Devoir à la maison (facultatif)

Soit G un groupe simple d'ordre 168.

1) $168 = 2^3.3.7$.

2) $n_7 = 1 \bmod 7$ et $n_7 | 2^3.3$. Donc $n_7 = 1$ ou 8. Comme G est simple, $n_7 \neq 1$ et $n_7 = 8$.

3) $[G : H] = n_7$ donc $|H| = 21$. Soit Q un 3$-$Sylow de H. Comme $P \lhd H$, $H = PQ$.

4) Si $H < K < G$, alors P n'est pas distingué dans K (sinon $K = H$) donc $n_7(K) = 8$. Donc $8||K|$. Donc $21.8 = 168||K|$ *absurde !*.

5) Soit S un groupe d'ordre 21. Forcément dans un groupe d'ordre $21 = 3.7$, il y a un seul 7$-$Sylow donc $S = \mathbb{Z}/7\mathbb{Z} \rtimes_\phi \mathbb{Z}/3\mathbb{Z}$. Si $\phi_1, \phi_2 : \mathbb{Z}/3\mathbb{Z} \to (\mathbb{Z}/7\mathbb{Z})^\times$ non triviaux, alors comme il y a un seul sous-groupe d'ordre 3 dans $(\mathbb{Z}/7\mathbb{Z})^\times \simeq \mathbb{Z}/6\mathbb{Z}$, $\phi_1 = \phi_2 \circ \gamma$ pour un $\gamma \in \mathrm{Aut}(\mathbb{Z}/3\mathbb{Z})$; donc $\mathbb{Z}/7\mathbb{Z} \rtimes_{\phi_1} \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/7\mathbb{Z} \rtimes_{\phi_2} \mathbb{Z}/3\mathbb{Z}$. Si H était abélien, alors $Q \lhd H$ donc $H \subseteq N_G(Q) < G$ donc $H = N_G(Q)$ par maximalité et $n_3 = [G : N_G(Q)] = 8$: *absurde !* car $n_3 = 1 \bmod 3$.

6) $H = PQ$. Comme $P \lhd H$, si $Q \lhd H$, alors $H \simeq P \times Q$ est abélien absurde. Donc Q n'est pas le seul 3$-$Sylow de H. Donc $n_3(H) = 7$. Soient Q_1, Q_2 2 3$-$Sylow de H. Soit $H' := \langle Q_1, Q_2 \rangle$. Alors $n_3(H') = 7$ donc $7||H'|$ donc $|H'| = 21$ et $H' = H$. On a $n_3 = 1 \bmod 3$ et $n_3|56$. Donc $n_3 = 1, 4, 7$ ou 28. Comme $n_3 > 7$ (sinon tous les 3$-$Sylow sont dans H. Mais alors, si $x \notin H$, $xQx^{-1} = pHp^{-1}$ pour un $p \in P$ donc $p^{-1}x \in N_H(Q) = Q$ donc $x \in PQ = H$ absurde !), $n_3 = 28$.

7) Le groupe K a $[G : N_G(K)] = [G : K] = n_3 = 28$ conjugués. comme $|K| = 6$, $K \simeq \mathfrak{S}_3$ ou $\mathbb{Z}/6\mathbb{Z}$. Si K est cyclique, alors les conjugués de K aussi. Or K contiendrait exactement $\varphi(6) = 2$ éléments d'ordre 6. Un élément d'ordre 6 ne peut pas être dans 2 conjugfués distincts. On aurait donc $2.28 = 56$ éléments d'odre 6, $2.28 = 56$ éléments d'ordre 3, $8.6 = 48$ éléments d'ordre 7, cela ait $56 + 56 + 48 = 160$ éléments. On aurait donc alors un seul groupe d'ordre 8, absurde car $n_2 > 1$.

8) Comme tPt^{-1} est d'ordre 7, $tPt^{-1} \cap H = 1 out Pt^{-1}$. Si $tPt^{-1} \cap H = tPt^{-1}$, alors $tPt^{-1} \leqslant H$. Or, P est le seul 7$-$Sylow de H donc on aurait $t \in N_G(P) = PQ = H$ *absurde !* car t d'ordre 2 et H d'ordre 21. Donc $tP^{-1} \cap H = 1$. Si $htp = t$, alors $tpt^{-1} = h^{-1} \in H \cap tPt^{-1} = 1 \Rightarrow h = 1$, $p = 1$. On a alors $|H \cup HtP| = |H| + |H \times P| = 21 + 21.7 = 168 = |G| \Rightarrow G = H \cup HtP$.

9) $tPt^{-1} \cap H = 1$ comme montré ci-dessus.

10) $tP^*t = tP^*t \cap (G \setminus H) = tP^*t \cap PQtP$. Or $PQtP = PtP \cup PstP \cup Ps^2tP$. On a :

$$s^{-1}Ps^itPs = Ps^{-1}s^itsP$$

comme $K \simeq \mathfrak{S}^3$, on a $st = ts^{-1}$ et $ts = s^{-1}t$ donc :

$$s^{-1}A_is = Ps^{i-2}tP = Ps^{i+1}tP = A_{i+1} \ .$$

Donc $|A_0| = |A_1| = |A_2|$. De plus, $H \times P$ agit librement sur HtP donc les A_i sont deux à deux disjoints. Donc $|A_i| = |P^*|/3 = 2$.

11) Comme $1 \notin PtP$, $1 = tt \notin tPtPt$. Donc $tA_0t = P \cap tPtPt$ est de cardinal 2 et c'est stable par passage à l'inverse. La question précédente entraîne directement :

$$A_0 = \{tu^{\pm 1}t\},\ A_1 = \{s^{-1}tu^{\pm 1}ts\},\ A_2 = \{stu^{\pm 1}ts^{-1}\}\ .$$

12) Comme P est d'ordre 7 et $1 \neq u \in P$, $P = \langle u \rangle$ donc $P^* = \{u^{\pm 1}, u^{\pm 2}, u^{\pm 4}\}$. On a $s^{-1}us = u^i$ pour un $i \in (\mathbb{Z}/7\mathbb{Z})^\times$. Donc $u = s^{-3}us^3 = u^{i^3} \Rightarrow i^3 = 1 \bmod 7 \Rightarrow i = 1, 2$ ou 4. Or $i \neq 1$ car s et u ne commutent pas. On suppose $s^{-1}us = u^2$. *(C'est possible quitte à échanger s et s^{-1}).*
On a $tut \in PtP$. Donc $tut = u^itu^j$ pour certains $i, j \in \mathbb{Z}/7\mathbb{Z}$. Mais alors :

$$stuts^{-1} = ts^{-1}ust = tu^2t = su^itu^js^{-1} = su^is^{-1}sts^{-1}su^js^{-1} = u^{4i}s^2tu^{4j}$$

(e effet, $su^2s^{-1} = u \Rightarrow su^8s^{-1} = sus^{-1} = u^4$.
De même, on a :

$$tu^4t = u^{2i}stu^{2j},\ tu^{-1}t = u^{-j}tu^{-i},\ tu^{-2}t = u^{-4j}s^2tu^{-4i},\ tu^{-4}t = u^{-2j}stu^{-2i}.$$

On a aussi : $tu^2t = tuttut = u^itu^{i+j}u^j$. Donc : $u^{4i}s^2tu^{4j} = u^itu^{i+j}u^j$. D'où :

$$u^{3i}s^2tu^{3j} = tu^{i+j}t\ .$$

Or, $i + j = 0, \pm 1, \pm 2$ ou$\pm 4 \bmod 7$.
D'après les formules ci-dessus qui donne tu^kt sous la forme $pqtp'$ (pour un unique triplet $(p, q, p') \in P \times Q \times P$, on a forcément $i + j = \pm 2$ et $i + j = 2 \Rightarrow 3i = 4i$ et $3j = 4j$ *impossible !* Donc $i + j = -2$ et $3i = -4j$, $3j = -4i$ d'où : $i = j = -1$.
On a donc bien :

$$(1)\qquad \begin{aligned} &tut = u^{-1}tu^{-1},\ tu^2t = u^{-4}s^2tu^{-4},\ tu^4t = u^{-2}stu^{-2},\\ &tu^{-1}t = utu,\ tu^{-2}t = u^4s^2tu^4,\ tu^{-4}t = u^2stu^2\ . \end{aligned}$$

13) Soient $g, g' \in G$.
Si $g, g' \in H$, gg' se calcule dans H.
Si $g \in H$, $g' = htp$, $h \in H$, $p \in P$, $gg' = (gh)tp$ et gh se calcule dans H.
Si $g = htp \in HtP$, $h \in H$, $p \in P$, et $g' \in H$, alors : $gg' = htpg'$. Or $pg' \in QP$ donc $pg' = qp'$ pour un certain $q \in Q$ et un certain $p' \in P$ (déterminés par la loi de groupe de H. Donc $gg' = htqp'$. Or $K \simeq \mathfrak{S}_3$ donc $tq = q^{-1}t$ et $gg' = hq^{-1}tp'$.
Si $g = htp$ et $g' = h'tp'$ avec $h, h' \in H$, $p, p' \in P$, alors $gg' = htph'tp'$. On a $ph' = qp''$ pour un $q \in Q$, un $p'' \in P$ (déterminés par le produit dans H). Donc $gg' = hq^{-1}tp"tp'$. Si $p" = 1$, $gg' = hq^{-1}p'$ sinon, $p" \in \{u^{\pm 1}, u^{\pm 2}, u^{\pm 4}\}$ et la décomposition de $tp''t \in HtP$ est déterminée par les relations (1).

14) On a en fait montré que tous les groupes d'ordre 168 dont aucun Sylow n'est distingué sont isomorphes.

15) Si $n \in \mathbb{N}$ et K est un corps tels que $(n, |K|) \neq (2, 2), (2, 3)$, alors le groupe $\mathrm{PSL}_n(K)$ est simple (*cf.* Lang, *Algebra*, th. 8.4 et 9.3). Or $\mathrm{PSL}_3(\mathbb{F}_2) = \mathrm{GL}_3(\mathbb{F}_2)$.

16) Si $60 < n < 168$, alors voici les décompositions possibles de n en produits de nombres premiers :
— $n = pqr$ pour des nombres premiers distincts,
— $n = pq$, p, q premiers distincts,
— $n = p^\alpha$, p premier, $\alpha \geqslant 1$,
— $n = p^2q$, p, q premiers distincts,
— $n = p^2qr$, p, q, r premiers distincts : dans ce cas, $n = 90$ ou 150,
— $n = p^3qr$, p, q, r premiers distincts : dans ce cas, $n = 120$,
— $n = p^2q^2$, p, q premiers distincts : dans ce cas : 100,
— $n = p^\alpha q^\beta$, p, q premiers distincts, $\alpha \geqslant 3$, $\beta \geqslant 2$: dans ce cas : $n = 72, 108, 144$,
— $n = p^\alpha q$, p, q premiers distincts et $\alpha \geqslant 3$. Dans ce cas, $p \neq 1 \bmod q$.
Dans tous les cas, G d'ordre n n'est pas simple. Par exemple si $n = 120 = 2^3.3.5$. Le nombre de $5-$Sylow est $n_5 = 1$ ou 6. Si $n_5 = 6$, on a un morphisme $G \to S_6$ injectif si G est simple. Mais alors $G \simeq \mathfrak{S}_5$ (comme tout sous-groupe d'indice 6 dans S_6). Et $\mathfrak{S}_5$ n'est pas simple.
Remarque : tout groupe d'ordre $p^\alpha q^\beta$, p, q premiers distincts, est résoluble (théorème de Burnside)