Concours Agrégation, Mathématiques générales, 2014-2015

Leçon 04- Groupes finis. Exemples et applications.

Commentaires du jury 2015 :

On attend des candidats de savoir manipuler correctement les éléments de quelques structures usuelles ($\mathbb{Z}/n\mathbb{Z}, S_n$, etc.). Par exemple, proposer un générateur simple de $(\mathbb{Z}/n\mathbb{Z}, +)$ voire tous les générateurs, calculer aisément un produit de deux permutations, savoir décomposer une permutation en produit de cycles à support disjoint. Il est important que la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Les exemples doivent figurer en bonne place dans cette leçon. On peut par exemple étudier les groupes de symétries A_4 , S_4 , A_5 et relier sur ces exemples géométrie et algèbre, les représentations ayant ici toute leur place. Il est utile de connaître les groupes diédraux, et pour les candidats aguerris, les spécificités de groupes plus exotiques comme le groupe quaternionique. Le théorème de structure des groupes abéliens finis doit être connu.

Commentaires du jury 2016 :

Dans cette leçon il faut savoir manipuler correctement les éléments de différentes structures usuelles (($\mathbb{Z}/n\mathbb{Z}, S_n$, etc.) comme par exemple, en proposer un générateur ou une famille de générateurs, savoir calculer un produit de deux permutations, savoir décomposer une permutation en produit de cycles à supports disjoints. Il est important que la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Le théorème de structure des groupes abéliens finis doit être connu. Les exemples doivent figurer en bonne place dans cette leçon. Les groupes d'automorphismes fournissent des exemples très naturels dans cette leçon. On peut par exemple étudier les groupes de symétries A_4, S_4, A_5 et relier sur ces exemples géométrie et algèbre, les représentations ayant ici toute leur place ; il est utile de connaître les groupes diédraux. S'ils le désirent, les candidats peuvent ensuite mettre en avant les spécificités de groupes comme le groupe quaternionique, les sous-groupes finis de SU_2 ou les groupes $GL_n(\mathbb{F}_q)$.

Remarque : Les représentations linéaires complexes des groupes finis trouvent une place naturelle dans cette leçon.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2']Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. B.C.D.] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
[Fr. E.] Fresnel J. *Groupes* (Hermann 2001)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)
[Fr. MMG96] Fresnel J. *Méthodes modernes en géométrie* (Hermann 1996)
[Fr. MMG10] Fresnel J. *Méthodes modernes en géométrie* (Hermann 2010)
et
[Se.] Serre J.P. *Cours d'arithmétique* (PUF 1970)

Développements conseillés :

(1) Le théorème de structure des groupes abéliens finis, [F. M. 2] p. 121. Si on a le temps on peut inclure l'application suivante : Un sous-groupe fini du groupe multiplicatif d'un corps commutatif est cyclique (voir exercice 1).

(2) Les théorèmes de Sylow, [Fr. E.] p. 34.

(3) Groupes des isométries du cube et du tétraèdre [F. M. 1] $n°133$ et représentations linéaires de A_4, S_4.

(4) Les groupes d'ordre 12 et leurs représentations irréductibles, [F. M. 2] p. 173.

Exercice 1 La formule d'Euler (1) $n = \sum_{d|n} \varphi(d)$.

— Montrer la formule en considérant la partition du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ par l'ordre de ses éléments.

— Notez une variante arithmétique. Soit $n > 1$ et $X := \{\frac{a}{n},\ 1 \leq a \leq n\}$ alors $|X| = n$. La fraction $\frac{a}{n}$ admet d'autre part une écriture unique irréductible $\frac{a'}{d}$ avec $(a', d) = 1$ (si $\delta = (a, n)$ alors $a' = \frac{a}{\delta}$ et $d = \frac{n}{\delta}$). Si on fixe $d|n$, le nombre de fractions dans X de la forme $\frac{a'}{d}$ avec $(a', d) = 1$ est $\varphi(d)$ par définition de la fonction d'Euler. D'où la formule.

Remarque. Ces deux démonstrations sont en fait identiques moyennant l'isomorphisme entre les groupes $(\mathbb{Z}/n\mathbb{Z}, +)$ et $\mu_n(\mathbb{C})$, le groupe des racines n-ièmes de l'unité ; un isomorphisme non élémentaire puisque donné par la fonction exponentielle !

Exercice 2 Soit K, un corps commutatif et G un sous-groupe fini du groupe multiplicatif $K^\times = K - \{0\}$ de K, alors G est cyclique.

Preuve.

— On utilise le théorème de structure des groupes abéliens finis.

Si $|G| > 1$, il existe une suite d'entiers $1 < a_1|a_2|...|a_r$ avec $(G, \times) \simeq (\frac{\mathbb{Z}}{a_1\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{a_r\mathbb{Z}}, +)$. Il s'agit de montrer que $r = 1$. Puisque $a_r G = \{0\}$, il suit que le cardinal de $\{z \in K \mid z^{a_r}\} = 1$ est $\geq |G| = a_1 a_2 ... a_r$ et d'autre part le nombre de racines dans K du polynôme $X^{a_r} - 1 \in K[X]$ est inférieur ou égal à son degré parce que le corps K est commutatif (c'est faux pour le corps des quaternions sur $\mathbb{R}$ par exemple). Ainsi $a_1 a_2 ... a_r \leq a_r$ ce qui implique $r = 1$.

— Une variante utilise le lemme clé qui sert à démontrer le théorème de structure des groupes abéliens finis à savoir que si G est un groupe abélien fini il existe $g \in G$ avec $o(g) = ppcm\{o(x) \mid x \in G\}$, voir [Fr. F.] p. 33.

— Une preuve inspirée de la preuve de [Se] p. 11, pour montrer que le groupe multiplicatif d'un corps fini est cyclique.

L'idée de base est de considérer la partition de G par l'ordre de ses éléments et d'utiliser la formule classique d'Euler (1) $n = \sum_{d|n} \varphi(d)$ vue dans l'exercice 1.

On note $n = |G|$ et $\varphi_G(d)$ le nombre d'éléments de G d'ordre d. On a donc (2) $n = |G| = \sum_{d|n} \varphi_G(d)$. Si $\varphi_G(d) \geq 1$ alors $d|n$ et il existe $g \in G$ qui est d'ordre d, ainsi il y a d éléments dans le groupe cyclique $< g >$ et ce sont donc les d racines du polynôme $X^d - 1 \in K[X]$. Il suit que si $g' \in G$ est un élément d'ordre d alors $g' \in < g >$ et donc $\varphi_G(d) = \varphi(d)$, le nombre d'éléments d'ordre d dans le groupe cyclique $< g >$. Ainsi il suit de (1) et (2) que $0 = \sum_{d|n}(\varphi(d) - \varphi_G(d))$ est une somme de nombres positifs et donc en particulier $\varphi_G(n) = \varphi(n) > 0$. Nous avons montré que G qui est d'ordre n contient un élément d'ordre n ; il est donc cyclique.

Exercice 3 Une application de l'exercice précédent.

Soient K un corps commutatif et $(K^\times)_{tors} = \{x \in K^\times \mid \exists n_x \in \mathbb{N}^\star,\ x^{n_x} = 1\}$, le sous-groupe de torsion de $K^\times$. Soit $S := \{o(x) \mid x \in (K^\times)_{tors}\}$. Soit $m \in S$, montrer qu'il existe un unique sous- groupe G_m de $K^\times$ d'ordre m. Montrer que G_m est cyclique et que $(K^\times)_{tors} = \cup_{m \in S} G_m$.

Exercice 4 Pour aller plus loin. Sous-groupe de torsion du groupe multiplicatif d'un corps commutatif, [F. M. 2] Compléments-Errata, p. 121 "Les sous-groupes de $\frac{\mathbb{Q}}{\mathbb{Z}}$" par. 3

Exercice 5 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: Si G est un tel sous-groupe alors le théorème de Lagrange montre que $d := |G|$ divise n ainsi $a + n\mathbb{Z} \in G$ implique $da = 0 \mod n$ et donc $a \in \frac{n}{d}\mathbb{Z}$ et donc $G \subset \frac{n}{d}\mathbb{Z}/n\mathbb{Z} = \{\frac{n}{d} + n\mathbb{Z}, ..., d\frac{n}{d} + n\mathbb{Z}\}$ et donc $G = \frac{n}{d}\mathbb{Z}/n\mathbb{Z}$. Il suit que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n dans $\mathbb{N}$.

Rappelons que si $H \subset G$ sont 2 groupes avec H distingué dans G alors la surjection canonique $\pi : G \to \frac{G}{H}$, induit une bijection entre l'ensemble des sous groupes de G qui contiennent H et l'ensemble des sous-groupes de $\frac{G}{H}$. Dans le cas où $G = \mathbb{Z}$ on connait les sous-groupes d'où une preuve "classique".

Exercice 6 Soit $n, m \in \mathbb{N}^\star$. On se propose de déterminer les homomorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Pour $k \in \mathbb{N}^\star$, on note π_k la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/k\mathbb{Z}$.

(1) Soit f un homomorphisme de groupe de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Soit $a \in \mathbb{Z}$ avec $f \circ \pi_n(1) = \pi_m(a)$. Montrer que $\frac{m}{(m,n)}$ divise a.

Preuve. Par construction si $x \in \mathbb{Z}$ alors $f_a \circ \pi_n(x) = x f_a \circ \pi_n(1) = x\pi_m(a)$ et pour $x = n$ puisque $\pi_n(x) = 0 \mod n$ on obtient $0 \mod m$. Ainsi $na = dm$ avec $d \in \mathbb{Z}$ ce qui équivaut à $\frac{n}{(m,n)}a = \frac{m}{(m,n)}d$ et qui par le lemme de Gauss implique que $\frac{m}{(m,n)}$ divise a. ///

(2) Réciproquement soit $a \in \frac{m}{(m,n)}$, montrer qu'il existe un unique homomorphisme de groupes $f_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ avec $f_a \circ \pi_n(1) = \pi_m(a)$.

Preuve. Soit $a = d\frac{m}{(m,n)}\mathbb{Z}$ avec $d \in \mathbb{Z}$ et $h_a : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ l'homomorphisme $h_a(x) = ax \mod m$ alors $h_a = f_a \circ \pi_n$. Puisque $h_a(n) = d\frac{nm}{(m,n)} \mod m = 0 \mod m$, on a $\operatorname{Ker}\pi_n \subset \operatorname{Ker} h_a$ et on conclut avec le théorème de factorisation des homomorphismes de groupes. ///

(3) A quelle condition sur m, n y a-t-il un seul homomorphisme de groupe de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?

Preuve. Puisque l'on dispose toujours de l'homomorphisme $h_0(x) = 0 \mod m$ la condition est que $\frac{m}{(m,n)} \in m\mathbb{Z}$ i.e. $(m, n) = 1$. ///

(4) Calculer en fonction de m, n le nombre d'homomorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

Preuve. On cherche donc le nombre de restes modulo m des entiers $a = d\frac{m}{(m,n)}$ avec $d \in \mathbb{Z}$. Si r est le reste de d modulo (m, n) alors le reste de $d\frac{m}{(m,n)}$ modulo m est $r\frac{m}{(m,n)}$, ainsi le nombre de classes modulo m des entiers multiples de $\frac{m}{(m,n)}$ est (m, n). ///

Exercice 7 Soit $(G, +)$ un groupe abélien fini. On se propose de calculer $\Sigma(G) := \sum_{g\in G} g$.

(1) On note $G[2] := \{g \in G, |2g = 0\}$. Montrer que $G[2]$ est un sous-groupe de G et que $\Sigma(G) = \Sigma(G[2])$.
(2) Soit G et G', 2 groupes abéliens. Montrer que $(G \times G')[2] = G[2] \times G'[2]$.
(3) On suppose que $G \simeq \mathbb{Z}/a\mathbb{Z}$. Déterminer $G[2]$ en fonction de la parité de a.
(4) On suppose que $G \simeq (\mathbb{Z}/2\mathbb{Z})^n$ avec $n > 1$. Montrer que $\Sigma(G) = 0$.
(5) Déduire de ce qui précède $\Sigma(G)$ pour un groupe abélien fini.
(6) Examiner le cas $G = (\mathbb{Z}/n\mathbb{Z})^\times$, le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$.

Exercice 8

Soit $(G, +)$ un p-groupe abélien fini.

— Montrer que A engendre G si et seulement si l'image de A dans $\frac{G}{pG}$ engendre $\frac{G}{pG}$.

Preuve. Supposons que l'image de A dans $\frac{G}{pG}$ engendre $\frac{G}{pG}$. Ainsi $G =< A > +pG$ où $< A >$ est le groupe engendré par A. Par récurrence sur k, on déduit que $G =< A > +p^kG$ pour $k \geq 1$. Si $|G| = p^n$, alors $p^nG = \{0\}$; ainsi $G =< A > +p^nG =< A >$.La réciproque est immédiate.///

— En déduire que le nombre minimal de générateurs de G est égal à la dimension du $\mathbb{F}_p$-espace vectoriel $\frac{G}{pG}$.

Remarque. Si G est un groupe abélien fini alors $G \simeq \prod_{1\leq i\leq r} \frac{\mathbb{Z}}{a_i\mathbb{Z}}$ avec $1 < a_1|a_2|...|a_r$ et r est le nombre minimal de générateurs de G, [Fr. E.] p. 100.

Si G est un p-groupe non nécessairement abélien, voir [F. M. 1] $n°76$ p 192 "Sur le groupe de Frattini d'un p-groupe".

Exercice 9 Sous-groupes abéliens finis de $\mathrm{GL}_n(\mathbb{C})$, [F. M. 2] p. 130.

Exercice 10 Groupes d'ordre 8,[Fr. E.] p. 43. Groupes d'ordre 12, [F. M. 2] p. 173.

Exercice 11 Voir [Fr. MMG10] p. 221 et [F. M. 2'] complément à la page 121. On rappelle la présentation du groupe diédral $D_{2n} =< r, s >$ avec ordre de r égal n, ordre de s égal 2 et $srs^{-1} = r^{-1}$. Pour $\theta \in \mathbb{R}$ on note $R(\theta) := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in M_2(\mathbb{R})$ et $S(\theta) := \begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix} \in M_2(\mathbb{R})$

(1) Montrer que $S(\theta) \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ est la symétrie orthogonale par rapport à $\mathbb{R}(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$.

Preuve. On vérifie que $S(\theta)\ {}^tS(\theta) = Id$ et que $S(\theta)^2 = Id$; ainsi $S(\theta)$ est une symétrie orthogonale et puisque $S(\theta)\ {}^t(1,0) = {}^t(\cos\theta, \sin\theta)$ le résultat suit.///

(2) Montrer que le groupe $G_n(\theta)$ engendré par $R(\frac{2\pi}{n})$ et $S(\theta)$ est isomorphe au groupe diédral D_{2n} de cardinal $2n$.

Preuve. On vérifie que $S(\theta)R(\frac{2\pi}{n})S(\theta)\ {}^t(1,0) = {}^t(\cos\frac{2\pi}{n}, -\sin\frac{2\pi}{n})$ et puisque $\det S(\theta)R(\frac{2\pi}{n})S(\theta) = 1$ il suit que $S(\theta)R(\frac{2\pi}{n})S(\theta) = R(-\frac{2\pi}{n})$.///

(3) Soit G un sous-groupe de $SO_2(\mathbb{R})$. Montrer que G est soit dense dans $SO_2(\mathbb{R})$ soit fini et si son cardinal est n alors $G =< R(\frac{2\pi}{n}) >$ (on pourra utiliser le fait qu'un sous groupe de $(\mathbb{R}, +)$ est soit dense soit monogène i.e. de la forme $\mathbb{Z}a$, [Fr. B-C-D] p. 84).

Preuve. L'application $R : \mathbb{R} \to SO_2(\mathbb{R})$ est un homomorphisme de groupes (formules d'addition). Il est surjectif par la paramétrisation polaire du cercle unité. Enfin le noyau est $2\pi\mathbb{Z}$; ainsi R induit un isomorphisme $\tilde{R}$ entre $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ et $SO_2(\mathbb{R})$. De plus $\frac{\mathbb{R}}{2\pi\mathbb{Z}}$ est compact, il suit que $\tilde{R}$ est un homéomorphisme. Il s'agit donc de préciser la nature des sous-groupes G de $\mathbb{R}$ qui contiennent $2\pi\mathbb{Z}$. Si G est discret alors $G = a\mathbb{Z}$ avec $2\pi \in a\mathbb{Z}$; ainsi $2\pi = na$ avec $n \in \mathbb{N}$ et donc $a = \frac{2\pi}{n}$. Il suit que $R(G) =< R(\frac{2\pi}{n}) >$ est fini de cardinal n. Si G n'est pas discret, il est dense dans $\mathbb{R}$ et il en est donc de même de $R(G)$.///

(4) Soit G un sous-groupe de $O_2(\mathbb{R})$ et $G^+ := G \cap SO_2(\mathbb{R})$. On suppose qu'il existe $\sigma \in G - G^+$. Montrer que $G = G^+ \cup \sigma G^+$, en déduire que G est soit dense dans $O_2(\mathbb{R})$ soit fini et si son cardinal est m alors $m = 2n$ et G est isomorphe au groupe diédral D_{2n}.

Preuve. Seule l'inclusion $G^+ \cup \sigma G^+ \subset G$ est à prouver. Si $g \in G - G^+$ alors $\sigma g \in G^+$ et puisque $\sigma^2 = Id$ l'inclusion suit. Notez que la réunion $G^+ \cup \sigma G^+ \subset G$ est de plus disjointe (déterminant).///

(5) Le groupe $G_n(\theta) \subset O_2(R)$ opère sur l'ensemble T des points $m = (x_m, y_m) \in \mathbb{R}^2$ avec $x_m^2 + y_m^2 = 1$ par la formule $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \star (x_m, y_m) = (ax_m + by_m, cx_m + dy_m)$. On note $G_n(\theta)_m$ le groupe d'isotropie de m.

Montrer que $G_n(\theta)_m$ est d'ordre 1 ou 2 ; en déduire une description de l'orbite de M sous $G_n(\theta)$.

Preuve. Puisque $m \neq (0,0)$ il suit que $SO_2(\mathbb{R})_m = \{Id\}$ et donc $G_n(\theta)^+_m = \{Id\}$. Si $\sigma, \tau \in G_n(\theta)_m - G_n(\theta)^+_m$ alors $\sigma\tau^{-1} \in G_n(\theta)^+_m$; ainsi $\sigma = \tau$ et $G_n(\theta)_m = \{Id, \sigma\}$ est d'ordre 2. Si $G_n(\theta)_m = \{Id\}$, alors l'orbite $G_n(\theta) \star m$ est le polygone régulier à n côtés $< R(\frac{2\pi}{n}) > \star m$ et si $G_n(\theta)_m = \{Id, \sigma\}$ c'est la réunion de deux polygones réguliers à n côtés qui sont $< R(\frac{2\pi}{n}) > \star m$ et $< R(\frac{2\pi}{n}) > \sigma \star m$; de plus ils sont distincts puisque l'orbite a $2n$ éléments et c'est un polygone régulier à $2n$ côtés pour les n valeurs de $\theta = k\frac{\pi}{n}$ avec $k = 1, 3, ..., 2n-1$ avec k impair (cf. 2.c) de l'exercice suivant).///

(6) Montrer que l'application qui à $\theta \in [0, \frac{2\pi}{n}[$ associe $G_n(\theta)$ définit une bijection sur les sous-groupes de $O_2(\mathbb{R})$ d'ordre $2n$ qui ne sont pas inclus dans $SO_2(\mathbb{R})$.

Preuve. Il faut montrer que tout groupe $G_n(\varphi)$ avec $\varphi \in \mathbb{R}$ est égal à un unique groupe $G_n(\theta)$ avec $\theta \in [0, \frac{2\pi}{n}[$. Pour cela on remarque que l'ensemble des symétries dans $G_n(\varphi)$ est $G_n(\varphi) - G_n(\varphi)^+ = \{R(k\frac{2\pi}{n})S(\varphi) = S(\varphi + k\frac{2\pi}{n}),\ k = 0, 1, ..., n-1\}$ et puisqu'il n'y a qu'une seule valeur $k_0 := -\lfloor\frac{n\varphi}{2\pi}\rfloor \bmod n$ de k telle que $0 \leq \varphi + k\frac{2\pi}{n} < \frac{2\pi}{n}$, le résultat suit avec $G_n(\varphi) = G_n(\theta)$ et $\theta = \varphi - \lfloor\frac{n\varphi}{2\pi}\rfloor\frac{2\pi}{n}$.///

Exercice 12 Orbites sous l'action d'un sous-groupe de $O_2(\mathbb{R})$ sur l'ensemble T des points $m = (x_m, y_m) \in \mathbb{R}^2$ avec $x_m^2 + y_m^2 = 1$.

Soit G un sous-groupe de $O_2(\mathbb{R})$ et $G^+ := G \cap SO_2(\mathbb{R})$, on rappelle que si il existe $\sigma \in G - G^+$ alors $G = G^+ \cup \sigma G^+$.

Soit $\Sigma \subset T$ une partie non vide de T avec $G \star \Sigma = \Sigma$, alors Σ est réunion disjointe d'orbites $G \star s$ de points $s \in \Sigma$.

Dans ce qui suit Σ est réduit à un point s, G désigne un sous-groupe de $O_2(\mathbb{R})$ et $O(s) := G \star s$, l'orbite de s sous l'action de G. Enfin $\hat{G} := \{g \in O_2(\mathbb{R}) \mid g \star O(s) = O(s)\}$ le stabilisateur dans $O_2(\mathbb{R})$ de $O(s)$.

(1) On suppose que $G \subset SO_2(\mathbb{R})$.

(a) Montrer que $\hat{G}^+ = G$.

Preuve. Soit $r \in \hat{G}^+$, ainsi r est une rotation avec $r \star O(s) = O(s)$; ainsi il existe $g \in G$ avec $r \star s = g \star s$ et puisque $G \subset SO_2(\mathbb{R})$ il suit que la rotation $g^{-1}r$ fixe le point s ; c'est donc l'identité.///

(b) Soit σ_s la symétrie orthogonale avec $\sigma_s(s) = s$. Montrer que $\hat{G} = G^+ \cup \sigma_s G^+$.///

Preuve. On a $\sigma_s \in \hat{G}^+$ et puisque $\hat{G}$ est un sous-groupe de $O(2)(\mathbb{R})$, il suit que $\hat{G} = \hat{G}^+ \cup \sigma_s \hat{G}^+ = G^+ \cup \sigma_s G^+$.///

(2) On suppose qu'il existe $\sigma \in G - G^+$. Soit ρ, l'unique rotation telle que $\rho(s) = \sigma(s)$. On note $O(s)^+ := G^+ \star s$ et $O(s)^- := G^+\sigma \star s$; ainsi $O(s) = O(s)^+ \cup O(s)^-$.

(a) Montrer que $O(s)^+ = O(s)^-$ ou bien que $O(s)^+ \cap O(s)^- = \emptyset$.

Preuve. L'intersection $O(s)^+ \cap O(s)^-$ est non vide si et seulement si il existe $r, r' \in G^+$ avec $r \star s = r'\sigma \star s$ autrement dit si $r'^{-1}r \star s = \rho \star s$ et donc puisque $\rho \in SO_2(\mathbb{R})$, $O(s)^+ \cap O(s)^-$ est non vide si $\rho = r'^{-1}r \in G^+$ (réciproquement si $\rho \in G^+$, $r = \rho$ et $r' =$ conviennent). Dans ce cas on a $O(s)^+ = G^+ \star s = G^+\rho \star s = G^+\sigma \star s = O(s)^-$.///

(b) On suppose que $O(s)^+ = O(s)^-$. Montrer que $\hat{G} = G$. Construire un exemple.

Preuve. On a $O(s) = O(s)^+ \cup O(s)^- = O(s)^+ = O(s)^-$. Si $g \in \hat{G}^+$ il existe $r \in G^+$ avec $g \star s = r \star s$ et donc $g = r \in G$. Enfin si $g \in \hat{G}^+\sigma$, puisque $g \star O(s)^- = O(s)^-$ il existe $r \in G^+$ avec $g \star s = r\sigma \star s$, ainsi $g\sigma \star (\sigma \star s) = r \star (\sigma \star s)$ i.e. les deux rotations $g\sigma$ et r sont égales et donc $g = r\sigma \in G$.

Exemples. Soit $n > 1$ et $G_n :=< r, \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et σ la symétrie orthogonale avec $\sigma(1,0) = (1,0)$. Soit $s := (1,0)$ alors $O(s)^+ = O(s)^-$ (on peut aussi noter que $\rho =$). ///

(c) On suppose que $O(s)^+ \cap O(s)^- = \emptyset$. Montrer que si $\rho^2 \notin G^+$ alors $\hat{G} = G$ et que si $\rho^2 \in G^+$ alors $\hat{G}^+ = G^+ \cup \rho G^+$ et donc $\hat{G} = \hat{G}^+ \cup \hat{G}^+\sigma$. Construire un exemple dans chacune des deux situations.

Preuve. Nous sommes donc dans la situation où $\rho \notin G$ et $O(s)$ est réunion disjointe de $G^+ \star s$ et de $G^+\sigma \star s$. Soit donc $h \in \hat{G}$ i.e. $h \in O_2(\mathbb{R})$ avec $h \star O(s) = O(s)$ ce qui équivaut aux deux conditions $h \star s \in O(s)$ et $h \star (\sigma \star s) \in O(s)$ (discuter en fonction de la nature de h, on n'a pas besoin de l'équivalence) . On distingue 2 cas.

- *On suppose que la rotation $\rho^2 \in G$ (et $\rho \notin G$). Il s'agit de montrer que $h \in G^+ \cup \rho G^+$. Il existe $g, g' \in G$ avec (1) $h \star s = g \star s$ et (2) $h \star (\sigma \star s) = g' \star s$. On discute en fonction de la nature de h.*
  - *Supposons que $h \in SO_2(\mathbb{R})$. Si $g \in SO_2(\mathbb{R})$ la relation (1) montre que $h = g \in G^+$. Si $g \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ la relation (1) devient $h \star s = g\sigma \star (\sigma \star s) = g\sigma\rho \star s$; ainsi (3) $h = (g\sigma)\rho = \rho(g\sigma)$ puisque $SO_2(\mathbb{R})$ est commutatif. Ainsi $h \in \rho G^+$.*
  - *Supposons que $h \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$. Alors $h' := \sigma h \in SO_2(\mathbb{R})$ et puisque les relations (1) et (2) sont équivalentes aux relations analogues pour h' à condition de remplacer g resp. g' par σg resp. $\sigma g'$ le résultat est alors conséquence du cas précédent appliqué à h'.*

Exemples. Soit $n > 1$ et $G = G_n :=< R(2\frac{\pi}{n}), \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et $\sigma = S(\theta)$ la symétrie orthogonale avec $S(\theta) \star (1,0) = (\cos\theta, \sin\theta)$. Soit $s := (1,0)$ alors $\rho = R(\theta)$, ainsi il faut et il suffit de choisir $\theta \notin \{2k\frac{\pi}{n} \mod 2\pi\}$ mais que $2\theta \in \{2k\frac{\pi}{n} \mod 2\pi\}$ avec $k \in \{0, 1, .., n-1\}$ pour que $\rho \notin G_n^+$ et $\rho^2 \in G_n^+$. Cela donne n possibilités qui sont $\theta = k\frac{\pi}{n}$ avec $k = 1, 3, ..., 2n-1$ avec k impair. L'orbite $O(s)$ est l'ensemble des $2n$ sommets d'un polygone régulier dont le groupe des isométries est G_{2n} puisque $\hat{G_n} = G_{2n}$.

— *On suppose que la rotation $\rho^2 \notin G$. Il s'agit de montrer que $h \in G$.*

— *Si $h \in SO_2(\mathbb{R})$ et si $g \in SO_2(\mathbb{R})$ comme précédemment on déduit que $h \in G$ et si $g \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ que (3) $h = \rho(g\sigma)$. On va conclure à l'aide de la relation (2) $h \star (\sigma \star s) = g' \star s$.*

Si $g' \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ on a $\sigma h \sigma \star s = \sigma g' \star s$ avec $\sigma h \sigma$, $\sigma g' \in SO_2(\mathbb{R})$, ainsi $\sigma h \sigma = \sigma g'$ et donc $h = g'\sigma \in G^+$.

Si $g' \in SO_2(\mathbb{R})$ on a $h \star (\sigma \star s) = h\rho \star s = g' \star s$, ainsi avec (3) $g' = h\rho = \rho(g\sigma)\rho = (g\sigma)\rho^2$ et donc $\rho^2 \in G$; contradiction !

— *Supposons que $h \in O_2(\mathbb{R}) - SO_2(\mathbb{R})$ on conclut comme précédemment en considérant σh.*

Exemples. Soit $n > 1$ et $G = G_n :=< R(2\frac{\pi}{n}), \sigma >$, avec r la rotation d'angle $2\frac{\pi}{n}$ et $\sigma = S(\theta)$ la symétrie orthogonale avec $S(\theta) \star (1,0) = (\cos\theta, \sin\theta)$. Soit $s := (1,0)$ alors $\rho = R(\theta)$, ainsi il faut et il suffit de choisir $\theta \notin \{k\frac{\pi}{n} \mod 2\pi\}$ avec $k \in \{0, 1, .., n-1\}$ pour que $\rho^2 \notin G_n^+$ et donc aussi $\rho \notin G_n^+$; autrement dit il faut éviter les exemples construits dans la question précédente. Dans ce cas $O(s)$ est l'ensemble des $2n$ sommets d'un polygone convexe qui n'est pas régulier et dont le groupe des isométries est G_n puisque $\hat{G_n} = G_n$.///

Exercice 13 Sous-groupes finis de $\mathrm{GL}_2(\mathbb{R})$ (voir [Fr. B-C-D] p. 165), $\mathrm{GL}_2(\mathbb{Z})$ et $\mathrm{GL}_2(\mathbb{Q})$ (voir [F. M. 1] $n°26$ question 4) p. 49 et question 1) p. 46).

(1) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{R})$. On va montrer qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ avec $PGP^{-1} \subset O_2(\mathbb{R})$; ainsi si $G \subset \mathrm{SL}_2(\mathbb{R})$, le groupe G est cyclique et sinon G est diédral.

(a) On note q la forme quadratique euclidienne sur $\mathbb{R}^2$ i.e. $q((x,y)) = x^2 + y^2$. Montrer que $q_G((x,y)) = \sum_{g \in G} q((x,y)\ {}^t g))$ est une forme quadratique définie positive sur $\mathbb{R}^2$.

Preuve. La forme $\Phi_G((x,y),(x',y')) := \sum_{g \in G}((x,y)\ {}^t g)|(x,y)\ {}^t g))$ où $(.|.)$ désigne le produit scalaire, est une forme bilinéaire symétrique et $q_G((x,y)) = \Phi_G((x,y),(x,y))$ est la forme quadratique associée. Enfin puisque $q((x,y)\ {}^t g))) \geq 0$ et c'est nul si et seulement si $(x,y) = (0,0)$ il suit que Φ_G est un produit scalaire.///

(b) Montrer que $G \subset O(q_G)$, le groupe orthogonal de q_G.

Preuve. Soit $g \in G$, alors $q_G((x,y)\ {}^t g') = \sum_{g \in G} q((x,y)\ {}^t g'\ {}^t g)) = q_G((x,y))$ puisque $Gg' = G$.///

(c) Montrer que $O(q_G)$ et $O(q)$ sont des sous-groupes conjugués de $\mathrm{GL}_2(\mathbb{R})$.

Preuve. Soit $S \in Sym_2(\mathbb{R})$ avec $q_G((x,y)) = (x,y)S\ {}^t(x,y)$. Soit (e_1, e_2) une BON de $\mathbb{R}^2$ pour q_G ; si P est la matrice de passage telle que $(x,y) = (x',y')\ {}^t P$ avec $x'e_1 + y'e_2 = (x,y)$ alors $q_G((x,y)) = x'^2 + y'^2$; ainsi si $g \in O(q_G)$ alors $q_G((x,y)) = q_G((x,y)\ {}^t g) = q_G((x',y')\ {}^t P\ {}^t g)$ ainsi ${}^t P\ {}^t g S g P = Id$ et puisque ${}^t P S P = Id$ (cas $g = Id$) on a $P^{-1} g P \in O_2(\mathbb{R})$.///

(d) Montrer qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ avec $P^{-1}GP \subset O_2(\mathbb{R})$ en déduire que si $G \subset \mathrm{SL}_2(\mathbb{R})$, le groupe G est cyclique et sinon G est diédral.

Preuve. L'inclusion $P^{-1}GP \subset O_2(\mathbb{R})$ est conséquence de la question qui précède. Ainsi le groupe fini $P^{-1}GP$ est cyclique et sinon G est diédral par l'exercice 1 .///

(e) On suppose que G est un sous-groupe fini de $\mathrm{SL}_2(\mathbb{R})$ de cardinal n. Montrer qu'il existe $P \in \mathrm{SL}_2(\mathbb{R})$ avec $PGP^{-1} =< R(\frac{2\pi}{n}) >$ où $R(\theta) := \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \in M_2(\mathbb{R})$.

Preuve. Puisque $\det PgP^{-1} = 1$ *si* $g \in G$, *ainsi* PGP^{-1} *est égal à l'unique sous-groupe de* $SO_2(\mathbb{R})$ *de cardinal* n *(voir exercice 1).///*

(f) Pour $a \in \mathbb{R}$, on note $B_{1,2}(a) := \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{R})$.

On suppose que $n \neq 2$, montrer que les deux groupes $< B_{1,2}(a)R(\frac{2\pi}{n})B_{1,2}(-a) >$ et $< B_{1,2}(b)R(\frac{2\pi}{n})B_{1,2}(-b) >$ sont égaux si et seulement si $a = b$.

Preuve. Pour simplifier le calcul on écrit $c(k)$ *resp.* $s(k)$ *pour* $\cos k$ *resp.* $\sin k$. *Une CNS est qu'il existe* $k \mid (k, n) = 1$ *avec* $B_{1,2}(a-b)R(\frac{2\pi}{n})B_{1,2}(b-a) = R(\frac{2k\pi}{n})$. *Ce qui donne les 4 conditions* $c(1)+(a-b)s(1) = c(k)$, $s(1) = s(k)$, $(a-b)c(k)-s(k) = -s(1)+(a-b)c(1)$, $c(k)+(a-b)s(k) = c(1)$. *Il suit que* $s(k) = s(1)$ *et* $c(k) = c(1)$ *; ainsi* $k = 1 \mod n$ *et donc* $(a-b)s(1) = 0$. *Si* $n \neq 2$ *alors* $s(1) \neq 0$ *et donc* $a = b.///$

(2) Montrer que $\mathrm{SL}_2(\mathbb{R})$ contient un unique sous-groupe d'ordre 2.

Preuve. Soit $A := \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{R})$, *avec* $A^2 = Id$. *Ainsi le polynôme minimal de* A *divise* $X^2 - 1$ *; il est donc scindé à racines simples. Il suit que* A *est diagonalisable et puisque* $\det A = 1$, *il suit que* A *est l'homothétie* $\pm Id.///$

(3) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$ non inclus dans $\mathrm{SL}_2(\mathbb{Z})$. Ainsi par ce qui précède on sait que $G \simeq D_{2n}$.

(a) En considérant la trace des éléments de G, montrer que $n \in \{1, 2, 3, 4, 6\}$.

Preuve. On a montré précédement qu'il existe $P \in \mathrm{GL}_2(\mathbb{R})$ *avec* $G^+ = P < R(\frac{2\pi}{n}) > P^{-1} \subset \mathrm{SL}_2(\mathbb{Z})$ *; ainsi* $\mathrm{Tr}\, R(\frac{2\pi}{n}) = 2\cos\frac{2\pi}{n} \in \mathbb{Z}$ *et donc* $2\cos\frac{2\pi}{n} \in \{-2, -1, 0, 1, 2\}.///$

(b) Réciproquement montrer que pour $n \in \{1, 2, 3, 4, 6\}$, $\mathrm{GL}_2(\mathbb{Z})$ contient un sous-groupe isomorphe à D_{2n} (on pourra considérer la matrice compagnon du polynôme caractéristique de la rotation $R(2\frac{\pi}{n})$).

Preuve. Si $n \in \{1, 2, 3, 4, 6\}$, *comme vu précédement* $\mathrm{Tr}\, R(\frac{2\pi}{n}) \in \mathbb{Z}$ *et puisque* $\det R(\frac{2\pi}{n}) = 1$, *il suit que le polynôme caractéristique de* $R(\frac{2\pi}{n})$ *est dans* $\mathbb{Z}[X]$ *et par conséquent la matrice compagnon* $CompR(2\frac{\pi}{n})$ *du polynôme caractéristique de la rotation* $R(2\frac{\pi}{n})$ *est dans* $\mathrm{SL}_2(\mathbb{Z})$ *; c'est la matrice de la rotation dans la base* $(1,0), (1,0)\ {}^tR(2\frac{\pi}{n})$ *(l'espace est monogène !) si* $n \notin \{1, 2\}$ *auquel cas* $s(1) \neq 0$.

Supposons que $n \notin \{1, 2\}$. *La matrice de passage est* $P = \begin{bmatrix} 1 & c(1) \\ 0 & s(1) \end{bmatrix}$ *et* $P^{-1} = \begin{bmatrix} 1 & -\frac{c(1)}{s(1)} \\ 0 & -\frac{1}{s(1)} \end{bmatrix}$. *On vérifie que* $P^{-1}R(\frac{2\pi}{n})P = \begin{bmatrix} 0 & -1 \\ 1 & 2c(1) \end{bmatrix} = CompR(2\frac{\pi}{n})$.

On calcule $P^{-1}\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}P = \begin{bmatrix} 1 & 2c(1) \\ 0 & -1 \end{bmatrix} =: S \in \mathrm{GL}_2(\mathbb{Z})$. *Ainsi* $G =< CompR(2\frac{\pi}{n}), S >$ *convient.*

Supposons que $n \in \{1, 2\}$. *Dans ces cas* $R(\frac{2\pi}{n}) \in \mathrm{SL}_2(\mathbb{Z})$ *et alors* $G =< R(\frac{2\pi}{n}), \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} >$ *convient.///*

(4) Soit G un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Q})$. On note $M := \sum_{g\in G} \mathbb{Z}(1,0)g + \sum_{g\in G} \mathbb{Z}(0,1)g \in \mathbb{Q}^2$ et $p_1 : \mathbb{Q}^2 \to \mathbb{Q}$ la première projection i.e. $p_1((x, y)) = x$.

(a) Montrer qu'il existe $d \in \mathbb{N} - \{0\}$ avec $d\mathbb{Z}^2 \subset dM \subset \mathbb{Z}^2$.

Preuve. Puisque $G \subset \mathrm{GL}_2(\mathbb{Q})$ *est fini ; il existe* $d \in \mathbb{N}-\{0\}$ *un dénominateur commun aux coefficients des matrices dans* G *; ainsi* $dG \subset M_2(\mathbb{Z})$ *et donc le sous groupe* dM *de* $\mathbb{Q}^2$ *engendré par* dG *est dans* $\mathbb{Z}^2$. *Enfin par construction* M *contient* $\mathbb{Z}^2$ *donc* $d\mathbb{Z}^2 \subset dM.///$

(b) Montrer que $p_1(dM) = a\mathbb{Z}$ avec $a \in \{\mathbb{Z} - \{0\}$.

Preuve. Il suit de la question précédente que la projection $p_1(dM)$ *est un sous-groupe de* $p_1(\mathbb{Z}^2) = \mathbb{Z}$ *et donc* $p_1(dM) = a\mathbb{Z}$ *avec* $a \in \mathbb{Z}$. *Puisque* $d\mathbb{Z}^2 \subset dM$, *il suit que* $d\mathbb{Z} \subset a\mathbb{Z}$ *; ainsi* $a \neq 0.///$

(c) Montrer que $dM \cap \mathbb{Z}(0,1) = \mathbb{Z}(0,b)$ avec $b \neq 0$.

Preuve. Puisque $d\mathbb{Z}^2 \subset dM$, il suit que $d\mathbb{Z}(0,1) \subset dM \cap \mathbb{Z}(0,1)$; ainsi $dM \cap \mathbb{Z}(0,1)$ est un sous-groupe non réduit à 0 du groupe monogène $\mathbb{Z}(0,1)$.///

(d) Montrer que $M = \mathbb{Z}m_1 \bigoplus \mathbb{Z}m_2$.

Preuve. Soit $m \in M$.Par ce qui précède $dm = (x,y)$ avec $x = p_1(dm) \in a\mathbb{Z}$ ainsi $x = \lambda a$ avec $\lambda \in \mathbb{Z}$. Puisque $p_1(dM) = a\mathbb{Z}$, il existe $m_1 \in M$ avec $p_1(dm_1) = a$; ainsi $p_1(dm - \lambda m_1) = 0$ et donc $dm - \lambda m_1 \in dM \cap \mathbb{Z}(0,1) = \mathbb{Z}(0,b)$. Soit $m_2 \in M$ avec $dm_2 = (0,b)$, alors $m \in \mathbb{Z}m_1 + \mathbb{Z}m_2$. Puisque $p_1(m_2) = 0$, il suit que la somme est directe.///

(e) Soit $H := \{h \in \mathrm{GL}_2(\mathbb{Q}) \mid M\ {}^t h = M$, montrer que $H = P\,\mathrm{GL}_2(\mathbb{Z})P^{-1}$, avec $P \in \mathrm{GL}_2(\mathbb{Q})$.

Preuve. Soit $B := ((1,0),(0,1))$ et $B' := (m_1, m_2)$; ce sont des bases de $\mathbb{Q}^2$. Si $h \in H$ alors $m_1\ {}^t h \in \mathbb{Z}m_1 \bigoplus \mathbb{Z}m_2$; ainsi la matrice $[h]_{B'}$ de h dans la base B' est dans $M_2(\mathbb{Z})$; en considérant h^{-1} il suit que son inverse est aussi dans $M_2(\mathbb{Z})$ et donc $[h]_{B'} \in \mathrm{GL}_2(\mathbb{Z})$. Réciproquement si $h \in \mathrm{GL}_2(\mathbb{Q})$ avec $[h]_{B'} \in \mathrm{GL}_2(\mathbb{Z})$ on a $M\ {}^t h = M$ et donc $h \in H$. Soit P la matrice de l'identité de la base B' dans la base B alors P convient.///

(f) En déduire la liste des sous-groupes finis à isomorphisme près de $\mathrm{GL}_2(\mathbb{Q})$.

Preuve. Soit G un sous-groupes fini de $\mathrm{GL}_2(\mathbb{Q})$. On a construit précédemment un sous groupe M de $\mathbb{Q}^2$. Par construction $G \subset H$; ainsi $P^{-1}HP$ est un sous-groupe fini de $\mathrm{GL}_2(\mathbb{Z})$ et donc les sous-groupes finis à isomorphisme près de $\mathrm{GL}_2(\mathbb{Q})$ sont les sous-groupes finis de $\mathrm{GL}_2(\mathbb{Z})$ donc les sous-groupes de D_{2n} avec $n \in \{1,2,3,4,6\}$.///

Exercice 14 Groupes des isométries du cube et du tétraèdre [F. M. 1] n° 133 et application au coloriage du cube [F. M. 1] n° 60

Exercice 15 Le défaut de commutativité d'un groupe non abélien [F. M. 1] n°61 p 151.

Exercice 16 p-sous-groupes de Sylow de S_n, [F. M. 1] n°69 p. 165.

Le cas $n = p$ ou p^2 (exercice corrigé).

Soit $n \in \mathbb{N}^\star$ et p un nombre premier. On note S_n le groupe symétrique sur $\{1,2,....,n\}$.

(1) Les p sous-groupes de Sylow de S_p

(a) Si $a \in \mathbb{N}$, on note $r(a)$ l'entier de $\{1,2,...,p\}$ avec $p|(a - r(a))$. Soit $1 \leq k \leq p-1$, montrer que $(1,2,...,p)^k$ est égal au cycle $(r(1), r(1+k), r(1+2k), ..., r(1+(p-1)k))$ de longueur p.

Preuve. Soit $0 \leq i \leq j \leq p-1$, alors $1 + ik = 1 + jk \mod p$ si et seulement $p|(j-i)k$ i.e. $i = j$. Il suit que $|\{r(1), r(1+k), r(1+2k), ..., r(1+(p-1)k)\} = p$.Puisque $(1,2,...,p)^k(j) = r(j+k)$ pour $1 \leq j \leq p$ il suit que les deux permutations coïncident.///

(b) Montrer que les p sous-groupes de Sylow de S_p sont cycliques d'ordre p et que leurs éléments sont soit l'identité, soit des cycles de longueur p.

Preuve. Par le théorème de Sylow les p sous-groupes de Sylow sont conjugués. La question précédente montre que le groupe $< (1,2,...,p) >$ est cyclique d'ordre p et que ses éléments sont soit l'identité, soit des cycles de longueur p. Ces propriétés étant stables par conjugaison le résultat suit.///

(c) Soit n_p le nombre de p sous-groupes de Sylow de S_p . Vérifier que n_p divise $(p-1)!$ et que $n_p = 1 \mod p$.

Preuve. Le nombre de p cycles est égal au nombre de p-uplets d'éléments distincts de $\{1,2,...,p\}$ en identifiant les p écritures d'un p cycle. Il y en a donc $\frac{p!}{p} = (p-1)!$ (on peut aussi bien compter les orbites de 1). Ainsi $n_p = \frac{(p-1)!}{p-1} = (p-2)!$. Le théorème de Wilson dit que $(p-1)! = -1 \mod p$; ainsi $n_p = 1 \mod p$.///

(2) Les p sous-groupes de Sylow de S_{p^2}

(a) Soit $0 \leq i \leq p-1$ et σ_i le cycle $(1+ip, 2+ip, ..., p+ip) \in S_{p^2}$. Soit $H :=< \sigma_0, ..., \sigma_{p-1} > \subset S_{p^2}$. Montrer que H est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^p$.

Preuve. Les cycles σ_i sont à supports disjoints, ainsi l'application $\varphi : \mathbb{Z}^p \to S_{p^2}$ avec $\varphi(a_0, a_1, ..., a_{p-1}) = \sigma_0^{a_0}...\sigma_{p-1}^{a_{p-1}}$ est un homomorphisme de groupes dont le noyau est $(p\mathbb{Z})^p$. D'autre part soit $\pi : \mathbb{Z}^p \to (\mathbb{Z}/p\mathbb{Z})^p$ l'homomorphisme obtenu par réduction modulo p sur chaque composante ; son noyau est aussi $(p\mathbb{Z})^p$. On conclut avec le théorème de factorisation des homomorphismes de groupes.///

(b) Soit τ défini par $\tau(x) = x + p \mod p^2$ pour $x \in \{1, 2, ..., p^2\}$. Montrer que $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$ pour $0 \leq i \leq p-2$ et $\tau\sigma_{p-1}\tau^{-1} = \sigma_0$.

Preuve. On a $\tau\sigma_i\tau^{-1} = (\tau(1+ip), \tau(2+ip), ..., \tau(p+ip))$ et puisque $\tau(1+ip) = 1+(i+1)p \mod p^2$, il suit que $\tau\sigma_i\tau^{-1} = \sigma_{i+1}$ pour $0 \leq i \leq p-2$ et $= \sigma_0$ pour $i = p-1$.///

(c) Soit $K =< \tau >$. Montrer que $H \cap K = Id$.

Preuve. Le groupe $H \cap K$ est un sous-groupe de $< \tau >$, ainsi il existe $0 \leq a \leq p-1$ avec $H \cap K =< \tau^a >$. Il suit de b) que $\tau^a\sigma_i\tau^{-a} = \sigma_{t_i}$ avec $t_i = a + i \mod p$ et puisque H est abélien on a $t_i = i$, d'où $a = 0$.///

(d) Soit $Syl_p := HK := \{hk \mid h \in H,\ k \in K$. Montrer que Syl_p est un sous-groupe de Sylow de S_{p^2}.

Preuve. Le groupe H est stable par conjugaison par σ_i par τ (question b), ainsi $hkh'k' = h(kh'k^{-1})kk' \in HK$ pour $h, h' \in H$ et $k, k' \in K$ et $(hk)^{-1} = k^{-1}h^{-1} = (k^{-1}h^{-1}k)k^{-1} \in HK$. Enfin il suit de c) que $|HK| = |H||K| = p^2$.///

(e) Montrer que les p sous-groupes de Sylow de S_{p^2} sont isomorphes au produit semi-direct $(\mathbb{Z}/p\mathbb{Z})^p \times_\tau \mathbb{Z}/p\mathbb{Z}$ où $\mathbb{Z}/p\mathbb{Z}$ agit via τ sur $(\mathbb{Z}/p\mathbb{Z})^p$ par permutation circulaire des p composantes.

Preuve. On calcule $\tau\sigma_0^{a_0}...\sigma_{p-1}^{a_{p-1}}\tau^{-1} = \sigma_1^{a_0}...\sigma_{p-1}^{a_{p-2}}\sigma_0^{a_{p-1}} = \sigma_0^{a_{p-1}}\sigma_1^{a_0}...\sigma_{p-1}^{a_{p-2}}$. Ainsi avec a) τ agit sur $(a_0, a_1, ..., a_{p-1})$ par $\tau \star (a_0, a_1, ..., a_{p-1}) = (a_1, a_2, ..., a_{p-1}, a_0)$.///

(f) Eléments d'ordre p^2 dans le groupe Syl_p.

Montrer que $\rho := (\prod_{1 \leq i \leq p-1} \sigma_i)\tau$ est d'ordre p^2.

Preuve. Soit $\pi := \prod_{0 \leq i \leq p-1} \sigma_i$, facilement $\tau\pi\tau^{-1} = \pi$; ainsi $\tau\rho\tau^{-1} = (\sigma_0\sigma_1^{-1})\rho$. On déduit que pour $1 \leq a \leq p$, on a $(*)$ $\rho^a = (\prod_{0 \leq k \leq a-1} \sigma_k^{-1})\pi^a\tau^a$. Ainsi $\rho^p = \pi^{-1}$ et ρ est d'ordre p^2.

Remarque. La formule $(*)$ vaut pour $a \geq 1$ avec la convention que $\sigma_k = \sigma_{r(k)}$ où $r(k)$ est le reste de la division de k par p. Ainsi $\tau\rho\tau^{-1} = \rho^a$ si et seulement si $\rho^{a-1} = \sigma_0\sigma_1^{-1}$ ce qui implique $a = p+1$ et donc que $p = 2$. Il suit que si $< \rho >$ est distingué dans Syl_p, alors $p = 2$. ///

(g) Examiner le cas $p = 2$.

Preuve. On s'interesse donc au 2-Sylow de S_4. Il est notoire qu'ils sont isomorphes au groupe diédral D_8 à 8 éléments (le groupe des isométries du carré est le produit semi-direct du groupe d'ordre 4 des rotations $< r >$, par le groupe engendré par une réflexion s ; d'où la présentation $D_8 =< r, s > \mid r^4 = s^2 = 1, srs^{-1} = r^{-1}$). Alors que dans l'exercice on a la présentation $< s_1 = (1,2), s_2 = (3,4), \tau = (1,3)(2,4) > \mid \tau s_1\tau^{-1} = s_2$. En revenant au groupe des isométries du carré on peut voir s_1, s_2 comme les 2 symétries par rapport aux médiatrices des côtés et τ comme une symétrie par rapport à une des diagonales. ///

Exercice 17 Sur les p-groupes : [F. M. 1] $n°77$ p. 193.