Corrigé du devoir 3.

Problème:

Soit G un groupe d'ordre 56. On note n_2 (resp. n_7) le nombre des 2-sous-groupes (resp. 7-sous-groupes) de Sylow de G.

A) Montrer que n_2 est égal à 1 ou à 7, et que n_7 est égal à 1 ou à 8.

On a $56 = 2^3 \times 7$. les 2-sous-groupes (resp. 7-sous-groupes) de Sylow de G sont donc les sous-groupes de G d'ordre 2^3 (resp. d'ordre 7). D'après les théorèmes de Sylow, on a:
d'une part, n_2 divise 7, d'où $n_2 \in \{1, 7\}$,
d'autre part, n_7 est congru à 1 modulo 7 et n_7 divise 2^3, ce qui implique que $n_7 \in \{1, 8\}$.

Dans la suite, les trois parties B), C) et D) sont indépendantes les unes des autres.

B) Etude de deux exemples.

(B.1) On suppose que G est cyclique engendré par un élément a.

(a) Donner en fonction de a un élément b d'ordre 8 et un élément c d'ordre 7.
On pose $b = a^7$ et $c = a^8$. Puisque a est d'ordre 56, l'ordre de b est égal à $\frac{56}{pgcd(56,7)} = 8$, et l'ordre de c est égal à $\frac{56}{pgcd(56,8)} = 7$.

(b) Quelles sont les valeurs de n_2 et de n_7?
Comme G est un sous-groupe cyclique et que son est ordre est divisible par 8 et par 7, il a un unique sous-groupe d'ordre 8 (engendré par b) et $n_2 = 1$ et il a un unique sous-groupe d'ordre 7 (engendré par c) et $n_7 = 1$.

(B.2) On suppose que G est un groupe diédral engendré par un élément a d'ordre 28 et un élément b d'ordre 2 tels que $bab^{-1} = a^{-1}$.

(a) On note S le sous-groupe de G engendré par a^4.

(i) Montrer que S est distingué dans G.
On veut montrer que le normalisateur $N_G(S)$ de S dans G est égal à G. Comme G est engendré par a et b, il suffit de montrer que $N_G(S)$ contient a et b.
On a $S = \{(a^4)^k | k \in \mathbb{Z}\}$.
Il est clair que a est dans $N_G(S)$ car a commute à a^4. D'autre part, on a, pour tout $k \in \mathbb{Z}$ $b(a^4)^k b^{-1} = ba^{4k}b^{-1} = (bab^{-1})^{4k} = (a^{-1})^{4k} = a^{-4k} = (a^4)^{-k} \in S$. Donc on a bien $b \in N_G(S)$. Ce qui achève la démonstration.

(ii) En déduire que $n_7 = 1$.
Comme a est d'ordre $28 = 4 \times 7$, a^4 est d'ordre 7 et S est un groupe cyclique d'ordre 7. C'est un 7-sous-groupe de Sylow de G. On vient de montrer que S est distingué dans G. Or d'après le deuxième théorème de Sylow, tous les 7-sous-groupes de Sylow de G sont conjugués. Donc, S est l'unique 7-sous-groupe de Sylow de G et $n_7 = 1$.

(b) (i) On note T le sous-groupe de G engendré par a^7 et b. Montrer que T est produit semi-direct (interne) du sous-groupe $\langle a^7 \rangle$ et du sous-groupe $\langle b \rangle$. En déduire que T est d'ordre 8.

Soit $H = \langle a^7 \rangle \langle b \rangle$. Montrons que c'est un sous-groupe de G et un produit semi-direct interne. On vérifie tout d'abord que b normalise $\langle a^7 \rangle$ de la même façon qu'on a montré que b normalise $S = \langle a^4 \rangle$. Le sous-groupe $\langle b \rangle = \{1, b\}$ normalise donc le groupe $\langle a^7 \rangle$.
Vérifions ensuite que l'intersection de $\langle a^7 \rangle$ et de $\langle b \rangle$ est triviale, il suffit de montrer que $b \notin \langle a^7 \rangle$. Ce qui est impossible car sinon on aurait $bab^{-1} = a$, or on a $bab^{-1} = a^{-1}$ où a est d'ordre 28.
Ainsi, H est un sous-groupe et c'est un produit semi-direct interne.
H contient a^7 et b et T est le sous-groupe engendré par a^7 et b donc, $T \subset H$. Réciproquement, T contient tous les produits de puissances de a^7 et de b donc, T contient tous les éléments de la forme $(a^7)^k b^l$, avec $k, l \in \mathbb{Z}$, ce qui implique que $H = \langle a^7 \rangle \langle b \rangle \subset T$.
Ainsi, T est le produit semi-direct interne du sous-groupe $\langle a^7 \rangle$ et du sous-groupe $\langle b \rangle$. On en déduit que $|T| = |\langle a^7 \rangle| \times |\langle b \rangle| = 4 \times 2 = 8$ (a étant d'ordre 28, a^7 est d'ordre 4 et b est d'ordre 2).

(ii) Démontrer que ab est d'ordre 2 et que $ab \notin T$.
On a $(ab)^2 = abab = a(bab) = a(bab^{-1}) = aa^{-1} = 1$, de plus, $ab \neq 1$ (sinon on aurait $a = b^{-1}$, ce qui est impossible, car b est d'ordre 2 et a d'ordre 28), donc ab est d'ordre 2.
Montrons que $ab \notin T$. Si on avait $ab \in T$, comme on a $b \in T$ et que T est un sous-groupe de G, on aurait $a = (ab)b^{-1} \in T$, et par le théorème de Lagrange, l'ordre de a devrait diviser l'ordre de T, ce qui est impossible car, a est d'ordre 28 et T est d'ordre 8.

(iii) En déduire, en utilisant A), que $n_2 = 7$.
On sait que tout 2-sous-groupe de G est contenu dans un 2-sous-groupe de Sylow de G. En particulier, il existe un 2-sous-groupe de Sylow T' de G qui contient $\langle ab \rangle$. Puisque $ab \notin T$, T' est distinct de T. Ainsi, G possède au moins deux 2-sous-groupes de Sylow. Le A) permet de conclure que $n_2 = 7$.

C) Etude générale.
Dans cette question, on suppose que $n_7 = 8$. Quel est alors le nombre d'éléments d'ordre 7 de G? En déduire que, dans ce cas, n_2 est égal à 1.
On note S_1,..., S_8 les 7-sous-groupes de Sylow de G.
Chaque groupe S_i est cyclique d'ordre 7. On pose pour tout $i \in \{1, ..., 8\}$, $S_i = \langle x_i \rangle = \{1, x_i, ..., x_i^6\}$. Alors, comme 7 est un nombre premier, pour tout $i \in \{1, ..., 8\}$ et pour tout $k \in \{1, ..., 6\}$, x_i^k est d'ordre 7 et c'est un générateur de S_i. Donc, si $i \neq j$, $S_i \cap S_j = \{1\}$.
De plus, si y est un élément d'ordre 7 de G, le sous-groupe $\langle y \rangle$ est un 7-sous-groupe de Sylow de G et il existe i tel que $y \in S_i$.
Donc, tout élément d'ordre 7 de G est dans un unique 7-sous-groupe de Sylow S_i et un 7-sous-groupe de Sylow S_i contient 6 éléments d'ordre 7. Donc G contient $6 \times 8 = 48$ éléments d'ordre 7. Soit A l'ensemble des éléments d'ordre 7 de G.
Comme G est d'ordre 56. $G \setminus A$ est de cardinal 8. Soit T un 2-sous-groupe de Sylow de G. Alors, T est d'ordre 8 et $T \subset G \setminus A$. On en déduit que $T = G \setminus A$. Donc, G contient un unique 2-sous-groupe de Sylow et $n_2 = 1$.

D) Encore un exemple.
Soient V un espace vectoriel de dimension 3 sur le corps à 2 éléments $\mathbb{F}_2$ et $\mathbf{e} = (\mathbf{e_1}, \mathbf{e_2}, \mathbf{e_3})$ une base de V. On considère le produit semi-direct $H = V \rtimes GL(V)$ dont les éléments sont les couples (v, f), où $v \in V$ et $f \in GL(V)$, et dans lequel la multiplication est donnée par

$$(v, f) \star (v', f') = (v + f(v'), f \circ f').$$

(D.1) Vérifier que la loi $\star$ est bien une loi de groupe sur H.
On vérifie que $(0, Id_V)$ est élément neutre pour la loi $\star$ et que l'élément (v, f) admet $(-f^{-1}(v), f^{-1})$ pour inverse.

Quant à l'associativité, elle résulte des égalités suivantes:

$$\begin{aligned}((v,f)\star(v',f'))\star(v",f") = (v+f(v'), f\circ f')\star(v",f") &= (v+f(v')+f\circ f'(v"), (f\circ f')\circ f") \\ &= (v+f(v')+f(f'(v")), f\circ f'\circ f")\end{aligned}$$

et

$$\begin{aligned}(v,f)\star((v',f')\star(v",f")) = (v,f)\star(v'+f'(v"), f'\circ f") &= (v+f(v'+f'(v")), f\circ(f'\circ f")) \\ &= (v+f(v')+f(f'(v")), f\circ f'\circ f")\end{aligned}$$

La loi $\star$ est donc une loi de groupe sur H.

(D.2) On note g l'élément de $GL(V)$ dont la matrice dans la base $\mathbf{e}$ est

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Vérifier que g est d'ordre 7 dans $GL(V)$.
Les images successives de e_1 par les puissances de g sont données par le cycle suivant: $e_1 \mapsto e_2 \mapsto e_3 \mapsto e_1+e_2 \mapsto e_2+e_3 \mapsto e_1+e_2+e_3 \mapsto e_2+e_3+(e_1+e_2) = e_1+e_3 \mapsto e_2+(e_1+e_2) = e_1$ (V est un $\mathbb{F}_2(=\mathbb{Z}/2\mathbb{Z})$-espace vectoriel, donc $e_i + e_i = 0$). En particulier, on voit que g^7 fixe chacun de vecteurs e_1, e_2, e_3; on a donc $g^7 = Id_V$ et l'ordre de g divise 7. Comme 7 est un nombre premier et que $g \neq Id_V$, on en déduit que g est d'ordre 7 dans $GL(V)$.

(D.3) Soit $G = \{(v, g^i) | v \in V, 0 \leq i \leq 6\}$.
(a) Vérifier que G est un sous-groupe d'ordre 56 de H.

On a $H = V \rtimes GL(V)$ et l'ensemble G est le produit semi-direct $(V \rtimes \langle g \rangle)$ de V par le sous-groupe $\langle g \rangle$ de $GL(V)$. C'est donc un sous-groupe de H d'ordre égal au produit de l'ordre de V par l'ordre de $\langle g \rangle$. Or on a $|V| = |(\mathbb{F}_2)^8| = 2^3 = 8$ et $|\langle g \rangle| = 7$, donc $|G| = 8 \times 7 = 56$.

(b) Pour ce groupe G déterminer n_2 et n_7.
L'ensemble $\{(v, Id_V) | v \in V\}$ est un sous-groupe distingué d'ordre 8 de G; c'est un 2-sous-groupe de Sylow de G. De plus, il est distingué dans G. Donc, c'est l'unique 2-sous-groupe de Sylow de G et $n_2 = 1$.
L'ensemble $K = \{(0, g^i) | 0 \leq i \leq 6\}$ est un sous-groupe de G d'ordre 7, c'est un 7-sous-groupe de Sylow de G. Il n'est pas distingué dans G car, par exemple, on a

$$(e_1, Id_V) \star (0, g) \star (e_1, Id_V)^{-1} = (e_1, g) \star (-e_1, Id_V) = (e_1 - e_2, g) \notin K.$$

On a donc $n_7 \geq 2$, d'où $n_7 = 8$.