}/\delta\mathbb{Z}$. Comme $\delta \mid m$, $H = m\mathbb{Z} \leqslant \ker f = \delta\mathbb{Z}$ où $f : \mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$, $x \longmapsto \bar{x}$. Par passage au quotient, il existe un morphisme $\psi_1 : \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$. Idem, $\exists\, \psi_2 : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$

Ainsi, on définit $\psi : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/\delta\mathbb{Z}$ est bien défini, et c'est un

$$(x, y) \longmapsto \psi_1(x) - \psi_2(y)$$

morphisme de groupes additifs : $\psi\big((x,y) + (x',y')\big) = \psi\big((x+x'), y+y'\big)\big) = \psi_1(x) + \psi_1(x') \ldots$

Il est surjectif car f l'est.

(iii) $\nu_m \psi \subset \ker \psi$: ~~bon raisonnement~~. Soit $\bar{x} \in \mathbb{Z}/\mu\mathbb{Z}$

Alors $\psi\big((\bar{x}_m, \bar{x}_n)\big) = \bar{x}_\delta - \bar{x}_\delta = 0$.

Donc $|\nu_m \psi| \overset{\psi \text{ surjectif}}{=} \mu = \frac{mn}{\delta} = \frac{|\mathbb{Z}_m \times \mathbb{Z}_n|}{|\ker \psi|} = |\nu_m \psi|$

Donc $\nu_m \psi = \ker \psi$.

∎

Preuve 2 :

(i) Supposons que $x \in \mathbb{Z}$ soit solution, i.e $\varphi(x) = (\bar{2}_{11}, \bar{11}_{35}) \in \ker \psi$

et donc ~~$\delta = 7$~~ on aurait $\bar{2}_7 - \bar{11}_7 = -\bar{9}_7 = \bar{0}_7$ impossible.

(ii) $\bar{a}_\delta = \bar{b}_\delta$ donc $\exists k \in \mathbb{Z}$ tq $a = b + k\delta \iff b = a - k\delta$.

$$x_0 = \frac{1}{\delta}\big((b+k\delta)vn + bum\big) = \frac{1}{\delta}\big(b(vn+um) + k\delta vn\big) = b + kvn \equiv b\,[n]$$

$$= a - k\delta + kvn = a + k(vn - \delta) = a + kum \equiv a\,[m]$$

Si $x \in \mathbb{Z}$ est solution du système, $\tilde{\varphi}(x) = \varphi(x_0)$ et donc $x - x_0 \in \ker \varphi = \mu\mathbb{Z}$

D'où $S = x_0 + \mu\mathbb{Z}$.

Ex : $S \begin{cases} x \equiv 3\,[11] \\ x \equiv 10\,[35] \end{cases}$ $2 \times 11 - 35 = 7$ $x_0 = \frac{1}{7}\big(-1 \times 3 \times 35 + 2 \times 10 \times 11\big) = 45$. $S = 45 + 385\mathbb{Z}$.