UNIVERSITÉ DE RENNES 1

Théorie des Groupes et Géométrie

Feuille n°2

Espaces homogènes

Exercice 1 (Topologie quotient sur un espace homogène)

On appelle *groupe topologique* un groupe G muni d'une topologie telle que la multiplication $m : G \times G \to G$ et l'inversion $\mathrm{inv} : G \to G$ sont continues. Soit H un sous-groupe et $\pi : G \to G/H$ la projection vers le quotient de G par H agissant par multiplication à droite. On munit G/H de la topologie telle que : $V \subset G/H$ est ouvert ssi $\pi^{-1}(V)$ est ouvert.

1. Démontrez que π est continue. *Correction : L'image réciproque par π d'un ouvert est par définition ouvert, donc π est continue.*
2. Démontrez que π est ouverte (i.e l'image de tout ouvert est un ouvert). *Correction : Soit Ω un ouvert de G. Pour montrer que $\pi(\Omega)$ est ouvert, il suffit de montrer que $\pi^{-1}\big(\pi(\Omega)\big)$ est ouvert. Mais*

$$\begin{aligned} g \in \pi^{-1}\big(\pi(\Omega)\big) &\iff \pi(g) \in \pi(\Omega) \\ &\iff \text{il existe } \omega \in \Omega \text{ tel que } \pi(g) = \pi(\omega) \\ &\iff \text{il existe } \omega \in \Omega \text{ tel que } gH = \omega H \\ &\iff \text{il existe } \omega \in \Omega \text{ tel que } g \in \omega H \text{ (car } H \text{ est un sous-groupe)} \\ &\iff \text{il existe } \omega \in \Omega \text{ et } h \in H \text{ tels que } g = \omega h \\ &\iff \text{il existe } h \in H \text{ tel que } g \in \Omega h. \end{aligned}$$

   Ainsi, on en déduit que $\pi^{-1}\big(\pi(\Omega)\big) = \cup_{h\in H}\Omega h$ est une réunion d'ouverts (Ωh est bien un ouvert car les translations sont continues !) donc est ouvert.
3. Démontrez que si Y est un espace topologique et $f : G \to Y$ une application continue constante sur les classes modulo H, alors l'application induite $\bar{f} : G/H \to Y$ est continue. *Correction : Soit Ω un ouvert de Y. On veut montrer que $\bar{f}^{-1}(\Omega)$ est un ouvert de G/H, c'est-à-dire que $\pi^{-1}\big(\bar{f}^{-1}(\Omega)\big)$ est un ouvert de G. Mais :*

$$\begin{aligned} g \in \pi^{-1}\big(\bar{f}^{-1}(\Omega)\big) &\iff \pi(g) \in \bar{f}^{-1}(\Omega) \\ &\iff \bar{f} \circ \pi(g) \in \Omega \\ &\iff f(g) \in \Omega \\ &\iff g \in f^{-1}(\Omega) \end{aligned}$$

   donc $\pi^{-1}\big(\bar{f}^{-1}(\Omega)\big) = f^{-1}(\Omega)$ est ouvert par continuité de f.
4. Démontrez que si H et G/H sont connexes, alors G est connexe.
   Indication : il suffit de montrer que toute application continue $f : G \to \{0,1\}$ est constante. Correction : Soit $f : G \to \{0,1\}$ continue. Pour $g \in G$, l'application restreinte $f_g : gH \to \{0,1\}$ reste continue. Par continuité de la multiplication, la partie gH est connexe donc f_g est constante. Ainsi, par la question précédente on sait que $\bar{f} : G/H \to \{0,1\}$ est continue, donc est constante par connexité de G/H. On conclut que $f = \bar{f} \circ \pi$ est également constante, ce qui montre que G est connexe.

Exercice 2 (La sphère)

On note $S^n \subset \mathbb{R}^{n+1}$ la sphère euclidienne de dimension n.

1. Montrez que le groupe $\mathrm{SO}_{n+1}(\mathbb{R})$ des *déplacements* (isométries de déterminant 1) de $\mathbb{R}^{n+1}$ agit transitivement sur S^n. *Correction : Si $x, y \in S^n$, ces vecteurs sont non nuls et on peut donc chacun les compléter en des bases orthonormales $(x_0 = x, x_1, \ldots, x_n)$ et $(y_0 = y, y_1, \ldots, y_n)$ de $\mathbb{R}^{n+1}$. Il existe donc un élément $M \in \mathrm{SO}_{n+1}(\mathbb{R})$ qui envoie la première base sur la deuxième, en particulier $Mx = y$. On a bien montré ce qu'on voulait.*
2. Décrivez les stabilisateurs des points. *Correction : Soit $M \in \mathrm{SO}_{n+1}(\mathbb{R})$ qui stabilise un vecteur $x \in S^n$. Puisque M est une isométrie, la matrice M stabilise également $x^\perp$. Ainsi, la matrice M est semblable à un élément de $\mathrm{diag}\big(1, \mathrm{SO}_n(\mathbb{R})\big)$ (on vérifie bien que la sous-matrice M' vérifie $M'M'^\top = I_n$, par un calcul par bloc, et $\det M' = 1$ par triangularité par blocs de M).*

3. En utilisant la relation stabilisateur-orbite et l'exercice 1, démontrez par récurrence sur n que $\mathrm{SO}_n(\mathbb{R})$ est connexe. *Correction : Le groupe $\mathrm{SO}_1(\mathbb{R}) = \{1\}$ est bien connexe. Par récurrence, le groupe $\mathrm{SO}_{n+1}(\mathbb{R})$ est connexe puisque, étant donné $x_0 \in \mathrm{SO}_{n+1}(\mathbb{R})$, le stabilisateur $G \simeq \mathrm{SO}_n(\mathbb{R})$ de x_0 dans $\mathrm{SO}_{n+1}(\mathbb{R})$ est connexe par hypothèse de récurrence et $\mathrm{SO}_{n+1}(\mathbb{R})/G \simeq$ orbite de $x_0 = S^n$ est connexe également (on conclut avec l'exo 1.4). Il reste quand même à justifier pourquoi la bijection $f : \mathrm{SO}_{n+1}(\mathbb{R})/G \simeq S^n$ est un homéomorphisme. C'est bien une bijection, elle est continue par l'exo 1.3 car constante sur les classes (par définition du stabilisateur). Pour montrer que f^{-1} est continue, on va montrer que l'image réciproque par f^{-1} de tout fermé est fermé, c'est-à-dire l'image de tout fermé par f est fermé (c'est-à-dire f est fermée). Si F est un fermé de $\mathrm{SO}_{n+1}(\mathbb{R})/G$, il est compact car $\mathrm{SO}_{n+1}(\mathbb{R})/G$ est compact (car $\mathrm{SO}_{n+1}(\mathbb{R})$ l'est et la projection est continue par l'Exercice 1... il faut aussi montrer que $\mathrm{SO}_{n+1}(\mathbb{R})/G$ est séparé, ce que l'on admet[1]) donc comme f est continue on en déduit que $f(F)$ est également compact (car S^n est séparé) donc fermé (car S^n est fermé). (Remarque : pour démontrer ce résultat on peut aussi utiliser un théorème de réduction et raisonner comme dans l'exercice 12.)*

Exercice 3 (Bases d'un espace vectoriel)

Soient k un corps et E un k-espace vectoriel de dimension finie n.

1. Montrez que l'ensemble des bases de E est un espace principal homogène sous $\mathrm{GL}(E)$. *Correction : Le groupe $\mathrm{GL}(E)$ agit par translation sur l'ensemble des bases car l'image d'une base est une base, et l'action est simplement transitive car il existe une unique application linéaire inversible qui envoie une base sur une autre.*

2. Déduisez-en le calcul du cardinal de $\mathrm{GL}(E)$ lorsque k est fini de cardinal q. *Correction : Par la relation orbite-stabilisateur, le cardinal $\#\,\mathrm{GL}_n(q)$ est donné par le nombre de bases de $\mathbb{F}_q^n$. On en déduit que :*

$$\#\,\mathrm{GL}_n(q) = \prod_{i=0}^{n-1}(q^n - q^i) = q^{\frac{n(n-1)}{2}}\prod_{i=1}^{n}(q^i - 1).$$

Décompositions et drapeaux

Exercice 4 (Transformations linéaires identiques sur une droite)

Soient k un corps et E un k-espace vectoriel de dimension finie $n \geq 2$. On fixe une droite vectorielle D de E et on étudie le fixateur $\mathrm{GL}_D(E) := \{u \in \mathrm{GL}(E); u_{|D} = \mathrm{Id}_D\}$.

1. On note $\pi : E \to E/D$ la projection canonique.

(a) Montrer que pour tout $u \in \mathrm{GL}_D(E)$ il existe un unique $\bar{u} \in \mathrm{GL}(E/D)$ tel que $\pi \circ u = \bar{u} \circ \pi$. *Correction : (Note[2].) Comme $u_{|D} = \mathrm{Id}_D$, en particulier $u(D) \subset D$. On en déduit que l'application linéaire composée $E \xrightarrow{u} E \xrightarrow{\pi} E/D$ s'annule sur D. D'après la propriété universelle du quotient E/D, il existe alors un unique $\bar{u} \in \mathrm{GL}(E/D)$ tel que $\pi \circ u = \bar{u} \circ \pi$.*

(b) Montrer que $p : \mathrm{GL}_D(E) \to \mathrm{GL}(E/D)$ défini par $p(u) = \bar{u}$ est un morphisme de groupes. *Correction : Soient u, v deux éléments de $\mathrm{GL}_D(E)$. Si $x \in D$, on a $(uv)(x) = u(v(x)) = u(x) = x$ ce qui montre que $uv \in \mathrm{GL}_D(E)$. D'après la question précédente on dispose donc de $\bar{u}$, $\bar{v}$ et $\bar{uv}$ tels que*

$$\pi u = \bar{u}\pi \quad , \quad \pi v = \bar{v}\pi \quad et \quad \pi uv = \overline{uv}\pi.$$

Utilisant ces relations, on trouve $\bar{u}\bar{v}\pi = \bar{u}(\bar{v}\pi) = \bar{u}(\pi v) = (\bar{u}\pi)v = \pi uv$. Comme $\overline{uv}\pi$ et $\bar{u}\bar{v}\pi$ sont toutes deux égales à πuv, l'assertion d'unicité démontrée dans la question précédente implique que $\overline{uv} = \bar{u}\bar{v}$. En d'autres termes $p(uv) = p(u)p(v)$ i.e. p est un morphisme de groupes.

2. On note U_D la partie de $\mathrm{GL}_D(E)$ composée de Id_E et des transvections de droite D. Montrer que $\ker(p) = U_D$. *Correction : On note a un vecteur directeur de la droite D. Un élément de $\ker(p)$ est une application linéaire $u : E \to E$ telle que $u_{|D} = \mathrm{Id}_D$ et $\bar{u} = \mathrm{Id}_{E/D}$. La deuxième condition signifie que pour tout $x \in E$ on a $u(x) - x \in D$, donc il existe un scalaire $f(x) \in k^\times$ tel que $u(x) - x = f(x)a$. Comme u et Id_E sont linéaires, on a*

$$f(\lambda x + \mu y)a = (u - \mathrm{Id}_E)(\lambda x + \mu y) = \lambda(u - \mathrm{Id}_E)(x) + \mu(u - \mathrm{Id}_E)(y) = (\lambda f(x) + \mu f(y))a$$

donc $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ c'est-à-dire que f est une forme linéaire. Si $f = 0$ on a $u = \mathrm{Id}_E$, et sinon les conditions $f \neq 0$, $a \neq 0$ assurent que que u est une transvection de droite D.

Réciproquement, si u est Id_E ou une transvection de droite D, on peut écrire $u(x) = x + f(x)a$ pour une certaine forme linéaire (nulle si $u = \mathrm{Id}_E$ et non nulle sinon) qui s'annule en a. Dans tous les cas u est égale à l'identité sur $\ker(f)$, qui contient D, donc $u \in \mathrm{GL}_D(E)$. De plus $u(x) = x + f(x)a \equiv x \mod D$ ce qui implique que l'application linéaire induite $\bar{u}$ est égale à l'identité. Donc $u \in \ker(p)$.

1. C'est un fait général : si G est un groupe topologique et H un sous-groupe fermé alors G/H est séparé.

2. La correction de cet exercice est due à Matthieu Romagny : voir l'Exercice 3 de `https://perso.univ-rennes1.fr/matthieu.romagny/THGG_2122/CC1_2021_2022_corrige.pdf`.

3. Soit F un supplémentaire de D dans E. On identifie $\mathrm{GL}(F)$ à un sous-groupe de $\mathrm{GL}_D(E)$ en associant à une application linéaire $v \in \mathrm{GL}(F)$ l'application linéaire $\tilde{v} \in \mathrm{GL}_D(E)$ telle que $\tilde{v}_{|F} = v$ et $\tilde{v}_{|D} = \mathrm{Id}_D$. Montrer que $p_{|\,\mathrm{GL}(F)} : \mathrm{GL}(F) \longrightarrow \mathrm{GL}(E/D)$ est un isomorphisme.
Indication : choisir des bases et utiliser des descriptions matricielles. Correction : Notons $q : E \to F$ la projection associée à la décomposition en somme directe $E = F \oplus D$. C'est un morphisme surjectif de noyau D, qui induit donc un isomorphisme $\bar{q} : E/D \xrightarrow{\sim} F$ tel que $q = \bar{q}\pi$. Soit $\mathcal{B}_F = \{e_2, \dots, e_n\}$ une base de F et notons $\bar{e}_i = \pi(e_i)$ pour tout i. Alors $\mathcal{B}_E := \{a\} \cup \mathcal{B}_F$ est une base de E et $\mathcal{B}_{E/D} = \{\bar{e}_i\}$ est une base de E/D. Enfin notons aussi

$$\mathrm{GL}_n(k)_a = \left\{ M \in \mathrm{GL}_n(k), M = \begin{pmatrix} 1 & * & \cdots & * \\ 0 & \vdots & & \vdots \\ 0 & * & \cdots & * \end{pmatrix} \right\}$$

le stabilisateur dans $\mathrm{GL}_n(k)$ du premier vecteur de base. Ces bases fournissent des identifications :

$$\alpha : \mathrm{GL}(F) \xrightarrow{\sim} \mathrm{GL}_{n-1}(k), \quad f \mapsto \mathrm{Mat}_{\mathcal{B}_F}(f)$$
$$\beta : \mathrm{GL}_D(E) \xrightarrow{\sim} \mathrm{GL}_n(k)_a, \quad f \mapsto \mathrm{Mat}_{\mathcal{B}_E}(f)$$
$$\gamma : \mathrm{GL}(E/D) \xrightarrow{\sim} \mathrm{GL}_{n-1}(k), \quad f \mapsto \mathrm{Mat}_{\mathcal{B}_{E/D}}(f).$$

L'application $p_{|\,\mathrm{GL}(F)} : \mathrm{GL}(F) \to \mathrm{GL}(E/D)$ est la composée $\mathrm{GL}(F) \hookrightarrow \mathrm{GL}_D(E) \to \mathrm{GL}(E/D)$ qui avec les identifications précédentes s'écrit :

$$A \in \mathrm{GL}_{n-1}(k) \longmapsto \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & A \end{array}\right) \in \mathrm{GL}_n(k)_a \longmapsto A \in \mathrm{GL}_{n-1}(k).$$

C'est l'identité de $\mathrm{GL}_{n-1}(k)$, qui est un isomorphisme.

4. En déduire que p est surjectif et qu'on a un isomorphisme $\mathrm{GL}_D(E) \simeq U_D \rtimes \mathrm{GL}(F)$. *Correction : Le résultat de la question précédente montre que chaque automorphisme $w \in \mathrm{GL}(E/D)$ peut se relever dans $\mathrm{GL}_D(E)$ en un élément du sous-groupe $\mathrm{GL}(F)$; en particulier p est surjectif. Pour montrer que $\mathrm{GL}_D(E)$ est produit semi-direct de ses sous-groupes U_D et $\mathrm{GL}(F)$ il y a deux choses à vérifier :*

(i) $U_D \cap \mathrm{GL}(F) = \{1\}$: or on a $U_D \cap \mathrm{GL}(F) = \ker(p) \cap \mathrm{GL}(F) = \ker(p_{|\,\mathrm{GL}(F)})$ qui est égal à $\{1\}$ puisque $p_{|\,\mathrm{GL}(F)}$ est injectif, d'après la question précédente.

(ii) $U_D \cdot \mathrm{GL}(F) = \mathrm{GL}_D(E)$: soit $u \in \mathrm{GL}_D(E)$, notons $\bar{u} = p(u) \in \mathrm{GL}(E/D)$ son image par p. Puisque p est surjectif, il existe $v \in \mathrm{GL}(F)$ tel que $p(v) = p(u)$. Ceci implique que $p(uv^{-1}) = 1$, c'est-à-dire que $w := uv^{-1}$ appartient à $\ker(p) = U_D$. On peut donc écrire $u = wv$ avec $W \in U_D$ et $v \in \mathrm{GL}(F)$, ce qui est le résultat recherché.

En conclusion $\mathrm{GL}_D(E)$ est produit semi-direct du sous-groupe distingué U_D par $\mathrm{GL}(F)$.

Exercice 5 (Nombre de drapeaux complets sur un corps fini)

Soient k un corps fini à q éléments et E un k-espace vectoriel de dimension finie n. On note $\mathcal{F}(E)$ l'ensemble des drapeaux complets $F_0 = \{0\} \subsetneq F_1 \subsetneq \cdots \subsetneq F_n = E$.

1. Combien y a-t-il de vecteurs non nuls dans E ? Combien y a-t-il de droites vectorielles dans E ? En utilisant une partition $\mathcal{F}(E) = \amalg_D \mathcal{F}_D(E)$ où $\mathcal{F}_D(E)$ est l'ensemble des drapeaux complets dont le premier espace F_1 est égal à une droite D fixée, déduisez-en le cardinal de $\mathcal{F}(E)$. *Correction : Il y a $q^n - 1$ vecteurs non nuls dans E. Chaque droite vectorielle contient exactement $q - 1$ vecteurs non nuls (c'est le cas $n = 1$), et un vecteur non nul v est sur une unique droite (kv) donc il y a $\frac{q^n-1}{q-1} = q^{n-1} + \cdots + q + 1$ droites vectorielles. Si d_n est le nombre de drapeaux complets pour $\dim E = n$, on en déduit que $d_n = (q^{n-1} + \cdots + q + 1)d_{n-1}$ et donc :*

$$d_n = d_1 \prod_{i=1}^{n-1} (q^i + \cdots + q + 1),$$

et on conclut puisque $d_1 = 1$.
Il faut quand même justifier proprement que $d_n = \#\mathcal{F}_D(E)$. Pour cela, soit D une droite vectorielle et S un supplémentaire. On a un isomorphisme de k-espaces vectoriels $S \simeq k^{n-1}$ donc $\mathcal{F}(S) \simeq \mathcal{F}(k^{n-1})$ (simplement en appliquant l'isomorphisme à chaque élément du drapeau). On va maintenant montrer que $\mathcal{F}_D \simeq \mathcal{F}(S)$. Si $\pi : E \to S$ est la projection sur S parallèlement à D, on va montrer que l'application $\Pi : (F_i)_{0 \leqslant i \leqslant n} \mapsto \big(\pi(F_i)\big)_{1 \leqslant i \leqslant n}$ induite par π est une bijection $\mathcal{F}_D(E) \simeq \mathcal{F}(S)$ comme recherchée.

- *L'application Π est bien définie puisque si $(F_i)_{0 \leqslant i \leqslant n} \in \mathcal{F}_D(E)$ alors pour tout $i \geqslant 1$ on a :*

$$\begin{aligned} \dim \pi(F_i) &= \dim F_i - \dim \ker \pi|_{F_i} \\ &= \dim F_i - \dim F_i \cap D \\ &= \dim F_i - \dim D \\ &= \dim F_i - 1, \end{aligned}$$

donc on obtient bien un élément de $\mathcal{F}(S)$.

- *L'application* Π *est bien surjective, puisque si* $(G_i)_{0\leqslant i\leqslant n-1} \in \mathcal{F}(S)$ *alors avec* $F_0^G \coloneqq \{0\}$ *et* $F_i^G \coloneqq D \oplus G_{i-1}$ *pour* $1 \leqslant i \leqslant n$ *on définit bien un élément de* $\mathcal{F}_D(E)$ *(noter que* $G_{i-1} \cap D = \{0\}$ *puisque* $G_{i-1} \subseteq S$*).*
- *L'application* Π *est injective. On va montrer que si* $\Pi(F) = G$ *alors nécessairement* $F = F^G$*. Pour* $i \geqslant 2$ *on a* $\pi(F_i) = G_{i-1}$*, donc pour* $x \in F_i$ *il existe* $y \in G_{i-1}$ *tel que* $y = \pi(x)$*. Puisque* $G_{i-1} \subseteq S$ *on a* $\pi(y) = y$ *donc* $\pi(x) = \pi(x)$ *donc* $\pi(x-y) = 0$ *donc* $x - y \in D$ *donc* $x \in D + y \subseteq D + G_{i-1} = F_i^D$*. On a donc* $F_i \subseteq F_i^D$ *et on conclut par égalité des dimensions.*

Pour montrer que $\mathcal{F}_D(E)$ *et* $\mathcal{F}(k^{n-1})$ *sont en bijection, on peut aussi utiliser l'espace vectoriel quotient* E/D*. En effet, le théorème de correspondance des sous-groupes se précise ici en :*

$$\{\textit{sous-}k\textit{-espaces vectoriels de } E \textit{ qui contiennent } D\} \overset{1:1}{\longleftrightarrow} \{\textit{sous-}k\textit{-espaces vectoriels de } E/D\},$$

une bijection et son inverse, toutes les deux croissantes, étant donnés par $F \mapsto \pi(F)$ *et* $\pi^{-1}(G) \hookleftarrow G$*, où* $\pi : E \to E/D$ *est la surjection canonique. On en déduit alors que l'application* $(F_i)_{0\leqslant i\leqslant n} \in \mathcal{F}(E) \mapsto \big(\pi(F_i)\big)_{1\leqslant i\leqslant n} \in \mathcal{F}(E/D)$ *est une correspondance comme recherchée, l'inverse d'un drapeau* $(G_i)_{0\leqslant i<n} \in \mathcal{F}(E/D)$ *étant donné par* $(F_i^G)_{0\leqslant i\leqslant n} \in \mathcal{F}_D(E)$ *avec* $F_0^G \coloneqq \{0\}$ *et* $F_i^G \coloneqq \pi^{-1}(G_{i-1})$ *pour* $i \in \{1, \dots, n\}$*.*

2. Quel est le cardinal de $\mathrm{GL}(E)$? En faisant agir $\mathrm{GL}(E)$ transitivement sur $\mathcal{F}(E)$, déduisez-en d'autre manière le cardinal de $\mathcal{F}(E)$. *Correction : Le groupe* $\mathrm{GL}(E)$ *est de cardinal* $q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - 1)$ *(cf. Exercice 3). Puisqu'un drapeau est déterminé par une base (la famille* (e_i) *est une base associée au drapeau* (F_i) *où* $F_i = F_{i-1} \oplus ke_i$*) et que l'action de* $\mathrm{GL}(E)$ *sur les bases est transitive, on en déduit par la formule orbite-stabilisateur que le cardinal de* $\mathcal{F}(E)$ *est donné par celui de* $\mathrm{GL}(E)$ *divisé par le cardinal d'un stabilisateur. Mais le stabilisateur d'un drapeau est isomorphe au groupe des matrices triangulaires supérieures inversibles, qui est de cardinal* $(q-1)^n q^{\frac{n(n-1)}{2}}$*. On trouve alors que le cardinal de* $\mathcal{F}(E)$ *est :*

$$\frac{q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q^i - 1)}{q^{\frac{n(n-1)}{2}} \prod_{i=1}^n (q-1)} = \prod_{i=2}^n (q^{i-1} + \cdots + q + 1),$$

qui est bien la formule trouvée précédemment.

Exercice 6 (Décompte des automorphismes diagonalisables)

On note E un espace vectoriel de dimension n sur un corps fini à q éléments.

1. Montrez que $f \in \mathrm{GL}(E)$ est diagonalisable si et seulement si $f^{q-1} = \mathrm{Id}$. *Correction : Si* f *est diagonalisable alors* π_f *divise* $\prod_{\lambda\in\mathbb{F}_q^\times}(X-\lambda) = \frac{X^q-1}{X-1} = X^{q-1} - 1$ *(la valeur propre* 0 *est absente puisque* f *est inversible). Réciproquement, si* $f^{q-1} = \mathrm{Id}$ *alors* f *est annulé par un polynôme scindé à racines simples (les éléments de* $\mathbb{F}_q^\times$*) donc* f *est diagonalisable.*

On fixe un générateur ζ du groupe multiplicatif (cyclique) $\mathbb{F}_q^\times$.

2. On pose $E_i = \ker(f - \zeta^i)$, pour $f \in \mathrm{GL}(E)$ et $i = 1, \dots, q-1$. Montrez que l'application $f \mapsto (E_1, \dots, E_{q-1})$ établit une bijection entre l'ensemble des automorphismes diagonalisables de $\mathrm{GL}(E)$ et l'ensemble des décompositions de E en somme directe de $q-1$ sous-espaces. *Correction : L'automorphisme* f *est diagonalisable ssi* $E = \oplus_{i=1}^{q-1} E_i$*, donc on a bien une décomposition en somme directe de* $q-1$ *sous-espaces (certains étant possiblement nuls). Réciproquement, étant donné une décomposition* $E = \oplus_{i=1}^{q-1} F_i$*, l'automorphisme* $f \in \mathrm{GL}(E)$ *défini par* $f_{|F_i} = \zeta^i \mathrm{Id}_{F_i}$ *vérifie* $E_i = F_i$ *et* f *est bien diagonalisable (et inversible). C'est de plus l'unique automorphisme possible car si* f' *vérifie* $\ker(f' - \zeta^i) = E_i$ *alors* $f' = f = \zeta^i \mathrm{Id}_{F_i}$*.*

3. On fixe un $(q-1)$-uplet d'entiers $\nu = (n_1, \dots, n_{q-1})$ tel que $\sum n_i = n$. On note X_ν l'ensemble des décompositions de E en somme directe de $q-1$ sous-espaces E_i tels que $\dim(E_i) = n_i$. Montrez que l'action de $\mathrm{GL}(E)$ sur X_ν définie par $g \cdot (E_1, \dots, E_{q-1}) \coloneqq (g(E_1), \dots, g(E_{q-1}))$ est transitive et décrivez le stabilisateur d'un point. *Correction : Tout d'abord l'action est bien définie puisque* $g \in \mathrm{GL}(E)$ *ne change pas la dimension. Un tel* g *existe puisqu'il suffit de le définir sur des bases. Si maintenant* $g(E_i) = E_i$ *pour tout* i *alors* g *induit un élément de* $\mathrm{GL}(E_i)$*, réciproquement si on se donne des éléments de* $\mathrm{GL}(E_i)$ *alors on les recolle en un élément de* $\mathrm{GL}(E)$ *qui stabilise* $(E_1, \dots, E_{q-1})$*, ainsi le stabilisateur est isomorphe à* $\prod_i \mathrm{GL}(E_i) \simeq \prod_i \mathrm{GL}_{n_i}(q)$*.*

4. Déduisez-en que le nombre d'automorphismes diagonalisables de $\mathrm{GL}(E) \simeq \mathrm{GL}_n(\mathbb{F}_q)$ est égal à :

$$\sum_{\substack{(n_1,\dots,n_{q-1}) \\ \text{t.q. } n_1+\cdots+n_{q-1}=n}} \frac{|\mathrm{GL}_n(\mathbb{F}_q)|}{|\mathrm{GL}_{n_1}(\mathbb{F}_q)| \dots |\mathrm{GL}_{n_{q-1}}(\mathbb{F}_q)|}.$$

Correction : On applique la relation orbite-stablisateur.

Exercice 7 (Stabilisateur versus fixateur)

Lorsqu'un groupe G agit sur un ensemble X, on appelle

- *stabilisateur* d'une partie $Y \subset X$ le sous-groupe $\mathrm{Stab}(Y)$ composé des $g \in G$ tels que $g(Y) = Y$,

- *fixateur* de Y le sous-groupe $\mathrm{Fix}(Y) \subset \mathrm{Stab}(Y)$ composé des $g \in G$ tels que $g_{|Y} = \mathrm{Id}_Y$.

Soient k un corps, E un k-espace vectoriel de dimension finie, $G = \mathrm{GL}(E)$ le groupe linéaire de E, et $D \subset E$ une droite vectorielle. Démontrez qu'on a un isomorphisme $\mathrm{Stab}(D) \simeq \mathrm{Fix}(D) \rtimes k^\times$. *Correction : Soit H le sous-groupe de* $\mathrm{Stab}(D)$ *formé des homothéties (inversibles) de E. On a $H \simeq k^\times$ et on va montrer que* $\mathrm{Stab}(D) \simeq \mathrm{Fix}(D) \rtimes H$.

- *Le sous-groupe* $\mathrm{Fix}(D)$ *est distingué dans* $\mathrm{Stab}(D)$ *car si $y \in \mathrm{Fix}(D)$ et $x \in \mathrm{Stab}(D)$ alors pour tout $d \in D$ on a :*

$$\begin{aligned} x^{-1}yx(d) &= x^{-1}y\big(x(d)\big) \\ &= x^{-1}\big(x(d)\big) \text{ puisque } x(d) \in D \\ &= d, \end{aligned}$$

  donc $x^{-1}xy \in \mathrm{Fix}(D)$.
- *Si $y \in \mathrm{Fix}(D) \cap H$ alors y est une homothétie de E qui possède un point fixe non nul (puisque D est une droite) donc $y = \mathrm{Id}_E$. Ainsi, on a bien* $\mathrm{Fix}(D) \cap H = \{1_G\}$.
- *On va montrer que* $\mathrm{Stab}(D) = H\ \mathrm{Fix}(D)$. *Soit v un vecteur non nul de D. Pour $x \in \mathrm{Stab}(D)$, puisque $x \in \mathrm{GL}(E)$ on a $x(v) \in D \setminus \{0\}$ donc il existe $\lambda \neq 0$ tel que $x(v) = \lambda v$. Ainsi, puisque $D = kv$ on en déduit que $x|_D = \lambda \mathrm{Id}_D$ donc avec $h \coloneqq \lambda \mathrm{Id}_E \in H$ on en déduit que $y \coloneqq h^{-1}x \in \mathrm{Fix}(Y)$ et donc $x = hy \in H\ \mathrm{Fix}(D)$.*

On a donc montré que $\mathrm{Stab}(D) \simeq \mathrm{Fix}(D) \rtimes H$ *comme voulu.*

Le groupe (projectif) (spécial) linéaire

Exercice 8 (PSL et PGL)

On note $e_n : k^\times \to k^\times$ l'application donnée par $e_n(x) = x^n$, ainsi que $\mu_n(k)$ son noyau et $k^{\times n}$ son image. On note Z le centre de $\mathrm{GL}_n(k)$. On rappelle que $\mu_n(\mathbb{F}_q)$ est un groupe cyclique d'ordre $n \wedge (q-1)$.

1. Rappeler pourquoi le noyau du morphisme canonique $\varphi : \mathrm{SL}_n(k) \to \mathrm{PGL}_n(k)$ est $\mu_n(k)$. *Correction : Une matrice M est dans* $\ker\varphi$ *ssi c'est une matrice scalaire. On conclut puisque les matrices scalaires de* $\mathrm{SL}_n(k)$ *sont les $\mu_n(k)I_n$. En particulier, on obtient une injection $\bar\varphi : \mathrm{PSL}_n(k) \hookrightarrow \mathrm{PGL}_n(k)$.*
2. Montrer que le morphisme $\det : \mathrm{GL}_n(k) \to k^\times$ induit un morphisme surjectif $\det : \mathrm{PGL}_n(k) \to k^\times/k^{\times n}$ de noyau $\mathrm{PSL}_n(k)$. *Correction : (Faire un dessin.) On a un morphisme surjectif $f : \mathrm{GL}_n(k) \twoheadrightarrow k^\times/k^{\times n}$ par composition de morphismes surjectifs. On a $M \in \ker f \iff \det(M)$ est une puissance n-ième (d'un élément de k). Les matrices scalaires étant des exemples de telles matrices, on en déduit que f passe au quotient et on trouve donc un morphisme surjectif $g : \mathrm{PGL}_n(k) \to k^\times/k^{\times n}$. Si $M \in \mathrm{GL}_n(k)$ est telle que $g(\pi_{\mathrm{PGL}}M) = 1$ alors $\lambda \coloneqq \det M$ est une puissance n-ième, d'un élément μ. Ainsi la matrice $N \coloneqq \mu^{-1}M$ est dans $\mathrm{SL}_n(k)$ et vérifie $\pi_{\mathrm{PGL}}N = \pi_{\mathrm{PGL}}M$. On a donc bien montré que $M \in \mathrm{im}\,\bar\varphi$, autrement dit $\ker g \subseteq \mathrm{PSL}_n(k)$. L'inclusion réciproque est immédiate puisque si $N \in \mathrm{SL}_n(k)$ alors $g(\varphi(N)) = g(\pi_{\mathrm{PGL}}N) = \det N = 1$.*
3. Montrer que le morphisme canonique $\mathrm{SL}_n(k) \to \mathrm{PGL}_n(k)$ est un isomorphisme si et seulement si e_n est un isomorphisme. *Correction : Par la question 1, on sait déjà que $\varphi : \mathrm{SL}_n(k) \to \mathrm{PGL}_n(k)$ est injective ssi e_n l'est (puisque $\mu_n(k) = \ker e_n$). On suppose maintenant e_n surjective et soit $\pi_{\mathrm{PGL}}M \in \mathrm{PGL}_n(k)$. Par hypothèse on peut trouver $\lambda \in k^\times$ tel que $\det M = \lambda^n$, ainsi $N \coloneqq \lambda^{-1}M \in \mathrm{SL}_n(k)$ vérifie $\pi_{\mathrm{PGL}}N = \pi_{\mathrm{PGL}}M$ donc φ est surjective. Réciproquement, supposons φ surjective soit $\mu \in k^\times$. Par hypothèse il existe une matrice $N \in \mathrm{SL}_n(k)$ telle que $\varphi(N) = \pi_{\mathrm{PGL}}\mathrm{diag}(\mu, 1, \dots, 1)$. Ainsi N et $\mathrm{diag}(\mu, 1, \dots, 1)$ sont dans la même classe dans $\mathrm{GL}_n(k)$ modulo Z donc $\mu/\det(N)$ est une puissance n-ième, donc on conclut puisque $\det N = 1$.*
4. Pour $k = \mathbb{R}, \mathbb{C}, \mathbb{F}_q, \mathbb{Q}$, $n \geqslant 2$ discuter l'assertion $e_n : k^\times \to k^\times$ est un isomorphisme. *Correction : Sur $\mathbb{R}$ elle est surjective ssi n est impair ssi elle est injective. Sur $\mathbb{C}$ elle est toujours surjective et jamais injective. Sur $\mathbb{F}_q$ elle est injective ssi elle est surjective ssi $q-1 \mid n$ (puisque $|\mu_n(\mathbb{F}_q)| = n \wedge q - 1$). Sur $\mathbb{Q}$ elle n'est jamais surjective, mais injective ssi n impair.*

Exercice 9 (PSL et PGL, suite)

À l'aide de l'exercice 8, montrer que :

1. Si k est algébriquement clos alors l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est un isomorphisme. *Correction : Par l'exo 8.1 on sait que c'est bien une inclusion. Par la question 3 de ce même exercice on sait qu'elle est surjective car e_n l'est.*
2. Si $k = \mathbb{R}$ et n est impair alors l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est un isomorphisme. *Correction : Même argument.*
3. Si $k = \mathbb{R}$ et n est pair alors l'image de l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est d'indice 2. *Correction : D'après l'exo 8.2 et le premier théorème d'isomorphisme, le déterminant induit un isomorphisme* $\mathrm{PGL}_n(k)/\mathrm{PSL}_n(k) \simeq k^\times/k^{\times n}$. *Ainsi sous nos hypothèses on a* $\big|\mathrm{PGL}_n(k)/\mathrm{PSL}_n(k)\big| = 2$ *puisque* $\big|\mathbb{R}^*/\mathbb{R}_+^*\big| = 2$ *(car $\mathbb{R}^* = \mathbb{R}_+^* \sqcup (-1)\mathbb{R}_+^*$).*

4. Si k est un corps fini alors l'image de l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est d'indice $n \wedge (q-1)$. En particulier, d'indice 2 si $n = 2$ et k de caractéristique différente de 2. *Correction : Par le même argument, il suffit de voir que* $\left|\mathbb{F}_q^\times / \mathbb{F}_q^{\times n}\right| = n \wedge (q-1)$ *(où* $k = \mathbb{F}_q$*). Cette égalité est bien vérifiée car le morphisme* $\mathbb{F}_q^\times \to \mathbb{F}_q^{\times n}$ *donné par la puissance* n *est de noyau* $\mu_n(\mathbb{F}_q)$ *et on conclut en prenant les cardinaux. La dernière assertion s'en déduit car si* q *n'est pas une puissance de* 2 *alors* q *est impair et donc* $2 \mid (q-1)$*.*

Exercice 10 (GL_n n'est pas souvent un produit direct de SL_n)

On rappelle que $\mathrm{SL}_n(k)$ *possède un complément dans* $\mathrm{GL}_n(k)$*, c'est-à-dire un sous-groupe* $H' \subset \mathrm{GL}_n(k)$ *tel que :*

$$H' \cap \mathrm{SL}_n(k) = 1 \quad \textit{et} \quad H' \,\mathrm{SL}_n(k) = \mathrm{GL}_n(k)$$

ou de façon équivalente : $\mathrm{GL}_n(k) = \mathrm{SL}_n(k) \rtimes H'$*. On cherche une condition nécessaire et suffisante sur* (n, k) *pour qu'il existe un complément tel que ce produit est en fait* direct*.*

On suppose qu'il existe un sous-groupe $H \subset \mathrm{GL}_n(k)$ tel que $\mathrm{GL}_n(k) = \mathrm{SL}_n(k) \times H$, ou de façon équivalente :

$$H \cap \mathrm{SL}_n(k) = 1, \quad H \,\mathrm{SL}_n(k) = \mathrm{GL}_n(k), \quad [H, \mathrm{SL}_n(k)] = 1.$$

1. Montrer que le déterminant induit un isomorphisme de H sur $k^\times$. *Correction : On a* $\ker(\det|_H) = \ker(\det) \cap H = \mathrm{SL}_n(k) \cap H = 1$ *donc* $\det|_H$ *est injectif. De plus, pour* $\lambda \in k^\times$ *il existe* $h \in H$ *et* $s \in \mathrm{SL}_n(k)$ *tel que* $hs = \mathrm{diag}(\lambda, 1, \dots, 1)$ *donc* $\det h = \lambda$ *donc* $\det|_H$ *est surjectif.*

2. Montrer que $H \subset Z \coloneqq Z\big(\mathrm{GL}_n(k)\big)$. *Correction : On sait déjà que* H *commute avec tous les éléments de* $\mathrm{SL}_n(k)$*. Puisque* $H\,\mathrm{SL}_n(k) = \mathrm{GL}_n(k)$*, pour montrer que* $H \subseteq Z$ *il suffit de montrer que* H *est commutatif. Mais c'est clair par la question précédente puisque* $H \simeq k^\times$*.*

3. Montrer que Z est un complément de $\mathrm{SL}_n(k)$ si et seulement si l'application déterminant de Z vers $k^\times$ est un isomorphisme. *Correction : La première question montre le sens direct. Réciproquement, on suppose que* $\det|_Z : Z \to k^\times$ *est un isomorphisme. Pour montrer que* Z *est un complément de* $\mathrm{SL}_n(k)$*, il suffit de montrer que* $Z\,\mathrm{SL}_n(k) = \mathrm{GL}_n(k)$*. Si* $M \in \mathrm{GL}_n(k)$*, alors il existe* $z \in Z$ *tel que* $\det M = \det z$ *donc il existe* $s \in \mathrm{SL}_n(k)$ *tel que* $s = z^{-1}M$ *donc* $M = zs \in Z\,\mathrm{SL}_n(k)$*.*

4. En déduire une condition nécessaire et suffisante sur k et n pour qu'il existe un tel H. *Correction : On va montrer que nécessairement* $H = Z$*, donc une CNS est que l'élévation* $e_n : k^\times \to k^{\times n}$ *à la puissance* n *est un isomorphisme (notation de l'Exercice 8 ; cf. question 4 de ce même exercice pour diverses CNS). On sait déjà par la question 2 que* $H \subseteq Z$*. Ainsi, pour chaque* $h \in H$ *il existe* $\lambda_h \in k^\times$ *tel que* $h = \lambda_h I_n$*. Mais clairement la partie* $\Lambda \coloneqq \{\lambda_h : h \in H\}$ *est un sous-groupe de* $k^\times$*, et l'isomorphisme* $\det|_H \to k^\times$ *est donné par l'élévation à la puissance* n *de* Λ *dans* $k^\times$*. En particulier, on a* $\Lambda^n = k^\times$ *donc puisque* Λ *est un sous-groupe on en déduit que* $\Lambda \subseteq \Lambda^n = k^\times$*. Finalement, par double inclusion on a donc* $\Lambda = k^\times$ *donc* $H = Z$*.*

Exercice 11 (Groupe affine d'un espace vectoriel)

Soit E un espace vectoriel sur un corps k. On appelle *groupe affine de* E noté $\mathrm{GA}(E)$ l'ensemble des bijections $f : G \to G$ de la forme $f(x) = a(x) + b$ avec $a \in \mathrm{GL}(E)$ et $b \in E$.

1. Dans $\mathrm{GA}(E)$, décrivez le produit et l'inverse. *Correction : Si* $f(x) = a(x) + b$ *et* $g(x) = c(x) + d$ *alors*

$$fg(x) = f\big(c(x) + d\big) = a\big(c(x) + d\big) + b = ac(x) + b + a(d).$$

L'inverse de f *est donc* $x \mapsto a^{-1}(x) - a^{-1}(b)$*.*

2. Montrez que $\mathrm{GA}(E)$ est produit semi-direct du sous-groupe distingué T des translations ($a = \mathrm{Id}$) et du sous-groupe L des applications linéaires ($b = 0$). Quel est le morphisme d'action de L sur T ? *Correction : Immédiat par la question précédente (on voit bien la structure multiplicative apparaître) : on a* $\mathrm{GA}(E) \simeq T \rtimes L$ *; on peut aussi vérifier les conditions* $T \cap L = \{1\}$ *et* $TL = \mathrm{GA}(E)$*. En particulier, le sous-groupe* T *est bien ditingué car c'est le noyau du morphisme qui à* $f \in \mathrm{GL}(E)$ *associe sa partie linéaire (c'est bien un morphisme par la question précédente). Le sous-groupe* L *agit sur* T *par conjugaison, et avec les identifications* $L \simeq \mathrm{GL}(E)$ *et* $T \simeq E$ *alors l'action correspondante est l'action naturelle de* $\mathrm{GL}(E)$ *sur* E*. En effet, pour* $a \in \mathrm{GL}(E)$ *et* $t_b : x \mapsto x + b$ *on a* $at_ba^{-1}(x) = at_b\big(a^{-1}(x)\big) = a\big(a^{-1}(x) + b\big) = x + a(b) = t_{a(b)}(x)$ *donc* $at_ba^{-1} = t_{a(b)}$*. Ainsi, l'action de* $a \in \mathrm{GL}(E)$ *sur* $b \in E$ *est bien donnée par* $a(b)$ *comme annoncé.*

3. On appelle *homothétie-translation* un morphisme qui est le composé d'une homothétie et d'une translation. Montrez que les homothéties-translations forment un sous-groupe. *Correction : L'ensemble* H *des homothéties est bien un sous-groupe de* $\mathrm{GA}(E)$*. On a vu dans la question précédente que le sous-groupe* T *des translations est distingué dans* $\mathrm{GA}(E)$*, ainsi d'après le TD précédent l'ensemble* HT*, qui n'est rien d'autre que l'ensemble des homothéties-translations, est un sous-groupe de* $\mathrm{GA}(E)$ *(en particulier* $HT = TH$*). On peut remarquer qu'une homothétie* h *de centre* $x_0 \in E$ *et de rapport* $\lambda \in k^\times$ *est donnée par* $h(x) - x_0 = \lambda(x - x_0)$ *donc* $h(x) = \lambda x + (1 - \lambda)x_0$*, donc en composant avec les translations on obtient simplement les éléments de* $\mathrm{GA}(E)$ *dont la partie linéaire est une homothétie.*

Transvections

Dans les exercices qui suivent, E est un espace vectoriel de dimension finie sur un corps k. De plus, pour toute forme non nulle $f \in E^*$ et tout vecteur non nul $a \in \ker(f)$ on note $u_{a,f}$ la transvection définie par $u(x) = x + f(x)a$.

Exercice 12 (Connexité par arcs de SL)

Lorsque $k = \mathbb{R}$ ou $\mathbb{C}$, déduisez du fait que $\mathrm{SL}(E)$ est engendré par les transvections qu'il est connexe par arcs. *Correction : Il suffit de montrer que tout élément de* $\mathrm{SL}(E)$ *est relié à l'identité par un chemin continu. Soit* $u \in \mathrm{SL}(E)$*. On peut écrire* $u = \prod_{i=1}^n u_{a_i,f_i}$ *où* f_i *est une forme linéaire et* $a_i \in \ker f_i$*. Le chemin*

$$\begin{array}{ccc} [0,1] & \longrightarrow & \mathrm{SL}(E) \\ t & \longmapsto & \prod_{i=1}^n u_{(1-t)a_i,f_i} \end{array}$$

est bien continu, vaut u *en* $t = 0$ *et* Id_E *en* $t = 1$ *(puisque* $u_{0,f_i} = \mathrm{Id}_E$*). C'est gagné.*

Exercice 13 (Décompte des transvections)

On considère un espace vectoriel de dimension finie E sur un corps fini k de cardinal q.

1. Pour tout choix d'un vecteur $a \neq 0$ et d'une forme linéaire $f \neq 0$ tels que $f(a) = 0$, on note $u_{a,f}$ la transvection définie par $u(x) = x + f(x)a$. Montrez que $u_{a,f} = u_{a',f'}$ si et seulement s'il existe $\lambda \in k^\times$ tel que $f' = \lambda f$ et $a' = \lambda^{-1}a$. *Correction : On a pour tout* $x \in E$*,* $x + f(x)a = x + f'(x)a'$ *donc* $f(x)a = f'(x)a'$*. Puisque* $a, a' \neq 0$ *on a donc* $\ker f = \ker f'$*, donc* f *et* f' *(qui sont des formes linéaires) sont proportionnelles : il existe* $\lambda \in k^\times$ *tel que* $f' = \lambda f$*. En réinjectant dans l'égalité précédente on trouve* $f(x)a = \lambda f(x)a'$*, et en prenant* $x \notin \ker f$ *on trouve* $a = \lambda a'$ *comme voulu.*

2. On note $H = \ker(f)$ et on fixe un vecteur $b \notin H$. Démontrez que le commutant de $u_{a,f}$ dans $\mathrm{GL}(E)$ est l'ensemble des $g \in \mathrm{GL}(E)$ de la forme $g = \lambda v$ avec $\lambda \in k^\times$ et $v \in \mathrm{GL}(E)$ vérifiant $v(a) = a$, $v(H) = H$, $v(b) \in b + H$. La matrice de v dans une base obtenue en complétant une base de H avec b est donc de la forme :

$$\left(\begin{array}{c|ccc|c} 1 & * & \cdots & * & * \\ \hline 0 & & & & * \\ \vdots & & * & & \vdots \\ 0 & & & & * \\ \hline 0 & 0 & \cdots & 0 & 1 \end{array}\right)$$

Correction : Soit $g \in \mathrm{GL}(E)$ *qui commute avec* $u_{a,f}$*. Pour tout* $x \in E$ *on a* $g\big(u_{a,f}(x)\big) = g\big(x + f(x)a\big) = g(x) + f(x)g(a)$ *et* $u_{a,f}\big(g(x)\big) = g(x) + f\big(g(x)\big)a$ *donc en en déduit que*

$$f(x)g(a) = f\big(g(x)\big)a.$$

Ainsi, si $x \in \ker f$ *alors* $g(x) \in \ker f$ *donc* H *est stable par* g*. Puisque* g *est inversible on a en fait* $g(H) = H$*. De plus, en prenant* $x = b$ *on trouve que* $g(a) = \lambda a$ *pour un* $\lambda \in k^\times$ *et donc* $f(b)\lambda a = f\big(g(b)\big)a$ *donc* $f\big(g(b)\big) = \lambda f(b)$ *donc* $g(b) - \lambda b \in \ker f$*. Ainsi, la matrice de* g *dans une base adaptée à* $E = H \oplus \langle b \rangle$ *est de la forme* $\lambda\times$ *la forme annoncée. Réciproquement, soit* $v \in \mathrm{GL}(E)$ *vérifiant* $v(a) = a, v(H) = H$ *et* $v(b) \in b + H$*. Vérifions que* $vu_{a,f} = u_{a,f}v$*. Pour* $x \in H$ *on a,*

$$v\big(u_{a,f}(x)\big) = v\big(x + f(x)a\big) = v(x) + f(x)v(a) = v(x),$$

puisque $x \in H = \ker f$*, et*

$$u_{a,f}\big(v(x)\big) = v(x) + f\big(v(x)\big)a = v(x),$$

puisque $v(x) \in H = \ker f$*, donc on a bien* $vu_{a,f} = u_{a,f}v$ *sur* H*. De plus, on a*

$$v\big(u_{a,f}(b)\big) = v(b) + f(b)v(a) = v(x) + f(b)a,$$

et

$$u_{a,f}\big(v(b)\big) = v(b) + f\big(v(b)\big)a = v(b) + f(b)a,$$

en effet $v(b) - b \in H$ *donc* $f\big(v(b)\big) = f(b)$*. On conclut que* $vu_{a,f} = u_{a,f}v$ *sur une base et donc ces deux automorphismes sont égaux.*

3. Calculez le cardinal de ce commutant et déduisez-en que le nombre de transvections dans $\mathrm{GL}(E)$ vaut :

$$\frac{(q^n - 1)(q^{n-1} - 1)}{q - 1}.$$

Correction : On rappelle la formule suivante :

$$\big|\mathrm{GL}_n(q)\big| = q^{n(n-1)/2} \prod_{i=1}^n (q^i - 1).$$

Le groupe $\mathrm{GL}(E)$ *agit sur l'ensemble des transvections par conjugaison. On sait que cette action est transitive puisque toutes les transvections ont une même matrice dans une certaine base. Le stabilisateur d'une transvection est exactement son commutant, et d'après la question précédente son cardinal est, où* $n = \dim_k E$ *(le* $q-1$ *correspond au* $\lambda \in k^\times$*)*

$$\begin{aligned}(q-1)\big|\mathrm{GL}_{n-2}(q)\big| \times q^{2(n-2)+1} &= (q-1)q^{(n-2)(n-3)/2}(q-1)\prod_{i=1}^{n-2}(q^i-1)\times q^{2n-3}\\ &= (q-1)q^{(n^2-5n+6)/2+2n-3}\prod_{i=1}^{n-2}(q^i-1)\\ &= (q-1)q^{(n^2-n)/2}\prod_{i=1}^{n-2}(q^i-1).\end{aligned}$$

Par la relation orbite-stabilisateur on en déduit donc que le nombre de transvections dans $\mathrm{GL}(E)$ *vaut le cardinal de* $\mathrm{GL}_n(q)$ *divisé par l'entier précédent, on trouve donc directement l'entier voulu.*

Exercice 14 (Transvections d'hyperplan fixé)

Soit H un hyperplan de E. On note $\mathrm{T}(H)$ la réunion de l'ensemble des transvections d'hyperplan H et de l'identité.

1. Démontrez que $\mathrm{T}(H) = \{u \in \mathrm{SL}(E); u_{|H} = \mathrm{Id}_H\}$ et que c'est un sous-groupe de $\mathrm{SL}(E)$. Donnez une représentation matricielle de $\mathrm{T}(H)$ dans une base bien choisie. *Correction : On a bien l'inclusion* $\subseteq$*. Si maintenant* $u \in \mathrm{SL}(E)\setminus\{\mathrm{Id}\}$ *vérifie* $u_{|H} = \mathrm{Id}_H$ *alors écrivant* $E = H \oplus \langle x\rangle$*, la matrice de* u *dans une base adaptée est de la forme* $\begin{pmatrix}\alpha & 0 & \dots & 0\\ * & & & \\ \vdots & & & \\ \vdots & & \mathrm{Id} & \\ * & & & \end{pmatrix}$ *donc* $\alpha = 1$ *puisque* $\det u = 1$*. On en déduit que* $u(x) - x \in H$*, puisque* $u \neq \mathrm{Id}$ *on a que* $\mathrm{im}(u-\mathrm{Id})$ *est une droite incluse dans* $\ker(u-\mathrm{Id}) = H$ *donc* $u \in \mathrm{T}(H)$*. Les éléments de* $\mathrm{T}(H)$ *sont tous, dans une base de* $E = H \oplus \langle x\rangle$ *fixée, de la forme précédente avec* $\alpha = 1$*, c'est-à-dire* $\begin{pmatrix}1 & 0 & \dots & \dots & 0\\ * & 1 & \ddots & & \vdots\\ \vdots & 0 & \ddots & \ddots & \vdots\\ \vdots & \vdots & \ddots & \ddots & 0\\ * & 0 & \dots & 0 & 1\end{pmatrix}$*. Finalement, on déduit de l'égalité ensembliste que* $\mathrm{T}(E)$ *est bien un sous-groupe de* $\mathrm{SL}(E)$*.*

2. Démontrez que pour toute forme linéaire f_0 de noyau H, l'application $a \mapsto u_{a,f_0}$ induit un isomorphisme de groupes $H \xrightarrow{\sim} \mathrm{T}(H)$. *Correction : Soit* $\phi : H \to \mathrm{T}(H)$ *l'application de l'énoncé. Soit* $f_0 \in E^*$ *de noyau* H *et* $a \in H$*. L'application* ϕ *est bien à valeurs dans* $\mathrm{T}(H)$ *puisque pour tout* $h \in H$ *on a* $u_{a,f_0}(h) = h + f_0(h)a = h$ *donc* $u_{a,f_0|H} = \mathrm{Id}_H$*, et on utilise la question 1.*

Montrons maintenant que ϕ *est bien un morphisme de groupes. Pour tout* $x \in E$ *on a, en utilisant le fait que* $H = \ker f_0$*,*

$$\begin{aligned}u_{a,f_0}u_{a',f_0}(x) &= u_{a,f_0}\big(x + f_0(x)a'\big)\\ &= x + f_0(x)a' + f_0\big(x + f_0(x)a'\big)(a)\\ &= x + f_0(x)a' + f_0(x)a + f_0(x)f_0(a')a\\ &= x + f_0(x)a' + f_0(x)a\\ &= x + f_0(x)(a+a')\\ &= u_{a+a',f_0}(x),\end{aligned}$$

ainsi on a bien $u_{a,f_0}u_{a',f_0} = u_{a+a',f_0}$*, autrement dit* $\phi : H \to \mathrm{T}(H)$ *est un morphisme de groupes.*

Montrons maintenant que ϕ *est surjective. Pour* $u \in \mathrm{T}(H)$*, par définition il existe* $a \in H$ *et* $f \in E^*$ *de noyau* H *tels que* $u = u_{a,f}$*. Puisque* $\ker f = \ker f_0 = H$*, on sait que* f *et* f_0 *sont proportionnelles donc si* $f = \lambda f_0$ *on a* $u = u_{a,f} = u_{a,\lambda f_0} = u_{\lambda a,f_0}$ *et c'est gagné.*

Montrons finalement que ϕ *est injective. Soit* $a \in H$ *telle que* $u_{a,f_0} = \mathrm{Id}_E$*. On a donc* $x = x + f(x)a$ *pour tout* $x \in E$ *donc* $f(x)a = 0$ *pour tout* $x \in E$*. En prenant* $x \notin H$ *on trouve* $a = 0$*.*

Finalement, on a montré que $\phi : H \to \mathrm{T}(H)$ *est un isomorphisme de groupes. En particulier, cela montre que* $\mathrm{T}(H)$ *est commutatif.*

Exercice 15 (Transvections de droite fixée)

Soit D une droite de E. On note $\mathrm{U}(D)$ la réunion de l'ensemble des transvections de droite D et de l'identité.

1. Démontrez que $\mathrm{U}(D) = \{u \in \mathrm{SL}(E);\ \mathrm{im}(u - \mathrm{Id}) \subset D\}$ et que c'est un sous-groupe de $\mathrm{SL}(E)$. Donnez une représentation matricielle de $\mathrm{U}(D)$ dans une base bien choisie. *Correction : Appelons V l'ensemble de droite. Si $u \in \mathrm{U}(D)$ alors on a bien $u \in \mathrm{SL}(E)$, de plus si $u = \mathrm{Id}_E$ alors $\mathrm{im}(u - \mathrm{Id}) = \{0\} \subseteq D$ et sinon alors $\mathrm{im}(u - \mathrm{Id}) = D$ donc $u \in V$. Réciproquement, si $u \in V$ alors si $\mathrm{im}(u - \mathrm{Id}) = \{0\}$ alors $u = \mathrm{Id} \in \mathrm{U}(D)$ et sinon on a $\mathrm{im}(u - \mathrm{Id}) = D$. Ainsi, si $a \in D \setminus \{0\}$ alors il existe une forme linéaire f sur E telle que $u(x) = x + f(x)a$ pour tout $x \in E$. On va montrer que $f(a) = 0$, ce qui prouvera que $u \in \mathrm{U}(D)$. Si $f(a) \neq 0$, alors si $\mathcal{B}$ est une base de $\ker f = \ker(u - \mathrm{Id}_E)$ (puisque $a \neq 0$ puisque $f(a) \neq 0$) alors $\mathcal{B} \cup \{a\}$ est une base de E dans laquelle la matrice de u est $\mathrm{diag}\big(1, \dots, 1, 1 + f(a)\big)$, mais donc $1 + f(a) = \det u = 1$ donc $f(a) = 0$ ce qui est absurde.*

L'ensemble $\mathrm{U}(D)$ est bien un sous-groupe, puisque $\mathrm{Id} \in \mathrm{U}(D)$ et si $u, v \in \mathrm{U}(D)$ alors $uv^{-1} \in \mathrm{SL}(E)$ et :

$$\begin{aligned}\mathrm{im}(uv^{-1} - \mathrm{Id}) &= \mathrm{im}\big[(u - \mathrm{Id})v^{-1} + v^{-1} - \mathrm{Id}\big] \\ &\subseteq \mathrm{im}\big[(u - \mathrm{Id})v^{-1}\big] + \mathrm{im}\big[(\mathrm{Id} - v)v^{-1}\big] \\ &\subseteq \mathrm{im}(u - \mathrm{Id}) + \mathrm{im}(\mathrm{Id} - v) \\ &= D,\end{aligned}$$

donc $uv^{-1} \in \mathrm{U}(D)$.

Finalement, en prenant $\mathcal{B}$ une base d'un supplémentaire de D et en la complétant avec un vecteur v non nul de D, on a $u(x) - x \in kv$ donc les éléments de $\mathrm{U}(D)$ dans la base obtenue s'écrivent (le dernier 1 étant vraiment un 1 pour des raisons de déterminant) :

$$\begin{pmatrix} 1 & & & & \\ 0 & \ddots & & & \\ \vdots & \ddots & \ddots & & \\ 0 & \dots & 0 & 1 & \\ \lambda_1 & \dots & \dots & \lambda_{n-1} & 1 \end{pmatrix},$$

avec $n \coloneqq \dim E$ et $\lambda_i \in k$, et réciproquement tout élément u de cette forme dans cette base vérifie bien $u \in \mathrm{SL}(E)$ et $u(x) - x \in kv$ donc $u \in \mathrm{U}(D)$.

2. Démontrez que pour tout vecteur directeur a_0 de D, l'application $f \mapsto u_{a_0,f}$ induit un isomorphisme de groupes $D^\perp \xrightarrow{\sim} \mathrm{U}(D)$, où $D^\perp = \{f \in E^*, f_{|D} = 0\}$ est l'orthogonal de D. *Correction : Tout d'abord, l'application est bien définie puisque $a_0 \in \ker f$. Vérifions que c'est un morphisme : pour tout $x \in E$ on a :*

$$\begin{aligned}u_{a_0,f}u_{a_0,g}(x) &= u_{a_0,g}(x) + f\big(u_{a_0,g}(x)\big)a_0 \\ &= x + g(x)a_0 + f\big(x + g(x)a_0\big)a_0 \\ &= x + g(x)a_0 + f(x)a_0 + g(x)f(a_0)a_0 \\ &= x + g(x)a_0 + f(x)a_0 \text{ puisque } f(a_0) = 0 \\ &= x + (f + g)(x)a_0 \\ &= u_{a_0,f+g}(x).\end{aligned}$$

Pour l'injectivité, si $u_{a_0,f} = \mathrm{Id}$ alors $x = x + f(x)a_0$ pour tout $x \in E$ donc $f(x) = 0$ pour tout $x \in E$ puisque $a_0 \neq 0$ donc $f = 0$. Pour la surjectivité, c'est immédiat par définition d'une transvection de droite D. Finalement, on a bien $D^\perp \simeq \mathrm{U}(D)$, en particulier $\mathrm{U}(D)$ est commutatif.

Exercice 16 (Transvections d'hyperplan et droite fixés)

Soient D une droite et H un hyperplan tels que $D \subset H$. On choisit a_0 et f_0 tels que $D = \mathrm{Vect}(a_0)$ et $H = \ker(f_0)$.

1. Démontrez que l'application $\lambda \mapsto u_{\lambda a_0,f_0}$ induit un isomorphisme de groupes $(k, +) \xrightarrow{\sim} \mathrm{T}(H) \cap \mathrm{U}(D)$. *Correction : Tout d'abord, on sait par les exercices précédents que $\mathrm{T}(H)$ et $\mathrm{U}(H)$ sont des sous-groupes de $\mathrm{SL}(E)$, donc $\mathrm{T}(H) \cap \mathrm{U}(H)$ est*

non nul, engendre D. L'injectivité se déduit de l'injectivité de celle de $H \to \mathrm{T}(H)$ de l'Exercice 14. Pour la surjectivité, pour $u \in \mathrm{T}(H) \cap \mathrm{U}(H)$, toujours par l'Exercice 14 on sait qu'il existe $a \in H$ tel que $u = u_{a,f_0}$. De plus, on sait par l'Exercice 15 qu'il existe $f \in E^*$ avec $f|_D = 0$ tel que $u = u_{a_0,f}$. Ainsi, pour tout $x \in E$ on a :

$$f_0(x)a = f(x)a_0,$$

donc $a \in D$, en particulier il existe $\lambda \in k$ tel que $a = \lambda a_0$. On a donc $u = u_{a,f_0} = u_{\lambda a_0,f_0}$ ce qui conclut.

2. Donnez la représentation matricielle de $\mathrm{T}(H) \cap \mathrm{U}(D)$ lorsque $H = \ker(e_j^*)$ et $D = \mathrm{Vect}(e_i)$, où $\{e_1, \dots, e_n\}$ est une base de E et $\{e_1^*, \dots, e_n^*\}$ est sa base duale. (*Il s'agit des matrices $T_{i,j}(\lambda)$!*) *Correction : Soient $\mu, \nu \in k^*$ tels que $a_0 = \mu e_i$ et*

$f_0 = \nu e_j^*$. *On a :*

$$u_{\lambda a_0, f_0}(e_k) = e_k + \lambda\mu f_0(e_k)e_i = \begin{cases} e_k, & \text{si } k \neq j, \\ e_k + \lambda\mu\nu e_i, & \text{si } k = j. \end{cases}$$

Ainsi, la matrice de $u_{\lambda a_0, f_0}$ dans la base $\{e_k\}$ est $I_n + \lambda\mu\nu E_{i,j} = T_{i,j}(\lambda\mu\nu)$. Si a_0 et f_0 sont choisis tels que $\mu = \nu = 1$ (i.e. $a_0 = e_i$ et $f_0 = e_j^*$) alors on obtient $T_{i,j}(\lambda)$.

Exercice 17 (Dualité pour les transvections)

Pour tout $u \in \mathrm{L}(E)$, on note $u^* \in \mathrm{L}(E^*)$ la transposée de u, définie par $u^*(\varphi) = \varphi \circ u$.

1. Démontrez que $u : E \to E$ est une transvection d'hyperplan H et de droite D si et seulement si $u^* : E^* \to E^*$ est une transvection d'hyperplan $D^\perp$ et de droite $H^\perp$. *Correction : Soit $u \in \mathrm{SL}(E)$ une transvection d'hyperplan H et de droite $D \subseteq H$. Ainsi, il existe $a \in D$ et $f \in E^*$ de noyau H tels que $u = u_{a,f}$, autrement dit $u(x) = x + f(x)a$ pour tout $x \in E$. Pour $\varphi \in E^*$, on a, pour tout $x \in E$:*

$$\begin{aligned} u^*(\varphi)(x) &= \varphi\big(u(x)\big) \\ &= \varphi\big(x + f(x)a\big) \\ &= \varphi(x) + f(x)\varphi(a) \\ &= \big(\varphi + \varphi(a)f\big)(x), \end{aligned}$$

donc :

$$u^*(\varphi) = \varphi + \varphi(a)f = \varphi + \mathrm{ev}_a(\varphi)f.$$

Ainsi, on a $u^* = u^*_{f,\mathrm{ev}_a}$. De plus, puisque $f(a) = 0 \iff \mathrm{ev}_a(f) = 0$, on a $f \in \ker \mathrm{ev}_a$ donc $u^* \in \mathrm{L}(E^*)$ est la transvection de droite $\langle f \rangle \subseteq E^*$ et d'hyperplan $\ker \mathrm{ev}_a$.

- *On a $g \in \langle f \rangle \iff g$ et f sont proportionnelles $\iff \ker g = \ker f = H$, donc la droite $\langle f \rangle \subseteq E^*$ est l'ensemble des $g \in E^*$ tels que $g|_H = 0$ donc c'est $H^\perp$.*
- *On a $g \in \ker \mathrm{ev}_a \iff \mathrm{ev}_a(g) = 0 \iff g(a) = 0 \iff g \in D^\perp$ puisque a engendre D.*

Ainsi, la transvection u^* est bien d'hyperplan $D^\perp$ et de droite $H^\perp$.

Réciproquement, en fixant des bases, si M est la matrice de u alors $M^\top$ est une transvection. Ainsi, si $M^\top$ est une transvection alors $M = (M^\top)^\top$ aussi, d'hyperplan $(H^\perp)^\perp = H$ et de droite $(D^\perp)^\perp = D$.

2. Pour souligner la dépendance en E, on utilise maintenant les notations $\mathrm{T}(E, H)$ et $\mathrm{U}(E, D)$ pour les groupes de transvections de $\mathrm{SL}(E)$ introduits dans les exercices 14 et 15. Démontrez qu'on a un isomorphisme de groupes :

$$\begin{aligned} \mathrm{T}(E, H) &\xrightarrow{\sim} \mathrm{U}(E^*, H^\perp) \\ u &\longmapsto u^*. \end{aligned}$$

Correction : L'application est bien définie par la question précédente. On a montré dans l'Exercice 14 que $\mathrm{T}(E, H) \simeq H$ est commutatif donc $(uv)^* = (vu)^* = u^*v^*$ pour $u, v \in \mathrm{T}(E, H)$. L'injectivité découle de celle de $u \mapsto u^*$ de $E \to E^*$, et la surjectivité découle de la question précédente car on a vu que si $u \in \mathrm{L}(E)$ est tel que $u^* \in \mathrm{U}(E^*, H^\perp)$ alors $u \in \mathrm{T}(E, H)$.

3. Vérifiez que les résultats des exercices 14 et 15 se déduisent l'un de l'autre par dualité. *Correction : Avec $D = H^\perp$, on a $D^\perp = H$ et :*

$$H \simeq \mathrm{T}(E, H) \iff H \simeq \mathrm{U}(E^*, H^\perp) \iff D^\perp \simeq \mathrm{U}(E^*, D),$$

donc l'énoncé de l'Exercice 14 dans E est équivalent à l'énoncé de l'Exercice 15 dans E^* (et donc dans E puisqu'on est en dimension finie).

Transvections élémentaires

Exercice 18 (Engendrement par les transvections élémentaires)

On fixe une base $\mathcal{B}$ de E. On fait alors les identifications $E = k^n$ et $\mathrm{GL}(E) = \mathrm{GL}_n(k)$. On appelle *matrices de transvection élémentaires* (relativement à la base fixée) les matrices $T_{i,j}(\lambda) = \mathrm{I}_n + \lambda E_{i,j}$ pour $i \neq j$.

1. Quel est l'effet sur une matrice M de la multiplication à gauche, resp. à droite, par $T_{i,j}(\lambda)$? *Correction : Multiplier à gauche par la matrice $\lambda E_{i,j}$ revient à conserver uniquement la ligne j, à la multiplier par λ et à la placer ligne i (les autres lignes étant nulles). Ainsi, multiplier à gauche par $T_{i,j}(\lambda)$ revient à ajouter λ fois la ligne j à la ligne i (on vérifie que c'est bien ça avec $T_{1,2}(\lambda)$). Pour l'effet de la multiplication à droite par $T_{i,j}(\lambda)$ on peut raisonner par transposition : si $MT_{i,j}(\lambda) = N$ alors $T_{j,i}(\lambda)M^\top = N^\top$ donc dans la ligne j de $M^\top$ on a mis λ fois la ligne i donc dans la colonne j de M on a mis λ fois la colonne i. On vérifie avec $T_{2,1}(\lambda)$.*

2. On note $L_1, \dots, L_n$ les lignes de M. Montrez que la multiplication de M à gauche par $T_{i,j}(1)T_{j,i}(-1)T_{i,j}(1)$ a pour effet de remplacer L_i par L_j et L_j par $-L_i$. *Correction : Après la première multiplication (celle à droite), la ligne L_i devient :*

$$L_i^{(1)} \coloneqq L_i + L_j,$$

et L_j reste $L_j^{(1)} \coloneqq L_j$. Après la deuxième, la ligne $L_i^{(1)}$ reste $L_i^{(2)} \coloneqq L_i^{(1)}$ et $L_j^{(1)}$ devient :

$$\begin{aligned} L_j^{(2)} &\coloneqq L_j^{(1)} - L_i^{(1)} \\ &= L_j - (L_i + L_j) \\ &= -L_i. \end{aligned}$$

Finalement, après la dernière multiplication $L_i^{(2)}$ devient :

$$\begin{aligned} L_i^{(3)} &\coloneqq L_i^{(2)} + L_j^{(2)} \\ &= L_i^{(1)} - L_i \\ &= (L_i + L_j) - L_i \\ &= L_j, \end{aligned}$$

et $L_j^{(2)}$ reste $L_j^{(3)} \coloneqq L_j^{(2)} = -L_i$.

3. En appliquant le pivot de Gauss, montrez que les matrices de transvection élémentaires engendrent $\mathrm{SL}(E)$. *Correction : Soit $M \in SL_n(k)$. Le pivot de Gauss appliqué à M consiste à éliminer successivement les coefficients sous le pivot puis à sa droite. Le pivot est un coefficient non nul que l'on a amené en position (i,i). Le transport du pivot est effectué grâce à l'opération décrite en 2 (et à son analogue pour les colonnes), et les élimination de coefficients via le pivot en (i,i) se font via des multiplication à gauche par des matrices $T_{i,j}(\lambda)$ (pour les lignes) et des multiplications à droite par des matrices $T_{j,i}(\lambda)$ (pour les colonnes) pour $j > i$.*
Les matrices $T_{k,l}(\lambda)$ pour $k \neq l$ étant de déterminant 1, à la fin de la procédure on obtient une matrice diagonale de déterminant 1. Si tous les coefficients sont égaux à 1 c'est gagné, sinon il suffit de montrer que l'on peut transformer une matrice $\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ avec $a, b \neq 0$ en $\left(\begin{smallmatrix} 1 & 0 \\ 0 & ab \end{smallmatrix}\right)$ avec des opérations élémentaires (les opérations effectuées ne changent pas les autres coefficients non extraits de la matrice).

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} &\longrightarrow \begin{pmatrix} a & 0 \\ 1 & b \end{pmatrix} && C_1 \leftarrow C_1 + b^{-1}C_2 \\ &\longrightarrow \begin{pmatrix} 1 & -(a-1)b \\ 1 & b \end{pmatrix} && L_1 \leftarrow L_1 - (a-1)L_2 \\ &\longrightarrow \begin{pmatrix} 1 & -(a-1)b \\ 0 & ab \end{pmatrix} && L_2 \leftarrow L_2 - L_1 \\ &\longrightarrow \begin{pmatrix} 1 & 0 \\ 0 & ab \end{pmatrix} && C_2 \leftarrow C_2 + (a-1)bC_1 \end{aligned}$$

Exercice 19 (Petites parties génératrices de $\mathrm{SL}(E)$)

On note $\mathbb{F}_q$, avec $q = p^d$ et p premier, un corps fini à q éléments.

1. Combien y a-t-il de matrices de transvection élémentaires dans $\mathrm{SL}_n(\mathbb{F}_q)$? *Correction : Pour $T_{i,j}(\lambda)$ on a $n(n-1)$ choix pour le couple (i,j) et $q-1$ choix pour le λ donc il y a $n(n-1)(q-1)$ matrices de transvection élémentaires.*

2. En utilisant l'identité $T_{i,j}(\lambda)T_{i,j}(\mu) = T_{i,j}(\lambda+\mu)$, montrez que $\mathrm{SL}_n(\mathbb{F}_q)$ peut être engendré par $d(n^2-n)$ éléments. *Correction : Soit $(e_1, \dots, e_d)$ une $\mathbb{F}_p$-base de $\mathbb{F}_q$ (qui possède d éléments puisque $q = p^d$). Un élément de $\lambda \in \mathbb{F}_q$ s'écrit donc $\lambda = \sum_{k=1}^{l} \lambda_k e_k$ avec $\lambda_k \in \mathbb{F}_p$ donc :*

$$T_{i,j}(\lambda) = T_{i,j}(\lambda_1 e_1) \cdots T_{i,j}(\lambda_d e_d).$$

Mais puisque $\lambda_k \in \mathbb{F}_p$ on a $\lambda_k e_k = e_k + \cdots + e_k$ (avec λ_k facteurs, où par exemple on a choisi $\lambda_k \in \{0, \dots, p-1\}$) donc :

$$T_{i,j}(\lambda_k e_k) = T_{i,j}(e_k)^{\lambda_k}.$$

Ainsi, le groupe $\mathrm{SL}_n(\mathbb{F}_q)$ peut être engendré par les matrices $T_{i,j}(e_k)$ avec encore $n(n-1)$ choix pour les couples (i,j) et cette fois d choix pour k.

3. Démontrez que $\mathrm{SL}_2(\mathbb{F}_p)$ peut être engendré par les deux éléments $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$. *Correction : On a $n = 2$ et $d = 1$ donc $d(n^2-n) = 2$, les deux éléments correspondant $T_{1,2}(1)$ et $T_{2,1}(1)$ étant justement ceux indiqués (le vecteur $e_1 \coloneqq 1 \in \mathbb{F}_p$ étant une $\mathbb{F}_p$-base de $\mathbb{F}_p$).*