STRUCTURES QUOTIENTS

PLAN

I : Ensemble quotient

1- Quelques rappels

Soit E un ensemble muni d'une relation $\equiv$. Cette relation est une **relation d'équivalence** si elle est :

réflexive : $\forall\, x \in E, x \equiv x$
symétrique : $\forall\, (x, y) \in E^2, x \equiv y \Rightarrow y \equiv x$
transitive : $\forall\, (x, y, z) \in E^3, x \equiv y$ et $y \equiv z \Rightarrow x \equiv z$

On appelle **classe d'équivalence** d'un élément x de E la partie $\{y \in E, y \equiv x\}$. On la notera souvent $\overline{x}$ ou $\pi(x)$. Ainsi :

$$x \equiv y \Leftrightarrow \overline{x} = \overline{y}$$

Les classes d'équivalence forment une partition de E (voir L1/ENSEMBLE.PDF pour une démonstration). L'ensemble des classes d'équivalence s'appelle l'**ensemble quotient**, noté $E/\equiv$. L'application $\pi: x \in E \to \overline{x} \in E/\equiv$ s'appelle **projection canonique**.

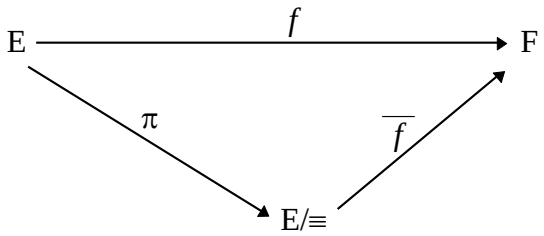
2- Factorisation canonique d'une fonction

Soit F un ensemble et f une application de E dans F. Définissons sur E la relation suivante :

$$x \equiv y \Leftrightarrow f(x) = f(y)$$

Il est facile de vérifier qu'il s'agit d'une relation d'équivalence.

On peut alors définir sur l'ensemble quotient une unique application $\overline{f}$ à valeur dans F telle que $f = \overline{f} \circ \pi$.



Puisqu'on veut que $f = \overline{f} \circ \pi$, il est nécessaire que, pour tout x de E, $f(x) = \overline{f}(\overline{x})$, ce qui prouve l'unicité de $\overline{f}$.

En ce qui concerne l'existence, posons $\overline{f}(\overline{x}) = f(x)$ où x est un représentant quelconque de la classe $\overline{x}$. Il convient de vérifier que l'expression $f(x)$ dépend seulement de $\overline{x}$ mais pas du représentant particulier x choisi. Or, si on prend un autre représentant y, on a $y \equiv x$, donc, par hypothèse $f(x) = f(y)$.

On constate qu'on a seulement utilisé la propriété $x \equiv y \Rightarrow f(x) = f(y)$, permettant de généraliser la propriété énoncée.

DEFINITION

On dit qu'une fonction $f : E \to F$ *est* **compatible** *avec la relation d'équivalence* $\equiv$ *sur* E *si* :

$$\forall (x, y) \in E^2, x \equiv y \Rightarrow f(x) = f(y)$$

On peut donc énoncer :

PROPOSITION

(i) *Si f est compatible avec* $\equiv$, *il existe une unique application* $\overline{f} : E/\equiv \to F$ *telle que* :

$$f = \overline{f} \circ \pi.$$

(ii) *Dans le cas particulier où* $x \equiv y \Leftrightarrow f(x) = f(y)$ (*et pas seulement* $\Rightarrow$), $\overline{f}$ *est injective. Et si, de plus, f est surjective,* $\overline{f}$ *est bijective.*

Démonstration :

❑ (ii) Si on a $\overline{f}(\overline{x}) = \overline{f}(\overline{y})$, alors :

$f(x) = f(y)$ où x est un représentant de $\overline{x}$, et y de $\overline{y}$

$\Rightarrow$ $x \equiv y$

$\Rightarrow$ $\overline{x} = \overline{y}$

et $\overline{f}$ est bien injective.
Si f est surjective, alors :

$$\forall\, y \in F, \exists\, x \in E, y = f(x) = \overline{f}(\overline{x})$$

donc $\overline{f}$ est surjective.

3- Exemples

❑ Soit $\mathbb{K}$ un corps et $E = \mathbb{K}^{n+1} \setminus \{(0, 0, ..., 0)\}$. On définit la relation suivante sur E :

$$X \sim Y \Leftrightarrow \exists\, \lambda \in \mathbb{K}^*, X = \lambda Y$$

Le lecteur verifiera facilement qu'il s'agit d'une relation d'équivalence. L'ensemble quotient $E/\sim$ s'appelle l'**espace projectif** $\mathbb{P}^n(\mathbb{K})$. Cette construction est à la base de la géométrie projective, dans laquelle on peut faire de la géométrie, avec des "points à l'infini". En effet, $\mathbb{K}^n$ s'injecte dans $\mathbb{P}^n(\mathbb{K})$ par exemple par l'application qui, à $(x_1, ..., x_n)$, associe la classe de $(x_1, ..., x_n, 1)$. Si on prend un vecteur non nul $(x_1, ..., x_n)$ et qu'on parcourt la droite $(tx_1, ..., tx_n)$, $t \in \mathbb{K}$, engendrée par ce vecteur, le point général de cette droite s'éloigne vers l'infini. Mais dans $\mathbb{P}^n(\mathbb{K})$, la classe de $(tx_1, ..., tx_n, 1)$ est aussi celle de $(x_1, ..., x_n, \frac{1}{t})$ qui tend vers le point $(x_1, ..., x_n, 0)$ quand t tend vers l'infini. Bien mieux, si on prend la droite affine $(tx_1 + 1, tx_2, ..., tx_n)$ parallèle à la première droite, elle n'a pas d'élément commun avec cette première droite dans $\mathbb{K}^n$, mais dans $\mathbb{P}^n(\mathbb{K})$, la classe de $(tx_1 + 1, tx_2, ..., tx_n, 1)$ est aussi celle de $(x_1 + \frac{1}{t}, x_2, ..., x_n, \frac{1}{t})$ et la deuxième droite rejoint la première au "point à l'infini" $(x_1, ..., x_n, 0)$.
On appelle polynôme P des $n + 1$ variables $X_1, ..., X_{n+1}$ une expression obtenue par combinaison linéaire de produits des X_i. Ce polynôme est homogène si tous les produits comportent le même nombre de facteurs, appelé le degré de P. Ainsi, $P = XYZ^2 + 3X^2Y^2$ est un polynôme élément de $\mathbb{K}[X, Y, Z]$, homogène de degré 4.

Pour tout polynôme homogène P, définissons la fonction $Z_P : E \to \{True, False\}$ de la façon suivante :

$$\forall\, (x_1, ..., x_{n+1}) \in E, Z_P(x_1, ..., x_{n+1}) = \begin{cases} \text{True si } P(x_1, ..., x_{n+1}) = 0 \\ \text{False si } P(x_1, ..., x_{n+1}) \neq 0 \end{cases}$$

Comme P est homogène, soit k son degré. On a alors $P(\lambda x_1, ..., \lambda x_{n+1}) = \lambda^k P(x_1, ..., x_{n+1})$. On en déduit que :

$$\begin{aligned} (x_1, ..., x_{n+1}) \sim (y_1, ..., y_{n+1}) &\Rightarrow \exists\, \lambda \in \mathbb{K}^*, (x_1, ..., x_{n+1}) = (\lambda y_1, ..., \lambda y_{n+1}) \\ &\Rightarrow \exists\, \lambda \in \mathbb{K}^*, P(x_1, ..., x_{n+1}) = P(\lambda y_1, ..., \lambda y_{n+1}) \\ &\Rightarrow \exists\, \lambda \in \mathbb{K}^*, P(x_1, ..., x_{n+1}) = \lambda^k P(y_1, ..., y_{n+1}) \end{aligned}$$

donc $P(x_1, ..., x_{n+1}) = 0 \Leftrightarrow P(y_1, ..., y_{n+1}) = 0$
donc $Z_P(x_1, ..., x_{n+1}) = Z_P(y_1, ..., y_{n+1})$

Ainsi, la fonction Z_P est compatible avec la relation $\sim$ et passe au quotient. La fonction $\overline{Z_p}$ prend la valeur True en un point du quotient $\mathbb{P}^n(\mathbb{K})$ si et seulement si le polynôme P s'annule en ce point. Mais si P ne s'y annule pas, on ne peut attribuer une valeur de P en ce point puisque celle-ci est définie à un facteur près.

Soient maintenant deux polynômes P et Q homogènes de même degré k. On aura alors, pour $(x_1, ..., x_{n+1})$ et $(y_1, ..., y_{n+1})$ équivalents :

$$P(x_1, ..., x_{n+1}) = \lambda^k P(y_1, ..., y_{n+1})$$
$$Q(x_1, ..., x_{n+1}) = \lambda^k Q(y_1, ..., y_{n+1})$$

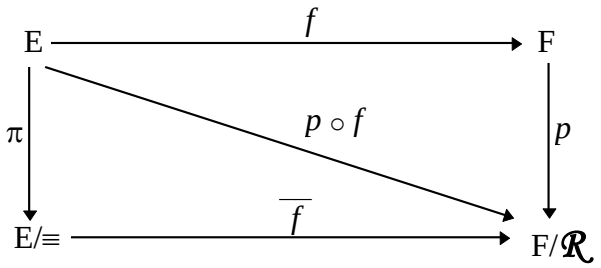
donc $\dfrac{P(x_1, ..., x_{n+1})}{Q(x_1, ..., x_{n+1})} = \dfrac{P(y_1, ..., y_{n+1})}{Q(y_1, ..., y_{n+1})}$ aux points où Q ne s'annule pas. Donc la fonction $\dfrac{P}{Q}$ passe au quotient, et on peut dénir la fonction $\dfrac{P}{Q}$ sur les éléments de $\mathbf{P}^n(\mathbf{K})$ en lesquels Z_Q est False.

❑ Soit E et F muni chacun d'une relation d'équivalence, ≡ pour E et $\mathcal{R}$ pour F. Soit $f : E \to F$ une application telle que :

$$\forall (x, y) \in E^2, x \equiv y \Rightarrow f(x)\ \mathcal{R}\ f(y)$$

Notons $\pi : E \to E/\equiv$ et $p : F \to F/\mathcal{R}$ les projections canoniques. Alors, il existe une unique application $\overline{f} : E/\equiv \to F/\mathcal{R}$ telle que $\overline{f} \circ \pi = p \circ f$.

En effet, l'hypothèse signifie que $p \circ f : E \to F/\mathcal{R}$ est compatible avec la relation ≡, donc passe au quotient :



❑ **Factorisation à droite d'une fonction par une autre**.

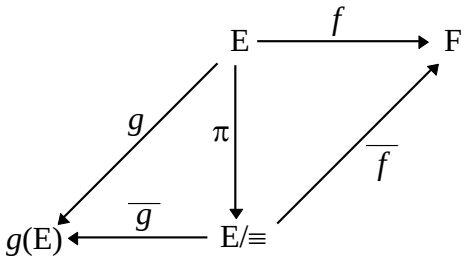
Un cas particulier de l'exemple précédent avec $f : E \to F$ est obtenu en prenant pour $\mathcal{R}$ la relation d'égalité, de sorte que $F/\mathcal{R} = F$ et $p = Id$. Supposons que l'on ait par ailleurs une application $g : E \to G$ telle que :

$$\forall (x, y) \in E^2, g(x) = g(y) \Rightarrow f(x) = f(y)$$

Nous allons montrer qu'il existe une application $h : g(E) \to F$ telle que $f = h \circ g$. Posons :

$$x \equiv y \Leftrightarrow g(x) = g(y)$$

On est alors dans le cadre de l'exemple précédent : f se factorise via l'ensemble quotient E/≡. Mais par ailleurs, on peut aussi procéder à la factorisation canonique de g via le même ensemble E/≡. Quitte à remplacer G par g(E), on obtient le diagramme suivant :



avec $\overline{g}$ bijective, d'après le (ii) de la proposition sur la factorisation canonique. On a alors :

$f = \overline{f} \circ \overline{g}^{-1} \circ g = h \circ g$ avec $h = \overline{f} \circ \overline{g}^{-1}$

Pour rendre les choses plus concrètes, on définit h comme suit. Si $y \in g(\mathrm{E})$, de la forme $y = g(x)$, on pose tout naturellement $h(y) = f(x)$, mais cette démarche n'est pas suffisante si on ne montre pas que la valeur $h(y)$ ne dépend pas du représentant x choisi vérifiant $y = g(x)$. Cette vérification se fait aisément à partir de l'hypothèse sur f et g, mais l'utilisation de la structure quotient E/≡ nous en dispense, donnant directement la factorisation, bien qu'elle nécessite une abstraction plus grande.

A noter qu'il existe aussi un théorème de factorisation à gauche, mais qui se montre beaucoup plus facilement : Soient $f : \mathrm{F} \to \mathrm{E}$ et $g : \mathrm{G} \to \mathrm{E}$ deux applications. Alors il existe une application $h : \mathrm{F} \to \mathrm{G}$ telle que $f = g \circ h$ si et seulement si $f(\mathrm{F}) \subset g(\mathrm{G})$. La condition nécessaire est triviale. Réciproquement, pour tout x de F, on pose $h(x)$ égal à un antécédent par g de $f(x)$. Un tel antécédent existe puisque $f(x) \in f(\mathrm{F}) \subset g(\mathrm{G})$. Cependant, nous serons amenés à revoir plus bas ce théorème dans le cas des applications linéaires, car, telle quelle, la démonstration ne garantit en rien que h puisse être linéaire.

❑ Soit $f : \mathbb{C}^n \to \mathbb{C}[\mathrm{X}]$ qui, à un n-uplet $(z_1, ..., z_n)$ associe le polynôme $\mathrm{P} = (\mathrm{X} - z_1)...(\mathrm{X} - z_n)$. $f(\mathbb{C}^n)$ est égal à l'ensemble des polynômes unitaires de degré n puisqu'un tel polynôme se factorise en facteurs du premier degré, d'après le théorème de d'Alembert. La relation d'équivalence associée à f est :

$$(z_1, ..., z_n) \equiv (z_1', ..., z_n') \Leftrightarrow f(z_1, ..., z_n) = f(z_1', ..., z_n')$$
$$\Leftrightarrow (\mathrm{X} - z_1)...(\mathrm{X} - z_n) = (\mathrm{X} - z_1')...(\mathrm{X} - z_n')$$

En vertu de l'unicité de la factorisation des polynômes, cela ne peut se produire que si $z_1', ..., z_n'$ sont les permutés de $z_1, ..., z_n$. Autrement dit, en notant $\mathfrak{S}_n$ le groupe symétrique :

$$(z_1, ..., z_n) \equiv (z_1', ..., z_n') \Leftrightarrow \exists\, \sigma \in \mathfrak{S}_n,\ \forall\, i,\ z_i' = z_{\sigma(i)}$$

Notons $\mathbb{C}^n/\mathfrak{S}_n$ l'ensemble quotient. Cet ensemble est en bijection avec les polynômes unitaires de degré n. On montre dans L3/TOPOLOG.PDF qu'il existe un homéomorphisme entre ces deux ensembles, autrement dit, à permutation près des racines, les coefficients d'un polynôme sont des fonctions continues des racines et les racines sont des fonctions continues des coefficients.

Dans la suite du chapitre, on se propose d'étudier quelle structure on peut affecter à l'ensemble quotient lorsque l'ensemble E lui-même est doté d'une structure.

II : Groupe quotient

1- Sous-groupe distingué et structure de groupe sur l'ensemble quotient

Soit G un groupe dont la loi est notée multiplicativement, et soit ≡ une relation d'équivalence sur ce groupe. Soit G/≡ l'ensemble quotient. Soit $\pi : \mathrm{G} \to \mathrm{G}/\equiv$ la projection canonique. On se pose la question de savoir s'il est possible de munir l'ensemble quotient d'une structure de groupe pour laquelle π est un morphisme de groupe.

Si tel est le cas, notons $*$ la loi sur cet hypothétique groupe. Pour tout x, y et z de G, on a :

$$x \equiv y \Rightarrow \pi(x) = \pi(y) \Rightarrow \pi(x) * \pi(z) = \pi(y) * \pi(z) \Rightarrow \pi(xz) = \pi(yz) \Rightarrow xz \equiv yz$$

Ainsi :

$$x \equiv y \Rightarrow xz \equiv yz$$

On montre de même qu'on a $zx \equiv zy$. Ainsi, on peut multiplier la relation $x \equiv y$ à droite ou à gauche par n'importe quel élément z.

DEFINITION
On dit que la relation d'équivalence $\equiv$ *est* **compatible** *avec la loi du groupe* G *si* :

$$\forall\, x, y, z \in G,\ x \equiv y \Rightarrow xz \equiv yz \text{ et } zx \equiv zy$$

On vient donc de montrer que, pour que π soit un morphisme de groupe, il faut que $\equiv$ soit compatible avec la loi de G. Nous allons montrer que cette condition est suffisante.

PROPOSITION
Soit G *un groupe muni d'une relation d'équivalence* $\equiv$. *Les deux propriétés suivantes sont équivalentes :*

(i) $\equiv$ *est compatible avec la loi du groupe* G.

(ii) *On peut munir l'ensemble quotient* G/$\equiv$ *d'une structure de groupe pour laquelle la projection canonique est un morphisme.*

Démonstration :

❑ (ii) $\Rightarrow$ (i) a été montré en préambule de ce paragraphe pour introduire la notion de relation compatible.

❑ (i) $\Rightarrow$ (ii) : Définissons une loi $*$ interne à G/$\equiv$ en posant :

$$\pi(x) * \pi(y) = \pi(xy)$$

Il convient de montrer que le résultat de ce calcul ne dépend pas des représentants choisis dans chaque classe. Supposons donc que $\pi(x) = \pi(x')$ et que $\pi(y) = \pi(y')$. On a alors :

$x \equiv x'$ et $y \equiv y'$

donc $xy \equiv x'y \equiv x'y'$ en mulitpliant la première relation à droite par y, et la seconde à gauche par x'

donc $\pi(xy) = \pi(x'y')$.

Le neutre est $\pi(e)$, car, pour tout x :

$$\pi(x) * \pi(e) = \pi(xe) = \pi(x) = \pi(ex) = \pi(e) * \pi(x)$$

Le symétrique de $\pi(x)$ est $\pi(x^{-1})$ car :

$$\pi(x) * \pi(x^{-1}) = \pi(xx^{-1}) = \pi(e) = \pi(x^{-1}x) = \pi(x^{-1}) * \pi(x).$$

Ainsi, les relations d'équivalence compatibles avec la loi du groupe jouent un rôle essentiel dans le passage au quotient. Etudions la structure de telles relations.

Soit H un sous-groupe de G. Pour x élément de G, notons :

$xH = \{xy, y \in H\}$

$Hx = \{yx, y \in H\}$

$xHx^{-1} = \{xyx^{-1}, y \in H\}$

PROPOSITION
Soit $\equiv$ *une relation d'équivalence compatible avec la loi du groupe* G, *et soit* H = $\pi(e)$ *la classe d'équivalence du neutre e du groupe* G. *Alors* :

(i) H *est un sous-groupe de* G

(ii) *Pour tout x, y* de G, *x*H *est la classe d'équivalence de x* : $x\mathrm{H} = y\mathrm{H} \Leftrightarrow x \equiv y$

(iii) *Pour tout x de* G, $x\mathrm{H}x^{-1} = \mathrm{H}$, *ou encore* $x\mathrm{H} = \mathrm{H}x$. *On dit qu'un sous-groupe* H *de* G *vérifiant cette propriété est* **distingué** *ou* **normal**.

(iv) *La loi* $*$ *définie sur l'ensemble quotient est* : $x\mathrm{H} * y\mathrm{H} = xy\mathrm{H}$..*On notera désormais* G/H *le groupe quotient.*

Démonstration :

❑ (i) La relation étant compatible, la projection canonique est un morphisme de groupe, donc son noyau est un sous-groupe de G. (On rappelle que, si on a un morphisme $f : \mathrm{G} \to \mathrm{F}$, le **noyau** de f est $\mathrm{Ker}(f) = \{x \in \mathrm{G}, f(x) = \varepsilon\}$, où ε est le neutre de f). Or :

$x \in \mathrm{Ker}(\pi) \Leftrightarrow \pi(x) = \pi(e)$ puisque $\pi(e)$ est le neutre du groupe quotient

$\Leftrightarrow x \equiv e$

$\Leftrightarrow x \in \mathrm{H}$

Donc H est un sous-groupe de G.

On peut aussi le montrer directement comme suit : si x et y sont éléments de H, alors $x \equiv e$ et $e \equiv y$, donc en multipliant les deux relations à droite par y^{-1}, on obtient :

$xy^{-1} \equiv ey^{-1} \equiv yy^{-1} = e$

donc $xy^{-1} \in \mathrm{H}$

H est donc bien un sous-groupe de G.

❑ (ii) Montrons que xH est la classe d'équivalence de x, autrement dit : $y \in x\mathrm{H} \Leftrightarrow y \equiv x$.

Si $y \in x\mathrm{H}$, il existe z élément de H tel que $y = xz$. Mais z élément de H signifie que $z \equiv e$, donc $xz \equiv xe = x$ en multipliant à gauche par x, donc $y \equiv x$. Réciproquement si $y \equiv x$, alors $x^{-1}y \equiv e$ en multipliant à gauche par x^{-1}. Donc $x^{-1}y$ est élément de H et $y = x(x^{-1}y)$ est élément de xH. Ainsi, la classe de x est xH. Autrement dit, $\pi(x) = x\mathrm{H}$.

Par conséquent, $x \equiv y \Leftrightarrow x$ et y ont la même classe d'équivalence $\Leftrightarrow x\mathrm{H} = y\mathrm{H}$.

❑ (iii) Soit y élément de $x\mathrm{H}x^{-1}$. Il existe z élément de H tel que $y = xzx^{-1}$. Mais z élément de H signifie que $z \equiv e$, donc $xzx^{-1} \equiv xex^{-1} = e$ en multipliant à gauche par x et à droite par x^{-1}. Donc $y \equiv e$ et $y \in$H. Réciproquement, si $y \in$ H, alors $y \equiv e$, donc $x^{-1}yx \equiv x^{-1}ex = e$ donc $x^{-1}yx \in$ H. Comme $y = x(x^{-1}yx)x^{-1}$, on a bien $y \in x\mathrm{H}x^{-1}$.

En utilisant la bijection $y \in \mathrm{G} \to yx \in \mathrm{G}$, on déduit également de $x\mathrm{H}x^{-1} = \mathrm{H}$ la relation $x\mathrm{H} = \mathrm{H}x$.

❑ (iv) On a $\pi(x) = x$H est la loi donnée dans la proposition est bien celle que nous avons définie plus haut.

Ainsi, une relation d'équivalence compatible avec la loi du groupe introduit naturellement un sous-groupe distingué H de G, à savoir la classe du neutre. Réciproquement, si on se donne un sous-groupe distingué H de G, on peut définir une relation d'équivalence compatible avec la loi du groupe G, et donc définir le groupe quotient G/H.

PROPOSITION

Soit H *un sous-groupe distingué de* G. *Posons* $x \equiv y$ *si et seulement si* $x\mathrm{H} = y\mathrm{H}$. *Il s'agit d'une relation d'équivalence compatible avec la loi du groupe, et* H *est la classe de e.*

Démonstration :

❑ Le fait qu'il s'agisse d'une relation d'équivalence est facile. Montrons la compatibilité avec la loi du groupe. Supposons que $x \equiv y$, et donc $x\mathrm{H} = y\mathrm{H}$. On a donc, pour tout z :

$x\mathrm{H}z = y\mathrm{H}z$

donc $xz\mathrm{H} = yz\mathrm{H}$ car $\mathrm{H}z = z\mathrm{H}$

donc $xz \equiv yz$

On montrerait de même que $zx \equiv zy$.

Enfin la classe de e est l'ensemble des x tels que $x \equiv e$, soit $x\mathrm{H} = \mathrm{H}$. Ce sont les éléments de H eux-mêmes puisque tout x vérifiant cette relation est de la forme xe, avec $e \in \mathrm{H}$, donc $x \in x\mathrm{H} = \mathrm{H}$, donc $x \in \mathrm{H}$. Inversement, tout x de H vérifie $x\mathrm{H} \subset \mathrm{H}$, mais aussi $x^{-1} \in \mathrm{H}$ car H est un sous-groupe, donc $x^{-1}\mathrm{H} \subset \mathrm{H}$, donc $\mathrm{H} \subset x\mathrm{H}$. Donc $x\mathrm{H} = \mathrm{H}$.

Les sous-groupes normaux sont caractérisés par la propriété suivante, d'un usage fréquent :

PROPOSITION

Soit G *un groupe et soit* H *un sous-groupe de* G. *Il y a équivalence entre* :

(i) H *est distingué.*

(ii) H *est le noyau d'un morphisme de* G *dans un autre groupe*.

Démonstration :

❑ (i) $\Rightarrow$ (ii) : Si H est distingué, on dispose de la projection canonique $\pi : \mathrm{G} \to \mathrm{G/H}$ qui est un morphisme et dont on a déjà montré que le noyau est H.

❑ (ii) $\Rightarrow$ (i) : Si $\mathrm{H} = \mathrm{Ker}(f)$ avec $f : \mathrm{G} \to \mathrm{F}$, montrons que, pour tout x de G, $x\mathrm{H}x^{-1} = \mathrm{H}$. Soit y élément de H. Alors :

$f(xyx^{-1}) = f(x)f(y)f(x^{-1}) = f(x)\varepsilon f(x^{-1})$ où ε est le neutre de F

donc $f(xyx^{-1}) = f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = \varepsilon$

donc $xyx^{-1} \in \mathrm{Ker}(f) = \mathrm{H}$

On a montré que $x\mathrm{H}x^{-1} \subset \mathrm{H}$.

On a de même $x^{-1}\mathrm{H}x \subset \mathrm{H}$ donc $\mathrm{H}x \subset x\mathrm{H}$ donc $\mathrm{H} \subset x\mathrm{H}x^{-1}$.

Donc $x\mathrm{H}x^{-1} = \mathrm{H}$.

EXEMPLES :

❑ Dans un groupe commutatif, tous les sous-groupes sont normaux. Les groupes quotients y abondent. Ainsi, pour $\mathrm{G} = \mathbb{Z}$, $\mathrm{H} = n\mathbb{Z}$ est un sous-groupe distingué pour tout entier n et le groupe quotient est le bien connu $\mathbb{Z}/n\mathbb{Z}$. La relation d'équivalence déduite de H est compatible avec la loi notée ici additivement :

$x \equiv y$

$\Leftrightarrow$ $x + \mathrm{H} = y + \mathrm{H}$

$\Leftrightarrow$ $x \in y + \mathrm{H}$

$\Leftrightarrow$ $\exists\, k,\ x = y + kn$

et on constate que la relation définie par H est la congruence modulo n.

❑ Le groupe orthogonal $\mathrm{SO}_n(\mathbb{R})$ est un sous-groupe distingué de $\mathrm{O}_n(\mathbb{R})$. C'est en effet le noyau du morphisme det : $\mathrm{O}_n(\mathbb{R}) \to \{-1, 1\}$. Le groupe quotient $\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R})$ ne comporte que deux éléments, à savoir la classe d'équivalence des isométries directes et celle des isométries indirectes). Il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

❑ Dans le groupe linéaire $GL_n(\mathbb{K})$, $H = \{\lambda I_n, \lambda \in \mathbb{K}\}$ est un sous-groupe distingué. Les éléments du quotient sont définis à un scalaire non nul près. Ce quotient est isomorphe à $SL_n(\mathbb{K})$, groupe spécial linéaire des matrices de déterminant 1.

❑ $O_n(\mathbb{R})$ est un sous-groupe de $GL_n(\mathbb{R})$ mais n'en est pas un sous-groupe distingué si $n \geq 2$. En effet, il faudrait que, pour tout A dans $GL_n(\mathbb{R})$ et tout B dans $O_n(\mathbb{R})$, on ait $ABA^{-1} \in O_n(\mathbb{R})$. Il faudrait pour cela que, pour tout A dans $GL_n(\mathbb{R})$ et tout B dans $O_n(\mathbb{R})$:

$${}^t(ABA^{-1})ABA^{-1} = I_n$$
$$\Leftrightarrow \quad {}^tA^{-1}{}^tB{}^tAABA^{-1} = I_n$$
$$\Leftrightarrow \quad {}^tB{}^tAAB = {}^tAA$$
$$\Leftrightarrow \quad B^{-1}{}^tAAB = {}^tAA$$
$$\Leftrightarrow \quad {}^tAAB = B{}^tAA$$

égalité dont on peut montrer qu'elle n'est vraie pour tout A de $GL_n(\mathbb{R})$ que pour B de la forme λI_n. (Voir exercices)

❑ Soit G un groupe et H un sous-groupe de G. Soit $N(H) = \{g \in G \mid gHg^{-1} = H\}$. N(H) s'appelle le **normalisateur** de H dans G. Il n'est pas difficile de vérifier que N(H) est un sous-groupe de G contenant H. Comme, pour tout g de N(H), on a $gHg^{-1} = H$, il en résulte que H est distingué dans N(H). De plus, si K est un groupe contenant H tel que H soit distingué dans K, alors pour tout g de K, on a $gHg^{-1} = H$, donc $g \in N(H)$. Donc $K \subset N(H)$. Ainsi, N(H) est le plus grand sous-groupe de G dans lequel H est distingué.
Par exemple, soit $G = GL_n(\mathbb{R})$, et $H = O_n(\mathbb{R})$. Pour toute matrice A, on a :

$$A \in N(H)$$
$$\Leftrightarrow \quad \forall B \in O_n(\mathbb{R}),\ ABA^{-1} \in O_n(\mathbb{R})$$
$$\Leftrightarrow \quad \forall B \in O_n(\mathbb{R}),\ {}^tAAB = B{}^tAA \text{ d'après le calcul effectué dans le paragraphe précédent}$$

On montre, dans les exercices, que A est le multiple d'une matrice orthogonale (ou matrice de similitude). Ainsi, le normalisateur de $O_n(\mathbb{R})$ dans $GL_n(\mathbb{R})$ est le groupe des similitudes.

2- Factorisation canonique d'un morphisme de groupe

Soit G un groupe, H un sous-groupe distingué de G, F un autre groupe, $f : G \to F$ un morphisme de groupe, compatible avec la relation d'équivalence induite par H. Que signifie cette compatibilité ?

PROPOSITION
Soit G *un groupe,* H *un sous-groupe distingué de* G, F *un autre groupe,* $f : G \to F$ *un morphisme de groupe. Il y a équivalence entre* :
(i) *f est compatible avec la relation d'équivalence sur* G *induite par* H.
(ii) $H \subset \mathrm{Ker}(f)$

Démonstration :
❑ (i) $\Rightarrow$ (ii) : Si f est compatible avec la relation d'équivalence induite par H, alors :
$\forall (x, y) \in G^2,\ xH = yH \Rightarrow f(x) = f(y)$
C'est vrai en particulier pour $y = e$, neutre de G. Donc :
$\forall x \in G,\ xH = H \Rightarrow f(x) = f(e) = \varepsilon$ où ε est le neutre de F
Mais $xH = H$ est équivalent à $x \equiv e$ et donc à $x \in H$. Ainsi, f doit vérifier :
$\forall x \in G,\ x \in H \Rightarrow f(x) = \varepsilon$

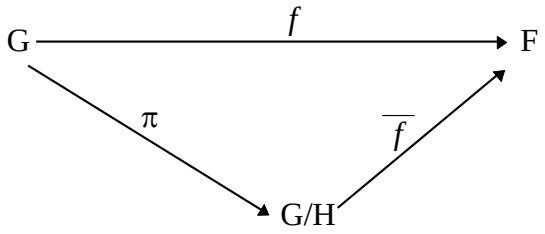
Cela signifie que H est inclus dans le noyau Ker(*f*) de *f*.

❑ (ii) $\Rightarrow$ (i) : Si H $\subset$ Ker(*f*), soient *x* et *y* tels que *x*H = *y*H. Puisque *x* = *xe* est élément de *x*H, il est élément de *y*H, donc il existe *z* élément de H tel que *x* = *yz* et donc *f*(*x*) = *f*(*yz*) = *f*(*y*)*f*(*z*) = *f*(*y*)ε = *f*(*y*), et *f* est bien compatible.

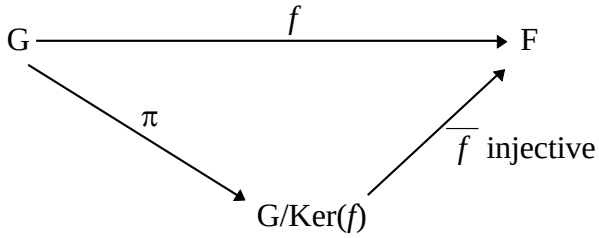
Dans le cas d'une application compatible avec une relation d'équivalence, on peut procéder à sa factorisation canonique $f = \overline{f} \circ \pi$. Dans le cas d'un groupe, $\overline{f}$ est un morphisme de groupe.

PROPOSITION
Soit G *un groupe,* H *un sous-groupe distingué de* G, F *un autre groupe,* $f : G \to F$ *un morphisme de groupe tel que* H $\subset$ Ker(*f*). *Alors* :

(i) *il existe un unique morphisme* $\overline{f} : G/H \to F$ *tel que* $f = \overline{f} \circ \pi$.



(ii) *De plus, si* H = Ker(*f*), $\overline{f}$ *est injective. Et si, de plus* F = Im(*f*), $\overline{f}$ *est un isomorphisme.*



Démonstration :

❑ (i) Nous avons vu que, sur le plan ensembliste, $\overline{f}$ est défini par $\overline{f}(\overline{x}) = f(x)$ où *x* est un représentant quelconque de $\overline{x}$, et que cette expression ne dépendait pas du représentant choisi. On peut le prouver de nouveau comme suit. Soit $x \equiv y$, alors :

	$xy^{-1} \equiv e$	car la relation $\equiv$ est compatible avec la loi de groupe
donc	$xy^{-1} \in$ H	car H est la classe de *e*
donc	$f(xy^{-1}) = \varepsilon$	car H $\subset$ Ker(*f*)
donc	$f(x)f(y)^{-1} = \varepsilon$	car *f* est un morphisme
donc	$f(x) = f(y)$	

Il reste à montrer que $\overline{f}$ est un morphisme. On rappelle que la loi du groupe quotient est définie par (en la notant multiplicativement) :

$\forall\ (\overline{x}, \overline{y}) \in (G/H)^2,\ \overline{x}\,\overline{y} = x\mathrm{H}\ y\mathrm{H} = xy\mathrm{H} = \overline{xy}$

où x est un représentant quelconque de $\overline{x}$ et y de $\overline{y}$ (ce qui traduit le fait que π est un morphisme de groupes). Donc :

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

et $\overline{f}$ est un morphisme.

❑ (ii) Si H = Ker(f), alors on a l'équivalence $x \equiv y \Leftrightarrow f(x) = f(y)$. L'implication $\Rightarrow$ ayant déjà été prouvée dans la proposition précédente, montrons la réciproque.

$f(x) = f(y)$
$\Rightarrow$ $f(xy^{-1}) = \varepsilon$
$\Rightarrow$ $xy^{-1} \in \mathrm{Ker}(f)$
$\Rightarrow$ $xy^{-1} \in \mathrm{H}$
$\Rightarrow$ $xy^{-1} \equiv e$ car H est la classe de e
$\Rightarrow$ $x \equiv y$ car $\equiv$ est compatible avec la loi du groupe.

L'injectivité de $\overline{f}$ en résulte dans ce cas puisqu'elle a déjà été prouvée dans le cas ensembliste (de même que la surjectivité si F = Im(f)).

On peut aussi en donner une démonstration directe. Puisqu'on a montré que $\overline{f}$ est un morphisme de groupe, il suffit de montrer que $\mathrm{Ker}(\overline{f}) = \{\overline{e}\}$. Or :

$\overline{x} \in \mathrm{Ker}(\overline{f})$
$\Rightarrow$ $\overline{f}(\overline{x}) = \varepsilon$
$\Rightarrow$ $f(x) = \varepsilon$ où x est un représentant quelconque de $\overline{x}$
$\Rightarrow$ $x \in \mathrm{Ker}(f)$
$\Rightarrow$ $x \in \mathrm{H}$
$\Rightarrow$ $x \equiv e$ car H est la classe de e
$\Rightarrow$ $\overline{x} = \overline{e}$ neutre de G/H

3- Exemples

❑ Le groupe orthogonal $\mathrm{SO}_n(\mathbb{R})$ est un sous-groupe distingué de $\mathrm{O}_n(\mathbb{R})$. L'application det : $\mathrm{O}_n(\mathbb{R}) \to \{-1, 1\}$ est un morphisme surjectif. Son noyau est précisément $\mathrm{SO}_n(\mathbb{R})$. Donc la factorisation canonique définit un morphisme $\overline{\det}$: $\mathrm{O}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R}) \to \{-1, 1\}$ qui est surjectif, car det l'est, et injectif parce que le noyau de det est exactement $\mathrm{SO}_n(\mathbb{R})$. Il s'agit donc d'un isomorphisme.

❑ Dans $\mathrm{GL}_n(\mathbb{K})$, l'application det : $\mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$ est aussi un morphisme de groupe. Son noyau est $\mathrm{SL}_n(\mathbb{R})$. Le même raisonnement que ci-dessus prouve que $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ est isomorphe à $\mathbb{K}^*$.

❑ Dans le groupe symétrique $\mathfrak{S}_n$, la signature est un morphisme de groupe de $\mathfrak{S}_n$ dans $\{-1, 1\}$. Son noyau est $\mathfrak{A}_n$, le groupe alterné des permutations paires. Etant un noyau, il s'agit d'un sous-groupe distingué. Comme ci-dessus, on montre que $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\{-1, 1\}$ en factorisant la signature, et donc à $\mathbb{Z}/2\mathbb{Z}$.

III : Espace vectoriel quotient

1- Structure d'espace vectoriel quotient

Soit E un espace vectoriel sur un corps $\mathbb{K}$, et soit $\equiv$ une relation d'équivalence sur cet espace vectoriel. Soit E/$\equiv$ l'ensemble quotient. Soit π : E $\rightarrow$ E/$\equiv$ la projection canonique. On se pose la question de savoir s'il est possible de munir l'ensemble quotient d'une structure d'espace vectoriel pour laquelle π est une application linéaire.

Un espace vectoriel étant un groupe pour l'addition, il est nécessaire, d'après le cas des groupes quotient que la classe H du vecteur nul (élément neutre de l'addition) soit un sous-groupe. L'addition étant commutative, H est automatiquement un sous-groupe distingué de E. Regardons ce qu'il en est vis-à-vis du produit par un scalaire, en supposant que π est une application linéaire entre espaces vectoriels. On doit avoir, pour tout λ de $\mathbb{K}$ et tout x de E :

$$x \equiv y \Rightarrow \pi(x) = \pi(y) \Rightarrow \lambda\pi(x) = \lambda\pi(y) \Rightarrow \pi(\lambda x) = \pi(\lambda y) \Rightarrow \lambda x \equiv \lambda x$$

Ainsi, il faut que, pour tout x et y de E et tout λ de $\mathbb{K}$:

$$x \equiv y \Rightarrow \lambda x \equiv \lambda y$$

Cela signifie que la relation d'équivalence doit être non seulement compatible avec l'addition (pour avoir un groupe quotient), mais aussi avec le produit par un scalaire.

PROPOSITION

Soit E *un espace vectoriel muni d'une relation d'équivalence* $\equiv$*. Les deux propriétés suivantes sont équivalentes :*

(i) $\equiv$ *est compatible avec les lois de* E

(ii) *On peut munir l'ensemble quotient* E/$\equiv$ *d'une structure d'espace vectoriel pour laquelle la projection canonique est une application linéaire.*

Démonstration :

❑ (ii) $\Rightarrow$ (i) résulte du préambule de ce paragraphe.

❑ (i) $\Rightarrow$ (ii) : Etant compatible avec la loi de groupe +, on sait déjà que E/$\equiv$ est un groupe muni de l'addition suivante, qui fait de π un morphisme de groupe :

$$\pi(x) + \pi(y) = \pi(x + y)$$

Vérifions qu'on peut poser $\lambda\pi(x) = \pi(\lambda x)$ pour tout x de E et tout λ de $\mathbb{K}$, i.e. que le résultat ne dépend pas du représentant choisi dans la classe de x. On a :

$x \equiv y \Rightarrow \lambda x \equiv \lambda y$ car $\equiv$ est compatible avec le produit par un scalaire

$\Rightarrow \pi(\lambda x) = \pi(\lambda y)$

On laisse au lecteur le soin de vérifier que l'addition et le produit par un scalaire satisfont tous les axiomes nécessaires aux espaces vectoriels. Le vecteur nul est $\pi(0)$, image du vecteur nul de E par l'application linéaire π. L'opposé de $\pi(x)$ est $-\pi(x) = \pi(-x)$.

Les lois définies sur le quotient sont exactement celles qui font de π une application linéaire.

Comment caractériser les relations $\equiv$ compatibles avec les lois d'un espace vectoriel. Etant compatible avec la loi de groupe +, on sait déjà que H, la classe de 0, est un groupe. (Il est inutile de préciser qu'il est distingué car + est commutatif). On a mieux :

PROPOSITION

Soit $\equiv$ *une relation d'équivalence sur un espace vectoriel* E*, compatible avec l'addition et le produit par un scalaire, et soit* H *la classe d'équivalence du vecteur nul. Alors* :

(i) H *est un sous-espace vectoriel de* E

(ii) *Pour tout* x*,* y de E, x + H *est la classe d'équivalence de* x*,* et $x \equiv y \Leftrightarrow x - y \in H$

(iii) *L'ensemble quotient est un espace vectoriel avec les deux lois suivantes :*

$(x + H) + (y + H) = (x + y) + H$

$\lambda(x + H) = (\lambda x) + H$

et la projection canonique est une application linéaire. On note E/H *l'espace vectoriel quotient.*

Démonstration :

❑ (i) H est le noyau de la projection canonique. Celle-ci étant linéaire, ce noyau est un sous-espace vectoriel de E. Donc H est un sous-espace vectoriel de E.

On peut aussi le montrer directement comme suit : si x et y sont éléments de H et λ élément de $\mathbf{K}$, alors $x \equiv 0$ et $y \equiv 0$, et la relation d'équivalence étant compatible avec les deux opérations, on a d'abord $\lambda y \equiv \lambda 0 = 0$ puis $x + \lambda y \equiv 0 + 0 = 0$. Donc $x + \lambda y \in H$.

❑ (ii) Le fait que x + H soit la classe d'équivalence de x a déjà été montré dans le cas du groupe quotient. La loi est ici notée additivement.

On a ensuite, en utilisant la compatibilité de la relation d'équivalence avec l'addition :

$$x \equiv y \Leftrightarrow x - y \equiv 0 \Leftrightarrow x - y \in H$$

❑ (iii) On a montré ci-dessus que $\pi(x) = x + H$. Les relations énoncées sont celles qui ont permis de définir une somme et un produit par un scalaire dans l'ensemble quotient, et de rendre π linéaire.

Nous sommes partis d'une relation d'équivalence compatible avec les lois de l'espace vectoriel pour introduire le sous-espace vectoriel H, classe d'équivalence de 0. On peut procéder en sens inverse, partir d'un sous-espace vectoriel H et en déduire une relation d'équivalence compatible avec les lois de l'espace vectoriel E. Il suffit de prendre la propriété (ii) ci-dessus.

PROPOSITION

Soit H *un sous-espace vectoriel de* E*. Posons* $x \equiv y$ *si et seulement si* $x - y \in H$*. Il s'agit d'une relation d'équivalence compatible avec les lois de l'espace vectoriel, et* H *est la classe de* 0.

Démonstration :

❑ Le fait qu'il s'agisse d'une relation d'équivalence est facile. Montrons la compatibilité avec le produit par un scalaire. Supposons que :

$x \equiv y$

donc $x - y \in H$

donc $\lambda(x - y) \in H$ car H est un sous-espace vectoriel

donc $\lambda x - \lambda y \in H$

donc $\lambda x \equiv \lambda y$

La compatibilité avec la somme est comparable, ou a déjà été prouvée dans le cas des groupes quotients.

On a également $x \equiv 0 \Leftrightarrow x - 0 \in H \Leftrightarrow x \in H$, donc H est la classe de 0.

EXEMPLE :

❑ Comme nous le verrons dans le paragraphe suivant, E/H peut se substituer à un supplémentaire de H dans E quand on n'a pas besoin d'un supplémentaire particulier.

2- Factorisation canonique d'une application linéaire

Soit E un espace vectoriel, H un sous-groupe espace vectoriel de E, F un autre espace vectoriel, $f : E \to F$ une application linéaire, compatible avec la relation d'équivalence induite par H. Que signifie cette compatibilité ?

PROPOSITION

Soit E *un espace vectoriel,* H *un sous-espace vectoriel de* E, F *un autre espace vectoriel,* $f : E \to F$ *une application linéaire. Il y a équivalence entre* :

(i) *f est compatible avec la relation d'équivalence sur* E *induite par* H.

(ii) $H \subset \text{Ker}(f)$

Démonstration :

L'équivalence a déjà été montrée dans le cas des groupes quotients. Nous redonnons une démonstration, adaptée aux notations des espaces vectoriels, un peu plus familières que celles des groupes.

❑ (i) $\Rightarrow$ (ii) : Si f est compatible avec la relation d'équivalence induite par H, alors :

$\forall (x, y) \in E^2, x - y \in H \Rightarrow x \equiv y \Rightarrow f(x) = f(y)$

C'est vrai en particulier pour $y = 0$. Donc :

$\forall x \in E, x \in H \Rightarrow f(x) = f(0) = 0$

Donc $H \subset \text{Ker}(f)$.

❑ (ii) $\Rightarrow$ (i) : Si $H \subset \text{Ker}(f)$, soient x et y tels que $x \equiv y$ et donc $x - y \in H$. On a alors :

$x - y \in \text{Ker}(f)$

donc $f(x - y) = 0$

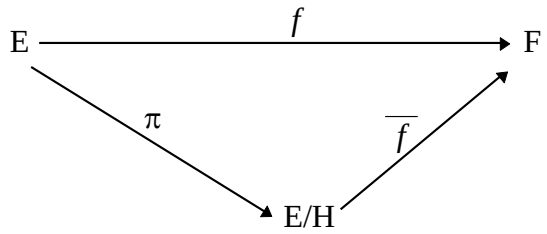
donc $f(x) = f(y)$

Dans le cas d'une application compatible avec une relation d'équivalence, on peut procéder à sa factorisation canonique $f = \overline{f} \circ \pi$. Dans le cas d'un espace vectoriel, $\overline{f}$ est une application linéaire.

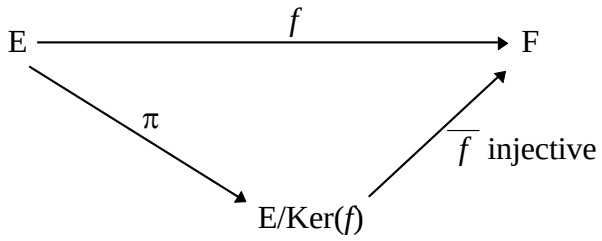
PROPOSITION

Soit E *un espace vectoriel,* H *un sous-espace vectoriel de* E, F *un autre espace vectoriel,* $f : E \to F$ *une application linéaire telle que* $H \subset \text{Ker}(f)$. *Alors* :

(i) *il existe une unique application linéaire* $\overline{f} : E/H \to F$ *telle que* $f = \overline{f} \circ \pi$.



(ii) *De plus, si* $H = \text{Ker}(f)$, $\overline{f}$ *est injective. Si, de plus,* $F = \text{Im}(f)$, $\overline{f}$ *est un isomorphisme.*



Démonstration :
Elle a déjà été vue dans le cas ensembliste et celui des groupes quotients. Il suffit juste de vérifier la linéarité.

❑ (i) : $\overline{f}$ est défini par $\overline{f}(\overline{x}) = f(x)$ où x est un représentant quelconque de $\overline{x}$, et que cette expression ne dépendait pas du représentant choisi. Montrons que $\overline{f}$ est une application linéaire. On rappelle que la loi du quotient est définie par (en la notant multiplicativement) :

$$\forall (\overline{x}, \overline{y}) \in (E/H)^2, \overline{x} + \overline{y} = xH + yH = (x + y) + H = \overline{x + y}$$

$$\lambda\overline{x} = \lambda(x + H) = (\lambda x) + H = \overline{\lambda x}$$

où x est un représentant quelconque de $\overline{x}$ et y de $\overline{y}$ (ce qui traduit le fait que π est une application linéaire). Donc :

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

$$\overline{f}(\lambda\overline{x}) = \overline{f}(\overline{\lambda x}) = f(\lambda x) = \lambda f(x) = \lambda\,\overline{f}(\overline{x})$$

et $\overline{f}$ est bien linéaire.

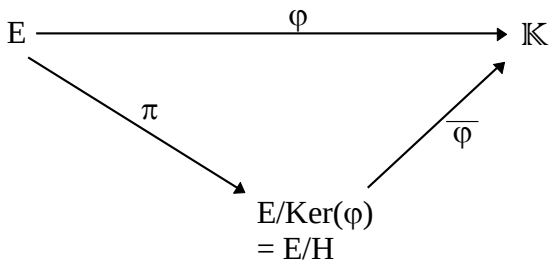
❑ (ii) : La démonstration a déjà été donnée dans le cas des groupes quotients. On redonne rapidement une démonstration de l'injectivité avec les notations des espaces vectoriels. $\overline{f}$ étant linéaire, il suffit de déterminer son noyau :

$\overline{f}(\overline{x}) = 0$
$\Rightarrow$ $f(x) = 0$ avec un représentant x de $\overline{x}$
$\Rightarrow$ $x \in \mathrm{Ker}(f) = H$
$\Rightarrow$ $x \equiv 0$
$\Rightarrow$ $\overline{x} = \overline{0}$

3- Exemples

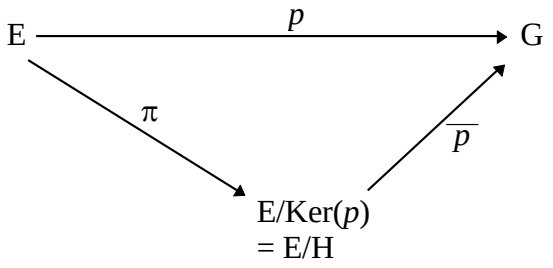
❑ Si on prend F = Im(f), f devient surjective, $\overline{f}$ aussi, et on obtient un isomorphisme naturel entre E/Ker(f) et Im(f).

❑ Soit E un espace vectoriel et H un sous-espace vectoriel. Il y a équivalence entre :
(i) H est le noyau d'une forme linéaire non nulle
(ii) E/H est une droite
Supposons (i) et soit φ la forme linéaire non nulle dont H est le noyau. Procédons à la factorisation canonique de φ, $\varphi = \overline{\varphi} \circ \pi$:



φ étant non nulle est surjective sur $\mathbb{K}$. Donc $\overline{\varphi}$ est surjective. D'autre part, quand on quotiente par le noyau, le facteur $\overline{\varphi}$ est injectif. Donc $\overline{\varphi}$ est bijectif. $\overline{\varphi}$ est un isomorphisme linéaire, et E/H est une droite vectorielle, isomorphe à $\mathbb{K}$.
Réciproquement, Si E/H est une droite, elle est isomorphe à $\mathbb{K}$ par un isomorphisme que nous noterons également $\overline{\varphi}$. L'application $\overline{\varphi} \circ \pi$ est une forme linéaire, et son noyau est celui de π, et ce n'est que H lui-même.
On a substitué la propriété "(ii) E/H est isomorphe à une droite" à la propriété usuelle des hyperplans "H admet une droite comme supplémentaire".

❑ Plus généralement, soit E un espace vectoriel et H un sous-espace vectoriel de E. E/H est isomorphe à tout supplémentaire G de H. En effet, soit *p* le projecteur sur G parallèlement à H. *p* est une application surjective de E sur G, admet pour noyau H, et la factorisation canonique de *p* donne, comme ci-dessus, l'isomorphisme cherché :



❑ Soit *f* un endomorphisme de E et F un sous-espace vectoriel stable par F. Alors *f* induit un endomorphisme de E/F. En effet, considérons la composée de fonctions :

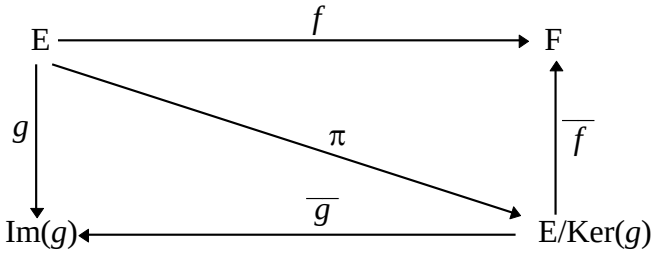
$$E \xrightarrow{f} E \xrightarrow{\pi} E/F$$

Puisque $f(F) \subset F$, on a $(\pi \circ f)(F) = \{0\}$ donc $F \subset \mathrm{Ker}(\pi \circ f)$, donc l'application $\pi \circ f$ passe au quotient : $E/F \to E/F$.

Plus concrètement, un élément $\overline{x}$ de E/F est représenté par n'importe quel $x + y$, $y \in F$, et l'image de ce représentant par *f* est $f(x) + f(y)$, avec $f(y) \in F$. Il en résulte que $(\pi \circ f)(x)$ ne dépend que de $\overline{x}$ et non de *y*. On peut donc définir $\widetilde{f} : \overline{x} \in E/F \to \widetilde{f}(\overline{x}) = (\pi \circ f)(x) \in E/F$.

Si *f* est surjective, alors $\widetilde{f}$ aussi. En effet, soit $\overline{z}$ élément de E/F représenté par *z* élément de E. *z* admet un antécédent *x* par F et on a alors $\widetilde{f}(\overline{x}) = (\pi \circ f)(x) = \pi(z) = \overline{z}$.

❑ **factorisation à droite d'une application linéaire** : Soit f : E $\to$ F et g : E $\to$ G deux applications linéaires. Alors il existe une application linéaire h : Im(g) $\to$ F telle que $f = h \circ g$ si et seulement si Ker(g) $\subset$ Ker(f).
La condition nécessaire est facile à vérifier.
Réciproquement, supposons que Ker(g) $\subset$ Ker(f). Selon la proposition, en prenant H = Ker(g), il existe une unique application linéaire $\overline{f}$: E/Ker(g) $\to$ F telle que $f = \overline{f} \circ \pi$, où π : E $\to$ E/Ker(g) est la projection canonique. De plus, il existe un isomorphisme $\overline{g}$: E/Ker(g) $\to$ Im(g) tel que $g = \overline{g} \circ \pi$. On dispose alors du schéma suivant :



On a alors $f = h \circ g$ avec $h = \overline{f} \circ \overline{g}^{-1}$: Im(g) $\to$ F.
On reconnaîtra la même démarche adaptatée lors de la factorisation à droite d'une fonction f par une fonction g vue plus haut dans le cadre ensembliste, sous l'hypothèse :

$$\forall\ (x, y),\ g(x) = g(y) \Rightarrow f(x) = f(y).$$

❑ La factorisation à droite permet de montrer facilement le résultat suivant. Soit E un espace vectoriel sur le corps $\mathbb{K}$, φ_1, ..., φ_n et ψ des formes linéaires définies sur E telles que :

$$\mathrm{Ker}(\varphi_1) \cap ... \cap \mathrm{Ker}(\varphi_n) \subset \mathrm{Ker}(\psi)$$

Alors ψ est combinaison linéaire de (φ_1, ..., φ_n). En effet, considérons l'application linéaire Φ : E $\to \mathbb{K}^n$ définie par :

$$\forall\ x \in \mathrm{E},\ \Phi(x) = \begin{pmatrix} \varphi_1(x) \\ ... \\ \varphi_n(x) \end{pmatrix}$$

L'hypothèse signifie que Ker(Φ) $\subset$ Ker(ψ), donc il existe une application linéaire h : Im(Φ) $\to \mathbb{K}$ telle que $\psi = h \circ \Phi$. Prolongeons h par l'application nulle sur un supplémentaire de Im(Φ) dans $\mathbb{K}^n$ de façon à avoir une forme linéaire h définie sur $\mathbb{K}^n$. Il existe alors des scalaires a_1, ..., a_n tels que :

$$\forall \begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix} \in \mathbb{K}^n,\ h\left(\begin{pmatrix} y_1 \\ ... \\ y_n \end{pmatrix}\right) = a_1y_1 + ... + a_ny_n$$

On obtient alors :

$$\psi = h \circ \Phi = h \circ \begin{pmatrix} \varphi_1 \\ ... \\ \varphi_n \end{pmatrix} = a_1\varphi_1 + ... + a_n\varphi_n$$

et ψ est bien combinaison linéaire des φ_i.

❑ Plus généralement, soient E, F, F_1, ..., F_n des espaces vectoriels de dimension finie[1], et des applications linéaires $\psi : E \to F$, $\varphi_i : E \to F_i$, $1 \le i \le n$. On suppose que $\bigcap_{i=1}^{n} \mathrm{Ker}(\varphi_i) \subset \mathrm{Ker}(\psi)$. Alors il existe des applications linéaires $a_i : F_i \to F$, $1 \le i \le n$ telles que $\psi = \sum_{i=1}^{n} a_i \circ \varphi_i$. En effet, soit $\Phi : E \to \prod_{i=1}^{n} F_i$ définie par :

$$\forall\, x \in E,\ \Phi(x) = \begin{pmatrix} \varphi_1(x) \\ \dots \\ \varphi_n(x) \end{pmatrix}$$

Comme précédemment, $\mathrm{Ker}(\Phi) \subset \mathrm{Ker}(\psi)$, donc il existe une application linéaire $h : \mathrm{Im}(\Phi) \to F$ telle que :

$$\psi = h \circ \Phi = h(\varphi_1, ..., \varphi_n)$$
$$= h(\varphi_1, 0, ..., 0) + h(0, \varphi_2, 0, ..., 0) + ... + h(0, ..., 0, \varphi_n)$$

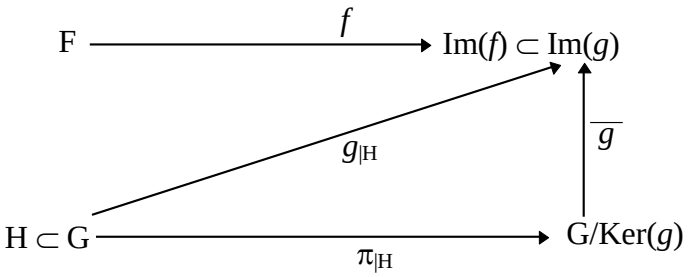
Prolongeons h par l'application nulle sur un supplémentaire de $\mathrm{Im}(\Phi)$ dans $\prod_{i=1}^{n} F_i$ de façon à définir h sur $\prod_{i=1}^{n} F_i$ tout entier. Posons :

$a_1 : y_1 \in F_1 \to h(y_1, 0, ..., 0)$
$a_2 : y_2 \in F_2 \to h(0, y_2, 0, ..., 0)$
etc.
$a_n : y_n \in F_n \to h(0, ..., 0, y_n)$

On obtient bien $\psi = \sum_{i=1}^{n} a_i \circ \varphi_i$.

❑ **Factorisation à gauche d'une application linéaire** : Soit $f : F \to E$ et $g : G \to E$ deux applications linéaires. Alors il existe une application linéaire $h : F \to G$ telle que $f = g \circ h$ si et seulement si $\mathrm{Im}(f) \subset \mathrm{Im}(g)$.
La condition nécessaire est facile à vérifier.
Réciproquement, supposons $\mathrm{Im}(f) \subset \mathrm{Im}(g)$. Soit $\pi : G \to G/\mathrm{Ker}(g)$ la projection canonique, $\overline{g} : G/\mathrm{Ker}(g) \to \mathrm{Im}(g)$ l'application résultant de la factorisation canonique de g, H un supplémentaire de $\mathrm{Ker}(g)$ dans G. Considérons le diagramme suivant :

[1] L'hypothèse de la dimension finie est uniquement utilisée pour valider l'existence d'un supplémentaire à un sous-espace vectoriel. En dimension infinie, cette existence nécessite un axiome, appelé l'axiome du choix.



$\overline{g}$ et $\pi_{|H}$ sont des isomorphismes (la réciproque de $\pi_{|H}$ est l'application qui, à une classe $\bar{x}$ de E/Ker(g) associe l'unique représentant de cette classe qui soit élément de H). On peut donc considérer l'application linéaire h : F → G (en fait h va de F dans H) définie par :

$$h = \pi_{|H}^{-1} \circ \overline{g}^{-1} \circ f$$

On a alors :

$$f = \overline{g} \circ \pi_{|H} \circ h = g_{|H} \circ h = g \circ h$$

4- Algèbre tensorielle, algèbre extérieure

Soit E et F deux espaces vectoriels sur un corps $\mathbb{K}$. On note $\mathbb{K}^{(E\times F)}$ l'espace vectoriel des fonctions de E × F dans $\mathbb{K}$, nulles partout sauf sur un nombre fini de couples (x, y), $x \in$ E, $y \in$ F. Une base de cet espace vectoriel est formé de la famille des fonctions que nous noterons $\delta_x \otimes \delta_y$ définies par :

$$\forall\ (t, u) \in E \times F,\ (\delta_x \otimes \delta_y)(t, u) = \begin{cases} 0 \text{ si } (t, u) \neq (x, y) \\ = 1 \text{ si } (t, u) = (x, y) \end{cases}$$

Un élément quelconque de $\mathbb{K}^{(E\times F)}$ s'écrit comme $\sum \lambda\ \delta_x \otimes \delta_y$, où ($x$, y) décrit une famille finie de E × F.

Soit H le sous-espace vectoriel engendré par les tous les éléments :

$\delta_{x+x'} \otimes \delta_y - \delta_x \otimes \delta_y - \delta_{x'} \otimes \delta_y$

$\delta_x \otimes \delta_{y+y'} - \delta_x \otimes \delta_y - \delta_x \otimes \delta_{y'}$

$\delta_{\lambda x} \otimes \delta_y - \lambda\ \delta_x \otimes \delta_y$

$\delta_x \otimes \delta_{\lambda y} - \lambda\ \delta_x \otimes \delta_y$

où x, x' sont des éléments quelconques de E, y et y' des éléments quelconques de F, et λ un scalaire quelconque. On pose alors E ⊗ F le quotient $\mathbb{K}^{(E\times F)}$/H, et on note $x \otimes y$ la classe d'équivalence de $\delta_x \otimes \delta_y$. E ⊗ F s'appelle le **produit tensoriel** de E et de F. Les éléments de E ⊗ F s'écrivent $\sum \lambda x \otimes y$, $x \in$ E, $y \in$ F, $\lambda \in \mathbb{K}$, avec les règles de calcul suivantes :

$(x + x') \otimes y = x \otimes y + x' \otimes y$

$x \otimes (y + y') = x \otimes y + x \otimes y'$

$(\lambda x) \otimes y = \lambda(x \otimes y) = x \otimes \lambda y$

On voit donc que ⊗ s'y comporte comme un produit, et l'application $(x, y) \to x \otimes y$ est bilinéaire.

L'intérêt du produit tensoriel est de transformer les applications bilinéaires f sur E × F dans un espace vectoriel quelconque G en une application linéaire de E ⊗ F vers G, la bilinéarité étant reportée des fonctions aux vecteurs. En effet, on associe à f une application linéaire définie sur $\mathbb{K}^{(E\times F)}$ (que nous noterons Φ) à valeur dans G en posant :

$$\forall\ (x, y) \in E \times F,\ \Phi(\delta_x \otimes \delta_y) = f(x, y)$$

On a donc, Φ étant linéaire :

$$\Phi(\delta_{x+x'} \otimes \delta_y - \delta_x \otimes \delta_y - \delta_{x'} \otimes \delta_y) = \Phi(\delta_{x+x'} \otimes \delta_y) - \Phi(\delta_x \otimes \delta_y) - \Phi(\delta_{x'} \otimes \delta_y)$$
$$= f(x + x', y) - f(x, y) - f(x', y)$$

$= 0$ car f est bilinéaire

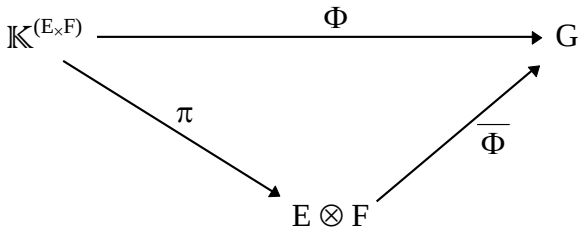
On montre de même que :

$\Phi(\delta_x \otimes \delta_{y+y'} - \delta_x \otimes \delta_y - \delta_x \otimes \delta_{y'}) = 0$

$\Phi(\delta_{\lambda x} \otimes \delta_y - \lambda\, \delta_x \otimes \delta_y) = 0$

$\Phi(\delta_x \otimes \delta_{\lambda y} - \lambda\, \delta_x \otimes \delta_y) = 0$

autrement dit, $H \subset \mathrm{Ker}(\Phi)$. Par conséquent, Φ se factorise en passant au quotient $\mathbb{K}^{(E\times F)}/H = E \otimes F$ en une application linéaire $\overline{\Phi}$:



Réciproquement, une fonction linéaire quelconque $\overline{\Phi}$: $E \otimes F \to G$ redonne une application bilinéaire f : $E \times F \to G$ en posant $f(x, y) = (\overline{\Phi} \circ \pi)(x \otimes y)$.

On prend maintenant E = F, et on considère le sous-espace vectoriel de $E \otimes E$ engendré par $x \otimes x$, $x \in E$. Le quotient de $E \otimes E$ par ce sous-espace vectoriel s'appelle l'**algèbre extérieure des bivecteurs** $\Lambda^2(E)$, et le produit s'y note $\wedge$. Les éléments de cette algèbre s'écrivent $\sum \lambda x \wedge y$, $x \in E$, $y \in E$, $\lambda \in \mathbb{K}$, avec les règles de calcul suivantes ;

$(x + x') \wedge y = x \wedge y + x' \wedge y$

$x \wedge (y + y') = x \wedge y + x \wedge y'$

$(\lambda x) \wedge y = \lambda\, (x \wedge y) = x \wedge \lambda y$

$x \wedge x = 0$

On a également :

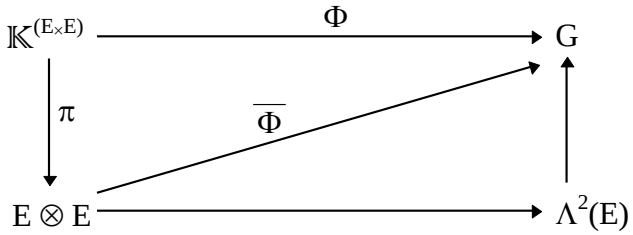
$x \wedge y = - y \wedge x$

car $0 = (x + y) \wedge (x + y) = x \wedge x + x \wedge y + y \wedge x + y \wedge y = x \wedge y + y \wedge x$.

Cet algèbre permet de transformer les applications bilinéaires alternées f de $E \times E$ vers un espace vectoriel G en une application linéaire sur $\Lambda^2(E)$. En effet, l'application linéaire $\overline{\Phi}$ de $E \otimes E$ à valeurs dans G associée à f vérifie :

$\overline{\Phi}(x \otimes x) = \Phi(\delta_x \otimes \delta_x) = f(x, x) = 0$ car f est alternée

Donc le sous-espace vectoriel engendré par les $x \otimes x$ est inclus dans $\mathrm{Ker}(\overline{\Phi})$ donc $\overline{\Phi}$ passe à son tour au quotient dans $\Lambda^2(E)$.



Si E est un espace vectoriel de dimension 2 de base (e_1, e_2), on a, compte tenu du fait que $e_1 \wedge e_1 = 0$, $e_2 \wedge e_2 = 0$, $e_2 \wedge e_1 = - e_1 \wedge e_2$:

$x \wedge y = (x_1e_1 + x_2e_2) \wedge (y_1e_1 + y_2e_2) = (x_1y_2 - x_2y_1)\, e_1 \wedge e_2 = \det(x, y)\, e_1 \wedge e_2$

C'est une façon originale d'introduire le déterminant.

IV : Anneau quotient

1- Structure d'anneau quotient

Soit (A, +, ×) un anneau unitaire, dont le produit n'est pas nécessairement commutatif, et soit ≡ une relation d'équivalence sur cet anneau. Soit A/≡ l'ensemble quotient. Soit $\pi : A \to A/\equiv$ la projection canonique. On se pose la question de savoir s'il est possible de munir l'ensemble quotient d'une structure d'anneau pour laquelle π est un morphisme d'anneau, i.e. :

$\forall\, (x, y) \in A^2,\ \pi(x + y) = \pi(x) + \pi(y)$

$\forall\, (x, y) \in A^2,\ \pi(xy) = \pi(x)\pi(y)$

$\pi(1) = 1$

où 1 est le neutre du produit, noté de la même façon dans A et dans A/≡. On notera de même 0 le neutre 0 pour la somme dans les deux anneaux. On déduit de la première relation que $\pi(0) = 0$ et que $\pi(-y) = -\pi(y)$ puisque π est un morphisme de groupe, mais la relation $\pi(1) = 1$ ne se déduit pas de la relation sur le produit et doit être donnée comme axiome.

Si π est un morphisme d'anneau, c'est aussi un morphisme du groupe additif (A, +), donc la relation ≡ doit être compatible avec la somme. Qu'en est-il pour le produit ? On doit avoir, pour tout *x*, *y*, *z* :

$x \equiv y \Rightarrow \pi(x) = \pi(y) \Rightarrow \pi(x)\pi(z) = \pi(y)\pi(z) \Rightarrow \pi(xz) = \pi(yz) \Rightarrow xz \equiv yz$

et on montrerait de même que $zx \equiv zy$. Donc ≡ doit être compatible avec les deux lois.

PROPOSITION

Soit A *un anneau muni d'une relation d'équivalence* ≡*. Les deux propriétés suivantes sont équivalentes :*

(i) ≡ *est compatible avec les lois de* A.

(ii) *On peut munir l'ensemble quotient* A/≡ *d'une structure d'anneau pour laquelle la projection canonique est un morphisme.*

Démonstration :

❑ (ii) ⇒ (i) résulte du préambule.

❑ (i) ⇒ (ii) : Etant compatible avec +, on sait déjà que A/≡ est un groupe avec l'addition :

$\pi(x) + \pi(y) = \pi(x + y)$

Posons maintenant, $\pi(x)\pi(y) = \pi(xy)$. Il s'agit de montrer que ce produit est bien défini, i.e. il ne dépend pas des représentants choisis. Le lecteur utilisera le même type de démonstration qu'on a vu dans le paragraphe concernant les groupes quotients.

On sait déjà que, si la relation est compatible, la classe de 0, neutre de l'addition, est un sous-groupe de A. Nous noterons I cette classe. Les éléments de I forment le noyau de π :

$$y \in I \Leftrightarrow y \equiv 0 \Leftrightarrow \pi(y) = \pi(0) \Leftrightarrow \pi(y) = 0$$

En ce qui concerne le produit, on a, pour tout *x* de A et tout *y* de I :

$\pi(xy) = \pi(x)\pi(y) = \pi(x)0 = 0$

donc $xy \in I$.

On montre de même que $yx \in I$. Cette propriété de I introduit une notion nouvelle :

DEFINITION
Soit A un anneau et I *un sous-groupe additif de* A. *On dit que* I *est un* **idéal** *de* A *si, pour tout x de* A *et tout y de* I, *xy et yx appartiennent à* I.

On peut abréger la propriété sur le produit par : $\forall\ x \in A$, $xI \subset I$ et $Ix \subset I$.

EXEMPLE :
❑ Soit u un endomorphisme d'un espace vectoriel de dimension finie E.
Soit $I = \{P \in \mathbb{K}[X],\ P(u) = 0\}$ l'ensemble des polynômes annulateurs de u. Alors I est un idéal. On laisse le lecteur montrer que c'est un sous-groupe de $\mathbb{K}[X]$. Montrons que :

$$\forall\ P \in I,\ \forall\ Q \in \mathbb{K}[X],\ QP = PQ \in I :$$

On a:

$$(QP)(u) = Q(u) \circ P(u) = Q(u) \circ 0 = 0$$

donc $QP \in I$.

❑ Soit $a_1, ..., a_n$ des éléments d'un anneau A commutatif. Il n'est pas difficile de montrer que :

$$I = \{ \sum_{i=1}^{n} a_i x_i,\ x_i \in A\}$$

forme un idéal de A. On l'appelle **idéal engendré** par les a_i.

❑ Les idéaux sont les $n\mathbb{Z}$, n entier positif ou nul. L'idéal engendré par deux entiers n et m est le même que l'idéal engendré par leur PGCD. Les idéaux de $\mathbb{K}[X]$ sont de la forme $\{PQ,\ P \in \mathbb{K}[X]\}$. (Voir le chapitre L2/ZSURNZ.PDF).

PROPOSITION
Soit $\equiv$ *une relation d'équivalence compatible avec les lois de l'anneau* A, *et soit* $I = \pi(0)$ *la classe d'équivalence du neutre* 0 *pour l'addition de* A. *Alors* :
(i) I *est un idéal de* A
(ii) *Pour tout x, y* de A, $x + I$ *est la classe d'équivalence de* x : $x \equiv y \Leftrightarrow x - y \in I$
(iii) *L'ensemble quotient est un anneau avec les deux lois suivantes :*
$(x + I) + (y + I) = (x + y) + I$
$(x + I)(y + I) = (xy) + I$
et la projection canonique est un morphisme d'anneau. On note A/I *l'anneau quotient.*

Démonstration :
❑ (i) a déjà été montré au moment d'introduire la notion d'idéal.

❑ (ii) se montre comme pour les espaces vectoriels. Ainsi, $\pi(x) = x + I$.

❑ (iii) résulte de la façon dont on doit définir somme et produit dans l'ensemble quotient pour que π soit un morphisme d'anneau.
Le neutre du produit est $\pi(1) = 1 + I$. En effet, pour tout x :

$$\pi(x)\pi(1) = \pi(x1) = \pi(x) = \pi(1x) = \pi(1)\pi(x)$$

Une relation ≡ compatible avec les lois de l'anneau met en évidence un idéal, la classe de 0. Réciproquement, un idéal permet de définir une relation d'équivalence compatible.

PROPOSITION
Soit I *un idéal de* A. *Posons* $x \equiv y$ *si et seulement si* $x - y \in$ I. *Il s'agit d'une relation d'équivalence compatible avec les loi de l'anneau, et* I *est la classe de* 0.

Démonstration :
❑ Bornons-nous à montrer la compatibilité avec le produit. Pour *x, y, z* quelconques :

$x \equiv y$
$\Rightarrow \quad x - y \in$ I
$\Rightarrow \quad z(x - y) \in$ I car I est un idéal
$\Rightarrow \quad zx - zy \in$ I
$\Rightarrow \quad zx \equiv zy$

et on aurait de même $xz \equiv yz$

Les idéaux sont caractérisés par la propriété suivante :
PROPOSITION
Soit A *un anneau et soit* I *une partie de* A. *Il y a équivalence entre* :
(i) I *est un idéal.*
(ii) I *est le noyau d'un morphisme de* A *dans un autre anneau*.

Démonstration :
❑ (i) $\Rightarrow$ (ii) : Si I est un idéal, on dispose de la projection canonique π : A $\rightarrow$ A/I qui est un morphisme. Son noyau est constitué des éléments équivalents à 0. Il s'agit de I lui-même.

❑ (ii) $\Rightarrow$ (i) : Si I = Ker(*f*) avec *f* : A $\rightarrow$ B, on sait déjà que I est un sous-groupe, puisque *f* est a fortiori un morphisme de groupe. Soit $x \in$ A et $y \in$ I. On a :

$f(xy) = f(x)f(y)$ car *f* est un morphisme d'anneau
$= f(x)0$ car $y \in$ I = Ker(*f*)
$= 0$

donc $xy \in$ Ker(*f*) = I.
De même $yx \in$ I. Ainsi, I est un idéal.

EXEMPLES :
❑ Dans l'anneau $\mathbb{Z}$, les parties $n\mathbb{Z}$ sont des idéaux. L'anneau quotient est le bien connu $\mathbb{Z}/n\mathbb{Z}$.

❑ Dans $\mathbb{R}$[X], l'ensemble des polynômes multiples de $X^2 + 1$ forme un idéal, noté $(X^2 + 1)$. L'anneau quotient $\mathbb{R}[X]/(X^2 + 1)$ est isomorphe à $\mathbb{C}$. En effet, dans l'anneau quotient, la classe de X joue le rôle du complexe *i*, puisque son carré sera égal à –1.

2- Factorisation canonique d'un morphisme d'anneau

Soit A un anneau, I un idéal de A, B un autre anneau, *f* : A $\rightarrow$ B un morphisme d'anneau, compatible avec la relation d'équivalence induite par I. *f* étant a fortiori un morphisme de groupes, et I étant un sous-groupe distingué de A, on a la propriété analogue, déjà montrée pour les groupes, et les espaces vectoriels et que nous ne redémontrons pas :

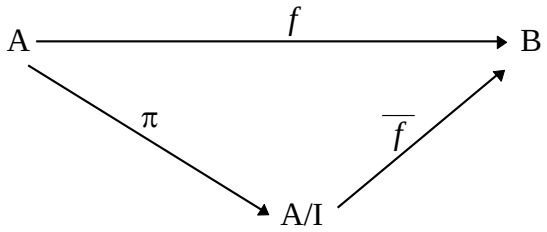
PROPOSITION
Soit A *un anneau,* I *un idéal de* A, B *un autre anneau,* $f : A \to B$ *un morphisme d'anneau. Il y a équivalence entre* :

(i) *f est compatible avec la relation d'équivalence sur* A *induite par* I.
(ii) $I \subset \text{Ker}(f)$

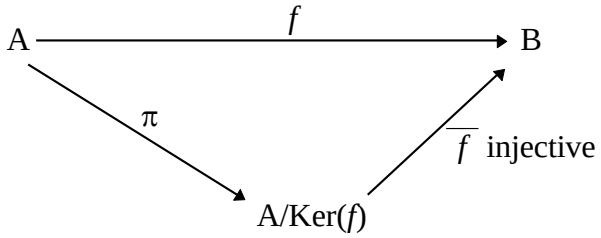
On peut alors procéder à la factorisation de *f* :

PROPOSITION
Soit A *un anneau,* I *un idéal de* A, B *un autre anneau,* $f : A \to B$ *un morphisme d'anneau tel que* $I \subset \text{Ker}(f)$. *Alors* :

(i) *il existe un unique morphisme* $\overline{f} : A/I \to B$ *tel que* $f = \overline{f} \circ \pi$.



(ii) *De plus, si* $I = \text{Ker}(f)$, $\overline{f}$ *est injective*.



Démonstration :
Elles sont analogues à celles déjà vues pour les groupes quotients ou les espaces vectoriels quotients.

3- Exemples

❑ Soit $f : P \in \mathbb{R}[X] \to P(i) \in \mathbb{C}$. Il n'est pas difficile de montrer que *f* est un morphisme d'anneau, et qu'il est surjectif. L'application $\overline{f} : \mathbb{R}[X]/\text{Ker}(f) \to \mathbb{C}$ sera donc à la fois injective et surjective. C'est donc un isomorphisme d'anneau. Mais :

$P \in \text{Ker}(f) \Leftrightarrow P(i) = 0 \Leftrightarrow$ P est divisible dans $\mathbb{C}$ par $X - i$
$\Leftrightarrow$ P est divisible dans $\mathbb{C}$ par $X - i$ et $X + i$ car P est à coefficients réels
$\Leftrightarrow$ P est divisible par $X^2 + 1$

L'idéal Ker(*f*) est l'ensemble des multiples de $X^2 + 1$. On retrouve l'isomorphisme entre $\mathbb{R}[X]/(X^2 + 1)$ et $\mathbb{C}$ vu plus haut.

Comment trouver rapidement la classe d'un polynôme P quelconque sous forme simple ? Effectuons la division euclidienne de P par $X^2 + 1$:

$\exists\, Q \in \mathbb{R}[X], \exists\, R \in \mathbb{R}[X], P = (X^2 + 1)Q + R, \deg(R) < 2$

Donc R est de la forme $a + bX$:

$P = (X^2 + 1)Q + a + bX$

Si on applique cette relation sur i, on obtient $P(i) = a + bi$.

Si on passe au quotient, puisque $X^2 + 1$ est dans la classe nulle, on obtient, en notant les classes avec une barre :

$$\overline{P} = a + b\overline{X}$$

Par ailleurs, $\overline{X}^2 = -1$ puisque $\overline{X}^2 + 1$ est la classe de $X^2 + 1$, donc la classe nulle.

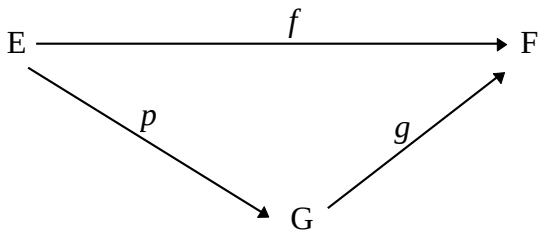
L'analogie entre les éléments $a + b\overline{X}$ du quotient et les complexes $a + bi$ est claire.

❑ Plus généralement, soit $\mathbb{K}$ un corps, P un polynôme irréductible dans $\mathbb{K}[X]$, (P) l'idéal engendré par P (i.e. constitué des polynômes divisibles par P). Alors $\mathbb{K}[X]/(P)$ est non seulement un anneau, mais un corps. En effet, soit $\overline{Q}$ un élément non nul de $\mathbb{K}[X]/(P)$. Cela signifie qu'un polynôme Q représentant de la classe $\overline{Q}$ n'appartient pas à l'idéal (P). Donc Q n'est pas divisible par P. P étant irréductible, cela signifie que P et Q sont premiers entre eux. D'après l'identité de Bézout, il existe deux polynômes tels que $AP + BQ = 1$. Si on repasse au quotient, on obtient $\overline{A}\,\overline{Q} = 1$ et $\overline{Q}$ admet bien un inverse.

Exercices

1- Enoncés

Exo.1) Soit trois ensembles E, F, G et trois applications $f : E \to F$, $p : E \to G$ et $g : G \to F$, telles que $f = g \circ p$. On suppose que p est surjective et g injective.



Montrer que G est en bijection avec $E/\equiv$ où $\equiv$ est la relation d'équivalence définie par :

$$x \equiv y \Leftrightarrow f(x) = f(y)$$

Exo.2) Soit $f : F \to G$ un morphisme de groupes.

a) Soit H un sous-groupe distingué de F. Montrer que $f(H)$ est un sous-groupe distingué de $\mathrm{Im}(f)$.

b) Soit K un sous-groupe distingué de G. Montrer que $f^{-1}(K)$ est un sous-groupe distingué de F.

Exo.3) Soit G un groupe. Soit H le sous-groupe de G engendré par les commutateurs $xyx^{-1}y^{-1}$, $x \in G$, $y \in G$. H est appelé le **groupe dérivé** de G.

a) Montrer que H est un sous-groupe distingué de G.

b) Montrer que G/H est commutatif.

c) Soit L un sous-groupe distingué de G. Montrer que G/L est commutatif si et seulement si $H \subset L$. Autrement dit, H est le plus petit sous-groupe distingué tel que le quotient de G par ce groupe soit commutatif.

Exo.4) Soit G un groupe, H et L deux sous-groupes distingués de G tels que $H \subset L$. Soit M un sous-groupe quelconque de G.

a) Montrer que H est distingué dans L, et que (G/H)/(L/H) est isomorphe à G/L.

b) Montrer que $ML = \{xy \mid x \in M, y \in L\}$ est un sous-groupe de G, que L est distingué dans ML, que $M \cap L$ est distingué dans M et que ML/L est isomorphe à $M/(M \cap L)$.

Exo.5) On dit qu'un groupe G est **résoluble** s'il existe une suite

$$\{e\} \subset G_1 \subset G_2 \subset ... \subset G_n = G$$

telle que, pour tout i, G_i est distingué dans G_{i+1} et G_{i+1}/G_i est abélien.

a) Montrer que le groupe symétrique $\mathfrak{S}_3$ est résoluble.

b) Montrer que $\mathfrak{S}_4$ est résoluble en considérant la suite :

$$\{\mathrm{Id}\} \subset \{\mathrm{Id}, (1\ 2)(3\ 4)\} \subset \{\mathrm{Id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \subset \mathfrak{A}_4 \subset \mathfrak{S}_4$$

où $(i\ \ j)$ désigne la transposition qui permute i et j, et où $\mathfrak{A}_4$ est le sous-groupe alterné des permutations paires.

Exo.6) Soit G un groupe, N un sous-groupe distingué de G, et H un sous-groupe de G. On pose $NH = \{nh,\ n \in N,\ h \in N\}$ en $N \times H = \{(n, h),\ n \in N,\ h \in H\}$. On suppose que $H \cap N = \{e\}$ et $G = NH$.

a) Montrer que l'application $p : (n, h) \in N \times H \to nh \in G$ est bijective.

b) On munit $N \times H$ de la loi composante par composante : $(n, h)(n', h') = (nn', hh')$, lui donnant une structure de groupe (**produit direct** de N et de H). Montrer que p est un morphisme de groupe si et seulement si les éléments de N commutent avec les éléments de H.

c) Dans le cas où p n'est pas un morphisme, on munit $N \times H$ de la loi $*$ suivante :

$$(n, h) * (n', h') = (nhn'h^{-1}, hh')$$

Montrer que $(N \times H, *)$ est un groupe et qu'il est isomorphe à G (**produit semi-direct** de N par H).

d) Montrer que $O_n(\mathbb{R})$ est le produit semi-direct de $SO_n(\mathbb{R})$ par un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

Exo.7) On se place dans le corps $\mathbb{Z}/3\mathbb{Z}$ et on considère l'anneau des polynômes $\mathbb{Z}/3\mathbb{Z}[X]$.

a) Montrer que le polynôme $X^2 + 1$ est irréductible dans $\mathbb{Z}/3\mathbb{Z}[X]$.

b) Soit $(X^2 + 1)$ l'idéal engendré par $X^2 + 1$. On considère l'anneau quotient $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$. Soit α la classe de X. Montrer que $1 + \alpha$ engendre le groupe multiplicatif des éléments non nuls de $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$.

Exo.8) Soit $(A, +, \times)$ un anneau commutatif **intègre**, i.e :

$$\forall\ (x, y) \in A^2,\ xy = 0 \Rightarrow x = 0 \text{ ou } y = 0.$$

Soit $S = A \setminus \{0\}$. On définit sur $A \times S$ une relation, ainsi que deux opérations. Pour a et b éléments de A, t et u éléments de S :

$$(a, t) \sim (b, u) \Leftrightarrow au = bt$$
$$(a, t) + (b, u) = (au + bt, tu)$$

$$(a, t) \times (b, u) = (ab, tu)$$

a) Montrer que $\sim$ est une relation d'équivalence, compatible avec les deux opérations + et $\times$.

b) Montrer que l'ensemble quotient est un corps. C'est le **corps des fractions** de A. Le cas type est A = $\mathbb{Z}$ donnant comme quotient $\mathbb{Q}$, et A = $\mathbb{K}$[X] donnant comme quotient $\mathbb{K}$(X), ensemble des fractions rationnelles $\frac{P}{Q}$ de polynômes en X.

Exo.9) Soit p un nombre premier. On considère l'anneau A des suites d'entiers relatifs $(a_n)_{n\geq 0}$ telles que, pour tout $n \geq 0$, $a_n \equiv a_{n+1} \bmod p^{n+1}$. Les opérations somme et produit se font composante par composante. (Autrement dit, A est une partie du produit direct de tous les $\mathbb{Z}/p^{n+1}\mathbb{Z}$, $n \in \mathbb{N}$).

a) Montrer que l'ensemble $I = \{(a_n) \mid \forall\, n, a_n \equiv 0 \bmod p^{n+1}\}$ est un idéal de A.

b) On note $\mathbb{Z}_p$ l'anneau quotient A/I, appelé **anneau des entiers *p*-adiques**. Si (r_n) est une suite d'entiers tels que, pour tout n, $0 \leq r_n < p$, et si on pose $a_n = \sum_{k=0}^{n} r_k\, p^k$, montrer que la suite (a_n) est élément de A. Réciproquement, montrer que tout élément de A est équivalent à une unique suite (a_n) ainsi définie. Autrement dit, les classes éléments de $\mathbb{Z}_p$ sont en bijection avec les suites (r_n), et on les notera symboliquement $\sum_{n=0}^{\infty} r_n\, p^n$.

c) On suppose dorénavant que $p = 2$. Montrer que, dans $\mathbb{Z}_2$, $\sum_{n=0}^{\infty} 2^n = -1$.

d) Montrer que l'élement de $\mathbb{Z}_2$ égal à $1 + \sum_{n=0}^{\infty} 2^{2n+1}$ est inversible dans $\mathbb{Z}_2$ et que son inverse est 3 = 1 + 2.

Exo.10) Soient E et F deux espaces vectoriels de dimension finie sur un même corps $\mathbb{K}$, E* et F* leur espace dual (espace vectoriel des formes linéaires de chaque espace dans le corps de base). Pour toute forme linéaire $\psi : E \to \mathbb{K}$ et $\chi : F \to \mathbb{K}$., posons $[\psi, \chi] : E \times F \to \mathbb{K}$ définie par

$$\forall\, (x, y) \in E \times F,\ [\psi, \chi](x, y) = \psi(x)\chi(y)$$

a) Vérifier que $[\psi, \chi]$ est bilinéaire. Il existe donc une forme linéaire, que nous noterons $\psi \,\#\, \chi : E \otimes F \to \mathbb{K}$ telle que :

$$\forall\, x \in E,\ \forall\, y \in F,\ (\psi \,\#\, \chi)(x \otimes y) = \psi(x)\chi(y)$$

On a ainsi défini une application :

$$(\psi, \chi) : E^* \times F^* \to \psi \,\#\, \chi \in (E \otimes F)^*$$

b) Montrer que l'application $(\psi, \chi) \to \psi \,\#\, \chi$ est elle-même bilinéaire. Elle induit une application linéaire $E^* \otimes F^* \to (E \otimes F)^*$ qui à $\psi \otimes \chi$ associe $\psi \,\#\, \chi$.

c) Montrer que cette application est un isomorphisme.

Exo.11) a) Dans $GL_n(\mathbb{R})$, montrer que : $(\forall\, A,\ {}^tAAB = B{}^tAA) \Leftrightarrow \exists\, \lambda,\ B = \lambda I_n$

b) Dans $GL_n(\mathbb{R})$, montrer que : $(\forall\, B \in O_n(\mathbb{R}),\ {}^tAAB = B{}^tAA) \Leftrightarrow \exists\, \lambda,\ \lambda A \in O_n(\mathbb{R})$

2- Solutions

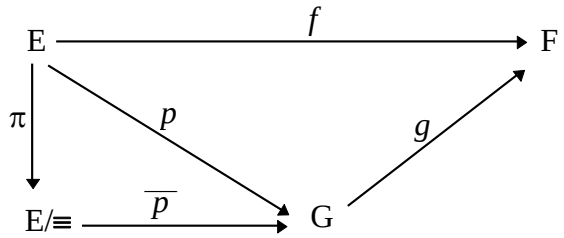
Sol.1) Soient x et y tels que $x \equiv y$. C'est équivalent à :

$f(x) = f(y)$

$\Leftrightarrow$ $(g \circ p)(x) = (g \circ p)(y)$

$\Leftrightarrow$ $p(x) = p(y)$ ($\Rightarrow$ car g est injective)

On constate donc que la relation $\equiv$ est aussi la relation d'équivalence définie par p. On peut donc procéder à la factorisation canonique de p via l'ensemble quotient E/$\equiv$:



où $\overline{p}$ est injective. Mais $p = \overline{p} \circ \pi$ et p surjective $\Rightarrow$ $\overline{p}$ surjective. Donc $\overline{p}$ est bijective.

A la bijection $\overline{p}$ près, on a montré que $f = g \circ p$ n'est autre que la factorisation canonique de f.

Sol.2) Le fait qu'il s'agisse de sous-groupes dans chaque cas est laissé au lecteur.

a) Pour tout x élément de Im(f), montrons que $xf(\mathrm{H})x^{-1} = f(\mathrm{H})$. Soit donc y élément de f(H), de la forme $f(u)$, $u \in$ H. Comme x appartient à Im(f), il existe z élément de F tel que $x = f(z)$. Donc :

$xyx^{-1} = f(z)f(u)f(z)^{-1} = f(zuz^{-1})$

mais $zuz^{-1} \in z\mathrm{H}z^{-1} = \mathrm{H}$ donc $xyx^{-1} \in f(\mathrm{H})$. On a montré que, pour tout x, $xf(\mathrm{H})x^{-1} \subset f(\mathrm{H})$.

Cela suffit car alors, on aura aussi $x^{-1}f(\mathrm{H})x \subset f(\mathrm{H})$ donc $f(\mathrm{H}) \subset xf(\mathrm{H})x^{-1}$.

b) Pour tout x de F, montrons que $xf^{-1}(\mathrm{K})x = f(\mathrm{K})$. Comme ci-dessus, il suffit de montrer l'inclusion. Soit y élément de $f^{-1}(\mathrm{K})$. On a :

$f(xyx^{-1}) = f(x)f(y)f(x)^{-1}$

donc $f(xyx^{-1}) \in f(x)\mathrm{K}f(x)^{-1}$ car $f(y) \in \mathrm{K}$

donc $f(xyx^{-1}) \in \mathrm{K}$ car K étant distingué, $f(x)\mathrm{K}f(x)^{-1} \in \mathrm{K}$

donc $xyx^{-1} \in f^{-1}(\mathrm{K})$.

Ainsi, $xf^{-1}(\mathrm{K})x \subset f(\mathrm{K})$.

Sol.3) a) $z\mathrm{H}z^{-1}$ est engendré par les $zxyx^{-1}y^{-1}z^{-1} = (zx)y(zx)^{-1}y^{-1}$ $yzy^{-1}z^{-1}$ qui est bien élément de H.

b) Notons π la projection canonique. On a $\pi(xyx^{-1}y^{-1}) = \pi(e)$ puisque $xyx^{-1}y^{-1}$ est élément de H et que H est la classe d'équivalence du neutre e de G. Donc :

$\pi(x)\pi(y)\pi(x^{-1})\pi(y^{-1}) = \pi(e)$

donc $\pi(x)\pi(y) = \pi(y)\pi(x)$

c) Si H est inclus dans L, alors, en notant p la projection canonique de G sur G/L, on a, pour tout x et y de G :

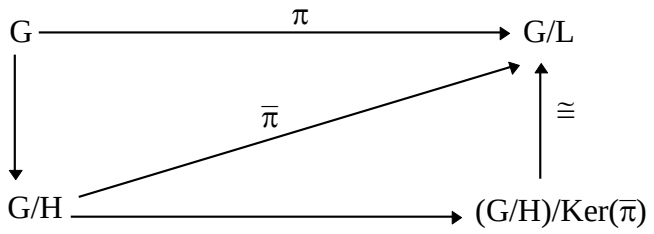
$p(x)p(y)p(x^{-1})p(y^{-1}) = p(xyx^{-1}y^{-1}) = e_{\mathrm{G/L}}$ puisque $xyx^{-1}y^{-1}$ est élément de H, donc de L

Réciproquement, si G/L est commutatif, alors par un calcul comparable au précédent :

$p(xyx^{-1}y^{-1}) = p(x)p(y)p(x^{-1})p(y^{-1}) = p(x)p(x^{-1})p(y)pw(y^{-1}) = e_{\mathrm{G/L}}$ donc $xyx^{-1}y^{-1}$ est élément de L donc H est inclus dans L.

Sol.4) a) Pour tout x de G, $x\mathrm{H}x^{-1} = \mathrm{H}$, donc c'est aussi vrai pour tout x de L, donc H est distingué dans L.

Considérons la projection canonique surjective $\pi : G \to G/L$ de noyau L. Comme $H \subset L = \mathrm{Ker}(\pi)$, cette projection se factorise en une application $\overline{\pi} : G/H \to G/L$ surjective, qui, à toute classe gH de G/H associe la classe gL de G/L. Un élément du noyau de $\overline{\pi}$ est une classe xH dans G/H telle que $\pi(x) = 0$, c'est-à-dire telle que xL = L, i.e. $x \in$ L. Comme H ⊂ L, et que $x \in$ L, xH est une classe de L/H. Ainsi, $\mathrm{Ker}(\overline{\pi})$ = L/H ce qui prouve que L/H est distingué dans G/H et que $\overline{\pi}$ se factorise en un isomorphisme de (G/H)/Ker($\overline{\pi}$) = (G/H)/(L/H) dans G/L.



b) Montrons que ML est stable pour la loi de composition interne. Si $x \in$ M, $y \in$ L, $x' \in$ M, $y' \in$ L, alors $xyx'y' = xx'x'^{-1}yx'y' \in$ ML car $xx' \in$ M, $x'^{-1}yx' \in$ L car L est distingué dans G, et donc $x'^{-1}yx'y \in$ L.

Montrons que ML est stable par passage au symétrique. Si $x \in$ M, $y \in$ L, alors :

$$(xy)^{-1} = y^{-1}x^{-1} = x^{-1}xy^{-1}x^{-1} \in \mathrm{ML}$$

En effet, $x^{-1} \in$ M et $xy^{-1}x^{-1} \in$ L car $y^{-1} \in$ L et L est distingué dans G.

Il est facile de montrer que L est distingué dans ML et que M ∩ L est distingué dans M.

Enfin, l'application $f : x \in \mathrm{M} \to x \in \mathrm{ML} \to x\mathrm{L} \in \mathrm{ML/L}$ est une application composée surjective de M dans ML/M, et son noyau est constitué des éléments x de M tels que xL = L, i.e. $x \in$ L. Ce noyau est donc égal à M ∩ L et la factorisation canonique de f donne un isomorphisme de M/(M ∩ L) sur ML/L.

Sol.5) a) Pour $\mathfrak{S}_3$, prendre $\{\mathrm{Id}\} \subset \mathfrak{A}_3 = \{\mathrm{Id}, (1\ 2\ 3), (1\ 3\ 2)\} \subset \mathfrak{S}_3$.

$\mathfrak{A}_3$ est abélien.

On a vu en exemple que, pour tout n, $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ et $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

b) Posons H = {Id, (1 2)(3 4)} et L = {Id, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)}.

H est commutatif car (1 2) et (3 4) commutent, n'ayant aucun élément en commun.

H est distingué dans L. En effet :

(1 2)(3 4)H = H = H(1 2)(3 4) puisque (1 2)(3 4) ∈ H

(1 3)(2 4)H = {(1 3)(2 4), (1 3)(2 4)(1 2)(3 4)} = {(1 3)(2 4), (1 4)(2 3)}

= H(1 3)(2 4) car on a aussi (1 2)(3 4)(1 3)(2 4) = (1 4)(2 3)

Le lecteur vérifiera de même que :

(1 4)(2 3)H = H(1 4)(2 3) = (1 3)(2 4)H

L/H ne comporte donc que deux classes, H et (1 3)(2 4)H. N'ayant que deux éléments, il est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ unique groupe à deux éléments donc est commutatif. On peut aussi vérifier directement que :

(1 3)(2 4)H (1 3)(2 4)H = H neutre de L/H.

L est distingué dans $\mathfrak{S}_4$. En effet, L est constitué de Id et de tous les produits de deux transpositions disjointes. Soit σ une permutation quelconque. Pour tout (i j), on a $\sigma(i\ j)\sigma^{-1} = (\sigma(i)\ \sigma(j))$. σ étant bijective, on aura :

$\sigma(1\ 2)(3\ 4)\sigma^{-1} = \sigma(1\ 2)\sigma^{-1}\ \sigma(3\ 4)\sigma^{-1} = (\sigma(1)\ \ \sigma(2))\ (\sigma(3)\ \ \sigma(4))$
produit de deux transpositions disjointes, donc élément de L, et de même pour les autres éléments de L. Etant distingué dans $\mathfrak{S}_4$, il l'est a fortiori dans $\mathfrak{A}_4$. $\mathfrak{A}_4$/L comporte $\frac{\text{Card}(\mathfrak{A}_4)}{\text{Card(L)}} = \frac{12}{4} = 3$ classes.
Or il n'y a qu'un seul groupe à trois éléments, $\mathbb{Z}/3\mathbb{Z}$ qui est commutatif, donc $\mathfrak{A}_4$/L est commutatif.
Pour tout n, $\mathfrak{A}_n$ est distingué dans $\mathfrak{S}_n$ et $\mathfrak{S}_n/\mathfrak{A}_n$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$.
On peut montrer que, pour $n \geq 5$, $\mathfrak{S}_n$ n'est pas résoluble. Ces questions sont liées à l'impossibilité, établie au XIXème siècle, de trouver des formules générales de résolution pour les polynômes de degré supérieur ou égal à 5.

Sol.6) a) p est surjective puisqu'on a supposé que G = NH. Montrons qu'elle est injective. Soit (n, h) et (n', h') tels que $p(n, h) = p(n', h')$. On a :
$nh = n'h'$
donc $n'^{-1}n = h'h^{-1} \in \text{N} \cap \text{H}$
donc $n'^{-1}n = h'h^{-1} = e$
donc $n = n'$ et $h = h'$
Attention. En général, p n'est pas un morphisme, donc il n'est pas question de chercher le noyau de p.
b) Si les éléments de p commutent avec ceux de H, alors, pour tout n, n', h, h' :
$p(n, h)\ p(n', h') = nhn'h' = nn'hh' = p(nn', hh')$
Donc p est un morphisme du groupe produit vers G.
Réciproquement, si p est un morphisme de groupe, alors, pour tout n de N et h de H :
$nh = p(n, e)p(e, h) = p(ne, eh) = p(n, h) = p(en, he) = p(e, h)p(h, e) = hn$
et les éléments de N commutent avec ceux de H.
c) La loi est bien interne car, N étant distingué, $hn'h^{-1}$ est bien élément de N. Vérifions l'associativité :

$$\begin{aligned}((n, h) * (n', h')) * (n'', h'') &= (nhn'h^{-1}, hh') * (n'', h'') \\ &= (nhn'h^{-1}\ hh'n''h'^{-1}h^{-1}, hh'h'') \\ &= (nhn'h'n''h'^{-1}h^{-1}, hh'h'') \\ &= (n\ h(n'h'n''h'^{-1})h^{-1}, hh'h'') \\ &= (n, h) * (n'h'n''h'^{-1}, h'h'') \\ &= (n, h) * ((n', h') * (n'', h''))\end{aligned}$$

Le neutre est (e, e) puisque :
$(n, h) * (e, e) = (nheh^{-1}, he) = (n, h)$
et $(e, e) * (n, h) = (eene^{-1}, eeh) = (n, h)$
Le symétrique de (n, h) est $(h^{-1}n^{-1}h, h)$ car :
$(n, h) * (h^{-1}n^{-1}h, h^{-1}) = (nhh^{-1}n^{-1}hh^{-1}, hh^{-1}) = (e, e)$
$(h^{-1}n^{-1}h, h^{-1}) * (n, h) = (h^{-1}n^{-1}hh^{-1}nh, h^{-1}h) = (e, e)$
L'application $p : (n, h) \to nh$ est bijective et est un morphisme pour la loi $*$. En effet :
$p((n, h) * (n', h')) = p(nhn'h^{-1}, hh') = nhn'h^{-1}hh' = nhn'h' = p(n, h)\ p(n', h')$
d) N = $\text{SO}_n(\mathbb{R})$ est bien un sous-groupe distingué de $\text{O}_n(\mathbb{R})$. Prendre pour H le sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et égal à {Id, r} où r est une réflexion donnée. Vérifier que NH = $\text{O}_n(\mathbb{R})$ et H ∩ N = {Id}. On a alors, pour $u \in \text{SO}_n(\mathbb{R})$ et $r^m \in$ H, $m \in \{0, 1\}$: $p(u, r^m) = ur^m$
Il s'agit bien d'un morphisme de groupe pour le produit semi-direct. En effet :
$p((u, r^m) * (v, r^p)) = p(ur^mvr^{-m}, r^{m+p}) = ur^mvr^p = p(u, r^m)\ p(v, r^p)$

Sol.7) a) Si le polynôme $X^2 + 1$ était scindé, il aurait des racines dans $\mathbb{Z}/3\mathbb{Z}[X]$. Or ni 0, ni 1 ni 2 n'annule ce polynôme. Donc il est irréductible.
b) Il y a neuf éléments dans $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$, dont huit non nuls, tous de la forme $\lambda + \mu\alpha$, avec λ et μ éléments de $\mathbb{Z}/3\mathbb{Z}$. En effet, $\alpha^2 = -1 = 2 \bmod 3$ et on peut éliminer les puissances de α supérieures ou égal à 2.

$1 + \alpha$	$= 1 + \alpha$
$(1 + \alpha)^2 = 1 + 2\alpha + \alpha^2$	$= 2\alpha$
$(1 + \alpha)^3 = 2\alpha(1 + \alpha) = 2\alpha + 2\alpha^2$	$= 1 + 2\alpha$
$(1 + \alpha)^4 = (1 + 2\alpha)(1 + \alpha) = 1 + 2\alpha^2$	$= 2$
$(1 + \alpha)^5 = 2(1 + \alpha)$	$= 2 + 2\alpha$
$(1 + \alpha)^6 = (2 + 2\alpha)(1 + \alpha) = 2 + \alpha + 2\alpha^2$	$= \alpha$
$(1 + \alpha)^7 = \alpha(1 + \alpha) = \alpha + \alpha^2$	$= 2 + \alpha$
$(1 + \alpha)^8 = (2 + \alpha)(1 + \alpha) = 2 + \alpha^2$	$= 1$

On a bien trouvé tous les éléments non nuls de $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$. Cela prouve également que $\mathbb{Z}/3\mathbb{Z}[X]/(X^2 + 1)$ est un corps puisque tout élément non nul est de la forme $(1 + \alpha)^k$ et possède pour inverse $(1 + \alpha)^{8-k}$. Il s'agit du corps à neuf éléments $\mathbb{F}_9$.

Sol.8) a) La réflexivité et la symétrie sont triviales. Montrons la transitivité :

$$\begin{aligned}(a, t) \sim (b, u) \text{ et } (b, u) \sim (c, v) &\Rightarrow au = bt \text{ et } bv = cu \\ &\Rightarrow auv = btv = ctu \\ &\Rightarrow (av - ct)u = 0\end{aligned}$$

or $u \neq 0$ et A est intègre, donc $av = ct$ et donc $(a, t) \sim (c, v)$.

Montrons la compatibilité pour la somme. Soit $(a, t) \sim (a', t')$ alors :

$$(a, t) + (b, u) \sim (a', t') + (b, u)$$

$$\Leftrightarrow \quad (au + bt, tu) \sim (a'u + bt', t'u)$$

$$\Leftrightarrow \quad (au + bt)t'u = (a'u + bt')tu$$

$$\Leftrightarrow \quad aut'u + btt'u = a'utu + bt'tu$$

ce qui est bien vrai car, par hypothèse $at' = a't$. Ainsi, on peut remplacer dans la somme un élément par un élément équivalent. Cela signifie donc que l'opération pourra passer au quotient, la somme de deux classes ne dépendant pas du représentant choisi.
On a de même :

$$(a, t) \times (b, u) \sim (a', t') \times (b, u)$$

$$\Leftrightarrow \quad (ab, tu) \sim (a'b, t'u)$$

$$\Leftrightarrow \quad abt'u = a'btu$$

ce qui est bien vrai car $at' = a't$. Le produit passe donc également au quotient.
b) Les deux lois sont clairement commutatives. Le produit est clairement associatif. Vérifions que + l'est également :

$$\begin{aligned}((a, t) + (b, u)) + (c, v) &= (au + bt, tu) + (c, v) \\ &= (auv + btv + ctu, tuv) \\ &= (a, t) + (bv + cu, uv) \\ &= (a, t) + ((b, u) + (c, v))\end{aligned}$$

Le neutre de la somme est (0, 1). Le neutre du produit est (1, 1). Toutes ces propriétés passent au quotient.
Dans A × S, (a, t) n'a pas nécessairement de symétrique pour +, mais il en a un dans le quotient. Montrons que le symétrique de la classe de (a, t) est la classe de $(-a, t)$. On a en effet :

$$(a, t) + (-a, t) = (0, t^2) \sim (0, 1)$$

De même, si la classe de (a, t) est non nulle, c'est-à-dire différente de la classe de (0, 1), autrement dit si $a \neq 0$, alors elle admet un inverse pour le produit qui est (t, a). En effet :

$$(a, t) \times (t, a) = (at, at) \sim (1, 1)$$

Sol.9) a) trivial

b) Comme $a_{n+1} = \sum_{k=0}^{n+1} r_k p^k$, on a bien $a_{n+1} \bmod p^{n+1} \equiv \sum_{k=0}^{n} r_k p^k = a_n$.

Soit maintenant une suite (a_n) représentant une classe élément de $\mathbb{Z}_p$. On peut supposer $0 \leq a_n < p^{n+1}$ quitte à remplacer a_n par son reste module p^{n+1}. Comme $a_n \equiv a_{n-1} \bmod p^n$, $a_n - a_{n-1}$ est un multiple de p^n. Posons $r_0 = a_0$ et, pour $n \geq 1$, posons r_n le reste de la division euclidienne de $\frac{a_n - a_{n-1}}{p^n}$ par p.

On a $0 \leq r_n < p$, et pour tout $n \geq 1$:

$$\frac{a_n - a_{n-1}}{p^n} \equiv r_n \bmod p$$

donc $a_n - a_{n-1} \equiv r_n p^n \bmod p^{n+1}$

Montrons par récurrence sur n que $a_n = \sum_{k=0}^{n} r_k p^k$. Cette relation est vraie pour $n = 0$. Supposons qu'elle soit vraie au rang $n - 1$. On a donc :

$$a_{n-1} = \sum_{k=0}^{n-1} r_k p^k$$

Or $a_n \equiv a_{n-1} + r_n p^n \bmod p^{n+1}$

donc $a_n \equiv \sum_{k=0}^{n} r_k p^k \bmod p^{n+1}$. Mais ces deux nombres sont compris entre 0 et $p^{n+1} - 1$. Donc ils sont égaux. D'où la représentation cherchée.

c) Les coefficients r_n de $\sum_{n=0}^{\infty} 2^n$ valent tous 1, donc le a_n correspondant vaut $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$. Ainsi,

$\sum_{n=0}^{\infty} 2^n$ est représenté dans A par la suite $(2^{n+1} - 1)_{n\geq 0} = (1, 3, 7, 15, 31, ...)$

Les coefficients r_n de 1 sont tous nuls, sauf le premier qui vaut 1, donc le a_n correspondant vaut 1 pour tout n. Ainsi, 1 est représenté dans A par la suite constante (1, 1, ...) (qui est bien neutre pour le produit composante par composante). Donc $1 + \sum_{n=0}^{\infty} 2^n$ est la classe de l'élément de A égal à :

$$(2^{n+1} - 1)_{n\geq 0} + (1)_{n\geq 0} = (2^{n+1})_{n\geq 0}$$

ou $(1, 3, 7, 15, 31, ...) + (1, 1, ...) = (2, 4, 8, 16, 32, ...)$

Mais la suite $(2^{n+1})_{n\geq 0}$ appartient à l'idéal I donc sa classe est nulle.

Intuitivement, $\sum_{n=0}^{\infty} 2^n$ = ...111111 avec un développement infini de 1 vers la gauche, de sorte que S + 1 = 0, la retenue se propageant indéfiniment de la droite vers la gauche en annulant tous les chiffres, d'où S = –1.

d) La classe $1 + \sum_{n=0}^{\infty} 2^{2n+1}$ est représentée dans A par la suite (a_n) = (1, 3, 3, 11, 11, 43, 43, ...), dont le terme général vaut $a_{2n-1} = a_{2n} = 1 + \sum_{k=0}^{n-1} 2^{2k+1}$. Si on la multiplie par la suite (1, 3, 3, 3, 3, ...) représentant la classe 3 = 1 + 2, alors on obtient la suite (1, 9, 33, 33, 129, 129, ...) dont le premier terme vaut 1 et, pour $n \geq 1$, dont les termes de rang $2n - 1$ et $2n$ valent :

$$3 \times (1 + \sum_{k=0}^{n-1} 2^{2k+1}) = 3 \times (1 + 2\,\frac{4^n - 1}{3}) = 3 + 2(4^n - 1) = 2^{2n+1} + 1 \equiv 1 \bmod 2^{2n+1}$$

donc la suite produit est équivalente à la suite constante (1, 1, ...) dont la classe est le neutre du produit.

$\mathbb{Z}_p$ admet un anneau des fractions noté $\mathbb{Q}_p$. On vient de montrer que, dans $\mathbb{Z}_2$, $1 + \sum_{n=0}^{\infty} 2^{2n+1} = \frac{1}{3}$.

Sol.10) a) Pas de difficulté.
b) Montrons la linéarité de l'application $(\psi, \chi) \to \psi \# \chi$ par rapport à ψ, une démonstration analogue s'appliquant sur χ. Il s'agit de montrer que, pour tout ψ, ψ' de E* et tout λ de $\mathbb{K}$, on a :

$(\psi + \lambda\psi') \# \chi = \psi \# \chi + \lambda(\psi' \# \chi)$
$\Leftrightarrow$ $\forall (x, y) \in E \times F, ((\psi + \lambda\psi') \# \chi)(x \otimes y) = (\psi \# \chi + \lambda(\psi' \# \chi))(x \otimes y)$
$\Leftrightarrow$ $\forall (x, y) \in E \times F, ((\psi + \lambda\psi') \# \chi)(x \otimes y) = (\psi \# \chi)(x \otimes y) + \lambda(\psi' \# \chi)(x \otimes y)$
$\Leftrightarrow$ $\forall (x, y) \in E \times F, (\psi + \lambda\psi')(x)\chi(y) = \psi(x)\chi(y) + \lambda\psi'(x)\chi(y)$
ce qui est bien vrai.
c) L'application est surjective. Soit φ un élément de $(E \otimes F)^*$. C'est une application linéaire de $E \otimes F$ vers $\mathbb{K}$, donc elle définit une forme bilinéaire $B : E \times F \to \mathbb{K}$ par :

$$\forall (x, y) \in E \times F, \varphi(x \otimes y) = B(x, y)$$

Dans une base $(e_1, ..., e_n)$ de E et $(\varepsilon_1, ..., \varepsilon_p)$ de F, et leurs bases duales (e_i^*) et (ε_j^*), on a :

$$\varphi(x \otimes y) = B(x, y) = \sum_{i,j} x_i\, y_j\, B(e_i, \varepsilon_j) = \sum_{i,j} B(e_i, \varepsilon_j)\, e_i^*(x)\, \varepsilon_j^*(y) = \sum_{i,j} B(e_i, \varepsilon_j)\, (e_i^* \# \varepsilon_j^*)(x \otimes y)$$

donc $\varphi = \sum_{i,j} B(e_i, \varepsilon_j)\, e_i^* \# \varepsilon_j^*$. Donc φ est l'image de $\sum_{i,j} B(e_i, \varepsilon_j)\, e_i^* \otimes \varepsilon_j^*$.

L'application est injective. Cherchons son noyau. Soit un élément de $E^* \otimes F^*$ qu'on peut supposer de la forme $\sum_{i,j} \lambda_{ij}\, e_i^* \otimes \varepsilon_j^*$ avec les notations précédentes, et dont l'image $\sum_{i,j} \lambda_{ij}\, e_i^* \# \varepsilon_j^*$ est identiquement nulle. En appliquant cette image au couple $e_i \otimes \varepsilon_j$, i et j quelconques, on obtient $\lambda_{ij} = 0$. Donc l'application initiale est bien nulle.

Sol.11) a) $GL_n(\mathbb{R})$ est dense dans $\mathcal{M}_n(\mathbb{R})$ (voir les exercices de L2/EVNORME.PDF), donc, si la relation $\forall\ A \in GL_n(\mathbb{R})$, ${}^tAAB = B{}^tAA$ est vérifiée, alors on aura aussi $\forall\ A \in \mathcal{M}_n(\mathbb{R})$, ${}^tAAB = B{}^tAA$.
Prenons donc A dont tous les éléments sont nuls sauf un 1 en position diagonale (m, m), $1 \le m \le n$. On a ${}^tA = A$ et ${}^tAA = A^2 = A$. La relation devient donc $AB = BA$, ce qui donne, pour tout i et j :

$$\sum_{k=1}^{n} a_{ik}\, b_{kj} = \sum_{k=1}^{n} b_{ik}\, a_{kj}$$

Si $i \neq m$, et $j = m$, on obtient $0 = b_{im}$
Ceci étant vrai pour tout m et tout $i \neq m$, il en résulte que la matrice B est diagonale.
Notons $\lambda_1, ..., \lambda_n$ les éléments de la diagonale de B. Il reste à montrer que tous les λ_i sont égaux. $(e_1, ..., e_n)$ étant la base canonique de $\mathbb{R}^n$, soit $i < j$ et soit P la matrice orthogonale associée à l'isométrie définie par :

$$Pe_i = \frac{1}{\sqrt{2}}(e_i + e_j)$$

$$Pe_j = \frac{1}{\sqrt{2}}(-e_i + e_j)$$

$$Pe_k = e_k \text{ pour } k \neq i \text{ et } k \neq j$$

Pour toute matrice A de $GL_n(\mathbb{R})$, on a ${}^tAAB = B{}^tAA$ donc ${}^tP{}^tAABP = {}^tPB{}^tAAP$ ou ${}^tP{}^tAP{}^tPAP{}^tPBP = {}^tPBP{}^tP{}^tAP{}^tPAP$ puisque, P étant orthogonale, ${}^tPP = I_n$. Quand A parcourt $GL_n(\mathbb{R})$, $A' = {}^tPAP$ parcourt aussi $GL_n(\mathbb{R})$ car l'application $A \to {}^tPAP$ est une bijection de $GL_n(\mathbb{R})$ dans $GL_n(\mathbb{R})$. Remarquant que ${}^tA' = {}^tP{}^tAP$, on a donc : $\forall\ A' \in GL_n(\mathbb{R})$, ${}^tA'A'{}^tPBP = {}^tPBP{}^tA'A'$. Donc, en appliquant la première partie de la démonstration à ${}^tPBP$, on en déduit que ${}^tPBP$ est une matrice diagonale. Il existe donc μ tel que :

$${}^tPBPe_i = \mu e_i$$

$$\Leftrightarrow \quad BPe_i = P\mu e_i$$

$$\Leftrightarrow \quad \frac{1}{\sqrt{2}} B(e_i + e_j) = \frac{\mu}{\sqrt{2}}(e_i + e_j)$$

$$\Leftrightarrow \quad \lambda_i e_i + \lambda_j e_j = \mu\,(e_i + e_j)$$

$$\Leftrightarrow \quad \lambda_i = \lambda_j = \mu$$

Ceci étant vrai pour tout i et tout j, B est une matrice scalaire.
La réciproque est triviale.

b) Posons $C = {}^tAA$, de sorte que $\forall\ B \in O_n(\mathbb{R})$, $CB = BC$. Soit $1 \le i < j \le n$, $\theta \neq 0 \bmod \pi$ et B la matrice telle que $B_{ii} = B_{jj} = \cos(\theta)$, $B_{ij} = -B_{ji} = \sin(\theta)$, $B_{kk} = 1$ pour tout $k \notin \{i, j\}$ et tous les autres coefficients de B nuls. B est une matrice orthogonale. On a :

$$(CB)_{ij} = \sum_{k=1}^{n} C_{ik}B_{kj} = \sin(\theta)C_{ii} + \cos(\theta)C_{ij}$$

et $$(BC)_{ij} = \sum_{k=1}^{n} B_{ik}C_{kj} = \cos(\theta)C_{ij} + \sin(\theta)C_{jj}$$

donc $C_{ii} = C_{jj}$. Il en résulte que tous les termes diagonaux de C sont égaux.

Soit $l \neq j$ et $l \neq i$ On a :

$$(CB)_{il} = \sum_{k=1}^{n} C_{ik}B_{kl} = C_{il}$$

et $$(BC)_{il} = \sum_{k=1}^{n} B_{ik}C_{kl} = \cos(\theta)C_{il} + \sin(\theta)C_{jl}$$

donc $(1 - \cos(\theta))C_{il} = \sin(\theta)C_{jl}$ ou encore $2\sin^2(\frac{\theta}{2})\, C_{il} = 2\sin(\frac{\theta}{2})\cos(\frac{\theta}{2})\, C_{jl}$ ou enfin :

$$\sin(\frac{\theta}{2})\, C_{il} = \cos(\frac{\theta}{2})\, C_{jl}$$

Ceci devant être vrai pour tout $\theta \neq 0 \bmod \pi$, on a nécessairement $C_{il} = C_{jl} = 0$. Donc C est une matrice scalaire μI_n. Ainsi, ${}^tAA = \mu I_n$. Mais $\mu > 0$ car, pour X n'appartenant pas au noyau de A, on a :

$$0 < \| AX \|^2 = \langle AX, AX \rangle = {}^tX{}^tAAX = \mu {}^tXX = \mu \| X \|^2$$

Posant $\lambda = \frac{1}{\sqrt{\mu}}$, on a alors $A' = \lambda A$ qui vérifie ${}^tA'A' = I_n$. On a bien $\lambda A \in O_n(\mathbb{R})$.

◆