Théorie des Groupes et Géométrie

TD n°2

Produit semi-direct

Exercice 1 (Holomorphe d'un groupe)

On appelle *holomorphe* d'un groupe de G le produit semi-direct $\mathrm{Hol}(G) = G \rtimes_\varphi \mathrm{Aut}(G)$ défini par l'action tautologique $\varphi = \mathrm{Id} : \mathrm{Aut}(G) \to \mathrm{Aut}(G)$ de $\mathrm{Aut}(G)$ sur G. Écrivez les formules décrivant le produit et l'inverse dans $\mathrm{Hol}(G)$.

Pour $g, h \in G$ et $\alpha, \beta \in \mathrm{Aut}(G)$ on a $(g, \alpha)(h, \beta) = \big(g\alpha(h), \alpha\beta\big)$ dans $\mathrm{Hol}(G)$ et $(g, \alpha)^{-1} = \big(\alpha^{-1}(g^{-1}), \alpha^{-1}\big)$.

Exercice 2 (Sur-groupes et conjugaisons)

1. Soient G un groupe et $f : G \to G$ un automorphisme. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que f est la restriction à G d'un automorphisme intérieur (ou conjugaison) de G'.
   On pourra prendre pour G' l'holomorphe $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$.
2. Soient G un groupe fini et $x, y \in G$ deux éléments de même ordre. Montrez qu'il existe un sur-groupe $G' \supset G$ tel que x et y sont conjugués dans G'.
   On pourra prendre pour G' le groupe symétrique $\mathfrak{S}_G$.

1. On prend $G' = \mathrm{Hol}(G)$ comme suggéré. Soit $f \in \mathrm{Aut}(G)$ et $g \in G$. L'élément $g \in G$ s'identifie à l'élément $(g, 1) \in G'$ (avec le 1 de droite étant id_G). On a $\big(f(g), 1\big) = (1, f)(g, 1)(1, f)^{-1}$, en effet d'après l'exercice précédent on a $(1, f)^{-1} = (1, f^{-1})$ puis $(1, f)(g, 1) = \big(f(g), f\big)$ et
   $$(1, f)(g, 1)(1, f)^{-1} = \big(f(g), f\big)(1, f^{-1}) = \big(f(g)f(1), 1\big) = \big(f(g), 1\big),$$
   qui s'identifie bien à $f(g) \in G$. On a donc montré que la restriction à G de l'automorphisme intérieur donné par la conjugaison par $(1, f)$ dans G coincide avec f.
2. Soit x' l'image de x dans G', c'est-à-dire la multiplication à gauche par x. Par hypothèse, pour tout élément $g \in G$ on a $x'^n g = g$, et en fait la décomposition en cycles à supports disjoints de x' ne contient que des n-cycles. C'est la même chose pour y' donc x' et y' sont conjugués dans G'.

Exercice 3 (Automorphismes du groupe diédral)

Soit $n \geq 3$ et $\mathbb{D}_n$ le groupe diédral engendré par deux élements r, s satisfaisant les relations $r^n = s^2 = (rs)^2 = 1$.

1. On rappelle que tout élément $x \in \mathbb{D}_n$ peut s'écrire d'une unique manière sous la forme $x = s^\epsilon r^i$ avec $\epsilon \in \{0, 1\}$ et $i \in \mathbb{Z}/n\mathbb{Z}$. Montrez que le produit de $x = s^\epsilon r^i$ avec $y = s^\eta r^j$ est donné par la formule $xy = s^{\epsilon+\eta} r^{(1-2\eta)i+j}$.
2. Montrez que pour tout morphisme de groupes $f : \mathbb{D}_n \to H$, les éléments $R = f(r)$ et $S = f(s)$ vérifient les relations $R^n = S^2 = (RS)^2 = 1$. Réciproquement montrez que pour tout couple $(R, S) \in H^2$ tel que $R^n = S^2 = (RS)^2 = 1$ il existe un unique morphisme de groupes $f : \mathbb{D}_n \to H$ tel que $f(r) = R$ et $f(s) = S$.
3. Déduisez de la question précédente que les automorphismes $f : \mathbb{D}_n \to \mathbb{D}_n$ sont les morphismes $f = f_{i,j}$ déterminés par $f(r) = r^i$ et $f(s) = sr^j$, pour $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ et $j \in \mathbb{Z}/n\mathbb{Z}$.
4. Montrez que $\mathrm{Aut}(\mathbb{D}_n)$ est l'holomorphe de $\mathbb{Z}/n\mathbb{Z}$.
   On pourra montrer que $\mathrm{Aut}(\mathbb{D}_n) = N \rtimes H$ *avec* $N = \{f_{1,j};\, j \in \mathbb{Z}/n\mathbb{Z}\}$ *et* $H := \{f_{i,0};\, i \in (\mathbb{Z}/n\mathbb{Z})^\times\}$.

Exercice 4 (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.
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 ?
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.

1. 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. Immédiat par la question précédente (on voit bien la structure multiplicative apparaître). Le morphisme d'action est $a \cdot d \coloneqq a \circ d$ pour $a \in L$ et $d \in T$. Les translations sont bien distinguées par la question précédentes (les parties linéaires se composant) et donc $\mathrm{GA}(E) \simeq T \rtimes L$.
3. 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 $HT = TH$).

Exercice 5 (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 iumage. 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 $\mu_n(k)$.
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 $\mathrm{PSL}_n(k)$.
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.
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.

1. 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. 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 $M \in \operatorname{im} \bar{\varphi}$, 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. 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 $\varphi(N) = \pi_{\mathrm{PGL}} \mathrm{diag}(\mu, 1, \ldots, 1)$. Ainsi N et $\mathrm{diag}(\mu, 1, \ldots, 1)$ 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. 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 6 (PSL et PGL, suite)

À l'aide de l'exercice 5, montrer que :

1. Si k est algébriquement clos alors l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est un isomorphisme.
2. Si $k = \mathbb{R}$ et n est impair alors l'inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est un isomorphisme.
3. Si $k = \mathbb{R}$ et n est pair alors l'image de inclusion $\mathrm{PSL}_n(k) \to \mathrm{PGL}_n(k)$ est d'indice 2.
4. Si k est un corps fini alors l'image de 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.

1. Par l'exo 5.1 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. Même argument.
3. D'après l'exo 5.2 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 $\left|\mathrm{PGL}_n(k)/\mathrm{PSL}_n(k)\right| = 2$ puisque $\left|\mathbb{R}^*/\mathbb{R}_+^*\right| = 2$ (car $\mathbb{R}^* = \mathbb{R}_+^* \sqcup (-1)\mathbb{R}_+^*$).
4. 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 7 (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 :*

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

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 $k^\times$.

2. Montrer que $H \subset Z \coloneqq Z\big(\mathrm{GL}_n(k)\big)$.

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.

4. En déduire une condition nécessaire et suffisante sur k et n pour qu'il existe un tel H.

Espaces homogènes

Exercice 8 (Bases d'un espace vectoriel)

Montrez que l'ensemble des bases d'un espace vectoriel de dimension finie E est un espace principal homogène sous $\mathrm{GL}(E)$.

Exercice 9 (Classes à gauche versus classes à droite)

Soient G un groupe et H un sous-groupe. On note G/H le quotient de G par la relation d'équivalence définie par la multiplication à *droite* par des éléments de H, i.e. $g' \sim g$ ssi il existe $h \in \mathrm{H}$ tel que $g' = gh$. On note H\G le quotient par la relation d'équivalence de multiplication à *gauche* par des éléments de H. Produisez une bijection entre G/H et H\G.

Exercice 10 (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.

2. Démontrez que π est ouverte (i.e l'image de tout ouvert est un 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.

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.*

Exercice 11 (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.

2. Décrivez les stabilisateurs des points.

3. Utilisant la relation stabilisateur-orbite et l'exercice 10, démontrez par récurrence sur n que $\mathrm{SO}_n(\mathbb{R})$ est connexe.

1. 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. 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. 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 10.4). Il reste quand même à justifier pourquoi la bijection $f : \mathrm{SO}_{n+1}(\mathbb{R})/G \simeq S^n$ est un homéomphisme. C'est bien une bijection, elle est continue par l'exo 10.3 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 $\mathrm{SO}_{n+1}(\mathbb{R})$, 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 10.1) donc comme f est continue on en déduit que $f(F)$ est également compact (car S^n est séparé) donc fermé (toujours car S^n est fermé). *(Remarque : pour démontrer ce résultat on peut aussi utiliser un théorème de réduction et raisonner comme dans l'exercice 15.)*

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 (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.

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 $H \xrightarrow{\sim} \mathrm{T}(H)$.

1. 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. 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. Soit $u \in \mathrm{T}(H)$. Par la construction matricielle précédente, on sait qu'il existe $b \in H$ tel que $\mathrm{im}(u - \mathrm{Id}_E) = \langle b \rangle$. Si $f \in E^*$ est la forme linéaire telle que $(u - \mathrm{Id}_E)(x) = f(x)b$ pour tout $x \in E$, alors $\ker f = H = \ker f_0$ donc f et f_0 sont proportionelles. Ainsi, on a $f = \lambda f_0$ et avec $a := \lambda b$ on a bien $u = u_{a,f_0}$.

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.

Exercice 13 (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.

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.

Exercice 14 (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 $(k,+) \xrightarrow{\sim} \mathrm{T}(H) \cap \mathrm{U}(D)$.

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* $T_{i,j}(\lambda)$ *!*)

Exercice 15 (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. 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

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

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 16 (Dualité pour les transvections)

Pour tout $u \in \mathrm{L}(E)$, on note u^* ou ${}^{\mathrm{t}}u$ 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 $H^\perp$.

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 12 et 13. Démontrez qu'on a un isomorphisme de groupes :

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

3. Vérifiez que les résultats des exercices 12 et 13 se déduisent l'un de l'autre par dualité.

Exercice 17 (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 $T_{i,j}(\lambda)$?

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 $-L_i$.

3. En appliquant le pivot de Gauss, montrez que les matrices de transvection élémentaire engendrent $\mathrm{SL}(E)$.

Groupe linéaire sur les corps finis

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

Exercice 18 (Décompte des transvections)

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 $a' = \lambda^{-1}a$.

2. 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 $v(a) = a$, $v(H) = H$, $v(b) \in b + H$, où $b \notin H$ est fixé. La matrice de v dans une base obtenue en complétant une base de H avec le vecteur b est donc de la forme :

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

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

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

1. 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 proportionelles : 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. 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 $f(b)\lambda g = f\big(g(b)\big)a$ donc $f\big(g(b)\big) = \lambda f(b)$. 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. 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 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 transvection élémentaires dans $\mathrm{SL}_n(\mathbb{F}_q)$?

2. 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.

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 $\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$.

Exercice 20 (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 $f^{q-1} = \mathrm{Id}$.

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 $i = 1, \ldots, q-1$. Montrez que l'application $f \mapsto (E_1, \ldots, E_{q-1})$ 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.

3. On fixe un $(q-1)$-uplet d'entiers $\nu = (n_1, \ldots, n_{q-1})$ tels 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 $g \cdot (E_1, \ldots, E_{q-1}) := (g(E_1), \ldots, g(E_{q-1}))$ est transitive et décrivez le stabilisateur d'un point.

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

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

1. 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.

2. 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. 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 $(E_1, \ldots, E_{q-1})$, ainsi le stabilisateur est isomorphe à $\prod_i \mathrm{GL}(E_i) \simeq \prod_i \mathrm{GL}_{n_i}(q)$.

4. On applique la relation orbite-stablisateur.