Groupe opérant sur un ensemble

Préparation à l'agrégation interne année 2009-10

Séance du mardi 2 décembre

Programme de la séance :

1. On traitera les exercices 3.5 et 3.6 de la feuille 2
2. G est un sous-groupe d'ordre n ; Démontrer que pour tout diviseur d de n, il existe un unique sous-groupe H de G d'ordre d et il est cyclique (par édouard Dorard).
3. Un groupe ayant tous ses sous-groupes (stricts) cycliques est-il lui-même cyclique ?
4. Questions autour du théorème des restes chinois
   (a) Rappel rapide de la démonstration (les entiers m et n sont premiers entre eux) : On définit l'application

   $$\begin{array}{rcl} f:\mathbb{Z} & \rightarrow & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \\ x & \mapsto & (x \bmod m; x \bmod n) \end{array}$$

   et on vérifie que f est un homomorphisme (d'anneaux) de noyau $mn\mathbb{Z}$ donc d'après la propriété universelle du quotient il existe $\overline{f}$ un homomorphisme de $\mathbb{Z}/mn\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ et de plus $\overline{f}$ est injectif puis bijectif par cardinalité. Exhiber l'isomorphisme inverse de $\overline{f}$

   (b) Résoudre le système $\left\{\begin{array}{l} x \pmod 5 \\ x \pmod 3 \end{array}\right.$

   (c) La réciproque du théorème des restes chinois est-elle vraie ?

   (d) Démontrer que $\mathbb{Z}/20\mathbb{Z}\times\mathbb{Z}/15\mathbb{Z}\times\mathbb{Z}/30\mathbb{Z}$ est isomorphe à $\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}\times\mathbb{Z}/c\mathbb{Z}$ avec $a|b|c$.
5. Les exercices ci-dessous.

1 Notations et quelques rappels

- Si E est un ensemble fini, on notera $\#E$ son cardinal.
- Si σ est une permutation de $\mathfrak{S}_n$, on note :

$$supp(\sigma) = \{x \in \{1, ..., n\}/\sigma(x) \neq x\}$$

.
- Soit G un groupe et H un sous-groupe de G,on dit que H est distingué (ou invariant ou normal) si $gHg^{-1} = H$ pour tout $g \in G$.
- On dit qu'un groupe est simple s'il n'admet que deux sous-groupes distingués : $\{1\}$ et lui-même.

2 Groupe symétrique

Exercice 2.1

1. Déterminer tous les sous groupes de $\mathfrak{A}_4$.
2. Ecrire les produits suivants sous forme de produits de cycles à supports disjoints :
   (a) (1 2 3 4 5)(1 5 6)(2 4 6).
   (b) (1 2)(2 3)(3 4)(4 5)(5 1).

Exercice 2.2 (Générateurs de $\mathfrak{S}_n$)
Dans cet exercice, n est un entier supérieur ou égal à 2.

1. Démontrer que $\mathfrak{S}_n$ est engendré par les transpositions.
2. Démontrer que $\mathfrak{S}_n$ est engendré par $(1,\,2)$, $(1,\,3), ..., (1,\,n)$.
3. En déduire que $\mathfrak{S}_n$ est engendré par $(1,\,2)$, $(2,\,3), ..., (n-1,\,n)$.
4. (a) Démontrer que, dans $\mathfrak{S}_n$: $(i;\,i+1) = (1,\,2, ...,\,n)^{i-1}(1,2)(1,\,2, ...,\,n)^{1-i}$ pour tout $i \in \{2; ...; n-1\}$.
   (b) En déduire que $\mathfrak{S}_n$ est engendré par $(1,\,2, ...,\,n)$ et $(1,2)$.
5. Démontrer que les 3-cycles engendrent $\mathfrak{A}_n$ où $n \geq 3$.

Exercice 2.3 (Simplicité de $\mathfrak{A}_n$ pour $n \geq 5$)

1. Etudier les cas de $\mathfrak{A}_3$ et de $\mathfrak{A}_4$
2. Soit n un entier supérieur ou égal à 5.
   (a) Démontrer que deux 3-cycles sont conjugués dans $\mathfrak{A}_n$.
   (b) Soit H un sous groupe invariant de $\mathfrak{A}_n$ non réduit à l'élément neutre. D'après la question précédente, il suffit de démontrer que H contient un 3-cycle. Soit g un élément de H distinct de 1 de plus petit support. On suppose que $\#\, supp(g) \geq 4$ (sinon c'est fini).
   - Question préliminaire : Démontrer que pour tout $\sigma \in \mathfrak{A}_n$, $[g;\sigma] = g\sigma g^{-1}\sigma^{-1} \in H$.
   - Supposons $\#\, supp(g) = 4$; démontrer que $g = (a,b)(c,d)$ avec a,b,c,d deux à deux distincts puis en choisissant $\sigma = (a,b,e)$ avec e distinct de a,b,c et d montrer que $[g;\sigma]$ est un 3-cycle.
   - Traiter de manière analogue le cas où $\#\, supp(g) = 5$.
   - On suppose que $\#\, supp(g) \geq 6$ et on pose $\sigma = (a,b,c)$ où $a \in supp(g), b = g(a)$ et $c \neq a,b,g(b)$, étudier $[g;\sigma]$ et conclure.

3 Applications à la géométrie

Exercice 3.1 (groupe diédral)

Soit n un entier supérieur à 3, on appelle D_n le groupe des isométries du plan qui préserve un polygone régulier à n côtés (on notera $A_0, A_1, ..., A_{n-1}$ les sommets du polygone et O son centre).

1. Démontrer que D_n est d'ordre $2n$ (on pourra étudier l'orbite et le fixateur de A_0 sous l'action de D_n sur l'ensemble des sommets du polygone).
2. Soit r la rotation de centre O et d'angle $\dfrac{2\pi}{n}$ et s la symétrie d'axe (OA_0).
   (a) Démontrer que $D_n =< r, s >$.
   (b) Que vaut srs^{-1} ?
3. Dresser les tables de multiplication de D_3 et de D_4.

Exercice 3.2 (Isométries du cube)

1. Préliminaire :Soit E un espace euclidien et s une involution de E (c'est-à-dire $s \in L(E)$ $s^2 = id$; démontrer que les propriétés suivantes sont équivalentes :
   (a) s est orthogonale
   (b) $E = \ker(s - id) \oplus \ker(s + id)$ et la somme est orthogonale.
2. On note G le groupe des isométries qui préserve le cube $A_1A_2A_3A_4A_5A_6A_7A_8$ (avec $\overrightarrow{A_1A_5} = \overrightarrow{A_2A_6} = \overrightarrow{A_3A_7} = \overrightarrow{A_4A_8}$),$O$ son centre et G^+ le sous-groupe des isométries positives de G.
   (a) Démontrer que $f(O)$ pour tout $f \in G$; on peut considérer que G est un sous-groupe de $O(\mathbb{R}^3)$.
   (b) Démontrer que G agit sur les grandes diagonales du cube. On note alors $\varphi : G \to \mathfrak{S}_4$ l'homomorphisme (de groupes) induit par cette action.
   (c) Démontrer que φ est surjective (On pourra commencer par étudier le retournement passant par le milieu de $[A_1A_2]$).
   (d) Démontrer que $\ker\varphi = \{-id; id\}$ (On pourra utiliser la question préliminaire). Quel est donc le cardinal de G ?
   (e) Démontrer que $\varphi_{|G^+}$ est un isomorphisme.
   (f) Démontrer que $G \simeq \mathfrak{S}_4 \times \{Id; -Id\}$.
   (g) (Pour les courageux) Donner tous les éléments de G, en précisant leur ordre.

4 Applications aux groupes d'ordre p^n

Exercice 4.1

1. Démontrer que tout groupe d'ordre p premier est cyclique.
2. En déduire, à isomorphisme près, les groupes d'ordre 2, 3, 5, 7, 11...
3. Déterminer tous les groupes abéliens simples.

Exercice 4.2
Dans cet exercice, p désigne un nombre premier.

1. Soit G est un groupe d'ordre p^n agissant sur un ensemble fini E ; on note $\mathrm{Fix} = \{x \in E / \forall g \in G, g.x = x\}$.
   Démontrer que $\#\mathrm{Fix} \equiv \#E \pmod p$.
2. Application :
   (a) Démontrer que le centre Z d'un groupe $G \neq \{1\}$ d'ordre une puissance de p n'est jamais trivial(on fera agir G sur lui-même par conjugaison).
   (b) En déduire tous les groupes d'ordre p^2.
   (c) En déduire, à isomorphisme près, les groupes d'ordre 4, 9,...
   (d) Existe-t-il un groupe non commutatif d'ordre p^3 ? (Considérer le sous-groupe G de $\mathcal{M}_3(\mathbb{Z}/p\mathbb{Z})$ constitué des matrices de la forme

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \text{ où } a, b, c \in \mathbb{Z}/p\mathbb{Z}.$$

Exercice 4.3 (Théorème de Sylow)
On rappelle si p est un nombre premier, on appelle p-groupe un groupe fini d'ordre une puissance de p.
L'objectif de cet exercice est de démontrer le théorème suivant :

> Soit G un groupe fini d'ordre $n = p^r \times m$ où p est premier,$r, m \in \mathbb{N}^*$ et m non divisible par p.
>
> – Il existe des sous groupes de G d'ordre p^r et de tels sous groupes sont conjugués (on les appelle p-sous groupes de Sylow).
> – Tout p-sous groupe de G est contenu dans un p-Sylow.
> – Le nombre s_p de p-Sylow divise m et est congru à 1 modulo p.

1. Existence d'un p-Sylow
   (a) Montrer que $\begin{pmatrix} m \\ p^r \end{pmatrix} = m \mod p$.
   (Indication : développer $(X+Y)^n$ dans $\mathbb{Z}[X, Y]$ puis dans $\mathbb{Z}/p\mathbb{Z}[X, Y]$).
   (b) Notons l'ensemble $\mathcal{E}$ des parties de G à p^r éléments et $\bullet : \begin{array}{ccc} G \times \mathcal{E} & \to & \mathcal{E} \\ (g, E) & \mapsto & g.E \end{array}$
   – Vérifier que $\bullet$ définie une action de G sur $\mathcal{E}$.
   – Démontrer qu'il existe une orbite, que l'on notera Σ, dont le cardinal n'est pas un multiple de p.
   – Soit $x \in \Sigma$ et H_x son fixateur,démontrer que p^r divise le cardinal de H_x.
   – Démontrer que le cardinal de H_x est inférieur à p^r.
   – Conclure.
2. Soit H un p-Sylow et K un p-groupe. G agit sur G/H, on restreint cette action à K.
   (a) On note F l'ensemble des points fixes, démontrer que $\#F = m \mod p$.
   (b) Démontrer qu'il existe $g \in G$ tel que $\mathrm{K} \in gHg^-1$
3. On note $\mathcal{P}$ l'ensemble des p-Sylow de G.
   (a) Démontrer que G agit sur $\mathcal{P}$ par conjugaison,
   (b) En déduire que s_p divise m.
4. En restreignant l'action (par conjugaison) de G sur $\mathcal{P}$ à H ; démontrer que $s_p = 1 \mod p$.
5. Application : démontrer qu'un groupe d'ordre $p \times q$, où p et q sont des nombres premiers, n'est jamais simple.