EPFL Printemps 2020
Geometrie, MATH-125

Série 1: Correction

Exercice 1. Exhiber des domaines fondamentaux (jolis) pour

1. L'action de $\mathrm{Isom}(\mathbb{R}^2)$ sur $\mathbb{R}^2$.
2. L'action de $\mathrm{Isom}(\mathbb{R}^2)^+_{\mathbf{0}}$ sur $\mathbb{R}^2$.
3. L'action de $(q.\mathbb{Z}, +)$ sur $\mathbb{Z}$ par translations ($q \geqslant 1$).
4. L'action de $(\mathbb{Z}, +)$ sur $\mathbb{R}$ par translations.
5. L'action de $(\mathbb{Z}^2, +)$ sur $\mathbb{R}^2$ par translations.
6. L'action de $(\mathbb{Z} + j\mathbb{Z}, +)$ sur $\mathbb{C}$ par translations ($j = \frac{-1+i\sqrt{3}}{2}$).
7. L'action du groupe de rotations lineaires de parametres complexes i^n, $n \in \mathbb{Z}$ agissant sur $\mathbb{R}^2$.

Preuve:

1. Any point $P \in \mathbb{R}^2$.
2. Any half-line passing through the origin, e.g. $y = ax$ with $x \geqslant 0$. Here a is a non-zero real number.
3. $\{0, 1, ..., q-1\}$.
4. The interval $[0, 1)$.
5. $\{(x, y) : 0 \leqslant x < 1, 0 \leqslant y < 1\}$.
6. $\{a + bi \in \mathbb{C} : 0 < a \leqslant \frac{1}{2}, 0 < b \leqslant \frac{\sqrt{3}}{2}\}$.
   To see this, note that $\mathbb{Z} + j\mathbb{Z} = \mathbb{Z} + \frac{-1+i\sqrt{3}}{2}\mathbb{Z} = \frac{1}{2}\mathbb{Z} + \frac{i\sqrt{3}}{2}\mathbb{Z}$. The action of $\frac{1}{2}m + \frac{i\sqrt{3}}{2}n \in \mathbb{Z} + j\mathbb{Z}$ (where $m, n \in \mathbb{Z}$) on any element $a + bi \in \mathbb{C} = \mathbb{R} + \mathbb{R}i$ is given by
   $$(\frac{1}{2}m + \frac{i\sqrt{3}}{2}n) \star (a + bi) = a + \frac{1}{2}m + (b + \frac{\sqrt{3}}{2})i.$$
   We know that for any $a \in \mathbb{R}$ there exists some $m \in \mathbb{Z}$ such that
   $$a + \frac{1}{2}m \in (0, \frac{1}{2}],$$
   and for any $b \in \mathbb{R}$ there exists some $n \in \mathbb{Z}$ such that
   $$b + \frac{\sqrt{3}}{2}m \in (0, \frac{\sqrt{3}}{2}].$$

Therefore one fundamental domain of the action of $(\mathbb{Z}+j\mathbb{Z},+)$ on $\mathbb{C}$ is given by

$$\{a+bi\in\mathbb{C} : 0<a\leqslant\frac{1}{2}, 0<b\leqslant\frac{\sqrt{3}}{2}\}.$$

7. The first quadrant, i.e., $\{(x,y) : x>0, y\geqslant 0\}\cup(0,0)$. □

Exercice 2. Soit $\mathbf{P}_4$ un carre (centre en $\mathbf{0}$), P un sommet et $D_8=\langle r_4,s\rangle$ son groupe d'isometries (engendre par une rotation d'ordre 4 et une symetrie axiale).

1. Pour les groupes $G=D_8,\ R=\langle r_4\rangle,\ S=\langle s\rangle$ verifier que le Theoreme orbite/quotient/stabilisateur est bien correct : calculer dans chaque cas, l' orbite de P, le stabilisateur de P et verifier l'equalite $|G.P|=|G/G_P|$.

Preuve: We only verify the Orbit-Stabilizer Theorem for the case $G=D_8$. The orbit $G.P$ of P is $\mathbf{P}_4$. The stabilizer G_P is $\{e_G,s_P\}$, where s_P is the axial symmetry which fixes P. In particular $|G_P|=2$. Then $|G.P|=|\mathbf{P}_4|=4$ and $|G/G_P|=|G|/|G_P|=8/2=4$. Hence we have $|G.P|=|G/G_P|$.

Exercice 3. Dans cet exercice on va boucher les trous de la preuve de Zagier vue en cours sur Theoreme de Fermat pour les sommes de 2 carres.

Théorème 1 (Fermat)**.** *Soit p un nombre premier impair alors p est somme de deux carres d'entiers, cad. il existe $a,b\in\mathbb{Z}^2$ tels que*

$$p=a^2+b^2$$

ssi $p\equiv 1\pmod 4$ *(ie.* $4|p-1$*).*

1. Montrer que si $p\equiv 3\pmod 4$ alors p n'est pas somme de deux carres d'entiers. Pour cela on montrera que pour toute paire d'entiers a,b, a^2+b^2 est soit $\equiv 0\pmod 2$ soit $\equiv 1\pmod 4$.
2. On suppose que $p\equiv 1\pmod 4$ et on a vu qu'il "suffit" de montrer que l'ensemble
$$R_p=\{(x,y,z)\in\mathbb{N}^3,\ p=x^2+4yz\},$$
est fini et d'ordre impair. Montrer que R_p est bien fini.
3. On considere l'application
$$S:(x,y,z)\mapsto\begin{cases}(x+2z,z,y-x-z) & si\ x<y-z\\ (2y-x,y,x-y+z) & si\ y-z<x<2y\\ (x-2y,x-y+z,y) & si\ x>2y\end{cases}$$
Montrer que cette application envoie R_p su R_p et est une involution sur R_p : $S\circ S=\mathrm{Id}_{R_p}$.

4. Montrer que si on pose $p = 1 + 4k$, S (sur R_p) a comme unique point fixe $(1, 1, k)$.
5. En deduire que R_p est impair.

Preuve:

1. Given any integers a and b. If both of them are even, then $a^2 + b^2 \equiv 0 \pmod 4$. If one of them is even and the other is odd, then $a^2 + b^2 \equiv 1 \pmod 4$. If both of them are odd, then $a^2 + b^2 \equiv 2 \pmod 4$. This implies that sum of two squares can never be congruent to $3 \pmod 4$.
2. Note that p is a fixed number and $x, y, z \geqslant 1$. From the equation $p = x^2 + 4yz$, we have $x \leqslant \sqrt{p}$ and $y, z \leqslant p/4$. In particular, the number of elements $|R_p|$ in R_p is at most $\leqslant p \cdot p/4 \cdot p/4$, which is finite.
3. We can divide the set R_p into three regions : $R_p = A_1 \cup A_2 \cup A_3$, where

$$A_1 = \{(x, y, z) \in R_p : x < y - z\}$$

$$A_2 = \{(x, y, z) \in R_p : y - z < x < 2y\}$$

$$A_3 = \{(x, y, z) \in R_p : x > 2y\}.$$

   One can show that $S(A_1) \subseteq A_3$, $S(A_2) \subseteq A_2$ and $S(A_3) \subseteq A_1$. To see this, we only verify the first case.

   For $(x, y, z) \in A_1$, $S(x, y, z) = (x+2z, z, y-x-z)$. We first check that the tuple $S(x, y, z) = (x + 2z, z, y - x - z)$ lies in R_p, i.e., $(x + 2z)^2 + 4z(y - x - z) = p$. The latter is equivalent to $x^2 + 4xz + 4z^2 + 4yz - 4xz - 4z^2 = p$, which is $x^2 + 4yz = p$. This is indeed the case since $(x, y, z) \in R_p$. Next we check that $(x + 2z, z, y - x - z) \in A_3$. This follows by observing that $x + 2z > 2z$, since $z > 0$. Hence we have shown that $S(A_1) \subseteq A_3$. Similarly one can verify that $S(A_2) \subseteq A_2$ and $S(A_3) \subseteq A_1$.

   To see S is an involution on R_p, we verify the case where $(x, y, z) \in A_1$. Then $(S \circ S)(x, y, z) = S(x + 2z, z, y - x - z) = (x, y, z)$. Similarly one can verify the other two regions. Hence $S \circ S = \mathrm{Id}_{R_p}$.
4. Since $S(A_1) \subseteq A_3$, $S(A_2) \subseteq A_2$ and $S(A_3) \subseteq A_1$, the only fixed points of S on R_p can only lie in A_2. Let $(x, y, z) \in R_p$ be a fixed point of S. Then $S(x, y, z) = (2y - x, y, x - y + z) = (x, y, z)$. This implies that $x - y + z = z$. That is, $x = y$. But (x, y, z) also satisfies

$$1 + 4k = p = x^2 + 4yz = x^2 + 4xz = x(x + 4z).$$

   Since p is a prime, the only possibility is $x = 1$ and $x + 4z = 1 + 4k$. Hence $(x, y, z) = (1, 1, k)$ is the only fixed point.

5. We observe that the elements of R_p which are not fixed points of S appear in pairs. To see this, let $r \in R_p$ and assume that r is not a fixed point of S. Then there exists $r' \in R_p, r' \neq r$, such that $S(r) = r'$. Since S is an involution, $r = S(S(r)) = S(r')$, i.e., $S(r') = r$. This together with the fact that the action of S on R_p has a unique fixed point implies that R_p is of odd order.

$\square$

Exercice 4. Montrer le theoreme suivant

Théorème 2. *Soit $G \curvearrowright X$ un groupe fini d'ordre premier p agissant sur un ensemble fini X. Si p ne divise pas le cardinal de X alors l'action de G sur X admet un point fixe : il existe $x \in X$ tel que*

$$\forall g \in G,\ g.x = x.$$

Preuve: It follows from the Orbit-Stabilizer Theorem that

$$|\mathcal{O}_x| = |G \cdot x| = |G/G_x| = \frac{|G|}{|G_x|}.$$

Since by assumption $|G| = p$, this implies that either $|\mathcal{O}_x| = 1$ or $|\mathcal{O}_x| = p$. Recall that

$$X = \bigsqcup_{\mathcal{O}_x \in G\backslash X} \mathcal{O}_x.$$

Then

$$|X| = \sum_{\mathcal{O}_x \in G\backslash X} |\mathcal{O}_x|.$$

Since $p \nmid |X|$, it can not happen that for all $\mathcal{O}_x \in G\backslash X$, $|\mathcal{O}_x| = p$. (Otherwise the right hand side of the equation above would be divisible by p.) Therefore there must exist some orbit $\mathcal{O}_x \in G\backslash X$ such that $|\mathcal{O}_x| = 1$. In other words, there exists some $x \in X$ such that $G \cdot x = \{x\}$, which is what we want to prove.

$\square$

Exercice 5. Le but de cet exercice est de demontrer le Theoreme de Cauchy :

Théorème 3. *Soit G un groupe fini d'ordre n et $p \geqslant 2$ un nombre premier divisant n alors G admet un element g d'ordre p.*

Pour cela on considere le groupe quotient $\mathbb{Z}/p\mathbb{Z}$ dont on notera les elements

$$\overline{m} = m \pmod{p} = m + p\mathbb{Z}$$

et

$$\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0 = \{\overline{n} \in \mathbb{Z}/p\mathbb{Z} \mapsto g(\overline{n}) \in G,\ g(\overline{0}).g(\overline{1}) \cdots g(\overline{p-1}) = e_G\} \subseteq (\mathbb{Z}/p\mathbb{Z})^G$$

l'ensemble des fonctions de $\mathbb{Z}/p\mathbb{Z}$ a valeurs dans G et dont le produit de toutes les valeurs est egal a l'element neutre e_G.

1. Montrer que $|\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0| = |G|^{p-1}$.
2. Montrer que l'action par translations de $\mathbb{Z}/p\mathbb{Z}$ sur lui-meme induit une action de $\mathbb{Z}/p\mathbb{Z}$ sur l'espace $\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$. Cette action est a gauche ou a droite, pourquoi ?
3. Montrer que les orbites de l' action $\mathbb{Z}/p\mathbb{Z} \curvearrowright \mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$ sont de taille 1 ou p.
4. Montrer que les orbites qui sont de taille 1 sont exactement celles des fonctions constantes $\overline{n} \mapsto g$ avec $g \in G$ verifiant
$$g^p = e_G.$$
5. Donner un exemple d'une telle orbite.
6. A l'aide de la formule des classes montrer que le nombre d'orbites de taille 1 est divisible par p.
7. Montrer qu'il existe au moins deux telles orbites et que G possede au moins un element d'ordre p.

Preuve:

1. Any function g of $\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$ is completely determined by its values
$$g(\overline{0}),\ g(\overline{1}), \cdots, g(\overline{p-2})$$
because the value of $g(\overline{p-1})$ is equal to $(g(\overline{0}).\ g(\overline{1}), \cdots .g(\overline{p-2}))^{-1}$. For each of the first $p-1$ values $g(\overline{0}),\ g(\overline{1}), \cdots, g(\overline{p-2})$, each of them has $|G|$ many possible choices. Hence
$$|\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0| = |G|^{p-1}.$$
2. The action is defined as follows : for $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ and $g \in \mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$, we let
$$(\overline{n} \star g)(\overline{m}) = g(\overline{n} + \overline{m}).$$
One can verify that this defines an action of $\mathbb{Z}/p\mathbb{Z}$ on $\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$. This action is both on the left and on the right, since the group $\mathbb{Z}/p\mathbb{Z}$ is commutative.
3. Let $g \in \mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$. By the Orbit-Stabilizer Theorem, the orbit $\mathbb{Z}/p\mathbb{Z} \cdot g$ of g satisfies
$$|\mathbb{Z}/p\mathbb{Z} \cdot g| = |(\mathbb{Z}/p\mathbb{Z})/(\mathbb{Z}/p\mathbb{Z})_g| = \frac{p}{|(\mathbb{Z}/p\mathbb{Z})_g|},$$
where $(\mathbb{Z}/p\mathbb{Z})_g$ is the stabilizer of g. By the Lagrange Theorem, $|(\mathbb{Z}/p\mathbb{Z})_g|$ divides p, hence taking values 1 or p, and then the quotient $p/|(\mathbb{Z}/p\mathbb{Z})_g|$ equals to p or 1.
4. Suppose that $|\mathbb{Z}/p\mathbb{Z} \cdot f| = 1$, then necessarily $\mathbb{Z}/p\mathbb{Z} \cdot f = \{f\}$. In other words, $\overline{n} \star f = f$, for all $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$. Then we have $f(\overline{0}) = f(\overline{n})$ for all $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$, and hence f is a constant function. Let $g = f(\overline{n})$. By definition of $\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0$, we obtain $g^p = e_G$.

5. The constant function which sends any element $\overline{n} \in \mathbb{Z}/p\mathbb{Z}$ to e_G.
6. By the Classes Formula we have

$$|\mathcal{F}(\mathbb{Z}/p\mathbb{Z}, G)_0| = |G|^{p-1} = \sum_{\mathcal{O}} |\mathcal{O}| = \sum_{|\mathcal{O}|=1} 1 + \sum_{|\mathcal{O}|=p} p.$$

   Since p divides $|G|^{p-1}$ and p also divides $\sum_{|\mathcal{O}|=p} p$, we imply that p must divide $\sum_{|\mathcal{O}|=1} 1$ which is the number of orbits of size 1.
7. By Part 5 there exists at least one orbit of size 1 and by Part 6 the number of such orbit has to be a non-zero multiple of p. Since $p \geqslant 2$, there are at least two such orbits. In particular, at least one of such orbits has to be a constant function whose image does not equal to e_G. In other words, there exists $g \neq e_G$ such that $g^p = e_G$.

$\square$