Examen du cours d'Algèbre 1, ENS Ulm, 19 Janvier 2022

Aucun document n'est autorisé. Temps de composition : 3h. Il n'est pas du tout nécessaire de traiter toutes les questions pour avoir le maximum des points. On soignera la rédaction.

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* $x_i y_j$*, 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]

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

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* $\eta = g_{\{1,\dots,m\}} = g_1 g_2 \cdots g_m \in G$*. 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* $n = 2$*.*

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

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

(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.*

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

(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]

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

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

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

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

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

(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 commencera par traiter le cas* $|Z| = 2$*).*

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

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

1. Bien entendu, 1_n désigne ici la matrice identité de $\mathrm{M}_n(\mathbb{C})$.
2. En fait, les deux cas peuvent se produire en général, donc on n'essaiera pas de montrer qu'on est dans un cas ou l'autre.

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 pour $n = 4$. (Bonus : une idée dans le cas $n = 8$?)

(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 $x \in E$.

(iii) En déduire $\mathrm{M}(\varepsilon_i) \in \mathrm{O}(n)$ pour tout $i = 1, \ldots, n$, et ${}^{\mathrm{t}}\mathrm{M}(\varepsilon_i)\mathrm{M}(\varepsilon_j) + {}^{\mathrm{t}}\mathrm{M}(\varepsilon_j)\mathrm{M}(\varepsilon_i) = 0$ pour $i \neq j$.

(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

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

(v) Montrer que n est pair.

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

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

Soit p un nombre premier. 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 $|\mathrm{PGL}_2(\mathbb{Z}/p\mathbb{Z})| = p^3 - p$.

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

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

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 $x \mapsto x + 1$.

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

(iv) *Montrer que G possède 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 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 $|G_\infty| = p^2 - p$.*

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

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

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

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

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

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.*

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

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

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

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

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

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

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

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

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

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 $d = p + 1$.*

(ii) *En déduire $|X| = p + 1$.*

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

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

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* $|H| = 168$.

(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* $h \in \mathrm{GL}_3(\mathbb{Z}/2\mathbb{Z})$.

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

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

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