Devoir Maison n° 14

Exercice 1 - Une LCI sur $\mathbb{Z}$

On définit sur $\mathbb{Z}$ une LCI notée $\top$ par :

$$\forall (a,b) \in \mathbb{Z}^2, a \top b = a^2 + b^2$$

Cette loi est-elle associative ? commutative ? Admet-elle un élément neutre ? Existe-t-il des éléments symétrisables ?

Exercice 2 - Le premier groupe diédral

On se donne un triangle ABC équilatéral direct. On note s la symétrie d'axe la médiatrice de $[BC]$ et r la rotation de centre le centre de gravité du triangle et d'angle $2\pi/3$.

1. Faire un dessin.
2. Justifier (juste en regardant les images des sommets) que les six éléments $\mathrm{Id}, r, r^2, s, s \circ r$ et $s \circ r^2$ sont distincts.
3. Donner sans démonstration la table de la composition sur l'ensemble $D_3 = \{\mathrm{Id}; r; r^2; s; s \circ r; s \circ r^2\}$.
4. En déduire que $(D_3, \circ)$ est un groupe non abélien (l'associativité découle de l'associativité de la composition et ne sera pas redémontrée).

Exercice 3 - Groupes d'ordre p^2

Dans tout l'exercice, p désigne un nombre premier et G un p-groupe, c'est-à-dire un groupe de cardinal une puissance de p dont la loi est notée multiplicativement, c'est-à-dire que la loi du groupe peut être notée par une croix $(x \times y)$ ou par une absence de symbole (xy).

1. Soit $x \in G$. On appelle stabilisateur de x et on note $\mathrm{Stab}(x)$ l'ensemble $\{g \in G \,|\, gxg^{-1} = x\}$. Montrer que $\mathrm{Stab}(x)$ est un sous-groupe de G.
2. On définit sur G la relation $\sim$ par : $x \sim y \iff \exists g \in G, gxg^{-1} = y$. Montrer que $\sim$ est une relation d'équivalence.
3. On appelle orbite de x et on note $O(x)$ la classe d'équivalence de x pour la relation $\sim$, c'est-à-dire que :

   $$O(x) = \{gxg^{-1} \,|\, g \in G\}$$

   Justifier que les différentes orbites forment une partition de G et que, parmi les différentes orbites, une et une seule est un sous-groupe de G. On explicitera ce sous-groupe.
4. S'inspirer de l'exercice 32 du chapitre 18 pour prouver le résultat suivant :

   $$\forall x \in G, \mathrm{card}(G) = \mathrm{card}(O(x)) \times \mathrm{card}(\mathrm{Stab}(x))$$

   On pourra s'intéresser à la fonction :

   $$\varphi : \left\{ \begin{array}{ccc} G & \to & O(x) \\ g & \mapsto & gxg^{-1} \end{array} \right.$$
5. Soit $x \in G$. Montrer que : $\mathrm{card}(O(x)) = 1 \iff x \in Z(G)$, où, comme en classe, $Z(G)$ est le centre de G.
6. Montrer l'équation aux classes :

   $$\mathrm{card}(G) = \mathrm{card}(Z(G)) + \sum_{O(x) \,|\, \mathrm{card}(O(x)) \neq 1} \mathrm{card}(O(x))$$

   En déduire que $\mathrm{card}(Z(G)) \equiv 0[p]$.
7. On suppose dans cette question que $\mathrm{card}(G) = p^2$. Le but de cette question est de prouver que G est abélien.
   (a) Justifier que $\mathrm{card}(Z(G)) \neq 0$.
   (b) Supposons que $\mathrm{card}(Z(G)) = p$. Justifier qu'il existe $x \notin Z(G)$ et montrer que $Z(G) \subsetneq \mathrm{Stab}(x) \subsetneq G$. En déduire une absurdité (on pourra utiliser la question 4).
   (c) Conclure.

Problème - Dérivations dans un anneau

Soit $(A, +, \times)$ un anneau (qui n'est pas supposé commutatif). On note 0 et 1 les éléments neutres respectifs des lois + et $\times$. Le produit de x et y peut être noté $x \times y$, ou plus simplement par absence de symbole : xy.

Une application $\delta : A \to A$ est appelée une dérivation sur A si on a les deux propriétés :

- $\forall (x, y) \in A^2, \quad \delta(x + y) = \delta(x) + \delta(y)$.
- $\forall (x, y) \in A^2, \quad \delta(xy) = x\delta(y) + \delta(x)y$.

Partie I - Crochet de Lie et exemple de dérivation

Pour tous a, $b \in A$, on pose $[a, b] = ab - ba$.

1. Que vaut $[a, b]$ lorsque a et b commutent ?
2. On revient au cas général et on se donne a, b et c dans A.
   (a) Donner une relation liant $[a, b]$ et $[b, a]$.
   (b) Établir que $[a, b + c] = [a, b] + [a, c]$.
   (c) Démontrer que $[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0$. Cette relation est connue sous le nom d'identité de Jacobi.
3. Pour $a \in A$, on considère l'application $d_a : A \to A$ définie par $d_a(x) = ax - xa$ pour tout $x \in A$. Montrer que d_a est une dérivation sur A.

Partie II - Propriétés des dérivations

Soit δ une dérivation quelconque sur A.

1. Calculer $\delta(0)$ et $\delta(1)$.
2. Soit x un élément de l'anneau A.
   (a) Exprimer $\delta(-x)$ en fonction de $\delta(x)$.
   (b) On suppose que x est inversible. Exprimer $\delta(x^{-1})$ en fonction de $\delta(x)$ et de x^{-1}.
3. On se donne un entier strictement positif $n \in \mathbb{N}^*$.
   (a) Soient $x_1, x_2, \ldots, x_n$ des éléments de A. Exprimer $\delta(x_1 x_2 \ldots x_n)$ en fonction des x_k et des $\delta(x_k)$.
   (b) Pour $x \in A$, exprimer $\delta(x^n)$. Que devient cette formule si x et $\delta(x)$ commutent ?
4. Soit $C_\delta = \{x \in A \mid \delta(x) = 0\}$.
   (a) Montrer que C_δ est un sous-anneau de $(A, +, \times)$.
   (b) Montrer que si $(A, +, \times)$ est un corps, alors C_δ est un sous-corps de $(A, +, \times)$.

Partie III - Manipulation de dérivations

1. Dans cette question, δ_1 et δ_2 désignent deux dérivations sur A.
   (a) Est-ce que l'application $\delta_1 + \delta_2$ (qui à $x \in A$ associe $\delta_1(x) + \delta_2(x)$) est une dérivation ?
   (b) On note $[\delta_1, \delta_2] = \delta_1 \circ \delta_2 - \delta_2 \circ \delta_1$. Montrer que $[\delta_1, \delta_2]$ est une dérivation sur A.
2. Soit δ une dérivation sur A et a, b deux éléments de A.
   (a) Montrer que $[\delta, d_a] = d_{\delta(a)}$.
   (b) Montrer que $[d_a, d_b] = d_{[a,b]}$.

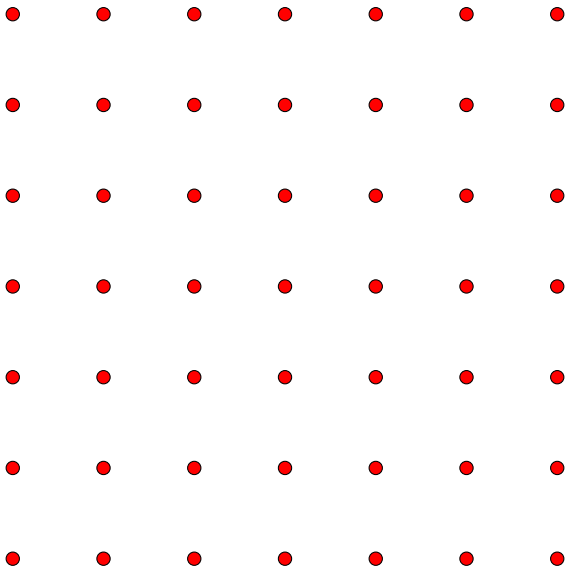
Exercice 4 (facultatif) - Le Dobble

Le Dobble est un jeu très simple d'observation et de rapidité qui se joue avec des cartes contenant huit dessins. Ces dessins sont variés et dépendent des éditions : j'ai chez moi l'édition Harry Potter, mais il y en a d'autres évidemment.

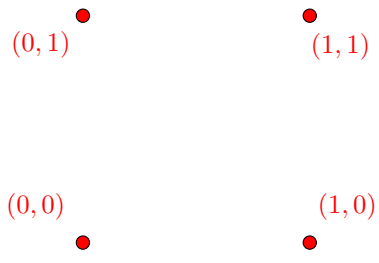
Les dessins peuvent varier, donc, mais le principe est toujours le même : chaque fois que l'on choisit deux cartes (différentes), elles ont exactement un dessin en commun. Par exemple, ci-dessus, les cartes ont en commun l'image « beuglante » (la lettre rouge avec des dents).

Nous allons décrire ici la structure mathématique sous-jacente de cette propriété, et voir qu'elle détermine avec précision les nombres de cartes possibles, ainsi que le nombre de dessins nécessaires.

On se donne dans la suite un corps fini noté $\mathbb{K}$ contenant q éléments (avec q un entier naturel supérieur ou égal à 2) et on travaille sur l'ensemble $\mathbb{K}^2$ (qui est, rappelons-le, l'ensemble des couples (x, y) avec x et y appartenant à $\mathbb{K}$). On peut par exemple représenter $\mathbb{K}^2$ sous forme de réseau comme ci-dessous (où l'on a pris $\mathbb{K} = \mathbb{Z}/7\mathbb{Z}$ qui est donc de cardinal $q = 7$) :



Dans la suite, sur chaque exemple [1], pour que cela reste lisible, on prendra à chaque fois $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$, qui est donc de cardinal $q = 2$, et donc on peut représenter $\mathbb{K}^2$ de la façon suivante :



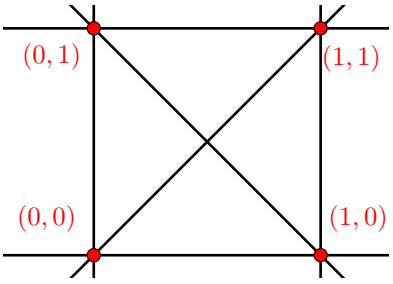
1. Mais uniquement dans les exemples : dans les questions, $\mathbb{K}$ reste un corps à q éléments.

Comme dans le plan $\mathbb{R}^2$, une droite sur $\mathbb{K}^2$ est un ensemble de points de l'un des deux types suivants :

- soit un ensemble de points admettant une équation du type $x = c$: les droites de ce type sont appelées droites verticales.
- soit un ensemble de points admettant une équation du type $y = ax + b$, où a et b sont deux éléments de $\mathbb{K}$ (et où a est appelé le coefficient directeur de la droite) : les droites de ce type sont appelées droites obliques (ou droites non verticales).

1. Montrer qu'il y a exactement $q^2 + q$ droites dans $\mathbb{K}^2$. On prouvera bien que les droites trouvées sont bien deux à deux distinctes.

   Par exemple, ci-dessous, on a représenté les six droites de $(\mathbb{Z}/2\mathbb{Z})^2$: les deux droites verticales d'équation $x = 0$ et $x = 1$, et les quatre droites obliques d'équation $y = x, y = 1 + x$ (précisons que, sur $\mathbb{Z}/2\mathbb{Z}$, $1 = -1$ donc la droite d'équation $y = 1 + x$ et la droite d'équation $y = 1 - x$ sont la même droite), $y = 0$ et $y = 1$:



   Précisons enfin que nous n'avons tracé les droites de façon continue « comme dans le plan normal » ce n'est que pour des notions de lisibilité, pour que vous puissiez visualiser la chose : en effet, sur l'exemple ci-dessus, chacune de ces droites ne comporte que deux points ! En particulier, les deux diagonales ci-dessus ne se coupent pas vraiment puisque leur « intersection » ne comporte aucun point !

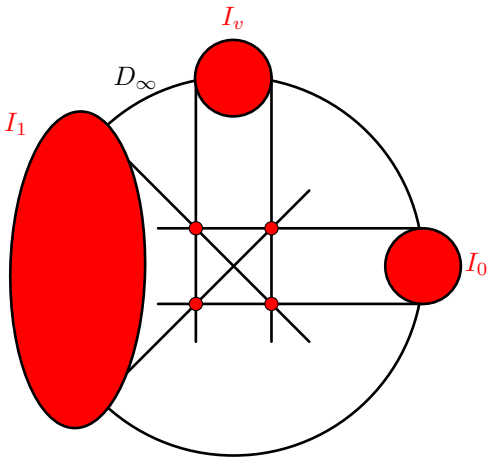
2. Montrer que tout point de $\mathbb{K}^2$ appartient à exactement $q + 1$ droites.
3. Montrer que par deux points distincts de $\mathbb{K}^2$ passe une et une seule droite. Bien sûr, j'attends ici une vraie démonstration qui utilisera le fait que $\mathbb{K}$ est un corps, pas un simple : « ben c'est évident, il suffit de tracer la droite qui les relie ». Les choses ne sont pas si évidentes que ça sur les corps finis : prenez par exemple les deux diagonales ci-dessus qui ne se coupent pas !

   Nous allons maintenant créer de nouveaux points et une nouvelle droite, un peu comme nous avons créé $\overline{\mathbb{R}}$ ou comme nous avons créé un degré égal à $-\infty$ pour les polynômes par exemple :

   - On se donne dont un élément n'appartenant pas à $\mathbb{K}$ que nous allons noter ∞, et notons $\overline{\mathbb{K}} = \mathbb{K} \cup \{\infty\}$.
   - Pour chaque $a \in \mathbb{K}$, on définit un point noté I_a qu'on appelle « point à l'infini dans la direction a » et nous décidons, par convention, qu'il appartient à toutes les droites obliques de coefficient directeur a et à aucune autre [2]. Par exemple, sur le dessin ci-dessous, I_1 appartient aux deux droites obliques mais pas aux droites horizontales « qui s'arrêtent avant I_1 ».
   - On définit de même un point noté I_v qu'on appelle « point à l'infini vertical » et qui, par convention, appartient à toutes les droites verticales et à aucune autre.
   - Précisons encore une fois que nous **définissons** ces points et que nous **déclarons arbitrairement** (c'est une définition : il n'y a rien à prouver) qu'ils appartiennent à certaines droites, un peu comme quand nous avons construit $\overline{\mathbb{R}}$ et que nous avons déclaré arbitrairement que $1 + \infty = +\infty$.
   - Enfin, on **définit** une nouvelle « droite » appelée « droite à l'infini » qu'on notera D_∞ et qui passe par tous les points à l'infini et uniquement par eux (et donc ne passe par aucun point « ordinaire » de $\mathbb{K}^2$).

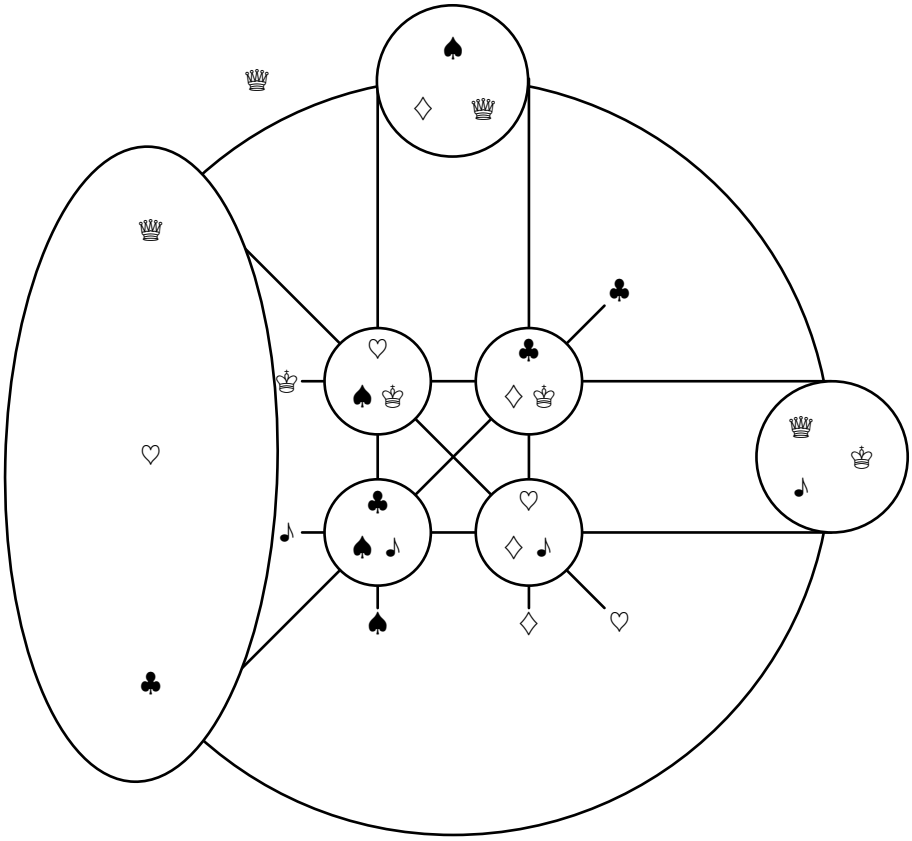
   On peut visualiser tout cela de la façon suivante : les deux droites verticales s'intersectent au (gros) point à l'infini I_v, les deux droites horizontales (de coefficient directeur 0, donc) s'intersectent au (gros) point à l'infini I_0, et les deux diagonales (d'équation $y = x$ et $y = x + 1$ puisque, sur $\mathbb{Z}/2\mathbb{Z}$, $1 = -1$) s'intersectent au (gros et de forme bizarre) point I_1. Ci-dessous ces trois nouveaux points, reliés par la droite D_∞ (représentée par un cercle sur le dessin [3]) :

2. Cette idée, qui est la base de ce que les mathématiciens appellent la géométrie projective date en fait des peintres de la Renaissance et consiste à ajouter un point (le point de fuite des peintres) pour chaque famille de droites parallèles. Ce point est alors le point d'intersection de la famille des droites. Les points de fuite sont tous alignés sur une droite, que les mathématiciens appellent « la droite à l'infini » et tous les autres « l'horizon ».
3. Bienvenue dans le monde merveilleux de la géométrie projective !



4. Montrer que tout point de (à l'infini ou non) appartient à exactement $q+1$ droites (à l'infini ou non).
5. Prouver que par deux points (à l'infini ou non) passe exactement une seule droite (à l'infini ou non).
6. Combien cela fait-il de points et de droites (à l'infini ou non) ? Combien de droites passent par chaque point (à l'infini ou non) ?

Remarque : Quel est donc le lien avec le Dobble ? Et bien, c'est très simple : l'analogue de « deux cartes contiennent exactement un symbole commun » est « par deux points passe exactement une droite ». Il suffit de remplacer les droites par des symboles et les points par des cartes. Pour être plus précis, on attribue à chaque droite un symbole, et chaque point sera la carte comprenant les symboles correspondant aux droites qui passent par ce point. Dans l'exemple ci-dessous, on a représenté à côté de chaque droite le symbole qu'il lui est attribué (♕ pour D_∞ par exemple) et on a représenté dans chaque point les trois symboles correspondant aux droites qui les traversent. On vient de créer un Dobble à 7 cartes (les 7 points) et 7 symboles (les 7 droites), chaque carte contenant 3 symboles (chaque point appartenant à trois droites). Vous pouvez vérifier vous-même que, par deux points quelconques, passe une unique droite, et cela se traduit bien par : deux cartes ont exactement un symbole en commun !



Pour la culture, le jeu de Dobble se place sur $\mathbb{Z}/7\mathbb{Z}$: chaque carte contient 8 symboles (chaque point appartient à 8 droites), il y a 57 symboles (il y a 57 droites) et... il devrait y avoir 57 cartes (car il y a 57 points), mais il n'y en a que 55 ! Cela n'est pas une erreur mathématique de la société mais vient de contraintes pratiques d'impression...

Problème - Actions de groupes

Partie I - Notion de loi externe, d'action de groupe, et premiers exemples

- Dans tout le problème, si rien n'est précisé, G est un groupe dont la loi est notée $*$, dont le neutre est noté e, et X est un ensemble non vide. On pourra comme d'habitude noter la loi du groupe multiplicativement, mais attention à ne pas confondre la loi du groupe avec la loi externe définie ci-dessous.
- Une loi externe de G sur X est une application φ de $G \times X$ dans X. En clair, contrairement à une loi interne qui prend deux éléments de G et renvoie un élément de G, une loi externe prend un élément de G et un élément de X (donc deux éléments qui, a priori, n'appartiennent pas au même ensemble) et renvoie un élément de X.
- De même qu'une LCI dans le chapitre 18, une loi externe sera plutôt notée de façon opérationnelle plutôt que fonctionnelle. Dans ce devoir, nous noterons en général les lois externes avec un point ($g.x$) ou avec une absence de symbole (gx).
- On dit enfin que G agit sur X s'il existe une loi externe de G sur X notée . qui vérifie les deux conditions suivantes :

  ⋆ $(C_1) : \forall x \in X, e.x = x.$

  ⋆ $(C_2) : \forall (g_1, g_2) \in G^2, \forall x \in X, g_1.\underbrace{(g_2.x)}_{\in E} = \underbrace{(g_1 * g_2)}_{\in G}.x.$

1. (a) Soit $n \in \mathbb{N}^*$. On note . la loi externe de $\mathbb{R}_+^*$ sur $\mathbb{R}^n$ définie par :

$$\forall u = (u_1, \dots, u_n) \in \mathbb{R}^n, \forall g \in \mathbb{R}_+^*, \qquad g.u = (g \times u_1, \dots, g \times u_n)$$

   En clair, pour cette loi externe, on multiplie toutes les coordonnées par g. Est-ce que le groupe $\mathbb{R}_+^*$ agit sur l'ensemble $\mathbb{R}^n$?

   (b) Soit $n \in \mathbb{N}^*$. On note . la loi externe de $\mathbb{R}$ sur $\mathbb{R}^n$ définie de la même façon, à savoir :

$$\forall u = (u_1, \dots, u_n) \in \mathbb{R}^n, \forall g \in \mathbb{R}, \qquad g.u = (g \times u_1, \dots, g \times u_n)$$

   Est-ce que le groupe $\mathbb{R}$ agit sur l'ensemble $\mathbb{R}^n$ pour cette loi externe ?

   (c) Proposer une loi externe de $\mathbb{R}$ sur $\mathbb{R}^n$ qui induise une action de groupe de $\mathbb{R}$ sur $\mathbb{R}^n$.

2. Soit $n \geq 1$ et soit $X = \{x_1; \dots; x_n\}$ un ensemble fini à n éléments. Montrer que S_n (l'ensemble des permutations de $[\![1\,;\, n]\!]$, un groupe pour la composition, cf. cours) agit sur X grâce à la loi externe définie par :

$$\forall i \in [\![1\,;\, n]\!], \forall \sigma \in S_n, \qquad \sigma.x_i = x_{\sigma(i)}$$

   Par exemple, cela permet de faire agir S_3 sur les trois sommets d'un triangle équilatéral : on voit bien qu'on peut faire agir, et donc appliquer des éléments d'un groupe, à des éléments qui n'ont a priori [4] rien à voir avec la théorie des groupes !

3. **Action d'un groupe sur lui-même.**

   (a) On définit une loi externe [5] . de G sur G par :

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

   où l'on rappelle que $*$ est la loi du groupe G. Montrer que l'on définit ainsi une action de groupe, appelée action de G sur lui-même par translation à gauche.

   (b) On définit une loi externe . de G sur G par :

$$\forall x \in G, \forall g \in G, \qquad g.x = g * x * g^{-1}$$

   Montrer que l'on définit ainsi une action de groupe, appelée action de G sur lui-même par conjugaison.

4. (Question difficile) On suppose que G agit sur X avec une loi externe notée comme d'habitude (avec un point).

   (a) Soit

$$\varphi : \begin{cases} G \longrightarrow & S_X \\ g \longmapsto \varphi(g) : & \begin{cases} X \longrightarrow X \\ x \longmapsto g.x \end{cases} \end{cases}$$

   c'est-à-dire que, pour tous g et x, $\varphi(g)$ est une bijection de X dans lui-même définie par $\varphi(g)(x) = g.x$ (on rappelle que S_X est l'ensemble des bijections de X dans lui-même). Montrer que φ est bien définie et est un morphisme de groupes.

4. Seulement a priori... La théorie des groupes est partout ! Déjà rien qu'avec un chou, une banane et une carotte on peut faire des groupes...
5. On parle encore de loi externe dans ce cadre, même si $X = G$ et donc même si on on pourrait parler de loi interne.

(b) Montrer que φ est injective si et seulement si e est le seul élément de G qui stabilise tous les éléments de X (on dit alors que l'action est fidèle), c'est-à-dire que si $g \in G$ vérifie : $\forall x \in X, g.x = x$, alors $g = e$.

Partie II - Orbites et stabilisateurs, équation aux classes et application aux p-groupes

On se donne dans cette partie un groupe G qui agit sur un ensemble X avec une loi externe notée . comme précédemment.

1. Montrer que la relation R définie sur X par :

$$xRy \iff \exists g \in G, y = g.x$$

est une relation d'équivalence. Les classes d'équivalence de cette relation sont appelées orbites (de l'action de groupe de G sur X) et, pour tout $x \in X$, on note $\omega(x)$ l'orbite de x. En d'autres termes, on note

$$\omega(x) = \{g.x \,|\, g \in G\}$$

Intuitivement, $\omega(x)$ peut être vu comme l'ensemble des « images » de x (même si cette formulation est un peu impropre car on applique des éléments de G et pas des fonctions) quand on lui applique les différents éléments de G ou, de façon propre cette fois, l'ensemble des images de x par les différentes fonctions $\varphi(g)$ (cf. question 4 de la partie I) lorsque g décrit G.

2. Soit $x \in X$. On appelle stabilisateur de x, noté $\mathrm{Stab}(x)$, l'ensemble des éléments de G qui laissent x invariant, c'est-à-dire :

$$\mathrm{Stab}(x) = \{g \in G \,|\, g.x = x\}$$

Montrer que $\mathrm{Stab}(x)$ est un sous-groupe de G. Est-ce que $\omega(x)$ est un sous-groupe de G ?

3. On suppose dans cette question que X est un ensemble fini.

(a) Justifier que :

$$\mathrm{card}(X) = \sum_{\omega(x)} \mathrm{card}(\omega(x))$$

la somme étant prise sur les différentes orbites.

(b) On note X^G l'ensemble des éléments de X fixés par tous les éléments de G, c'est-à-dire :

$$X^G = \{x \in X \,|\, \forall g \in G, g.x = x\}$$

Montrer l'équation aux classes :

$$\mathrm{card}(X) = \mathrm{card}\left(X^G\right) + \sum_{\omega(x) \,|\, x \notin X^G} \mathrm{card}(\omega(x))$$

4. On suppose dans cette question que p est un nombre premier et que G est un p-groupe, c'est-à-dire qu'il existe $n \geq 1$ tel que $\mathrm{card}(G) = p^n$. Enfin, on se place dans le cadre de la question 3.(b) de la partie I, c'est-à-dire qu'on prend $X = G$ et qu'on fait agir G sur lui-même par conjugaison. On fera donc attention de ne pas confondre $g * x = gx$ (où $*$ est la loi du groupe de G, qu'on pourra tout de même noter multiplicativement) avec $g.x = g * x * g^{-1}$.

(a) Montrer que l'ensemble X^G défini à la question précédente (avec donc $X = G$ ici) est égal à $Z(G)$, le centre de G.

(b) S'inspirer de l'exercice 32 du chapitre 18 pour prouver le résultat suivant :

$$\forall x \in G, \mathrm{card}(G) = \mathrm{card}(\omega(x)) \times \mathrm{card}(\mathrm{Stab}(x))$$

On pourra s'intéresser à la fonction suivante :

$$u : \begin{cases} G \longrightarrow & \omega(x) \\ g \longmapsto & g.x = gxg^{-1} \end{cases}$$

(c) À l'aide de l'équation aux classes, prouver que $\mathrm{card}(Z(G)) \equiv 0[p]$.

(d) En déduire que $Z(G)$ n'est pas un sous-groupe trivial de G, c'est-à-dire que $Z(G) \neq \{e\}$.

Partie III - Théorème de Cauchy

On se donne dans toute cette partie p un nombre premier et G un groupe fini de cardinal n divisible par p. On pose

$$X = \{(x_1, \dots, x_p) \in G^p \,|\, x_1 * \cdots * x_p = e\}$$

Enfin, on définit une loi externe de $\mathbb{Z}/p\mathbb{Z}$ sur X de la façon suivante :

$$\forall k \in \mathbb{Z}/p\mathbb{Z}, \forall x = (x_1, \dots, x_p) \in X, \qquad k.x = (x_{k+1}, \dots, x_{k+p})$$

les indices $k+1, \dots, k+p$ étant pris modulo p. Si on utilise les parties précédentes, on fera attention à ne pas confondre G et $\mathbb{Z}/p\mathbb{Z}$: c'est $\mathbb{Z}/p\mathbb{Z}$ le groupe qui agit sur l'ensemble X !

1. Si $x = (x_1, \dots, x_p) \in X$, donner $0.x, 1.x$ et $2.x$. On admet (cela n'est pas très compliqué à voir) que cela définit bien une action de groupe (on dit qu'on fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire).
2. Justifier que $\text{card}(X) = n^{p-1}$.
3. Soit $x \in X$. À l'aide de la partie précédente, montrer que $\text{card}(\omega(x)) = 1$ ou p.
4. À l'aide de l'équation aux classes, prouver que $\text{card}\left(X^{\mathbb{Z}/p\mathbb{Z}}\right) \equiv 0[p]$ (la notation $X^{\mathbb{Z}/p\mathbb{Z}}$ a été introduite dans la question 3.(b) de la partie II).
5. Exhiber une bijection de $\{x \in G \,|\, x^p = e\}$ dans $X^{\mathbb{Z}/p\mathbb{Z}}$. On n'oubliera pas de justifier que cette fonction est bien à valeurs dans X et plus précisément dans $X^{\mathbb{Z}/p\mathbb{Z}}$.
6. Montrer qu'il existe $x \neq e$ appartenant à G tel que $x^p = e$. On en déduit d'après le poly de botanique (il n'est pas demandé de le prouver) que x est d'ordre p donc que le groupe engendré par x est de cardinal p. On vient donc de prouver le théorème de Cauchy :

> **Théorème de Cauchy :** Si G est un groupe fini et si p est un nombre premier divisant $\text{card}(G)$, alors G admet un sous-groupe de cardinal p.

Partie IV - Notion de p-Sylow et premiers résultats

- Dans toute la suite du problème, p est un nombre premier.
- On appelle p-groupe un groupe fini dont le cardinal est une puissance de p.
- Si G est un groupe (dont on pourra noter la loi avec une étoile $*$ ou multiplicativement), A une partie non vide de G et g un élément de G, on définit comme en TD les ensembles :

$$gA = \{g * a \,|\, a \in A\} \qquad \text{et} \qquad gAg^{-1} = \{g * a * g^{-1} \,|\, a \in A\}$$

- On rappelle le théorème de Lagrange : si G est un groupe fini et si S est un sous-groupe de G alors $\text{card}(S)$ divise $\text{card}(G)$.
- Si G est un groupe fini de cardinal $n = p^\alpha \times m$ avec $m \wedge p = 1$ et $\alpha \geq 1$, et si S est un sous-groupe de G, on dit que S est un p-sous-groupe de Sylow de G, ou plus simplement un p-Sylow de G, si $\text{card}(S) = p^\alpha$. En d'autres termes, un p-Sylow de G est un p-sous-groupe de G de cardinal maximal, c'est-à-dire que S est un p-Sylow de G si S est un p-groupe et si $\text{card}(G)/\text{card}(S)$ (qui est un entier d'après le théorème de Lagrange) est un entier premier avec p. Par exemple, si $\text{card}(G) = 24$, un 2-Sylow de G est un sous-groupe de G de cardinal 8.

1. Montrer que si G_1 et G_2 sont deux groupes finis isomorphes et si G_1 admet un p-Sylow noté S_1, alors G_2 admet un p-Sylow.
2. Soient G est un groupe fini, a un élément de G, et S un p-Sylow de G. Montrer que

$$\varphi : \begin{cases} G \longrightarrow G \\ x \longmapsto axa^{-1} \end{cases}$$

est un automorphisme (i.e. un morphisme bijectif de G dans lui-même). En déduire que aSa^{-1} est un p-Sylow de G.
3. Soient A une partie non vide de G, g_1 et g_2 deux éléments de G. Montrer que $g_1(g_2A) = (g_1g_2)A$.
4. Soit S un sous-groupe de G et soit $s \in S$. Montrer que $sS = S$.
5. Que se passe-t-il [6] si $\alpha = 0$?

6. Je sais, c'est vague !

Partie V - Lemme - clef et premier théorème de Sylow

Le but de cette partie est de prouver le lemme-clef suivant, et d'en déduire le premier théorème de Sylow, à savoir... qu'il existe des p-Sylow !

> **Lemme - clef :** Si G admet un p-Sylow S et si H est un sous-groupe de G, alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H. En particulier, H admet un p-Sylow.

On se met donc dans les conditions du lemme, c'est-à-dire qu'on suppose que G est un groupe fini, que S est un p-Sylow de G et que H est un sous-groupe de G. On note $n = p^\alpha \times m$ (avec $p \wedge m = 1$ et $\alpha \geq 1$) le cardinal de G (et donc S est de cardinal p^α).

1. (a) Montrer que la relation définie sur G par :

$$a \sim b \iff a^{-1} * b \in S$$

est une relation d'équivalence.

(b) Soit $a \in G$. Montrer que $\mathrm{cl}(a) = aS$ où $\mathrm{cl}(a)$ est, comme en classe, la classe d'équivalence de a (pour la relation d'équivalence de la question précédente).

(c) Montrer que, pour tout $a \in G$, $\mathrm{card}(aS) = \mathrm{card}(S)$.

(d) On note dans la suite X l'ensemble des classes d'équivalence de la question 1.(a), c'est-à-dire :

$$X = \{aS \,|\, a \in G\}$$

Montrer que $\mathrm{card}(X) = m$.

On a montré plus haut que, pour tous $a \in G$ et $h \in H, h(aS) = (ha)S$. On en déduit donc que $e(aS) = aS$ et que si h_1, h_2 sont deux éléments de H, alors $h_1(h_2(aS)) = (h_1 * h_2 * a)S$ c'est-à-dire que H agit sur l'ensemble $X = \{aS \,|\, a \in G\}$ grâce à la loi externe définie par :

$$\forall h \in H, \forall aS \in X, h.(aS) = h(aS) = (ha)S$$

On dit que H agit sur X par translation à gauche. On pourra donc mettre ou ne pas mettre le point de la loi externe puisque cela ne change rien.

2. Soit $a \in G$.

(a) Soit $x \in aSa^{-1} \cap H$. Justifier que $x(aS) = aS$.

(b) Soit $x \in H$ tel que $x(aS) = aS$. Justifier que $x \in aSa^{-1} \cap H$. On a donc prouvé que le stabilisateur de aS est $aSa^{-1} \cap H$.

(c) Justifier que que $aSa^{-1} \cap H$ est un sous-groupe de aSa^{-1} et en déduire que $aSa^{-1} \cap H$ est un p-groupe.

3. À l'aide de la question 3.(a) de la partie II, prouver qu'il existe $a \in G$ tel que

$$\frac{\mathrm{card}(H)}{\mathrm{card}(aSa^{-1} \cap H)} \wedge p = 1$$

4. Conclure.

Le lemme-clef est à présent démontré. Si G est un groupe fini quelconque de cardinal n :

- nous avons prouvé dans l'exercice 35 du chapitre 18 que G est isomorphe à un sous-groupe de S_n.
- nous prouverons dans l'exercice 35 du chapitre 21 que S_n est isomorphe à un sous-groupe de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$, ce qui implique donc que G est isomorphe à un sous-groupe H de $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.
- nous prouverons dans l'exercice 34 du chapitre 31 que $\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$ admet un p-Sylow : d'après le lemme-clef, H admet un p-Sylow donc G également d'après la question 1 de la partie IV.

Nous avons donc (en anticipant les résultats des exercices cités ci-dessus) prouvé le premier théorème de Sylow, à savoir... qu'il en existe !

> **Premier théorème de Sylow :** Si G est un groupe fini de cardinal divisible par p alors G admet (au moins) un p-Sylow.

Partie VI - Deuxième théorème de Sylow

On se donne encore G un groupe fini.

1. Soit S un p-Sylow de G. Montrer que le seul p-Sylow de S est S tout entier.
2. Soient S_1 et S_2 deux p-Sylow de G. Montrer, en utilisant le lemme-clef, qu'il existe $a \in G$ tel que $aS_1a^{-1} = S_2$. On a donc prouvé le deuxième théorème de Sylow :

> **Deuxième théorème de Sylow :** Si G est un groupe fini alors tous les p-Sylow de G sont conjugués.

Partie VII - Troisième théorème de Sylow

- On se donne encore dans cette partie G un groupe fini de cardinal $n = p^\alpha \times m$ avec $m \wedge p = 1$ et $\alpha \geq 1$.
- On note X l'ensemble des p-Sylow de G et $n_p = \text{card}(X)$ le nombre de p-Sylow de G.
- On a vu dans la partie IV que, si S est un p-Sylow de G et a un élément de G, alors aSa^{-1} est encore un p-Sylow de G.
- On montrerait facilement comme dans la partie IV (et donc on l'admettra) que pour tout $g \in G, g.(aSa^{-1})g^{-1} = (ga)S(ga)^{-1}$. On en déduit donc de même que précédemment que G agit sur X avec la loi externe :

$$\forall g \in G, \forall S \in X, g.S = gSg^{-1}$$

  On dit que G agit sur X par conjugaison. Contrairement à la partie V, on fera attention ici à mettre le point puisque $g.S$ désigne l'ensemble gSg^{-1} et non pas l'ensemble gS tel qu'il est défini dans la partie IV.
- Enfin, S agit sur X avec la même loi externe par restriction.

1. (a) En appliquant l'équation aux classes à l'ensemble X et le groupe S, prouver que $\text{card}(X) \equiv \text{card}(X^S)[p]$.
   (b) Montrer que, pour tout $s \in S, sSs^{-1} = S$: on en déduit que $S \in X^S$.
   (c) Soit $T \in X^S$. Justifier que, pour tout $s \in S, sTs^{-1} = T$.

   En appliquant la question 1.(a) à T, il vient : $\forall t \in T, tTt^{-1} = T$. Si on note N le groupe engendré par S et T, alors tous ses éléments peuvent s'écrire comme un produit d'éléments de S et d'éléments de T et donc, pour tout $n \in N, nTn^{-1} = T$ (il n'est pas demandé de le prouver).

   (d) Justifier que S et T sont des p-Sylow de N et prouver que $S = T$.
   (e) Montrer finalement que $n_p \equiv 1[p]$.
2. Montrer que, si on fait à présent agir G sur X, alors l'orbite de S est égale à X tout entier et en déduire que n_p divise m.

   On en déduit finalement le troisième théorème de Sylow :

> **Troisième théorème de Sylow :** Si G est un groupe fini de cardinal $p^\alpha \times m$ avec $p \wedge m = 1$ et $\alpha \geq 1$, et si n_p est le nombre de p-Sylow de G, alors $n_p \equiv 1[p]$ et $n_p | m$.

3. Donner le nombre de 7-Sylow d'un groupe de cardinal 63. En déduire qu'un groupe de cardinal 63 n'est pas simple, c'est-à-dire (cf. exercice 34 du chapitre 18) contient un sous-groupe distingué non trivial (i.e. différent de $\{e\}$ et de lui-même).