

Composé de quelques exercices
(A. OULD HOUCINE)

Fiche 4, Exercice 15:

Rappels) ① Une classe de conjugaison est une classe d'équivalence par rapport à la relation :

$$a \sim b \quad \text{ssi} \quad \exists g \in G \text{ tq } g a g^{-1} = b.$$

② Dans S_n , si $\sigma = (a_1 a_2 \dots a_p)$ est un p -cycle alors $\tau \circ \sigma \circ \tau^{-1} = (\tau(a_1) \tau(a_2) \dots \tau(a_p))$ pour toute permutation $\tau \in S_n$ (voir exercices 23 et 24 de la fiche 1).

Dans S_3 : S_3 est composé des éléments suivants :

$$\text{Id}, \quad \sigma = (123), \quad \sigma^2 = (132), \quad \alpha = (12), \quad \beta = (23), \quad \gamma = (13).$$

$$\text{On a} \quad \beta \sigma \beta^{-1} = \sigma^2, \quad \sigma \alpha \sigma^{-1} = \beta, \quad \tau \beta \tau^{-1} = \gamma.$$

Donc il existe 3 classes de conjugaisons :

$$\mathcal{C}(\text{Id}) = \{ \text{Id} \}, \quad \mathcal{C}(\sigma) = \{ \sigma, \sigma^2 \}, \quad \mathcal{C}(\alpha) = \{ \alpha, \beta, \gamma \}.$$

Rq: D'une façon plus générale dans S_n , deux permutations sont conjuguées ssi elles ont la même structure de cycles (voir exercice 24 de la fiche 1).

Dans A_4 : $|A_4| = \frac{|S_4|}{2} = \frac{4!}{2} = 12.$ On peut

écrire :

$$A_4 = \{ \text{Id}, (123), (132), (124), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23) \}.$$

Si deux éléments de A_4 sont conjugués dans A_4 alors ils sont conjugués dans S_4 et donc ils ont la même structure de cycles.

En conjuguant (123) et (132) par les permutations $(12)(34)$, $(13)(24)$, $(14)(23)$, après calculs, on a:

$$cl((123)) = \{ (123), (142), (134), (243) \}$$

$$cl((132)) = \{ (132), (143), (124), (234) \}.$$

On vérifie également que $(12)(34)$, $(13)(24)$, $(14)(23)$ sont conjugués dans $\mathcal{A}_4$. En effet,

$$(143)(12)(34)(143)^{-1} = (42)(13)$$

en utilisant la formule rappelée plus haut. De même pour les autres permutations.

Donc il existe 4 classes de conjugaisons:

$$cl(\text{Id}), cl((123)), cl((132)), cl((12)(34)).$$

Dans D_8 : Nous avons:

$$D_8 = \{ \text{Id}, r, r^2, r^3, s, sr, sr^2, sr^3 \}$$

et $r^4 = s^2 = \text{Id}$ et $rs = sr^{-1}$. On a

$$sts = s \cdot sr^{-1} = s^2 r^{-1} = r^{-1} = r^3.$$

Par le même type de calculs, s et sr^2 sont conjugués et sr et sr^3 sont conjugués.

On conclut qu'il existe 5 classes de conjugaisons:

$$cl(\text{Id}), cl(r), cl(r^2), cl(s), cl(sr).$$

Dans Q_8 : On a:

$$Q_8 = \{ \text{Id}, -\text{Id}, I, -I, J, -J, K, -K \}$$

avec les relations: $I^2 = J^2 = K^2 = -\text{Id}$

$$IJ = K, JK = I, KI = J.$$

On a : $JIJ = -I$, $KJK = -J$, $IKI = -K$,

On voit que $-Id$, I , J , K ne sont pas conjugués. On a donc 5 classes de conjugaisons

$$cl(I) = \{ Id \}, \quad cl(J) = \{-J, J\}$$

$$cl(-Id) = \{-Id\}, \quad cl(K) = \{-K, K\}$$

$$cl(I) = \{-I, I\}.$$

Fiche 4, Exercice 17:

$$\gamma = (12345) \in S_5.$$

(a) On a

$$\gamma^2 : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}$$

qui est un 5-cycle. Si $\tau \in S_5$ tq $\tau\gamma\tau^{-1} = \gamma^2$

On aurait :

$$\tau\gamma\tau^{-1} = (\tau(1)\tau(2)\tau(3)\tau(4)\tau(5)) = \gamma^2$$

On a

$$\gamma^2 = (13524)$$

et donc on peut prendre, par identification:

$$\tau(1) = 1, \tau(2) = 3, \tau(3) = 5, \tau(4) = 2, \tau(5) = 4$$

et donc

$$\tau : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix}.$$

(b) On calcule γ^{-1} . On a $\gamma^{-1} = (54321)$

On peut aussi utiliser la décomposition :

$$\gamma = (12345) = (12)(23)(34)(45)$$

$$\text{et donc } \gamma^{-1} = (45)^{-1}(34)^{-1}(23)^{-1}(12)^{-1}$$

$$= (45)(34)(23)(12)$$

$$= (15432)$$

D'ici, en procédant comme dans (a) :

$$\begin{aligned} Z \sigma Z^{-1} &= (\sigma(1) \sigma(2) \sigma(3) \sigma(4) \sigma(5)) \\ &= (15432) \end{aligned}$$

et donc on peut prendre :

$$Z: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}.$$

Fiche 4, Exercice 19: Toute permutation de S_n ,

peut s'écrire comme un produit d'un nombre pair de transpositions. Il suffit donc de montrer que tout produit de la forme :

$$(ab)(cd)$$

est un produit de 3-cycles.

si $\{a, b\} \cap \{c, d\} = \emptyset$, alors (vérification immédiate)

$$(ab)(cd) = (abc)(bcd)$$

et donc $(ab)(cd)$ est produit de deux 3-cycles.

si $|\{a, b\} \cap \{c, d\}| = 1$, alors $a = c$ ou $a = d$ ou $b = c$ ou $b = d$. On peut supposer que $b = c$.

$$\text{Donc } (ab)(bd) = (abd)$$

qui est un 3-cycle également.

$$\text{si } |\{a, b\} \cap \{c, d\}| = 2, \text{ alors } (ab) = (cd)$$

$$\text{et donc } (ab)(cd) = (ab)^2 = \text{Id}$$

qui peut s'écrire comme produit de 3-cycles.

Fiche 4, Exercice 21: Posons $|G| = p$, impair
avec $p \geq 1$. Soit $x \in G \setminus \{e\}$: $\exists g \in G, gxg = x^{-1}$.

On déduit par récurrence sur n que

$$\begin{cases} g^n x g^{-n} = x, & \text{si } n \text{ est pair} \\ g^n x g^{-n} = x^{-1}, & \text{si } n \text{ est impair} \end{cases}$$

En effet par récurrence :

$$g(g^n x g^{-n}) \cdot g^{-1} = g^{n+1} x g^{-(n+1)} = (g x g^{-1})^s = x^{-s}$$

où $s = \pm 1$ selon la parité de n .

On: $g^p = 1$ et donc, comme p impair

$$x = g^p x g^{-p} = x^{-1}.$$

Soit $x \neq e$, on a $\text{ord}(x) = 2$ et donc

$2 \mid |G|$ contradiction.

Fiche 4, Exercice 23: Par la formule de

Burnside

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|$$

où Ω l'ensemble des orbites. Comme l'action
est transitive $|\Omega| = 1$. On sait également

que $\text{Fix}(e) = \{a \in A \mid ea = a\} = A$ et par

hypothèse $|\text{Fix}(e)| = |A| \geq 2$.

Supposons par l'absurde que

$$\forall g \in G, |\text{Fix}(g)| \geq 1.$$

$$\text{D'un côté } 1 = \frac{1}{|G|} \cdot (|\text{Fix}(e)| + \sum_{\substack{g \in G \\ g \neq e}} |\text{Fix}(g)|)$$

Et d'un autre côté

$$\frac{1}{|G|} \left(| \text{Fix}(e) | + \sum_{\substack{g \in G \\ g \neq e}} | \text{Fix}(g) | \right) \\ \geq \frac{1}{|G|} (2 + |G| - 1) = \frac{|G| + 1}{|G|}$$

car $| \text{Fix}(g) | > 1$, $\forall g \in G, g \neq e$.

Contradiction :

$$1 \geq \frac{|G| + 1}{|G|}.$$

Fiche 4, Exercice 27:

(a) On remarque que les deux quantités ont deux façons différentes de compter les membres de l'ensemble :

$$A = \{ (g, x) \in G \times X \mid gx = x \}.$$

En effet, d'un côté

$$A = \bigsqcup_{g \in G} \{ (g, x) \mid \underbrace{gx = x}_{\text{Fix}(g)} \}$$

et pour g fixé, $|\{ (g, x) \mid \underbrace{gx = x}_{\text{Fix}(g)} \}| = |\{ x \mid gx = x \}|$
et donc

$$|A| = \sum_{g \in G} | \text{Fix}(g) |$$

et d'un autre côté

$$A = \bigsqcup_{x \in X} \{ (g, x) \mid \underbrace{gx = x}_{G_x} \}$$

et pour x fixé $|\{ (g, x) \mid \underbrace{gx = x}_{G_x} \}| = |G_x|$.

et donc $|A| = \sum_{x \in X} |G_x|$.

D'où finalement

$$\sum_{x \in X} |G_x| = \sum_{g \in G} |\text{Fix}(g)|.$$

(b) On a

$$|A| = \sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|O_x|}$$
$$= \sum_{w \in \Omega} \left(\sum_{x \in w} \frac{|G|}{|O_x|} \right), \text{ car}$$

$$\sum_{x \in w} \frac{|G|}{|O_x|} = \frac{|G|}{|O_x|} \cdot |w| = |G|, |w| = |O_x|$$

D'où $|A| = \sum_{w \in \Omega} |G| = |\Omega| \cdot |G|$

Dmcl $\sum_{g \in G} \frac{|\text{Fix}(g)|}{|G|} = \frac{|A|}{|G|} = |\Omega|.$

Petite révision des groupes diédraux

Soit $n \in \mathbb{N}, n \geq 1$. Le groupe diédral D_n est l'unique groupe (à isomorphisme près) engendré par deux éléments r, s vérifiant :

$$\text{ord}(r) = n, \text{ord}(s) = 2 \text{ et } srs^{-1} = r^{-1}.$$

(pour $n=2$, on exige aussi que $s \notin \langle r \rangle$).

Il peut être identifié au sous-gp engendré par une rotation r d'angle $\frac{2\pi}{n}$ et de la symétrie orthogonale s d'axe (Ox) . C'est également le groupe des isométries du plan qui conservent globalement un polygone régulier à n côtés.

Sait $g \in D_{2n}$. Comme D_{2n} est engendré par r et s , il existe $n_1, m_1, n_2, m_2, \dots, n_p, m_p \in \mathbb{Z}$ tels

$$g = s^{n_1} r^{m_1} \dots s^{n_p} r^{m_p},$$

mais grâce à la relation $sr s^{-1} = sr s = r^{-1}$, on a

par récurrence

$$s^{n_1} r^{m_1} s^{n_2} = s^{n_1 + n_2} r^{\pm m_1}$$

et donc finalement par récurrence :

$$g = s^\alpha r^\beta \quad \text{où} \quad \alpha, \beta \in \mathbb{Z}.$$

Or comme $s^2 = 1$ et $r^n = 1$, le nombre

des cas est limité, $\alpha \in \llbracket 0, 1 \rrbracket$, $\beta \in \llbracket 0, n-1 \rrbracket$

et donc :

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}.$$

Supposons que $n = 2m$, où $m \geq 1$.

Sait $H \leq D_{2n}$ engendré par $\{r^2, s\}$.

Alors $\text{ord}(r^2) = m$ et $sr^2 s^{-1} = (sr s^{-1})^2 = (r^2)^{-1}$.

Donc $H \cong D_{2m}$. On remarque

également que $H \trianglelefteq D_{2n}$. En effet, il

suffit de vérifier pour tout $g \in \{r^{\pm 1}, s^{\pm 1}\}$

et $h \in \{(r^2)^{\pm 1}, s^{\pm 1}\}$, $g^{-1} h g \in H$, ce

qui est immédiat.

Rappel: $C_G(H) = \{ g \in G \mid ghg^{-1} = h, \forall h \in H \}$.

Calculons $C_{D_{2n}}(H)$ où $H = \langle r^2, s \rangle$
 où $n = 2m$. Soit $\alpha \in \mathbb{I}0,1\mathbb{I}$, $\beta \in \mathbb{I}0, n-1\mathbb{I}$.

Alors $(s^\alpha r^\beta) r^2 (r^{-\beta} s^{-\alpha}) = r^2$

ssi $s^\alpha r^2 s^{-\alpha} = r^2$

ssi $\alpha = 0$ ou $(\alpha = 1 \text{ et } r^2 = r^{-2})$

Si $\alpha = 0$: $r^\beta s r^{-\beta} = s$

ssi $r^\beta = r^{-\beta}$

ssi $2\beta = n$ ssi $\beta = m$

Dans ce cas $s^\alpha r^\beta = r^m$

Si $\alpha = 1$: Alors $r^2 = r^{-2}$ et donc $m = 2$.

Dans le cas : $s^\alpha r^\beta = s r^2$, $\beta = 2$.

Donc si $n = 4$, $C_{D_{2n}}(H) = H$ et si

$n > 4$, alors $C_{D_{2n}}(H) = \{ r^m, \text{Id} \}$.

Fiche 5, Exercice 7(b), version détaillée:

Donc on considère :

$$\varphi: D_{16} \longrightarrow \text{Aut}(H)$$

$$g \longmapsto \varphi(g): H \longrightarrow H$$

$$x \mapsto \varphi(g)(x) = gxg^{-1}$$

ici $H = \langle r^2, s \rangle \cong D_8$ et $H \trianglelefteq D_{16}$

Alors φ est un morphisme et

$$\begin{aligned}\text{Ker}(\varphi) &= \{ g \in D_{16} \mid \varphi(g) = \text{Id} \} \\ &= \{ g \in D_{16} \mid gxg^{-1} = x, \forall x \in H \} \\ &= C_{D_{16}}(H) = \{ r^4, \text{Id} \}\end{aligned}$$

D'après: $\left| \frac{D_{16}}{\text{Ker}(\varphi)} \right| = \frac{16}{2} = 8 = |\text{Im}(\varphi)|$

et comme $|\text{Im}(\varphi)| \leq \text{Aut}(D_8) \leq 8$

On a $\text{Im}(\varphi) = \text{Aut}(D_8)$.

Donc φ est surjectif et

$$\hat{\varphi}: \frac{D_{16}}{\text{Ker}(\varphi)} \longrightarrow \text{Aut}(D_8)$$

induit par φ est un isomorphisme.

Soit $\pi: D_{16} \longrightarrow \frac{D_{16}}{\text{Ker}(\varphi)}$ la projection

canonique. Posons $r' = \pi(r)$, $s' = \pi(s)$.

Alors $\frac{D_{16}}{\text{Ker}(\varphi)} = \langle r', s' \rangle$ et on

vérifie $\text{ord}(r') = 4$, $\text{ord}(s') = 2$ et

$s'r's' = r'^{-1}$. Donc $\frac{D_{16}}{\text{Ker}(\varphi)} \cong D_8$.

Enfin: $D_8 \cong \frac{D_{16}}{\text{Ker}(\varphi)} \cong \text{Aut}(D_8)$.

Remarque: (1) $Z(D_{16}) = \text{Ker}(\varphi)$.

(2) Une autre propriété importante de D_{2n} ,

si on pose $R = \langle r \rangle$, $S = \langle s \rangle$, alors

$$D_{2n} = R \rtimes S.$$

Fiche 5, Exercice 11:

(a) $|G| = 6545 = 5 \times 7 \times 11 \times 17$. Soit pour $p \in \{5, 7, 11, 17\}$, A_p un p -Sylow. On va montrer qu'il existe p tq $A_p \triangleleft G$. Pour cela il suffit de montrer que $N_p = 1$ ou N_p est le nombre des p -Sylow. Supposons $N_p \neq 1$ pour tout $p \in \{5, 7, 11, 17\}$. En utilisant le fait que $N_p \equiv 1 \pmod{p}$ et $N_p \mid \frac{|G|}{p}$, les seules possibilités qui restent sont : $N_5 = 11$, $N_7 = 85$, $N_{11} = 595$, $N_{17} = 35$.

Comme p est premier, si A_p et A_p' sont deux p -Sylow distincts, alors $A_p \cap A_p' = \{1\}$.

Donc le nombre total des éléments de G est au moins

$$|G| \geq \underset{\substack{\uparrow \\ \text{pour l'élément neutre}}}{1} + \sum_p N_p (|A_p| - 1)$$

$$= 1 + 10 \times 5 + 85 \times 6 + 595 \times 10 + 35 \times 16$$

$$= 7071 > 6545$$

Donc il existe p tq $N_p = 1$ et donc $A_p \triangleleft G$.

(On remarque qu'on peut prendre $p \in \{7, 11, 17\}$)

(b) & (c) : On procède de la même façon.

Fiche 5, Exercice 12: On a $|G| = 3 \times 5 \times 7$.

Soit A_5 (resp. A_7) un 5-Sylow (resp. 7-Sylow).

$$\text{Alors } \begin{cases} N_5 \equiv 1 \pmod{5} \text{ et } N_5 \mid 3 \times 7, \\ N_7 \equiv 1 \pmod{7} \text{ et } N_7 \mid 3 \times 5. \end{cases}$$

$$\text{Donc } (N_5 = 1 \text{ ou } N_5 = 21) \\ \text{et } (N_7 = 1 \text{ ou } N_7 = 15)$$

Si $N_5 = 21$ et $N_7 = 15$, alors G aurait au moins

$$1 + \sum_p N_p (|A_p| - 1) \\ = 1 + 1 \times (3-1) + 21 \times (5-1) + 15 \times (7-1) \\ = 177 > 105$$

éléments, ce qui est impossible.

$$\text{Donc } N_5 = 1 \text{ ou } N_7 = 1.$$

Supposons $N_5 = 1$. Soit $A_3 \trianglelefteq G$ l'unique 3-Sylow.

$$\text{Soit } H = \langle A_5, A_7 \rangle. \text{ Alors } H = A_5 \times A_7$$

$$\text{car } A_5 \cap A_7 = \{1\} \text{ et } A_5 \trianglelefteq G \text{ et donc } A_5 \trianglelefteq H.$$

$$\text{D'où } |H| = 35. \text{ Comme } [G:H] = 3 \text{ et}$$

3 est le plus petit premier qui divise $|G|$,
on a $H \trianglelefteq G$. On a $A_3 \cap H = \{1\}$
(par le théorème de Lagrange) et donc $G = A_3 \times H$.

On voit que A_7 est l'unique 7-Sylow de

$$H \text{ et donc } A_7 \trianglelefteq H \text{ et donc finalement}$$

$$H = A_5 \times A_7. \text{ Enfin } G = A_3 \times A_5 \times A_7$$

qui est abélien. Le cas $N_7 = 1$ est
symétrique et se traite de la même façon.

Fiche 5, Exercice 3 (c), version détaillée.

Soient $\alpha: C_p \rightarrow \text{Aut}(C_q)$, $\beta: C_p \rightarrow \text{Aut}(C_q)$
deux morphismes non-triviaux. On a pour
tout $k \in \mathbb{I}0, q-1\mathbb{I}$ et tout $h \in \mathbb{I}0, p-1\mathbb{I}$,

$$\alpha(h.\bar{i})(k.\bar{i}) = k.\alpha(h.\bar{i})(\bar{i})$$

et comme $\alpha(h+h')\bar{i}$ est la composition d'applications
qui se transforme en produit, on a.

$$\alpha(h.\bar{i})(\bar{i}) = (\alpha(\bar{i})(\bar{i}))^h.$$

(Voir Exercice 28, Fiche 3). Donc finalement
pour tout $k \in \mathbb{I}0, q-1\mathbb{I}$ et tout $h \in \mathbb{I}0, p-1\mathbb{I}$

$$\alpha(h.\bar{i})(k.\bar{i}) = k.(\alpha(\bar{i})(\bar{i}))^h$$

et de même pour β

$$\beta(h.\bar{i})(k.\bar{i}) = k.(\beta(\bar{i})(\bar{i}))^h.$$

posons $\alpha_0 = \alpha(\bar{i})(\bar{i})$ et $\beta_0 = \beta(\bar{i})(\bar{i})$. Comme
 $(C_q^\times, \cdot)$ est cyclique, d'ordre $q-1$, et $p \mid q-1$,
il a exactement $\varphi(p)$ éléments d'ordre p
où φ est l'indicatrice d'Euler (Voir Exercice
15, Fiche 1). Donc il existe $p-1$ éléments
d'ordre p et ainsi il existe un unique $g \in C_p$
d'ordre p , notons-le D . Or $\text{ord}(\alpha_0) = \text{ord}(\beta_0) = p$
et donc $D = \langle \alpha_0 \rangle = \langle \beta_0 \rangle$. D'où $\exists m \in \mathbb{N}$

$$\text{tg } \alpha_0 = \beta_0^m.$$

$$\text{Soit } \varphi: C_q \rtimes_{\alpha} C_p \rightarrow C_q \rtimes_{\beta} C_p$$
$$(x, y) \mapsto (x, my)$$

et montrer que φ est un morphisme.

$$\begin{aligned} \text{On a } & \varphi((x, y) \cdot \alpha(x', y')) \\ &= \varphi(x + \alpha(y)(x'), y + y') \\ &= (x + \alpha(y)(x'), m(y + y')) \end{aligned}$$

$$\begin{aligned} & \varphi(x, y) \cdot_{\beta} \varphi(x', y') \\ &= (x, my) \cdot_{\beta} (x', my') \\ &= (x + \beta(my)(x'), my + my') \end{aligned}$$

O2: $\beta(my)(x') = x' \cdot \beta_0^m y = x' (\beta_0^m) y = x' \cdot \alpha_0 y$
 $= \alpha(y)(x').$

Donc φ est bien un morphisme.

$$\text{On a } \text{Ker}(\varphi) = \left\{ (x, y) \mid \begin{array}{l} my \equiv 0 [p] \\ x \equiv 0 [q] \end{array} \right\}$$

Or $my \equiv 0 [p] \rightarrow p \mid my$ et comme $p \nmid m$ (car sinon $\beta_0^m = 1$), on a $y \equiv 0 [p]$.

Donc $\text{Ker}(\varphi) = \{(0, 0)\}$ et φ est injectif.

Par un argument de cardinalité, φ est surjectif.

Donc φ est bien un isomorphisme.

Version courte: Soit $\alpha: C_p \rightarrow \text{Aut}(C_q)$,

$\beta: C_p \rightarrow \text{Aut}(C_q)$ deux morphismes non triviaux. Alors $\alpha(\bar{1}), \beta(\bar{1})$ sont des éléments d'ordre p dans $\text{Aut}(C_q) \cong (C_q^{\times}, \cdot) \cong (C_{q-1}, +)$ et donc (comme précédemment), $\langle \alpha(\bar{1}) \rangle = \langle \beta(\bar{1}) \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

(Il existe un unique sos-gp d'ordre p dans C_q^X)

Donc il existe un automorphisme $\varphi \in \text{Aut}(C_p)$
tq $\beta = \alpha \circ \varphi$. On utilise alors un fait
général.

Fait: Soit H et K deux gps et
 $\alpha: H \rightarrow \text{Aut}(K)$, $\beta: H \rightarrow \text{Aut}(K)$
deux morphismes. Supposons qu'il
existe $\varphi \in \text{Aut}(H)$ tq $\beta = \alpha \circ \varphi$.
Alors $K \rtimes_{\alpha} H \cong K \rtimes_{\beta} H$.

Preuve: On définit:

$$\psi: K \rtimes_{\alpha} H \longrightarrow K \rtimes_{\beta} H$$

$$(k, h) \longmapsto (k, \varphi^{-1}(h)).$$

On vérifie bien que ψ est un isomorphisme.

Fiche 5, Exercice 15: $|G| = 30 = 2 \times 3 \times 5$.

(a) Supposons que $n_3 = 10$ et $n_5 = 6$.

Alors $|G|$ a au moins $1 + 10 \times 2 + 6 \times 4 = 45$
éléments, ce qui est impossible.

D'après le théorème de Sylow, $n_3 \equiv 1 [3]$
 $n_3 \mid 10$, $n_5 \equiv 1 [5]$, $n_5 \mid 6$. Donc la
seule possibilité est $n_3 = 1$ ou $n_5 = 1$.

(b) Supposons $n_3 = 1$. Le cas $n_5 = 1$ se
traite de la même façon.

Soit A_3 un 3-Sylow et A_5 un 5-Sylow.

Posons $H = \langle A_3, A_5 \rangle$. On va montrer que $H \cong C_{15}$ et $H \trianglelefteq G$. Comme $n_3 = 1$, $A_3 \trianglelefteq G$. Comme $A_3 \cap A_5 = \{1\}$, on a $H = A_3 \rtimes A_5$. Donc $|H| = 15$ et A_5 est l'unique 5-Sylow de H (par le 3-ième théorème de Sylow). Donc $A_5 \trianglelefteq H$ et finalement $H = A_3 \times A_5$. Donc H est cyclique $\cong C_{15}$. Comme $[G:H] = 2$, $H \trianglelefteq G$.

(c) Soit $\pi: G \rightarrow G/H$ la surjection canonique.

Abs $|G/H| = 2$. Soit $g \in G \setminus H$ ord(g) = 2.

Abs $g \notin H$ et $\pi(g)$ engendre G/H .

Donc si A_2 est un 2-Sylow de G

$G = \langle H, A_2 \rangle$. Comme $H \trianglelefteq G$ et

$A_2 \cap H = \{1\}$, on a

(d) On a $\text{Aut}(C_{15}) \cong (C_{15}^\times, \cdot)$

le groupe des éléments inversibles de $(C_{15}, \cdot)$.

On a un élément $\bar{m}$, $m \in \llbracket 0, 14 \rrbracket$ est inversible

ssi $\text{pgcd}(m, 15) = 1$. Donc

$$(C_{15}^\times, \cdot) = \{ \bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}, \bar{14} \}$$

O₂: $\bar{4} = \bar{2}^2, \bar{8} = \bar{2}^3, \bar{11}^2 = \bar{1}, \bar{2} \times \bar{11} = \bar{7}, \bar{2}^2 \times \bar{11} = \bar{14}$
 $\bar{2}^3 \times \bar{11} = \bar{13},$

et donc $(C_{15}^\times, \cdot) = \{ \bar{1}, \bar{2}, \bar{2}^2, \bar{2}^3 \} \times \{ \bar{1}, \bar{11} \}$
 $\cong C_4 \times C_2$.

(e) Écrivons $C_2 = \{\bar{0}, \bar{1}\}$ avec la notation additive.

Un morphisme non-trivial $\alpha: C_2 \rightarrow \text{Aut}(\mathbb{Z}/_{15}\mathbb{Z})$ est entièrement déterminé par $\alpha(\bar{1})$, un élément d'ordre 2 dans $\text{Aut}(\mathbb{Z}/_{15}\mathbb{Z})$. D'après (d), il existe 3 éléments d'ordre 2 dans $(\mathbb{Z}/_{15}\mathbb{Z}^\times, \cdot)$: $\bar{2}^2, \bar{11}, \bar{2}^2 \cdot \bar{11}$.

Donc on a 3 morphismes non-triviaux :

$$\begin{aligned} \downarrow \chi : C_2 &\longrightarrow \text{Aut}(\mathbb{Z}/_{15}\mathbb{Z}) \\ x &\longmapsto \alpha_1(x) : \mathbb{Z}/_{15}\mathbb{Z} \longrightarrow \mathbb{Z}/_{15}\mathbb{Z} \\ y &\longmapsto \alpha_1(x)(y) = y \cdot (\bar{2})^x \end{aligned}$$

$$\begin{aligned} \alpha_2 : C_2 &\longrightarrow \text{Aut} \left(\frac{\mathbb{Z}}{15\mathbb{Z}} \right) \\ x &\longmapsto \alpha_2(x) : \frac{\mathbb{Z}}{15\mathbb{Z}} \longrightarrow \frac{\mathbb{Z}}{15\mathbb{Z}} \\ y &\longmapsto \alpha_2(x)(y) = y \cdot (\overline{11})^x \end{aligned}$$

$$\begin{aligned} \alpha_3: \quad C_2 &\longrightarrow \text{Aut}(\mathbb{Z}/15\mathbb{Z}) \\ x &\longmapsto \alpha_3(x): \mathbb{Z}/15\mathbb{Z} \longrightarrow \mathbb{Z}/15\mathbb{Z} \\ y &\longmapsto \alpha_3(x)(y) = y \cdot (2^2 \cdot \bar{11})^x \end{aligned}$$

$$\begin{aligned} \text{On } a \quad \frac{7}{15} &= \frac{7}{3} \oplus \frac{7}{5} \\ &= \{ \bar{0}, \bar{5}, 2 \cdot \bar{5} \} \oplus \{ \bar{0}, \bar{3}, 2 \times \bar{3}, 3 \times \bar{3}, 4 \times \bar{3} \} \\ &\quad \begin{matrix} \text{"} \\ \langle \bar{5} \rangle \end{matrix} \quad \begin{matrix} \text{"} \\ \langle \bar{3} \rangle \end{matrix} \\ &\quad \text{ord}(\bar{5}) = 3, \quad \text{ord}(\bar{3}) = 5 \end{aligned}$$

Posons $a = \sqrt{5}$ et $b = \sqrt{3}$. On étudie l'action de $\alpha_1, \alpha_2, \alpha_3$ sur a et b .

On a: $\chi_1(\bar{1})(a) = \overline{2^2} \cdot a = \bar{4} \cdot \bar{5} = \bar{20} = \bar{5}.$

Donc α_n est injective sur $\mathbb{Z}/5\mathbb{Z}$.

On déduit dans ce cas que

$$\left(\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}} \right) \rtimes_{\alpha_1} C_2 \cong \mathbb{Z}/_{3\mathbb{Z}} \times \left(\mathbb{Z}/_{5\mathbb{Z}} \rtimes_{\alpha_1} C_2 \right)$$

On étudie la structure de $\mathbb{Z}/_{5\mathbb{Z}} \rtimes_{\alpha_1} C_2$.

On peut utiliser ici la classification des groupes d'ordre $p \cdot q$ avec p et q premiers.

Comme $\mathbb{Z}/_{5\mathbb{Z}} \rtimes_{\alpha_1} C_2$ est non-abélien et

comme $D_{10} \cong \mathbb{Z}/_{5\mathbb{Z}} \rtimes C_2$, on a $D_{10} \cong \mathbb{Z}/_{5\mathbb{Z}} \rtimes_{\alpha_1} C_2$.

Donc finalement $G \cong C_3 \times D_{10}$.

$$\begin{aligned} \text{On a } \alpha_2(\bar{1})(\bar{b}) &= \alpha_2(\bar{1})(\bar{3}) \\ &= \bar{3} \cdot \bar{1} = \bar{3} \end{aligned}$$

et donc α_2 laisse invariant $\mathbb{Z}/_{5\mathbb{Z}}$. D'où :

$$\left(\mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}} \right) \rtimes_{\alpha_2} C_2 \cong \mathbb{Z}/_{5\mathbb{Z}} \times \left(\mathbb{Z}/_{3\mathbb{Z}} \rtimes_{\alpha_2} C_2 \right).$$

De même ici, on étudie la structure de $\mathbb{Z}/_{3\mathbb{Z}} \rtimes_{\alpha_2} C_2$. De même on utilise la

classification des groupes d'ordre $p \cdot q$.

Ainsi $D_6 \cong \mathbb{Z}/_{3\mathbb{Z}} \rtimes_{\alpha_2} C_2$.

Finalement, dans ce cas $G \cong C_5 \times D_6$.

On remarque que $\alpha_3(x) = \alpha_1 \circ \alpha_2(x)$ et

on a, en posant $s = (\bar{0}, \bar{1})$, $t = (\bar{3} + \bar{5}, \bar{0})$

$$\begin{aligned} s \cdot d_3 t &= (\bar{0}, \bar{1}) \cdot d_3 (\bar{3} + \bar{5}, \bar{0}) \\ &= (d_3(\bar{1})(\bar{3} + \bar{5}), \bar{1}) = (\bar{7}, \bar{1}) \end{aligned}$$

$$\begin{aligned} t^{-1} \cdot d_3 s &= (\bar{7}, \bar{0}) \cdot d_3 (\bar{0}, \bar{1}) \\ &= (\bar{7} + d_3(\bar{0})(\bar{0}), \bar{1}) = (\bar{7}, \bar{1}) \end{aligned}$$

et donc $s \cdot d_3 t = t^{-1} \cdot d_3 s$.

Donc $(\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}) \rtimes_{d_3} C_2$ est engendré par s, t , avec $\text{ord}(s) = 2$, $\text{ord}(t) = 15$ et vérifiant $s \cdot t = t^{-1} \cdot s$. Dans ce cas

$$G \cong D_{30}.$$

En fin pour le morphisme trivial, on obtient $G \cong C_3 \times C_5 \times C_2 \cong C_{30}$.

Conclusion. G est isomorphe à un des groupes : C_{30} , $C_3 \times D_{10}$, $C_5 \times D_6$, D_{30} .

(f) En étudiant le centre des différents groupes on a :

$$Z(C_{30}) = C_{30}$$

$$Z(C_3 \times D_{10}) = C_3 \times Z(D_{10}) = C_3$$

$$Z(C_5 \times D_6) = C_5 \times Z(D_6) = C_5$$

$$Z(D_{30}) = \{1\}$$

et donc ces groupes sont deux-à-deux non isomorphes.

Fiche 5, Exercice 15: Soit G un gp d'ordre 75. On a $75 = 3 \times 5^2$. Soit A_3 (resp. A_5) un 3-Sylow (resp. 5-Sylow) de G . Alors, d'après le 3-ième théorème de Sylow, $N_5 \equiv 1 [5]$ et $N_5 \mid 3$. Dnc $N_5 = 1$. Donc A_5 est distingué dans G . Soit $A_3 \cap A_5 = \{1\}$, le sous-gp $H = \langle A_3, A_5 \rangle$ est $A_5 \rtimes A_3$ et comme $|A_5 \rtimes A_3| = 75$ on conclut que $G = A_5 \rtimes A_3$.

On a $|A_5| = 5^2$ et il est donc abélien. En effet tout gp d'ordre p^2 , p premier, est abélien. (Si $Z(G) < G$ alors $|Z(G)| = p$ et $G/Z(G)$ est cyclique et donc G est abélien).

D'nc $A_5 \cong C_5 \times C_5$ ou $A_5 \cong C_{25}$.

Déterminons les morphismes de C_3 dans $\text{Aut}(C_5 \times C_5)$ et dans $\text{Aut}(C_{25})$.

On a $\text{Aut}(C_{25}) \cong (C_{25}^\times, \cdot)$. Un élément $m \cdot 1$ de $C_{25}^\times$ est inversible ssi $m \wedge 25 = 1$ ssi $m \not\equiv 0 [5]$. Donc $|C_{25}^\times| = 20$ et il n'existe pas d'éléments d'ordre 3 (Par le théorème de Lagrange, $3 \nmid 20$). Dans ce cas l'unique morphisme est le morphisme trivial et donc $G \cong C_3 \times C_{25}$.

Comme 5 est premier $C_5 \times C_5$ est un espace vectoriel sur le corps $\mathbb{F}_5$ et donc

$$\text{Aut}(C_5 \times C_5) \cong GL_2(\mathbb{F}_5).$$

$$\text{On a } |GL_2(\mathbb{F}_5)| = (5^2 - 1)(5^2 - 5) = 24 \times 20 \\ = 2^5 \times 3 \times 5$$

Soit A_3 un 3-Sylow de $GL_2(\mathbb{F}_5)$. Soit

donc $\alpha: C_3 \rightarrow GL_2(\mathbb{F}_5)$, $\beta: C_3 \rightarrow GL_2(\mathbb{F}_5)$

deux morphismes non-triviaux. On va

montrer que $(C_5 \times C_5) \rtimes_{\alpha} C_3 \cong (C_5 \times C_5) \rtimes_{\beta} C_3$.

Soit a un élément générateur de C_3 . Alors

$\alpha(a)$, $\beta(a)$ sont dans des 3-Sylows.

Sans perte de généralité, on peut supposer
que $\alpha(a) \in A_3$ et $\beta(a) \in A_3$ pour

un certain $g \in GL_2(\mathbb{F}_5)$ (Rappelons que

les p-tps de Sylow sont conjugués).

Donc $\beta(a)^{g^{-1}} \in A_3$ et donc il existe

un automorphisme $\varphi: C_3 \rightarrow C_3$ tq

$$\alpha(\varphi(a)) = \beta(a)^{g^{-1}}.$$

On conclut

qu'il existe $\varphi \in \text{Aut}(C_3)$ et

une conjugaison $\text{conj}: x \mapsto x g^{-1}$ de $GL_2(\mathbb{F}_5)$ tq

$$\begin{array}{ccc} C_3 & \xrightarrow{\alpha} & A_3 \subseteq GL_2(\mathbb{F}_5) \\ \uparrow \varphi & & \uparrow \text{conj} \\ C_3 & \xrightarrow{\beta} & A_3 \subseteq GL_2(\mathbb{F}_5) \end{array}$$

$g x g^{-1}$

et donc

$$\alpha \circ \varphi = \text{conj} \circ \beta.$$

On utilise le fait suivant:

Fait: Soit H et K deux groupes et

$\alpha : H \rightarrow \text{Aut}(K)$, $\beta : H \rightarrow \text{Aut}(K)$ deux morphismes.

Supposons qu'il existe $g \in \text{Aut}(K)$ tq
 $\beta(h) = g \alpha(h) g^{-1}$ pour tout $h \in H$.

Alors $K \rtimes_{\alpha} H \cong K \rtimes_{\beta} H$.

Preuve: On définit

$$\begin{aligned} \psi : K \rtimes_{\alpha} H &\longrightarrow K \rtimes_{\beta} H \\ (k, h) &\longmapsto (g(k), h) \end{aligned}$$

Alors ψ est un isomorphisme. $\square$

Par un fait précédent :

$$C_5^2 \rtimes_{\alpha} C_3 \cong C_5^2 \rtimes_{\alpha \circ \beta} C_3$$

et par le fait ci-dessus, on a

$$C_5^2 \rtimes_{\alpha \circ \beta} C_3 \cong C_5^2 \rtimes_{\beta} C_3.$$

$$\text{Donc } C_5^2 \rtimes_{\alpha} C_3 \cong C_5^2 \rtimes_{\beta} C_3.$$

Conclusion: Fixons $\alpha: C_3 \rightarrow \text{Aut}(C_5^2)$

un morphisme non-trivial.

En incluant le morphisme trivial, on conclut que $G \cong C_{25} \times C_3$ ou

$$G \cong C_5^2 \times C_3 \quad \text{ou} \quad G \cong C_5^2 \rtimes_{\alpha} C_3.$$

Fiche 5, Exercice 17: On procède comme

dans l'exercice précédent. Soit G tq $|G| = 28 = 2^2 \times 7$. Soit A_2 (resp. A_7) un 2-Sylow

(resp. 7-Sylow). On a $N_7 \equiv 1 \pmod{7}$ et $N_7 \mid 4$ et donc $N_7 = 1$. Donc $N_7 \trianglelefteq G$.

Donc, en procédant comme dans l'exercice

précédent $G = A_7 \rtimes A_2$. On étudie les

morphismes $\alpha: A_2 \rightarrow \text{Aut}(A_7)$. Ici $A_7 \cong \mathbb{Z}/7\mathbb{Z}$

et $A_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$ ou $A_2 \cong \mathbb{Z}/4\mathbb{Z}$.

On sait que $\text{Aut}(A_7) \cong (A_7^{\times}, \cdot)$.

Supposons d'abord que $A_2 \cong C_2^2$.

En procédant comme dans l'exercice (3)(e)

$(A_7^{\times}, \cdot)$ a un unique sous-gp d'ordre 2 et donc un unique élément, appelons-le γ ,

d'ordre 2.

Posons $C_2^2 = \langle a \rangle \oplus \langle b \rangle$. Donc

tout morphisme $\alpha: C_2^2 \rightarrow \text{Aut}(A_7)$
non trivial est déterminé par le couple
 $(\alpha(a), \alpha(b))$ où $\alpha(a)$ (resp. $\alpha(b)$) est
ou bien trivial ou est égale à γ . Donc
 $(\alpha(a), \alpha(b)) \in \{ (1, \gamma), (\gamma, 1), (\gamma, \gamma) \}$.

Les deux morphismes α_1, α_2 déterminés par
 $(1, \gamma)$ et $(\gamma, 1)$ sont liés par un
automorphisme φ de C_2^2 qui envoie
 a sur b et b sur a . Dans ce cas, en
utilisant un fait précédent,

$$A_7 \rtimes_{\alpha_1} C_2^2 \cong A_7 \rtimes_{\alpha_2} C_2^2$$

Soit $\alpha_3: C_2^2 \rightarrow \text{Aut}(A_7)$ déterminé
par (γ, γ) (i.e. $\alpha_3(a) = \alpha_3(b) = \gamma$).

Abrs: $G \cong A_7 \rtimes_{\alpha_3} C_2^2$.

Supposons maintenant que $A_2 \cong C_4$.

Abrs $|A_7^x| = 7-1 = 6$ qui n'est pas
divisible par 4 et donc tout morphisme
 $\alpha: C_4 \rightarrow \text{Aut}(A_7)$ est trivial. Dans
ce cas $G \cong C_7 \times C_4$.

Conclusion: $G \cong C_7 \times C_4$ ou $G \cong C_7 \times C_2^2$
ou $G \cong C_7 \rtimes_{\alpha_1} C_2^2$ ou $G \cong C_7 \rtimes_{\alpha_3} C_2^2$.