# Intersections d'idéaux et systèmes de congruences

Jean-François Burnol, v1 13 avril 2018, v2 16 avril

Parmi les sujets des épreuves d'admission en agrégation interne se trouve une planche sur les idéaux dans les anneaux commutatifs.

On va commencer ici avec des anneaux principaux, puis dire des choses générales et revenir à la fin aux anneaux principaux.

En France, un anneau principal est intègre. Si l'on ne suppose pas l'intégralité (ou intégrité ? doute...) on parle d'anneau quasi-principal.

Nos exemples de base sont $\mathbb{Z}$, $\mathbb{K}[X]$, et leurs quotients. Par exemple l'algèbre engendrée par un endomorphisme $f$ d'un espace vectoriel $V$ est isomorphe à $\mathbb{K}[X]/(P)$ avec $P$ le polynôme minimal unitaire de $f$. [1]

Pour le théorème qui suit, on applique essentiellement la méthode de

http://jf.burnol.free.fr/agreg180411chinoiseriesII.pdf

(dans la preuve par les idéaux de son Lemme 2, bas de la page 3), mais il y a une difficulté car l'anneau $A$ est seulement supposé quasi-principal. Les possibles diviseurs de zéro obligent à procéder avec ténacité, prudence et méthode.

**Théorème 1.** *Soit $A$ un anneau quasi-principal, $I_1$, $I_2$, $J$ trois idéaux. Alors :*

$$I_1 \cap I_2 + J = (I_1 + J) \cap (I_2 + J) \tag{1}$$

*Preuve qui a nécessité une mûre réflexion.* Comme l'anneau est quasi-principal on peut écrire $I_1 = (a_1)$, $I_2 = (a_2)$, $I_1 + I_2 = (d)$. On a donc des relations :

$$\exists u_1, u_2 \in A \qquad u_1 a_1 + u_2 a_2 = d \tag{2}$$

$$\exists b_1 \in A \qquad a_1 = b_1 d \tag{3}$$

$$\exists b_2 \in A \qquad a_2 = b_2 d \tag{4}$$

On a besoin d'une succession de lemmes :

**Lemme 1.** *Pour tout $x$ de $I_1 + I_2$ il vaut $x = u_1 b_1 x + u_2 b_2 x$.*

En effet, c'est vrai avec $x = d = u_1 a_1 + u_2 a_2 = u_1 b_1 d + u_2 b_2 d$ donc pour tous les $x = vd$, $v \in A$.

**Lemme 2.** *Pour tout $x$ de $I_1 + I_2 + J$, il vaut $x \equiv u_1 b_1 x + u_2 b_2 x \pmod{J}$.*

1. On est un peu embêté par le cas $f = 0$ qui est le seul qui donne $P = 1$, et le quotient est alors l'anneau nul, dont il faut toujours un peu se méfier, bien qu'il soit unitaire, mais avec $1 = 0$. IMPORTANT : l'anneau nul n'est PAS intègre, par convention. Donc l'anneau nul n'est PAS un anneau principal.

C'est une conséquence immédiate du lemme précédent.

**Lemme 3**. *Si $x \in x_1 + J$ et aussi $x \in x_2 + J$ avec $x_1, x_2 \in I_1 + I_2 + J$ alors*

$$x \equiv u_1 b_1 x_2 + u_2 b_2 x_1 \pmod{J} \tag{5}$$

En effet on applique le lemme précédent et on fait remarquer ensuite que $u_1 b_1 x \equiv u_1 b_1 x_2 \pmod{J}$ et $u_2 b_2 x \equiv u_2 b_2 x_1 \pmod{J}$.

On peut maintenant démontrer le théorème. Supposons $x$ dans l'intersection de $I_1 + J$ et de $I_2 + J$. Il existe donc $x_1 \in I_1$ et $x_2 \in I_2$ tels que le lemme précédent s'applique. Bien sûr $b_1 x_2$ est dans $I_2$. Mais comme il existe $k \in A$ avec $x_2 = k a_2$, on a $b_1 x_2 = k b_1 a_2 = k b_1 b_2 d = k b_2 b_1 d = k b_2 a_1 \in I_1$. Ainsi $b_1 x_2 \in I_1 \cap I_2$. De même $b_2 x_1 \in I_1 \cap I_2$. Donc $x \in I_1 \cap I_2 + J$.

La réciproque est immédiate. □

*Remarque* 1. Si l'on regarde la fin de la preuve, on constate qu'on a prouvé un peu plus : on a montré que l'intersection était dans $(b_1 b_2 d) + J$, donc en fait avec $J = 0$ on a prouvé $(a_1) \cap (a_2) = (b_1 b_2 d)$. Dans un anneau intègre, on reconnaît le PPCM (défini à une unité près) $a_1 a_2 / d$ et la formule $\operatorname{pgcd}(a_1, a_2) \operatorname{ppcm}(a_1, a_2) \sim a_1 a_2$ mais dans un anneau non-nécessairement intègre il n'y a pas de corps des fractions et pas d'utilisation directe possible de l'écriture $a_1 a_2 / d$ pour le PPCM. Néanmoins elle reste moralement valable puisque ça marche avec $b_1 b_2 d$.

*Remarque* 2. Si l'on relit on voit qu'on a seulement utilisé que $I_1$, $I_2$ et $I_1 + I_2$ étaient principaux. Donc l'énoncé peut-être reformulé de manière plus puissante : soit $A$ un anneau commutatif (unitaire) et $f, g \in A$, et $J$ un idéal quelconque. Si $(f) + (g)$ est principal, alors $(f) \cap (g) + J = ((f) + J) \cap ((g) + J)$. Ou encore *Sous l'hypothèse que $(f) + (g)$ est principal alors si $x$ modulo $J$ est à la fois multiple de $f$ modulo $J$ et de $g$ modulo $J$ alors il est congru modulo $J$ à un $x'$ qui est à la fois multiple de $f$ et de $g$.*

*Remarque* 3. Dans $A$ un anneau commutatif (unitaire) quelconque, si $f, g \in A$, et $(f) + (g) = A$ alors $(f) \cap (g) = (fg)$. En effet on a une identité de Bézout par hypothèse $uf + vg = 1$, donc pour tout $x \in A$, $x = ufx + vgx$ et si $x \in (f) \cap (g)$ alors $ufx \in (fg)$, $vgx \in (fg)$ et finalement $x \in (fg)$.

**Corollaire 1**. *Soit $A$ un anneau quasi-principal, $I_1$, $I_2$, ..., $I_n$ et $J$ des idéaux. Alors :*

$$I_1 \cap \cdots \cap I_n + J = \bigcap_{1 \leqslant i \leqslant n} (I_i + J) \tag{6}$$

*Preuve.* Par récurrence. □

**Corollaire 2**. *Soit $A$ un anneau quasi-principal, $I_1$, $I_2$, ..., $I_n$ et $J$ des idéaux. Si pour chaque $1 \leqslant i \leqslant n$ les idéaux $I_i$ et $J$ sont premiers entre eux (i.e. $I_i + J = A$) alors $\cap_i I_i$ et $J$ sont premiers entre eux.*

*Preuve.* C'est un cas particulier de l'énoncé précédent. □

Ce dernier énoncé admet une généralisation à **tous** les anneaux commutatifs unitaires avec une formulation plus forte et une démonstration plus simple !

**Théorème 2.** *Soit $A$ un anneau commutatif unitaire, $n \geqslant 2$, $I_1$, $I_2$, ..., $I_n$ et $J$ des idéaux. Si pour chaque $1 \leqslant i \leqslant n$ les idéaux $I_i$ et $J$ sont premiers entre eux (i.e. $I_i + J = A$) alors $I_1 I_2 \dots I_n$ et $J$ sont premiers entre eux.*

*Preuve.* Je rappelle pour la compréhension de cet énoncé que $I_1 I_2$ est défini comme l'idéal engendré par les $i_1 i_2$, $i_1 \in I_1$, $i_2 \in I_2$ et donc $I_1 I_2 \dots I_n$ est l'idéal engendré par les $i_1 i_2 \dots i_n$, avec $i_j \in I_j$, $1 \leqslant j \leqslant n$.

On a pour chaque $i$ une écriture $a_i + b_i = 1$ avec $a_i \in I_i$ et $b_i \in J$. Si l'on fait le produit et qu'on développe totalement on obtient

$$a_1 a_2 \dots a_n + \text{quelque chose dans } J = 1 \tag{7}$$

d'où $I_1 I_2 \dots I_n + J = A$. □

**Théorème 3.** *Soit $A$ un anneau commutatif unitaire, $n \geqslant 2$ et $I_1$, $I_2$, ..., $I_n$ des idéaux deux-à-deux premiers entre eux. Alors*

$$I_1 \cap \dots \cap I_n = I_1 I_2 \dots I_n \tag{8}$$

*Preuve.* L'inclusion $I_1 I_2 \dots I_n \subset I_1 \cap \dots \cap I_n$ est immédiate, il faut montrer l'inclusion opposée.

Par le théorème précédent, pour chaque $i$ on a

$$I_i + \prod_{j \neq i} I_j = A \tag{9}$$

Écrivons donc $x_i + y_i = 1$ avec $x_i \in I_i$, $y_i \in \prod_{j \neq i} I_j$.

Supposons $t \in I_1 \cap \dots \cap I_n$. Alors $t = t x_i + t y_i$. Comme $t \in I_i$ on a $t y_i \in \prod_i I_i$, donc

$$t \equiv t x_i \pmod{I_1 I_2 \dots I_n} \tag{10}$$

Bien sûr tout multiple $tf$ de $t$ est à nouveau dans l'intersection des idéaux donc on peut itérer et on obtient :

$$t \equiv t x_1 \equiv t x_1 x_2 \equiv \dots \equiv t x_1 x_2 \dots x_n \equiv 0 \pmod{I_1 I_2 \dots I_n} \tag{11}$$

et la preuve est faite. □

**Théorème 4** (« Chinois dans un anneau commutatif »). *Soit $A$ un anneau commutatif unitaire, $n \geqslant 2$ et $I_1$, $I_2$, ..., $I_n$ des idéaux de $A$ deux-à-deux premiers entre eux. Le morphisme canonique*

$$\psi : A/\bigcap_i I_i \longrightarrow \prod_i A/I_i \tag{12}$$

*est un isomorphisme.*

*Preuve.* L'injectivité est claire, il faut montrer la surjectivité, c'est-à-dire le fait qu'on peut résoudre tout système

$$\begin{array}{lll} x \equiv x_1 & (\mathrm{mod}\ I_1) \\ x \equiv x_2 & (\mathrm{mod}\ I_2) \\ \vdots \quad & \vdots \quad & \vdots \\ x \equiv x_n & (\mathrm{mod}\ I_n) \end{array} \tag{$S_n$}$$

sous les conditions de l'énoncé. C'est vrai pour $n = 1$, donc supposons-le vrai pour $n$ et montrons-le pour $n + 1$. Par l'hypothèse de récurrence il existe une solution $x_0 \in A$ (qui est unique modulo $I_1 \cap \cdots \cap I_n$) aux $n$ premières équations, et il suffira de résoudre le nouveau système

$$\begin{array}{ll} x \equiv x_0 & (\mathrm{mod}\ I_1 \cap \cdots \cap I_n) \\ x \equiv x_{n+1} & (\mathrm{mod}\ I_{n+1}) \end{array} \tag{13}$$

Grâce au théorème 2 on sait que $\prod_{i\leqslant n} I_i$ et $I_{n+1}$ sont premiers entre eux, et donc aussi $\bigcap_{i\leqslant n} I_i$ et $I_{n+1}$. À ce propos on sait $\prod_{i\leqslant n} I_i = \bigcap_{i\leqslant n} I_i$ mais on n'a pas besoin de cela ici, simplement l'inclusion $\prod_{i\leqslant n} I_i \subset \bigcap_{i\leqslant n} I_i$. On est ramené au cas de $S_n$ avec $n = 2$.

On revient donc à un système à deux congruences

$$\begin{array}{ll} x \equiv x_1 & (\mathrm{mod}\ I_1) \\ x \equiv x_2 & (\mathrm{mod}\ I_2) \end{array} \tag{$S_2$}$$

avec l'hypothèse $I_1 + I_2 = A$, donc une relation

$$i_1 + i_2 = 1, i_1 \in I_1, i_2 \in I_2 \tag{14}$$

On note que $i_1$ résout $(S_2)$ pour $x_1 = 0, x_2 = 1$ et $i_2$ résout $(S_2)$ pour $x_1 = 1, x_2 = 0$. D'où une solution en général :

$$x_0 \coloneqq i_1 x_2 + i_2 x_1 \tag{15}$$

Fin de la preuve du théorème chinois pour les anneaux commutatifs généraux. □

Exercice : peut-on avoir $I_1 = 0$ dans l'énoncé ci-dessus ? que se passe-t-il alors ? l'énoncé est-il vrai ? (il a intérêt on vient de le prouver...)

**Théorème 5** (« Chinois général dans un anneau quasi-principal »). *Soit $A$ un anneau* quasi-principal, *$n \geqslant 2$ et $I_1$, $I_2$, ..., $I_n$ des idéaux de $A$. On ne fait aucune hypothèse de co-primalité. Le système*

$$\begin{aligned} x &\equiv x_1 \pmod{I_1} \\ x &\equiv x_2 \pmod{I_2} \\ &\vdots \quad \vdots \quad\quad \vdots \\ x &\equiv x_n \pmod{I_n} \end{aligned} \tag{16}$$

*admet une solution si et seulement si $x_i - x_j \in I_i + I_j$ pour tout couple $(i, j)$.*

*Preuve.* Commençons par la nécessité. Si $x - x_i \in I_i$ et $x - x_j \in I_j$ alors par différence $x_j - x_i \in I_j + I_i$.

Pour la suffisance on procède par récurrence.

Il faut tout d'abord traiter le cas $n = 2$. Il s'agit de résoudre

$$\begin{aligned} x &\equiv x_1 \pmod{I_1} \\ x &\equiv x_2 \pmod{I_2} \end{aligned} \tag{17}$$

sous l'hypothèse $x_1 - x_2 \in I_1 + I_2$. Donc il existe (mais on ne dit pas comment les trouver !) $i_1 \in I_1$, $i_2 \in I_2$ avec

$$x_1 - x_2 = i_1 + i_2 \tag{18}$$

Soit alors $x = x_1 - i_1 = x_2 + i_2$. Clairement ce $x$ résout (17) !

Pour le cas général on procède par récurrence. Supposons vrai pour $n$ et prenons un système avec $n+1$ équations et les conditions de compatibilité toutes satisfaites. Les $n$ premières équations admettent une solution $x_0 \in A$ (qui est unique modulo $I_1 \cap \cdots \cap I_n$), et il suffira de résoudre le nouveau système

$$\begin{aligned} x &\equiv x_0 \pmod{I_1 \cap \cdots \cap I_n} \\ x &\equiv x_{n+1} \pmod{I_{n+1}} \end{aligned} \tag{19}$$

Il nous faut donc nous assurer que $x_0 - x_{n+1}$ appartient à la somme d'idéaux

$$I_1 \cap \cdots \cap I_n + I_{n+1} \tag{20}$$

Mais d'après notre Corollaire 1 au Théorème 1, qui est valable pour les idéaux dans un anneau quasi-principal, on a

$$I_1 \cap \cdots \cap I_n + I_{n+1} = \bigcap_{1 \leqslant i \leqslant n} (I_i + I_{n+1}) \tag{21}$$

Donc il suffit de montrer que $x_0 - x_{n+1}$ appartient à chaque $I_i + I_{n+1}$. Par hypothèse $x_i - x_{n+1} \in I_i + I_{n+1}$, il suffit donc de montrer que $x_0 - x_i \in I_i + I_{n+1}$. Mais par construction de $x_0$, $x_0 \equiv x_i \pmod{I_i}$, donc $x_0 - x_i$ en fait appartient à $I_i$.

La démonstration est complète. □

Dans le cas d'un anneau *principal*, on peut résoudre le système

$$\begin{aligned} x &\equiv x_1 \pmod{I_1} \\ x &\equiv x_2 \pmod{I_2} \end{aligned} \tag{22}$$

un peu différemment. Tout d'abord on choisit des générateurs $I_1 = (a_1)$, $I_2 = (a_2)$, $I_1 + I_2 = (d)$. Ainsi

$$\exists u_1, u_2 \in A, \qquad u_1 a_1 + u_2 a_2 = d \tag{23}$$

On traite en premier le cas $d = 0$. Cela ne se produit que si $I_1 = I_2 = \{0\}$. Le système réclame $x = x_1$ et $x = x_2$, et l'hypothèse est $x_1 - x_2 \in I_1 + I_2 = \{0\}$ donc $x_1 = x_2$ et en effet il y a une solution (unique).

Si $d \neq 0$, on peut, puisque $A$ est intègre, diviser l'identité de Bézout par $d$ pour obtenir

$$u_1 \frac{a_1}{d} + u_2 \frac{a_2}{d} = 1 \tag{24}$$

et on résout 22 par la formule magique

$$x_0 = u_1 \frac{a_1}{d} x_2 + u_2 \frac{a_2}{d} x_1 \tag{25}$$

Car par hypothèse $x_1 - x_2$ est de la forme $x_1 - x_2 = kd$, $k \in A$. Ainsi

$$x_0 = u_1 \frac{a_1}{d}(x_1 - kd) + u_2 \frac{a_2}{d} x_1 = x_1 - k u_1 a_1 \tag{26}$$

De même

$$x_0 = u_1 \frac{a_1}{d} x_2 + u_2 \frac{a_2}{d}(x_2 + kd) = x_2 + k u_2 a_2 \tag{27}$$

La première formule montre $x \equiv x_1 \pmod{a_1}$ et la seconde $x \equiv x_2 \pmod{a_2}$.

En quoi cela diffère-t-il de notre démonstration dans le cas quasi-principal ?

On y écrivait $x_1 - x_2 = i_1 + i_2$ et la solution était $x = x_1 - i_1 = x_2 + i_2$. Ici on a écrit $x_1 - x_2 = kd$ avec $d = u_1 a_1 + u_2 a_2$. Donc cela correspond à $i_1 = k u_1 a_1$ et $i_2 = k u_2 a_2$ et la méthode pour le cas quasi-principal nous aurait amenés à la solution $x = x_1 - k u_1 a_1 = x_2 + k u_2 a_2$. Mais c'est bien le $x_0$ de la formule (25) comme l'ont montré (26) et (27).

La formule magique (25) nous incite à essayer de trouver pour tout $n$ une solution comme « combinaison linéaire » des $x_j$. C'est ce que réalise l'énoncé suivant :

**Théorème 6**. *Soit $A$ un anneau* principal *et $a_1, \ldots, a_n$ dans $A$. On suppose que les $a_i$ sont tous non nuls et on note $M$ un générateur de l'idéal $(a_1) \cap \cdots \cap (a_n)$.*

*Il existe une identité de Bézout*

$$y_1 \frac{M}{a_1} + \cdots + y_n \frac{M}{a_n} = 1 \qquad y_1, \ldots, y_n \in A \tag{28}$$

*De plus tout système*

$$\begin{array}{lll} x \equiv x_1 & (\text{mod } a_1) \\ x \equiv x_2 & (\text{mod } a_2) \\ \vdots \quad & \vdots \quad & \vdots \\ x \equiv x_n & (\text{mod } a_n) \end{array} \tag{29}$$

*vérifiant les compatibilités* $\forall i, j\ x_i - x_j \in (a_i) + (a_j)$ *a son unique solution modulo* $(M)$ *donnée par*

$$x \equiv y_1 \frac{M}{a_1} x_1 + \cdots + y_n \frac{M}{a_n} x_n \pmod{M} \tag{30}$$

*Preuve.* On considère $K$ le corps des fractions de l'anneau intègre (qui est donc distinct de l'anneau nul) $A$. L'équation (28) dit que $\frac{1}{M} \in \frac{1}{a_1}A + \cdots + \frac{1}{a_n}A$ ce qui se prête bien à une preuve par récurrence, et on voit qu'il suffit de traiter le cas $n = 2$. Mais alors, avec $d$ un PGCD de $a_1$ et $a_2$ on a vu précédemment qu'on a à un inversible près (que l'on pourra intégrer aux $y_j$) $M = a_1 a_2/d$, et il s'agit donc d'obtenir $y_1 \frac{a_2}{d} + y_2 \frac{a_1}{d} = 1$, ce qui est garanti par $(d) = (a_1) + (a_2)$.

Donc il existe en général une équation (28). Considérons maintenant le système (29). Par hypothèse les conditions de compatibilité sont satisfaites, et ce système possède une solution $x \in A$. Définissons maintenant

$$x' = y_1 \frac{M}{a_1} x_1 + \cdots + y_n \frac{M}{a_n} x_n \tag{31}$$

On remarque que $\frac{M}{a_j}(x - x_j)$ est un multiple de $M$ puisque $x - x_j$ est divisible par $a_j$. Donc

$$x' \equiv y_1 \frac{M}{a_1} x + \cdots + y_n \frac{M}{a_n} x \pmod{M} \tag{32}$$

Mais d'après (28) le terme de droite après avoir mis $x$ en facteur est simplement $1x = x$. Donc en effet la formule de l'énoncé donne la solution… s'il en existe une ! □

*Remarque* 4. Si les $a_i$ sont premiers entre eux deux à deux, alors on peut prendre $M = a_1 \ldots a_n$ et les $\epsilon_j = y_j M/a_j$ dont la somme vaut 1 résolvent les congruences $\epsilon_j \equiv \delta(i, j)$ (mod $a_i$), d'où la solution comme combinaison linéaire. Une autre façon de voir est de dire que $y_j$ est un inverse modulaire de $M/a_j$ modulo $a_j$. C'est la présentation plus habituelle de la solution du problème Chinois lorsque les modules sont premiers entre eux deux-à-deux.

Le théorème 6 donne une formulation qui fonctionne sans hypothèse de co-primalité. Il y suffit d'ailleurs que la somme des $y_j M/a_j$ soit congrue à 1 modulo $M$, elle n'a pas à être stricto sensu égale à 1 (d'ailleurs si c'est congru à 1 modulo $M$ on peut ajuster par exemple $y_1$ par un multiple de $a_1$ pour rendre exactement égal à 1).