Théorie des groupes

Correction feuille 8

Exercice 1 (Actions de groupes matricielles)

1. $\forall a, b \in \mathrm{GL}_n(\mathbb{R}), (a.b).x = a.(b.x)$.
   $\forall x \in \mathbb{R}^n$, $Id.x = x$.
2. Soient x, y dans dans $\mathbb{R}^n \setminus \{0\}$. (x) se complète en une base B dont x est le premier vecteur et (y) se complète en une base B_2 dont y est le premier vecteur. Alors en prenant P l'application linéaire qui envoie B sur B_2, on a $Px = y$ et $P \in \mathrm{GL}_n(\mathbb{R})$.
   Il y a donc deux orbites qui sont $\{0\}$ et $\mathbb{R}^n \setminus \{0\}$.
3. Soit $P \in \mathrm{O}_n(\mathbb{R})$. Alors pour tout $y \in \mathbb{R}^n$, $\|Py\| = \|y\|$.
   Réciproquement. Soient x et y de même norme. On complète $\frac{x}{\|x\|}$ en une base orthonormée. Il existe alors P orthogonale qui envoie cette base sur celle obtenue en complétant $\frac{y}{\|y\|}$ en une base orthonormée. Alors $Px = y$ et donc x et y sont dans la même orbite.
   Les orbites sont donc les lignes de niveau de l'application norme, c'est à dire les $A_t = \{x, \ \ \|x\| = t\}$ pour $t \in \mathbb{R}_+$.

Exercice 2 On note $\star$ l'action de $\mathfrak{S}_n$ par conjugaison sur lui-même.

1. D'après la formule vue au TD 7, exercice 3. 1), les seuls conjugués possibles de $(12)(34)$ sont les trois doubles transpositions de $\mathfrak{S}_4$. Réciproquement, on peut bien les obtenir en conjuguant par Id, (23) et (24).
2. Il y a donc 3 conjugués de $(12)(34)$. D'après la relation orbite-stabilisateur appliquée à l'action de conjugaison de $\mathfrak{S}_4$ sur lui-même, on a :
   $|\mathfrak{S}_4| = |\mathrm{N}_{\mathfrak{S}_4}((12)(34))| \,.\, |\mathfrak{S}_4 \star x|$.
   Or, $\mathrm{N}_{\mathfrak{S}_4}((12)(34))$ (le normalisateur de $(12)(34)$) est l'ensemble des éléments qui fixent $(12)(34)$ par conjugaison, c'est à dire l'ensemble des éléments permutants avec $(12)(34)$.
   $8 = |\mathrm{N}_{\mathfrak{S}_4}((12)(34))|$, il y a donc 8 éléments qui commutent avec $(12)(34)$.
3. De la même façon que précédemment, les conjugués de $(12)(34)$ ne peuvent être que des doubles transpositions.
   Réciproquement : Soit $\{i, j, k, l\}$ une partie de cardinal 4 de $[\![1, n]\!]$. Montrons que $(12)(34)$ est conjugué à $(ij)(kl)$. On note $a_5, \ldots, a_n$ les autres éléments de $[\![1, n]\!]$. On a donc $[\![1, n]\!] = \{i, j, k, l, a_5, \ldots, a_n\}$.
   On pose $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & \ldots & n \\ i & j & k & l & a_5 & a_6 & \ldots & a_n \end{pmatrix}$.
   Alors $\sigma(12)(34)\sigma^{-1} = (ij)(kl)$. Et donc $(12)(34)$ est bien conjugué à toutes les doubles transpositions de $\mathfrak{S}_n$.
   Calculons le cardinal de l'orbite de $(12)(34)$ par l'action de conjugaison de $\mathfrak{S}_n$, c'est à dire le nombre de double transpositions de $\mathfrak{S}_n$.
   Choisir une double transposition revient à choisir 4 éléments parmi $[\![1, n]\!]$ puis à choisir parmi les trois doubles transpositions possibles sur un ensemble à 4 éléments.
   D'où $|\mathfrak{S}_n \star x| = 3\frac{n!}{4!(n-4)!}$. En appliquant la relation orbite stabilisateur, on obtient que :
   $|\mathrm{Stab}_{\mathfrak{S}_n}((12)(34))| = \frac{|\mathfrak{S}_n|}{|\mathfrak{S}_n \star x|} = \frac{n!4!(n-4)!}{3.n!} = 8.(n-4)!$.

Exercice 3 1. D'après la formule des classes, on a que $|E| = \sum |G.x_i|$ avec la famille des (x_i) une famille de représentants des orbites.
On a jamais que $G.x_i = \{x_i\}$ (par hypothèse "pas de point de fixe"), donc les seules tailles d'orbites possibles sont $3, 5$ et 15

On cherche donc x, y, z dans $\mathbb{N}$ tels que $3x + 5y + 15z = 17$. Avec x le nombre d'orbites de longueur 3, y le nombre d'orbites de longueur 5 et z le nombre d'orbites de longueur 15.
On a clairement pas que $z \geq 2$.
Si $z = 1$, on est ramenés à $3x + 5y = 2$, qui n'a pas de solutions dans $\mathbb{N}$.
Donc $z = 0$ et $3x + 5y = 17$.
En passant cette équation modulo 5, on a $x \equiv 4$ mod 5. Comme $3x$ doit être plus petit que 17, la seule possibilité est $x = 4$ et alors $y = 1$.
Il y a donc une orbite de longueur 5 et 4 orbites de longueur 3.

2. Les longueurs possibles pour les orbites sont les diviseurs de $|G|$, soit $1, 3, 11$ et 33. Donc la partition de X en orbites donne :
$19 = x + 3y + 11z + 33u$ avec $(x, y, z, u) \in \mathbb{N}^4$.
On a forcément que $u = 0$ et $z \leq 1$.
Si $z = 1$, l'équation prise modulo 3 devient $2 \equiv x$ mod 3, et donc $x \neq 0$.
Si $z = 0$, l'équation prise modulo 3 devient $1 \equiv x$ mod 3, et donc $x \neq 0$.
L'action a donc forcément un point fixe.

Exercice 4 (p-groupes et groupes d'ordre p^2)

1. Formule des classes : $|X| = \sum_i [G : \mathrm{Stab}_G(x_i)]$ où (x_i) est une famille de représentants des classes.
on sépare la somme comme :
$|X| = \sum_{i,[G:\mathrm{Stab}_G(x_i)]=1} [G : \mathrm{Stab}_G(x_i)] + \sum_{i,[G:\mathrm{Stab}_G(x_i)]\neq 1} [G : \mathrm{Stab}_G(x_i)]$.
$\sum_{i,[G:\mathrm{Stab}_G(x_i)]=1} [G : \mathrm{Stab}_G(x_i)] = |X_G|$
$[G : \mathrm{Stab}_G(x_i)]$ divise l'ordre de G, donc si $[G : \mathrm{Stab}_G(x_i)]$ n'est pas 1, c'est un multiple de p.
En prenant l'équation modulo p, on obtient $|X_G| \equiv |X|\ (mod\ p)$.
2. En prenant l'action de G sur lui-même par conjugaison, $Z(G)$ est l'ensemble des points fixes par cette action. D'après la question précédente, on a alors que : $|Z(G)| \equiv 0 (modp)$. Comme $Z(G)$ contient au moins l'élément neutre, il n'est pas de cardinal 0, donc est de cardinal au moins p.
3. Supposons que $|Z(G)| = p$. Soit $g \in G \setminus Z(G)$.
Alors $Z(G) \subset C_G(g)$ et $g \in C_G(g)$. Donc $|C_G(g)|$ est un sous-groupe d'ordre $> p$, donc est d'ordre p^2.
Cela signifie que $g \in Z(G)$. Absurde
Donc le centre de G ne peut pas être d'ordre p.
4. Par les questions précédentes, $Z(G)$ ne peut pas être d'ordre 1 ou p, donc est d'ordre p^2, ce qui signifie que G est abélien.
5. Soit G un groupe d'ordre p^2. Il est alors abélien. Supposons qu'il n'est pas cyclique. Alors tous les éléments non triviaux sont d'ordre p. Soit $g \in G$ différent de e. Soit $h \in G \setminus < g >$.
Alors $< g > \cap < h >= \{e\}$.
Les éléments de $< g >$ commutent avec ceux de $< h >$ car G abélien.
Pour tout $i \neq j$ plus petits que p, on a facilement que $h^i < g > \cap h^j < g >= /emptyset$. Donc les $h^j < g >$ réalisent une partition de G en classes d'équivalences, d'où $< g >< h >= G$.
Par théorème de produit direct, $G \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.
Bilan : Tout groupe d'ordre p^2 est isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$ ou à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Exercice 5 (Sous-groupes d'indice le plus petit premier)

1. on note $|G| = ps$ avec s n'ayant que des facteurs premiers $\geq p$.
$|im(\varphi)| \mid |G| = ps$.
$im(\varphi)$ est un sous-groupe de $\mathfrak{S}_p$, donc $|im(\varphi)| \mid p!$.
On en déduit que $|im(\varphi)| \mid p$. Comme $|im(\varphi)|$ n'est pas triviale, on a $|im(\varphi)| = p$.
2. D'où $|G| = p.\,|\ker\varphi|$ et $\ker\varphi$ est d'indice p.
$\ker\varphi = \bigcap_{g\in G} \mathrm{Stab}_G(gH)$ et $H = \mathrm{Stab}_G(e)$ donc $\ker\varphi \subset H$. Comme ils sont de même indice dans un groupe fini, on a $H = \ker\varphi$.

Exercice 6 1. Soit x sur le cercle unité. Notons α l'angle de Ox avec l'axe des abscisses. Alors R_0 la rotation d'angle α centrée en 0 est un élément de $\mathrm{O}_2^+(\mathbb{R})$ tel que $R_0.1 = x$. Donc x est dans l'orbite de 1. Il n'y a donc qu'une seule orbite.

2. Soit $x \neq 1$ sur la sphère unité. Alors il existe un unique plan vectoriel P contenant 1 et x. Notons D la droite vectorielle orthogonale à P. Notons α l'angle de Ox avec l'axe des abscisses. Alors R_1 la rotation d'angle α autour de la droite D est un élément de $\mathrm{O}_3^+(\mathbb{R})$ tel que $R_1.1 = x$. Donc toute la sphère unité est dans l'orbite de 1. Il n'y a donc qu'une seule orbite.

Exercice 7 (Isométries du tétraèdre régulier) Une isométrie préserve les distances. Or les seuls segments dans le tétraèdre de longueur supérieure ou égale à $\sqrt{2}$ sont les arrêtes, donc une arrête est envoyée sur une arrête et un sommet sur un sommet. Comme les isométries sont inversibles, une isométrie permute les sommets du tétraèdre et G le groupe d'isométrie agit sur $\{a_1, a_2, a_3, a_4\}$.

On note $\varphi : G \to \mathfrak{S}_4$ le morphisme défini par cette action.

φ est injective : En effet, si $f \in \ker\varphi$, alors f est une isométrie de $\mathbb{R}^3$ fixant 4 points non-coplanaires donc est l'identité.

φ est surjective : La transposition des sommets a_1 et a_2 peut être réalisée par s la symétrie par rapport au plan contenant a_3, a_4 et le milieu de $[a_1, a_2]$ (faire un dessin). Il en va de même pour toute les transpositions de sommets. Comme les transpositions engendrent $\mathfrak{S}_4$, φ est surjective.

Donc $G \cong \mathfrak{S}_4$.

On note G^+ l'ensemble des isométries positives. $G^+ = \ker det$. det est surjective de G dans $\{-1, 1\}$, donc $G/\{-1, 1\} \cong G^+$. Le seul sous-groupe d'indice 2 dans $\mathfrak{S}_4$ est $\mathfrak{A}_4$, donc $G^+ = \mathfrak{A}_4$.

Exercice 8 (Devinette) Soit $n \geq 1$.

Supposons pour simplifier que les noms des mathématiciens sont les entiers de 1 à $2n$.

Les mathématiciens décident d'une numérotation des coffres de 1 à $2n$.

Ainsi, la répartition des noms dans les coffres est simplement le choix d'une permutation $\sigma \in \mathfrak{S}_{2n}$.

La stratégie est :

Le mathématicien k ouvre le k-ième coffre. Si il trouve son nom, il peut ouvrir n'importe quel autres coffres pour arriver à un total de n. Sinon, le coffre contient le nom $k_1 \neq k$. Le mathématicien va alors ouvrir le coffre k_1. A nouveau, si il trouve son nom, il a terminé, sinon, il y trouve un nom k_2, et va ouvrir le coffre k_2. Il continue ce processus jusqu'à avoir trouvé son nom ou jusqu'à ce qu'il ait ouvert n coffres sans le trouver. De la même manière que l'on fait pour déterminer la décomposition d'une permutation en produit de cycles disjoints, le mathématicien suit le cycle dans lequel est son nom.

Le point clé de la stratégie est : Le mathématicien k trouve son nom si et seulement si k n'est pas dans un m-cycle de σ avec $m > n$.

D'où la propriété : La stratégie est gagnante si est seulement si la décomposition de σ ne contient pas de cycle de longueur plus grande que $n + 1$.

Reste à dénombrer ces cas.

Calcul de a_m le nombre de permutations de $\mathfrak{S}_{2n}$ contenant un m-cycle, avec $m > n$:

1/ Il faut choisir les m entiers du cycle parmi les $2n$.

2/ Il y a $(m-1)!$ m-cycles possibles sur ces points.

3/ il y a $|\mathfrak{S}_{2n-m}| = (2n-m)!$ possibilités de permuter les $2n - m$ points restants.

Soit un total de $\frac{(2n)!}{m!(2n-m)!}.(m-1)!.(2n-m)!$ permutations de $\mathfrak{S}_{2n}$ contenant un m-cycle.

$a_m = \frac{(2n)!}{m!(2n-m)!}.(m-1)!.(2n-m)! = \frac{(2n)!}{m}$.

Le nombre total de possibilités pour σ telles que la stratégie soit perdante est $\displaystyle\sum_{m=n+1}^{2n} a_m = (2n)! \sum_{m=n+1}^{2n} \frac{1}{m}$.

Pour avoir la proportion de permutations σ perdantes, il suffit de diviser par $(2n)!$.

La probabilité de perdre est alors $\displaystyle\sum_{m=n+1}^{2n} \frac{1}{m}$.

Par comparaison série-intégrale, on obtient que $\displaystyle\sum_{m=n+1}^{2n} \frac{1}{m} \leqslant ln(2n) - ln(n+1) \leqslant ln(\frac{2n}{n+1}) \leq ln(2)$.

La probabilité que la stratégie soit gagnante est donc supérieure à $1 - ln(2) > 0.3$.