Lemme chinois

Recasages :

- 120 : Anneaux Z/nZ. Applications.
- 122 : Anneaux principaux. Exemples et applications.
- 142 : PGCD et PPCM, algorithmes de calcul. Applications.

Références :

- Mathématiques pour l'agrégation : Algèbre et géométrie, Rombaldi, p249-283

Définition 1. ***Elements premiers entre eux [ROM 245]***

Soit A un anneau principal. Soit $a_1, \dots, a_r \in A^*$. On dit que $a_1, \dots, a_r$ sont premiers entre eux dans leur ensemble si leur pgcd est dans $A^\times$.

[ROM 249] Soit A un anneau principal.

Soit $a_1, \dots, a_r \in A$ des éléments non nuls et non inversibles. On note $a = \prod_{j=1}^{r} a_j$.

Pour tout $j \in [\![1; r]\!]$, on pose $\pi_j : A \to A/(a_j)$ la surjection canonique. Soit $\pi : A \to A/(a)$.

Pour tout $j \in [\![1; r]\!]$, on pose $b_j = \frac{a}{a_j} = \prod_{i=1, i\neq j}^{r} a_i$.

Lemme 1. *Si les a_j, pour $j \in [\![1; r]\!]$, sont deux à deux premiers entre eux, alors les b_j, pour $j \in [\![1; r]\!]$, sont premiers entre eux dans leur ensemble.*

Démonstration :

Par l'absurde, si les b_j ne sont pas premiers entre eux dans leur ensemble, il existe un élément p premier de A qui divise tous les b_j. Ainsi $p | b_1 = \prod_{i=2}^{r} a_i$. Donc il existe $i \in [\![2; r]\!]$ tel que $p | a_i$. Mais on a aussi que $p | b_i$ donc p divise un a_k avec $k \in [\![1; r]\!]$ et $k \neq i$. Contradiction car a_i et a_k sont premiers entre eux. □

Lemme 2. ***Lemme chinois [ROM 249]***

Soit A un anneau principal. On suppose que les a_j pour $j \in [\![1; r]\!]$ sont deux à deux premiers entre eux. Alors l'application :

$$\begin{aligned} f : A &\to \prod_{j=1}^{r} A/(a_j) \\ x &\mapsto (\pi_1(x), \dots, \pi_r(x)) \end{aligned}$$

est un morphisme d'anneaux surjectif de noyau $\mathrm{Ker}(f) = (\prod_{j=1}^{r} a_j) = (a)$.

Ainsi f induit un isomorphisme d'anneaux :

$$\begin{aligned} \bar{f} : A/(a) &\to \prod_{j=1}^{r} A/(a_j) \\ \pi(x) &\mapsto (\pi_1(x), \dots, \pi_r(x)) \end{aligned}$$

Démonstration :

Il est clair que f est un morphisme d'anneaux (il y a 3 axiomes à vérifier).

Son noyau est formé des multiples de tous les a_j, donc de leur ppcm $a = \prod_{j=1}^{r} a_j$ étant donné qu'ils sont deux à deux premiers entre eux.

D'après le lemme (1), comme les $b_i = \frac{a}{a_i}$ sont premiers entre eux dans leur ensemble, d'après le théorème de Bézout, il existe une suite $(u_i)_{1 \leqslant i \leqslant r}$ d'éléments de A tel que :

$$\sum_{i=1}^{r} u_i b_i = 1.$$

Or pour $j \in [\![1; r]\!]$, on a que $\pi_j(b_i) = \pi_j(0)$ pour $i \neq j$ car b_i est divisible par a_j. On obtient donc :

$$\pi_j(1) = \pi_j\left(\sum_{i=1}^{r} u_i b_i\right) = \pi_j(u_j)\pi_j(b_j).$$

Maintenant soit $(\pi_j(x_j))_{1 \leqslant j \leqslant r} = (\pi_1(x_1), \ldots, \pi_r(x_r))$ donné dans $\prod_{j=1}^{r} A/(a_j)$.

On pose alors $x = \sum_{i=1}^{r} x_i u_i b_i$ et on obtient que pour tout $j \in [\![1; r]\!]$,

$$\pi_j(x) = \pi_j(x_j)\pi_j(u_j)\pi_j(b_j) = \pi_j(x_j)\pi_j(1) = \pi_j(x_j).$$

Ainsi $f(x) = \big(\pi_1(x), \ldots, \pi_r(x)\big) = \big(\pi_1(x_1), \ldots, \pi_r(x_r)\big) = (\pi_j(x_j))_{1 \leqslant j \leqslant r}$. Donc f est surjectif.

D'après le premier théorème d'isomorphisme, on obtient bien que :

$$A/(a) \simeq \prod_{j=1}^{r} A/(a_j)$$

et la surjectivité nous a même donné l'inverse de $\bar{f}$. □

Application : indicatrice d'Euler [ROM 283]

On se place sur $A = \mathbb{Z}$.

Définition 2. ***Indicatrice d'Euler***

On appelle fonction indicatrice d'Euler la fonction qui à tout $n \in \mathbb{N}^*$ associe $\varphi(n)$ le nombre d'entiers compris entre 1 et n qui sont premiers avec n.

Cela correspond au nombre d'inversibles de $\mathbb{Z}/n\mathbb{Z}$.

- Si p est premier, alors tout entier compris entre 1 et $p-1$ est premier avec p donc $\varphi(p) = p-1$.
- Si p est premier et $\alpha \in \mathbb{N}^*$, alors :

$$\begin{aligned}
\varphi(p^\alpha) &= \#\{k \in [\![1; p^\alpha]\!] \,;\, k \wedge p^\alpha = 1\} \\
&= p^\alpha - \#\{k \in [\![1; p^\alpha]\!] \,;\, k \text{ et } p^\alpha \text{ ont un diviseur commun}\} \\
&= p^\alpha - \#\{k \in [\![1; p^\alpha]\!] \,;\, p | k\} \\
&= p^\alpha - \#\{p; 2p; 3p; \ldots; p^{\alpha-1}p\} \\
&= p^\alpha - p^{\alpha-1} \\
\varphi(p^\alpha) &= (p-1)p^{\alpha-1}
\end{aligned}$$

- Si $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ est la décomposition en produit de facteurs premiers de n, d'après le lemme chinois on a un isomorphisme d'anneaux :

$$\mathbb{Z}/n\mathbb{Z} \simeq \prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$$

ce qui induit un isomorphisme de groupes :

$$(\mathbb{Z}/n\mathbb{Z})^\times \simeq \left(\prod_{i=1}^{r} \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}\right)^\times = \prod_{i=1}^{r} (\mathbb{Z}/p_i^{\alpha_i}\mathbb{Z})^\times.$$

En prenant les cardinaux, on obtient que :

$$\varphi(n) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} (p_i - 1)p_i^{a_i - 1} = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

□

Remarque 1. [ROM 287]

Pour l'application sur l'indicatrice d'Euler, on a utilisé que :

Lemme 3. *Si $f : A \to B$ est un isomorphisme d'anneaux, alors il réalise un isomorphisme de groupes de $A^\times$ sur $B^\times$.*

Démonstration :

On a que $f(1_A) = 1_B$ par définition d'un morphisme d'anneaux.

Soit $a \in A^\times$. Alors $1_B = f(1_A) = f(aa^{-1}) = f(a)f(a^{-1})$, donc $f(a) \in B^\times$. Ainsi f est bien un morphisme de groupes de $A^\times$ dans $B^\times$.

Comme f est injectif, il en est de même pour sa restriction à $A^\times$.

On montre qu'il est surjectif. Soit $b \in B^\times$. Comme f est surjectif, il existe $a \in A$ tel que $b = f(a)$. Comme b est inversible, il existe $c = f(a') \in B^\times$ tel que $1_B = bc = f(aa') = f(1_A)$. Par injectivité de f, on a que $aa' = 1$ et donc $a \in A^\times$. Donc la restriction de f à $A^\times$ est surjective sur $B^\times$.

On a donc bien un isomorphisme de groupes.

Remarque 2. [ROM 290]

Le théorème chinois peut-être utilisé pour résoudre des systèmes de congruences, grâce à l'expression du morphisme inverse.

En effet, supposons que l'on cherche les solutions k du système :

$$k \equiv x_j \, [a_j] \quad (1 \leqslant j \leqslant r)$$

où $(x_j)_j$ est une suite donnée d'entiers relatifs.

Si les $a_1, \ldots, a_r$ sont deux à deux premiers entre eux, cela revient à trouver l'antécédent dans $\mathbb{Z}/a\mathbb{Z}$ de $\big(\pi_1(x_1), \ldots, \pi_r(x_r)\big)$ par l'isomorphisme :

$$\begin{array}{rccc} \bar{f} : & \mathbb{Z}/a\mathbb{Z} & \to & \displaystyle\prod_{j=1}^{r} \mathbb{Z}/a_j\mathbb{Z} \\ & \pi(k) & \mapsto & (\pi_1(k), \ldots, \pi_r(k)) \end{array}$$

Or celui-ci est $\bar{k_0}$ où $k_0 = \sum_{i=1}^{r} x_i u_i b_i$ où la suite $(u_i)_i$ est telle que $\sum_{i=1}^{r} u_i b_i = 1$ avec $b_i = \frac{a}{a_i}$.

Exemple : résoudre

$$\begin{cases} k \equiv 2\,[4] \\ k \equiv 3\,[5] \\ k \equiv 1\,[9] \end{cases}$$

On a alors que $a_1 = 4$, $a_2 = 5$ et $a_3 = 9$, qui sont bien premiers entre eux deux à deux. On a $a = 4 \times 5 \times 9 = 180$.

On cherche : $u_1b_1 + u_2b_2 + u_3b_3 = 1$ où $b_1 = a_2a_3 = 45$, $b_2 = a_1a_3 = 36$ et $b_3 = a_1a_2 = 20$.

On utilise alors l'associativité du pgcd.

On calcule la relation pour b_2 et b_3 :

$$\begin{aligned} 36 &= 1 \times 20 + 16 \\ 20 &= 1 \times 16 + 4 \\ 16 &= 4 \times 4 + 0 \end{aligned}$$

Donc $\text{pgcd}(36, 20) = 4$ et :

$$4 = 20 - 16 = 20 - (36 - 20) = (-1) \times 36 + 2 \times 20.$$

On calcule maintena la relation pour b_1 et 4 :

$$\begin{aligned} 45 &= 11 \times 4 + 1 \\ 4 &= 4 \times 1 + 0 \end{aligned}$$

Donc $\text{pgcd}(4, 45) = 1$ et :

$$1 = 45 - 11 \times 4.$$

Finalement $1 = b_1 \wedge b_2 \wedge b_3 = b_1 \wedge (b_2 \wedge b_3)$, d'où :

$$\begin{aligned} 1 &= 1 \times 45 - 11 \times 4 \\ &= 1 \times 45 - 11 \times \Big((-1) \times 36 + 2 \times 20 \Big) \\ &= \underbrace{1}_{u_1} \times 45 + \underbrace{11}_{u_2} \times 36 + \underbrace{(-22)}_{u_3} \times 20. \end{aligned}$$

Donc on obtient la solution particulière :

$$\begin{aligned} k_0 &= 2 \times 1 \times 45 + 3 \times 11 \times 36 + 1 \times (-22) \times 20 \\ &= 90 + 11 \times (108 - 40) \\ &= 90 + 11 \times 68 \\ &= 90 + 748 \\ &= 838 \equiv 118\,[180]. \end{aligned}$$

La solution générale est finalement : $k = 118 + 180q$ avec $q \in \mathbb{Z}$. □

Remarque 3. [ROM 291]

Si l'on est dans le cas :

$$\begin{cases} k \equiv x_1\,[a_1] \\ k \equiv x_2\,[a_2] \end{cases}$$

avec a_1 et a_2 pas forcément premiers entre eux, alors ce système a des solutions si et seulement si $x_2 - x_1$ est un multiple de $\text{pgcd}(a_1, a_2)$.

Et les solutions sont alors : $S = \{k_0 + q \times \text{ppcm}(a_1, a_2)\,;\, q \in \mathbb{Z}\}$ où k_0 est une solution particulière. □