Cours

Autour du théorème des restes chinois

Mathieu Mansuy - Préparation à l'Agrégation Interne de Mathématiques, Université de Franche Comté
mathieu.mansuy@ac-besancon.fr

1 Deux exercices

1.1 Un exercice d'arithmétique

Énoncé

17 pirates s'emparent d'un navire. S'ils se partagent le butin, il reste 3 pièces d'or pour le cuisinier chinois. Mais les pirates se querellent et 6 d'entre eux sont tués. S'ils se partagent alors le butin, il resterait 4 pièces d'or pour le cuisinier. Le navire faire alors naufrage, et seuls 6 pirates survivent. Le partage laisserait 5 pièces d'or au cuisinier.
Combien celui-ci aura-t-il au minimum lorsqu'il empoisonnera les pirates survivants ?

Solution de l'exercice

On est amené à résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \\ x \equiv 5[6] \end{cases}.$$

Soit x une solution d'un tel système. Il existe donc $k, \ell \in \mathbb{Z}$ tels que $x-3 = 17k$ et $x-4 = 11\ell$. En soustrayant ces deux égalités, on se ramène à la résolution de l'équation diophantienne :

$$1 = 17k - 11\ell.$$

Cette équation admet bien des solutions, puisque $17 \wedge 11 = 1$ divise bien 1. Pour la résoudre, donnons une identité de Bezout entre 17 et 11. On observe que :

$$1 = 2 \times 17 - 3 \times 11.$$

En soustrayant ces deux égalités, on obtient :

$$0 = (k-2) \times 17 - (\ell - 3) \times 11$$

ce qui se récrit :

$$(\ell - 3) \times 11 = (k-2) \times 17.$$

Par Gauss, 17 et 11 étant premiers entre eux, il existe $u \in \mathbb{Z}$ tel que $k - 2 = 11 \times u$. Ainsi,

$$x = 17k + 3 = 17(11u + 2) + 3 = 17 \times 11 \times u + 37 \equiv 37[17 \times 11].$$

x est donc solution du système de congruences :

$$\begin{cases} x \equiv 37[17 \times 11] \\ x \equiv 5[6] \end{cases}.$$

De même, il existe $r, s \in \mathbb{Z}$, tels que $x - 37 = 17 \times 11 \times r$ et $x - 5 = 6 \times s$, d'où par soustraction :

$$32 = 6s - 17 \times 11 \times r.$$

Là aussi, cette équation diophantienne admet bien une solution puisque $(17 \times 11) \wedge 6 = 1$ divise bien 32. Remarquons que :

$$17 \times 11 - 31 \times 6 = 1 \quad \Rightarrow \quad 32 \times 17 \times 11 - 31 \times 32 \times 6 = 1.$$

D'où en soustrayant :

$$6 \times (s + 32 \times 31) - 17 \times 11 \times (m + 32) = 0.$$

Toujours par Gauss, il existe $v \in \mathbb{Z}$ tel que $m + 32 = 6v$. En substituant, on obtient :

$$x = 37 + 17 \times 11 \times (6v - 32).$$

D'où, modulo $17 \times 11 \times 6$:

$$x \equiv 37 - 17 \times 11 \times 32 \equiv 37 + 17 \times 11 \times 4 \equiv 785[17 \times 11 \times 6].$$

Réciproquement, on vérifie qu'un tel x satisfait bien le système de congruences de départ. On obtient ainsi l'équivalence suivante :

$$\begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \\ x \equiv 5[6] \end{cases} \quad \Leftrightarrow \quad x \equiv 785[17 \times 11 \times 6].$$

Le cuisinier chinois peut donc espérer au minimum 785 pièces d'or.

1.2 Un exercice d'algèbre linéaire

Énoncé

Soit E un $\mathbb{K}$-espace vectoriel de dimension finie ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$). Soit $f \in \mathscr{L}(E)$ annulant le polynôme scindé sur $\mathbb{K}$ à racines simples :

$$P(X) = (X - \lambda_0)(X - \lambda_1)\dots(X - \lambda_p).$$

1. Montrer que $E = \mathrm{Ker}(f - \lambda_0 \mathrm{Id}_E) \oplus \mathrm{Ker}(f - \lambda_1 \mathrm{Id}_E) \oplus \cdots \oplus \mathrm{Ker}(f - \lambda_p \mathrm{Id}_E)$, et que pour tout $0 \leq i \leq n$, la projection q_i sur $\mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$ parallèlement à $\bigoplus_{j \neq i} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$ est un polynôme en f.

2. Pour tout $Q \in \mathbb{K}[X]$, exprimer $Q(f)$ en fonction des projecteurs $q_0, \dots, q_p$.

Polynômes de Lagrange

Avant de résoudre cet exercice, commençons par quelques rappels sur les polynômes de Lagrange.

Propriété 1

Soient $\lambda_0, \lambda_1, \dots, \lambda_p \in \mathbb{K}$ des éléments deux à deux distincts.

(1) Pour tout $0 \leq i \leq p$, il existe un unique polynôme $L_i \in \mathbb{K}_p[X]$ tel que :

$$\forall j \in [\![0, p]\!], \quad L_i(\lambda_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}$$

(2) $L_0 + L_1 + \cdots + L_p = 1$.

Preuve.

(1) On raisonne par analyse-synthèse.

- **Analyse.** Soit $P \in \mathbb{K}_p[X]$ tel que :

$$\forall j \in [\![0, p]\!], \quad P(\lambda_j) = \begin{cases} 1 & \text{si } i = j, \\ 0 & \text{si } i \neq j. \end{cases}.$$

En particulier, $\lambda_0, \dots, \lambda_{i-1}, \lambda_{i+1}, \dots, \lambda_p$ sont des racines distinctes de P, de sorte qu'il existe $Q \in \mathbb{K}[X]$ tel que :

$$P = Q \times \prod_{\substack{j=0 \\ j \neq i}}^{p} (X - \lambda_j).$$

En considérant le degré de cette expression, et en notant que $\deg(P) \leq p$, on obtient $\deg(Q) \leq 0$. Le polynôme Q est donc constant. Notons le $\lambda \in \mathbb{K}$, et récrivons l'égalité :

$$P = \lambda \times \prod_{\substack{j=0 \\ j \neq i}}^{p} (X - \lambda_j).$$

En évaluant cette égalité en $X = \lambda_i$:

$$1 = \lambda \times \prod_{\substack{j=0 \\ j \neq i}}^{p} (\lambda_i - \lambda_j), \quad \text{soit encore} \quad \lambda = \frac{1}{\prod_{\substack{j=0 \\ j \neq i}}^{p} (\lambda_i - \lambda_j)}.$$

Ainsi, si un tel polynôme P existe, il est unique, donné par l'expression :

$$P = \prod_{\substack{j=0 \\ j \neq i}}^{p} \frac{X - \lambda_j}{\lambda_i - \lambda_j}.$$

- **Synthèse.** Posons $P = \prod_{\substack{j=0 \\ j\neq i}}^{p} \frac{X-\lambda_j}{\lambda_i-\lambda_j}$. Ce polynôme est de degré p, et on vérifie qu'il satisfait bien, pour tout $j \in [\![0,p]\!]$:
$$P(\lambda_j) = \begin{cases} 1 & \text{si } i=j, \\ 0 & \text{si } i \neq j. \end{cases}.$$

(2) Le polynôme $Q = L_0 + L_1 + \cdots + L_p - 1$ admet $p+1$ racines distinctes, les λ_i pour $0 \leq i \leq p$, et est de degré au plus p. C'est donc le polynôme nul, de sorte que :
$$L_0 + L_1 + \cdots + L_p = 1.$$

□

Exercice. Montrer que $(L_0, L_1, \ldots, L_p)$ est une base de l'espace vectoriel $\mathbb{K}_p[X]$.

Polynômes d'endomorphismes

Poursuivons avec des rappels sur les polynômes d'endomorphismes.

Définition.

Soit $P(X)\sum_{k=0}^{d} a_k X^k$ un polynôme à cœfficients dans $\mathbb{K}$, et soit $f \in \mathscr{L}(E)$.
On note $P(f)$ l'endomorphisme de E défini par :
$$P(f) = \sum_{k=0}^{d} a_k f^k = a_d f^d + \cdots + a_1 f + a_0 \mathrm{Id}_E$$
où $f^0 = \mathrm{Id}_E$ et pour tout $k \in \{1, \ldots, d\}$, $f^k = \underbrace{f \circ f \circ \cdots \circ f}_{k \text{ termes}}$.

Exemples.

- Soient $f \in \mathscr{L}(E)$, $P(X) = X^2 + 3X - 10$. Alors on a $P(f) = f^2 + 3f - 10\mathrm{Id}_E$.
- Soit $f \in \mathscr{L}(E)$. En reprenant les notations et résultats obtenus précédemment, on a :
$$L_0(f) + L_1(f) + \cdots + L_p(f) = \mathrm{Id}_E.$$

Mise en garde.

Le terme constant a_0 dans P devient $a_0\mathrm{Id}_E$ dans $P(f)$.

Propriété 2

Soient $P, Q \in \mathbb{R}[X]$, $f \in \mathscr{L}(E)$ et $\alpha, \beta \in \mathbb{R}$.

(1) $(\alpha P + \beta Q)(f) = \alpha P(f) + \beta Q(f)$; (2) $(P \times Q)(f) = P(f) \circ Q(f)$.

Remarque. Il est important de bien identifier les objets mathématiques en jeu :
$$(\underbrace{P \times Q}_{\substack{\text{produit} \\ \text{de} \\ \text{polynômes}}})(f) = \underbrace{P(f) \circ Q(f)}_{\substack{\text{composition} \\ \text{d'endomorphismes}}}.$$

Mise en garde.

Pour $x \in E$, ne pas confondre $P(f)(x)$ et $P(f(x))$:

$$P(f(x)) = a_n(f(x))^n + \cdots + a_1 f(x) + a_0$$

n'a pas de sens (pas de produit dans E). Alors que $P(f)(x)$ est l'évaluation en $x \in E$ de l'endomorphisme $P(f) \in \mathscr{L}(E)$.

Propriété 3

Soit $\lambda \in \mathbb{K}$ et $x \in \mathrm{Ker}(f - \lambda \mathrm{Id}_E)$. Pour tout $P \in \mathbb{K}[X]$:

$$P(f)(x) = P(\lambda) \cdot x.$$

Preuve. Par une récurrence immédiate, on vérifie que pour tout $k \in \mathbb{N}$, $f^k(x) = \lambda^k \cdot x$.

Soit $P(X) = a_0 + a_1 X + \cdots + a_d X^d$ un polynôme. Calculons :

$$\begin{aligned} P(f)(x) &= (a_0 \mathrm{Id}_E + a_1 f + \cdots + a_d f^d)(x) = a_0 x + a_1 f(x) + \cdots + a_d f^d(x) \\ &= a_0 x + a_1 \lambda x + \cdots + a_d \lambda^d x = (a_0 + a_1 \lambda + \cdots + a_d \lambda^d) \cdot x = P(\lambda) \cdot x. \end{aligned}$$

□

Définition.

Soit $P \in \mathbb{K}[X]$ et $f \in \mathscr{L}(E)$. On dit que P est un *polynôme annulateur de* f lorsque $P(f) = 0_{\mathscr{L}(E)}$.

Exemple. Soit $q \in \mathscr{L}(E)$. p est un projecteur si, et seulement si, $X^2 - X$ est un polynôme annulateur de q. Rappelons que c'est un projecteur sur $F = \mathrm{Im}(q)$ parallèlement à $\mathrm{Ker}(q)$.

Solution de l'exercice

1. Pour tout $0 \leq i \leq p$, notons q_i l'endomorphisme $L_i(f)$ de E. On va procéder en plusieurs étapes.

   Étape 1 : les endomorphismes q_i sont des projecteurs « associés ».

   On l'a remarqué précédemment :

   $$q_0 + q_1 + \cdots + q_p = \mathrm{Id}_E. \tag{E}$$

   D'autre part, pour tout $0 \leq i, j \leq p$, $i \neq j$, le polynôme $L_i \times L_j$ admet $\lambda_0, \ldots, \lambda_p$ pour racines distinctes. Il existe donc $Q \in \mathbb{K}[X]$ tel que :

   $$L_i \times L_j = Q \times \underbrace{\prod_{k=0}^{p} (X - \lambda_k)}_{=P}.$$

   Le polynôme P étant supposé annulateur de f, on en déduit :

   $$L_i(f) \circ L_j(f) = (L_i \times L_j)(f) = (Q \times P)(f) = Q(f) \circ \underbrace{P(f)}_{0_{\mathscr{L}(E)}} = 0_{\mathscr{L}(E)}.$$

   Ainsi,

   $$q_i \circ q_j = 0_{\mathscr{L}(E)}.$$

   Soit $i \in [\![0, p]\!]$. En composant (E) à gauche par l'endomorphisme q_i, on obtient :

   $$\underbrace{q_i \circ q_0 + \cdots + q_i \circ q_{i-1}}_{=0_{\mathscr{L}(E)}} + q_i \circ q_i + \underbrace{q_i \circ q_{i+1} + \cdots + q_i \circ q_n}_{} = q_i.$$

   Ainsi, $q_i \circ q_i = q_i$, et q_i est bien un projecteur, sur $F_i = \mathrm{Im}(q_i)$ parallèlement à $G_i = \mathrm{Ker}(q_i)$.

Étape 2 : $E = \bigoplus_{i=0}^{p} \mathbf{Im}(q_i)$.

Pour tout $x \in E$, on obtient à l'aide de (E) :

$$x = q_0(x) + q_1(x) + \cdots + q_p(x) \in \sum_{i=0}^{p} \mathrm{Im}(q_i).$$

D'où l'égalité $E = \sum_{i=0}^{p} \mathrm{Im}(q_i)$.

Montrons à présent que cette somme est directe. Pour cela, soit $(y_0, y_1, \ldots, y_p) \in \mathrm{Im}(q_0) \times \mathrm{Im}(q_1) \times \cdots \times \mathrm{Im}(q_p)$ tels que :

$$y_0 + y_1 + \cdots + y_p = 0_E.$$

Montrons que $y_0 = y_1 = \cdots = y_p = 0_E$. Pour tout $0 \leq j \leq p$, il existe $x_j \in E$ tel que $y_j = q_j(x_j)$. L'égalité précédente se récrit :

$$q_0(x_0) + q_1(x_1) + \cdots + q_p(x_p) = 0_E.$$

Fixons $0 \leq i \leq p$, et composons cette égalité par l'endomorphisme q_i :

$$0_E = q_i \circ q_0(x_0) + \cdots + q_i \circ q_i(x_i) + \cdots + q_p(x_p).$$

À l'aide des résultats de l'étape 1, on en déduit :

$$0_E = 0_E + \cdots + q_i \circ q_i(x_i) + \cdots + 0_E = q_i \circ q_i(x_i) = q_i(x_i) = y_i.$$

Ceci étant vrai pour tout $0 \leq i \leq p$, on obtient bien $y_0 = y_1 = \cdots = y_p = 0_E$. La somme $\sum_{i=0}^{p} \mathrm{Im}(q_i)$ est donc directe.

On conclut que $E = \bigoplus_{i=0}^{p} \mathrm{Im}(q_i)$.

Étape 3 : $F_i = \mathbf{Ker}(f - \lambda_i \mathbf{Id}_E)$ et $G_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^{p} \mathbf{Ker}(f - \lambda_j \mathbf{Id}_E)$.

Soit $i \in [\![0, p]\!]$. Montrons que $F_i = \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$ par double inclusion.

- $\subset$ Soit $y \in F_i = \mathrm{Im}(q_i)$. Il existe donc $x \in E$ tel que $y = q_i(x)$. Montrons que $y \in \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$:

  $$(f - \lambda_i \mathrm{Id}_E)(y) = (f - \lambda_i \mathrm{Id}_E) \circ q_i(x) = (f - \lambda_i \mathrm{Id}_E) \circ L_i(f)(x) = [(X - \lambda_i) \times L_i](f)(x).$$

  Le polynôme $(X - \lambda_i) \times L_i$ étant un multiple de P, annulateur de f, il suit :

  $$(f - \lambda_i \mathrm{Id}_E)(y) = 0_{\mathscr{L}(E)}(x) = 0_E.$$

  Ainsi y appartient bien à $\mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$. D'où l'inclusion $F_i \subset \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$.
- $\supset$ Soit $x \in \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$. Calculons :

  $$q_i(x) = L_i(f)(x) = L_i(\lambda_i)x = x.$$

  En particulier, x appartient à $\mathrm{Im}(q_i)$. D'où l'inclusion réciproque $\mathrm{Ker}(f - \lambda_i \mathrm{Id}_E) \subset F_i$.

Ainsi, $F_i = \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$ et $E = \bigoplus_{i=0}^{p} \mathrm{Im}(q_i) = \bigoplus_{i=0}^{p} \mathrm{Ker}(f - \lambda_i \mathrm{Id}_E)$.

Reste à montrer l'égalité $G_i = \bigoplus_{\substack{j=0 \\ j \neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$. On procède également par double inclusion.

$\subset$ Soit $x \in G_i = \mathrm{Ker}(q_i)$. Toujours avec l'égalité (E) :

$$x = q_0(x) + \cdots + q_{i-1}(x) + \underbrace{q_i(x)}_{=0_E} + q_{i+1}(x) + \cdots + q_p(x) \in \bigoplus_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Im}(q_j) = \bigoplus_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E).$$

D'où l'inclusion $G_i \subset \bigoplus_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$.

$\supset$ Réciproquement, prenons $x \in \bigoplus_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$. Il existe $(x_0, \ldots, x_{i-1}, x_{i+1}, \ldots, x_p) \in \prod_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$ tel que :

$$x = x_0 + \cdots + x_{i-1} + x_{i+1} + \cdots + x_p.$$

Appliquons à cette égalité l'endomorphisme q_i :

$$\begin{aligned} q_i(x) &= q_i(x_0) + \cdots + q_i(x_{i-1}) + q_i(x_{i+1}) + \cdots + q_i(x_p) \\ &= \underbrace{L_i(\lambda_0)}_{=0} x_0 + \cdots + \underbrace{L_i(\lambda_{i-1})}_{=0} x_{i-1} + \underbrace{L_i(\lambda_{i+1})}_{=0} x_{i+1} + \cdots + \underbrace{L_i(\lambda_p)}_{=0} x_p = 0_E. \end{aligned}$$

D'où l'inclusion réciproque.

Ainsi $G_i = \bigoplus_{\substack{j=0\\ j\neq i}}^{p} \mathrm{Ker}(f - \lambda_j \mathrm{Id}_E)$.

2. Soit $x \in E$. D'après la question précédente, il existe un unique $(p+1)$-uplet $(x_0, \ldots, x_p) \in \mathrm{Ker}(f - \lambda_0 \mathrm{Id}_E) \times \cdots \times \mathrm{Ker}(f - \lambda_p \mathrm{Id}_E)$ tel que :

$$x = x_0 + x_1 + \cdots + x_p.$$

Appliquons f à cette égalité :

$$\begin{aligned} f(x) &= f(x_0) + f(x_1) + \cdots + f(x_p) = \lambda_0 x_0 + \lambda_1 x_1 + \cdots + \lambda_p x_p \\ &= \lambda_0 q_0(x) + \lambda_1 q_1(x) + \cdots + \lambda_p q_p(x). \end{aligned}$$

Ceci étant vrai pour tout vecteur $x \in E$, on obtient l'égalité suivante dans $\mathscr{L}(E)$:

$$f = \lambda_0 q_0 + \lambda_1 q_1 + \cdots + \lambda_p q_p.$$

On vérifie alors par une récurrence immédiate que pour tout $k \in \mathbb{N}$:

$$f^k = \lambda_0^k q_0 + \lambda_1^k q_1 + \cdots + \lambda_p^k q_p.$$

Par combinaison linéaire, on en déduit pour tout $Q \in \mathbb{K}[X]$:

$$Q(f) = Q(\lambda_0) q_0 + Q(\lambda_1) q_1 + \cdots + Q(\lambda_p) q_p.$$

2 Rappels et compléments sur les anneaux

Ces deux exercices peuvent être traités de manière unifiée, dans un cadre plus théorique. C'est l'objet de la suite de ce document.

2.1 Anneaux

Définition.

Soit A un ensemble muni de deux lois internes notées « + » et « × ». On dit que $(A, +, \times)$ est un *anneau* si :

(i) $(A, +)$ est un groupe abélien ;

(ii) la loi $\times$ est associative ;

(iii) la loi $\times$ est distributive par rapport à la loi $+$.

Si la loi $\times$ admet un élément neutre, on parle d'anneau *unitaire*. Si la loi $\times$ est commutative, on parle d'anneau *commutatif*.

Notation. Le neutre pour la loi $+$ sera noté 0_A ou simplement 0, celui pour la loi $\times$ sera noté 1_A ou 1. Dans le suite, on supposera que $0_A \neq 1_A$.

Exemples.

- $(\mathbb{Z}, +, \times)$, $(\mathbb{K}[X], +, \times)$ (où $\mathbb{K}$ corps) sont des anneaux commutatifs et unitaires.
- $(\mathscr{M}_n(\mathbb{R}), +, \times)$ est un anneau unitaire non commutatif.

Dans toute la suite, $(A, +, \times)$ désigne un anneau commutatif et unitaire.

2.2 Idéaux

Définition.

Soit $I \subset A$. On dit que I est un *idéal* de l'anneau A si :

(i) $(I, +)$ est un sous-groupe de $(A, +)$,

(ii) I est *absorbant* : $\forall (x, a) \in I \times A$, $a \times x \in I$.

On dit que I est un idéal *propre* si de plus $I \neq A$.

Remarques.

- Un idéal est un sous-anneau.
- $\{0_A\}$ et A sont des idéaux de A.
- Pour tout $x \in A$, l'ensemble $xA = \{x \times a,\ a \in A\}$ est un idéal de A. Un idéal de cette forme est dit *principal*. On le note aussi (x).

Remarque. On peut montrer que pour les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$, tous les idéaux sont principaux.

Propriété 4

Soit I un idéal de A.

$$I = A \quad \Leftrightarrow \quad 1_A \in I.$$

Preuve. Le sens direct est immédiat. Réciproquement, supposons que $1_A \in I$. Pour tout $a \in A$,

$$a = a \times 1_A \in I$$

car I est absorbant. D'où l'inclusion $A \subset I$, et donc l'égalité $A = I$. □

Propriété 5

- Une intersection quelconque d'idéaux de A est un idéal de A.
- Si $I_1, \ldots, I_k$ sont des idéaux de A, la *somme* de $I_1, \ldots, I_k$, notée $\sum_{j=1}^{k} I_j$ et définie par :

$$\sum_{j=1}^{k} I_j = \{i_1 + \cdots + i_k,\ \forall j \in [\![1, k]\!],\ i_j \in I_j\}$$

est un idéal de A.

Preuve. Laissée en exercice. □

3 Théorème des restes chinois, version congruence

3.1 Idéaux premiers entre eux

Définition.

- Deux idéaux I et J de A sont dits *premiers entre eux* (ou *étrangers*) si $A = I + J$.
- Soit $n \geq 2$. n idéaux $I_1, \ldots, I_n$ sont dits *premiers entre eux deux à deux* si, pour tout $1 \leq j < k \leq n$, I_j et I_k sont premiers entre eux.
- Soit $n \geq 2$. n idéaux $I_1, \ldots, I_n$ sont dits *premiers entre eux dans leur ensemble* si $I_1 + \cdots + I_n = A$.

Remarques.

- Si $I_1, \ldots, I_n$ sont deux à deux premiers entre eux, alors ils sont premiers entre eux dans leur ensemble. La réciproque est fausse en général.
- $I_1, \ldots, I_n$ sont premiers entre eux dans leur ensemble si, et seulement si, $1_A \in I_1 + \cdots + I_n = A$, ce qui équivaut encore à l'existence d'un n-uplet $(i_1, \ldots, i_n) \in I_1 \times \cdots \times I_n$ satisfaisant :

$$1_A = i_1 + \cdots + i_n.$$

Propriété 6

Soit $n \geq 2$, et $I_1, \ldots, I_n$ des idéaux de A premiers entre eux deux à deux. Pour tout $1 \leq i \leq n$, posons $J_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j$. Alors les idéaux $J_1, \ldots, J_n$ sont premiers entre eux dans leur ensemble.

Preuve. On va procéder par récurrence sur $n \geq 2$.

- La propriété est trivialement vérifiée lorsque $n = 2$, puisqu'alors $J_1 = I_2$ et $J_2 = I_1$.
- Soit $n \geq 2$. Supposons la propriété vraie au rang n, et montrons la au rang $n+1$. Soient pour cela $I_1, \ldots, I_{n+1}$ des idéaux de A deux à deux premiers entre eux. Posons $K_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j$. Par hypothèse de récurrence, les idéaux $K_1, \ldots, K_n$ sont premiers entre eux dans leur ensemble, de sorte qu'il existe $(k_1, \ldots, k_n) \in K_1 \times \cdots \times K_n$ tel que :
$$k_1 + \cdots + k_n = 1_A.$$
D'autre part, puisque pour tout $1 \leq i \leq n$, I_i et I_{n+1} sont premiers entre eux, il existe $a_i \in I_i$ et $b_i \in I_{n+1}$ tels que :
$$a_i + b_i = 1_A.$$
Dès lors, on en déduit l'égalité :
$$k_1 \times (a_1 + b_1) + \cdots + k_n(a_n + b_n) = 1_A$$
qui se récrit :
$$(k_1 \times a_1 + \cdots + k_n \times a_n) + k_1 \times b_1 + \cdots + k_n b_n = 1_A.$$
Pour tout $1 \leq i \leq n$, k_i appartient à $K_i = \bigcap_{\substack{j=1 \\ j \neq i}}^{n} I_j$ et a_i à I_i. Par absorption, le produit $k_i \times a_i$ appartient donc à l'idéal $J_{n+1} = \bigcap_{\substack{j=1 \\ j \neq n+1}}^{n+1} I_j$, et par stabilité par somme :
$$(k_1 \times a_1 + \cdots + k_n \times a_n) \in J_i.$$

De même pour tout $1 \leq i \leq n$, $k_i \times b_i$ appartient à l'idéal $J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n+1} I_j$. On a ainsi montré que $1_A \in J_1 + \cdots + J_{n+1}$, soit en d'autres termes que $J_1, \ldots, J_{n+1}$ sont premiers entre eux dans leur ensemble.

□

Exemples.

- Les entiers $6, 11, 17$ étant deux à deux premiers entre eux, il en est de même des idéaux $I_1 = 6\mathbb{Z}$, $I_2 = 11\mathbb{Z}$ et $I_3 = 17\mathbb{Z}$. Par la propriété précédente, les idéaux $J_3 = 6\mathbb{Z} \cap 11\mathbb{Z} = (6 \times 11)\mathbb{Z}$, $J_2 = 6\mathbb{Z} \cap 17\mathbb{Z} = (6 \times 17)\mathbb{Z}$ et $J_1 = 11\mathbb{Z} \cap 17\mathbb{Z} = (11 \times 17)\mathbb{Z}$ sont premiers entre eux dans leur ensemble. D'où l'existence d'un triplet $(j_1, j_2, j_3) \in J_1 \times J_2 \times J_3)$ tel que :
$$j_1 + j_2 + j_3 = 1.$$
Déterminons de tels éléments. Nous avions remarqué que :
$$1 = 17 \times 2 - 3 \times 11 \quad \text{et} \quad 1 = 17 \times 11 - 31 \times 6.$$
En substituant, on obtient :
$$\begin{aligned} 1 &= 17 \times 11 - 31 \times 6 \times (17 \times 2 - 3 \times 11) \\ &= 17 \times 11 - 62 \times 6 \times 17 + 93 \times 6 \times 11. \end{aligned}$$
Ainsi, les entiers $j_3 = 17 \times 11$, $j_2 = -62 \times 6 \times 17$ et $j_1 = 93 \times 6 \times 11$ conviennent.
- Les polynômes $(X - \lambda_0), \ldots, (X - \lambda_p)$ étant deux à deux premiers entre eux, il en est de même des idéaux $I_j = \langle X - \lambda_j \rangle$. Là aussi par la propriété précédente, les idéaux $J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j = \langle \prod_{\substack{j=1 \\ j\neq i}}^{n} (X - \lambda_j) \rangle$ sont premiers entre eux dans leur ensemble. On l'avait établi (sans le dire en ces termes), puisque :
$$1_{\mathbb{K}[X]} = L_0 + \cdots + L_n \in I_0 + \cdots + I_p.$$

3.2 Théorème des restes chinois, version congruence

Définition.

Soit I un idéal de A, et soient $x, y \in A$. On dit que x est congru à y modulo I, et on note $x \equiv y[I]$, si $x - y \in I$.

Exemple. Pour $A = \mathbb{Z}$ et $I = n\mathbb{Z}$ (avec $n \in \mathbb{N}^*$) :
$$x \equiv y[n\mathbb{Z}] \quad \Leftrightarrow \quad x - y \in n\mathbb{Z} \quad \Leftrightarrow \quad n \text{ divise } x - y \quad \Leftrightarrow \quad x \equiv y[n].$$

Théorème 7 (des restes chinois, version congruence)

Soient $n \geq 2$, et $I_1, \ldots, I_n$ des idéaux de A premiers entre eux deux à deux. Alors :

(1) pour tout $x_1, \ldots, x_n \in A$, il existe $x \in A$ tel que $x \equiv x_j[I_j]$ pour tout $1 \leq j \leq n$;

(2) pour tout $y \in A$:
$$(\forall j \in [\![1, n]\!],\ y \equiv x_j[I_j]) \quad \Leftrightarrow \quad x \equiv y[I_1 \cap \cdots \cap I_n].$$

Preuve.

(1) Puisque les idéaux $I_1, \ldots, I_n$ sont premiers entre eux deux à deux, les idéaux $J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j$ pour $1 \leq i \leq n$ sont premiers entre eux dans leur ensemble. Il en résulte l'existence d'un n-uplet $(j_1, \ldots, j_n) \in J_1 \times \cdots \times J_n$ tel que :
$$j_1 + \cdots + j_n = 1_A.$$

Remarquons dès lors que pour tout $1 \leq i \leq n$, j_i est solution du système de congruences :

$$x \equiv 1[I_i] \text{ et pour tout } 1 \leq k \neq i \leq n,\ x \equiv 0[I_k].$$

Il est alors aisé d'exhiber une solution du système de congruence de départ. Posons pour cela $x = x_1 \times j_1 + \cdots + x_n \times j_n$, et montrons qu'un tel élément convient. Pour tout $1 \leq i \leq n$:

$$\begin{aligned} x - x_i &= x_1 j_1 + \cdots + x_{i-1} j_{i-1} + x_i(j_i - 1_A) + x_{i+1} j_{i+1} + \cdots + x_n j_n \\ &= (x_1 - x_i) j_1 + \cdots + (x_{i-1} - x_i) j_{i-1} + (x_{i+1} - x_i) j_{i+1} + \cdots + (x_n - x_i) j_n \in I_i \end{aligned}$$

(2) On procède par double implication.

□

Méthode. Résolution d'un système de congruences.

Soient $n \geq 2$, et $I_1, \ldots, I_n$ des idéaux de A premiers entre eux deux à deux. Pour résoudre le système de congruences :

$$\begin{cases} x \equiv x_1[I_1] \\ \quad \cdots \\ x \equiv x_n[I_n] \end{cases},$$

on procèdera comme suit :

- *on définit les idéaux $J_i = \bigcap_{j \neq i} I_j$ pour tout $1 \leq i \leq n$;*
- *les idéaux J_i étant premiers entre eux dans leur ensemble, il existe un n-uplet $(j_1, \ldots, j_n) \in J_1 \times \cdots \times J_n$ tel que :*

  $$j_1 + \cdots + j_n = 1_A. \qquad (*)$$

  Un tel n-uplet (de Bezout) s'obtiendra par l'algorithme d'Euclide étendu lorsque A sera supposé euclidien ;
- *Pour tout $i \in [\![1, n]\!]$, on a d'après $(*)$ que :*

  $$\forall k \in [\![1, n]\!], \quad j_i = \begin{cases} 1\ [I_i] & \text{si } k = i \\ 0\ [I_k] & \text{si } k \neq i \end{cases}.$$

  Une solution du système de congruences est $x = x_1 j_1 + \cdots + x_n j_n$, et est unique modulo $I_1 \cap \cdots \cap I_n$.

Exemples.

- Revenons à la résolution du système de congruence (dans $\mathbb{Z}$) :

  $$\begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \\ x \equiv 5[6] \end{cases}.$$

  En reprenant la méthode proposée ci-dessus, nous avons déjà introduit les idéaux I_j et J_i, et obtenu les éléments j_1, j_2, j_3 tels que :

  $$j_1 + j_2 + j_3 = 1.$$

  Une solution du système de congruence est donc :

  $$x = 3 \times j_1 + 4 \times j_2 + 5 \times j_3,$$

  et elle est unique modulo $I_1 \cap I_2 \cap I_3 = 17 \times 11 \times 6\mathbb{Z}$. Explicitons-là :

  $$\begin{aligned} x &\equiv 5 \times 11 \times 17 - 62 \times 4 \times 17 \times 6 + 3 \times 93 \times 11 \times 6[17 \times 11 \times 6] \\ &\equiv -11 \times 17 - (-4) \times 4 \times 17 \times 6 + 3 \times 8 \times 11 \times 6[17 \times 11 \times 6] \\ &\equiv -11 \times 17 + 5 \times 17 \times 6 + 7 \times 11 \times 6[17 \times 11 \times 6] \\ &\equiv 19 \times 17 + 42 \times 11[17 \times 11 \times 6] \equiv 785[17 \times 11 \times 6] \end{aligned}$$

- Dans l'anneau $A = \mathbb{K}[X]$, en conservant les notations introduites précédemment, résolvons le système de congruences suivant (dans l'anneau $A = \mathbb{K}[X]$) :

$$\begin{cases} Q \equiv \lambda_0[I_1] \\ \quad \dots \\ Q \equiv \lambda_p[I_p] \end{cases}.$$

Remarquons que le $(p+1)$-uplet $(j_0, \dots, j_p) = (L_0, \dots, L_p) \in J_0 \times \dots \times J_p$ satisfait bien :

$$j_0 + \dots + j_p = 1_A.$$

Une solution du système de congruences est donc :

$$Q = \lambda_0 j_0 + \dots + \lambda_p j_p = \lambda_0 L_0 + \dots + \lambda_p L_p,$$

et cette solution est unique modulo $I_0 \cap \dots \cap I_p$, c'est-à-dire à un multiple de $P = (X - \lambda_0) \dots (X - \lambda_p)$ près.

4 Théorème des restes chinois, version anneaux quotients

4.1 Quotient d'un anneau par un idéal

Propriété 8

Soit I un idéal de A.

(1) La relation de congruence modulo I est une relation d'équivalence sur A.

(2) Cette relation d'équivalence est compatible avec la somme et le produit de A.

Preuve.

(1) On vérifie que cette relation est :

- *réflexive :* pour tout $x \in A$, $x - x = 0_A$ appartient à I puisque $(I, +)$ est un sous-groupe de $(A, +)$, de sorte que $x \equiv x[I]$
- *symétrique :* pour tout $x, y \in A$ tels que $x \equiv y[I]$, $x - y$ appartient à I. $(I, +)$ étant un sous-groupe de $(A, +)$, $y - x = -(x - y)$ appartient à I, ce qui s'écrit $y \equiv x[I]$.
- *transitive :* soient $x, y, z \in A$ tels que $x \equiv y[I]$ et $y \equiv z[I]$. Ceci se récrit $x - y \in I$ et $y - z \in I$. Toujours parce que $(I, +)$ est un sous-groupe de $(A, +)$, $x - z = (x - y) + (y - z)$ appartient à I. Ainsi, $x \equiv z[I]$ et la relation de congruence est bien transitive.

(2) Vérifions-le pour le produit par exemple. Prenons x, x', y, y' des éléments de A tels que $x \equiv x'[I]$ et $y \equiv y'[I]$. Alors $x - x' \in I$ et $y - y' \in I$, d'où :

$$\begin{aligned} x \times y - x' \times y' &= x \times y - x \times y' + x \times y' - x' \times y' \\ &= x \times \underbrace{(y - y')}_{\in I} + \underbrace{(x - x')}_{\in I} \times y' \in I \end{aligned}$$

Ainsi $x \times y \equiv x' \times y'[I]$ et la relation d'équivalence est compatible avec le produit de A. On vérifie de même pour la somme de A.

□

Notation. Pour $x \in A$, on notera $\overline{x}$ (ou $\overline{x}^I$ s'il y a une ambiguïté) la classe d'équivalence de x pour la relation de congruence modulo I. Ainsi :

$$\overline{x} = \{y \in A,\ y - x \in I\} = x + I.$$

On notera A/I l'ensemble des classes d'équivalences sur A pour cette relation d'équivalence.

Propriété 9

Le quotient A/I, muni des opérations

$$\overline{x} + \overline{y} = \overline{x+y} \quad \text{et} \quad \overline{x} \times \overline{y} = \overline{x \times y}$$

est un anneau commutatif et unitaire, appelé *anneau quotient de A par I*.

Preuve. Ces lois de compositions internes sur A/I sont bien définies puisque la relation de congruence modulo I est compatible avec la somme et le produit de A. Les axiomes définissant un anneau commutatif unitaire sont alors trivialement vérifiés pour $(A/I, +, \times)$ puisqu'ils le sont pour $(A, +, \times)$. □

4.2 Compléments sur les anneaux

Définition.

Soient A, B des anneaux unitaires. Une application $f : A \to B$ est un *morphisme d'anneaux* si :

- $\forall x, y \in A,\ f(x+y) = f(x) + f(y)$,
- $\forall x, y \in A,\ f(x \times y) = f(x) \times f(y)$,
- $f(1_A) = 1_B$.

Lorsque f est bijective, on parle d'*isomorphisme d'anneaux*.

Propriété 10

Soient $A_1, \ldots, A_n$ des anneaux commutatifs et unitaires. Alors $A_1 \times \cdots \times A_n$ muni des opérations suivantes :

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n)$$

et

$$(a_1, \ldots, a_n) \times (b_1, \ldots, b_n) = (a_1 \times b_1, \ldots, a_n \times b_n)$$

est un anneau commutatif et unitaire.

Preuve. On vérifie sans difficulté que les axiomes définissant un anneau commutatif unitaire sont bien satisfaites. □

4.3 Théorème des restes chinois, version anneaux quotients

Propriété 11

Soient $n \geq 2$ et $I_1, \ldots, I_n$ des idéaux de A deux à deux premiers entre eux. On dispose de l'isomorphisme d'anneaux :

$$A/I_1 \cap \cdots \cap I_n \simeq (A/I_1) \times \cdots \times (A/I_n)\,.$$

Preuve. On considère l'application :

$$\theta : A/I_1 \cap \cdots \cap I_n \to (A/I_1) \times \cdots \times (A/I_n)$$

qui à un élément $x + I_1 \cap \cdots \cap I_n$ associe le n-uplet $(x + I_1, \ldots, x + I_n)$. Commençons par remarquer que cette application est bien définie, c'est-à-dire que l'image de $x + I_1 \cap \cdots \cap I_n$ par θ est indépendante du représentant choisi dans la classe de $x + I$. Prenons pour cela $x' \in A$ tel que $x - x' \in I_1 \cap \cdots \cap I_n$. On a alors pour tout $1 \leq j \leq n$:

$$x - x' \in I_1 \cap \cdots \cap I_n \subset I_j.$$

L'application θ est donc bien définie. Elle est bijective par le théorème des restes chinois, version congruence. Et on vérifie sans aucune difficulté que c'est bien un morphisme d'anneaux. □

Remarque. On peut de plus expliciter la bijection réciproque. En reprenant les notations introduites auparavant, on a établi l'existence d'éléments $j_i \in J_i = \bigcap_{\substack{j=1 \\ j\neq i}}^{n} I_j$ tels que :

$$j_1 + \cdots + j_n = 1_A.$$

La bijection réciproque de θ est donnée par :

$$\theta^{-1} : \begin{cases} (A/I_1) \times \cdots \times (A/I_n) & \to & A/I_1 \cap \cdots \cap I_n \\ \\ (\overline{x_1}^{I_1}, \ldots, \overline{x_n}^{I_n}) & \mapsto & \overline{x_1 j_1 + \cdots + x_n j_n}^{I_1 \cap \cdots \cap I_n} \end{cases}.$$

Exemple. Les entiers $6, 11$ et 17 étant premiers entre eux deux à deux, les idéaux principaux associés le sont aussi, et l'on dispose de l'isomorphisme :

$$\mathbb{Z}/(6 \times 11 \times 17)\mathbb{Z} \simeq (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}) \times (\mathbb{Z}/17\mathbb{Z}).$$

Pour aller plus loin. Notons $\mathbb{K}[f] = \{Q(f),\ Q \in \mathbb{K}[X]\}$ le sous-anneau de $\mathscr{L}(E)$ des polynômes en f. Par le premier théorème d'isomorphisme (en supposant que $P = (X - \lambda_0)(X - \lambda_1)\ldots(X - \lambda_p)$ est le polynôme minimal de f) :

$$\mathbb{K}[f] \simeq \mathbb{K}[X]/\langle P \rangle.$$

Par le théorème des restes chinois, on obtient :

$$\mathbb{K}[f] \simeq (\mathbb{K}[X]/\langle X - \lambda_0 \rangle) \times \cdots \times (\mathbb{K}[X]/\langle X - \lambda_p \rangle).$$

Et puisque $\mathbb{K}[X]/\langle X - \lambda_0 \rangle \simeq \mathbb{K}$ (toujours par le premier théorème d'isomorphisme), on peut conclure que :

$$\mathbb{K}[f] \simeq \mathbb{K} \times \cdots \times \mathbb{K} = \mathbb{K}^{p+1}.$$

Notons que cet isomorphisme aurait pu être identifié plus tôt, puisque pour tout $Q \in \mathbb{K}[X]$:

$$Q(f) = Q(\lambda_0)q_0 + \cdots + Q(\lambda_p)q_p.$$

L'isomorphisme est donné par l'application $Q(f) \in \mathbb{K}[f] \mapsto (Q(\lambda_0), \ldots, Q(\lambda_p)) \in \mathbb{K}^{p+1}$.