Université Claude Bernard–Lyon I
Agrégation interne de Mathématiques : Oral 1
Année 2011–2012

Lemme des noyaux

Prologue : projecteurs
Soit E un espace vectoriel sur un corps $\mathbb{K}$. Tout d'abord, si on se donne une décomposition de E comme somme de deux supplémentaires, $E = E_1 \oplus E_2$, on construit un projecteur π_1 (et même un deuxième π_2) de la façon suivante. Tout vecteur v de E s'écrit de façon unique $v = v_1 + v_2$ avec $v_1 \in E_1$ et $v_2 \in E_2$. On pose alors : $\pi_1(v) = v_1$ et $\pi_2(v) = v_2$. On appelle π_1 le projecteur sur E_1 parallèlement à E_2. On a les propriétés suivantes :

– L'application π_1 est linéaire. C'est un exercice de routine de le vérifier.
– On a : $\pi_1^2 = \pi_1 = \mathrm{Id} - \pi_2$. La première égalité provient de l'écriture, valable pour tout v de E : $\pi_1(v) = \pi_1(v) + 0$, avec $\pi_1(v) \in E_1$ et $0 \in E_2$; la deuxième provient de l'égalité $v = \pi_1(v) + \pi_2(v)$.
– On a : $E_2 = \mathrm{Ker}\,\pi_1 = \mathrm{Im}\,\pi_2$ et, de même, $E_1 = \mathrm{Ker}\,\pi_2 = \mathrm{Im}\,\pi_1$. En effet, si $v \in E_2$, alors l'écriture $v = 0+v$ avec $0 \in E_1$ et $v \in E_2$ donne, par définition de π_1 : $\pi_1(v) = 0$. Si $v \in \mathrm{Ker}\,\pi_1$, on écrit $v = v - \pi_1(v) + \pi_1(v) = \pi_2(v) + 0$. Enfin, si $v \in \mathrm{Im}\,\pi_2$, alors $v \in E_2$ par construction de π_2.

Inversement, soit π un idempotent, c'est-à-dire un endomorphisme tel que $\pi^2 = \pi$. Pour $v \in E$, écrivons :
$$(*) \qquad v = \pi(v) + (v - \pi(v)).$$
L'égalité $\pi = \pi^2$ entraîne que $v - \pi(v) \in \mathrm{Ker}\,\pi$. On en déduit : $\mathrm{Im}\,\pi + \mathrm{Ker}\,\pi = E$. Si $v \in \mathrm{Ker}\,\pi \cap \mathrm{Im}\,\pi$, on a : $v = \pi(w)$ pour w convenable et $0 = \pi(v) = \pi^2(w) = \pi(w) = v$, si bien que $\mathrm{Ker}\,\pi$ et $\mathrm{Im}\,\pi$ sont toujours en somme directe. [1] Si on appelle π_1 le projecteur sur $E_1 = \mathrm{Im}\,\pi$ parallèlement à $E_2 = \mathrm{Ker}\,\pi$, on constate grâce à $(*)$ que $\pi_1 = \pi$.

Remarques : On vient de démontrer à la main le lemme des noyaux pour le polynôme $X^2 - X$... D'autre part, en réunissant une base de $\mathrm{Im}\,\pi$ et une base de $\mathrm{Ker}\,\pi$, on constate que π est diagonalisable et que sa trace est égale à son rang.

Lemme des noyaux

Théorème (Lemme des noyaux) *Soit φ un endomorphisme d'un espace vectoriel E, P_1 et P_2 deux polynômes premiers entre eux. Alors :*
$$\mathrm{Ker}\, P_1P_2(\varphi) = \mathrm{Ker}\, P_1(\varphi) \oplus \mathrm{Ker}\, P_2(\varphi).$$
De plus, les restriction à $\mathrm{Ker}\, P_1P_2(\varphi)$ des projections sur un noyau parallèlement à l'autre sont des polynômes en φ.

Démonstration. Quitte à remplacer E par $\mathrm{Ker}\, P_1P_2(\varphi)$ et φ par sa restriction à ce noyau, on peut supposer que P_1P_2 annule φ.
Comme P_1 et P_2 sont premiers entre eux, on peut trouver deux polynômes U_1 et U_2 tels que
$$P_1U_1 + P_2U_2 = 1,$$

1. En dimension finie, par le théorème du rang, on a : $\dim \mathrm{Ker}\,\pi + \mathrm{rg}\,\pi = \dim E$, si bien que $\mathrm{Ker}\,\pi$ et $\mathrm{Im}\,\pi$ sont en somme directe.

d'où on tire :

$$P_1U_1(\varphi) + P_2U_2(\varphi) = \mathrm{Id}.$$

Notons

$$\pi_1 = P_2U_2(\varphi), \quad \pi_2 = P_1U_2(\varphi).$$

Vu que $P_1P_2(\varphi) = 0$, on calcule :

$$\pi_1\pi_2 = U_1U_2P_1P_2(\varphi) = 0,$$

puis

$$\pi_1^2 = \pi_1\pi_1 = \pi_1(\mathrm{Id} - \pi_2) = \pi_1, \quad \pi_2^2 = \pi_2(\mathrm{Id} - \pi_1) = \pi_2.$$

Par suite, π_1 et π_2 sont des projecteurs. De plus, la relation $\pi_2 = \mathrm{Id} - \pi_1$ entraîne que le noyau de l'un est l'image de l'autre. Cela entraîne que $\operatorname{Im} U_1P_1(\varphi)$ et $\operatorname{Im} U_2P_2(\varphi)$ sont supplémentaires. Pour terminer la preuve, il suffit de vérifier que l'on a :

$$\operatorname{Ker} P_1(\varphi) = \operatorname{Im} U_2P_2(\varphi) \quad \text{et} \quad \operatorname{Ker} P_2(\varphi) = \operatorname{Im} U_1P_1(\varphi).$$

D'une part, si un vecteur v s'écrit $U_2P_2(\varphi)(v_0)$, alors $P_1(\varphi)(v) = U_2P_1P_2(\varphi)(v_0) = 0$. D'autre part, si $P_1(\varphi)(v) = 0$, alors :

$$v = U_1P_1(\varphi)(v) + U_2P_2(\varphi)(v) = U_2P_2(\varphi)(v) \in \operatorname{Im} U_2P_2(\varphi).$$

Remarque : la preuve précédente *est* la preuve classique mais la présentation fait la part belle aux projecteurs/idempotents. La dernière assertion du théorème est souvent oubliée dans l'énoncé alors qu'elle est très utile pour :
– la décomposition de Dunford (c'est crucial),
– (plus anecdotique) calculer l'exponentielle ou une racine carrée ou je ne sais quelle fonction d'un endomorphisme quand on en connaît un polynôme annulateur.

Appendice : comme il restait de la place en bas de la page 2, j'ai eu l'idée d'ajouter ce qui suit. Mais ça débordait alors j'ai préféré passer à la page.

Le lemme chinois, c'est pareil que le lemme des noyaux !
Prouvons le lemme chinois de la même façon que le lemme des noyaux.

Théorème (Lemme chinois) *Soit a_1 et a_2 deux entiers premiers entre eux. Alors on a un isomorphisme de $\mathbb{Z}$-modules ou même d'anneaux :*

$$\mathbb{Z}/a_1a_2\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z}.$$

La preuve va rendre à peu près explicite l'isomorphisme. Soit u_1 et u_2 deux entiers tels que

$$a_1u_1 + a_2u_2 = 1.$$

Posons [2]

$$e_1 = a_2u_2, \qquad e_2 = a_1u_1.$$

Dans $\mathbb{Z}/a_1a_2\mathbb{Z}$, on a : $a_1a_2 = 0$ donc :

$$e_1e_1 = u_1u_2a_1a_2 = 0,$$

puis

$$e_1^2 = e_1(1-e_2) = e_1, \quad e_2^2 = e_2(1-e_1) = e_2.$$

Posons [3] $I_1 = e_1\mathbb{Z}/a_1a_2\mathbb{Z}$ et $I_2 = e_2\mathbb{Z}/a_1a_2\mathbb{Z}$. Au niveau « linéaire », on a :

$$\mathbb{Z}/a_1a_2\mathbb{Z} = I_1 \oplus I_2,$$

dans le sens où tout élément de $\mathbb{Z}/a_1a_2\mathbb{Z}$ s'écrit de façon unique comme somme d'un élément de I_1 et d'un élément de I_2. En effet, si v est un élément de $\mathbb{Z}/a_1a_2\mathbb{Z}$, on a : $v = e_1v + e_2v$, où $e_1 \in I_1$ et $e_2 \in I_2$, d'où l'existence ; de plus, si $v \in I_1 \cap I_2$, on a d'une part : $v = e_1w_1$ pour w_1 convenable donc $e_1v = e_1^2w_1 = e_1w_1 = v$ et d'autre part : $v = e_2w_2$ pour w_2 convenable, si bien que $v = e_1v = e_1e_2w_2 = 0$.
De plus, l'application $\mathbb{Z} \to \mathbb{Z}/a_1a_2\mathbb{Z}$, $n \mapsto a_1n$ est surjective et son noyau est $a_2\mathbb{Z}$, d'où une identification $\mathbb{Z}/a_2\mathbb{Z} \to \alpha_1\mathbb{Z}/a_1a_2\mathbb{Z}$. Or la relation de Bézout ci-dessus exprime en particulier que u_1 et a_2 sont premiers entre eux. La multiplication par u_1 est un automorphisme (de ce qu'on veut, groupe abélien, $\mathbb{Z}$-module ou anneau ; son inverse est... la multiplication par a_1), il vient alors : $u_1\mathbb{Z}/a_2\mathbb{Z} \simeq \mathbb{Z}/a_2\mathbb{Z}$. En composant, on obtient :

$$\mathbb{Z}/a_2\mathbb{Z} \simeq u_1\mathbb{Z}/a_2\mathbb{Z} \simeq a_1u_1\mathbb{Z}/a_1a_2\mathbb{Z} = e_2\mathbb{Z}/a_1z_2\mathbb{Z} = I_2.$$

De même, $\mathbb{Z}/a_1\mathbb{Z} \simeq I_1$, ce qui prouve la version linéaire du lemme chinois.
En fait, I_1 et I_2 sont des idéaux et, comme e_1 et e_2 sont des idempotents ($e_i^2 = e_i$), ce sont des anneaux unitaires, dont les unités sont les e_i (et donc pas des sous-anneaux de $\mathbb{Z}/a_1a_2\mathbb{Z}$ car l'unité n'est pas la même). On se convainc alors que les isomorphismes précédents étaient en fait des isomorphismes d'anneaux. Et c'est fini.

Ne pas oublier l'obsession du jury sur le thème « lemme chinois » : la réciproque est vraie, c'est-à-dire : si $\mathbb{Z}/a_1a_2\mathbb{Z} \simeq \mathbb{Z}/a_1\mathbb{Z} \oplus \mathbb{Z}/a_2\mathbb{Z}$ alors a_1 et a_2 sont premiers entre eux.

---

2. Les propriétés de e_1 et e_2 en font des analogues de $P_2U_2(\varphi) = \pi_1$ et $P_1U_1(\varphi) = \pi_2$.
3. De la sorte, I_1 est un analogue de $\operatorname{Im}\pi_1$ et I_2 est un analogue de $\operatorname{Im}\pi_2$.