Algèbre et théorie de Galois - TD1

Exercice 1 : Donner une représentation fidèle M de S_n sur un $\mathbb{Z}$-module convenable. En déduire une description matricielle des éléments de S_n. Si $\sigma \in S_n$, que vaut $\det(\sigma)$?

Exercice 2 : Expliciter les classes de conjugaison dans S_3 et S_4. Déterminer la cardinalité et l'ordre commun de tous les éléments de chaque classe de conjugaison.

Exercice 3 : Soit $n \geq 3$.

a) Montrer que le produit de deux transpositions distinctes est un 3-cycle ou un produit de deux 3-cycles. En déduire que le groupe A_n est engendré par les 3-cycles.

b) Montrer qu'un sous-groupe $H \subset S_n$ d'ordre $n!/2$ est forcément égal à $H = A_n$.

Exercice 4 : Montrer que si un groupe simple G agit transitivement sur un ensemble X tel que $|X| \geq 2$, alors l'action est fidèle. Que se passe-t'il si G n'est pas simple ?

Exercice 5 : Conjugaison dans S_n et A_n.

a) Pour tout $\sigma \in S_n$, déterminer $|C_{S_n}(\sigma)|$ en termes de la longueur des cycles disjoints dans la notation cyclique de σ.

b) Soit $\sigma \in A_n$ ($n \geq 2$). Montrer qu'il y a deux cas possibles :

i) $C_{S_n}(\sigma) \subset A_n \Rightarrow C_{S_n}(\sigma) \subset C_{A_n}(\sigma) \Rightarrow$ la classe de conjugaison de σ and S_n est une réunion de deux classes de conjugaison dans A_n.

ii) $C_{S_n}(\sigma) \subsetneq A_n \Rightarrow C_{A_n}(\sigma)$ est un sous-groupe de $C_{S_n}(\sigma)$ d'indice $2 \Rightarrow$ la classe de conjugaison de σ dans S_n est égale à la classe de conjugaison de σ dans A_n.

c) Distinguer les deux cas précédents en termes du type cyclique de σ.

d) Expliciter les classes de conjugaison dans A_3 et A_4.

Exercice 6 : Si $X \subset \mathbb{R}^d$ est un sous-ensemble, on note $G(X) = \{g \in O(n) |\, g(X) = X\}$ et $G^+(X) = \{g \in O^+(n) |\, g(X) = X\}$. Soit $C_n \subset \mathbb{R}^n$ l'hypercube de sommets $(\pm 1, \ldots, \pm 1)$.

a) Montrer que l'action de $G(C_3)$ sur les 4 diagonales de C_3 induit un isomorphisme $G^+(C_3) \xrightarrow{\sim} S_4$.

b) En déduire que $G(C_3)$ est isomorphe à $S_4 \times \{\pm 1\}$.

c) Ecrire explicitement toutes les matrices de $G(C_3) \subset O(3)$.

d) Calculer l'ordre de $G(C_n)$.

e) Ecrire explicitement toutes les matrices de $G(C_n)$.

f) Montrer que le groupe $G(C_n)$ contient un sous-groupe N (resp. H) isomorphe à $\{\pm 1\}^n$ (resp. à S_n). Décrire la structure de $G(C_n)$ en termes de N et H.

Exercice 7 : Soit T le tétraèdre régulier de centre l'origine. En choisissant une numérotation des quatres sommets de T, on obtient un morphisme de groupes $\alpha : G(T) \to S_4$. Montrer que α définit des isomorphismes $G(T) \xrightarrow{\sim} S_4$ et $G^+(T) \xrightarrow{\sim} A_4$.

Exercice 8 : Le "corps à un élément" (Tits). Soit K un corps fini et $q = |K|$. Calculer ($n \geq 1$) :

a) $|\mathrm{GL}_n(K)|$, $|\mathrm{SL}_n(K)|$.

b) $|\mathrm{Gr}_n^k(K)|$ où $\mathrm{Gr}_n^k(K)$ est l'ensemble $\{V \subset K^n |\, V$ sous-espace vectoriel de dimension $k\}$, pour $1 \leq k \leq n-1$.

c) $|\mathrm{GA}_n(K)|$.

d) $|\mathrm{Graff}_n^k(K)|$ pour $\mathrm{Graff}_n^k(K) = \{V \subset K^n | \, V \text{ sous-espace affine de dimension } k\}$, pour $1 \leq k \leq n-1$.

e) Pour chaque domaine X de l'exercice, on note $|X(\mathbb{F}_1)| := \lim_{q \to 1}(q-1)^{-k}|X(\mathbb{F}_q)|$ où k est le plus petit entier naturel pour lequel cette limite n'est pas nulle. Calculer $|X(\mathbb{F}_1)|$ pour chaque domaine X. Donner des ensembles naturels, qu'on notera $X(\mathbb{F}_1)$, représentant ces cardinaux.

Exercice 9 : (Difficile) Construire un ensemble naturel à 5 éléments muni d'une action de $\mathrm{PSL}_2(\mathbb{F}_5)$. En déduire un isomorphisme $\mathrm{PSL}_2(\mathbb{F}_5) \cong A_5$.

Exercice 10 : Soit C un groupe cyclique d'ordre $n \geq 1$. Soit σ un générateur de C.

a) Montrer que tout sous-groupe de C est cyclique.

b) Pour tout $a \in \{1, \ldots, n\}$, montrer que l'ordre de σ^a est égal au dénominateur d (on écrit $\frac{a}{n} = \frac{p}{d}$ avec $(p,d) = 1$) de la fraction $\frac{a}{n}$.

c) Montrer que, pour tout diviseur d de n, le nombre d'éléments de C d'ordre d est égal à $\varphi(d)$.

Exercice 11 : Montrer que $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.

Exercice 12 :

a) Montrer qu'il n'y a que quatre anneaux (commutatifs, unitaires) à 4 éléments, à savoir $A = \mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_2[\epsilon]/(\epsilon^2)$.

b) Dans chacun des cas, déterminer la structure des groupes $A^\times$ et $GA_1(A) \subset S_A \xrightarrow{\sim} S_4$.

Exercice 13 :

a) Montrer que l'ordre du groupe $G = \mathrm{PGL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2) = \mathrm{SL}_3(\mathbb{F}_2) = \mathrm{PSL}_3(\mathbb{F}_2)$ est égal à $168 = |\mathrm{PSL}_2(\mathbb{F}_7)|$.

b) Définir un morphisme injectif de groupe $G \hookrightarrow S_7$.

Exercice 14 : Sous-groupes finis de $\mathrm{SO}(3)$**.** Soit G un sous-groupe fini de $\mathrm{SO}(3)$. On considère l'action naturelle de $\mathrm{SO}(3)$ sur la sphère S^2.

a) Montrer que tout élément non trivial g de $\mathrm{SO}(3)$ a exactement deux points fixes sur S^2.

b) On note $X \subset S^2$ l'ensemble (fini) des axes des éléments de G, c'est à dire l'ensemble des points de S^2 qui ont un stabilisateur non trivial dans G. Montrer que G agit sur X.

c) On note $Y = \{(x,g) | \, x \in X,\, g \in G \backslash \{1\},\, gx = x\}$. Calculer le cardinal de Y de deux manières pour montrer l'égalité

$$2.|G| - 2 = \sum_{x \in X}(|G_x| - 1) = \sum_{[y] \in X/G} |G| - |yG|.$$

où G_x désigne le stabilisateur de x dans G et $[y] = yG$ est l'orbite de y sous G.

d) Si $n = |G|$, montrer que

$$2 - \frac{2}{n} = \sum_{y \in X/G} 1 - \frac{1}{|G_y|}.$$

e) En déduire que la somme ci-dessus ne peut contenir que $k = 2$ ou 3 termes.

f) Si $k = 2$, montrer que tous les éléments de G ont même axe de rotation : G est un groupe cyclique.

g) Si $k = 3$, on note $a \leq b \leq c$ les ordres des stabilisateurs. Montrer que les seules possibilités pour ces ordres sont $(2, 2, n/2)$ (groupe dihédral), $(2, 3, 3)$ (tétraèdre), $(2, 3, 4)$ (cube), $(2, 3, 5)$ (dodécaèdre).

Exercice 15 : Quaternions et groupes de Chevalley linéaires. Soit K un corps commutatif de caractéristique différente de 2 et $a, b \in K^\times$. On définit les quaternions $\mathbb{H}_{a,b}$ comme la K-algèbre de base 1, i, j, $k = ij$, où les éléments i, j vérifient les relations

$$i^2 = a,\ j^2 = b,\ ij = -ji.$$

Les quaternions classiques d'hamilton se retrouvent en posant $a = b = -1$. Pour $h = x+yi+zj+tk$ un quaternion, on appelle $Nm(h) = x^2 - ay^2 - bz^2 + abt^2$ la norme de h. On remarque que les quaternions peuvent s'écrire comme des matrices à coordonnées dans une extension de K contenant une racine carrée de a et de b de la forme

$$\begin{pmatrix} x + \sqrt{a}y & \sqrt{b}(z + \sqrt{a}t) \\ \sqrt{b}(z - \sqrt{a}t) & x - \sqrt{a}y \end{pmatrix}$$

et que la norme correspond alors au déterminant.

a) Donner une description du groupe spécial orthogonal de la forme quadratique $Nm(0, y, z, t)$ sur K^3 en termes des quaternions.

b) Exprimer le sous-groupe $G^+(C_3) \subset \mathrm{SO}(3)$ en termes des quaternions.

c) En déduire que pour tout nombre premier $p \neq 2$, il existe un morphisme injectif de groupes $\beta : S_4 \to \mathrm{PGL}_2(\mathbb{F}_p)$ tel que $\beta(A_4) \subset \mathrm{PSL}_2(\mathbb{F}_p)$.

d) Montrer que $\beta(S_4) \subset \mathrm{PSL}_2(\mathbb{F}_p)$ si et seulement si 2 est un carré dans $\mathbb{F}_p$ (si et seulement si $p \equiv \pm 1 \mod 8$).

e) En déduire que l'action du groupe $G_5 = \mathrm{PGL}_2(\mathbb{F}_5)$ (resp. $G_7 = \mathrm{PSL}_2(\mathbb{F}_7)$) sur l'espace homogène $X_5 = G_5/\beta(S_4)$ (resp. sur $X_7 = G_7/\beta(S_4)$) donne lieu à un morphisme de groupes $G_p \to S_{X_p}$ $(p = 5, 7)$.

f) En admettant que l'action de G_5 sur X_5 est fidèle, montrer que $\mathrm{PSL}_2(\mathbb{F}_5) = A_5$.

Exercice 16 : Montrer qu'un groupe abélien non nul est simple si et seulement si il est cyclique d'ordre p, où p est un nombre premier.

Exercice 17 :

a) Décrire tous les groupes abéliens Y (à isomorphisme près) d'ordre $|Y| = 8$.

b) Décrire tous les groupes abéliens X (à isomorphisme près) d'ordre $|X| = 16$. Pour tout X décrire tous les Y (d'ordre $|Y| = 8$) qui sont isomorphes à un sous-groupe de X.

Exercice 18 : On rappelle que si X est un groupe abélien, sa partie de p-torsion $X[p]$ est définie par $X[p] = \{x \in X \,|\, px = 0\}$ et sa partie p-primaire est définie par $X(p) = \{x \in X \,|\, \exists n,\ p^n x = 0\}$. Soit X un groupe abélien d'ordre $|X| = 216$. Déterminer la structure de X en terme de ses parties 2- et 3-primaires. Déterminer la structure de X en terme des i et j tels que $|X[2]| = 2^i$ et $|X[3]| = 3^j$. Que se passe-t-il si l'on remplace 216 par 432 ?

Exercice 19 : Soit X un groupe abélien d'ordre $|X| = n$. Montrer que, pour tout diviseur d de n il existe un sous-groupe (resp., un quotient de X) d'ordre d.

Exercice 20 :

a) Décrire tous les groupes abéliens X (à isomorphisme près) qui admettent un sous-groupe Y isomorphe à $\mathbb{Z}/4\mathbb{Z}$ tel que X/Y soit isomorphe à $\mathbb{Z}/2\mathbb{Z}$.

b) Idem pour $Y \cong \mathbb{Z}/6\mathbb{Z}$ et $X/Y \cong \mathbb{Z}/12\mathbb{Z}$.