Fiche 5

Exercice 8

Pour commencer, deux rappels:

1. Le groupe diédral D_{2n} est engendré par deux éléments, r (la rotation plane d'angle $\frac{2\pi}{n}$) et s (une réflexion plane) d'ordres respectifs n et 2 et satisfaisant à la relation $rs = sr^{-1}$.
Si $\langle r\rangle \leq D_{2n}$ désigne le sous-groupe cyclique engendré par r, alors

$$D_{2n} = \langle r\rangle \bigcup s\langle r\rangle \text{ (réunion de } \langle r\rangle - \text{ classes à gauche).}$$

2. Tout sous-groupe d'un groupe cyclique G est cyclique. Pour tout diviseur d de l'ordre $|G|$, G admet un unique sous-groupe (cyclique) d'ordre d.

Venons-en à l'exercice.
Si le nombre premier $p \geq 3$ divise $|D_{2n}| = 2n$, alors p divise n. Ecrivons $n = p^l\, m$ avec m non multiple de p.
Le sous-groupe $\langle r\rangle$ étant d'ordre n, il admet un $p-$ Sylow P d'ordre p^l. Par le rappel, P est cyclique et c'est l'unique $p-$ Sylow de $\langle r\rangle$.
Comme ord $(r^m) = \frac{n}{\text{pgcd}(m,n)} = \frac{n}{m} = p^l$, ce $p-$ Sylow s'écrit $P = \langle r^m\rangle$.

Puisque $|D_{2n}| = p^l 2m$ et p ne divise pas $2m$, les $p-$ Sylow de D_{2n} sont les sous-groupes d'ordre p^l, en particulier $P \leq D_{2n}$ est un $p-$ Sylow et tout $p-$ Sylow $P' \leq D_{2n}$ est conjugué à P, i.e. il existe $g \in D_{2n}$ tel que $P' = gPg^{-1} = \langle gr^m g^{-1}\rangle = \langle (grg^{-1})^m\rangle$.

Si $g \in \langle r\rangle$, i.e. si $g = r^j$, alors $grg^{-1} = r$ et $P' = P$; si $g \in s\langle r\rangle$, i.e. si $g = sr^j$, alors $grg^{-1} = sr^j rr^{-j}s = srs = r^{-1}$ et $P' = \langle r^{-m}\rangle = \langle r^m\rangle = P$.

Conclusion: $P = \langle r^m\rangle$ est l'unique $p-$ Sylow de D_{2n}.

Exercice 10

Quelques rappels: on note $F_p = \mathbf{Z}/p\mathbf{Z}$ le corps à p éléments et $Gl_n(F_p)$ le groupe des matrices inversibles de taille n à coefficients dans F_p.
On sait que $|Gl_n(F_p)| = (p^n-1)(p^n-p)\cdots(p^n-p^{n-1})$ (c'est le nombre de base de l'espace vectoriel $(F_p)^n$).
Le déterminant $Det : Gl_n(F_p) \to F_p^\times$ est un morphisme surjectif de groupes de noyau

$$Sl_n(F_p) = \{M \in Gl_n(F_p),\, Det(M) = \overline{1}\}.$$

Par le théorème d'isomorphisme $Gl_n(F_p)/Sl_n(F_p) \simeq F_p^\times$ et

$$|Sl_n(F_p)| = \frac{|Gl_n(F_p)|}{|F_p^\times|} = \frac{(p^n-1)\cdots(p^n-p^{n-1})}{(p-1)}.$$

L'exercice maintenant.

(a) Le F_p- espace $(F_p)^n$ est de cardinal p^n. Il contient p^n-1 points $\neq (\overline{0},\dots,\overline{0})$ et toute droite vectorielle $\Delta = F_p v,\ v \in F_p^n$, en contient $p-1$. Le nombre de droites est donc

$$\frac{p^n-1}{p-1} = 1 + p + \cdots + p^{n-1}.$$

(b) La matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est dans le centre de $Sl_2(F_3)$ ssi elle commute avec toute $B \in Sl_2(F_3)$. L'algorithme de Gauss montre que les matrices de transvections

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ y & 1 \end{pmatrix} \quad x, y \in F_3$$

engendrent le groupe $Sl_2(F_3)$. Il suffit donc de faire commuter A avec ces matrices:

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donne $c = 0$ et $a = d$ et ensuite $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ donne $b = 0$.

A est donc nécessairement une homothétie $A = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ avec $Det(A) = a^2 = 1$. Comme toute homothétie est centrale,

$$Z(Sl_2(F_3)) = \{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\}.$$

(c) Si K est un corps commutatif, on note $P(K^n)$ l'ensemble dont les éléments sont les droites vectorielles de K^n. ($P(K^n)$ est appelé l'espace projectif.)

$Sl_n(K)$ agit naturellement sur $P(K^n)$: si $A \in Sl_n(K)$ et $\Delta = K\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in P(K^n)$, alors

$$A \cdot \Delta = K\,(A\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}).$$

Venons-en à la question: ici $p = 3, n = 2$, $|P(F_3^2)| = 1 + 3 = 4$, $|Sl_2(F_3)| = \frac{(3^2-1)(3^2-3)}{(3-1)} = 24$ et le morphisme d'action λ s'écrit

$$\lambda : Sl_2(F_3) \to S_{P(F_3^2)} \simeq S_4 : A \mapsto \lambda(A) = A \cdot\ .$$

Son noyau $Ker\lambda$ est l'ensemble des matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ qui fixent toutes les droites: si $\Delta_1 = K\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\Delta_2 = K\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ et $\Delta_3 = K\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, alors $A \cdot \Delta_1 = \Delta_1$ ssi $c = 0$, $A \cdot \Delta_2 = \Delta_2$ ssi $b = 0$ et $A \cdot \Delta_3 = \Delta_3$ entraine $a = d$. Il reste les deux homothéties du centre qui conservent bien toutes les droites, i.e.

$$Ker\lambda = Z(Sl_2(F_3)).$$

Par le théorème d'isomorphisme le groupe quotient $Sl_2(F_3)/Ker\lambda$ d'ordre $\frac{24}{2} = 12$ est isomorphe au sous-groupe $Im\,\lambda \leq S_4$.

Pour voir que $Im\lambda = A_4$, il suffit de montrer que le seul sous-groupe d'ordre 12 (i.e. d'indice 2) de S_4 est le groupe alterné A_4:
on sait déjà que tout sous-groupe $K \leq S_4$ d'indice 2 est distingué et c'est le noyau du morphisme

$$S_4 \xrightarrow{\pi} S_4/K : \sigma \mapsto \sigma K.$$

Etant d'ordre 2, le groupe quotient S_4/K est isomorphe au groupe $(\{1, -1\}, \times)$. Si

$$\varphi : S_4/K \to \{1, -1\}$$

désigne cet isomorphisme, $\varphi \circ \pi$ est un morphisme *non trivial* de S_4 sur $\{1, -1\}$, il est donc égal au morphisme de signature: $\varphi \circ \pi = \epsilon$. Donc $K = Ker(\varphi \circ \pi) = Ker\,\epsilon = A_4$.

Un commentaire sur les sous-groupes distingués de S_4: pour faire la liste des sous-groupes distingués de S_4 on peut se servir du fait que tout sous-groupe distingué $K \leq S_4$ est réunion de classes de conjugaison (pour tout $\sigma \in S_4$ et tout $\tau \in K$, $\sigma\tau\sigma^{-1} \in K$) et de propriétés d'engendrement.

On sait que la classe de $\tau \in S_4$ correspond à son type:

- id est de type 1111 et $cl(id) = \{id\}$
- (12) est de type 211 et $cl((12))$ = les 6 transpositions.
- (12)(34) est de type 22 et $cl((12)(34))$ = les 3 double-transpositions
- (123) est de type 31 et $cl((123))$ = les 8 cycles de longueur 3
- (1234) est de type 4 et $cl((1234))$ = les 6 cycles de longueur 4.

Si le sous-groupe distingué K contient une transposition, il contient les 6 transpositions. Comme celles-ci engendrent S_4, $K = S_4$.

Si K contient un cycle de longueur 3, il les contient tous auquel cas $K = A_4$ (les $3-$ cycles engendrent A_4) ou $K = S_4$ (si $|K| > 12$).

Si K contient un cycle de longueur 4, il les contient tous. Il contient aussi $(1234)(1324) = (142)$, donc tous les $3-$ cycles, d'où $A_4 \leq K$. Comme (1234) est de signature -1, K est d'ordre > 12, i.e. $K = S_4$.

Si K contient une double transposition, il contient le sous-groupe distingué

$$V_4 = \{id, (12)(34), (13)(24), (14)(23)\}$$

(isomorphe au groupe de Klein $\mathcal{C}_2 \times \mathcal{C}_2$). S'il est d'ordre 4, $K = V_4$. Sinon il contient au moins 10 éléments donc au moins 12 (car 10 ne divise pas 24) et c'est soit A_4 soit S_4.

Exercice 15 (14 dans la version 1 de la fiche)

Un rappel sur les produits semi-directs: soit G un groupe, $H \leq G$ un sous-groupe distingué et $K \leq G$ un sous-groupe.

On dit que G est produit semi-direct (interne) de H par K si $G = HK$ et $H \cap K = \{e\}$.

On peut dire cela autrement: G est produit semi-direct de H par K si l'application

$$\psi : H \times K \to G : (h, k) \mapsto hk$$

est une bijection.

Dans ce cas, la loi

$$(h,k)\cdot(h',k') = \psi^{-1}(\psi(h,k)\psi(h',k'))$$

est une loi de groupe sur $H \times K$ qui s'écrit

$$(h,k)\cdot(h',k') = \psi^{-1}(hkh'k') = \psi^{-1}(hkh'k^{-1}\,kk') = (hkh'k^{-1}, kk') = (h\varphi_k(h'), kk').$$

On sait que pour $k \in K$ fixé, la conjugaison $\varphi_k : G \to G : x \mapsto kxk^{-1}$ est un automorphisme de G conservant H (car il est distingué) et l'application

$$\varphi : K \to Aut(H) : k \mapsto \varphi_k$$

est un morphisme de groupes.

L'exercice maintenant: on suppose G d'ordre $30 = 2\cdot 3\cdot 5$. G contient donc des Sylow d'ordre 2, 3 et 5.

(a) $n_3 \equiv 1[3]$ et $n_3 \mid 10$. Par la deuxième condition $n_3 \in \{1,2,5,10\}$ et par la première $n_3 = 1$ ou $n_3 = 10$.

$n_5 \equiv 1[5]$ et $n_5 \mid 6$, ce qui donne $n_5 \in \{1,2,3,6\}$ et ensuite $n_5 = 1$ ou $n_5 = 6$.

On procède par l'absurde en montrant que si $n_3 = 10$ et $n_5 = 6$, le décompte des éléments d'ordre 3 et 5 conduit à une contradiction.

Pour ce décompte on se sert de trois observations:

i) si S et S' sont deux sous-groupes tels que pgcd $(|S|,|S'|) = 1$ alors $S \cap S' = \{e\}$: $S \cap S'$ étant un sous-groupe de S et de S', par Lagrange $|S \cap S'|$ divise $|S|$ et $|S'|$ donc aussi leur pgcd égal à 1.

ii) Si S et S' sont des sous-groupes distincts d'ordre premier p, alors $S \cap S' = \{e\}$: par Lagrange, $S \cap S'$ est d'ordre 1 ou p. S'il est d'ordre p, on a $S \cap S' = S = S'$.

iii) Tout groupe d'ordre premier p a $p-1$ éléments d'ordre p: à nouveau par Lagrange, tout élément $x \neq e$ est d'ordre p.

Dès lors, si $n_3 = 10$ et $n_5 = 6$, G a $10\cdot 2 = 20$ éléments d'ordre 3 et $6\cdot 4 = 24$ éléments d'ordre 5: total $20 + 24 = 44 > 30$.

(b) Supposons $n_5 = 1$ (le cas $n_3 = 1$ est analogue), soit Q l'unique $5-$ Sylow et P un $3-$ Sylow.

On a $Q \simeq \mathcal{C}_5$ et $P \simeq \mathcal{C}_3$.

Q étant distingué dans G, QP est un sous-groupe de G. Comme $Q \cap P = \{e\}$, le groupe QP est produit semi-direct de Q par P.

Par l'exercice 2 (e) avec ici $q = 5$ et $p = 3$ (et p ne divise pas $q-1 = 4$), QP est isomorphe au produit direct de Q par P:

$$QP \simeq Q \times P \simeq \mathcal{C}_5 \times \mathcal{C}_3 \simeq \mathcal{C}_{15}$$

(le dernier isomorphisme $\simeq$ par restes chinois).
Enfin $QP \leq G$ est distingué car il est d'indice $\frac{30}{15} = 2$.

Pour la suite on note $H = QP$.

(c) Tout $2-$ Sylow K est d'ordre 2. En raisonnant comme au (b) pour le sous-groupe HK et en observant que $|HK| = |H \times K| = |G|$, on conclut que G est produit semi-direct de $H = QP$ par K.

(d) Pour rappel, l'application

$$Aut(\mathbf{Z}/n\mathbf{Z}) \to (\mathbf{Z}/n\mathbf{Z})^\times : \varphi \mapsto \varphi(\overline{1})$$

est un isomorphisme du groupe des automorphismes du groupe $(\mathbf{Z}/n\mathbf{Z}, +)$ sur le groupe $((\mathbf{Z}/n\mathbf{Z})^\times, \cdot)$ des inversibles de l'anneau $\mathbf{Z}/n\mathbf{Z}$.
L'unique automorphisme φ tel que $\varphi(\overline{1}) = \overline{a}$ s'écrit

$$\varphi : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n\mathbf{Z} : \overline{x} \mapsto \overline{ax}.$$

On a $\mathcal{C}_{15} \simeq (\mathbf{Z}/15\mathbf{Z}, +)$ donc $Aut(\mathcal{C}_{15}) \simeq ((\mathbf{Z}/15\mathbf{Z})^\times, \cdot)$.
$(\mathbf{Z}/15\mathbf{Z})^\times = \{\overline{a},\ \text{pgcd}\ (a, 15) = 1\}$ est d'ordre $\varphi_E(15) = \varphi_E(3)\varphi_E(5) = 2 \cdot 4 = 8$ et

$$(\mathbf{Z}/15\mathbf{Z})^\times = \{\overline{1}, \overline{2}, \overline{4}, \overline{7}, \overline{8}, \overline{11}, \overline{13}, \overline{14}\}.$$

C'est donc un groupe *abélien* d'ordre 8 (de neutre $\overline{1}$).

Pour l'identifier, on détermine l'ordre (multiplicatif) de ses éléments:

$\overline{2}^2 = \overline{4}, \overline{2}^3 = \overline{8}, \overline{2}^4 = \overline{1}$, i.e. $\overline{2}$ est d'ordre 4; par des calculs analogues, on constate que $\overline{2}, \overline{7}, \overline{8}, \overline{13}$ sont d'ordre 4 et $\overline{4}, \overline{11}, \overline{14}$ sont d'ordre 2.

Le choix d'un sous-groupe cyclique d'ordre 4, par exemple $\langle\overline{2}\rangle = \{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$ et d'un élément d'ordre 2 dans le complémentaire de $\langle\overline{2}\rangle$, par exemple $\overline{11}$, donne l'application

$$\langle\overline{2}\rangle \times \langle\overline{11}\rangle \to (\mathbf{Z}/15\mathbf{Z})^\times : (\overline{2}^j, \overline{11}^k) \mapsto \overline{2}^j\overline{11}^k$$

qui est un isomorphisme de groupes, i.e. $(\mathbf{Z}/15\mathbf{Z})^\times \simeq \mathcal{C}_4 \times \mathcal{C}_2$.

(e), (f)

Pour limiter les écritures, je traite (e) et (f) en même temps.

Par le (c), G est produit semi-direct de $H \simeq \mathcal{C}_{15}$ par $K \simeq \mathcal{C}_2$ et un tel produit semi-direct provient d'un morphisme

$$\phi : \mathcal{C}_2 \to Aut(\mathcal{C}_{15}) \simeq \mathcal{C}_4 \times \mathcal{C}_2.$$

Or on sait (cf partiel 1) que si $\mathcal{G}$ est un groupe, l'ensemble des morphismes $\phi : \mathcal{C}_n \to \mathcal{G}$ est en bijection avec l'ensemble $\mathcal{G}_n = \{g \in \mathcal{G}, g^n = e\}$. Lorsque $n = 2$, $\mathcal{G}_2$ a pour éléments le neutre e et les éléments d'ordre 2.
On sait (cf (d)) que $\mathcal{C}_4 \times \mathcal{C}_2$ a 3 éléments d'ordre 2. Il y a donc quatre morphismes de $\mathcal{C}_2$ dans $Aut(\mathcal{C}_{15}) \simeq \mathcal{C}_4 \times \mathcal{C}_2$, donc quatre produits semi-directs de $\mathcal{C}_{15}$ par $\mathcal{C}_2$, i.e. il y a *au plus* quatre classes d'isomorphismes de groupes d'ordre 30.

Pour conclure la classification, il suffit de vérifier qu'aucuns des quatre groupes

$$\mathcal{C}_{30}, \quad \mathcal{C}_3 \times D_{10}, \quad \mathcal{C}_5 \times D_6, \quad D_{30} \qquad (L)$$

d'ordre 30 ne sont isomorphes.

C'est clair pour $\mathcal{C}_{30}$: il est abélien et les autres ne le sont pas.

Pour les autres, on peut par exemple essayer de comparer les ordres des centres ou les nombres d' éléments d'un ordre donné.

Comptons par exemple les éléments d'ordre 2:

- Pour n impair, D_{2n} a n éléments d'ordre 2 qui sont les $sr^j, j \in [0, n-1]$.

- Si A et B sont des groupes finis, l'ordre de $(a, b) \in A \times B$ (produit direct) est le ppcm des ordres de a et de b.

$\mathcal{C}_3 \times D_{10}$ a donc 5 éléments d'ordre 2, $\mathcal{C}_5 \times D_6$ en a 3 et D_{30} en a 15.

Comme tout isomorphisme conserve l'ordre des éléments ces groupes ne sont pas isomorphes.

Conclusion: tout groupe d'ordre 30 est isomorphe à un et un seul groupe de la liste L.

Exercice 18 (17 dans la version 1 de la fiche)

Cette preuve du théorème de Sylow figure en p 18 et 19 du *Cours d'Algèbre* de Daniel Perrin - Ellipses (dont plusieurs exemplaires sont à l'étage 4 de la BU). Je la détaille ici.

On suppose $|G| = p^\alpha m$ où p ne divise pas m et soit $P \leq G$ un $p-$ Sylow (P est d'ordre p^α).

G agit sur G/P par multiplication à gauche:

$$G \times G/P \to G/P : (g, aP) \mapsto g \cdot (aP) = ga\,P.$$

Le stabilisateur G_{aP} de aP pour cette action est le sous-groupe $G_{aP} = \{g \in G,\, g \cdot aP = aP\}$. Comme $gaP = aP$ ssi $a^{-1}gaP = P$ ssi $a^{-1}ga \in P$, on a $G_{aP} = aPa^{-1}$.

Venons-en à l'exercice.

(a) Par restriction, tout sous-groupe $H \leq G$ agit sur G/P

$$H \times G/P \to G/P : (h, xP) \mapsto hx\,P$$

et le stabilisateur H_{aP} de aP pour cette action est le sous-groupe $H_{aP} = G_{aP} \cap H = aPa^{-1} \cap H$. Comme sous-groupe du $p-$ Sylow aPa^{-1}, H_{aP} est un $p-$ groupe.

On suppose $|H| = p^\beta d$ où p ne divise pas d et $\beta \geq 1$, et il s'agit de montrer que l'un des H_{aP} est un $p-$ Sylow de H:
notons $O(aP) \subset G/P$ l'orbite de aP sous l'action de H et

$$G/P = \bigcup_i O(a_i P)$$

la partition de G/P en $H-$ orbites. On a

$$m = |G/P| = \sum_i |O(a_i P)| = \sum_i \frac{|H|}{|H_{a_i P}|}.$$

Si p divisait $|O(a_i P)|$ pour tout i, alors p diviserait m, ce qui est faux. Il existe donc i_0 pour lequel p ne divise pas $|O(a_{i_0} P)| = \frac{|H|}{|H_{a_{i_0} P}|}$, i.e. pour lequel le $p-$ groupe $H_{a_{i_0} P} = a_{i_0} P a_{i_0}^{-1} \cap H$ est d'ordre p^β.

(b) Il s'agit de vérifier que le sous-groupe $P \leq Gl_n(F_p)$ des matrices triangulaires de la forme

$$\begin{pmatrix} 1 & \star & \cdots & \star \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \star \\ 0 & \cdots & 0 & 1 \end{pmatrix}$$

est un $p-$ Sylow de $Gl_n(F_p)$. Observer que P est d'ordre $p^{\frac{(n-1)n}{2}}$ (les éléments $\star \in F_p$).
On a

$$\begin{aligned}|Gl_n(F_p)| &= (p^n-1)(p^n-p)(p^n-p^2)\cdots(p^n-p^{n-1}) \\ &= (p^n-1)p(p^{n-1}-1)p^2(p^{n-2}-1)\cdots p^{n-1}(p-1) \\ &= p^{1+2+\cdots+(n-1)}(p^n-1)(p^{n-1}-1)\cdots(p-1) \\ &= p^{\frac{(n-1)n}{2}}(p^n-1)\cdots(p-1).\end{aligned}$$

où p ne divise pas $(p^n-1)\cdots(p-1)$ (sinon p diviserait l'un des facteurs (p^j-1) donc aussi $p^j-(p^j-1)=1$).

Les $p-$ Sylow de $Gl_n(F_p)$ sont donc les sous-groupes d'ordre $p^{\frac{(n-1)n}{2}}$, en particulier P est un $p-$ Sylow.

(c) Soit H un groupe fini d'ordre n tel que $p \mid n$. Pour obtenir l'existence d'un $p-$ Sylow $S \leq H$ on commence par plonger H dans $Gl_n(F_p)$ en deux étapes.

Etape 1: l'action par multiplication $H \times H \to H : (h,y) \mapsto l_h(y) = hy$ induit le morphisme injectif de Cayley

$$H \to S_H \simeq S_n : h \mapsto l_h.$$

Etape 2: le groupe S_n agit linéairement sur l'espace F_p^n comme suit: si $(e_1, e_2, \ldots, e_n)$ est la base canonique de F_p^n et $\sigma \in S_n$, on note $P_\sigma \in Gl_n(F_p)$ la matrice (dans la base canonique) de l'unique isomorphisme linéaire de F_p^n envoyant e_i sur $e_{\sigma(i)}$.

L'application $S_n \to Gl_n(F_p) : \sigma \mapsto P_\sigma$ est alors un morphisme injectif de groupes.

Noter que les P_σ sont les matrices usuelles de permutations:

Pour $n=2$: $P_{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, P_{(12)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Pour $n \geq 2$, ce sont les matrices ayant exactement un coefficient non nul égal à 1 sur chaque ligne et chaque colonne. (Le déterminant de P_σ est égal à la signature de σ.)

En composant ces deux morphismes, on obtient le morphisme injectif

$$\psi : H \to S_n \to Gl_n(F_p) : h \mapsto P_{l_h}$$

H est donc isomorphe au sous-groupe $\psi(H) \leq Gl_n(F_p)$.

Par les questions (a) et (b), $\psi(H)$ admet un $p-$ Sylow de la forme $aPa^{-1} \cap \psi(H)$ pour un certain $a \in Gl_n(F_p)$ et P le $p-$ Sylow triangulaire de la question (b).

Les $p-$ Sylow étant conservés par isomorphisme, H lui-même admet un $p-$ Sylow.