

TD 1 – Groupes

Solutions des exercices

Exercice 1.

- 1) — Étape 1 : Nous allons montrer que $H_d = \langle c^{n/d} \rangle$ est d'ordre d .
Soit d un diviseur de n . On peut donc écrire $n = dq$. Considérons $H = \langle c^q \rangle$. On a

$$H = \langle e, e^q, e^{2q}, \dots, e^{(d-1)q} \rangle \text{ } d \text{ éléments distincts.}$$

De plus, pour tout $k \in \mathbb{Z}$, $k = nd + r$, $c^{qk} = c^{qnd} c^{qr} = c^{qr}$

- Étape 2 : On va montrer qu'un sous-groupe de C_n s'écrit $H = \langle c^{n/d} \rangle$.

Soit $H < C_n$. $\forall h \in H, \exists k \in \mathbb{Z}$ tel que $h = e^k$.

Si $H = \{e\}$, il n'y a rien à faire car $H = \{e^n\}$ et $n \mid n$.

Si $H \neq \{e\}$, $\exists h \in H, h = e^k$ tel que $n \nmid k$. On peut supposer que $0 < k < n$.

Soit $k_0 = \min\{k > 0 \mid c^k \in H\}$.

Montrons que $k_0 \mid n$ et que $\langle c^{k_0} \rangle = H$.

Soit $n = mk_0 + r$, $0 \leq r < k_0$.

$$c^r = c^n c^{-mk_0} = (c^{k_0})^{-m} \in H.$$

Donc $r = 0$ par minimalité de k_0 .

Montrons que $H = \langle c^{k_0} \rangle$.

Supposons que pour $l \in \mathbb{Z}$, $c^l \in H$.

On écrit $l = mk_0 + r$ $0 < r < k_0$:

$$c^r = c^l (c^{k_0})^{-m} \in H.$$

Ce qui est en contradiction avec la minimalité de k_0 .

On a donc montré que les sous-groupes de C_n sont les $\langle c^{k_0} \rangle$, où k_0 parcourt les diviseurs positifs de n .

- Étape 3 : On va montrer que $H_d = \{x \in C_n \mid x^d = e\}$

Pour l'inclusion, on remarque que comme $|H_d| = d$, alors $x^d = e$.

Pour l'inclusion réciproque, on prend $x \in C_n$ tel que $x^d = e$. Alors il existe $k \in \mathbb{Z}$, $c^k = x$ et $(c^k)^d = e$.

Alors $n \mid kd$. Donc $qd \mid kd$, où $q = n/d$.

Donc $q \mid k$ et $c^k \in \langle c^q \rangle = H_d$.

- 2) D'après la question précédente, les sous-groupes de C_{15} sont : $H_1 = \{e\}$, $H_3 = \langle c^5 \rangle$, $H_5 = \langle c^3 \rangle$, $H_{15} = C_{15}$.
- 3) Soit $\varphi : G \rightarrow H$. Montrons que $v(\varphi(a)) \mid v(a) \forall a \in G$.
 Soit $k = v(a)$. Alors $a^k = e$.
 Comme φ est un morphisme, alors $\varphi(a^k) = \varphi(a)^k = e$.
 Donc $v(\varphi(a)) \mid k = v(a)$.
- 4) Soit $\varphi : C_{12} \rightarrow C_{15}$ un morphisme non trivial.

$$\forall y \in \text{Im } \varphi, \exists a \in C_{12}, \varphi(a) = y \text{ et } v(y) \mid v(a) \mid 12.$$

Alors $v(y) \mid 12$, mais aussi $v(y) \mid 15$ (car $y \in C_{15}$). Donc $v(y)$ divise le pgcd de 12 et 15, c'est-à-dire 3. Donc $v(y) \in \{1, 3\}$.

Si $v(y) = 3$, $\langle y \rangle \subset C_{15}$ est un sous-groupe d'ordre 3. Donc $\langle y \rangle = \langle c^5 \rangle$.

$$\langle y \rangle = \{e, y, y^2\} = \{e, c^5, c^{10}\}$$

$$\text{Im } \varphi = \langle c^5 \rangle$$

- 5) φ est entièrement déterminé par $\varphi(c)$. En effet, pour tout x de C_{12} , il existe un entier k tel que $x = c^k$. Alors $\varphi(x) = \varphi(c)^k$ est déterminé par $\varphi(c)$.
 Si φ est non trivial, alors $\text{Im } \varphi = \langle c^5 \rangle$, et il n'y a que deux possibilités pour $\varphi(c) \neq e$:

$$\varphi(c) = c^5 \text{ ou } \varphi(c) = c^{10}$$

Donc, en comptant le morphisme trivial, il y a au plus 3 morphismes $\varphi_i : c \mapsto c^{5i}$.

Il reste à montrer que les trois morphismes satisfaisant cette condition existent.

En effet, si la condition est vérifiée, $\forall k \in \mathbf{Z}$, $\varphi_i(c^k) = c^{5ik}$

Pour utiliser la dernière formule comme définition de φ_i , vérifions sa cohérence : $\forall x \in X^{12}$, si $x = c^k = c^l$, alors $c^{5ik} = c^{5il}$.

De plus, $c^k = c^l$ si et seulement si 12 divise $k - l$ donc $c^{5ik}(c^{5il})^{-1} = c^{5i(k-l)} = c^{60im} = e$.

Cela montre l'existence de l'application φ , et il est clair que c'est un morphisme.

- 6) Si $\text{pgcd}(m, n) = 1$, alors le seul morphisme $C_n \rightarrow C_m$ est trivial.
 Soit $d = \text{pgcd}(n, m)$. L'ordre de $\varphi(c)$ divise m et n . Donc :

$$v(\varphi(c)) \mid d \implies \varphi(c) \in H_d = \langle c^{n/d} \rangle = \{y \in C_m \mid y^d = e\}$$

Comme dans la question 5, on montre l'existence et l'unicité de morphisme

$$\varphi_i : C_n \rightarrow C_m, c \mapsto c^{n/d \cdot ik} \quad i = 0, 1, \dots, d-1, k \in \mathbf{Z}$$

— Injectivité :

Si $n \nmid m$, alors $d < n$ et φ ne peut être injectif.

Si $n \mid m$, $d = n$ et $\varphi_i : c^k \mapsto c^{m/n \cdot k}$ est injectif et $\varphi_i(c) = c^{m/n}$ est un générateur de $H_n \subset C_m$.

φ_i est une bijection de $C_n \rightarrow H_n$.

— Si $m \nmid n$, alors le morphisme n'est pas surjectif.

Si $m \mid n$, alors $d = m$ et $H_d = C_m$ est l'image de φ_i .

- 7) On a décrit tous les morphismes $C_n \mapsto C_n$. Il y en a n :
 $\varphi_i : C_n \mapsto C_n$ tels que $\varphi_i(c) = c^i$, $i \in \{0, 1, \dots, n-1\}$. Alors :

$$\begin{aligned} \varphi_i \in \text{Aut}(C_n) &\iff \varphi_i \text{ est surjective.} \\ &\iff c^i \text{ est un générateur de } C_n. \\ &\iff i \in n\mathbb{Z} \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z}. \\ &\iff i \text{ est premier à } n. \end{aligned}$$

Donc, parmi les n morphismes, il y a $\phi(n)$ automorphismes.

Exercice 2.

Considérons

$$\begin{aligned} f : K \times H &\rightarrow KH \\ (k, h) &\mapsto kh \end{aligned}$$

Idée : Montrer que $|f^{-1}(kh)| = |K \cap H|$. Cela entraîne que $|K \times H| = |KH| \cdot |K \cap H|$

$$\begin{aligned} (k_1, h_1) \in f^{-1}(kh) &\iff k_1 h_1 = kh \\ &\iff k^{-1} k_1 = h h_1^{-1} \in K \cap H \end{aligned}$$

Si on note $s = k^{-1} k_1$, on a $k_1 = ks$ et $h_1 = s^{-1} h$. On a donc montré :

$$f^{-1}(kh) = \{(ks, s^{-1}h) \mid s \in K \cap H\}$$

Donc $|f^{-1}(kh)| = |K \cap H|$

Exercice 3. Soit G un groupe d'ordre $|G| > 1$ et p le plus petit diviseur premier de $|G|$.

Pour tout g dans G , $gHg^{-1} < G$ est un sous-groupe distingué de H .

On considère l'action de G sur l'ensemble des sous-groupes de G par *conjugaison*.

On note \mathcal{O}_H l'orbite de H sous cette action. Alors le stabilisateur de H pour cette action n'est autre que le normalisateur.

$$\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$$

Il est évident que $H \triangleleft \mathcal{N}_G(H)$ par définition du normalisateur.

$$|\mathcal{O}_H| = [G : \mathcal{N}_G(H)]$$

Alors,

$$\begin{aligned} H \triangleleft G &\iff \mathcal{O}_H = \{H\} \text{ (ie : } |\mathcal{O}_H| = 1) \\ &\iff G = \mathcal{N}_G(H) \end{aligned}$$

Soit donc $H < G$ d'indice p . Alors $H \triangleleft \mathcal{N}_G(H) < G$.

$$[\mathcal{N}_G(H) : H] \mid [G : H]$$

Donc $[\mathcal{N}_G(H) : H] = 1$ ou p .

Or, $[\mathcal{N}_G(H) : H] = 1$ si et seulement si $\mathcal{N}_G(H) = G$, c'est-à-dire $H \triangleleft G$.

Supposons que $[\mathcal{N}_G(H) : H] = 1$, c'est-à-dire $\mathcal{N}_G(H) = G$.

Dans ce cas, $|\mathcal{O}_H| = p$, ce qui donne un morphisme non-trivial $\varphi : G \rightarrow \mathfrak{S}_p$.

Soit $K = \ker \varphi$. Alors $\text{Im } \varphi \cong G/K$ et $\text{Im } \varphi < \mathfrak{S}_p$.

Donc $|G/K| \mid |\mathfrak{S}_p| = p!$

Or, $|G/K|$ divise aussi $|G|$, et le seul premier commun de $p!$ et $|G|$ est p . Donc $|G/K| = p$.

$$|G/K| = [G : K] = [G/H] = p \quad (1)$$

Et, $\forall h \in H, hHh^{-1} = H$.

$$h \in K \iff hgHg^{-1}h^{-1} = gHg^{-1} \quad \forall g \in G$$

Donc $H \subset K$. Montrons que $K \subset H$.

$$k \in K \iff kgHg^{-1}k^{-1} = gHg^{-1} \quad \forall g \in G$$

En particulier, en prenant $g = 1$, on a : kHk^{-1} . Donc $k \in \mathcal{N}_G(H)$.

Or, $\mathcal{N}_G(H) = H$. Donc $K \subset H$. Par (1), on a alors $K = H$.

Donc $H = \ker \varphi \triangleleft G$, ce qui est absurde. Donc $\mathcal{N}_G(H) \neq H$ par l'absurde.

Cela démontre que $\mathcal{N}_G(H) = G$, c'est-à-dire $H \triangleleft G$.

Exercice 4.

Montrons que si $|G| = p^n$, alors $|\mathcal{Z}_G| = p^r$, $r \neq 0$.

G agit sur lui-même par conjugaison. Cela définit une partition de G en orbites, celles-ci étant les classes de conjugaison.

Les stabilisateurs pour cette action s'appellent *centralisateurs*.

$$C_G(g) = \{x \in G \mid xgx^{-1} = g\}$$

Soient g_1, \dots, g_m les représentants distincts des classes de conjugaison. On a, par la formule des classes :

$$G = \Omega_{g_1} \cup \dots \cup \Omega_{g_m}$$

$$|G| = p^n = |\Omega_{g_1}| + \dots + |\Omega_{g_m}|$$

Et, pour tout g dans G , $|\Omega_g| \mid |G|$, $|C_G(g)| \mid |G|$ et $|\Omega_g| \times |C_G(g)| = |G|$. Comme $|G| = p^n$, il existe m nombres n_i tels que $|C_G(g_i)| = p^{n_i}$ et

$$p^n = p^{n_1} + \dots + p^{n_m}$$

De plus, on a $g_1 = e$, donc $\Omega_{g_1} = \Omega_e = \{e\}$. Donc $n_1 = 0$ et $p^{n_1} = 1$.

Cela entraîne qu'il y a des termes $p^{n_i} = 1$ autre que p^{n_1} . (En effet, dans le cas contraire on aurait $p \mid 1 \nmid$)

$$\forall g \in G, |\Omega_g| = 1 \iff g \in \mathcal{Z}_G$$

Donc $\mathcal{Z}_G \neq \{e\}$, et alors $|\mathcal{Z}_G| = p^r$.

Exercice 5.

Remarque. Tout sous-groupe du centre est distingué.

Raisonnons par l'absurde. Supposons que G/H est cyclique. Alors il existe $c \in G$ tel que $\bar{c} = cH$ est un générateur de G/H . (ie : $G/H = \langle \bar{c} \rangle$)

Montrons que dans ce cas, G est abélien.

En effet, soient $g, g' \in G$ quelconques. Alors :

$$\exists k, k' \in \mathbb{Z}, \bar{g} = \bar{c}^k \text{ et } \bar{g'} = \bar{c}^{k'}$$

Donc il existe $h, h' \in H$ tels que $g = c^k h$ et $g' = c^{k'} h'$.

Mais alors on voit que $gg' = g'g$.

$$gg' = c^k h c^{k'} h' = c^k c^{k'} h h' = c^{k+k'} h' h = c^{k'} c^k h' h = g' g$$

Donc G est abélien, ce qui est absurde.

Exercice 6.

Soit p un nombre premier. Montrons que tout groupe d'ordre p^2 est abélien.

Notons que $|\mathcal{Z}_g| = p$ ou p^2 par l'exercice 4.

Si $|\mathcal{Z}_G| = p^2$, alors $\mathcal{Z}_G = G$ est abélien.

Supposons que $|\mathcal{Z}_G| = p$. Alors $\mathcal{Z}_G \triangleleft G$ et G/\mathcal{Z}_G est un groupe d'ordre p .

Puisque p est premier, G/\mathcal{Z}_G est cyclique, ce qui contredit l'exercice 5.

Exercice 7. $p^k \mid |G|$, p^k est la puissance max de p divisant $|G|$. Par le premier théorème de SYLOW, G admet un sous-groupe K d'ordre p^k . Ainsi $q \mid |G|$, et q est la puissance max de q divisant $|G|$, donc G admet un sous-groupe H d'ordre q . (K est un p -Sylow, H est un q -Sylow).
vérifions les axiomes de produit semi-direct :

— Pour le point (i), deux solutions :

- 1) $K \triangleleft G$ par l'exercice 2. En effet, K est un sous-groupe de G d'ordre q , et q est le plus petit premier divisant $|G| = p^k q$
- 2) Par le deuxième théorème de SYLOW, si on note N_p le nombre de p -Sylows distincts, on a :

$$N_p \equiv 1[p]$$

De plus, par le troisième théorème de SYLOW, tous les p -Sylows sont conjugués entre eux, donc forment une orbite de l'action G par conjugaison, de stabilisateur $\mathcal{N}_G(K) \supset K$, donc

$$N_p = [G : \mathcal{N}_G(K)]$$

Dans notre cas, $[G : K] = q$. Donc

$$N_p \equiv 1[p] \text{ et } N_p \mid q$$

Or, $q < pn$ et si $N_p \neq 1$, alors $N_p = lp + 1$ avec $l > 0$, d'où $N_p \geq p + 1 > q$. Donc N_p ne peut pas être diviseur de q , ce qui est absurde.

Donc $N_p = 1$ et $K \triangleleft G$.

— Montrons que K, H engendrent G .

Remarque. Quelques soient deux sous-groupes K, H d'un groupe G , on a :

- $K \triangleleft G \implies KH = HK$ et $KH < G$
- $KH < G \implies KH = HK$

On a déjà montré que $K \triangleleft G$, donc KH est un groupe, et

$$K < KH < G \implies [KH : K] \mid [K : G] = q \implies [KH : K] = 1 \text{ ou } q$$

Or, $[KH : K] = 1$ si et seulement si $KH = K$, or $KH \neq K$ car $KH \supset H$ a des éléments d'ordre q tandis que l'ordre de chaque élément de K est un diviseur de $p^k = |K|$; donc est une puissance de p .

Donc $KH \neq K$ et $[KH : K] = q = [G : K]$, d'où $G = KH$.

- Montrons que $H \cap K = \{e\}$.

Soit $x \in H \cap K$. On a :

$$v(x) \mid |K| = p^k \quad v(x) \mid |H| = q$$

Donc $v(x) \mid \text{pgcd}(p^k, q) = 1$. Donc $v(x)$ divise 1, c'est-à-dire $x = e$. **Remarque.** On pouvait commencer par démontrer le troisième point et déduire le second en utilisant la formule du produit. (exercice 2).

Exercice 8.

- 1) Table des classes de conjugaison de \mathfrak{S}_4 ($g_i : \text{Cl}_{\mathfrak{S}_4}(g_i)$).

- $g_1 = e$, $|\Omega_{\mathfrak{S}_4}(g_1)| = 1$
- $g_2 = (12)$, $|\Omega_{\mathfrak{S}_4}(g_2)| = 6$
- $g_3 = (12)(34)$, $|\Omega_{\mathfrak{S}_4}(g_3)| = 3$
- $g_4 = (123)$, $|\Omega_{\mathfrak{S}_4}(g_4)| = 8$
- $g_5 = (1234)$, $|\Omega_{\mathfrak{S}_4}(g_5)| = 6$

- 2) Si $N < G$, alors $N \triangleleft G \iff \forall x \in N \forall g \in G, gxg^{-1} \in N \iff \forall x \in N, \text{Cl}_G(x) \in N$.

Donc $N \triangleleft G$ si et seulement si N est réunion de classes de conjugaison dans G .

- 3) La cardinalité d'une réunion de classes de conjugaison parmi $\Omega_{\mathfrak{S}_4}(g_i)$, $i = 1, \dots, 5$ est donnée par

$$n = \delta_1 + 6\delta_2 + 3\delta_3 + 8\delta_4 + 6\delta_5$$

où $\delta_i = 1$ si $\Omega_{\mathfrak{S}_4}(g_i) \subset N$, 0 sinon.

De plus, $e \in N \implies \delta_1 = 1$, et on cherche les autres $\delta_i \in \{0, 1\}$ tels que $n \mid 24$.

- Solutions triviales : $\delta_2 = \delta_3 = \dots = \delta_5 = 0$, alors $n = 1 \mid 24$; $N = \{e\} \triangleleft \mathfrak{S}_4$, et $\delta_2 = \dots = \delta_5 = 1$, alors $n = 24 \mid 24$; $N = \mathfrak{S}_4 \triangleleft \mathfrak{S}_4$.
- Si $\delta_2 \neq 0$, alors $n \geq 1 + 6 = 7$, $n \mid 24 \implies n \in \{8, 12, 24\}$. $n = 24$ est une solution triviale, $n = 8$ est impossible car $\min\{3, 8, 6\} = 3 \neq n - 7 = 1$; pareil pour $n = 12$: $n - 7 = 5$ n'est pas somme de quelques uns des nombres 3, 8, 6. Donc il n'y a pas de solution non triviale avec $\delta_2 = 1$. Par le même raisonnement, $\delta_5 = 1$ est impossible.

- On considère les solutions non triviales avec $\delta_2 = \delta_5 = 0$.
Si $\delta_3 = 1$, on a : $\delta_1 + 3\delta_3 = 1 + 3 = 4 \mid 24$. De plus, $\Omega_{\mathfrak{S}_4}(e) = \Omega_{\mathfrak{S}_4}((12)(34)) = V_4$ est un sous groupe de \mathfrak{S}_4 ,

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft \mathfrak{S}_4$$

(groupe de Klein d'ordre 4).

Si $\delta_4 = 1$, on a : $n \geq 1 + 8 = 9$, donc la seule solution non triviale possible correspond à $n = 12$, et cela donne une unique solution : $\delta_3 = \delta_4 = 1$,

$$N = \{e\} \cup \{(12)(34), (13)(24), (24)(23)\} \cup \{3\text{-cycles}\} = A_4 \triangleleft \mathfrak{S}_4$$

Conclusion : $\{e\}, V_4, A_4, \mathfrak{S}_4$

Exercice 9.

On les énumère suivant l'ordre $d \mid 24$.

- $d = 1$; $\{e\}$, 1 sous-groupe d'ordre 1, $\mathcal{N}_{\mathfrak{S}_4}(\{e\}) = \mathfrak{S}_4$
- $d = 2$;
 - $\langle (ij) \rangle, 1 \leq i < j \leq 4$, 6 sous-groupes engendrés par une transposition, deux à deux conjugués; $\mathcal{N}_{\mathfrak{S}_4}(\langle (12) \rangle) = \langle (12), (34) \rangle$ (on a choisi un représentant)
 - $\langle (ij)(kl) \rangle, \{i, j\} \cap \{k, l\} = \emptyset$, 3 sous-groupes donnant une orbite sous les conjugaisons, $N_G(\langle (12)(34) \rangle) \supset V_4$ car $(12)(34) \in V_4$ et V_4 est commutatif.
On remarque que $(12), (34) \in N_G(\langle (12)(34) \rangle)$. Donc

$$N_G(\langle (12)(34) \rangle) = V_4 \cup \{(12), (34), (13)(24)(12) = (1423), (1324)\}.$$

C'est le groupe diédral \mathcal{D}_8 .

Résumé pour $d = 2$, il y a 2 orbites de conjugaison d'ordre 2, une de longueur 6, l'autre de longueur 3.

- $d = 3$; 4 sous-groupes d'ordre 3, $\langle (ijk) \rangle = \langle (ikj) \rangle$ de normalisateur $S_{\{i,j,k\}} \cong \mathfrak{S}_3$
- $d = 4$;
 - 3 sous-groupes cycliques d'ordre 4, $\langle (1ijk) \rangle = \langle (1kji) \rangle$, $((ijk)$ parcourt les permutations cycliques de $(2,3,4)$). $\mathcal{N}_{\mathfrak{S}_4}(\langle (1ijk) \rangle) = \mathcal{N}_{\mathfrak{S}_4}(\langle (1j)(ik) \rangle) \cong \mathcal{D}_8$ (le premier est contenu dans le second, et les deux sont d'ordre 8 car les orbites respectives sont de longueur 3, donc les deux normalisateurs coïncident)
 - V_4 est distingué, l'orbite est un singleton et son normalisateur est le groupe tout entier, \mathfrak{S}_4 .
 - $H = \{e, (ij), (kl), (ij)(kl)\}$, où $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Il est normalisé par $(13)(24)$ et $(14)(23)$. Donc $|N_G(H)| \geq 6$.
On trouve encore un élément : (1324) , et deux cycles de même longueur sont conjugués, donc $N_G(H) \supset H \cup \{(13)(24), (12)(34), (1324), (1423)\} = K < \mathfrak{S}_4$. $K \cong \mathcal{D}_8$.
De plus, la longueur de l'orbite $\mathcal{O}(H)$ de H divise $|\mathfrak{S}_4|/|\mathcal{N}_{\mathfrak{S}_4}(H)|$ | $|\mathfrak{S}_4|/|K| = 3$.
Il n'y a que deux possibilités pour $|\mathfrak{S}_4|/|\mathcal{N}_{\mathfrak{S}_4}(H)|$: 1 et 3. Or 1 est impossible car H n'est pas parmi les sous-groupes distingués (cf exo 8), donc $|\mathfrak{S}_4|/|\mathcal{N}_{\mathfrak{S}_4}(H)| = 3$ et

$$\mathcal{N}_{\mathfrak{S}_4} = K \cong \mathcal{D}_8.$$

On a trouvé trois types (trois orbites) de sous groupes d'ordre 4. Montrons qu'il n'y en a pas d'autres.

Soit $H < \mathfrak{S}_4$, $|H| = 4$. $\forall g \in H$, $v(g) \mid |H| = 4$, donc $g \in \{1, 2, 4\}$.

Si H contient un élément g d'ordre 4, H est cyclique et g est un des cycles de \mathfrak{S}_4 , donc $H = \langle g \rangle$ est de type 1.

Si H ne contient pas d'élément d'ordre 4, alors $H = \{e, a, b, ab\}$ où $a, b, ab = ba$ sont d'ordre 2. Il y a alors deux sous-cas :

- $H < A_4$ (H ne contient pas de transpositions). Alors $H = V_4$, donc de type 2, parce qu'il n'y a que 3 éléments d'ordre 2 dans \mathfrak{S}_4 qui ne sont pas des transpositions, et donc $\{a, b, ab\}$ coïncide avec l'ensemble de ces 3 éléments d'ordre 2, $\{(12)(34), (13)(24), (14)(23)\}$
- H contient une transposition. Alors H n'est pas contenu dans A_4 et $\ker \epsilon = \pm 1$ est d'ordre 2. Donc H contient 2 transpositions (ie : 2 permutations impaires, toujours d'ordre 2), et une permutation paire : on peut poser $a = (ij)$, $b = (kl)$, $ab = (ij)(kl)$.
De plus, puisque a et b commutent, les supports de (ij) et de (kl) sont disjoints, c'est-à-dire $\{i, j, k, l\} = \{1, 2, 3, 4\}$. Donc H est de type 3.

- $d = 6$; Soit $H < \mathfrak{S}_4$. Comme \mathfrak{S}_4 n'a pas d'éléments d'ordre 6, $H \setminus \{e\}$ est formé d'éléments d'ordre 3 ou 2, il y a au moins un élément d'ordre 3 et au moins un élément d'ordre 2 d'après le lemme de Cauchy.

Les éléments d'ordre 3 de \mathfrak{S}_4 sont les cycles de longueur 3. Donc il existe un cycle $(ijk) \in H$. Quitte à conjuguer H par un élément de \mathfrak{S}_4 , on peut supposer que $(123) \in H$.

Soit $\tau \in H$ un élément d'ordre 2.

- $\tau = (ij)$, $\{i, j\} \subset \{1, 2, 3\}$ donc $H = \langle (123), (ij) \rangle = \mathfrak{S}_3 = S_{\{1,2,3\}} = \text{Stab}_{\mathfrak{S}_4}(4) = \{g \in \mathfrak{S}_4 \mid g(4) = 4\}$
- $\tau = (i4)$ Dans ce cas H contiendrait $\sigma(i4)\sigma^{-1} = (\sigma(i)4)$ et $\sigma^2 = (i4)\sigma^{-2} = (\sigma^2(i)4)$, donc toutes les transpositions $(i4)$, (24) , (34) .
Donc $H \ni (124) = (34)(123)(34)$, c'est-à-dire qu'on a trouvé 7 éléments distincts de H , donc ce cas est impossible.

Remarque : $\langle (132), (i4) \rangle = \mathfrak{S}_4$

- $\tau = (ij)(k4)$ où $\{i, j, k\} = \{1, 2, 3\}$
On voit comme plus haut que $(12)(34)$, $(13)(24)$, $(14)(23) \in H$. Donc $V_4 \subset H$ et $|H|$ est un multiple de 4. Ce qui est absurde car on cherche les sous-groupes d'ordre 6.

On a donc montré que tout sous-groupe d'ordre 6 de \mathfrak{S}_4 est conjugué à $\mathfrak{S}_3 = \text{Stab}_{\mathfrak{S}_4}(4)$. Si on conjugue ce \mathfrak{S}_3 par un $g \in \mathfrak{S}_4$, on aura : $g\text{Stab}_{\mathfrak{S}_4}(4)g^{-1} = \text{Stab}_{\mathfrak{S}_4}(g(4))$.

Or, $g(4)$ peut prendre 4 valeurs : 1, 2, 3, 4. Donc l'orbite de \mathfrak{S}_3 dans \mathfrak{S}_4 est formée de 4 sous-groupes conjugués, $|\mathcal{N}_{\mathfrak{S}_4}(\mathfrak{S}_3)| = 24/4 = 6 = |\mathfrak{S}_3|$

Donc $\mathcal{N}_{\mathfrak{S}_4}(\mathfrak{S}_3) = \mathfrak{S}_3$.

- $d = 8$. On a rencontré des sous-groupes d'ordre 8 : les normalisateurs des sous-groupes d'ordre 4.

Ils sont conjugués au sous-groupe diédral $\mathcal{D}_8 = \langle (1234), (12)(34) \rangle$.

On a donc 3 sous-groupes de cette forme. Y en a-t-il d'autres?

$\mathcal{N}_{\mathfrak{S}_4}(\mathcal{D}_8)$

Les deux sous-groupes de SYLOW de \mathfrak{S}_4 sont tous deux à deux conjugués donc il n'y a qu'une orbite de sous-groupe d'ordre 8, c'est l'ensemble des conjugués de \mathcal{D}_8 .

- $d = 12$; On connaît un sous-groupe d'ordre 12, c'est \mathfrak{A}_4 . Montrons que c'est le seul.
Si $H < \mathfrak{S}_4$ est d'ordre 12, alors H est d'indice 2, donc $H \triangleleft \mathfrak{S}_4$. Or on connaît la liste des sous-groupes distingués de \mathfrak{S}_4 . Il n'y en a qu'un d'ordre 12, c'est \mathfrak{A}_4 et $\mathcal{N}_{\mathfrak{S}_4}(\mathfrak{A}_4) = \mathfrak{S}_4$
- Le seul sous-groupe d'ordre 24 est $\mathfrak{S}_4 = \mathcal{N}_{\mathfrak{S}_4}(\mathfrak{S}_4)$

Exercice 10.

- 1) $|\mathfrak{S}_4| = 24 = 3 \times 2^3$; donc $N_2 = 3$ (cf exo précédent), $N_3 = 4$.
Une façon de voir que $N_2 = 3$ sans référence à l'exercice précédent est d'invoquer le théorème de SYLOW,

$$N_2 \mid |\mathfrak{S}_4|/|H| = 24/8 = 3 \implies N_2 \equiv 1[2]$$

Donc $N_2 \in \{1, 3\}$. Par l'exercice 8, \mathfrak{S}_4 n'a pas de sous-groupes distingués d'ordre 8. Donc $N \neq 1$ et $N_2 = 3$.

- 2) $|\mathfrak{A}_4| = 12 = 2^2 \times 3$. Par l'exercice 8, $V_4 \triangleleft \mathfrak{A}_4$. Donc \mathfrak{A}_4 n'a qu'un seul 2-Sylow qui est V_4 , et $N_2 = 1$. Tous les sous-groupes d'ordre 3 de \mathfrak{S}_4 sont contenus dans \mathfrak{A}_4 , donc le nombre de 3-Sylows pour \mathfrak{A}_4 est le même que pour \mathfrak{S}_4 : $N_3 = 4$.
- 3) $|\mathfrak{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$ donc $n_2 \equiv 1[2]$, $N_2 \mid 15 \implies N_2 \in \{1, 3, 5, 15\}$.
De plus $N_2 \geq 3$ car $\mathfrak{S}_4 \subset \mathfrak{S}_5$, et on a trouvé 3 sous-groupes d'ordre 8 dans \mathfrak{S}_4 .
De plus, on a 5 façons de plonger \mathfrak{S}_4 dans \mathfrak{S}_5 :

$$\psi_i : \mathfrak{S}_4 \cong \mathfrak{S}_{\{1,2,3,4,5\} \setminus \{i\}} = \text{Stab}_{\mathfrak{S}_5}(i)$$

Chacune des 5 images $\psi_i(\mathfrak{S}_4)$, contient 3 2-Sylow, donc \mathfrak{S}_5 en contient 15.

On a montré que $N_2 = 15$.

$$N_3 = \frac{|\{\text{cycles de longueur 3}\}|}{2}$$

Et $|\{(ijk) \in \mathfrak{S}_5\}| = \binom{5}{3} \times \frac{3!}{3}$ (le coefficient binomial représente le choix du support $\{i, j, k\} \subset \{1, 2, 3, 4, 5\}$ du cycle).

Donc $N_3 = 10$.

$$N_5 = \frac{|\{\text{cycles de longueur 5}\}|}{4} = \frac{5!}{5 \times 4} = 6$$

(5 façons d'écrire un 5-cycle)

- 4) $|\mathfrak{A}_5| = 60 = 2^2 \cdot 3 \cdot 5$.
 $N_3 = 10, N_5 = 6$, car les sous-groupes de \mathfrak{S}_5 d'ordre 3 ou 5 sont automatiquement sous-groupes de \mathfrak{A}_5 .
On a : $N_2 \equiv 1[2]$, $N_2 \mid 15$ donc $N_2 \in \{1, 3, 5, 15\}$

Remarque : Si on utilise le résultat de l'exercice 13, la simplicité de \mathfrak{A}_5 , on a le raisonnement suivant :

- $N_2 \neq 1$ car si $N_2 = 1$, alors un 2-Sylow est distingué, mais par la simplicité de \mathfrak{A}_5 , il est soit $\{e\}$ soit \mathfrak{A}_5 .

- $N_2 \neq 3$, car si $N_2 = 3$, l'action de \mathfrak{A}_5 sur les 2-Sylows définit un morphisme $\mathfrak{A}_5 \rightarrow \mathfrak{S}_3$ non-trivial. Donc son noyau $\ker \varphi \triangleleft \mathfrak{A}_5$ est non trivial. (ie : est propre)

$$1 < |\operatorname{Im} \varphi| = |\mathfrak{A}_5|/|\ker \varphi| = 60/|\ker \varphi| \leq 6 = |\mathfrak{S}_3|$$

$$1 < 60/|\ker \varphi| \leq 6 \iff 10 \leq |\ker \varphi| < 60$$

Cela contredit la simplicité. Donc $N_2 \neq 3$.

- $N_2 \neq 15$. En effet, soit H un 2-Sylow. Alors $N_2 = 15 \iff \mathcal{N}_{\mathfrak{A}_5}(H) = H$.
On a $V_4 \subset \mathfrak{A}_4 \subset \mathfrak{A}_5$ et on sait que tous les 2-Sylow sont conjugués; donc ils sont conjugués à V_4 , on peut donc poser $H = V_4$.
A-t-on $\mathcal{N}_{\mathfrak{A}_5}(V_4) = V_4$? Non car $V_4 \triangleleft \mathfrak{A}_\Delta$, donc $\mathcal{N}_{\mathfrak{A}_5}(V_4)$ contient au moins \mathfrak{A}_4 .
Et $\mathcal{N}_{\mathfrak{A}_5}(V_4) > \mathfrak{A}_4 \implies 12 \mid |\mathcal{N}_{\mathfrak{A}_5}(V_4)| \implies N_2 \mid 5 = 60/|\mathfrak{A}_4| \implies N_2 \neq 15$

Conclusion : $N_2 = 5$

Si on ne se sert pas de la simplicité de \mathfrak{A}_5 , on devrait simplement éliminer les cas $N_2 = 1$ et $N_2 = 3$ par un autre raisonnement. On peut le faire comme suit : on connaît un 2-Sylow, qui est $V_4 \subset \mathfrak{A}_4 \subset \mathfrak{A}_5$. En prenant 5 plongements différents $\varphi_i : \mathfrak{S}_4 \rightarrow \mathfrak{S}_5$, on a 5 sous-groupes différents $\varphi_i(\mathfrak{A}_4)$ d'ordre 4, donc $N_2 \geq 5$ et on montre ensuite que $N_2 \neq 15$ comme dans le 3ème point au dessus.

Exercice 11. On a $p!$ permutations de $(1, 2, \dots, p)$, donc $p!/p$ cycles distincts de longueur p . Chaque sous-groupe d'ordre p contient $p-1$ cycles de longueur p , et deux sous-groupes distincts d'ordre p s'intersectent par $\{e\}$, donc $N_p = p!/p(p-1) = (p-2)!$

Remarque : Le 2ème théorème de Sylow nous dit que $N_p \equiv 1[p]$, donc on a démontré :

$$(p-2)! \equiv 1[p]$$

cf Théorème de Wilson.

Exercice 12. G est produit semi-direct de ses sous-groupes $K, H \iff K \triangleleft G, KH = G, K \cap H = \{e\}$.

- $G = \mathfrak{S}_3$; $\mathfrak{A}_3 \triangleleft \mathfrak{S}_3$, $\langle (ij) \rangle = H$, $\mathfrak{S}_3 = \mathfrak{A}_3 \rtimes H$
- $G = \mathfrak{A}_4$; le seul sous groupe distingué est V_4 , pour H on peut choisir n'importe quel sous-groupe d'ordre 3, $H = \langle (ijk) \rangle$, alors $\mathfrak{A}_4 = V_4 \rtimes H$.
Pour visualiser un peu mieux, on peut considérer $V_4 \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, $H \cong \mathbf{Z}/3\mathbf{Z}$.
- $G = \mathfrak{S}_4$; $\mathfrak{S}_4 = V_4 \rtimes \mathfrak{S}_3 = \mathfrak{A}_4 \rtimes H$, où $H = \langle (12) \rangle$.
Donc deux paires (K, H) de groupes à isomorphisme près : $(\mathfrak{A}_4, \mathbf{Z}/2\mathbf{Z})$ et $(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}, \mathfrak{S}_4)$
- $G = \mathcal{D}_8$; quels sont les sous-groupes distingués de \mathcal{D}_8 ?

$$\mathcal{D}_8 = \{e, \sigma, \sigma^2, \sigma^3, \tau, \tau\sigma, \tau\sigma^2, \tau\sigma^3\}$$

On remarque que $\mathcal{Z}(\mathcal{D}_8) = \{e, \sigma^2\} \triangleleft \mathcal{D}_8$ et il n'y a aucun autre sous-groupe d'ordre 2 distingué.

Les sous-groupes d'ordre 4 (tous distingués) :

- $\langle \sigma \rangle \cong \mathbf{Z}/4\mathbf{Z}$, cyclique

$$— \langle \tau, \sigma^2 \rangle, \langle \tau\sigma, \sigma^2 \rangle \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$$

Existe-t-il un sous-groupe $H < \mathcal{D}_8$ complémentaire à $\mathcal{Z}(\mathcal{D}_8)$? (c'est-à-dire tel que \mathcal{D}_8 est produit semi direct de $\mathcal{Z}(\mathcal{D}_8)$ et H)

Pour un tel H , on aurait $|H| = 4$, $H \cap \mathcal{Z}(\mathcal{D}_8) = \{e\}$. Or c'est impossible car tous les sous-groupes d'ordre 4 contiennent $\mathcal{Z}(\mathcal{D}_8)$.

Donc il n'existe pas de représentation de \mathcal{D}_8 comme produit semi-direct de $\mathcal{Z}(\mathcal{D}_8)$ et d'un sous-groupe d'ordre 4.

Pour $K' = \langle \tau, \sigma^2 \rangle$, il existe des sous-groupes d'ordre 2 complémentaires : $H' = \langle \tau\sigma \rangle$ ou $H' = \langle \tau\sigma^3 \rangle$.

Donc $\mathcal{D}_8 \cong (\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \rtimes \mathbf{Z}/2\mathbf{Z}$.

Pareil pour $K' = \langle \tau\sigma, \sigma^2 \rangle$ et $H' = \langle \tau \rangle$ ou $H' = \langle \tau\sigma^2 \rangle$.

Pour $K' = \langle \sigma \rangle$, on a 4 choix possibles pour H' , $H' = \langle \tau \rangle$ ou $\langle \tau\sigma \rangle$ ou $\langle \tau\sigma^2 \rangle$ ou $\langle \tau\sigma^3 \rangle$. On obtient une représentation :

$$\mathcal{D}_8 = \mathbf{Z}/4\mathbf{Z} \rtimes \mathbf{Z}/2\mathbf{Z}$$

$$— G = \mathcal{Q}_8$$

$$\mathcal{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$$

avec $i^2 = j^2 = k^2 = -1$ et $ij = -ji = k, jk = -kj = i, ki = -ik = j$. Dans ce cas :

$$\mathcal{Z}(\mathcal{Q}_8) = \{\pm 1\}$$

Et -1 est le seul élément d'ordre 2 de \mathcal{Q}_8 , tous les 6 éléments de $\mathcal{Q}_8 \setminus \mathcal{Z}(\mathcal{Q}_8)$ sont d'ordre 4.

Donc les sous-groupes propres de \mathcal{Q}_8 sont :

$$— \langle -1 \rangle \text{ d'ordre 2}$$

$$— \langle i \rangle = \langle -i \rangle, \langle j \rangle = \langle -j \rangle, \langle k \rangle = \langle -k \rangle \text{ d'ordres 4}$$

Tous les sous-groupes sont distingués. Mais aucun n'a de sous-groupe complémentaire. En effet, deux sous groupes contiennent toujours -1 , donc ont une intersection non triviale. Donc \mathcal{Q}_8 admet 4 sous-groupes distingués propres, mais aucun ne donne de produit semi-directe. En effet on a la suite exacte

$$1 \longrightarrow C_4 \longrightarrow \mathcal{Q}_8 \overset{s}{\longrightarrow} C_2 \longrightarrow 1$$

Cette suite n'est pas scindée. (pour une section s on aurait $gs = \text{Id}_{C_2}$ et donc l'image du générateur c_2 de C_2 par s serait un élément d'ordre 2, mais il n'y a pas d'éléments d'ordre 2 parmi les antécédents de c_2 : $g^{-1}(c_2) = \{\pm j, \pm k\}$ d'ordre 4)

Exercice 13.

1) Établissons une liste des classes de conjugaison pour \mathfrak{S}_5 :

$$— g_1 = e, |\Omega_{\mathfrak{S}_5}(g_1)| = 1$$

$$— g_2 = (12), |\Omega_{\mathfrak{S}_5}(g_2)| = 10$$

$$— g_3 = (123), |\Omega_{\mathfrak{S}_5}(g_3)| = 20$$

$$— g_4 = (12)(34), |\Omega_{\mathfrak{S}_5}(g_4)| = 15$$

- $g_5 = (1234), |\Omega_{\mathfrak{S}_5}(g_5)| = 30$
- $g_6 = (12345), |\Omega_{\mathfrak{S}_5}(g_6)| = 24$
- $g_7 = (123)(45), |\Omega_{\mathfrak{S}_5}(g_6)| = 20$

2) On fait pareil pour \mathfrak{A}_5 :

- $g_1 = e, |\Omega_{\mathfrak{S}_5}(g_1)| = 1$
- $g_2 = (12)(34), |\Omega_{\mathfrak{S}_5}(g_2)| = 15$
- $g_3 = (123), |\Omega_{\mathfrak{S}_5}(g_3)| = 20$
- $g_4 = (12345), |\Omega_{\mathfrak{S}_5}(g_4)| = 12$
- $g_5 = (15432), |\Omega_{\mathfrak{S}_5}(g_5)| = 12$

Remarque.

$|\Omega_{\mathfrak{S}_n}(\sigma)| = \frac{|\mathfrak{S}_n|}{|C_{\mathfrak{S}_n}(\sigma)|}$ avec $C_{\mathfrak{S}_n}(\sigma) = \{g \in \mathfrak{S}_n \mid g\sigma g^{-1} = \sigma\}$ le centralisateur de σ .

Si σ est produit de r_1 cycles de longueur l_1, \dots, r_s cycles de longueur l_s à support indépendant, $l_1 > l_2 > \dots > l_s \geq 1$, alors

$$|C_{\mathfrak{S}_n}(\sigma)| = l_1^{r_1} r_1! \dots l_s^{r_s} r_s!$$

Donc

$$|\Omega_{\mathfrak{S}_n}(\sigma)| = \frac{n!}{l_1^{r_1} r_1! \dots l_s^{r_s} r_s!}$$

Lorsqu'on passe à \mathfrak{A}_n , on a une dichotomie :

a) $C_{\mathfrak{S}_n}(\sigma) \subset \mathfrak{A}_n \implies C_{\mathfrak{S}_n}(\sigma) = C_{\mathfrak{A}_n}(\sigma)$ et

$$|\Omega_{\mathfrak{A}_n}(\sigma)| = \frac{|\mathfrak{A}_n|}{|C_{\mathfrak{A}_n}(\sigma)|} = \frac{1}{2} |\Omega_{\mathfrak{S}_n}(\sigma)|$$

b) $C_{\mathfrak{S}_n}(\sigma) \not\subset \mathfrak{A}_n \implies C_{\mathfrak{A}_n}(\sigma) = C_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n$ est d'ordre $\frac{1}{2} |C_{\mathfrak{S}_n}(\sigma)|$, ce qu'on déduit en observant le morphisme

$$C_{\mathfrak{S}_n} \hookrightarrow \mathfrak{S}_n \rightarrow \mathfrak{S}_n / \mathfrak{A}_n \cong C_2$$

Il est surjectif, donc son noyau $C_{\mathfrak{S}_n}(\sigma) \cap \mathfrak{A}_n$ est d'ordre égal à la moitié de $|C_{\mathfrak{S}_n}(\sigma)|$.

Dans ce cas :

$$|\Omega_{\mathfrak{A}_n}(\sigma)| = \frac{|\mathfrak{A}_n|}{|C_{\mathfrak{A}_n}(\sigma)|} = \frac{1/2 |\mathfrak{S}_n|}{1/2 |C_{\mathfrak{S}_n}(\sigma)|} = |\Omega_{\mathfrak{S}_n}(\sigma)|$$

Exercice 14.

Soit G un groupe simple d'ordre 60.

- 1) Soit N_5 le nombre de 5-Sylow de G .

Par les théorèmes de SYLOW, $N_5 \mid 60/5 = 12$ et $N_5 \equiv 1[5]$ donc $N_5 \in \{1, 6\}$. Mais $N_5 \neq 1$ puisque G est simple et si N_5 était 1, le 5-Sylow serait distingué. Donc $N_5 = 6$.

L'action de G par conjugaison sur les six 5-Sylow définit un morphisme

$$\varphi : G \mapsto \mathfrak{S}_6.$$

Il est non trivial car les 5-Sylow sont deux à deux conjugués, donc $\varphi(G)$ opère transitivement sur $\{1, 2, 3, 4, 5, 6\}$ et ne se réduit pas à l'identité. (ie : élément neutre)

Le noyau $\ker \varphi$ est un sous-groupe distingué. Puisque G est simple, $\ker \varphi = \{e\}$ ou G . Or φ est non-trivial, donc $\ker \varphi \neq G$, donc $\ker \varphi = \{e\}$, donc φ est injectif. Supposons que $\varphi(G) \not\subset \mathfrak{A}_6$. Alors la composée

$$G \mapsto \mathfrak{S}_6 \mapsto \mathfrak{S}_6/\mathfrak{A}_6$$

est surjective et son noyau est un sous-groupe distingué d'ordre 30 de G , ce qui est absurde car G est simple.

Donc $\varphi(G) \subset \mathfrak{A}_6$ et

$$|\varphi(G)| = |G| = 60, |\mathfrak{A}_6| = 360 \implies \varphi(G) \text{ est d'indice 6 dans } \mathfrak{A}_6$$

- 2) Soit $H < \mathfrak{A}_6$ d'indice 6. Montrons qu'il existe $\varphi : \mathfrak{A}_6 \mapsto \mathfrak{S}_6$ tel que

$$\varphi(H) = \mathfrak{S}_6 = \mathfrak{A}_5 \subset \mathfrak{S}_5 = \text{Stab}_{\mathfrak{S}_6}(6).$$

Soient g_1H, \dots, g_6H les 6 classes à gauche de \mathfrak{A}_6 mod H . Le groupe G opère par translations à gauche sur l'ensemble $\{g_1H, \dots, g_6H\}$.

Donc on a un morphisme $\varphi : \mathfrak{A}_6 \mapsto \mathfrak{S}_6$.

$$\varphi(g) : \begin{cases} g_1H \mapsto g g_1H = g_{i_1}H \\ \vdots \\ g_6H \mapsto g g_6H = g_{i_6}H \end{cases}$$

$$\varphi_0(g) = (i_1, \dots, i_6)$$

φ est non trivial car l'action de \mathfrak{A}_6 sur \mathfrak{A}_6/H est transitive.

On peut supposer que $g_6 = e$, $g_6H = H$, alors $H = g_6H$ est stabilisé par H et donc $\varphi_0(H) \subset \mathfrak{S}_5 = \text{Stab}_{\mathfrak{S}_6}(6)$

Montrons que φ_0 est injectif. Cela suit facilement de la simplicité de \mathfrak{A}_6 :

φ_0 est non trivial, donc $\ker \varphi_0 \neq \mathfrak{A}_6$ et donc $\ker \varphi_0 = \{e\}$.

Donc $\varphi_0(H)$ est un sous-groupe d'ordre 60 de \mathfrak{S}_5 . Il est facile de voir que $\varphi_0(H) \subset \mathfrak{A}_5$. En effet, dans le cas contraire, le morphisme $\alpha : \varphi_0(H) \mapsto \mathfrak{S}_6/\mathfrak{A}_5$ nous donnerait un sous-groupe distingué $\ker \alpha = \varphi_0(H) \cap \mathfrak{A}_5 \triangleleft \mathfrak{A}_5$ en tant que sous-groupe d'indice 2, or \mathfrak{A}_5 est simple. \nexists

Donc $\varphi_0(H) = \mathfrak{A}_5$.

3) Puisque $H \cong \varphi_0(H)$, on a démontré que $H \cong \mathfrak{A}_5$.

Exercice 15.

Ordre	Groupe
1	$\{e\}$
2	C_2
3	C_3
4	$C_4, C_2 \times C_2$
5	C_5
6	C_6, \mathfrak{S}_3
7	C_7
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2$
9	$C_9, C_3 \times C_3$
10	C_{10}, \mathcal{D}_{10}
11	C_{11}
12	$C_{12}, C_6 \times C_2, \mathfrak{A}_4, \mathcal{D}_{12}, C_3 \rtimes C_4$
13	C_{13}
14	C_{14}, \mathcal{D}_{14}
15	C_{15}

1) Pour les groupes d'ordre p premier, il n'y a qu'une classe d'isomorphisme pour chaque p , le groupe cyclique C_p .

2) Pour les groupes d'ordre p^2 , il y a cette fois-ci deux classes, C_{p^2} et $C_p \times C_p$.

3) Les groupes d'ordre p, q , $p > q$ premiers. D'après le cours (ou bien l'exo 7 avec $k = 1$), $G \cong C_p \rtimes_{\varphi} C_q$ pour un morphisme $\varphi : C_q \rightarrow \text{Aut}(C_p) \cong C_{p-1}$.

Conclusion 1 : Si $q \nmid p-1$, le seul morphisme $\varphi : C_p \rightarrow C_{p-1}$ est le morphisme trivial, donc dans ce cas $C_p \cong C_p \times C_q \cong C_{pq}$. Cela donne la réponse $G \cong C_{15}$ pour l'ordre 15.

Supposons que $q \mid p-1$. Alors il y a $q-1$ morphismes non triviaux $\varphi_i : C_q \rightarrow C_{p-1}$.

Si on note un générateur de C_n par c_n , on peut écrire

$$\varphi_i(c_q) = c_{p-1}^{\frac{p-1}{q}i}, \quad i = 1, \dots, q-1$$

Ces $q-1$ morphismes différents définissent en fait des produits semi-directs isomorphisme. L'application

$$\begin{aligned} \psi_i : C_p \rtimes_{\varphi_i} C_q &\rightarrow C_p \rtimes_{\varphi_1} C_q \\ (x, y) &\mapsto (x, y^i) \end{aligned}$$

est un isomorphisme de groupe.

Vérification :

$\text{Aut}(C_p) \cong (\mathbf{Z}/p\mathbf{Z})^{\times} \cong \langle [h_0] \rangle \cong C_{p-1}$; le générateur $c_{p-1} = [h_0]$ agit par $x \rightarrow x^{h_0}$ ($x \in C_p$).

Alors $c_{p-1}^{\frac{p-1}{q}}$ agit par $x \longrightarrow x^{n_1}$, où $n_1 = n_0^{\frac{p-1}{q}}$. Donc :

$$\varphi_1(c_q) : C_p \longrightarrow C_p, x \longrightarrow x^{n_1}$$

$$\varphi_i(c_q) : C_p \longrightarrow C_p, x \longrightarrow x^{n_1} \quad (i = 1, \dots, q-1)$$

$$(x, y) *_i (x', y') = (x\varphi_i(y)(x'), yy') = (xx'^{h_1^{ij}}, yy')$$

Où on a posé $y = c_q^j$;

$$\psi_i((x, y)) *_1 \psi_i((x', y')) = (x, y^i) *_1 (x', y'^i) = (xx'^{h_1^{ij}}, y^i y'^i) = \psi_i((x, y) *_i (x', y'))$$

La bijectivité de ψ_i suit de la bijectivité de $C_q \longrightarrow C_q, y \longrightarrow y^i$ pour chaque $i = 1, \dots, q-1$. On obtient :

Conclusion 2 : Lorsque $q \mid p-1$, il y a précisément deux classe d'isomorphisme des groupes $pq : C_p \times C_q = C_{pq}$ et un produit semi-direct $C_p \rtimes_{\varphi} C_q$ non trivial (pour un morphisme $\varphi : C_q \rightarrow C_{p-1}$ quelconque)

Exemple : $p = 7, q = 3$

$$(\mathbf{Z}/7\mathbf{Z})^{\times} = \langle 3 \rangle, [3] : C_7 \longrightarrow C_7, x \longrightarrow x^3$$

L'automorphisme $[3]$ est un élément d'ordre $6 = p-1$ de $\text{Aut}(C_7) \cong C_6$ (on le notait par $[n_0]$ et C_{p-1})

Pour un produit semi-direct $C_7 \rtimes_{\varphi} C_3$, il nous faut envoyer le gnérateur c_3 de C_3 sur un élément d'ordre 3 de $\text{Aut}(C_7)$. Les deux éléments d'ordre 3 sont $[3^2] = [9] = [2]$ (on calcule modulo $p = 7$) et $[3^4] = [2^2] = [4]$.

Voilà donc les deux morphismes non triviaux

$$\varphi_1 : c_3^j \longrightarrow [x \mapsto x^{2^j}]$$

$$\varphi_2 : c_3^j \longrightarrow [x \mapsto x^{4^j}]$$

Les deux groupes d'ordre 21 à isomorphisme près sont :

$$— C_7 \times C_3 \cong C_{21} \text{ et}$$

$$— C_7 \rtimes_{\varphi_1} C_3 = \langle \sigma, \tau \mid \sigma^7 = \tau^3 = e, \tau\sigma\tau^{-1} = \sigma^4 \rangle \text{ est isomorphe à celui du point 2.}$$

Remarque : Le groupe $C_7 \rtimes_{\varphi_2} C_3 = \langle \sigma, \tau \mid \sigma^7 = \tau^3 = e, \tau\sigma\tau^{-1} = \sigma^2 \rangle$

4) Groupes non-abéliens d'ordre 8 :

Soit G un groupe d'ordre 8, pour tout $g \in G \setminus \{e\}$, $v(g) \in \{2, 4, 8\}$.

S'il existe g d'ordre 8, alors $G = \langle g \rangle$ est abélien, ce qui n'est pas le cas.

Si tous les éléments de $G \setminus \{e\}$ sont d'ordre 2, G est abélien, en effet,

$$\forall a, b \in G \quad a^2 = b^2 = (ab)^2 = e \implies ab = ba$$

Donc G contient un élément d'ordre 4. Choisissons un tel élément et notons le σ .

— *Premier cas* : $G \setminus \langle \sigma \rangle$ contient un élément τ d'ordre 2.

Alors $\langle \sigma \rangle \cap \langle \tau \rangle = \{e\}$, $\langle \sigma \rangle \triangleleft G$ (car d'indice 2), $|\langle \sigma \rangle \langle \tau \rangle| = |\sigma| |\tau|$, car $\langle \sigma \rangle \cap \langle \tau \rangle = e$, donc $|\langle \sigma \rangle \langle \tau \rangle| = 8$ et $\langle \sigma \rangle \langle \tau \rangle = G$, donc G est produit semi direct de $\langle \sigma \rangle$ et $\langle \tau \rangle$:

$$G \cong C_4 \rtimes_{\varphi} C_2$$

Où $\varphi : C_2 \rightarrow \text{Aut}(C_4)$ est un morphisme de groupe. On a :

$$\text{Aut}(C_4) = \{c_4^j \mapsto c_4^j (= id_{C_4}) \quad c_4^j \mapsto c_4^{-j} = c_4^{3j}\} \cong C_2$$

Il y a un unique morphisme non trivial $C_2 \rightarrow C_2$ donc il y a un unique produit semi direct non abélien. C'est le groupe \mathcal{D}_8 .

— *Second cas* : Tous les éléments de $G \setminus \{\sigma\}$ sont d'ordre 4.

$$G = \{e, \sigma, \sigma^2, \sigma^3, \tau_1, \tau_1^{-1}, \tau_2, \tau_2^{-1}\}$$

où les τ_i sont d'ordre 4, et σ^2 est l'unique élément d'ordre 2. On a $\tau_1^2 = \tau_2^2 \sigma^2$.

G est engendré par σ et τ_1 . $\tau_1 \sigma \tau_1^{-1}$ est un élément d'ordre 4, $\langle \sigma \rangle$ est distingué, (car d'indice 2), donc $\tau_1 \sigma \tau_1^{-1} = \sigma$ ou σ^{-1} .

Si $\tau_1 \sigma \tau_1^{-1} = \sigma$, G est abélien, ce qui n'est pas le cas, donc on a

$$\tau_1 \sigma \tau_1^{-1} = \sigma^{-1}$$

$$(\tau_1 \sigma = \sigma^{-1} \tau_1 = \sigma^3 \tau)$$

$$G = \{e, \sigma, \sigma^2, \sigma^3, \tau_1, \sigma \tau_1, \sigma^2 \tau_1, \sigma^3 \tau_1\}$$

Les relations $\sigma^4 = \tau_1^4 = e$, $\sigma^2 = \tau_1^2$, $\tau_1 \sigma = \sigma^{-1} \tau$ déterminent complètement la table de multiplication de G .

Un tel groupe existe, c'est le groupe des quaternions.

5) Groupes non abéliens d'ordre 12

Soit G un groupe non abélien d'ordre $12 = 2^2 \cdot 3$.

Soient H_4, H_3 ses sous-groupes de SYLOW. On a $H_4 \cap H_3 = \{e\}$, donc $|H_4 \cdot H_3| = 12$ et $H_4 H_3 = G$.

— *Premier cas* : $H_4 \triangleleft G$. Si $H_4 \cong C_4$, $\text{Aut}(H_4) \cong (\mathbf{Z}/4\mathbf{Z})^\times \cong \mathbf{Z}/2\mathbf{Z}$, et tout morphisme $C_3 \rightarrow \text{Aut}(H_4)$ est trivial. Donc G est commutatif, ce qui est absurde. Donc H_4 n'est pas cyclique et $H_4 \cong C_2 \times C_2$. Dans ce cas, $\text{Aut}(H_4) \cong \mathfrak{S}_3$, agissant par permutations des trois éléments d'ordre 2.

$$G \cong (C_2 \times C_2) \rtimes_{\varphi} C_3 \quad \varphi : \begin{cases} e \mapsto e \\ a_1 \mapsto a_2 \\ a_2 \mapsto a_3 \\ a_3 \mapsto a_1 \end{cases}$$

$$C_2 \times C_2 = \{e, a_1, a_2, a_3\} \quad a_3 = a_1 a_2 \quad a_2 = a_3 a_1 \quad a_1 = a_2 a_3$$

Ce G est isomorphe à \mathcal{A}_1 :

$$\begin{aligned}(C_2 \times C_2) \rtimes_{\varphi} C_3 &\longrightarrow \mathcal{A}_4 \\ a_1 = (c_2, e, e) &\longrightarrow (12)(34) \\ a_2 = (e, c_2, e) &\longrightarrow (23)(24) \\ a_3 = (c_2, c_2, e) &\longrightarrow (14)(23) \\ (e, e, c_3) &\longrightarrow (132)\end{aligned}$$

— *Second cas* : $H_4 \not\triangleleft G$, $H_3 \triangleleft G$

— Si $H_4 \cong C_4$, $G \cong C_3 \rtimes_{\varphi} C_4$; avec $\varphi : c_4 \longrightarrow [c_3 \longrightarrow c_3^{-1}]$, le seul élément d'ordre non trivial de $\text{Aut}(C_4) \cong C_2$.

— Si $H_4 \cong C_2 \times C_2$, $G \cong C_3 \rtimes_{\varphi} (C_2 \times C_2)$, $\varphi : C_2 \times C_2 \longrightarrow \text{Aut}(C_3) \cong C_2 = \langle x \rangle, x^2 = e, x : c_3 \longrightarrow c_3^{-1}$.

φ est non trivial, donc injectif donc est déterminé par son noyau, il y a trois morphismes différents :

$$\varphi_1 : \begin{cases} c_2 \longrightarrow x \\ c'_2 \longrightarrow x \\ c_2 c'_2 \longrightarrow e \end{cases}$$

$$\varphi_2 : \begin{cases} c_2 \longrightarrow x \\ c'_2 \longrightarrow e \\ c_2 c'_2 \longrightarrow x \end{cases}$$

$$\varphi_3 : \begin{cases} c_2 \longrightarrow e \\ c'_2 \longrightarrow x \\ c_2 c'_2 \longrightarrow x \end{cases}$$

Ces morphismes sont équivalents par les changement de générateurs c_2, c'_2 de $C_2 \times C'_2$, donc il y a un unique produit semi-direct à isomorphisme près

$$G \cong C_3 \rtimes_{\varphi_3} (C_2 \times C_2) \cong (C_3 \times C_2) \rtimes C_2 \cong C_6 \rtimes C_2 \cong \mathcal{D}_{12}$$

Remarques :

— $K \rtimes_{\varphi \circ \psi} H \cong K \rtimes_{\varphi} H$ ($k, h \longrightarrow (k, \psi(h))$) Pour tout ψ automorphisme de H .

On l'a appliqué pour $K = C_p, H = C_q$.

— Tout automorphisme de K "changement de générateur" induit aussi un isomorphisme de produit semi direct respectifs

$$f \in \text{Aut}(K), \hat{f} \in \text{Aut}(\text{Aut}K), \hat{f} : g \longrightarrow f \circ g \circ f^{-1}$$

$$K \rtimes_{\varphi} H \cong K \rtimes_{\hat{f} \circ \varphi} H$$

Exercice 16.

$$|G| = 750 = 5^3 \cdot 2 \cdot 3$$

$N_5 \mid 6$, $N_5 \equiv 1[5]$, donc si G est simple, $N_5 = 6$, l'action de G sur les six 5-Sylows donne un morphisme non-trivial (car transitif) :

$$\varphi : G \longrightarrow S_6, \quad e < \varphi(G) < S_6$$

$$|\varphi(G)| < |S_6| = 6! = 720 < |G| = 750$$

donc φ est non injectif, donc le noyau est un sous groupe propre de G , et il est distingué, ce qui est absurde.

Exercice 17.

$$|G| = 45 = 3^2 \cdot 5$$

$N_3 \equiv 1[3]$, $N_3 \mid 5$ donc $N_3 = 1$. Donc H_9 , le 3 sylow est distingué et $G \cong H_9 \rtimes C_5$.

— Premier cas : $H_9 \cong C_9$, $\text{Aut}(C_9) \cong C_6$

Alors il n'existe pas de morphisme non trivial $C_5 \hookrightarrow C_6$ donc $H_9 \times C_5$ commutatif.

— Second cas : $H_9 \cong C_3 \times C_3$ et $\text{Aut}(C_9) \cong \text{Aut}(C_3 \times C_3)$.

Alors $|\text{Aut}(C_3 \times C_3)| = 8 \cdot 6 = 48$, donc il n'existe pas de morphisme non trivial $C_5 \hookrightarrow \text{Aut} C_3 \times C_3$ et on a la même conclusion.

Exercice 18.

1) Le cas $|G| = p^3 q$

Le cas où $p > q$ suit de l'exercice 7. ($G = H_{p^3} \rtimes H_q$)

Il reste à traiter le cas où $p < q$.

On suppose G simple, donc les Sylows de G ne sont pas distingués, et $N_p > 1$, $N_q > 1$.

On a $N_q \mid q$, $n_p \neq 1$, donc $N_p = q$.

De plus, $n_p \equiv 1[p]$, donc p divise $q - 1$. Puis, N_q divisant p^3 , on a que $N_q \in \{p, p^2, p^3\}$.

Si $N_q = p^3$, G contient $N_q(q - 1) = p^3(q - 1)$ éléments d'ordre q est les p^3 éléments restants ne peuvent former qu'un seul p -Sylow H_{p^3} donc H_{p^3} serait distingué dans G , $\frac{1}{2}$.

Donc $N_q \neq p^3$. Puis $N_q \equiv 1[q]$ donc $N_q \geq q + 1 > p$, et $n_q \neq p$, donc $N_q = p^2$ et q divise $p^2 - 1 = (p - 1)(p + 1)$, d'où q divise $p - 1$ ou $p + 1$. Or, $q > p$, donc la seule solution est $q = p + 1$. Donc $q = 3, p = 2$. (le seul couple de premiers dont la différence vaut 1).

Donc $|G| = 24$, $N_2 = 3$, donc l'action de G par conjugaison sur les trois 2-Sylows définit un morphisme non trivial $\varphi : G \longrightarrow \mathfrak{S}_3$. Comme $|\mathfrak{S}_3| = 6 < |G| = 24$, le noyau de φ est un sous groupe propre distingué de G , donc G n'est pas simple. Donc l'hypothèse de départ est fausse, et G est non simple.

Remarque : Pour $G = \mathfrak{S}_4$, on a bien $N_q = p^2, n_p = q$; on a montré, en fait, que $p = 2, q = 3$ est l'unique paire de premier pour lesquels un groupe d'ordre $p^3 q$, avec $N_q = p^2, N_q = p$ existe, et ce groupe n'est pas simple.

2) Traitons le cas $|G| = pqr$, $p > q > r$. Supposons G simple.

$$N_p \mid qr, N_p \geq p+1 \implies N_p = qr$$

$$N_q \mid pr, N_q \geq q+1 \implies N_q \geq p$$

$$N_r \mid pq, N_r \geq r+1 \implies N_r \geq q$$

$$\#\{\text{éléments d'ordre } p\} = N_p(p-1) = (p-1)qr$$

$$\#\{\text{éléments d'ordre } q\} = N_q(q-1) \geq p(q-1)$$

$$\#\{\text{éléments d'ordre } r\} = N_r(r-1) \geq q(r-1)$$

$$\begin{aligned} pqr &= |G| && \geq 1 + q(r-1) + p(q-1) + qr(p-1) \\ &= pqr + pq - p - q + 1 \\ &= pqr + (p-1)(q-1) \not\leq \end{aligned}$$

- 3) Le cas $|G| = p^2 q^2$. Supposons G simple, $N_p > 1$, $N_q > 1$, on suppose $p > q$ donc $N_p \mid q^2$, $N_p \geq p+1$ donc $N_p = q^2$.

Soient $H_{p,1}$, $H_{p,2}$ deux p -Sylow distincts et K l'intersection des deux. Supposons l'intersection non triviale, alors les deux $H_{p,i}$ sont abéliens, et alors ils centralisent K . Dans ce cas, $\mathcal{N}_G(K) \cup H_{p,1}H_{p,2}$, d'ordre $> |H_{p,i}| = p^2$, donc $|\mathcal{N}_G(K)| \geq p^2 q$. Si $|\mathcal{N}_G(K)| = p^2 q$ alors $\mathcal{N}_G(K) \triangleleft G$ par l'exercice 3.

Si $|\mathcal{N}_G(K)| = p^2 q^2$, alors $\mathcal{N}_G(K) = G$ et $K \triangleleft G$, ce qui est absurde.

On a démontré que $H_{p,1} \cap H_{p,2} = \{e\}$.

Par l'exercice 2;

$$|H_{p,1} \cdot H_{p,2}| = \frac{|H_{p,1}| \cdot |H_{p,2}|}{|H_{p,1} \cap H_{p,2}|} = p^4 > |G| \not\leq$$

Donc G est non simple.

m

Exercise 19.

Exercise 20.

Exercise 21.

Exercise 22.