Corrigé du devoir à la maison

Exercice 0 : *Montrer que si f est un endomorphisme de K^d tel que pour tout vecteur $v \in K^d$ il existe un scalaire $\lambda_v \in K$ tel que $f(v) = \lambda_v v$, alors il existe un unique $\lambda \in K$ tel que $f(v) = \lambda v$ pour tout $v \in K^d$.*

solution: Si v et w sont deux vecteurs linéairement indépendants, alors $\lambda_v v + \lambda_w w = f(v) + f(w) = f(v+w) = \lambda_{v+w} v + \lambda_{v+w} w$, donc $\lambda_v = \lambda_w$. D'autre part si v et w sont linéairement dépendants et non nuls, alors on peut supposer $w = \mu v$ pour un $\mu \in K^*$, et donc $\lambda_w \mu v = \lambda_w w = f(w) = \mu f(v) = \mu \lambda_v v$, soit $\lambda_v = \lambda_w$. Donc $v \to \lambda_v$ est constante sur $K^d \backslash \{0\}$, ce qu'il fallait démontrer.

Exercice 1 : *Montrer que le centre de $SL_d(K)$ est $Z_d(K)$.*

solution: Soit f dans le centre de $SL_d(K)$. L'idée est d'utiliser l'exercice 0 pour montrer que $f \in Z_d(K)$. Il nous suffit donc de montrer que quel que soit $v \in K^d \backslash \{0\}$ il existe $f(v) \in Kv$. Pour ce faire on pose $e_1 = v$ et on complète e_1 en une base $(e_1, ..., e_d)$ de K^d, puis on considère le bloc de Jordan $J \in SL_d(K)$ de taille d associé à cette base (c'est-à-dire l'endomorphisme défini par $Je_i = e_i + e_{i-1}$ pour $i \geq 2$ et $Je_1 = e_1$). Clairement l'ensemble $W := \{w \in K^d, Jw = w\}$ des vecteurs fixés par J coincide avec la droite $Ke_1 = Kv$. Mais $fJ = Jf$ par hypothèse sur f. Donc si $w \in W$, $Jf(w) = fJ(w) = f(w)$, i.e. $f(w) \in W$. On a donc montré que $f(v) \in Kv$. cqfd.

On admettra que le cardinal de $Z_d(\mathbb{F}_p)$ est le pgcd de d et $p-1$ (cela résulte du fait que le groupe multiplicatif $\mathbb{F}_p^*$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$).

Exercice 2 : *Montrer que le cardinal de $GL_d(\mathbb{F}_p)$ est $C(p,d) = (p^d - 1) \cdot ... \cdot (p^d - p^{d-1})$, que le cardinal de $SL_d(\mathbb{F}_p)$ est $\frac{C(p,d)}{p-1}$. Calculer le cardinal de $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$.*

solution: Pour $GL_d(\mathbb{F}_p)$ il s'agit de compter le nombre de bases de l'espace vectoriel $\mathbb{F}_p^d$. On choisit un premier vecteur non nul, soit $p^d - 1$ possibilités. Pour le deuxième vecteur de la base, on peut choisir n'importe quel vecteur sauf ceux qui sont colinéaires au premier vecteur, donc cela fait $p^d - p$ vecteurs. Pour le troisième on peut choisir n'importe quel vecteur sauf ceux qui sont dans le plan engendré par les deux premiers vecteurs de la base, soit $p^d - p^2$ possibilités. Etc. A la fin au obtient donc $(p^d - 1) \cdot ... \cdot (p^d - p^{d-1})$ possibilités.

Date: 5 avril 2008.

Pour $SL_d(\mathbb{F}_p)$ on fait comme pour $GL_d(\mathbb{F}_p)$ sauf que le dernier vecteur doit satisfaire une condition supplémentaire : le déterminant de la base construite doit être égal à 1. Si e_n est le dernier vecteur d'une base $(e_1, ..., e_n)$ alors parmi tous les vecteurs λv où λ varie dans $\mathbb{F}_p^*$, il y a un et un seul λ pour lequel la base $e_1, ..., e_{n-1}, \lambda e_n$ est de déterminant 1, car $\det(e_1, ..., e_{n-1}, \lambda e_n) = \lambda \det(e_1, ..., e_n)$. Donc $Card(SL_d(\mathbb{F}_p)) = \frac{Card(GL_d(\mathbb{F}_p))}{Card(\mathbb{F}_p^*)} = \frac{C(p,d)}{p-1}$.

On a $Card(GL_2(\mathbb{F}_2)) = (2^2-1)(2^2-2) = 6$ et $Card(GL_2(\mathbb{F}_3)) = (3^2-1)(3^2-3) = 48$. Donc $Card(SL_2(\mathbb{F}_2)) = 6$ et $Card(SL_2(\mathbb{F}_3)) = 24$. Mais $Card(Z_d(\mathbb{F}_p)) = pgcd(p-1, d)$, donc $Card(Z_2(\mathbb{F}_2)) = 1$ et $Card(Z_2(\mathbb{F}_3)) = 2$. Ainsi $Card(PSL_2(\mathbb{F}_2)) = 6$ et $Card(PSL_2(\mathbb{F}_3)) = 12$.

Exercice 3 : *Montrer que $PSL_2(\mathbb{F}_2) = GL_2(\mathbb{F}_2)$ est isomorphe au groupe symétrique $\mathcal{S}_3$ des permutations d'un ensemble à 3 éléments et que $PSL_2(\mathbb{F}_3)$ est isomorphe au groupe alterné des permutations paires d'un ensemble à 4 éléments. Indication : on pourra prendre comme ensemble l'ensemble des droites de l'espace vectoriel $\mathbb{F}_p \times \mathbb{F}_p$.*

solution: Soit X_p l'ensemble des droites de $\mathbb{F}_p \times \mathbb{F}_p$ (qui passent par 0). C'est un ensemble à $\frac{p^2-1}{p-1} = p+1$ éléments. En effet tout point différent de 0 définit une droite et chaque droite contient $p-1$ points différents de 0. $SL_2(\mathbb{F}_p)$ agit sur $\mathbb{F}_p \times \mathbb{F}_p$ naturellement par transformations linéaires et envoie toute droite sur une droite.

Ainsi $PSL_2(\mathbb{F}_p)$ agit sur X_p, donc induit un homomorphisme $PSL_2(\mathbb{F}_p) \to Bij(X_p)$ où $Bij(X_p)$ est le groupe des bijections de l'ensemble X_p. Cet homomorphisme est injectif, car si $g \in SL_2(\mathbb{F}_p)$ fixe chaque droite de X_p, alors on est dans la situation de l'exercice 0 et donc $g \in Z_d(\mathbb{F}_p)$ c'est-à-dire que l'image de g dans $PSL_d(\mathbb{F}_p)$ est triviale.

Mais d'après l'exercice 3, $PSL_2(\mathbb{F}_2)$ a 6 éléments, tout comme $Bij(X_2) = \mathcal{S}_3$. Donc cet homomorphisme est un isomorphisme. De même $PSL_2(\mathbb{F}_3)$ est isomorphe à un sous-groupe d'ordre 12 de $\mathcal{S}_4$. Mais on vérifie facilement qu'il existe un seul sous-groupe d'ordre 12 de $\mathcal{S}_4$ et que c'est le groupe alterné A_4.

(pour cela on peut procéder ainsi: soit G un sous-groupe d'ordre 12 de $\mathcal{S}_4$ soit $\varepsilon : G \to \{\pm 1\}$ la signature ; soit $\varepsilon(G) = 1$ et donc G est contenu et donc égal à A_4, soit $\varepsilon(G) = \{\pm 1\}$ et donc $G \cap A_4$ est d'ordre 6 ; on vérifie ensuite que A_4 n'a pas de sous-groupe d'ordre 6 : en effet un tel sous-groupe est soit isomorphe à $\mathbb{Z}/6\mathbb{Z}$ soit à $\mathcal{S}_3$: mais dans A_4 il y a, en plus de l'identité, 8 cycles d'ordre 3 et 3 produits de deux transpositions de supports disjoints (donc d'ordre 2), donc il n'y a pas d'éléments d'ordre 6, donc A_4 n'a pas de sous-groupe isomorphe à $\mathbb{Z}/6\mathbb{Z}$; finalement $\mathcal{S}_3$ a trois éléments d'ordre 2 et deux éléments d'ordre 3 donc si $G \simeq \mathcal{S}_3$ alors G est constitué, outre l'identité, de tous les produits τ de deux permutations à support disjoints et de deux cycles d'ordre 3 disons σ et σ^2 ; ces cycles fixent un points, mais τ ne fixe aucun point, donc $\tau\sigma\tau^{-1}$ est un autre cycle d'ordre 3 ce qui n'est pas possible.) Au passage on voit que cela fournit un contre-exemple

au théorème de Lagrange, i.e. 6 divise 12 mais A_4 n'a pas de sous-groupe d'ordre 6.

Soit G un groupe. On appelle commutateur tout élément de G de la forme $xyx^{-1}y^{-1}$. On appelle sous-groupe dérivé de G le sous-groupe $D(G)$ engendré par les commutateurs de G.

Exercice 4 : *Montrer que $D(G)$ est un sous-groupe distingué de G. Montrer que $D(PSL_2(\mathbb{F}_2))$ est strictement plus petit que $PSL_2(\mathbb{F}_2)$ et de même pour $D(PSL_2(\mathbb{F}_3))$ dans $PSL_2(\mathbb{F}_3)$. En déduire que $PSL_2(\mathbb{F}_2)$ et $PSL_2(\mathbb{F}_3)$ ne sont pas simples.*

solution: Pour montrer que $D(G)$ est distingué, il suffit de montrer que l'ensemble des commutateurs $\{xyx^{-1}y^{-1}, x \in G, y \in G\}$ est stable par conjugaison par n'importe quel élément de G. Ceci est évident car $gxyx^{-1}y^{-1}g^{-1} = x_g y_g x_g^{-1} y_g^{-1}$ où $x_g = gxg^{-1}$ et $y_g = gyg^{-1}$.

D'après l'exercice précédent, $PSL_2(\mathbb{F}_2) \simeq \mathcal{S}_3$ et l'homomorphisme signature $\varepsilon : \mathcal{S}_3 \to \{\pm 1\}$ est non triviale, donc $\ker \varepsilon = A_3$ est un sous-groupe non trivial de $\mathcal{S}_3$. Mais clairement $\varepsilon(D(\mathcal{S}_3)) = 1$, donc $D(\mathcal{S}_3) \subset A_3 \subsetneq \mathcal{S}_3$. Ainsi $D(PSL_2(\mathbb{F}_2)) \subsetneq PSL_2(\mathbb{F}_2)$. Pour $PSL_2(\mathbb{F}_3) \simeq A_4$ on remarque que A_4 possède un sous-groupe distingué Γ d'ordre 4 constitué des éléments d'ordre 2 de A_4 (il s'agit des produits de deux transpositions de supports disjoints). Ce sous-groupe Γ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$. Le groupe quotient est donc d'ordre 3 et isomorphe à $\mathbb{Z}/3\mathbb{Z}$. Il s'ensuit que $D(PSL_2(\mathbb{F}_2)) \subset \Gamma$ et $D(PSL_2(\mathbb{F}_3)) \subsetneq PSL_2(\mathbb{F}_3)$.

Ces groupes ne sont pas simples car ils possèdent un sous-groupe distingué non trivial.

On appelle transvection toute endomorphisme T de K^d tel qu'il existe un vecteur non nul $v \in K^d$ et une forme linéaire f de K^d (i.e. une application linéaire de K^d dans K) telle que $f(v) = 0$ et pour tout vecteur $x \in K^d$ on a $Tx = x + f(x)v$.

Exercice 5 : *Montrer que toute transvection est inversible, i.e. appartient à $GL_d(K)$. Montrer que $g \in GL_d(K)$ est une transvection si et seulement si il existe une base de K^d dans laquelle la matrice de g a tous ses coefficients diagonaux égaux à 1 et tous ses coefficients non diagonaux nuls sauf peut-être l'un d'entre eux .*

solution : T est injective car si $Tx = 0$ alors $x = -f(x)v$ et en appliquant f on obtient $f(x) = 0$ car $f(v) = 0$, et donc $x = 0$. D'autre part T est surjective car $T(y - f(y)v) = y$ pour tout vecteur y. Donc T est bijective, i.e. $T \in GL_d(K)$.

Soit g une transvection, soit H le noyau de f. On pose $e_1 = v$ et on complète e_1 pour former une base $(e_1, ..., e_{d-1})$ de H. Enfin on ajoute un vecteur $e_d \notin H$. Clairement, dans la base $(e_1, ..., e_d)$ la matrice de g a bien la forme demandée.

Réciproquement si g a une matrice de cette forme dans une base $(e_1, ..., e_d)$. Quitte à changer l'ordre des e_i on peut supposer que le seul coefficient non diagonal non nul de g (appelons-le λ) est celui sur la ligne 1 et la colonne d. On définit alors la forme linéaire f en posant $f(e_i) = 0$ si $i < d$ et $f(e_d) = \lambda$. Alors on a bien

$ge_i = e_i + f(e_i)e_1$ pour chaque i et donc g est une transvection.

Exercice 6 : *Montrer que $SL_d(K)$ est engendré par les transvections. Indication : utiliser le pivot de Gauss et les opérations sur les lignes et les colonnes.*

solution : Soit $A \in SL_d(K)$. On rappelle que multiplier A à gauche (resp. à droite) par une matrice de transvection revient à remplacer A par une nouvelle matrice que l'on obtient à partir de A est ajoutant un multiple de la i-ème ligne (resp. colonne) à la j-ème ligne (resp. colonne) pour $i \neq j$. Remarquer aussi que les matrices de transvection sont de déterminant 1, donc on reste toujours dans $SL_d(K)$ en faisant ces opérations.

Il suffit donc de montrer qu'après un nombre fini de telles opérations sur les lignes et les colonnes de la matrice A on obtient la matrice identité.

Remarquer aussi que l'on peut permuter deux lignes (resp. colonnes) L_i et L_j quitte à changer le signe de L_i ou de L_j car cela correspond à la suite d'opérations $L_i \leftarrow L_i - L_j$, $L_j \leftarrow L_i + L_j$, $L_i \leftarrow L_i + L_j$. Il est donc clair qu'après un nombre fini d'opérations sur les lignes on obtient une matrice avec des zéros sur toute la première colonne sauf le premier coefficient en haut à droite. En agissant maintenant sur les colonnes (i.e. en multipliant à droite par des transvections) on obtient aussi des zéros sur toute la première ligne, excepté le premier coefficient. On peut alors répéter cette opération sur la matrice carré de taille $d-1$, et ainsi de suite jusqu'à ce que l'on obtienne une matrice diagonale.

On peut de plus se ramener aux matrices de la forme $diag(\lambda, 1, ..., 1)$ pour $\lambda \in K$. En effet, en permutant deux lignes on aura alors toutes les matrices $diag(1, ..., 1, \lambda, 1, ..., 1)$, puis en multipliant ces matrices, on aura toutes les matrices diagonales.

Pour voir que $diag(\lambda, 1, ..., 1)$ est engendré par des transvections, il suffit de voir que $diag(\lambda, 1)$ est engendré par des transvections. Mais on vérifie facilement qu'une opération sur les lignes et une sur les colonnes suffisent à transformer cette matrice en l'identité. cqfd.

Exercice 7 : *Montrer que si K n'est pas de caractéristique 2, alors toute transvection T est un commutateur de $GL_d(K)$. En déduire dans ce cas que $D(GL_d(K)) = SL_d(K)$. Indication: montrer que T et T^2 sont semblables.*

solution : Si toute transvection est un commutateur, alors bien sur $D(GL_d(K)) = SL_d(K)$ car les transvections engendrent $SL_d(K)$ d'après l'exercice 6. Supposons d'abord que $d \geq 3$, et montrons que $T^2 = g^{-1}Tg$ pour une matrice $g \in SL_d(K)$. Cela entraînera que $T = T^{-1}g^{-1}Tg$, qui est un commutateur. En effet, on a $Tx = x + f(x)v$. On choisit $e_1 = v$ et on complète en une base $e_1, ..., e_{d-1}$ du noyau de f, puis on choisit e_d en dehors du noyau de f. Alors $(e_1, ..., e_d)$ est une base de K^d et on peut définir l'endomorphisme $g \in SL_d(K)$ en posant $ge_1 = e_1$, $ge_2 = \frac{1}{2}e_2$, $ge_i = e_i$ si $2 \leq i \leq d-1$ et $ge_d = 2e_d$. Alors on vérifie que $f(gx) = 2f(x)$ pour tout x et que $g^{-1}Tg = T^2$.

Cet argument ne marche pas si $d = 2$ (on pourrait trouver une matrice g, mais pas forcément de déterminant 1). Dans SL_2 on écrit simplement :

$$\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \cdot \begin{pmatrix} a & \\ & a^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & -x \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & (a^2-1)x \\ & 1 \end{pmatrix}$$

On peut fixer $a \neq \pm 1$ et pour tout $y \in K$ on pose $x = y/(a^2-1)$. Ainsi la tranvection $\begin{pmatrix} 1 & y \\ & 1 \end{pmatrix}$ est un commutateur.

Problème : *Soit G un groupe qui agit sur un ensemble X. On suppose que l'action de G sur X est doublement transitive, c'est-à-dire que pour tous $x \neq y \in X$ et tous $z \neq w$ dans X il existe $g \in G$ tel que $g \cdot x = z$ et $g \cdot y = w$. Pour tout $x \in X$ on note H_x le stabilisateur de x, c'est-à-dire le sous-groupe de G formé des éléments $g \in G$ tels que $g \cdot x = x$.*

Le but des questions a) à d) est de monter que tout sous-groupe distingué N de G agit soit transitivement (i.e. pour tout $x, y \in X$ il existe $g \in N$ tel que $g \cdot x = y$) soit trivialement (i.e. N fixe chaque point de X).

a) Soit $x \in X$. Montrer que H_x agit transitivement sur $X \backslash \{x\}$.

solution: soit $y, z \in X\backslash\{x\}$, d'après l'hypothèse, G agit transitivement sur les paires donc il existe $g \in G$ qui transporte la paire (x, y) en la paire (x, z), i.e. $gy = z$ et $gx = x$ (et donc $g \in H_x$).

b) Soit $x \in X$ et $g \notin H_x$. Monter que $G = H_x \cup H_x g H_x$.

solution: si $h \notin H_x$ alors hx et gx sont dans $H_x\backslash\{x\}$ et par a) il existe $k \in H_x$ tel que $hx = kgx$, ce qui veut dire que $h \in H_x g H_x$.

c) Soit $x \in X$. Montrer que H_x est maximal dans G, c'est-à-dire que si L est un sous-groupe de G tel que $H_x \subset L \subset G$ alors soit $L = G$ soit $L = H_x$.

solution: Si L contient H_x strictement, il existe $g \in L\backslash H_x$ et donc par b) $G = H_x \cup H_x g H_x$. Mais $H_x g H_x$ est contenu dans L, donc $G = L$.

d) Soit $x \in X$ et N un sous-groupe distingué de G. Montrer que NH_x est un sous-groupe de G. En déduire que soit N agit trivialement sur X soit N agit transitivement sur X.

solution: soit n_1, n_2 dans N et h_1 h_2 dans H_x, on a $n_1 h_1 n_2 h_2 = n_1 h_1 n_2 h_1^{-1} h_2 \in NH_x$ car $h_1 n_2 h_1^{-1} \in N$ puisque N est distingué. De même $(n_1 h_1)^{-1} = h_1^{-1} n_1^{-1} = h_1^{-1} n_1^{-1} h_1 h_1^{-1} \in NH_x$ car $h_1^{-1} n_1^{-1} h_1 \in N$. Donc NH_x est stable par multiplication et inverse : c'est un sous-groupe de G.

NH_x est un sous-groupe de G qui contient H_x donc d'après c), soit $NH_x = H_x$, soit $NH_x = G$. Dans le premier cas N est contenu dans H_x donc N fixe x,

mais en fait N fixe aussi gx quel que soit $g \in G$ car $ngx = gg^{-1}ngx = gx$ car $g^{-1}ng \in N$ puisque N est distingué. Finalement N fixe tout point de X car G agit transitivement sur X et donc $X = Gx$. Donc N agit trivialement sur X.

Dans le second cas, $NH_x = G$. Puisque G agit transitivement sur X, pour tout $y \in X$ il existe $g \in G$ tel que $gx = y$. Comme on peut écrire $g = nh$ où $n \in N$ et $h \in H_x$ on a donc $nx = y$. Ainsi N envoie x sur n'importe quel point de X. Donc en fait N agit transitivement sur X, car si z est un second point, alors il y a $m \in N$ tel que $mx = z$, d'où $mn^{-1}y = z$.

Maintenant on fait une hypothèse supplémentaire sur le groupe G. On suppose qu'il existe pour chaque $x \in X$ un sous-groupe U_x de G tel que U_x est abélien et $U_{g\cdot x} = gU_xg^{-1}$ pour tout $x \in X$ et tout $g \in G$. On suppose de plus que la réunion des U_x engendre G.

Attention! j'avais oublié une hypothèse à cet endroit : on doit supposer que aucun élément de G n'agit trivialement, c'est-à-dire que si $g \in G$ et $g \cdot x = x$ pour tout $x \in X$ alors g est l'identité.

e) Montrer que si $x \in X$ et N est un sous-groupe distingué de G, alors $NU_x = G$.

solution: Remarquons d'abord que NU_x est un sous-groupe de G (pour la même raison qu'au d)). Ensuite on observe qu'il suffit de montrer que NU_x contient tous les U_y pour $y \in X$, puisque ceux-ci engendrent G. Mais d'après le d) soit N agit trivialement sur X, soit il agit transitivement. Si N n'est pas réduit à l'identité, alors il ne peut pas agir trivialement d'après l'hypothèse manquante à l'énoncé. On sait donc que N agit transitivement sur X, c'est-à-dire que pour tout $y, x \in X$ il existe $n \in N$ tel que $n \cdot x = y$. D'où $nU_xn^{-1} = U_y$. Mais $nU_xn^{-1} \in NU_x$, donc tous les U_y sont dans NU_x, ce qu'il fallait démontrer.

f) Montrer que si N est un sous-groupe distingué de G, alors N contient le sous-groupe dérivé $D(G)$ de G (c'est-à-dire le sous-groupe de G engendré par les commutateurs, i.e. tous les éléments de la forme $xyx^{-1}y^{-1}$).

solution: le groupe quotient G/N est abélien car U_x est abélien. Donc tout commutateur $xyx^{-1}y^{-1}$ pour $x, y \in G$ est trivial dans G/N, c'est-à-dire que $xyx^{-1}y^{-1} \in N$. Ainsi $D(G)$ est contenu dans N.

Question subsidiaire: On admettra le fait suivant si K est un corps et d un entier ≥ 2:

$$D(SL_d(K)) = SL_d(K) \text{ sauf si } d = 2 \text{ et } K = \mathbb{F}_2 \text{ ou } \mathbb{F}_3. \tag{1}$$

En utilisant le problème et le fait (1) ci-dessus, montrer que si K est un corps et d un entier ≥ 2, alors $G = PSL_d(K)$ est un groupe simple (i.e. n'a pas de sous-groupes distingués non triviaux) sauf si $d = 2$ et K est soit $\mathbb{F}_2$ soit $\mathbb{F}_3$. Indication:

on fera agir G sur l'ensemble X des droites de K^d (appelé espace projectif) et on fera un choix judicieux pour U_x (penser aux transvections).

solution: Soit X l'ensemble des droites de K^d. Pour $x \in X$, on note D_x la droite de K^d associée. Vérifions d'abord que G agit fidèlement sur X (i.e. aucun $g \in G\backslash\{1\}$ n'agit trivialement). En effet si $g \in SL_d(K)$ fixe chaque droite de K^d alors on est dans la situation de l'exercice 0 et donc g doit être une homothétie, i.e. $g \in Z_d(K)$, donc g est l'identité dans $PSL_d(K)$.

Verifions aussi que G agit doublement transitivement sur X. En effet, soit $x_1, x_2, y_1, y_2 \in X$ et soit v_1 et v_2 deux vecteurs linéairement indépendants tels que $D_{x_1} = Kv_1$ et $D_{x_2} = Kv_2$ et soit w_1 et w_2 sont deux autres vecteurs linéairement indépendants tels que $D_{y_1} = Kw_1$ et $D_{y_2} = Kw_2$. On prolonge (v_1, v_2) en une base $(v_1, ..., v_d)$ de K^d et idem pour (w_1, w_2). Pour tout $\lambda \in K$, on définit $g \in GL_d(K)$ de la façon suivante $g(v_1) = \lambda w_1$ et $g(v_2) = w_2$ et $g(v_i) = w_i$ pour $i \geq 3$. On peut choisir λ de sorte que $\det g = 1$, i.e. $g \in SL_d(K)$. On a donc montrer qu'il existe $g \in G$ tel que $gx_1 = y_1$ et $gx_2 = y_2$.

Soit U_x l'ensemble de toutes les transvections de droite D_x, c'est-à-dire l'ensemble des transformations linéaires $T : K^d \to K^d$ de la forme $T(u) = u + f(u)v$, où $v \in D_x$ est un vecteur non nul et f une forme linéaire telle que $\ker f$ contient D_x. On vérifie aisément que U_x est un groupe abélien. Et de plus $gU_xg^{-1} = U_{g\cdot x}$ où $g \cdot x$ est la droite $g(D_x)$.

On est donc bien dans la situation du problème. On en conlcut que si N est un sous-groupe distingué non trivial de G, alors N contient le sous-groupe dérivé $D(G)$. D'après le fait admis, $D(SL_d(K)) = SL_d(K)$ sauf si $d = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$. Ainsi $D(G) = G$ et G n'a pas de sous-groupe disingué non trivial, i.e. G est simple.

Remarque : L'exercice 7 montre que si $car(K) \neq 2$, alors $D(GL_d(K)) = SL_d(K)$. On peut vérifier qu'en fait $D(SL_d(K)) = SL_d(K)$ (i.e. chaque transvection est un commutateur $xyx^{-1}y^{-1}$ où $x, y \in SL_d(K)$). Lorsque $car(K) = 2$, alors on peut vérifier que on a tout de même $D(SL_d(K)) = SL_d(K)$ sauf si $d = 2$ et $K = \mathbb{F}_2$ ou $\mathbb{F}_3$. Pour les détails voir F. Perrin, *Cours d'algèbre.*