Introduction aux espaces quotients

Marc SAGE

7 février 2005

Table des matières

1 Introduction

1.1 Quotient d'un groupe abélien par un sous-groupe

On considère dans cette partie un groupe abélien $(G,+)$ et H un sous-groupe de G.
Considérons la relation d'équivalence suivante sur G, appelée *relation de congruence modulo* H :

$$x \equiv y \iff y - x \in H.$$

On lira "x est congru à y modulo H", et on interprète dans le langage courant comme "x vaut y *à un élément de* H *près*" (l'élément en question étant la différence $y-x$, qui est dans H si $x \equiv y$). L'usage a voulu que cette dernière expression se transforme en "x est égal à y *modulo* un élément de H", comme on dirait "tout entier relatif se décompose en produit de nombres premiers *modulo* un facteur ± 1", ou bien "*modulo* un coefficient scalaire, tout polynôme non nul sur $\mathbb{C}$ s'écrit $\prod_{i=1}^{d}(X-\lambda_i)$", ou encore "*modulo* une astuce introuvable, cet exercie est une trivialité". Il convient donc de considérer le terme *modulo* comme du vocabulaire courant, et ainsi la relation de congruence modulo un ensemble devrait parler d'elle-même.

Vérifier que $\equiv$ est une relation d'équivalence est immédiat car H contient le neutre 0 (réflexivité), est stable par passage à l'opposé (symétrie) et par addition (transitivité). On notera $\overline{x}$ la classe d'équivalence de x pour la relation $\equiv$. Remarquons dès maintenant que

$$y \in \overline{x} \iff \overline{y} = \overline{x} \iff y - x \in H \iff y \in x + H$$

où l'on note

$$x + H := \{x + h \ ; \ h \in H\}.$$

Ainsi, la classe d'un élément x de G peut d'écrire explicitement comme

$$\overline{x} = x + H.$$

Par analogie avec le cas $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ (où l'on retrouve la congruence modulo n, les classes $\overline{a} = a + n\mathbb{Z}$, et l'ensemble ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$), on notera

$${}^{G}\!/_{H} := \{\overline{x} \ ; \ x \in G\} = \{x + H \ ; \ x \in G\}$$

l'ensemble quotient ${}^{G}\!/_{\equiv}$.

Cherchons à présent à munir l'ensemble quotient ${}^{G}\!/_{H}$ d'une structure de groupe. Soient X et Y deux éléments de ${}^{G}\!/_{H}$, x un représentant de X et y un représentant de Y. On peut essayer de définir une loi $+$ sur ${}^{G}\!/_{H}$ qui découlerait de celle de G, par exemple :

$$X + Y := \overline{x + y}$$

(on utilise volontairement le même symbole $+$ pour désigner les lois de G et de ${}^{G}\!/_{H}$, car la seconde découle de la première au vu de la définition, mais il faut garder à l'esprit qu'elle n'agissent pas sur les mêmes objets – la première sur des éléments de G, la seconde sur des classes d'élements de G).

Cette définition n'a aucune raison d'en être une, en cela que le membre de gauche $\overline{x+y}$ dépend *a priori* des représentants x et y choisis. Vérifions qu'il n'en est rien. Si x' est un autre représentant de X, on a $\overline{x} = X = \overline{x'}$, donc $x \equiv x'$, et la différence $(x' - x)$ est un élément h_x de H. De même, si y' est un autre représentant de Y, on a $(y' - y) = h_y$ élément de H. On en déduit

$$(x' + y') - (x + y) = (x' - x) + (y' - y) = h_x + h_y \in H$$

car H stable par $+$, *i.e.* $x + y \equiv x' + y'$, ou encore $\overline{x' + y'} = \overline{x + y}$.

On peut donc effectivement munir ${}^{G}\!/_{H}$ d'une loi $+$ définie par

$$\overline{x} + \overline{y} = \overline{x + y}.$$

Il est alors immédiat que le magma $\left({}^{G}\!/_{H}, +\right)$ est un groupe : observer que l'associativité dans ${}^{G}\!/_{H}$ découle de l'associativité dans G et que le neutre ainsi que l'inverse dans ${}^{G}\!/_{H}$ sont donnés par

$$0_{({}^{G}\!/_{H})} = \overline{0_G} \text{ et } -\overline{x} = \overline{-x}.$$

Le groupe $\left({}^{G}\!/_{H}, +\right)$ est alors appelé *groupe quotient de G par H*, ou plus simplement *quotient de G par H*, voire carrément *quotient par H*.

De façon plus générale, si $*$ est un loi quelconque sur un ensemble E non vide muni d'une relation d'équivalence $\sim$, on dit que la relation $\sim$ *est compatible avec la loi* $*$ si

$$\left\{ \begin{array}{l} x \sim x' \\ y \sim y' \end{array} \right. \text{ entraine } (x * y) \sim (x' * y') .$$

On peut alors définir une *loi quotient* $*_\sim$ sur ${}^{E}\!/_{\sim}$ par

$$\overline{x} *_\sim \overline{y} = \overline{x * y}$$

et l'on voit que toutes les propriétés de la loi $*$ (associativité, commutativité...) sont transportées dans le quotient et sont vérifiées par $*_\sim$.

C'est exactement ce que nous avons fait au-dessus en considérant la relation $\equiv$ de congruence modulo H sur l'ensemble G muni de la loi $+$ et en montrant que $\equiv$ était compatible avec $+$.

Remarque. Lorsqu'une relation d'équivalence est compatible avec une loi, on parle plutôt de relation de *congruence* et on la note généralement $\equiv$. On peut donc mener des calculs avec la loi considérer, la présence d'un troisième trait sur le signe $=$ rappelant qu'on travaille dans le quotient. Penser aux congruences d'entiers dans $\mathbb{Z}$!

Petit complément.

Réciproquement, si l'on se donne une relation d'équivalence $\sim$ sur G compatible avec la loi $+$, cherchons un sous-groupe H tel que ${}^{G}\!/_{\sim} = {}^{G}\!/_{H}$, *i.e.* tel que $\sim$ soit la relation de congruence modulo H. Par définition de celle-ci, un tel H doit vérifer $x \sim y$ si et seulement si $y - x \in H$, donc la seule possibilité est

$$H = \{y - x \ ; \ x \sim y\} .$$

H est bien un sous-groupe de G, car :

• en prenant un x dans G, on a (par réfléxivité de $\sim$) $x \sim x$, donc $0 = x - x \in H$;

• si $h \in H$, on a $h = y - x$ avec $x \sim y$, donc (par symétrie de la relation $\sim$) $y \sim x$, d'où $-h = x - y \in H$;

• si h_x et h_y sont dans H, on a $\left\{ \begin{array}{l} h_x = x' - x \text{ avec } x \sim x' \\ h_y = y' - y \text{ avec } y \sim y' \end{array} \right.$, donc (par compatibilité de $\sim$ avec $+$) $(x + y) \sim (x' + y')$, *i.e.* $(x' + y') - (x + y) \in H$, on encore $h_x + h_y \in H$.

De plus, on a bien $x \sim y$ si et seulement si $y - x \in H$ comme on le souhaitait.

En conclusion, un sous-groupe et une relation d'équivalence compatible avec la loi de groupe, c'est pareil.

1.2 Intérêt du quotient

Il est commun en mathématiques d'avoir à étudier des strutures où l'on ne s'intéresse qu'à quelques propriétés bien spécifiques des éléments étudiés. Par exemple :

• l'étude des entiers relatifs où l'on ne s'intéresse qu'à la divisibilité par un entier naturel donné ;

• l'étude d'un espace vectoriel affinisé où l'on ne s'intéresse qu'à la direction de la droite joignant deux points donnés ;

• l'étude d'un groupe muni d'un endomorphisme où l'on ne s'intéresse qu'à l'image des éléments par ce morphisme.

Dans tous ces exemples, le fait que deux éléments x et y aient la propriété étudiée (en d'autres termes, le fait qu'ils soient *équivalents* pour la propriété étudiée) peut se traduire par une relation compatible avec les lois qui nous intéressent. Pour reprendre les exemples ci-dessus :

• a et b sont même reste dans la division euclidienne par un entier n si et seulement si leur différence est dans $n\mathbb{Z}$, *i.e.* $a \equiv b \ [n]$, ce qui est bien une relation compatible avec les loi $+$ et $\times$ qui servent à étudier la divisibilité des entiers ;

• si l'on se fixe un direction x_0 (*i.e.* un vecteur) dans un K-espace vectoriel, le fait que deux points a et b soient alignés selon cette direction se traduit par $\overrightarrow{ab} \parallel x_0$, *i.e.* $a - b \in Kx_0$. On vérifie facilement que cette relation d'équivalence, qui consiste à quotienter l'espace par le sous-espace vectoriel Kx_0, est compatible avec les lois vectorielles ;

• si f est un morphisme d'un groupe G abélien dans un groupe H, le fait que deux éléments x et y aient même image s'écrit $f(x) = f(y)$, *i.e.* $f(x-y) = 0$, ou encore $x - y \in \operatorname{Ker} f$, ce qui revient à considérer le quotient ${}^{G}\!/_{\operatorname{Ker} f}$.

Dans les trois cas, on regroupe tous les éléments équivalents pour la propriété éudiée, on met les paquets obtenus dans des sacs (les éléments d'un même sac sont tous équivalents), puis on travaille sur les sacs (sur l'ensemble quotient) avec la même structure que sur l'ensemble de départ.

On a gagné à n'étudier que des objects distincts vis–vis de la propriété étudiée, même si en apparence ces objets sont plus compliqués. En apparence seulement car avec l'habitude on oublie leur définition ensembliste pour n'en garder que les propriétés essentielles. Par exemple, on peut construire $\mathbb{R}$ en quotientant l'ensemble des suites de Cauchy de $\mathbb{Q}$ par la relation "la différence tend vers 0" ; mais personne n'utilise le fait qu'un réel peut se représenter comme un ensemble de suites de Cauchy rationnelles ; seulent comptent les propriétés de l'ordre, de la complétude, et de la borne supérieure (essentiellement).

2 Structures quotients

2.1 Quotient d'un groupe par un sous-groupe

On considère cette fois un groupe multiplicatif $(G, \cdot)$ non nécessairement abélien et H un sous-groupe de G. Par analogie avec le cas abélien, on définit une relation $\equiv$ sur G par

$$x \equiv y \iff x^{-1}y \in H.$$

On vérifie immédiatement qu'il s'agit bien d'une relation d'équivalence. De plus, les équivalences

$$y \in \overline{x} \iff \overline{y} = \overline{x} \iff x^{-1}y \in H \iff y \in xH$$

assurent que la classe d'un élément x de G est donnée par

$$\overline{x} = xH = \{xh \ ; \ h \in H\}.$$

On peut dès à présent noter les propriétés :

$$\begin{cases} (xy)\,H = x\,(yH) \\ \forall h \in H, \ hH = H. \end{cases}$$

La première est triviale en vérifiant les deux inclusions (et ne nécessite pas que H soit un sous-groupe de G, toute partie de G convient), la seconde résulte de ce que H est stable par la loi $\cdot$ (d'où $hH \subset H$) et par passage à l'inverse (tout h_0 de H peut s'écrire $h\left(h^{-1}h_0\right)$, d'où $H \subset hH$). On a également de façon immédiate que pour toutes parties A et B de G :

$$A \subset B \implies \begin{cases} xA \subset xB \\ Ax \subset Bx \end{cases}.$$

On considère ensuite l'ensemble quotient ${}^{G}\!/_{\equiv} = \{\overline{x} \ ; \ x \in G\}$, généralement noté

$${}^{G}\!/_{H} := \{xH \ ; \ x \in G\}.$$

Petit commentaire : les classes xH ici obtenues sont appelées *classes à gauche de* H : le x dans le "xH" est "à gauche" de H – on dit aussi parfois que xH est le *translaté à gauche de* H *par* x. On peut également définir une relation $x \equiv y$ par $xy^{-1} \in H$, auquel cas les classes d'équivalence sont donnnées par $\overline{x} = Hx$ et sont alors appelées *classes à droite de* H (Hx est également appelé *translaté à droite de* H *par* x), l'ensemble quotient se notant dans ce cas

$${}_{H}\backslash^{G} := \{Hx \ ; \ x \in G\}.$$

Pour ne pas se mélanger les pinceaux, on pourra retenir que, dans les notations $\left\{ \begin{array}{l} {}^{G}\!/_{H} = \{xH \ ; \ x \in G\} \\ {}_{H}\backslash^{G} = \{Hx \ ; \ x \in G\} \end{array} \right.$, ce par quoi on translate (les éléments x de G) est du bon côté de H : pour les classes *à gauche*, le "x" de xH à est *à gauche* de H, et le "G" de ${}^{G}\!/_{H}$ est aussi *à gauche* de H. Évidemment, dans le cas abélien, tout commute et il n'y a pas lieu de différencier classe à gauche de classe à droite.

En pratique, on utilise la plupart du temps les classes à gauche et le quotient ${}^{G}\!/_{H}$.

Cherchons à présent à munir le quotient ${}^{G}\!/_{H}$ d'une structure de groupe, toujours par analogie avec le cas abélien. Un bon candidat serait la loi quotient définie par

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}.$$

On a déjà vu que, pour que la définition ci-dessus en soit vraiment une, *i.e.* que la classe $\overline{xy}$ ne dépende pas des représentants choisis, il faut que la relation $\equiv$ soit compatible avec la loi de G. Regardons ce que cela implique sur le sous-groupe H.

Soient g quelconque dans G, h quelconque dans H. On a

$$\left\{ \begin{array}{c} \overline{h} = hH = H = \overline{1} \\ \overline{gh} = (gh)\, H = g\,(hH) = gH = \overline{g} \end{array} \right. ,$$

donc, dans le cas où la relation $\equiv$ est compatible avec la loi $\cdot$, on doit avoir

$$\begin{array}{rcl} \left\{ \begin{array}{l} 1 \equiv h \\ gh \equiv g \end{array} \right. & \Longrightarrow & (1) \cdot (gh) \equiv (h) \cdot (g) \implies gh \equiv hg \implies (gh)^{-1}\,(hg) \in H \\ & \Longrightarrow & h^{-1}g^{-1}hg \in H \implies h\left(h^{-1}g^{-1}hg\right) \in hH \implies g^{-1}hg \in H. \end{array}$$

Ceci tenant pour tout h dans H, on doit avoir

$$\forall g \in G,\ g^{-1}Hg \subset H.$$

Un tel sous-groupe stable par les applications $i_g : x \mapsto g^{-1}xg$ (appelées *conjugaisons* ou *automorphismes intérieurs*), est dit *distingué dans* G (ou tout simplement *distingué*), et on note alors $H \lhd G$. Attention au symbole $\lhd$ qui fait penser à une relation d'ordre, en général la relation "être distingué dans" n'est pas transitive ! Noter que dans le cas abélien, tous les sous-groupes de G sont distingués dans G.

Montrons tout de suite deux caractérisations des sous-groupes distingués.

Lemme.
Les trois propositions suivantes sont équivalentes :
- $H \lhd G$;
- $\forall g \in G,\ gH = Hg$;
- $\forall g \in G,\ g^{-1}Hg = H$.

Démonstration.
- Supposons $H \lhd G$, et soit $g \in G$. En appliquant la définition à g et à g^{-1}, on obtient $\left\{ \begin{array}{l} g^{-1}Hg \subset H \\ gHg^{-1} \subset H \end{array} \right.$, d'où $\left\{ \begin{array}{l} g\left(g^{-1}Hg\right) \subset gH \\ \left(gHg^{-1}\right)g \subset Hg \end{array} \right.$, *i.e.* $\left\{ \begin{array}{l} Hg \subset gH \\ gH \subset Hg \end{array} \right.$, ou encore $Hg = gH$.
- Supposons $\forall g \in G,\ gH = Hg$. Pour g dans G, on vérifie que

$$g^{-1}Hg = \left(g^{-1}H\right)g = \left(Hg^{-1}\right)g = H\left(g^{-1}g\right) = H.$$

- Supposons $\forall g \in G,\ g^{-1}Hg = H$. *A fortiori* on a $\forall g \in G,\ g^{-1}Hg \subset H$, d'où $H \lhd G$.

On a donc montré que si l'on peut munir le quotient ${}^{G}\!/_{H}$ d'une loi $\cdot$ vérifiant $\overline{x}\cdot\overline{y} = \overline{x \cdot y}$, alors nécéssairement le sous-goupe H est distingué dans G (*i.e.* que H est stable par conjugaison), ce qui revient à dire (d'après le lemme) que les classes à gauche coïncident avec les classes à droite.

Réciproquement, vérifions que la condition $H \lhd G$ suffit à montrer la compatibilité de la relation $\equiv$ avec la loi $\cdot$. Pour $\left\{ \begin{array}{l} x \equiv x' \\ y \equiv y' \end{array} \right.$, on a

$$\begin{array}{rcl} \overline{xy} & = & (xy)\, H = x\,(yH) = x\,(y'H) = x\,(Hy') = (xH)\, y' \\ & = & (x'H)\, y' = (Hx')\, y' = H\,(x'y') = (x'y')\, H = \overline{x'y'},\ CQFD. \end{array}$$

Il reste juste à vérifier l'associativité de la loi quotient, mais elle découle naturellement de l'associativié de la loi dans G :

$$\overline{x} \cdot (\overline{y} \cdot \overline{z}) = \overline{x} \cdot (\overline{yz}) = \overline{x\,(yz)} = \overline{(xy)\,z} = (\overline{x} \cdot \overline{y}) \cdot \overline{z}.$$

Conclusion générale.
Soit H un sous-groupe de G. La loi quotient $\overline{x} \cdot \overline{y} = \overline{x \cdot y}$ sur ${}^{G}\!/_{H}$ est bien définie si et seulement si H est distingué dans G, et alors la projection canonique

$$\pi : \left\{ \begin{array}{ccc} (G, \cdot) & \longrightarrow & \left({}^{G}\!/_{H}, \cdot\right) \\ g & \longmapsto & \overline{g} = gH \end{array} \right.$$

est un morphisme de groupes – ce qui fournit au passage le neutre $1_{{}^{G}/_{H}} = \overline{1_G}$ et l'inverse $\overline{x}^{-1} = \overline{x^{-1}}$.

Juste un point pour finir concernant le terme de *projection canonique* : si E est un ensemble non vide muni d'une relation d'équivalence $\sim$ pour laquelle on note $\overline{x}$ la classe d'un élément x de E, l'application

$$\pi : \left\{ \begin{array}{ccc} E & \longrightarrow & {}^{E}\!/_{\sim} \\ x & \longmapsto & \overline{x} \end{array} \right.$$

est usuellement appelée *projection canonique*. Le terme *projection* (qui signifie surjection) vient du caractère surjectif de π (tout $\overline{x}$ a un antécédent x), et l'adjectif *canonique* découle de la définition simplissime de π (comment définir de manière moins compliquée une application de E dans le quotient ${}^{E}\!/_{\sim}$?). Ici, l'ensemble E considéré est notre groupe G, et on quotiente par la relation de congruence modulo H.

2.2 Quotient d'un anneau par un idéal

Considérons un anneau $(A, +, \times)$, et I un sous-groupe de $(A, +)$. Puisque $(A, +)$ est abélien, il est distingué dans A et on peut donc considérer le groupe quotient

$${}^{A}\!/_{I} = \{\overline{a} = a + I \ ; \ a \in A\}$$

muni de la loi $\overline{a} + \overline{b} = \overline{a + b}$.

On aimerait rajouter une loi multiplicative $\times$ de façon à ce que $\left({}^{A}\!/_{I}, +, \times\right)$ devienne un anneau. Autant le faire sans se fatiguer, et poser $\overline{a} \times \overline{b} = \overline{a \times b}$. Se pose à nouveau le problème de l'indépendance de $\overline{a \times b}$ par rapport aux représentants a et b. Cherchons les conditions que cela implique sur le sous-groupe I considéré.

Soit a quelconque dans A, i quelconque dans I. Puisque $\left\{ \begin{array}{c} \overline{a + i} = \overline{a} \\ \overline{0} = \overline{i} \end{array} \right.$, on devrait avoir $\overline{(a + i) \times 0} = \overline{a \times i}$, *i.e.* $\overline{ai} = \overline{0} = I$, ou encore $ai \in I$, et de même $ia \in I$. Ceci tenant pour tout i dans I, on doit donc avoir

$$\forall a \in A, \ \left\{ \begin{array}{l} aI \subset I \\ Ia \subset I \end{array} \right. ,$$

que l'on écrira de manière plus concise

$$\left\{ \begin{array}{l} AI \subset I \\ IA \subset I \end{array} \right. .$$

Un tel sous-groupe stable par multiplication scalaire à droite et à gauche est appelé *idéal bilatère de A*. On parle également d'*idéal à gauche* si $AI \subset I$, et d'*idéal à droite* si $IA \subset I$. Un idéal bilatère est donc un idéal à droite et à gauche, *i.e.* un idéal des deux côtés, d'où son nom. Évidemment, si l'anneau A est commutatif, les trois notions coïncident, et on parle alors d'*idéal* tout court. Donnons immédiatement une caractérisation "vectorielle" (ou "linéaire") des idéaux dans le cas où A est commutatif (le plus fréquent).

Lemme.
Soit A un anneau commutatif et I une partie de A. Les deux propositions suivantes sont équivalentes :
• *I est un idéal de A ;*

• *I contient 0_A et est stable par combinaisons linéaires à coefficients dans A.*

Démonstration.
• Supposons que I soit un idéal de A. $(I,+)$ est donc un sous-groupe de $(A,+)$, donc il contient 0_A. De plus, pour i,j dans I et a,b dans A, par définition d'un idéal, ai et bj sont dans I, donc leur somme aussi (puisque I est stable par $+$), donc I est stable par combinaisons linéaires.
• Supposons que I contienne 0_A et soit stable par combinaisons linéaires. Pour tout i,j de I, les combinaisons linéraires $i+j$ et $-i$ restent donc dans I, donc I est stable par $+$ et par passage à l'opposé, donc $(I,+)$ est un groupe. De plus, pour tout a dans A, la combinaison linéaire ai reste dans I. Il en résulte que I est un idéal.

Remarquer que cette caractérisation vectorielle des idéaux reste valable si A n'est plus supposé commutatif, à condition de remplacer "idéal" par "idéal à droite" et "combinaisons linéaires" par "combinaisons linéaires à droite" (idem à gauche, bien sûr).

Attention à ne surtout pas dire qu'un idéal (bilatère, à gauche, ou à droite) contient le neutre multiplicatif 1_A. D'une part il faudrait déjà que l'anneau A soit unitaire pour avoir l'existence de 1_A, d'autre part un idéal contenant 1_A contient tous les combinaisons linéaires $a1_A$ ou 1_Aa pour a dans A et donc vaut A tout entier.
En résumé, si I est un idéal (bilatère, à gauche, ou à droite) de A unitaire :

$$1_A \in I \iff I = A.$$

Vérifions maintenant que la condition I idéal bilatère de A suffit à définir une loi multiplicative $\times$ sur ${}^{A}\!/_{I}$ vérifiant $\overline{a}\times\overline{b} = \overline{a\times b}$. Pour $\begin{cases} a \equiv a' \\ b \equiv b' \end{cases}$, *i.e.* $\begin{cases} a'-a = i_a \in I \\ b'-b = i_b \in I \end{cases}$, on a

$$\overline{a'b'} = a'b' + I = (a+i_a)(b+i_b) + I = ab + \underbrace{ai_b}_{\in I} + \underbrace{i_a b}_{\in I} + \underbrace{i_a i_b}_{\in I} + I = ab + I = \overline{ab},\ \textit{CQFD.}$$

Il reste enfin à montrer la distributivité de $\times$ sur $+$ dans le quotient, mais ceci est immédiat en passant tout sous la barre et en utilisant les propriétés de $\times$ de l'anneau de départ :

$$\overline{a}\times\left(\overline{b}+\overline{c}\right) = \overline{a}\times\left(\overline{b+c}\right) = \overline{a\times(b+c)} = \overline{a\times b + a\times c} = \overline{a}\times\overline{b} + \overline{a}\times\overline{c}.$$

Conclusion générale.
Soit I un sous-groupe de $(A,+)$. La loi quotient $\overline{a}\times\overline{b} = \overline{a\times b}$ sur ${}^{A}\!/_{I}$ est bien définie si et seulement si I est un idéal bilatère de A et alors la projection canonique

$$\pi : \begin{cases} (A,+,\times) & \longrightarrow & \left({}^{A}\!/_{I},+,\times\right) \\ a & \longmapsto & \overline{a} = a + I \end{cases}$$

est un morphisme d'anneaux. Si de plus A est unitaire, alors ${}^{A}\!/_{I}$ est unitaire, et $1_{({}^{A}/_{I})} = \overline{1_A}$.

2.3 Quotient d'un espace vectoriel par un sous-espace vectoriel

Considérons un espace vectoriel $(E,+,\cdot)$ et F un sous-groupe de $(E,+)$. F étant distingué dans le groupe abélien $(E,+)$, on peut considérer le groupe quotient

$${}^{E}\!/_{F} = \{\overline{x} = x + F\ ;\ x \in E\}$$

muni de la loi $\overline{x}+\overline{y} = \overline{x+y}$.
Comme pour les anneaux, on aimerait rajouter une loi externe $\cdot$ de façon à ce que $\left({}^{E}\!/_{F},+,\cdot\right)$ devienne un espace vectoriel. Autant le faire sans se fatiguer, et poser $\lambda\cdot\overline{x} = \overline{\lambda\cdot x}$. Se pose à nouveau le problème de l'indépendance de $\overline{\lambda\cdot x}$ par rapport au représentant x de $\overline{x}$.

Si la définition est correcte, on doit avoir pour tout f de F, pour tout scalaire λ :

$$\overline{f} = f + F = F = \overline{0} \implies \lambda\overline{f} = \lambda\overline{0} \implies \overline{\lambda f} = \overline{\lambda 0} = \overline{0} \implies \lambda f \in F,$$

donc F doit être stable par multiplication scalaire ; comme F est déjà par hypothèse stable par somme, il en résulte que F doit être un sous-espace vectoriel de E.

Réciproquement, on a bien que, pour F sous-espace vectoriel de E,

$$\overline{x} = \overline{y} \implies x - y \in F \implies \lambda(x-y) \in F \implies \lambda x - \lambda y \in F \implies \overline{\lambda x} = \overline{\lambda y},$$

et donc la loi $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$ est bien définie sur ${}^{E}\!/_{F}$.

Les vérifications d'usage que $\left({}^{E}\!/_{F}, +, \cdot\right)$ est bien un espace vectoriel se font en passant tout sous la barre et en utilisant la structure d'espace vectoriel de E ; par exemple,

$$\lambda \cdot (\overline{x} + \overline{y}) = \lambda \cdot (\overline{x+y}) = \overline{\lambda \cdot (x+y)} = \overline{\lambda \cdot x + \lambda \cdot y} = \lambda \cdot \overline{x} + \lambda \cdot \overline{y}.$$

En dimension finie, on peut dire des choses concernant la dimension du quotient. On rappelle que si E est de dimension finie n, la *codimension* de F est définie par $\operatorname{codim} F = n - \dim F$.

Propriété.
Soit E un espace vectoriel de dimension finie, F un sous-espace vectoriel de E. On a alors :

$$\dim\left({}^{E}\!/_{F}\right) = \operatorname{codim} F.$$

Démonstration.
Soit $(e_1, ..., e_p)$ une base de F, que l'on complète en $(e_1, ..., e_p, e_{p+1}, ..., e_n)$ base de E. Alors $(\overline{e_{p+1}}, ..., \overline{e_n})$ est une base de ${}^{E}\!/_{F}$. En effet, elle est libre car

$$\sum_{i=p+1}^{n} \lambda_i \overline{e_i} = \overline{0} \implies \overline{\sum_{i=p+1}^{n} \lambda_i e_i} = \overline{0} \implies \sum_{i=p+1}^{n} \lambda_i e_i \in F \implies (\lambda_i) = (0)$$

par liberté de la base $(e_1, ..., e_n)$ et elle est génératrice car, pour $\overline{x} \in {}^{E}\!/_{F}$, x se décompose sur la base $(e_1, ..., e_n)$ en $x = \sum_{i=1}^{n} \lambda_i e_i$, d'où

$$\overline{x} = \overline{\sum_{i=1}^{n} \lambda_i e_i} = \overline{\underbrace{\sum_{i=1}^{p} \lambda_i e_i}_{\in F}} + \overline{\sum_{i=p+1}^{n} \lambda_i e_i} = \overline{0} + \sum_{i=p+1}^{n} \lambda_i \overline{e_i} \in \operatorname{Vect}\left(\overline{e_{p+1}}, ..., \overline{e_n}\right).$$

Petit complément.
Dans le cas où E est normé, on peut transporter la structure d'espace vectoriel normé dans le quotient ${}^{E}\!/_{F}$, sous réserve que le sous-espace vectoriel F par lequel on quotiente soit **fermé**. Le cararactère complet passe alors également au quotient au sens de la proposition suivante.

Proposition.
*Soit E un espace vectoriel normé, F un sous-espace vectoriel **fermé** de E. On peut définir une norme $\|\cdot\|$ sur ${}^{E}\!/_{F}$* par

$$\|\overline{x}\| = d(x, F) = \inf_{f \in F} \|x - f\|.$$

De plus, si E est complet, alors le quotient ${}^{E}\!/_{F}$ est complet pour la norme sus-décrite.

Démonstration.
Tout d'abord, $\|\overline{x}\| = d(x, F)$ est bien définie : deux représentants x et y d'une même classe différant d'un $f \in F$, ils vérifient

$$d(y, F) = d(y, F + f) = d(x + f, F + f) = d(x, F).$$

Vérifions ensuite les trois propriétés d'une norme :

• $\|\overline{x}\| = 0 \implies d(x,F) = 0 \implies x \in F$ car F est fermé.

• $\|\lambda\overline{x}\| = \left\|\overline{\lambda x}\right\| = d(\lambda x, F) = d(\lambda x, \lambda F) = |\lambda|\, d(x,F)$ car F est un sous-espace vectoriel (traiter à part le cas $\lambda = 0$).

• Pour l'inégalité triangulaire, on va être un peu plus fin. Soit x et y dans E et $\varepsilon > 0$. On prend des vecteurs f et g dans F tels que $\left\{ \begin{array}{l} \|x-f\| \leq d(x,F) + \varepsilon \\ \|y-g\| \leq d(y,F) + \varepsilon \end{array} \right.$, et on en déduit

$$\begin{aligned} \|\overline{x}+\overline{y}\| &= d(x+y,F) \leq \|(x+y)-(f+g)\| \leq \|x-f\| + \|y-g\| \\ &= d(x,F) + \varepsilon + d(y,F) + \varepsilon = \|\overline{x}\| + \|\overline{y}\| + 2\varepsilon, \end{aligned}$$

d'où le résultat en faisant tendre ε vers 0.

Supposons maintenant E complet et soit $(\overline{x_n})$ une suite de Cauchy de ${}^{E}\!/_{F}$. On a donc que, pour tout $n \in \mathbb{N}$, il existe un rang $\varphi(n)$ tel que

$$p, q \geq \varphi(n) \implies \|\overline{x_p} - \overline{x_q}\| \leq \frac{1}{2^n}.$$

Remarquer que l'on peut toujours imposer φ strictement croissante, quitte à remplacer φ par φ' définie par

$$\varphi'(n+1) = \max\{\varphi(n+1), \varphi'(n) + 1\}.$$

On en déduit $\left\|\overline{x_{\varphi(n+1)}} - \overline{x_{\varphi(n)}}\right\| \leq \frac{1}{2^n}$ pour tout n, *i.e.*

$$\inf_{f \in F} \left\|\left(x_{\varphi(n+1)} - x_{\varphi(n)}\right) - f\right\| \leq \frac{1}{2^n}.$$

Soit maintenant $f_n \in F$ tel que cet infimum soit atteint à moins de $\frac{1}{2^n}$, ce afin d'avoir

$$\left\|\left(x_{\varphi(n+1)} - x_{\varphi(n)}\right) - f_n\right\| \leq \left\|\overline{x_{\varphi(n+1)}} - \overline{x_{\varphi(n)}}\right\| + \frac{1}{2^n} \leq \frac{1}{2^n} + \frac{1}{2^n} = \frac{1}{2^{n-1}},$$

et posons

$$y_n = x_{\varphi(n)} + \sum_{i=0}^{n-1} f_i,$$

de façon à ce que la série $\sum (y_{n+1} - y_n)$ soit absolument convergente : en effet,

$$\begin{aligned} \sum_{n \geq 0} \|y_{n+1} - y_n\| &= \sum_{n \geq 0} \left\| x_{\varphi(n+1)} + \sum_{i=0}^{n} f_i - \left(x_{\varphi(n)} + \sum_{i=0}^{n-1} f_i \right) \right\| \\ &= \sum_{n \geq 0} \left\| x_{\varphi(n+1)} - x_{\varphi(n)} - f_n \right\| \leq \sum_{n \geq 0} \frac{1}{2^{n-1}} < \infty, \end{aligned}$$

et donc la série $\sum (y_{n+1} - y_n)$ converge simplement par complétude de E, *i.e.* y_n converge dans E vers un certain vecteur a. On en déduit

$$\left\|\overline{x_{\varphi(n)}} - \overline{a}\right\| = \left\|\overline{x_{\varphi(n)} - a}\right\| = \inf_{f \in F} \left\|\left(x_{\varphi(n)} - a\right) - f\right\| \leq \left\|\left(x_{\varphi(n)} - a\right) - \sum_{i=0}^{n-1} f_i\right\| = \|y_n - a\|$$

qui tend vers 0, *i.e.* $\overline{x_{\varphi(n)}}$ converge dans ${}^{E}\!/_{F}$ vers $\overline{a}$. On a trouvé une valeur d'adhérence $\overline{a}$ à la suite $(\overline{x_n})$, et comme $(\overline{x_n})$ est de Cauchy, elle converge vers cette valeur d'adhérence.

Conclusion générale.

Soit F un sous-groupe de $(E,+)$. La loi quotient $\lambda \cdot \overline{x} = \overline{\lambda \cdot x}$ sur ${}^{E}\!/_{F}$ est bien définie si et seulement si F est un sous-espace vectoriel de E et alors la projection canonique

$$\pi : \left\{ \begin{array}{ccc} (E,+,\cdot) & \longrightarrow & \left({}^{E}\!/_{F},+,\cdot\right) \\ x & \longmapsto & \overline{x} = x + F \end{array} \right.$$

est une application linéaire. Si de plus E est de dimension finie, alors

$$\dim\left({}^{E}\!/_{F}\right) = \operatorname{codim} F.$$

Conclusion complémentaire.

Si E est normé par $\|\cdot\|$ et si F est un sous-espace vectoriel ***fermé*** *de E, alors ${}^{E}\!/_{F}$ est normé pour $\|\overline{x}\| = d(x,F) = \inf_{f\in F}\|x-f\|$. Si de surcroît E est un Banach, alors ${}^{E}\!/_{F}$ est un Banach pour la norme ci-dessus.*

2.4 Quotient d'une algèbre unitaire par un idéal

Considérons une algèbre $(A,+,\times,\cdot)$ unitaire et I un sous-groupe de $(A,+)$. On peut considérer le quotient

$$ {}^{A}\!/_{I} = \{\overline{a} = a + I \ ; \ a \in A\}$$

muni de la loi $\overline{a} + \overline{b} = \overline{a+b}$.

On aimerait rajouter une loi $\times$ et une loi $\cdot$ de sorte que ${}^{A}\!/_{I}$ soit une algèbre avec les lois agréables

$$\left\{ \begin{array}{c} \lambda \cdot \overline{a} = \overline{\lambda \cdot a} \\ \overline{a} \times \overline{b} = \overline{ab} \end{array} \right. .$$

${}^{A}\!/_{I}$ devra en particulier être un anneau pour la loi quotient $\times$, donc I devra être un idéal bilatère de A. L'algèbre A étant unitaire, tout idéal est stable par multiplication scalaire en vertu de l'identité :

$$\lambda \cdot i = (\lambda \cdot 1) \times i.$$

Ainsi, en utilisant les résultats des deux paragraphes qui précèdent, on peut conclure, les propriétés d'une algèbre s'obtenant en passant tout sous la barre.

Conclusion générale.

Soit I un sous-groupe de $(A,+)$. Les lois quotients $\left\{ \begin{array}{c} \lambda \cdot \overline{a} = \overline{\lambda \cdot a} \\ \overline{a} \times \overline{b} = \overline{ab} \end{array} \right.$ *sur ${}^{A}\!/_{I}$ sont bien définies si et seulement si I est un idéal de A et alors la projection canonique*

$$\pi : \left\{ \begin{array}{ccc} (A,+,\times,\cdot) & \longrightarrow & \left({}^{A}\!/_{I},+,\times,\cdot\right) \\ a & \longmapsto & \overline{a} = a + I \end{array} \right.$$

est un morphisme d'algèbres.

3 Factorisation canonique des morphismes, théorèmes d'isomorphismes

3.1 Factorisation canonique d'une application quelconque

Soit f une application d'un ensemble E non vide dans un ensemble F non vide, ce que l'on note usuellement

$$f : \left\{ \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right. .$$

Généralement, f n'a aucune raison d'être injective, surjective, *a fortiori* bijective.

Observer que l'on peut toujours la "rendre" surjective en considérant l'application

$$f' : \left\{ \begin{array}{ccc} E & \longrightarrow & \operatorname{Im} f \\ x & \longmapsto & f(x) \end{array} \right. .$$

On n'a modifié en rien la façon dont f agit sur E, on a juste changé l'ensemble d'arrivée.

Cependant, il est plus difficile de rendre une application injective. L'ennui est qu'à une image $f(x)$ on pourrait trouver deux antécédents x et y (ou même plus) distincts. Le nombre d'antécédents nous ennuie ? Qu'à

cela ne tienne : pour une image $f(x)$ donnée, on regroupe tous ses antécédents, on les met dans un sac étiqueté $\overline{x}$, on note $\overline{E}$ l'ensemble des sacs d'antécédents, et on considère l'application

$$\widetilde{f} : \left\{ \begin{array}{ccc} \overline{E} & \longrightarrow & F \\ \overline{x} & \longmapsto & f(x) \end{array} \right. .$$

Avant, pour une image $f(x)$ donnée, on avait plusieurs antécédents par f ; maintenant, on en toujours autant (par f), mais en les regroupant et en les ficelant, il n'en reste qu'un seul par $\widetilde{f}$, qui est son sac d'antécédents par f. Il en résulte que $\widetilde{f}$ est injective.

Si l'on souhaite formaliser ce qui précède, on consière la relation d'équivalence $\sim$ sur E définie par $x \sim y \iff f(x) = f(y)$, on note $\overline{x}$ la classe d'un élément x de E, $\overline{E}$ l'ensemble quotient ${}^{E}\!/_{\sim}$, et on a alors

$$\widetilde{f}(\overline{x}) = \widetilde{f}(\overline{y}) \implies f(x) = f(y) \implies \overline{x} = \overline{y},$$

d'où l'injectivité de $\widetilde{f}$. Mais l'on voit peut-être moins ce qui se passe...

Si l'on résume les deux tranformations que l'on a effectuées, on peut "injectiviser" f en ligottant les éléments ayant même image, on obtient alors une application $\widetilde{f} : \left\{ \begin{array}{ccc} \overline{E} & \longrightarrow & F \\ \overline{x} & \longmapsto & f(x) \end{array} \right.$, puis on peut "surjectiviser" $\widetilde{f}$ en changeant l'ensemble d'arrivée, ce qui donne au final une application bijective $\overline{f} : \left\{ \begin{array}{ccc} \overline{E} & \longrightarrow & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right.$.

Pour faire le lien avec l'application $f : \left\{ \begin{array}{ccc} E & \longrightarrow & F \\ x & \longmapsto & f(x) \end{array} \right.$ de départ, la première transformation consiste envoyer un élément x de E sur sa classe $\overline{x}$ dans $\overline{E}$, ce qui se fait au moyen de la projection canonique

$$\pi : \left\{ \begin{array}{ccc} E & \longrightarrow & \overline{E} \\ x & \longmapsto & \overline{x} \end{array} \right. .$$

Puis on envoie le paquet $\overline{x}$ d'antécédents sur son unique image $f(x)$, ce qui se fait via l'application bijective

$$\overline{f} : \left\{ \begin{array}{ccc} \overline{E} & \longrightarrow & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right. .$$

À ce stade, notre élément x de départ est rendu dans $\operatorname{Im} f$, mais on voudrait retomber sur nos pieds, *i.e.* l'envoyer dans F ; c'est pourquoi on considère l'injection canonique

$$\iota : \left\{ \begin{array}{ccc} \operatorname{Im} f & \longrightarrow & F \\ x & \longmapsto & x \end{array} \right. .$$

Finalement, on a le parcours suivant :

$$E \xrightarrow{\pi} \overline{E} \xrightarrow{\overline{f}} \operatorname{Im} f \xrightarrow{\iota} F$$
$$f = \iota \circ \overline{f} \circ \pi.$$

C'est ce qu'on appelle la *factorisation canonique* de f (factorisation pour la loi $\circ$, bien sûr) En général, on aime bien représenter ces deux dernières relations sur un schéma, appelé *diagramme* (c'est juste des ensembles avec des flèches représentant des applications entre ces ensembles) *commutatif* (ca veut dire que, quand on suit les flèches le long de deux chemins différents qui mènent de A à B, les composées d'applications que l'on considère sont égales) :

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow \pi & & \uparrow \iota \\ \overline{E} & \xrightarrow{\overline{f}} & \operatorname{Im} f \end{array} .$$

Le point important à remarquer est que l'on dispose d'une bijection $\overline{f}$ reliant le quotient $\overline{E}$ à l'image $\operatorname{Im} f$. On verra bientôt la factorisation canonique des morphismes où cette bijection devient un isomorphisme qu'il est très souvent opportun de considérer.

3.2 Factorisation canonique d'un morphisme de groupes

Considérons G et H deux groupes et f un morphisme de groupes de G dans H, c'est-à-dire que pour tout x, y dans G on a

$$f(xy) = f(x) f(y).$$

On a déjà vu que la relation "x et y ont même image par f" définissait une relation d'équivalence sur G, déterminée par

$$\begin{aligned} f(y) = f(x) &\iff f(x)^{-1} f(y) = 1_H \iff f\left(x^{-1}\right) f(y) = 1_H \iff f\left(x^{-1}y\right) = 1_H \\ &\iff x^{-1}y \in \operatorname{Ker} f \iff y \in x \operatorname{Ker} f \iff y = x \pmod{\operatorname{Ker} f}, \end{aligned}$$

donc la relation considérée est la relation de congruence modulo $\operatorname{Ker} f$. Cela se comprend bien : les éléments du noyau de f n'ayant aucune action vis-à-vis de f, l'égalité modulo un élément du noyau se traduit nécessairement par une égalité des images.

Si l'on reprend les notations de la partie précédente, on a donc que l'ensemble quotient $\overline{G}$ est égal à ${}^{G}\!/_{\operatorname{Ker} f}$. Pour munir ce dernier d'une structure de groupe pour la loi quotient, il convient de vérifier que $\operatorname{Ker} f$ est distingué dans G. Pour $k \in \operatorname{Ker} f$ et $g \in G$ on a

$$f\left(x^{-1}kx\right) = f\left(x^{-1}\right) f(k) f(x) = f(x)^{-1} 1_H f(x) = f(x)^{-1} f(x) = 1_H,$$

d'où $x^{-1}kx \in \operatorname{Ker} f$; donc $x^{-1}(\operatorname{Ker} f)\, x \subset \operatorname{Ker} f$, *i.e.* $\operatorname{Ker} f \lhd G$ comme voulu.

D'autre part, la bijection $\overline{f} : \left\{ \begin{array}{ccc} {}^{G}\!/_{\operatorname{Ker} f} & \longrightarrow & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right.$ est un morphisme de groupes puisque

$$\overline{f}(\overline{x} \cdot \overline{y}) = \overline{f}(\overline{x \cdot y}) = f(xy) = f(x) f(y) = \overline{f}(\overline{x})\, \overline{f}(\overline{y})$$

(remarquer que ceci découle de ce que f est un morphisme ainsi que des lois quotients), la projection canonique π est également un morphisme de groupes (par construction de la loi quotient), et de même trivialement pour l'injection canonique ι.

On a donc la décomposition canonique de f en morphismes de groupes $f = \iota \circ \overline{f} \circ \pi$, ce que l'on peut représenter par le diagramme commutatif

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow \pi & & \uparrow \iota \\ {}^{G}\!/_{\operatorname{Ker} f} & \xrightarrow{\overline{f}} & \operatorname{Im} f \end{array}.$$

On dispose également de l'isomorphisme de groupes

$${}^{G}\!/_{\operatorname{Ker} f} \simeq \operatorname{Im} f.$$

Le caractère bijectif a déjà été expliqué dans le cas général (à une image correspond son unique paquet d'antécédents), et le caractère de morphisme vient juste de celui de f ainsi que de la structure de groupe qui passe de G à ${}^{G}\!/_{\operatorname{Ker} f}$ via la loi quotient.

On retiendra de tout ceci que, si $f : G \longrightarrow H$ est un morphisme de groupes, alors le noyau $\operatorname{Ker} f$ est distingué dans G et on a l'isomorphisme de groupes

$$\left\{ \begin{array}{ccc} {}^{G}\!/_{\operatorname{Ker} f} & \simeq & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right. .$$

3.3 Factorisation canonique d'un morphisme d'anneaux

Considérons A et B deux anneaux et f un morphisme d'anneaux de A dans B, c'est-à-dire que pour tout a, b, c dans A on a

$$f(ab+c) = f(a)\,f(b) + f(c).$$

Comme pour le cas d'un groupe, la relation "a et b ont même image par f" définit une relation d'équivalence sur A, donnée par

$$f(b) = f(a) \iff f(b-a) = 0_B \iff b - a \in \operatorname{Ker} f \iff b \in a + \operatorname{Ker} f,$$

i.e. la relation de congruence modulo $\operatorname{Ker} f$ (cette fois au sens de la loi $+$).

Toujours en suivant la première partie, on en déduit que l'ensemble quotient $\overline{A}$ est égal à ${}^{A}\!/_{\operatorname{Ker} f}$. Pour munir ce dernier d'une struture d'anneau pour les lois quotients, il suffit de montrer que $\operatorname{Ker} f$ est un idéal bilatère de A. Déjà, $\operatorname{Ker} f$ est un sous-groupe de $(A,+)$ en tant que noyau d'un morphisme de groupes additifs, et de plus, pour tout i dans $\operatorname{Ker} f$, pour tout a dans A, on a

$$f(ai) = f(a)\,f(i) = f(a)\,0_B = 0_B,$$

d'où $ai \in \operatorname{Ker} f$, et de même $ia \in \operatorname{Ker} f$. Il en résulte que $\operatorname{Ker} f$ est bien un idéal bilatère de A.

D'autre part, la bijection $\overline{f} : \left\{ \begin{array}{ccc} {}^{A}\!/_{\operatorname{Ker} f} & \longrightarrow & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{array} \right.$ est un morphisme d'anneaux puisque

$$\overline{f}\left(\overline{a}\overline{b} + \overline{c}\right) = \overline{f}\left(\overline{ab+c}\right) = f(ab+c) = f(a)\,f(b) + f(c) = \overline{f}(\overline{a})\,\overline{f}\left(\overline{b}\right) + \overline{f}(\overline{c})$$

(remarquer encore une fois que ceci découle de ce que f est un morphisme, ainsi que des lois quotients), la projection canonique π est aussi un morphisme d'anneaux (par construction des lois quotients), et idem pour l'injection canonique ι.

On a donc la décomposition canonique de f en morphismes d'anneaux $f = \iota \circ \overline{f} \circ \pi$, ce que l'on peut récapituler à l'aide du diagramme commutatif

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \downarrow \pi & & \uparrow \iota \\ {}^{A}\!/_{\operatorname{Ker} f} & \xrightarrow{\overline{f}} & \operatorname{Im} f \end{array},$$

ainsi que l'isomorphisme d'anneaux

$${}^{A}\!/_{\operatorname{Ker} f} \simeq \operatorname{Im} f.$$

Le caractère bijectif a déjà été commenté et se voit bien (à une image $f(a)$ correspond son unique paquet d'antécédents : $a + \operatorname{Ker} f$), et le caractère de morphisme découle comme dans le cas des groupes de celui de f ainsi que de la structure d'anneau qui passe de A à ${}^{A}\!/_{\operatorname{Ker} f}$ via les lois quotients.

Petit supplément sur le caratère unitaire : si f est un morphisme d'anneaux *unitaires*, *i.e.* si A et B sont unitaires et si $f(1_A) = 1_B$, alors $\overline{f}$ est aussi un morphisme d'anneaux unitaires puisque

$$\overline{f}\left(\overline{1_A}\right) = f(1_A) = 1_B = 1_{\operatorname{Im} f}.$$

On retiendra de tout ceci que, si $f : A \longrightarrow B$ est un morphisme d'anneaux (unitaires), alors le noyau $\operatorname{Ker} f$ est un idéal bilatère de A et on a l'isomorphisme d'anneaux (unitaires)

$$\left\{ \begin{array}{ccc} {}^{A}\!/_{\operatorname{Ker} f} & \simeq & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{array} \right. .$$

3.4 Factorisation canonique d'une application linéaire

Considérons E et F deux K-espaces vectoriels et f une application linéaire de E dans F, c'est-à-dire que pour tout x, y dans E et pour tout λ dans K on a

$$f(\lambda x + y) = \lambda f(x) + f(y).$$

Comme dans les cas précédents, la relation "x et y ont même image par f" définit une relation d'équivalence sur E, donnée par

$$f(x) = f(y) \iff f(y - x) = 0 \iff y - x \in \operatorname{Ker} f \iff y \in x + \operatorname{Ker} f,$$

i.e. la relation de congruence modulo $\operatorname{Ker} f$ (au sens de la loi $+$).

Toujours en suivant la première partie, on en déduit que l'ensemble quotient $\overline{E}$ est égal à ${}^{E}\!/_{\operatorname{Ker} f}$. Pour munir ce dernier d'une struture d'espace vectoriel pour les lois quotients, il suffit de montrer que $\operatorname{Ker} f$ est un sous-espace vectoriel de E. Or, c'est immédiat, car pour tout x, y dans $\operatorname{Ker} f$ et pour tout λ dans K, on a

$$f(\lambda x + y) = \lambda f(x) + f(y) = \lambda 0 + 0 = 0,$$

i.e. $\lambda x + y \in \operatorname{Ker} f$, d'où $\operatorname{Ker} f$ stable par combinaisons linéaires.

D'autre part, la bijection $\overline{f} : \left\{ \begin{array}{ccc} {}^{E}\!/_{\operatorname{Ker} f} & \longrightarrow & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right.$ est linéaire puisque

$$\overline{f}(\lambda \overline{x} + \overline{y}) = \overline{f}\left(\overline{\lambda x + y}\right) = f(\lambda x + y) = \lambda f(x) + f(y) = \lambda \overline{f}(\overline{x}) + \overline{f}(\overline{y})$$

(est-ce la peine de redire que ceci découle du fait que f est linéaire, ainsi que des lois quotients ?), la projection canonique π est aussi linéaire (par construction des lois quotients), et idem pour l'injection canonique.

On a donc la décomposition canonique de f en applications linéaires $f = \iota \circ \overline{f} \circ \pi$, le diagramme commutatif qui va avec

$$\begin{array}{ccc} E & \xrightarrow{f} & F \\ \downarrow \pi & & \uparrow \iota \\ {}^{E}\!/_{\operatorname{Ker} f} & \xrightarrow{\overline{f}} & \operatorname{Im} f \end{array},$$

et l'isomorphisme d'espaces vectoriels

$${}^{E}\!/_{\operatorname{Ker} f} \simeq \operatorname{Im} f.$$

Si E est de dimension finie, on en déduit en particulier que $\operatorname{Im} f$ est de dimension finie et que $\dim \operatorname{Im} f = \dim\left({}^{E}\!/_{\operatorname{Ker} f}\right) = \operatorname{codim} \operatorname{Ker} f$, d'où l'importantissime *théorème du rang* :

$$\operatorname{rg} f + \dim \operatorname{Ker} f = \dim E.$$

On retiendra de tout ceci **trois** choses : si $f : E \longrightarrow F$ est linéaire, alors le noyau $\operatorname{Ker} f$ est un sous-espace vectoriel de E, on a l'isomorphisme d'espaces vectoriels

$$\left\{ \begin{array}{ccc} {}^{E}\!/_{\operatorname{Ker} f} & \simeq & \operatorname{Im} f \\ \overline{x} & \longmapsto & f(x) \end{array} \right.,$$

et si de plus E est de dimension finie alors

$$\operatorname{rg} f + \dim \operatorname{Ker} f = \dim E.$$

3.5 Factorisation canonique d'un morphisme d'algèbres unitaires

Considérons A et B deux K-algèbres unitaires et f un morphisme d'algèbres unitaires de A dans B, c'est-à-dire que pour tout a, b, c dans A et pour tout λ dans K on a

$$f(\lambda a + bc) = \lambda f(a) + f(b) f(c) \text{ et } f(1_A) = 1_B.$$

f est en particulier un morphisme d'anneaux unitaires, donc $\operatorname{Ker} f$ est un idéal bilatère de A et on a l'isomorphisme d'anneaux unitaires

$$\overline{f} : \left\{ \begin{array}{ccc} {}^{A}\!/_{\operatorname{Ker} f} & \simeq & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{array} \right. .$$

f étant par ailleurs une application linéaire, $\overline{f}$ est également un isomorphisme d'espaces vectoriels.

Conclusion : si $f : A \longrightarrow B$ est un morphisme d'algèbres unitaires, alors le noyau $\operatorname{Ker} f$ est un idéal bilatère de A et on a l'isomorphisme d'algèbres unitaires

$$\left\{ \begin{array}{ccc} {}^{A}\!/_{\operatorname{Ker} f} & \simeq & \operatorname{Im} f \\ \overline{a} & \longmapsto & f(a) \end{array} \right. .$$

4 Un exemple important : quotient d'anneaux de polynômes

4.1 Introduction

Soit K un corps commutatif On considère l'anneau commutatif $K[X]$ des polynômes à coefficients dans K. Fixons-nous un polynôme $P = \sum_{i=0}^{d} a_i X^i$ de degré $d \geq 1$. Notre but est de chercher à scinder P.

Évidemment, cela n'est pas toujours possible, prendre par exemple $P = X^2 + 1$ dans $\mathbb{R}[X]$. Cependant, on peut trouver une extension de corps de $\mathbb{R}$ où P est scindé : prendre tout simplement $\mathbb{C}$, où $P = (X + i)(X - i)$. Noter que, ensemblistement, $\mathbb{R}$ n'est pas vraiment inclus dans $\mathbb{C}$, mais que l'on peut en revanche l'injecter dans $\mathbb{C}$ en conservant sa structure de corps ; on dit qu'*on plonge* $\mathbb{R}$ *dans* $\mathbb{C}$. Par exemple, si $\mathbb{C}$ a été construit comme $\mathbb{R}^2$ muni des lois

$$\left\{ \begin{array}{c} (x, y) + (x', y') = (x + x', y + y) \\ (x, y) \times (x', y') = (xx' - yy', xy' + x'y) \end{array} \right. ,$$

on peut considérer le morphisme de corps $\varphi : \left\{ \begin{array}{ccc} \mathbb{R} & \hookrightarrow & \mathbb{C} \\ x & \longmapsto & \widetilde{x} = (x, 0) \end{array} \right.$ qui injecte bien $\mathbb{R}$ dans $\mathbb{C}$; φ est alors appelée *plongement de* $\mathbb{R}$ *dans* $\mathbb{C}$.

Si l'on écrit les choses proprement, ce n'est *pas* le polynôme $P = X^2 + 1$ de départ qui devient scindé – P reste de toute façon égal à $(X_{\mathbb{R}})^2 + 1_{\mathbb{R}}$, le $\mathbb{R}$ en indice rappelant le corps de base où sont pris les coefficients du polynôme –, mais le plongé de P dans $\mathbb{C}[X]$ par l'application

$$\Phi : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \hookrightarrow & \mathbb{C}[X] \\ \sum_{k=0}^{n} \lambda_k (X_{\mathbb{R}})^k & \longmapsto & \sum_{k=0}^{n} \widetilde{\lambda_k} (X_{\mathbb{C}})^k \end{array} \right.$$

qui plonge naturellement $\mathbb{R}[X]$ dans $\mathbb{C}[X]$. On obtient donc un polynôme $P_{\mathbb{C}} = (X_{\mathbb{C}})^2 + 1_{\mathbb{C}}$ (à coefficients dans $\mathbb{C}$) qui *lui* est scindé.

On va montrer qu'on peut toujours, de façon analogue au cas de $\mathbb{R}$ et $\mathbb{C}$, injecter le corps de base K dans un corps plus grand où le polynôme P sera scindé.

4.2 Quotient par un polynôme, théorèmes de plongement

L'ensemble $(P) := P\,K[X]$ des polynômes multiples de P étant un idéal de $K[X]$, on peut considérer l'anneau quotient ${}^{K[X]}\!/_{(P)}$, généralement noté ${}^{K[X]}\!/_{P}$ par commodité. En notant $\overline{A}$ la classe d'un polynôme A, on a donc l'équivalence

$$\overline{A} = \overline{B} \iff P \mid A - B.$$

Proposition.
${}^{K[X]}\!/_{P}$ est une K-algèbre unitaire de dimension d de base canonique $\left(\overline{1}, \overline{X}, ..., \overline{X^{d-1}}\right)$. On a en particulier l'isomorphisme d'espaces vectoriels

$${}^{K[X]}\!/_{P} \simeq K^{\deg P}.$$

Démonstration.
• (P) étant un idéal de $K[X]$, ${}^{K[X]}\!/_{P}$ est une K-algèbre pour les lois quotients.
• Soit $\overline{A}$ un élément de ${}^{K[X]}\!/_{P}$. Pour montrer que la famille $\left(\overline{1}, \overline{X}, ..., \overline{X^{d-1}}\right)$ engendre ${}^{K[X]}\!/_{P}$, on effectue la division euclidienne de A par P : $A = PB + R$ avec $\deg R < d$, d'où

$$\overline{A} = \overline{PB + R} = \overline{PB} + \overline{R} = \overline{0}\overline{B} + \overline{R} = \overline{R} \in \mathrm{Vect}\{\overline{1}, \overline{X}, ..., \overline{X^{d-1}}\}$$

comme souhaité.
• Montrons maintenant que la famille $\left(\overline{1}, \overline{X}, ..., \overline{X^{d-1}}\right)$ est libre. Soient $\lambda_0, ..., \lambda_{d-1}$ des scalaires tels que $\sum_{i=0}^{d-1} \lambda_i \overline{X^i} = \overline{0}$. On a donc $P \mid \sum_{i=0}^{d-1} \lambda_i X^i$, *i.e.* $\sum_{i=0}^{d-1} \lambda_i X^i = PA$ pour un polynôme A : si $A \neq 0$, *i.e.* si $\deg A \geq 0$, on a

$$d = \deg P \leq \deg P + \deg A = \deg(PA) = \deg\left(\sum_{i=0}^{d-1} \lambda_i X^i\right) < d, \textit{ absurde.}$$

Donc $A = 0$ et $\sum_{i=0}^{d-1} \lambda_i X^i = 0$, *i.e.* $(\lambda_i) = (0)$ comme voulu.

L'opération de quotientage permet donc d'"augmenter" la taille de K, puisque l'on passe de la dimension 1 (le corps K en tant que K-espace vectoriel) en dimension $d = \deg P$ (le quotient ${}^{K[X]}\!/_{P}$ est isomorphe à K^d) ; cependant, on perd généralement la structure de corps (on a simplement une algèbre). La proposition suivante donne une condition nécessaire et suffisante pour que le quotientage conserve la structure de corps.

Proposition.
${}^{K[X]}\!/_{P}$ est un corps si et seulement si P est irréductible dans $K[X]$.

Démonstration.
• Supposons que ${}^{K[X]}\!/_{P}$ soit un corps. Si $P = AB$, on a alors $\overline{A}\,\overline{B} = \overline{AB} = \overline{P} = \overline{0}$, donc (puisque tout corps est intégre) $\overline{A}$ ou $\overline{B}$ vaut $\overline{0}$, mettons $\overline{A} = \overline{0}$, *i.e.* $P \mid A$. Puisque l'on a pris au départ P de degré ≥ 1, P est non nul, donc A non plus (car $P = AB$), donc $\deg A \geq \deg P = \deg A + \deg B$, d'où $\deg B \leq 0$, *i.e.* $\deg B = 0$ (car $B \neq 0$ à cause de $P = AB$), ou encore B constant. P est donc bien irréductible dans $K[X]$.
• Supposons que P soit irréductible dans $K[X]$. Déjà, $\overline{1} \neq \overline{0}$, sinon

$$\overline{P} = \overline{0} = \overline{1} \implies P \mid 1 \implies P \text{ constant, } \textit{absurde.}$$

De plus, si $\overline{A}$ est un élément non nul de ${}^{K[X]}\!/_{P}$, on a $\overline{A} \neq \overline{0}$, *i.e.* $P \nmid A$, ou encore P premier avec A, d'où par Bezout l'existence de U et V dans $K[X]$ tels que $AU + PV = 1$, et donc

$$\overline{1} = \overline{AU + PV} = \overline{A}\,\overline{U} + \overline{0}\,\overline{V} = \overline{A}\,\overline{U},$$

donc $\overline{A}$ est inversible. Il en résulte que ${}^{K[X]}\!/_{P}$ est un corps.

On arrive maintenant au théorème principal :

Théorème.

Si P est irréductible dans $K[X]$, il existe une extension de corps L de K où P admet une racine.

Démonstration.
Posons $L = {}^{K[X]}\!/_{P}$, qui est bien un corps d'après la proposition précédente. On note X_K le polynôme $(0, 1_K, 0, ...)$ de $K[X]$, et X_L le polynôme $(0, 1_L, 0, ...)$ de $L[X]$.

On plonge alors K dans L via l'application $\varphi : \begin{cases} K \longrightarrow L \\ \lambda \longmapsto \overline{\lambda} \end{cases}$ qui est bien un morphisme de corps au vu des lois quotients de L, puis on plonge $K[X]$ dans $L[X]$ via l'application $\Phi : \begin{cases} K[X] & \longrightarrow & L[X] \\ \sum_{i=0}^{n} \lambda_i (X_K)^i & \longmapsto & \sum_{i=0}^{n} \overline{\lambda_i} (X_L)^i \end{cases}$.

Le polyôme $P = \sum_{i=0}^{d} a_i (X_K)^i$ devient alors un polynôme

$$\Phi(P) = \sum_{i=0}^{d} \overline{a_i} (X_L)^i$$

à coefficients dans le plongé $\varphi(K)$ de K dans L, et si l'on note $\xi = \overline{X_K}$ (qui est un élément de L), on a

$$\Phi(P)(\xi) = \sum_{i=0}^{d} \overline{a_i}\xi^i = \sum_{i=0}^{d} \overline{a_i} \left(\overline{X_K}\right)^i = \sum_{i=0}^{d} \overline{a_i}\overline{(X_K)^i} = \sum_{i=0}^{d} \overline{a_i (X_K)^i} = \overline{\sum_{i=0}^{d} a_i (X_K)^i} = \overline{P} = \overline{0} = 0_L,$$

d'où une racine $\xi \in L$ au polynôme $\Phi(P)$.

On remarquera bien que ce n'est pas vraiment le polynôme P de départ qui devient scindé par miracle, mais c'est son plongé $\Phi(P)$ dans l'extension L adéquate qui l'est. Comme le prolongement est (par définition d'un plongement...) injectif, on idenfie P à $\Phi(P)$, et on dit alors (abusivement) que P est scindé dans L.

On peut enfin en déduire le résultat annoncé en début de partie :

Corollaire.
Soit P un polynôme de $K[X]$. Il existe une extension de corps L de K où P est scindé.

Démonstration.
On raisonne par récurrence sur le degré de P.
• Si $\deg P = 1$, P est trivialement scindé sur K.
• Soit $d \geq 2$; on suppose que pour tout corps K, pour tout polynôme A de degré $1 \leq n < d$ à coefficients dans K, on peut trouver une extension de K où A est scindé. Soit maintenant P un polynôme dans $K[X]$ de degré d.

Si P n'est pas irréductible, P peut s'écrire $P = AB$ avec A et B non constants, *i.e.* $1 \leq \deg A, \deg B < d$. En appliquant l'hypothèse de récurrence au corps K et au polyôme A, on peut trouver une extension L de K où A est scindé, puis une extension M de L où B est scindé. Il est alors clair que $P = AB$ est scindé dans $M[X]$.

Si P est irréductible, en appliquant le théorème précédent, on peut trouver une extension L de K où P admet une racine $\xi \in L$, donc P se factorise dans $L[X]$ en $P = (X - \xi) B$ où $1 \leq \deg B < d$; on procède alors comme dans le premier point.

4.3 Applications

4.3.1 Réduction – existence de valeur propres

Un des intérêts de scinder P est de pouvoir en exhiber une racine. Par exemple, en théorie de la réduction, si A est un endomorphisme de K^n où $n \geq 1$ et $\chi_A = \det(XI_n - A)$ son polynôme caractéristique, on peut montrer que

A est nilpotent si et seulement si $\chi_A = X^n$.

Le sens réciproque est immédiat par Cayley-Hamilton, et l'autre sens *semble* facile : si λ une valeur propre de A, x un vecteur propre associé, p l'indice de nilpotence de A, on a $0 = A^p(x) = \lambda^p x$, d'où $\lambda^p = 0$ puis $\lambda = 0$, et comme le spectre de A est exactement l'ensemble des zéros de χ_A, on en déduit que $\chi_A = (X - 0)^d$

où $d = \deg \chi_A = n$ comme souhaité. Problème de ce raisonnement : il est creux si le spectre de A est vide – par exemple, pour $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ dans $\mathbb{R}^2$.

Pour le faire proprement, considérons une extension L de K où χ_A est scindé. Plus précisément, si l'on note $\overline{A}$ la matrice A où l'on a remplacé les coefficients par leur plongés dans L, $\overline{A}$ est un endomorphisme de L^n, et

$$\chi_{\overline{A}} = \det\left(X_L I_n - \overline{A}\right)$$

n'est autre que le plongé de χ_A dans $L[X]$ (pour le voir, développer le déterminant, et utiliser le fait que les lois de L prolongent celles de K). Puisque $\chi_{\overline{A}}$ est scindé, il s'écrit $\chi_{\overline{A}} = \prod_{i=1}^{n}(X - \xi_i)$, avec $\operatorname{Sp} A = \{\xi_1, ..., \xi_n\}$ qui est bien non vide, et donc on peut appliquer le raisonnement qui ne marchait à $\overline{A}$ (qui est bien nilpotent, car $\overline{A}^p = \overline{A^p} = \overline{0}$), ce qui donne $\chi_{\overline{A}} = (X_L)^n$, d'où (par injectivité du plongement) $\chi_A = (X_K)^n$.

4.3.2 Extensions de corps par ajout d'éléments "à la main"

En pratique, il est très courant d'étendre des corps en rajoutant des éléments vérifiant telle ou telle propriété exprimable à l'aide d'une égalité polynomiale. Par exemple, on souhaite rajouter à $\mathbb{R}$ un élément i vérifiant $i^2 = -1$, ce qui revient à rajouter une racine i au polynôme irréductible $X^2 + 1$. On le fait tout simplement en considérant le quotient $\mathbb{R}[X]/_{X^2+1}$, qui est bien un corps car $X^2 + 1$ est irréductible sur $\mathbb{R}[X]$. On se doute bien qu'on va retomber sur $\mathbb{C}$...

Pour le montrer proprement, considérons le morphisme d'anneaux

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{R}[X] & \longrightarrow & \mathbb{C} \\ P & \longmapsto & P_{\mathbb{C}}(i) \end{array} \right.$$

et intéressons-nous à son noyau afin de préciser l'isomorphisme d'anneaux $\mathbb{R}[X]/_{\operatorname{Ker}\varphi} \simeq \operatorname{Im}\varphi$.

Si $P \in \operatorname{Ker}\varphi$, i est racine de $P_{\mathbb{C}}$, donc le conjugué $-i$ de i est également une racine de $P_{\mathbb{C}}$ (puisque $P_{\mathbb{C}}$ est à coefficients réels – enfin, dans le plongé de $\mathbb{R}$, quoi...), donc $(X_{\mathbb{C}})^2 + 1 = (X_{\mathbb{C}} - i)(X_{\mathbb{C}} + i) \mid P_{\mathbb{C}}$, *i.e.* $P_{\mathbb{C}} = A\left((X_{\mathbb{C}})^2 + 1\right)$ où $A \in \mathbb{C}[X]$. Or, il est facile voir que, si L est une extension de K, et que $P = AQ$ avec P, Q dans $K[X]$, A dans $L[X]$, alors A est nécessairement à coefficients dans K aussi (regarder d'abord les termes de plus haut degré, puis récurrer vers le bas). On en déduit que A est dans le plongé de $\mathbb{R}[X]$, d'où (par injectivité du plongement) $X^2 + 1 \mid P$. Comme il est de plus clair que $X^2 + 1 \mid P \implies P \in \operatorname{Ker}\varphi$, on en déduit

$$\operatorname{Ker}\varphi = \left(X^2 + 1\right)\mathbb{R}[X].$$

On peut alors appliquer le théorème d'isomorphisme d'anneaux en remarquant que φ est surjective ($\varphi(bX + a) = a + ib$), ce qui donne $\mathbb{R}[X]/_{(X^2+1)\mathbb{R}[X]} \simeq \operatorname{Im}\varphi$, *i.e.*

$$\mathbb{R}[X]/_{X^2+1} \simeq \mathbb{C}.$$

On peut même cela comme définition de $\mathbb{C}$, qui a le grand avantage de vérifier immédiatement l'existence d'un i tel que $i^2 = -1$ *par construction*. On est souvent amené en algèbre à construire ainsi des corps en rajoutant un racine à tel ou tel polynôme. Le procédé est analogue pour les anneaux, en remarquant que tout ce qui a été dit plus haut est adaptable en remplaçant le corps K de base par un anneau intègre. Par exemple, en rajoutant dans $\mathbb{Z}$ un élément i tel que $i^2 = -1$, ce qui revient à considérer le quotient $\mathbb{Z}[X]/_{X^2+1}$, on tombe sur l'ensemble $\mathbb{Z}[i] = \left\{a + ib \text{ où } (a, b) \in \mathbb{Z}^2\right\}$ des entiers de Gauss.

4.3.3 Détermination des corps finis de petit cardinal

Un autre exemple important du quotientage par des polynômes et la recherce des corps finis de petit cardinal. Par exemple, pour construire le corps à 4 éléments, on peut remarquer que

$$4 = \#\left(\left(\mathbb{Z}/_{2\mathbb{Z}}\right)^2\right) = \#\left(\mathbb{Z}/_{2\mathbb{Z}}[X]/_{P}\right)$$

où P est n'importe quel polynôme irréductible de degré 2 – *i.e.* sans racines. En cherchant un tel polynôme P sous la forme $\alpha X^2 + \beta X + \gamma$ où α, β, $\gamma \in \{0, 1\}$, on doit avoir $\alpha = 1$ (pour que $\deg P = 2$), $\gamma = 1$ (sinon 0 est racine de P), et $\beta = 1$ (sinon $P = X^2 + 1$ et $P(1) = 1 + 1 = 0$), donc le seul candidat possible est

$P = X^2 + X + 1$, qui est bien sans racine car $P(a) = a^2 + a + 1 = a + a + 1 = 2a + 1 = 1 \neq 0$. On a ainsi construit un corps ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}[X]\!/_{X^2+X+1}$ qui a 4 éléments.

On dispose ainsi d'une méthode pour décrire tous les corps finis, sachant que ceux-ci sont de cardinal $n = p^\alpha$ où p est un nombre premier et $\alpha \geq 1$ un entier, et en remarquant que

$$p^\alpha = \#\left(\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}\right)^\alpha\right) = \#\left({}^{\mathbb{Z}}\!/_{p\mathbb{Z}}[X]\!/_{P}\right)$$

où P est un polynôme irréductible de degré α quelconque. En pratique, il est cependant extrèment difficile de trouver des polynômes irréductibles de grand degré sur ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, ce qui rend en fait cette appoche peu fructueuse pour les grandes valeurs de n. On pourra quand même s'amuser à tester les petites puissances de p pour p pas très grand...