**Théorie des Groupes et Géométrie**

Contrôle Continu n°1 du vendredi 22 octobre 2021

**Exercice 1** (4 points)

1. (1pt) Démontrons par récurrence sur $i \geq 0$ que $D^i(G) \subset C^i(G)$. Pour $i = 0$ on a $D^0(G) = C^0(G) = G$ donc la propriété est vérifiée. Si elle est vérifiée pour un entier $i \geq 1$, alors du fait que $D^i(G) \subset G$ il découle que [1]

$$D^{i+1}(G) = [D^i(G), D^i(G)] \ \subset [G, D^i(G)] = C^{i+1}(G).$$

Ceci démontre la propriété. En particulier, si $G$ est nilpotent alors $C^i(G) = 1$ pour $i$ assez grand, donc aussi $D^i(G) = 1$ pour $i$ assez grand, donc $G$ est résoluble.

2. (1pt) Notons $G = \mathrm{Aff}(\mathbb{R})$. Notons $f_{a,b} = f : \mathbb{R} \to \mathbb{R}$, $x \mapsto ax + b$. Comme $f_{a,b}(f_{c,d}(x)) = a(cx + d) + b = acx + (ad + b)$ on voit que $f_{a,b} \circ f_{c,d} = f_{ac,ad+b}$. En notant $\pi : \mathrm{Aff}(\mathbb{R}) \to \mathbb{R}^\times$ l'application $f_{a,b} \mapsto a$ on a donc

$$\pi(f_{a,b} \circ f_{c,d}) = \pi(f_{ac,ad+b}) = ac = \pi(f_{a,b})\pi(f_{c,d})$$

c'est-à-dire que $\pi$ est un morphisme de groupes. Son noyau $T = \ker(\pi)$ est le sous-groupe des transformations $f_{1,b}$, $x \mapsto x + b$. Ce sont des translations, qui forment un sous-groupe commutatif isomorphe à $(\mathbb{R}, +)$. Le quotient $G/T$ s'identifie à l'image de $\pi$ qui est un sous-groupe de $\mathbb{R}^\times$ et est donc également un groupe commutatif. Ainsi $T$ et $G/T$ sont commutatifs donc résolubles. D'après une propriété du cours $G$ est donc résoluble. [1]

3. (2pt) Comme ci-dessus, notons $T$ le sous-groupe des translations de $G$. Pour voir que $G$ n'est pas nilpotent il suffit de démontrer que $C^i(G) = T$ pour tout $i \geq 1$. Pour cela calculons un commutateur bien choisi :

$$\left[f_{2,0}\,,\ f_{1,b}\right] = f_{2,0} f_{1,b} f_{2,0}^{-1} f_{1,b}^{-1} = f_{1,b}.$$

En particulier $f_{1,b} = \left[f_{2,0}\,,\ f_{1,b}\right] \in [G, T]$ et ceci démontre que $T \subset [G, T]$. En conséquence :

(i) $C^1(G) = [G, G] = T$ puisque l'inclusion $C^1(G) \subset T$ provient du fait que $G/T$ est abélien (vu en question 2), et l'inclusion réciproque vient du calcul $T \subset [G, T] \subset [G, G] = C^1(G)$. [2]

(ii) par récurrence, si $C^i(G) = T$ pour un $i \geq 1$ alors $C^{i+1}(G) \subset C^i(G) = T$ et l'inclusion réciproque vient du calcul $T \subset [G, T] = [G, C^i(G)] = C^{i+1}(G)$.

Ainsi $C^i(G) = T$ pour tout $i \geq 1$, donc la suite $C^i(G)$ ne peut pas stationner à 1.

**Exercice 2** (2 points)

Un $p$-groupe est un groupe fini d'ordre $|G| = p^\alpha > 1$ avec $\alpha \geq 1$. Faisons agir $G$ sur lui-même par conjugaison.

(i) (1pt) Les éléments $x \in G$ dont l'orbite (=la classe de conjugaison) est réduite à $\{x\}$ sont ceux pour lesquels $gxg^{-1} = x$ pour tout $g \in G$, c'est-à-dire les éléments du centre $Z = Z(G)$. Les autres éléments ont une orbite $\mathcal{O}_G(x)$ non réduite à un point. La bijection stabilisateur-orbite $G/G_x \xrightarrow{\sim} \mathcal{O}_G(x)$ montre que dans ce cas le cardinal $|\mathcal{O}_G(x)| = [G : G_x] = |G|/|G_x|$ est une puissance de $p$ distincte de 1, donc un multiple de $p$. [1]

(ii) (1pt) La partition en orbites s'écrit $G = Z \amalg \mathcal{O}_1 \amalg \cdots \amalg \mathcal{O}_d$ où $\mathcal{O}_1, \ldots, \mathcal{O}_d$ sont les orbites non ponctuelles. En prenant les cardinaux on trouve $|G| = |Z| + |\mathcal{O}_1| + \cdots + |\mathcal{O}_d|$. Compte tenu de ce qui précède $|Z| = |G| - |\mathcal{O}_1| - \cdots - |\mathcal{O}_d|$ est donc divisible par $p$. Comme $Z$ contient 1 son cardinal est non nul, il est donc $\geq p$. Ainsi $Z$ n'est pas réduit à l'élément neutre. [1]

**Exercice 3** (6 points)

1. (a) (0.5pt) 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 $\bar{u} \in \mathrm{L}(E/D)$ tel que $\pi \circ u = \bar{u} \circ \pi$. Comme de plus $u$ et $\pi$ sont surjectifs, alors $\bar{u} \circ \pi = \pi \circ u$ l'est, donc $\bar{u}$ également. Comme $E/D$ est de dimension finie, ceci implique que $\bar{u} \in \mathrm{GL}(E/D)$. [0.5]

Pour alléger, nous utilisons dans la suite la notation $uv$ pour la composée $u \circ v$.

1. (b) (0.5pt) 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

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

Il en découle que $\bar{u}\bar{v}\pi = \bar{u}(\bar{v}\pi) = \bar{u}(\pi v) = (\bar{u}\pi)v = \pi uv = \overline{uv}\pi$. Comme $\pi$ est surjectif, ceci implique $\overline{uv} = \bar{u}\bar{v}$. En d'autres termes $p(uv) = p(u)p(v)$ i.e. $p$ est un morphisme de groupes. [0.5]

2. (1.5pt) 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 $\mathrm{Id}_E$ sont linéaires, on a [1]

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

donc $f(\lambda x + \mu y) = \lambda f(x) + \mu f(y)$ et $f$ est une forme linéaire. Si $f = 0$, on a $u = \mathrm{Id}_E$. Sinon, la condition $u_{|D} = \mathrm{Id}_D$ impose que $f(a) = 0$, et les conditions $f \neq 0$, $a \neq 0$ assurent que que $u$ est une tranvection de droite $D$.

Réciproquement, si $u$ est $\mathrm{Id}_E$ 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 $u \in \ker(p)$. [0.5]

3. (2pt) 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 $\mathcal{B}_F = \{e_2, \ldots, e_n\}$ 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 : [2]

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

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. (1.5pt) 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 : 0.5

(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. 0.5

(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. 0.5

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

**Exercice 4** (4 points)

1. (1pt) La partie $H \cap \mathfrak{A}_n$ est un sous-groupe (comme intersection de sous-groupes) inclus dans $\mathfrak{A}_n$. Si $h \in H \cap \mathfrak{A}_n$ et $x \in \mathfrak{A}_n$, on a $xhx^{-1} \in \mathfrak{A}_n$ comme produit d'éléments de $\mathfrak{A}_n$ et $xhx^{-1} \in H$ car $H$ est distingué dans $\mathfrak{S}_n$. Donc $xhx^{-1} \in H \cap \mathfrak{A}_n$, ce qui montre que $H \cap \mathfrak{A}_n$ est distingué dans $\mathfrak{A}_n$. 0.5

Comme $n \geq 5$, le groupe $\mathfrak{A}_n$ est simple donc ses seuls sous-groupes distingués sont $\mathfrak{A}_n$ et $\{1\}$. Donc on a soit $H \cap \mathfrak{A}_n = \mathfrak{A}_n$, c'est-à-dire $H$ contient $\mathfrak{A}_n$, soit $H \cap \mathfrak{A}_n = \{1\}$. 0.5

2. (2pt) Notons $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ la signature. Si $H \cap \mathfrak{A}_n = \{1\}$, on a

$$\ker(\varepsilon_{|H}) = H \cap \ker(\varepsilon) = H \cap \mathfrak{A}_n = \{1\}.$$

Ceci montre que $\varepsilon_{|H} : H \to \{\pm 1\}$ est injective. On a donc $H \simeq \{\pm 1\}$ ou $H \simeq \{1\}$. Dans le premier cas $H$ possède un seul élément $c \neq 1$. Les conjugaisons par des éléments de $\mathfrak{S}_n$, qui stabilisent $H$, doivent envoyer tout élément distinct de 1 sur un élément distinct de 1, donc elles envoient $c$ sur $c$. Ceci signifie que $\sigma c \sigma^{-1} = c$ pour tout $\sigma \in \mathfrak{S}_n$, c'est-à-dire que $c$ est central dans $\mathfrak{S}_n$. Comme $n \geq 3$ le centre de $\mathfrak{S}_n$ est trivial, donc c'est impossible. Donc $H = \{1\}$. 1 1

3. (1pt) Supposons que $H$ contient $\mathfrak{A}_n$. Alors $2 = [\mathfrak{S}_n : \mathfrak{A}_n] = [\mathfrak{S}_n : H] \cdot [H : \mathfrak{A}_n]$ donc $[\mathfrak{S}_n : H]$ égale 1 ou 2. Si $[\mathfrak{S}_n : H] = 1$ on a $H = \mathfrak{S}_n$, et si $[\mathfrak{S}_n : H] = 2$ on a $[H : \mathfrak{A}_n] = 1$ donc $H = \mathfrak{A}_n$. 1

**Exercice 5** (8 points)

1. (1pt) Comme $a$ et $b$ commutent, pour tout entier $i \in \mathbb{Z}$ on a $(ab)^i = a^i b^i$.

(i) En particulier $(ab)^{mn} = a^{mn}b^{mn}$. Comme $a^m = b^n = 1$, on trouve $(ab)^{mn} = 1$.

(ii) Soit $i \geq 1$ tel que $(ab)^i = 1$. Alors $a^i = b^{-i}$. On en déduit que $a^{in} = b^{-in} = 1$ donc $m$ divise $in$. Comme $m$ est premier avec $n$, par le lemme d'Euclide $m$ divise $i$. De même, on a $b^{-im} = a^{im} = 1$ donc $n$ divise $im$ puis par Euclide $n$ divise $i$. Comme $m$ et $n$ sont premiers entre eux, $mn$ divise $i$.

D'après (i) et (ii) l'entier $mn$ est le plus petit entier $i \geq 1$ tel que $(ab)^i = 1$, c'est donc l'ordre de $ab$.

2. (1pt) Comme $p$ est premier et ne divise pas $2mnr$, il est premier avec $2mnr$. En conséquence $p$ est inversible dans l'anneau $\mathbb{Z}/(2mnr)\mathbb{Z}$. C'est donc un élément du groupe fini $(\mathbb{Z}/(2mnr)\mathbb{Z})^\times$ et il possède donc un ordre fini qui est un entier $\alpha \geqslant 1$. On a alors $p^\alpha = 1$ dans l'anneau $\mathbb{Z}/2mnr\mathbb{Z}$.

3. (1pt) Soit $\omega$ un générateur du groupe cyclique $\mathbb{F}_q^\times$. Son ordre est $q-1 = p^\alpha - 1$ qui est un multiple de $2mnr$ d'après le choix fait dans la question précédente : il existe un entier $k$ tel que $q - 1 = 2mnrk$. Comme $\omega$ est d'ordre $2mnrk$, les éléments $u = \omega^{nrk}$, $v = \omega^{mrk}$ et $w = \omega^{mnk}$ sont d'ordres respectifs $2m$, $2n$, $2r$.

4. (1pt) Le polynôme caractéristique de $a$ est $\chi_a = (X-u)(X-u^{-1})$. Du fait que $u^2$ est d'ordre $m \neq 1$, on a $u \neq u^{-1}$ si bien que $\chi_a$ scindé à racines simples. Il s'ensuit que que $a$ est semblable à $\mathrm{diag}(u, u^{-1})$ et il est donc d'ordre $2m$. De même, $b$ est d'ordre $2n$.

5. (1pt) La matrice

$$ab = \begin{pmatrix} uv+t & v^{-1} \\ u^{-1}t & u^{-1}v^{-1} \end{pmatrix}$$

a pour polynôme caractéristique

$$\chi_{ab} = X^2 - (uv + t + u^{-1}v^{-1})X + 1 = (X-w)(X-w^{-1})$$

puisque $t = (w + w^{-1}) - (uv + u^{-1}v^{-1})$. Ce polynôme est scindé à racines simples. On en déduit que la matrice $ab$ est semblable à $\mathrm{diag}(w, w^{-1})$, elle est donc d'ordre $2r$.

6. (1.5pt) Soit $M \in \mathrm{SL}_2(\mathbb{F}_q)$ une matrice telle que $M^2 = \mathrm{I}_2$. Alors $M$ est annulée par le polynôme $X^2-1$ qui est égal à $(X-1)(X+1)$ et est donc scindé à racines simples, puisque la caractéristique $p$ de $\mathbb{F}_q$ est différente de 2. Alors $M$ est diagonalisable i.e. $M = PDP^{-1}$ avec $D$ diagonale. Les coefficients diagonaux de $D$ sont 1 ou $-1$, et comme $\det(D) = 1$ ils sont nécessairement égaux. Donc $D = \pm\mathrm{I}_2$ ce dont on déduit que $M = \pm\mathrm{I}_2$. Ainsi il n'y a qu'un élément d'ordre exactement 2, c'est $M = -\mathrm{I}_2$.

7. (1.5pt) Posons $G = \mathrm{SL}_2(\mathbb{F}_q)/\{\pm\mathrm{I}_2\}$ et notons $\pi : \mathrm{SL}_2(\mathbb{F}_q)/\{\pm\mathrm{I}_2\} \to G$ le morphisme de quotient. Soit $x \in \mathrm{SL}_2(\mathbb{F}_q)$ un élément d'ordre $2k$ (pour un certain entier $k$) et montrons que l'ordre de son image $\bar{x} := \pi(x)$ dans $G$ est égal à $k$. D'une part $x^k$ est d'ordre 2 donc $x^k = -\mathrm{I}_2$ d'après la question précédente. On en déduit que $\bar{x}^k = 1$. D'autre part, si $\bar{x}^j = 1$ alors $x^j \in \ker(\pi) = \{\pm\mathrm{I}_2\}$ puis $x^{2j} = 1$ donc $2k \mid 2j$ et enfin $k \mid j$. Ces deux informations réunies montrent que l'ordre de $\bar{x}$ dans $G$ est $k$, comme annoncé.

En appliquant ceci pour $a$, $b$ et $ab$, on voit que leurs images $\bar{a}$, $\bar{b}$ et $\overline{ab}$ dans $G$ sont d'ordres $m$, $n$, $r$ respectivement.