Université Claude Bernard Lyon 1

MASTER M1 Recherche

Groupes Classiques et Géométrie

Correction de l'examen, 1ère session

24 Mai 2012

Problème 1. 1) a) Comme $\mathbb{Z}/p\mathbb{Z}$ est un groupe, il est stable par l'addition par k et les axiomes de l'action sont bien vérifiées. On a donc défini une action de $\mathbb{Z}/p\mathbb{Z}$ sur $\mathbb{F}_q^p$. De plus, la somme reste la même par permutation donc l'action se restreint sur X.

b) Les orbites à un élément correspondent à des p-uplets stables par $\mathbb{Z}/p\mathbb{Z}$. Soit (x_i) un tel p-uplet. Alors, $k.(x_i) = (x_i)$ implique que $x_{i+k} = x_i$ pour tout k. Ainsi, toutes les composantes sont égales.

c) Comme p est non nul modulo q, ce nombre est égal à 2 si p est un carré modulo q et 0 sinon. Donc le nombre de solutions coïncide avec $1 + \left(\begin{matrix} p \\ q \end{matrix}\right)$.

d) C'est la formule des classes : X est réunion disjointe d'orbites toutes en bijection avec un quotient de $\mathbb{Z}/p\mathbb{Z}$ par le stabilisateur d'un élément. Mais comme $\mathbb{Z}/p\mathbb{Z}$ est simple, le stabilisateur est soit tout le groupe, et dans ce cas on a une orbite singletonne comme dans le 1b), soit le stabilisateur est trivial et dans ce cas l'orbite est de cardinal p. Donc, modulo p, $|X|$ est égal au nombre d'orbites singletonnes, donc au nombre de solutions de l'équation $px^2 = 1$. D'où le résultat d'après c)

2) a) Le déterminant de A se calcule par blocs, on a $\det A = (-1)^{\frac{p-1}{2}} a = 1$. Donc, A et Id ont même discriminant (non nul) et donc elles sont congruentes.

b) Y est l'ensemble es y tels que $q(y) = 1$ où q est la forme quadratique qui a pour matrice A dans la base canonique de $\mathbb{F}_q^p$. On a ${}^tYAY = {}^tY^tPPY = {}^t(PY)Id(PY)$. On voit donc que $X \mapsto P^{-1}X$ fournit la bijection voulue.

c) Tout point d'Un hyperplan affine fournit une bijection avec son hyperplan vectoriel associé. Son nombre de points est égal à q puissance la dimension, c'est à dire q^{d-1}.

d) On calcule le cardinal de Y en fixant $(y_1, \dots, y_{\frac{p-1}{2}})$. Si $(y_1, \dots, y_{\frac{p-1}{2}}) = 0$, alors le nombre de solutions à l'équation définissant Y est $1 + \left(\begin{matrix} a \\ q \end{matrix}\right)$, comme dans 1)c). Sinon, alors chaaque x_p de $\mathbb{F}_q$ fournit un hyperplan affine

$$\{(z_i),\ 2(y_1 z_1 + \dots y_{\frac{p-1}{2}} z_{\frac{p-1}{2}}) = 1 - a x_p^2\} \in \mathbb{F}_q^{\frac{p-1}{2}}.$$

Il y a donc en tout dans Y

$$|Y| = q^{\frac{p-1}{2}}\left(1 + \left(\begin{matrix} a \\ q \end{matrix}\right)\right) + (q^{\frac{p-1}{2}} - 1)q^{\frac{p-1}{2}-1}q,$$

où dans le second terme, le premier facteur correspond au choix des y, le second au choix des z et le troisième au choix de x_p. On trouve finalement $|Y| = q^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} + q^{p-1}$.
3) En comparant les résultats de 2d) et 1)c), on a modulo p

$$1 + \binom{p}{q} = q^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\frac{q-1}{2}} + q^{p-1}.$$

En utilisant Fermat, on a $q^{p-1} = 1$. Donc, après simplification et utilisations des formules du symbole de Legendre, on a bien la loi de réciprocité annoncée. Attention, elle est dans $\mathbb{Z}/p\mathbb{Z}$. Mais comme p est impair et que les deux membres sont égaux à 1 ou à -1, cette égalité est valable dans $\mathbb{Z}$.
4)

$$\binom{27}{47} = \binom{3}{47}^3 = \binom{3}{47} = \binom{47}{3}(-1)^{1\times 23} = -\binom{2}{3} = 1.$$

Donc, 27 est un carré modulo 47.
5) Le cardinal de X pour $p = 2n+1$ vaut bien $q^n(q^n + (-1)^{n\frac{q-1}{2}})$. D'autre part, on sait que $O(2n+1, \mathbb{F}_q)$ agit sur la quadrique X et de façon transitive par le théorème de Witt. Soit x un élément de X, et g un élément du stabilisateur. Comme x est non isotrope (la forme quadratique q n'est pas nulle sur x), il en résulte que la droite engendrée par x est supplémentaire avec son orthogonal : $\mathbb{F}_q^{2n+1} = \langle x \rangle \oplus \langle x \rangle^{\perp}$. De plus le discriminant de la forme q' égale à q restreinte à $\langle x \rangle^{\perp}$ vérifie $\mathrm{d}isc(q\mid_{\langle x \rangle})\mathrm{d}isc(q') = \mathrm{d}isc(q)$, et comme $\mathrm{d}isc(q\mid_{\langle x \rangle}) = 1$, on a que q' est de discriminant 1. On a que le stabilisateur de x est isomorphe au stabilisateur de la forme q' et donc isomorphe à $O(2n, \mathbb{F}_q)$. Ce qui donne le résultat voulu.

Problème 2. A. 1) Soit φ l'application de $\mathbb{R}^4$ dans $\mathbb{R}$ qui envoie (x, y, z, t) sur $x^2 + y^2 - z^2 - t^2$. Sa différentielle en (x, y, z, t) est la forme linéaire de $\mathbb{R}^4$ qui a pour matrice $(2x, 2y, 2z, 2t)$ dans la base canonique. Elle est donc surjective en tout point non nul. En particulier, elle est surjective sur $\mathcal{C}$. Le théorème de submersion assure que $\mathcal{C}$ est une sous-variété de dimension $4 - 1 = 3$.
2) L'intersection est homéomorphe (via une projection) au cercle d'équation $x^2 + y^2 = 1$. Comme le cercle est connexe, il existe un arc de $\mathcal{C}$ qui relie deux points de l'intersection. En particulier les points $(1, 0, 0, 0)$ et $(-1, 0, 0, 0)$ sont dans la même composante connexe de $\mathcal{C}$.
3) Le théorème de Witt assure que $O(q)$ agit transitivement sur les nappes quadratiques de la forme quadratique q. On applique le théorème à la forme $q = x^2 + y^2 - z^2 - t^2$. Comme l'action est continue, un connexe maximal de $\mathcal{C}$ est envoyé sur un connexe maximal de $\mathcal{C}$. Donc, $O(2, 2)$ agit sur l'ensemble des composantes connexes de $\mathcal{C}$. Or l'identité de $O(2, 2)$ agit trivialement, et donc si $\mathcal{C}'$ est une composante connexe de $\mathcal{C}$, l'image de $SO_0(2, 2) \times \mathcal{C}'$ pour l'action continue est un connexe qui intersecte $\mathcal{C}'$, donc égal à $\mathcal{C}'$. Ainsi, $SO_0(2, 2)$ agit trivialement sur l'ensemble des composantes connexes de $\mathcal{C}$. D'où une action par

passage au quotient de $O(2,2)/SO_0(2,2)$ sur les composantes connexes de $\mathcal{C}$.
4) On sait d'après le cours que les matrices diagonales $diag(1,1,1,1)$, $diag(-1,1,1,1)$, $diag(1,1,1,-1)$, $diag(-1,1,1,-1)$ sont des représentants de $O(2,2)/SO_0(2,2)$ dans $O(2,2)$. Le point $(1,0,0,0)$ a pour image $(1,0,0,0)$, $(-1,0,0,0)$, $(1,0,0,0)$, $(-1,0,0,0)$ par ces quatre éléments. Donc, d'après 3) les composantes connexes de $\mathbb{C}$ sont celles de ces quatre points (en fait deux !). D'après, 2) ces deux points sont dans une même composante connexe. Conclusion, $\mathcal{C}$ est connexe.

B. 1) Le calcul donne directement que $U(1,1)$ est l'ensemble des matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ telles que $|a|^2 - |b|^2 = 1$, $|c|^2 - |d|^2 = -1$ et $\bar{a}c - \bar{b}d = 0$. Cette dernière équation donne que les vecteurs (c,d) et $(\bar{a},\bar{b})$ sont proportionnels et on peut poser $(c,d) = \lambda(\bar{a},\bar{b})$. Le resultat en découle aussitôt.
2) a) Le déterminant de la matrice obtenue est λ et donc $SU(1,1)$ est homéomorphe à $\mathcal{C}$. Le résultat en découle. $SU(1,1)$ est un sous-groupe du groupe de Lie $GL_2(\mathbb{C})$ tout en étant une sous-variété. C'est donc un groupe de Lie connexe.
b) L'algèbre de Lie $\mathfrak{su}(1,1)$ est l'espace tangent au groupe de Lie $SU(1,1)$ en l'identité. Tout courbe $\mathcal{C}^1$ de $SU(1,1)$ est aussi une courbe $\mathcal{C}^1$ incluse dans $U(1,1)$ et dans $SL_2(\mathbb{C})$. d'où l'inclusion par définition de l'espace tangent.
c) L'application φ de $M_2(\mathbb{C})$ dans l'espace des matrices hermitiennes qui envoie A sur $AI_{1,1}A^*$ a pour différentielle $K \mapsto AI_{1,1}K^* + KI_{1,1}A^*$. Si H est une matrice hermitienne quelconque, alors $K = \frac{H}{2}A^{*-1}I_{1,1}$ a pour image H et donc on a une submersion en tout A inversible. Ainsi, $U(1,1)$, qui est par définition $\varphi^{-1}(I_{1,1)}$, est un groupe de Lie et son sous-espace tangent en l'identité est donné par

$$\mathfrak{u}(1,1) = \{K,\ I_{1,1}K^* + KI_{1,1} = 0\} = \{\begin{pmatrix} iu & v+iw \\ v-iw & -ix \end{pmatrix},\ u,v,w,x \in \mathbb{R}\}$$

Le résultat en découle.
d) En déduire $\mathfrak{su}(1,1) = \mathfrak{u}(1,1) \cap \mathfrak{sl}_2(\mathbb{C})$. On a l'inclusion et l'égalité des dimensions.
3) C'est une propriété générale de tout groupe de Lie. Soit $\varphi_g(u) = gug^{-1}$ l'action par conjugaison de g sur $SU(1,1)$ alors φ_g est différentiable et envoie l'identité de $SU(1,1)$ vers l'identité de $SU(1,1)$. Donc envoie l'espace tangent en l'identité sur lui-même. On vérifie que cela fournit bien une action.
4) L'action de $SU(1,1)$ sur son espace tangent respecte le determinant car

$$\det(AKA^{-1}) = \det K$$

donc respecte la forme quadratique $-\det = -u^2 + v^2 + w^2$ qui est de signature $(2,1)$. Donc l'action fournit un morphisme de $SU(1,1)$ vers $O(2,1)$ et comme cette action est continue et envoie l'identité vers l'identité, elle envoie le groupe connexe $SU(1,1)$ vers la composante connexe $SO_0(2,1)$ de l'identité. Un petit calcul montre que le commutant de $\mathfrak{su}(1,1)$ est réduit aux scalaires et donc le noyau de l'action est le sous-groupe des homothéties de $SU(1,1)$. On a donc que

$PSU(1,1)$ s'envoie sur $SO_0(2,1)$. De même la différentielle de l'action est injective.
$SO_0(2,1)$ est la composante connexe de l'identité de $O(2,1)$, donc a même espace tangent en l'identité que $O(2,1)$. Comme précédemment, l'espace tangent en l'identité de $O(2,1)$ est $\{K,\ KI_{2,1} + I_{2,1}{}^tK = 0\}$ et on voit soit par le calcul, soit par l'isomorphisme $K \to KI_{2,1}$ avec l'espace des matrices antisymétriques que cet espace tangent est de dimension 3. La dimension est donc la même que la dimension de $\mathfrak{su}(1,1)$ donc la différentielle est un isomorphisme. Donc l'image du morphisme contient un ouvert, donc par le principe de translation cette image est un ouvert et donc est un sous-groupe fermé. Comme $SO_0(2,1)$ est connexe, on a la surjectivité.

C. Fait en TD.
D. 1) La droite des réels de $\mathbb{C}$ prolongée à l'infini sera appelée droite projective réelle $\mathbb{P}^1(\mathbb{R})$ de $\mathbb{P}^1(\mathbb{C})$. Montrer que le stabilisateur de $\mathbb{P}^1(\mathbb{R})$ dans $PGL_2(\mathbb{C})$ est $PGL_2(\mathbb{R})$.
Si un élément g de $PGL_2(\mathbb{C})$ stabilise $\mathbb{P}^1(\mathbb{R})$, alors il envoie trois points distincts de $\mathbb{P}^1(\mathbb{R})$ vers trois points distincts de $\mathbb{P}^1(\mathbb{R})$. Il envoie donc un repère vers un repère. Or, par définition d'un repère en géométrie projective réelle, il existe un unique élément g' de $PGL_2(\mathbb{R})$ qui envoie un repère (réel) vers un repère (réel). Conclusion, $g = g'$. Donc g' appartient à $PGL_2(\mathbb{R})$. La réciproque est claire.
2) a) La droite projective imaginaire est l'ensemble des $(1 : ix)$ avec x réel, union l'infini bien entendu. Alors $z \mapsto iz$ envoie la droite projective réelle sur la droite projective imaginaire. L'élément est donc la classe de $g_0 = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}$.
b) Forcément $g_0 PGL_2(\mathbb{R}) g_0^{-1}$ d'après ce qui précède.
3)a) L'action de $GL_2(\mathbb{C})$ sur les droites de $\mathbb{C}^2$ se factorise par l'action de $PGL_2(\mathbb{C})$ sur ces droites via la surjection canonique $\pi : GL_2(\mathbb{C}) \to PGL_2(\mathbb{C})$. Donc le stabilisateur d'une droite dans $GL_2(\mathbb{C})$ d'une droite est l'image réciproque du stabilisateur de cette droite dans $PGL_2(\mathbb{C})$.
b) La contrainte $z \in i\mathbb{R}z'$ s'écrit $h(z,z') := z\bar{z}' + \bar{z}z' = 0$. D'où la première assertion. Comme cette forme hermitienne h est de signature $(1,1)$ (on le voit facilement à sa matrice qui possède deux valeurs propres de signes opposés), $U(1,1)$ est isomorphe au stabilisateur de h, qui lui-même stabilise le cône isotrope $h(z,z') = 0$ (lire à ce sujet "Martine roule le cône isotrope"). Donc $SU(1,1)$ (via un isomorphisme) est dans le stabilisateur de la droite imaginaire. ce qui donne le résultat par ce qui précède.
c) C'est toujours la même méthode qui consiste à voir que les dimensions des espaces tangents en l'identité sont les mêmes (c'est à dire 3) et donc que l'injection devient surjective par le théorème d'inversion locale.