Université Pierre et Marie Curie — Année 2013-2014
Master de Mathématiques — MM002 Algèbre et théorie de Galois
Professeur: J. Oesterlé — E. Lepage

Feuille 1 - énoncés

Le groupe symétrique sur $[1, n]$ est noté $\mathfrak{S}_n$ et le groupe alterné $\mathfrak{A}_n$.

Exercice 1 Montrer que si la décomposition en cycles (de supports disjoints) de $\sigma \in \mathfrak{S}_n$ comporte r cycles (en comptant aussi les cycles de longueur 1), alors la signature de σ est $(-1)^{n-r}$.

Exercice 2

a) Écrire la table de multiplication de $\mathfrak{S}_3$.

b) Expliciter les classes de conjugaison de $\mathfrak{S}_3$ et de $\mathfrak{S}_4$. Pour chacune d'elles, préciser son cardinal et l'ordre de ses éléments.

c) énumérer tous les sous-groupes de $\mathfrak{S}_3$ et de $\mathfrak{A}_4$. Lesquels sont distingués ?

Exercice 3 Montrer que le groupe symétrique $\mathfrak{S}_n$ admet les systèmes minimaux de générateurs suivants :

a) Les transpositions $(1i)$ pour $2 \leq i \leq n$.

b) Les transpositions $(i(i+1))$ pour $1 \leq i \leq n-1$.

c) Le cycle $(12 \dots n)$ et la transposition (12).

d) Si n est premier, n'importe quel n-cycle et n'importe quelle transposition.

Exercice 4

a) Décomposer $(25)(56)(13254)$ et $(123)(124)$ en cycles à supports disjoints.

b) Faire de même pour l'élément $x \mapsto 10 - x$ de $\mathfrak{S}_9$

c) Faire de même pour $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 7 & 8 & 3 & 2 & 1 & 9 & 4 & 6 \end{pmatrix}$.

Exercice 5

a) Montrer que le groupe alterné $\mathfrak{A}_n$ est engendré par les 3-cycles.

b) Montrer que le seul sous-groupe de $\mathfrak{S}_n$ d'ordre $n!/2$ est $\mathfrak{A}_n$, pour $n \geq 2$.

Exercice 6 Montrer que $\mathfrak{A}_n$ admet les systèmes de générateurs suivants :

a) Les 3-cycles $(12i)$ pour $3 \leq i \leq n$.

b) Les 3-cycles $(i(i+1)(i+2))$ pour $1 \leq i \leq n-2$.

c) Montrer que le premier système est minimal, mais que le second ne l'est pas si $n \geq 5$.

Exercice 7 Montrer que si un groupe simple G agit transitivement sur un ensemble X tel que $|X| > 1$, l'action est fidèle.

Exercice 8

a) Montrer que le centralisteur d'un n-cycle $\sigma \in \mathfrak{S}_n$ est le groupe engendré par σ :

$$C_{\mathfrak{S}_n}(\sigma) =< \sigma >\simeq \mathbb{Z}/n\mathbb{Z}.$$

On appelle *partition* de n une suite $\kappa = (k_1, k_2, \ldots, k_n)$ d'entiers naturels tels que $\sum ik_i = n$. À toute permutation $\sigma \in \mathfrak{S}_n$ on fait correspondre une partition $\kappa(\sigma)$ de la façon suivante : k_i est le nombre de i-cycles qui interviennent dans la décomposition de σ en cycles à supports disjoints. Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si et seulement si elles ont même partition associée.

b) Expliciter en fonction de $\kappa(\sigma)$ l'ordre $|C_{\mathfrak{S}_n}(\sigma)|$ du centralisateur de $\sigma \in \mathfrak{S}_n$.

c) Soit $\sigma \in \mathfrak{A}_n$ une permutation paire, avec $n \geq 2$. Montrer qu'il y a deux cas possibles :

- $C_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n$. On a alors $C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma)$ et la classe de conjugaison de σ dans $\mathfrak{S}_n$ est réunion disjointe de deux classes de conjugaison dans $\mathfrak{A}_n$ de même cardinal.

- $C_{\mathfrak{S}_n}(\sigma) \not\subset \mathfrak{A}_n$. Alors $C_{\mathfrak{A}_n}(\sigma)$ est un sous-groupe d'indice 2 de $C_{\mathfrak{S}_n}(\sigma)$ et la classe de conjugaison de σ dans $\mathfrak{S}_n$ est égale à sa classe de conjugaison dans $\mathfrak{A}_n$.

d) Déterminer en fonction de la partition $\kappa(\sigma)$ dans lequel des cas précédents on se trouve.

e) Expliciter les classes de conjugaison dans $\mathfrak{A}_3$ et $\mathfrak{A}_4$.

Exercice 9 Soit $\sigma \in \mathfrak{S}_n$ une permutation.

a) Montrer que si au moins un cycle de σ est de longueur $k \geq 4$, il existe une permutation $\tau \in \mathfrak{A}_n$ telle que $\tau\sigma\tau^{-1}\sigma^{-1}$ est un 3-cycle.

b) Montrer que c'est encore le cas si σ a un 3-cycle et un 2-cycle, ou un 3-cycle et deux points fixes, ou un 2-cycle et un point fixe.

c) Montrer que si σ a deux 3-cycles, il existe une permutation $\tau \in \mathfrak{A}_n$ telle que $\tau\sigma\tau^{-1}\sigma^{-1}$ est un 5-cycle.

d) Montrer que si σ a trois 2-cycles, il existe une permutation $\tau \in \mathfrak{A}_n$ telle que $\tau\sigma\tau^{-1}\sigma^{-1}$ est un produit de deux 3-cycles disjoints.

e) Montrer que pour $n \geq 5$, $\mathfrak{A}_n$ est un groupe simple.

Exercice 10 Soit H un sous-groupe d'indice n de $\mathfrak{S}_n$. En faisant agir $\mathfrak{S}_n$ sur $\mathfrak{S}_n/H$, montrer que H est isomorphe à $\mathfrak{S}_{n-1}$.

Exercice 11 Soit G un groupe fini d'ordre $n > 1$, p le plus petit facteur premier de n et H un sous-groupe de G d'indice p. Montrer que H est distingué dans G. On pourra étudier le noyau de l'action de G sur l'ensemble quotient G/H.

Exercice 12 Soit G un groupe, H un sous-groupe distingué de G et K un sous-groupe quelconque de G. Montrer que l'image de K par la projection naturelle $K \to G \to G/H$ est isomorphe à $K/(H \cap K)$.

Exercice 13 Soit T un tétraèdre régulier centré à l'origine. Montrer que l'action de $G(T)$ sur les sommets de T induit des isomorphismes $G(T) \simeq \mathfrak{S}_4$ et $G^+(T) \simeq \mathfrak{A}_4$.

Exercice 14 Soit C un cube centré à l'origine.

a) Montrer que l'action sur les quatre diagonales du cube induit un isomorphisme $\beta : G^+(C) \simeq \mathfrak{S}_4$. En déduire que $G(C)$ est isomorphe à $\{\pm 1\} \times \mathfrak{S}_4$.

b) Expliciter les 48 matrices des éléments de $G(C)$ dans le cas où les sommets du cube sont $\begin{pmatrix} \pm 1 \\ \pm 1 \\ \pm 1 \end{pmatrix}$.

Exercice 15 L'hypercube $C(n)$ est l'enveloppe convexe dans $\mathbb{R}^n$ des points (les *sommets*) dont toutes les coordonnées sont dans $\{\pm 1\}$. Montrer que le cardinal de $G(C(n))$ est $2^n n!$. Expliciter les matrices des éléments de $G(C(n))$. Montrer que $G(C(n))$ a un sous groupe H isomorphe à $\{\pm 1\}^n$ et un sous-groupe distingué N isomorphe à $\mathfrak{S}_n$. Expliciter la structure de $G(C(n))$ en termes de N et H. Attention, ce n'est pas un produit direct.

Exercice 16 Soit G un sous-groupe fini d'ordre $n > 1$ du groupe $SO(3)$ des rotations de $\mathbb{R}^3$. On définit l'ensemble

$$Z = \{(\rho, x) \in (G \setminus \{Id\}) \times \mathbb{R}^3;\ ||x|| = 1 \text{ et } \rho(x) = x\}.$$

a) Montrer que $|Z| = 2(n-1)$.

b) On note P l'ensemble des *pôles* de G, c'est-à-dire la deuxième projection de Z. Montrer que G agit naturellement sur P.

c) Pour chaque $x \in P$, on note G_x le stabilisateur de x et Gx son orbite. Montrer que G_x est un groupe cyclique. On note n_x son ordre. Montrer que $n_x > 1$, que $n = n_x |Gx|$ et que, pour tout élément y de G_x, on a $n_y = n_x$.

d) Pour chacune des r orbites de l'action de G sur P, on note n_i le cardinal du stabilisateur d'un élément de l'orbite. Montrer que l'on a

$$2(1 - \frac{1}{n}) = \sum_{i=1}^{r} (1 - \frac{1}{n_i})$$

e) Montrer que $r = 2$ ou $r = 3$. Montrer que si $r = 2$, le groupe G est cyclique et $|P| = 2$.

On suppose désormais $r = 3$ et $n_1 \leq n_2 \leq n_3$.

f) Montrer que $n_1 = 2$ et $n_2 = 2$ ou 3. Montrer que si $n_2 = 2$, la deuxième orbite X est l'ensemble des sommets d'un $n/2$-gone régulier (la première orbite aussi). Le groupe G est alors le groupe diédral d'ordre n noté $D_n = G(X)$ dans le cours.

g) Montrer que si $n_2 = 3$, $n_3 = 3$, 4 ou 5. Calculer n dans chaque cas.

Exercice 17 Soit C un groupe cyclique d'ordre $n \geq 1$, et σ un générateur de C.

a) Montrer que pour tout entier $a \in \mathbb{Z}$, l'ordre de σ^a est le dénominateur de la fraction $\frac{a}{n}$, c'est-à-dire $\frac{n}{\text{pgcd}(a,n)}$. Par exemple, si $n = 6$, σ et σ^5 sont d'ordre 6, σ^2 et σ^4 sont d'ordre 3 et σ^3 est d'ordre 2.

b) Montrer que pour chaque diviseur d de n, le groupe C contient exactement $\varphi(d)$ éléments d'ordre d.

Exercice 18 Montrer qu'il y a, à isomorphisme près, quatre anneaux d'ordre 4 : $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{F}_2 \times \mathbb{F}_2$, F_4 et $F_2[X]/(X^2) = \mathbb{F}_2[\varepsilon] = \{a + b\varepsilon;\ a, b \in \mathbb{F}_2, \varepsilon^2 = 0\}$. Pour chaque R dans la liste ci-dessus, déterminer le groupe des unités $R^\times$ et la structure du groupe affine $GA_1(R) \subset \mathfrak{S}(R) \simeq \mathfrak{S}_4$.

Exercice 19 Soit q une puissance d'un nombre premier p et $m \geq 1$ un entier. On note $\mathbb{F}_q$ le corps à q éléments.

a) Pour tout entier $k \leq m$, déterminer le nombre $L(m, k, q)$ de familles libres $(x_1, \ldots, x_k)$ d'éléments de F_q^m.

En déduire successivement

b) $|GL_m(\mathbb{F}_q)|$,

c) $|GA_m(\mathbb{F}_q)|$,

d) $|PGL_m(\mathbb{F}_q)|$,

e) $|SL_m(\mathbb{F}_q)|$,

f) $|PSL_m(\mathbb{F}_q)|$,

g) $EV(k, m, q)$, le nombre de sous-espaces vectoriels de dimension k de $\mathbb{F}_q^m$,

h) $EA(k, m, q)$, le nombre de sous-espaces affines de dimension k de $\mathbb{F}_q^m$.

La *dimension* d d'un espace X est le nombre de paramètres réels nécessaires pour décrire un point générique de cet espace. Plus précisément, tout point de X a un voisinage homéomorphe à (la boule unité ouverte de) $\mathbb{R}^d$. Pour tous entiers $m \geq k \geq 1$, déterminer la dimension de

b') $|GL_m(\mathbb{R})|$,

c') $|GA_m(\mathbb{R})|$,

d') $|PGL_m(\mathbb{R})|$,

e') $|SL_m(\mathbb{R})|$,

f') $|PSL_m(\mathbb{R})|$,

g') $EV(k, m)$, l'espace des sous-espaces vectoriels de dimension k de $\mathbb{R}^m$,

h') $EA(k, m)$, l'espace des sous-espaces affines de dimension k de $\mathbb{R}^m$.

Exercice 20 On munit un $\mathbb{R}$-espace vectoriel $\mathbb{H}$ de base $\{1, i, j, k\}$ d'une multiplication bilinéaire pour laquelle 1 est élément neutre et $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ et $ki = -ik = j$. Il est facile de voir que cette multiplication est associative. Les élément de $\mathbb{H}$ sont appelés *quaternions*. Le *conjuqué* du quaternion $q = a + bi + cj + dk$, avec $a, b, c, d \in \mathbb{R}$ est le quaternion $\overline{q} = a - bi - cj - dk$. On a $\overline{qq'} = \overline{q'}\,\overline{q}$ pour tous quaternions q et q'. Un quaternion q est *réel* si $q = \overline{q}$, c'est-à-dire $b = c = d = 0$, et *pur* si $\overline{q} = -q$, c'est-à-dire $a = 0$. La *norme réduite* $n(q) = q\overline{q} = \overline{q}q = a^2 + b^2 + c^2 + d^2$ est un réel, strictement positif si $q \neq 0$. On en déduit que $\mathbb{H}$ est un corps gauche, l'inverse de q étant

$$q^{-1} = \frac{\overline{q}}{n(q)} = \frac{a}{n(q)} - \frac{b}{n(q)}i - \frac{c}{n(q)}j - \frac{d}{n(q)}k.$$

La norme réduite munit l'espace P des quaternions purs d'une structure d'espace euclidien de dimension 3. Si $x \in P$ est un quaternion pur et $q \in \mathbb{H}^*$ un quaternion non nul, le quaternion qxq^{-1} est pur et a même norme que x. Cette formule définit donc un morphisme $\rho : \mathbb{H}^* \to O(P) \simeq O(3)$.

a) Calculer $\ker \rho$ et Im ρ et en déduire un isomorphisme $\mathbb{H}^*/\mathbb{R}^* \simeq SO(3)$.

b) Expliciter l'image réciproque du groupe $G^+(C) \simeq \mathfrak{S}_4$ des rotations du cube par l'isomorphisme décrit ci-dessus.

c) Soit $p > 2$ un nombre premier. Montrer qu'il existe des éléments α et β de $\mathbb{F}_p$ tels que $\alpha^2 + \beta^2 = -1$.

d) Montrer que les matrices $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $J = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$ et $K = IJ$ de $GL_2(\mathbb{F}_p)$ vérifient $I^2 = J^2 = K^2 = -1$.

e) En déduire que pour tout nombre premier $p \neq 2$, il existe un morphisme injectif $\beta_p : \mathfrak{S}_4 \to PGL_2(\mathbb{F}_p)$ tel que $\beta_p(\mathfrak{A}_4) \subset PSL_2(\mathbb{F}_p)$.

f) Montrer que $\beta_p(\mathfrak{S}_4) \subset PSL_2(\mathbb{F}_p)$ si et seulement si 2 est un carré dans $\mathbb{F}_p$. On peut montrer par ailleurs que ceci équivaut à $p \equiv \pm 1 \pmod 8$.

g) On pose $G_5 = PGL_2(\mathbb{F}_5)$, $G_7 = PSL_2(\mathbb{F}_7)$ et $X_p = G_p/\beta_p(\mathfrak{S}_4)$ pour $p = 5, 7$. En admettant que $PSL_2(\mathbb{F}_q)$ est simple pour $q > 3$, montrer qu'il existe un plongement de G_p dans $\mathfrak{S}_p$, pour $p = 5, 7$.

Exercice 21 Montrer que le cardinal du groupe

$$G = PGL_3(\mathbb{F}_2) = GL_3(\mathbb{F}_2) = SL_3(\mathbb{F}_2) = PSL_3(\mathbb{F}_2)$$

est $|G| = 168$, comme $PSL_2(\mathbb{F}_7)$. Définir un plongement de G dans $\mathfrak{S}_7$.

Exercice 22 Soit X un groupe et Y un sous-groupe distingué de X. On note $p : X \to X/Y$ la projection canonique. À chaque sous-groupe Z de X qui contient Y, on fait correspondre $\overline{Z} = p(Z)$. De même, à chaque sous-groupe T de X/Y, on fait correspondre son image réciproque $p^{-1}(T)$. Montrer que l'on établit ainsi une bijection

$$\{\text{Sous-groupes de } X \text{ contenant } Y\} \leftrightarrow \{\text{Sous-groupes de } X/Y.\}$$