Corrigé de l'examen du cours d'Algèbre 1, ENS Ulm, Janvier 2022

Problème 1. (Sommes de carrés, suivant Hurwitz et Eckmann) *On se propose de démontrer, que si l'on a une identité remarquable dans* $\mathbb{R}[x_1,\dots,x_n,y_1,\dots,y_n]$ *de la forme*

$$(x_1^2+x_2^2+\cdots+x_n^2)(y_1^2+y_2^2+\cdots+y_n^2)=z_1^2+z_2^2+\cdots+z_n^2,$$

où les z_k *sont combinaisons* $\mathbb{R}$*-linéaires des* x_iy_j*, alors on a* $n=1,2,4$ *ou* 8 (Théorème de Hurwitz).

Partie 1

Soient m,n *des entiers* >1 *avec* m *impair, ainsi que* $g_1,\dots,g_m$ *des éléments de* $\mathrm{GL}_n(\mathbb{C})$ *vérifiant*[1]

$$(*)\qquad g_i^2=-1_n \text{ pour tout } i, \text{ et } g_ig_j=-g_jg_i \text{ pour tout } i\neq j.$$

On se propose dans cette partie de démontrer la congruence $n\equiv 0 \bmod 2^{\frac{m-1}{2}}$*. Pour cela, on note* G *le sous-groupe de* $\mathrm{GL}_n(\mathbb{C})$ *engendré par les* g_i*, avec* $i=1,\dots,m$*. Nous allons commencer par déterminer* $|G|$*, le centre* Z *de* G*, ainsi que le groupe dérivé* $\mathrm{D}(G)$ *de* G*. Pour* $I\subset\{1,\dots,m\}$*, disons* $I=\{i_1,\dots,i_k\}$ *avec* $i_1<i_2<\cdots<i_k$*, on pose* $g_I=g_{i_1}g_{i_2}\dots g_{i_k}\in G$*, avec la convention* $g_\emptyset=1_n$*. On pose enfin* $\eta=g_{\{1,\dots,m\}}=g_1g_2\cdots g_m\in G$*. On écrira « $a=\pm b$ » pour « $a=b$ ou $a=-b$ ».*

(i) Donner un exemple d'éléments g_1,g_2,g_3 *(cas* $m=3$*) satisfaisant les relations* $(*)$ *pour* $n=2$*.*

On pose $g_1=\mathrm{I}$*,* $g_2=\mathrm{J}$ *et* $g_3=\mathrm{K}$ *(quaternions). On a* $G=\mathrm{H}_8$*,* $\eta=\mathrm{IJK}=-1_2$ *et* $n=2^{\frac{m-1}{2}}$*.*

(ii) Soient $I,J\subset\{1,\dots,m\}$*, justifier brièvement l'égalité* $g_Ig_J=\pm g_K$ *avec* $K=(I\cup J)\smallsetminus(I\cap J)$*.*

En utilisant les relations données, on constate que l'on a $g_Ig_i=\pm g_{I'}$ *avec* $I'=I\smallsetminus\{i\}$ *ou* $J=I\cup\{i\}$*, selon que l'on a* $i\in I$ *ou non. La formule de l'énoncé pour* g_Ig_J *s'en déduit par récurrence sur* $|J|$*.*

(iii) En déduire $G=\{\pm g_I\mid I\subset\{1,\dots,m\}\}$ *et* $g^2=\pm 1_n$ *pour tout* $g\in G$*.*

Le (ii) montre $g_I^2=\pm 1_n$ *pour* $J=I$*, donc* $g_I^{-1}=\pm g_I$*, puis que* $X=\{\pm g_I\}$ *est un sous-groupe de* G *contenant les* g_i *: c'est donc* G*.*

(iv) Soit $I\subset\{1,\dots,m\}$*. Montrer que l'on a* $g_i\,g_I\,g_i^{-1}=(-1)^{|I|}\epsilon g_I$ *avec* $\epsilon=1$ *si* $i\notin I$*, et* $\epsilon=-1$ *sinon.*

On a $g_i(g_{i_1}\cdots g_{i_k})g_i^{-1}=(g_ig_{i_1}g_i^{-1})(g_ig_{i_2}g_i^{-1})\cdots(g_ig_{i_k}g_i^{-1})$*. On conclut car pour tout* $1\leq s\leq k$ *on a* $g_ig_{i_s}g_i^{-1}=-g_{i_s}$ *si* $i\neq i_s$*,* $+g_i$ *sinon.*

(v) (suite) En déduire que si $g=\pm g_I$*, la classe de conjugaison de* g *dans* G *est* $\{g,-g\}$*, sauf si* $|I|=0$ *ou* $|I|=m$*, auquel cas on a* $g\in Z$*.*

On a clairement $\pm 1_n=\pm g_\emptyset\in Z$*. Comme* m *est impair, le (iv) montre que pour tout* $i=1,\dots,m$ *on a* $g_i\eta=(-1)^{m-1}\eta g_i=\eta g_i$*. On a donc aussi* $\pm\eta\in Z$*. Supposons maintenant* $0<|I|<m$*. Le (iv) montre que* $g_igg_i^{-1}=\pm g$*, avec des signes opposés selon que l'on choisit* i *dans* I *ou non. Les deux cas se produisent comme* $0<|I|<m$*. On en déduit que la classe de conjugaison de* g *contient* $\pm g$*. Mais en itérant le (iv) on a* $g_Jgg_J^{-1}=\pm g$ *pour tout* J*, donc cette classe de conjugaison est exactement* $\{g,-g\}$*.*

1. Bien entendu, 1_n désigne ici la matrice identité de $\mathrm{M}_n(\mathbb{C})$.

(vi) *Montrer* $Z = \{\pm 1_n, \pm\eta\}$, *puis* $|Z| = 2$ *ou* $|Z| = 4$, *selon que l'on a* $\eta = \pm 1_n$ *ou non.*[2]

La question précédente et (iii) montrent $Z = \{\pm 1_n, \pm\eta\}$. *On a clairement* $|Z| = 2$ *si* $\eta = \pm 1_n$. *Sinon, les 4 éléments* $\pm 1_n, \pm\eta$ *sont distincts, et donc* $|Z| = 4$.

(vii) *Montrer* $|G| = 2^{m-1}|Z|$. *On pourra montrer que tout élément de* G *s'écrit de manière unique sous la forme* zg_I *avec* $z \in Z$ *et* $I \subset \{1, \dots, m-1\}$.

Pour l'existence, il suffit d'observer que si $g = \pm g_I$ *avec* $I \subset \{1, \dots, m\}$ *et* $m \in I$, *alors* $\eta g = \pm g_{I'}$ *avec* $I' \subset \{1, \dots, m-1\}$ *par le (ii), puis* $g = \pm\eta g_{I'}$. *Montrons l'unicité. Supposons* $zg_I = z'g_J$ *avec* $z, z' \in Z$ *et* $I, J \subset \{1, \dots, m-1\}$. *On a alors* $z^{-1}z' = g_J g_I^{-1} \in Z$. *Mais* $g_J g_I^{-1} = \pm g_J g_I$ *est de la forme* $\pm g_K$ *avec* $K = (I \cup J) \smallsetminus (I \cap J)$. *Le (iv) montre donc que l'on a* $K = \{1, \dots, m\}$ *ou* $K = \emptyset$. *Le premier cas est impossible car on a* $m \notin K$. *On a donc* $K = \emptyset$, *i.e.* $I = J$, *puis* $z = z'$.

(viii) *Montrer que* G *a exactement* $|Z| + \frac{|G|-|Z|}{2} = 2^{m-2}|Z| + \frac{|Z|}{2}$ *classes de conjugaison.*

Tout élément $h \in Z$ *est sa propre classe de conjugaison : on a* $ghg^{-1} = h$ *pour tout* $g \in G$. *Et si* $\pm h$ *n'est pas dans* Z *on a vu au (iv) que sa classe de conjugaison est* $\{h, -h\}$. *Le nombre total de classes de conjugaison est donc bien* $|Z| + \frac{|G|-|Z|}{2} = \frac{|Z|}{2} + \frac{|G|}{2}$. *On conclut car on a vu* $|G| = 2^{m-1}|Z|$.

(ix) *Montrer* $\mathrm{D}(G) = \{\pm 1_n\}$.

On a $-1_n = g_1 g_2 g_1^{-1} g_2^{-1}$ *(on utilise ici* $m > 1$*) donc* -1_n *est dans* $\mathrm{D}(G)$. *Soit* $g = \pm g_I$ *et* $h \in G$. *Par le (v) on a* $hgh^{-1} = \pm g$, *et donc* $[h, g] = \pm 1_n$. *On a bien montré* $\mathrm{D}(G) = \{\pm 1_n\}$.

(x) *En déduire qu'il existe exactement* $|G|/2 = 2^{m-2}|Z|$ *morphismes de groupes* $G \to \mathbb{C}^\times$.

Tout morphisme de groupes $G \to \mathbb{C}^\times$ *est trivial sur* $\mathrm{D}(G)$ *car* $\mathbb{C}^\times$ *est abélien. Par la propriété universelle du quotient, c'est la même chose de se donner un morphisme de groupes* $G \to \mathbb{C}^\times$ *et un morphisme de groupes* $G/\mathrm{D}(G) \to \mathbb{C}^\times$. *Mais* $G/\mathrm{D}(G)$ *est abélien, donc il a exactement* $|G/\mathrm{D}(G)|$ *tels morphismes, par un théorème du cours. On conclut car on a* $|G/\mathrm{D}(G)| = |G|/2$.

(xi) *Montrer que l'unique solution de l'équation* $2^m = a^2 + b^2$ *avec* a, b *entiers* ≥ 1 *est* $a = b = 2^{\frac{m-1}{2}}$.

Si on a $2^m = a^2 + b^2$ *avec* m *impair, on a* a *et* b *pairs par réduction modulo 4, puis* $a = 2a'$, $b = 2b'$ *et* $2^{m-2} = (a')^2 + (b')^2$ *et on conclut par récurrence sur* m.

(xii) *Montrer qu'à isomorphisme près,* G *possède* $|Z|/2$ *représentations* $\mathbb{C}$*-linéaires irréductibles de dimension* > 1, *et qu'elles sont de dimension* $2^{\frac{m-1}{2}}$ *(on traitera d'abord le cas* $|Z| = 2$*).*

Supposons d'abord $|Z| = 2$ *comme indiqué. On a alors* $|G| = 2^m$ *par (vii) et* G *possède* $2^{m-1} + 1$ *classes de conjugaison par (viii). D'après Frobenius, on sait que* G *possède* $2^{m-1} + 1$ *représentations* $\mathbb{C}$*-linéaires irréductibles non isomorphes. Par le (x), il y en a* 2^{m-1} *de degré 1. Il n'en reste donc qu'une seule, disons de degré* d *(en fait, avec* $d > 1$*). Mais toujours par Frobenius, on sait que la somme des carrés des degrés des dimensions irréductibles vaut* $|G|$. *On a donc* $|G| = 2^m = 2^{m-1} \cdot 1^2 + d^2$, *puis* $d = 2^{(m-1)/2}$.

Supposons maintenant $|Z| = 4$. *On a cette fois-ci* $|G| = 2^{m+1}$ *par (vii),* G *a* $2^m + 2$ *représentations irréductibles non isomorphes par (viii), dont* 2^m *de degré 1 par (x), il en reste donc 2 de degré* $a, b > 1$ *à déterminer. Mais on a* $2^{m+1} = 2^m.1^2 + a^2 + b^2 + 1^2$, *et donc* $a^2 + b^2 = 2^m$, *puis* $a = b = 2^{\frac{m-1}{2}}$ *par le (xi).*

2. En fait, les deux cas peuvent se produire en général, donc on n'essaiera pas de monter qu'on est dans un cas où l'autre.

(xiii) *Montrer que la représentation naturelle de G sur $\mathbb{C}^n$ n'a aucune droite G-stable.*

Soit $D \subset \mathbb{C}^n$ une droite G-stable. Soit $\lambda_i \in \mathbb{C}^\times$ la valeurs propre de $g_i \in \mathrm{GL}_n(\mathbb{C})$ sur la droite de D. La relation $g_i g_j = -g_j g_i$ pour $i \neq j$ (et deux tels indices existent car $m > 1$) montre $\lambda_i \lambda_j = -\lambda_j \lambda_i$, ce qui est absurde dans $\mathbb{C}^\times$.

(xiv) *Montrer que l'on a $2^{\frac{m-1}{2}} \mid n$.*

D'après Maschke, il existe une décomposition $\mathbb{C}^n = \oplus_{k=1}^s U_k$ où les U_k sont des sous-espaces vectoriels de $\mathbb{C}^n$ qui sont G-stables et irréductibles comme représentation de G. On a $\dim U_k > 1$ pour tout k par le (xi), et donc $\dim U_k \equiv 0 \bmod 2^{\frac{m-1}{2}}$ par le (xiii). On en déduit que $n = \dim \mathbb{C}^n = \sum_k \dim U_k$ est multiple de $2^{\frac{m-1}{2}}$.

Partie 2

Soit E un espace euclidien de dimension $n > 1$, de norme euclidienne notée $||.||$. On suppose qu'il existe une application $\mathbb{R}$-bilinéaire $E \times E \to E$, $(x, y) \mapsto x \star y$, telle que pour tout $x, y \in E$ on ait

$$||x \star y||^2 = ||x||^2 \, ||y||^2.$$

On se propose de montrer que l'on a $n = 2, 4$ ou 8. On fixe une base orthonormée $\varepsilon_1, \ldots, \varepsilon_n$ de E.

(i) *Donner un exemple pour $n = 2$ et $n = 4$. (Bonus : une idée dans le cas $n = 8$?)*

Pour $n = 2$, on peut prendre $E = \mathbb{C}$ muni de sa norme euclidienne $z \mapsto |z|^2$ et $\star$ la multiplication usuelle dans $\mathbb{C}$. Pour $n = 4$, on peut prendre $E = \mathbb{H}$ muni de sa norme n, et $\star$ la multiplication sur les quaternions (l'hypothèse est satisfaite par multiplicativité de la norme). Pour $n = 8$, il faudrait considérer les octonions de Cayley et Graves, dont la norme est aussi euclidienne et multiplcative.

(ii) *Pour $x \in E$ on note $\mathrm{m}_x : E \to E$ l'application linéaire $y \mapsto x \star y$, et $\mathrm{M}(x) \in \mathrm{M}_n(\mathbb{R})$ la matrice de m_x dans la base des ε_i. Montrer ${}^{\mathrm{t}}\mathrm{M}(x)\,\mathrm{M}(x) = ||x||^2 \, 1_n$ pour tout $x \in E$.*

C'est clair pour $x = 0$ donc on suppose $x \neq 0$. Par hypothèse, m_x est une similitude orthogonale de rapport $||x||^2$, ce qui conclut. On peut aussi dire que si $||x|| = 1$ alors on a $\mathrm{m}_x \in \mathrm{O}(E)$, donc $\mathrm{M}(x) \in \mathrm{O}(n)$. Pour $||x|| = \lambda > 0$, on a $\mathrm{m}_{x/\lambda} = \frac{1}{\lambda}\mathrm{m}_x$ par bilinéarité de $\star$, et donc $\frac{1}{||x||}\mathrm{M}(x) \in \mathrm{O}(n)$.

(iii) *En déduire $\mathrm{M}(\varepsilon_i) \in \mathrm{O}(n)$ et ${}^{\mathrm{t}}\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j) + {}^{\mathrm{t}}\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_i) = 0$ pour $i \neq j$.*

On a $||\varepsilon_i|| = 1$ donc $\mathrm{M}(\varepsilon_i) \in \mathrm{O}(n)$ par la question précédente. Pour $x = \varepsilon_i + \varepsilon_j$ avec $i \neq j$, on a $||x||^2 = 2$, mais aussi $\mathrm{M}(\varepsilon_i + \varepsilon_j) = \mathrm{M}(\varepsilon_i) + \mathrm{M}(\varepsilon_i)$ par linéarité de $x \mapsto \mathrm{m}_x$. En appliquant la question précédente à $\varepsilon_i, \varepsilon_j$ et $\varepsilon_i + \varepsilon_j$, on trouve la formule annoncée.

(iv) *On pose $g_i = \mathrm{M}(\varepsilon_i)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) \in \mathrm{O}(n)$. Vérifier, pour tout $1 \leq i \neq j \leq n-1$, les relations*

$$g_i^2 = -1_n \text{ et } g_i g_j = -g_j g_i.$$

C'est un calcul direct à partir de la question précédente : pour $i, j < n$ on a

$$g_i g_j = \mathrm{M}(\varepsilon_i)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n)\mathrm{M}(\varepsilon_j)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) = -\mathrm{M}(\varepsilon_i){}^{\mathrm{t}}\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_n)\,{}^{\mathrm{t}}\mathrm{M}(\varepsilon_n) = -\mathrm{M}(\varepsilon_i){}^{\mathrm{t}}\mathrm{M}(\varepsilon_j) = -\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j)^{-1}.$$

On a donc $g_i^2 = -1_n$. Pour $i \neq j$, on a par le (iii) l'égalité $\mathrm{M}(\varepsilon_i)^{-1}\mathrm{M}(\varepsilon_j) = -\mathrm{M}(\varepsilon_j)^{-1}\mathrm{M}(\varepsilon_i)$, qui s'écrit aussi $\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_i)^{-1} = -\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j)^{-1}$, et donc $g_i g_j = -g_j g_i$.

(v) *Montrer que n est pair.*

On a $g_i^2 = -1_n$ avec $g_i \in \mathrm{O}_n(\mathbb{R})$. On en déduit $1 = (\det g_i)^2 = (-1)^n$, puis n pair.

(vi) *Conclure, et expliquer pourquoi nous avons bien résolu la question initiale !*

On peut supposer $n > 2$. On est dans la situation de la Partie 1 avec $m = n-1$, qui est impair par la question (v). On en déduit que $2^{\frac{n-2}{2}}$ divise n, et en particulier l'inégalité $2^{\frac{n}{2}} \leq 2n$. On a égalité pour $n = 8$, mais la suite $x_n = 2^{\frac{n}{2}}$ croît plus vite que $y_n = 2n$ pour $n \geq 8$: on a $x_{n+1}/x_n = \sqrt{2}$ et $y_{n+1}/y_n \leq 1 + 1/8 < \sqrt{2}$. On a donc $n \leq 8$. Le cas $n = 6$ est exclus car $2^2 = 4$ ne divise pas 6.

On a bien répondu à la question initiale : si on a $z_k \in \mathbb{R}[x_1, \ldots, x_n, y_1, \ldots, y_n]$ pour $k = 1, \ldots, n$ comme dans la partie 1, la formule $(x_i) \star (y_i) = (z_k(x_1, \ldots, x_n, y_1, \ldots, y_n))$ définie une loi de composition sur l'espace euclidien standard $\mathbb{R}^n$. Elle est $\mathbb{R}$-bilinéaire car les z_k ne contiennent que des monômes de la forme $x_i y_j$, et elle vérifie $||x \star y||^2 = ||x||^2 ||y||^2$ par l'identité remarquable.

Problème 2. (Une caractérisation de $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$, suivant Zassenhaus)

Soit p un nombre premier. Un théorème de Zassenhauss affirme que si G est un sous-groupe d'ordre $p^3 - p = p(p-1)(p+1)$ de S_{p+1} agissant transitivement sur $\{1, 2, \ldots, p+1\}$, alors G est isomorphe au groupe $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$. Dans la première partie, on se propose de démontrer ce résultat sous l'hypothèse supplémentaire $p \equiv 3 \bmod 4$. Dans la seconde partie, indépendante, nous en donnons une application.

Partie 1

On considère l'ensemble[3] $X = \mathbb{Z}/p\mathbb{Z} \coprod \{\infty\}$, *qui a $p+1$ éléments. On rappelle que le groupe $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ s'identifie naturellement au sous-groupe $\mathcal{H}_X \subset \mathrm{S}_X$ des homographies de X, c'est-à-dire des bijections de X de la forme*

$$x \mapsto \frac{ax+b}{cx+d}, \quad \text{avec} \quad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}).$$

On note aussi $\mathrm{Aff}_X \subset \mathcal{H}_X$ le sous-groupe des homographies g telles que $g(\infty) = \infty$, i.e. de la forme $g(x) = ax + b$, avec $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ et $b \in \mathbb{Z}/p\mathbb{Z}$ (homographies « affines »).

(i) *Rappeler pourquoi on a $|\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})| = p^3 - p$.*

Comme on l'a vu en cours, le nombre de bases du $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $(\mathbb{Z}/p\mathbb{Z})^2$ est $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2-1)(p^2-p)$. On conclut car $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ est par définition le quotient du groupe $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ par son centre $(\mathbb{Z}/p\mathbb{Z})^\times$, d'ordre $p-1$.

(ii) *Montrer que $\mathcal{H}_X$ est engendré par l'homographie $x \mapsto 1/x$ et son sous-groupe Aff_X.*

Soit H le sous-groupe de $\mathcal{H}_X$ engendré par Aff_X et l'homographie $g(x) = 1/x$. Soit $f \in \mathcal{H}_X$. Si on a $f(\infty) = \infty$ alors $f \in \mathrm{Aff}_X \subset H$. Sinon, on a $f(\infty) = k$ avec $k \in \mathbb{Z}/p\mathbb{Z}$. Soit $t \in \mathrm{Aff}_X$ l'homographie $t(x) = x - k$. Alors $g\,t\,f$ envoie ∞ sur ∞, et donc $g\,t\,f \in H$, puis $t\,f \in H$ car $g^{-1} \in H$, puis $f \in H$ car $t^{-1} \in H$.

(iii) *Montrer que Aff_X agit 2-transitivement sur $\mathbb{Z}/p\mathbb{Z}$.*

(Rappel : Un groupe G agit k-transitivement sur un ensemble X si on a $|X| \geq k$ et si G agit transitivement sur l'ensemble Y des k-uples de la forme $(x_1, x_2, \ldots, x_k)$, où les x_i sont distincts et dans X. Il suffit de montrer que la G-orbite d'un k-uple donné est tout Y.) On a bien $|\mathbb{Z}/p\mathbb{Z}| = p \geq 2$. Pour montrer la 2-transitivité de Aff_X sur $\mathbb{Z}/p\mathbb{Z}$, il suffit donc de voir que si u et v sont deux éléments distincts de $\mathbb{Z}/p\mathbb{Z}$, il existe $h \in \mathrm{Aff}_X$ tel que $h(0) = u$ et $h(1) = v$. Mais $h(x) := (v-u)x+u$ convient.

3. Cet ensemble est aussi noté $\widehat{\mathbb{Z}/p\mathbb{Z}}$ dans le cours, où on l'a identifié à la droite projective $\mathrm{P}^1(\mathbb{Z}/p\mathbb{Z})$.

Soit G un sous-groupe de S_X de cardinal p^3-p et agissant transitivement sur X. On veut montrer qu'il existe $\sigma \in \mathrm{S}_X$ tel que $\sigma G \sigma^{-1} = \mathcal{H}_X$. On note $\alpha \in \mathrm{Aff}_X$ la translation $x \mapsto x+1$.

(iv) Montrer que G possède un p-cycle.

On a $p \mid |G|$, donc G possède un élément g d'ordre p par Cauchy. On sait que l'ordre d'une permutation dans un groupe symétrique est le ppcm des longueurs de ses cycles. Ainsi, une permutation d'ordre premier p est un produit de p-cycles à supports disjoints. Comme on a $|X| = p+1 < 2p$, la seule possibilité est que g soit un p-cycle.

(v) En déduire qu'il existe $\sigma \in \mathrm{S}_X$ tel que $\sigma G \sigma^{-1}$ contient α, puis que l'on peut supposer $\alpha \in G$.

On constate que α est le p-cycle $(0\,1\,2\,\ldots,p-1)$. Soit $g \in G$ un p-cycle (question (iv)). Comme deux p-cycles sont conjugués dans S_X, on en déduit qu'il existe $\sigma \in \mathrm{S}_X$ tel que $\sigma g \sigma^{-1} = \alpha$. Le conjugué $\sigma G \sigma^{-1}$ a même cardinal que G, contient α, et agit transitivement sur X (si g envoit $\sigma^{-1}(x)$ sur $\sigma^{-1}(y)$, alors $\sigma g \sigma^{-1}$ envoit x sur y).

On suppose désormais $\alpha \in G$. On veut montrer $G = \mathcal{H}_X$. On note $G_\infty \subset G$ le stabilisateur de $\infty \in X$ dans G.

(vi) Monter $|G_\infty| = p^2 - p$.

Comme G agit transitivement sur X, la formule orbite stabilisateur montre $|G| = |G_\infty||X|$, et donc $|G_\infty| = (p^3-p)/(p+1) = p^2-p$.

(vii) Montrer que $P = \langle \alpha \rangle$ est l'unique sous-groupe d'ordre p de G_∞, puis que l'on a $P \triangleleft G_\infty$.

Comme $|G_\infty| = p(p-1)$, les sous-groupes d'ordre p de G_∞, comme le sous-groupe P, sont ses p-Sylow. D'après les théorèmes de Sylow, le nombre de p-Sylow de G_∞ est un diviseur d de $p-1$ qui vérifie $d \equiv 1 \bmod p$. On a donc soit $d=1$, soit $d \geq p+1$: absurde. Ainsi, G_∞ possède un unique p-Sylow, qui comme on le sait est alors distingué (il est égal à ses conjugués).

(viii) En déduire que pour tout $g \in G_\infty$, il existe un entier $1 \leq a < p$ tel que $g\alpha = \alpha^a g$.

Soit $g \in G_\infty$. On a vu que $\langle \alpha \rangle$ est distingué dans G_∞. On a donc $g\alpha g^{-1} = \alpha^a$ avec $0 \leq a < p$. Mais $a = 0$ est impossible, sinon on aurait $g\alpha g^{-1} = 1$ puis $\alpha = 1$: absurde.

(ix) Montrer $G_\infty \subset \mathrm{Aff}_X$, puis $G_\infty = \mathrm{Aff}_X$.

Soit $g \in G_\infty$. On a vu qu'il existe un entier $1 \leq a < p$ avec $g\alpha = \alpha^a g$. Cela sécrit aussi $g(x+1) = g(x) + a$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$. Posons $b = g(0) \in \mathbb{Z}/p\mathbb{Z}$. On a donc $g(1) = a+b$, $g(2) = g(1)+a = 2a+b$, et par récurrence immédiate, $g(x) = ax+b$ pour tout $x \in \mathbb{Z}/p\mathbb{Z}$. On a montré $g \in \mathrm{Aff}_X$. L'égalité $G_\infty = \mathrm{Aff}_X$ en découle car $|G_\infty| = |\mathrm{Aff}_X| = p^2-p$ (question (vi)).

(x) En déduire que G agit 3-transitivement sur X.

On a $|X| = p+1 \geq 3$. Il faut montrer que pour tout x,y,z distincts dans X, il existe g dans G tel que $(g(0), g(1), g(\infty)) = (x,y,z)$. Comme G agit transitivement sur X, on peut trouver $h \in G$ avec $h(z) = \infty$. Quitte à remplacer (x,y,z) par $(h(x), h(y), h(z))$, ce qui est loisible, on peut donc suppser $z = \infty$. Mais alors on conclut par 2-transitivité de $G_\infty = \mathrm{Aff}_X$ sur $\mathbb{Z}/p\mathbb{Z}$ (question (iii)).

(xi) Montrer que si $g \in G$ fixe 3 points distincts dans X, alors $g = 1$ (on se ramenera au cas $g \in G_\infty$).

Soit $g \in G$ fixant 3 points distincts x,y,z de X. On veut montrer $g = 1$. Quitte à remplacer g par hgh^{-1} avec $h \in G$, qui fixe $h(x), h(y), h(z)$ et qui est trivial si et seulement si g l'est, on peut supposer $(x,y,z) = (0,1,\infty)$ par ce qu'on vient de démontrer. Mais alors on a $g \in G_\infty = \mathrm{Aff}_X$,

et donc $g(x) = ax + b$, puis $b = g(0) = 0$ (car g fixe 0) et enfin $a = g(1) = 1$ (car g fixe 1), donc $g = 1$.

On pose $C = \{g \in G_\infty \mid g(0) = 0\}$ et $C' = \{g \in \mathrm{S}_X \mid gc = cg \ \forall c \in C\}$ (centralisateur de C dans S_X). On fixe $\gamma \in G$ tel que $\gamma(0) = \infty$, $\gamma(1) = 1$ et $\gamma(\infty) = 0$ (on justifiera l'existence de γ).

(xii) Montrer que C est cyclique d'ordre $p-1$, et qu'il est engendré par un $p-1$ cycle.

On a démontré $G_\infty = \mathrm{Aff}_X$ (question (ix)). Ainsi, C est l'ensemble des homographies de la forme $m_a(z) = az$ avec $a \in (\mathbb{Z}/p\mathbb{Z})^\star$. L'application $a \mapsto \mathrm{m}_a, (\mathbb{Z}/p\mathbb{Z})^\times \to C$, est manifestement un isomorphisme de groupes. D'après le théorème de Gauss, on en déduit que $C \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique d'ordre $p-1$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$. Alors $\mathrm{m}_g \in C$ est le $p-1$-cycle $(1\, g\, g^2, \dots\, g^{p-1})$.

(xiii) En déduire que C' est engendré par C et la transposition $(0\,\infty)$.

Comme C fixe 0 et ∞, et C est commutatif, on a $C \subset C'$ et $(0\,\infty) \in C'$. Supposons réciproquement g est dans C'. Écrivons $C = \langle c \rangle$ avec c un $p-1$ cycle. Comme g commute à c, il préserve l'ensemble des points fixes de c, qui sont $\{0, \infty\}$. Quitte à multiplier g par (0∞), on peut donc supposer que g fixe 0 et ∞. Si $c = (i_1, \dots, i_{p-1})$ on a aussi $c = gcg^{-1} = (g(i_1), g(i_2), \dots, g(i_{p-1}))$. Mais quitte à remplacer g par gc^k avec $k \in \mathbb{Z}$, on peut supposer $g(i_1) = i_1$, mais alors on a aussi $g(i_k) = i_k$ pour tout $k > 1$, puis $g = 1$.

(xiv) Montrer que si G contient une transposition, ou si $p \leq 3$, on a $G = \mathrm{S}_X = \mathcal{H}_X$.

Si G contient une transposition, il contient tout ses conjugués, et donc toutes les transpositions par 2-transitivité de G sur X. On a donc $G = \mathrm{S}_X$. On conclut car on a $|G| = |\mathcal{H}_X| = |\mathrm{S}_X|$ si, et seulement si, $(p-1)p(p+1) = (p+1)!$, i.e. $p - 2 \leq 1$.

On peut donc supposer $(0\,\infty) \notin G$ et $p > 3$.

(xv) Montrer $C' \cap G = C$.

En effet, on a $C \subset C' \cap G$. Réciproquement, comme $(0\,\infty)$ et C commutent, un élément de C' non dans C est de la forme $(0\,\infty)c$ avec $c \in C$. Ainsi, si un tel élément est dans G, on a $(0\,\infty) \in G$, une contradiction.

(xvi) Montrer que $\mathrm{int}_\gamma : G \to G, g \mapsto \gamma g \gamma^{-1}$, induit un automorphisme d'ordre 2 de C.

Pour $c \in C$ on a $c(0) = 0$ et $c(\infty) = \infty$, donc $\gamma c \gamma^{-1}$ fixe aussi 0 et ∞. Ainsi, l'automorphisme int_γ de G préserve C. Il est non trivial car sinon on aurait $\gamma \in C' \cap G = C$: absurde car γ ne fixe pas ∞. Enfin, l'élément γ^2 fixe 0 et ∞, donc est dans C, qui est commutatif, et donc $(\mathrm{int}_\gamma)^2 = \mathrm{int}_{\gamma^2}$ est l'identité de C.

(xvii) Montrer qu'il existe un entier $1 < n < p-1$ avec $n^2 \equiv 1 \bmod p-1$ et $\gamma c \gamma^{-1} = c^n$ pour tout $c \in C$.

Comme C est cyclique d'ordre $p-1$, tout automorphisme de C est de la forme $c \mapsto c^n$ avec $n \in (\mathbb{Z}/(p-1)\mathbb{Z})^\times$, d'après un théorème du cours. S'il est d'ordre 2, on a $c^{n^2} = c$ pour tout c dans C, et donc $n^2 \equiv 1 \bmod p-1$ en considérant un élément c d'ordre $p-1$ dans C. De plus, s'il est non trivial on a $n \not\equiv 1 \bmod p-1$.

(xviii) (suite) Montrer $\gamma(x) = x^n$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times \subset X$.

On a $\gamma c = c^n \gamma$. Soit g un générateur de $(\mathbb{Z}/p\mathbb{Z})^*$. Cette identité appliquée à $c = \mathrm{m}_g$ s'écrit $\gamma(gx) = g^n \gamma(x)$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. On en déduit $\gamma(g^k) = g^{nk}\gamma(1)$ pour tout $k \in \mathbb{Z}$. Mais on a $\gamma(1) = 1$ par hypothèse. On a donc $\gamma(x) = x^n$ pour tout $x \in (\mathbb{Z}/p\mathbb{Z})^\times$.

(xix) *(suite) En considérant les point fixes de γ dans X, montrer $n+1 \equiv 0 \bmod \frac{p-1}{2}$.*

Comme $\gamma \neq 1$, on sait que γ a au plus 2 points fixes dans $(\mathbb{Z}/p\mathbb{Z})^\times$. Ces points fixes sont nécessairement 1 et -1 (noter $p > 2$ et donc n impair). On en déduit que le noyau de l'application $\mathbb{Z}/(p-1)\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}, k \mapsto (n-1)k$ est $\{0, \frac{p-1}{2}\}$. Cela implique que $\frac{n-1}{2}$ et premier avec $\frac{p-1}{2}$. Mais $\frac{p-1}{2}$ divise $\frac{n^2-1}{2} = \frac{n-1}{2}(n+1)$, et on conclut.

(xx) *(suite) On suppose enfin $p \equiv 3 \bmod 4$. Montrer $n \equiv -1 \bmod p-1$.*

On a n impair car $n^2 \equiv 1 \bmod p-1$. Par le (xix), on a soit $n \equiv -1 \bmod p-1$, soit $n \equiv \frac{p-1}{2} - 1 = \frac{p-3}{2} \bmod p-1$. Ce second cas est exclus car n est pair.

(xxi) *En déduire que si $p \equiv 3 \bmod 4$ on a $G = \mathcal{H}_X$.*

On a montré $\gamma(x) = 1/x$. Comme γ et $\mathrm{Aff}_X = G_\infty$ sont dans G, on a $\mathcal{H}_X \subset G$ par la question (ii), puis égalité pour des raisons de cardinal.

Partie 2

Dans cette seconde partie, indépendante, nous donnons des applications du résultat principal de la Partie 1 *(que l'on pourra donc admettre). On suppose d'abord que G est un groupe d'ordre $p^3 - p$, avec p premier, et que G ne possède pas de sous-groupe distingué H non trivial avec $|H| \mid p^2 - p$. On note X l'ensemble des sous-groupes d'ordre p de G, et on fait agir G sur X par conjugaison.*

(i) *Soit $d \geq 1$ un diviseur de $p^2 - 1$ avec $d \equiv 1 \bmod p$. Montrer $d = 1$ ou $d = p+1$.*

On a $p^2 - 1 = dd'$ avec $d, d' \geq 1$ et $d \equiv 1 \bmod p$, et donc $d' \equiv -1 \bmod p$. On en déduit $d' \geq p-1$. Si $d > 1$, on a $d \geq p+1$ et la seule possibilité est donc $d = p+1$ et $d' = 1$.

(ii) *En déduire $|X| = p+1$.*

Les sous-groupes d'ordre p de G sont ses p-Sylow car on a $|G| = p(p^2-1)$. Leur nombre d est un diviseur de $p^2 - 1$ par les théorèmes de Sylow, avec en outre $d \equiv 1 \bmod p$. On a donc $d = 1$ ou $d = p+1$ par le (i). Si $d = 1$, alors l'unique p-Sylow P de G est distingué, et de cardinal $p \mid p^2 - p$: absurde.

(iii) *Montrer que l'action de G sur X est transitive et fidèle.*

On sait que les p-Sylow de G sont conjugués, donc l'action de G sur X est transitive. Son noyau est un sous-groupe distingué de G inclus dans le stabilisateur d'un point de X, qui est d'ordre $|G|/|X| = p^2 - p$ par transitivité et formule orbite stabilisateur. Cela contredit l'hypothèse sur G par Lagrange.

(iv) *On suppose $p \equiv 3 \bmod 4$. Montrer que l'on a un isomorphisme $G \simeq \mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Le morphisme $G \to \mathrm{S}_X$ associé à l'action étant injectif, G est isomorphe à un sous-groupe de $\mathrm{S}_X \simeq \mathrm{S}_{p+1}$ agissant transitivement sur X, et d'ordre $p^3 - p$. Il est donc isomorphe à $\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})$ par le théorème de Zassenhaus.

On considère enfin les groupes $H = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ et $G = H \rtimes_\psi \mathbb{Z}/2\mathbb{Z}$, où $\psi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(H)$ est le morphisme envoyant l'élément non trivial de $\mathbb{Z}/2\mathbb{Z}$ sur l'automorphisme $h \mapsto {}^t h^{-1}$ de H (d'ordre 2).

(v) *Rappeler pourquoi H est un groupe simple, et montrer $|H| = 168$.*

On sait que $\mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z})$ est simple par le cours. Mais on a $\mathrm{SL}_3(\mathbb{Z}/2\mathbb{Z}) = \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ car $(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$, et pour la même raison le centre de ce groupe est trivial, donc on a $G \simeq \mathrm{PSL}_3(\mathbb{Z}/2\mathbb{Z}) \simeq \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. On sait que son cardinal est $(2^3-1)(2^3-2)(2^3-2^2) = 7 \cdot 6 \cdot 4 = 168$.

(vi) *Montrer qu'il n'existe aucun élément $M \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$ tel que ${}^t hMh = M$ pour tout $h \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.*

(Une preuve parmi d'autres) Un tel $M = (m_{i,j})$ commute à toutes les matrices de permutation $\mathrm{S}_3 \subset \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. Comme on a $\sigma(m_{i,j})\sigma^{-1} = (m_{\sigma(i),\sigma(j)})$, et que S_3 est 2-transitif, on en déduit que tous les $m_{i,i}$ sont égaux (à 0 ou 1) et de même que tous les autres coefficients sont égaux (à 0 ou 1). L'inversibilité de M implique alors $M = 1_3$, et donc ${}^t hh = 1_3$ pour tout $h \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$. C'est faux pour une transvection standard.

(vii) *En déduire que G ne possède pas de sous-groupe distingué d'ordre 2.*

Soit $N \subset G$ un sous-groupe distingué et d'ordre 2. Alors N n'est pas inclus dans le sous-groupe $H \subset G$, qui est simple. Donc N est engendré par un élément de la forme $g = (M, \overline{1})$ avec $M \in H$. On a nécessairement $hgh^{-1} = g$ pour tout h dans G. Utilisons simplement $(h,0)g = g(h,0)$ pour tout h dans H. On trouve $hM = M{}^t h^{-1}$ pour tout h dans H, une contradiction par la question (vi).

(viii) *Montrer que les seuls sous-groupes distingués de G sont $\{1\}, G$ et $H \times \{\overline{0}\} \simeq H$.*

On rappelle qu'on a une suite exacte naturelle $1 \to H \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$. En particulier, H est distingué (et d'indice 2) dans G. Soit N un sous-groupe distingué quelconque de G. Alors $N \cap H$ est distingué dans H, qui est simple. On a donc $N \cap H = \{1\}$ ou $H \supset N$. Dans le second cas, on a $N = G$ ou $N = H$ car H est d'indice 2. Dans le premier cas la projection $N \to \mathbb{Z}/2\mathbb{Z}$ est injective, donc $|N| \leq 2$, et on conclut par le (vii).

(ix) *En déduire $G \simeq \mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$, puis $H \simeq \mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$.*

On a $|G| = 2.|H| = 2.168 = 336 = 7^3 - 7$ avec $7 \equiv 3 \bmod 4$ premier. De plus, G n'a pas de sous-groupe distingué d'ordre divisant $7^2 - 7 = 42$ par le (viii). On a donc $G \simeq \mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$ par le (iv). Le sous-groupe distingué $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$ d'indice 2 de $\mathrm{PGL}_2(\mathbb{Z}/7\mathbb{Z})$ est donc isomorphe à un sous-groupe distingué d'indice 2 de G, i.e. à H.