$\boxed{P1}$ $|G| = 45 = 3^2 \cdot 5 \Rightarrow G$ abeliano

Llamemos n a la cantidad de 3-grupos de Sylow de G y sea H uno de ellos. Con una notación similar, sean m y K los objetos para 5-grupos de Sylow. Sabemos que:

$$\begin{matrix} n \mid 5 & m \mid 9 \\ n = 1 \bmod 3 & m = 1 \bmod 5 \end{matrix} \Rightarrow n = m = 1.$$

Luego, H y K son normales en G. Además, es claro que $H \cap K = \{e\}$.

$$\left.\begin{matrix} H, K \trianglelefteq G \\ H \cap K = \{e\} \end{matrix}\right. \Rightarrow HK \cong H \times K.$$

Y por asuntos de cardinalidad deducimos $H \times K \cong G$

¿Qué estructura tiene K? Tiene orden primo $\Rightarrow K$ cíclico

¿ " " " H? Lema: Un grupo G' de orden p^2, p primo, es isomorfo a $\mathbb{Z}_{p^2}$ o a $\mathbb{Z}_p^2$. En particular, G' es abeliano.

Dem. del Lema: Sea Z el centro de G'. Elijamos $g \in Z$ de orden máximo. Como $Z \supsetneq \{e\}$ (P7, tarea 2), orden$(g) \in \{p, p^2\}$. Si es p^2, $G' \cong \mathbb{Z}_{p^2}$. Si es p, elijamos $h \in G' \setminus \langle g \rangle$. Si orden$(h) = p^2$, $G' \cong \mathbb{Z}_{p^2}$. Si orden$(h) = p$, sea $G_1 = \langle g \rangle$, $G_2 = \langle h \rangle$. Tenemos $G_1 \cap G_2 = \{e\}$, $\forall x \in G_1, y \in G_2: xy = yx \Rightarrow G_1G_2 \cong G_1 \times G_2 \Rightarrow G_1 \times G_2 \cong G'$. Como $G_i \cong \mathbb{Z}_p$, $G' \cong \mathbb{Z}_p^2$

Volvamos al problema original: Deducimos que $G \cong \mathbb{Z}_5 \times \mathbb{Z}_3^2$ o $G \cong \mathbb{Z}_5 \times \mathbb{Z}_9$.

En particular, G es conmutativo.

$\boxed{P2}$ Sea G grupo de orden $20 = 4 \cdot 5$. Sea $n = |S_2(G)|$, $m = |S_5(G)|$, $H \in S_2(G)$ y $K \in S_5(G)$. Sabemos que:

$$\begin{matrix} n \mid 5 & m \mid 4 \\ n = 1 \bmod 2 & m = 1 \bmod 5 \end{matrix} \Rightarrow n \in \{1, 5\}, m = 1.$$

Como esta vez no podemos deducir el valor de n, vamos a proceder de otra forma:

$$\left.\begin{matrix} m = 1 \Rightarrow K \trianglelefteq G \\ H \cap K = \{e\} \end{matrix}\right\} \Rightarrow HK \cong H \rtimes_f K, \text{ donde } f: \begin{matrix} H \to \operatorname{aut}(K) \\ x \mapsto \varphi_x \end{matrix} \Rightarrow H \rtimes_f K \cong G.$$

$$\varphi_x: \begin{matrix} K \to K \\ y \mapsto xyx^{-1} \end{matrix}$$

$K \cong \mathbb{Z}_5$ y, gracias al lema del P1, $H \cong \mathbb{Z}_4$ o $H \cong \mathbb{Z}_2^2$.

Para entender $H \rtimes_f K$ basta entender f. Naturalmente esto depende de cómo e

• Si $H \cong \mathbb{Z}_4$: Sea h un generador de H. Como f es un morfismo con dominio H, f está determinado por su valor en h. A su vez, $f(h) = \varphi_h$ tiene dominio K, así q esta determinado por su valor en un generador de K. Sea $k \in K$ un generador. $\varphi_h(k) = hkh^{-1} \in K$, pues K normal $\Rightarrow \exists \alpha \in \{1,2,3,4\} : hkh^{-1} = k^\alpha$. Se tiene:

(i) $\alpha = 1 \Rightarrow \varphi_h = id_K \Rightarrow H \rtimes_f K \cong H \times K$

(ii) $\alpha \in \{2,3,4\} \Rightarrow \exists \beta \in \{1,2,3\} : \alpha\beta = 4 \mod 5$. Sea $\tilde{k} = k^\beta$. Como $hkh^{-1} = k^\alpha$, entonces $h\tilde{k}h^{-1} = (hkh^{-1})^\beta = (k^\alpha)^\beta = k^{\alpha\beta} = k^4$. Además, $\beta \in \{1,2,3\} \Rightarrow \tilde{k}$ generador de K.

$\therefore$ Los casos $\alpha = 2, \alpha = 3$, y $\alpha = 4$ nos llevan al mismo producto semidirecto, caracterizado por:

$G = \langle h \rangle \rtimes_f \langle k \rangle, \quad hk = k^{-1}h \quad (*)$

En particular, G no es conmutativo $(*)$, así que no es isomorfo al del caso (i)

• Si $H \cong \mathbb{Z}_2^2$. El procedimiento es similar al caso anterior. G es isomorfo, por las mismas razones que antes, a $H \rtimes_f K$, y f es el mismo que antes. Si h_1, h_2 son generadores de H, entonces f está caracterizado por sus valores en h_1 y h_2, y es fácil ver que los $\{h_i\}$ actúan como una base de H, de manera que hay 3 grupos distintos salvo isomorfismos en este caso:

$G \cong \mathbb{Z}_2^2 \times \mathbb{Z}_5$, caracterizado por $[h_1, k] = [h_2, k] = 1$.

$G \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_5$, " " $[h_1, k] = 1$, $h_2 k = k^{-1} h_2$

$G \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_5$, " " $h_i k = k^{-1} h_i$, $i \in \{1,2\}$.

Nota: $[x,y] = xyx^{-1}y^{-1} =$ el conmutador de x, y

Prop. $[x,y] = 1$ sii $xy = yx$.

$\boxed{P3}$ $N \trianglelefteq G$. G soluble sii G/N y N solubles. (Este teorema es <u>muy</u> útil).

$\boxed{\Rightarrow}$ Sea $\{e\} \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n = G$ una torre abeliana para G.

• N soluble: Sea $N_i = G_i \cap N$. $i: N_{i+1} \hookrightarrow G_{i+1}$ la inyección canónica. Como $G_i \trianglelefteq G_{i+1}$, el teo. de correspondencia nos dice que $N_i = G_i \cap N = i^{-1}(G_i) \trianglelefteq N_{i+1}$, y que se tiene el monomorfismo $N_{i+1}/N_i \hookrightarrow G_{i+1}/G_i$, de donde deducimos que N_{i+1}/N_i es abeliano. Luego, $\{e\} \trianglelefteq N_1 \trianglelefteq \ldots \trianglelefteq N_n = N$ es torre abeliana para N.

• G/N es soluble: Sea $M_i = G_i N$, $i \in \{1, \ldots, n\}$. Cada M_i es grupo pues $N \trianglelefteq G$, y $N \trianglelefteq M_1 \trianglelefteq M_2 \trianglelefteq \ldots \trianglelefteq M_n = G$, porque G_i es normal en G_{i+1} también

Consideremos la secuencia $G_{i+1} \xrightarrow{j} NG_{i+1} \xrightarrow{r} NG_{i+1}/N$, donde j es el monomorfismo canónico y r el epimorfismo canónico. Como $NG_i \supseteq N = \ker r$, el teorema de correspondencia nos da un morfismo inyectivo $f: G_{i+1}/G_i \to G_{i+1}N/N \,/\, G_iN/N \cong G_{i+1}N/G_iN$
↑ 3º teo de iso.

Todo queda descrito en el siguiente diagrama conmutativo:

$$\begin{array}{ccccc} G_{i+1} & \xrightarrow{j} & NG_{i+1} & \xrightarrow{r} & NG_{i+1}/N \\ \uparrow & & \uparrow & & \uparrow \\ G_i & \longrightarrow & NG_i & \longrightarrow & NG_i/N \end{array}$$

donde las flechas ascendentes son las inyecciones canónicas.

Es inmediato comprobar que f es epiyectiva. Deducimos que M_{i+1}/M_i es abeliano. ∎

$\boxed{E}$ Si $\{e\} \lhd N_1 \lhd \ldots \lhd N_n = N$ y $\{e\} \lhd M_1 \lhd \ldots \lhd M_m = G/N$ son torres abelianas y $r: G \to G/N$ es el epimorfismo canónico, entonces $\{e\} \lhd N_1 \lhd \ldots \lhd N_n \lhd r^{-1}(M_1) \lhd \ldots \lhd r^{-1}(M_m) = G$ es torre abeliana ∎

$\boxed{P4}$

2. $G_1 \cong \{(g,e) \in G_1 \times G_2\}$. Luego, por $\underline{P3}$, $G_1 \times G_2$ soluble $\Rightarrow G_i$ soluble.

Recíprocamente, $\{(g,e) \in G_1 \times G_2\}$ es soluble y normal en $G := G_1 \times G_2$. $G/G_1 \cong G_2$ también es soluble. Concluimos a través del $\underline{P3}$.

3. $K, L \lhd G$, G/K, G/L solubles. Es claro que $K \cap L \lhd G$, y por lo tanto, $K \cap L \lhd K$. Probar que $G/K\cap L$ es soluble equivale a probar que $K/K\cap L$, $G/K\cap L \,/\, K/K\cap L$ son solubles.

$G/K\cap L \,/\, K/K\cap L \cong G/K$, y así, soluble. (3º teo. de iso.)

$K/K\cap L \cong KL/L \leq G/L$, y por lo tanto, soluble. (2º teo de iso.).

4. • $D_n \cong \mathbb{Z}_2 \ltimes \mathbb{Z}_{n/2}$. Cada factor es soluble $\Rightarrow D_n$ soluble.

• $S_3 \cong D_6$

• A_4: $V_4 = \{id, (12)(34), (14)(23), (13)(24)\} \cong \mathbb{Z}_2^2$ es normal en A_4 y $A_4/V_4 \cong \mathbb{Z}_3$. $\underline{P3}$.

• $|G| = p^n$. Por inducción: si $n=1$, G es cíclico $\Rightarrow$ G abeliano. Si $n>1$, $Z = Z(G) \overset{?}{\neq} \{e\}$ (P7, Tarea 2). Z abeliano $\Rightarrow Z$ soluble, $Z \lhd G$. $|G/Z| < |G| \Rightarrow G/Z$ soluble, por hipótesis de inducción. Luego, G soluble.

P5 G de orden pq, $q > p$. $P \in S_p(G)$, $Q \in S_q(G)$.

1. La cantidad $\xi = |S_q(G)|$ satisface $\xi \mid p$, $\xi \equiv 1 \mod q$.

$\Rightarrow \xi \in \{1, p\}$. Si $p = \xi = q \cdot l + 1 \Rightarrow q > q \cdot l + 1 \Rightarrow l = 0 \Rightarrow \xi = 1 \rightarrow\leftarrow$

$\Rightarrow \xi = 1 \Rightarrow Q \lhd G$

Tenemos $\begin{matrix} P \cap Q = \{e\} \\ Q \lhd G \end{matrix} \Rightarrow PQ \cong P \rtimes_\varphi Q$, con $\varphi : P \to \mathrm{Aut}\, Q$, $x \mapsto f_x$; $f_x : Q \to Q$, $y \mapsto xyx^{-1}$ $\Rightarrow |PQ| = G \Rightarrow G \cong P \rtimes_\varphi Q$

Como P, Q cíclicos, $P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q \Rightarrow G \cong \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$.

2. $\zeta = |S_p(G)|$ satisface $\zeta \mid q$, $\zeta \equiv 1 \mod p$. Si $q = \zeta = p \cdot l + 1 \Rightarrow q - 1 = pl$ $\rightarrow\leftarrow$

Luego, $\zeta = 1 \Rightarrow P \lhd G$. Tenemos:

$\begin{matrix} P, Q \lhd G \\ P \cap Q = \{e\} \end{matrix} \Rightarrow \forall x \in P, y \in Q : xy = yx \Rightarrow \forall x \in P : f_x = id_Q \Rightarrow \varphi$ es el morfismo trivial

Ver el lema.

$\therefore G \cong P \rtimes_\varphi Q \cong P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$

__Lema__ Si n y m son coprimos, entonces $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$.

__Dem.__ $g : \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$, $x \mapsto (x \mod n, x \mod m)$. g está bien definida (¿por qué?).

$\exists \alpha, \beta \in \mathbb{Z} : \alpha n + \beta m = 1$.

g inyectiva: $g(x) = (0,0) \Rightarrow x = n l_1 = m l_2 \xRightarrow{n,m \text{ coprimos}} n \mid l_2,\ m \mid l_1 \Rightarrow x = nm l_3 \Rightarrow x \equiv 0 \mod nm$.

g epiyectiva: Sean $i, j \in \mathbb{Z}$. Definamos $x = \alpha n j + \beta m i$. Notemos que $\alpha n + \beta m = 1 \Rightarrow \beta m \equiv 1 \mod n$ $\Rightarrow x = \beta m i \equiv i \mod n$. De manera similar, $x \equiv j \mod m$.

__Nota__: Usamos la bien conocida estructura de anillo de $\mathbb{Z}_K$.

3. Es fácil ver que los automorfismos de $\mathbb{Z}_q$ son los de la forma $id_{\mathbb{Z}_q} \cdot K$, con K una cte. no nula (mod q). Más aún, $f \in \mathrm{aut}\, \mathbb{Z}_q \Rightarrow f = f(1) \cdot id_{\mathbb{Z}_q}$ y $f = id$ sii $K = 1$.

Si $\varphi : \mathbb{Z}_p \to \mathrm{aut}(\mathbb{Z}_q)$ es un morfismo y $b \in \mathbb{Z}_q$ entonces $(1,b)(2,b) = (2,b)(1,b)$

$\Leftrightarrow 1 + \varphi(b)(2) = 2 + \varphi(b)(1)$

$\Leftrightarrow (\varphi(b)(1) - 1) \cdot 1 = 0 \Leftrightarrow \varphi(b) = id_{\mathbb{Z}_q}$

Luego, $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ abeliano sii $\varphi = id_{\mathbb{Z}_q}$

(b) Sean $\varphi, \varphi' : \mathbb{Z}_p \longrightarrow \operatorname{aut}(\mathbb{Z}_q)$. $\exists\, \alpha, \alpha' \in \mathbb{Z} : \varphi(1)(1) = \alpha,\ \varphi'(1)(1) = \alpha'$.
También existe $\beta \in \mathbb{Z}_q : \underset{\beta \neq 0}{\alpha\beta} = \alpha'$ (¿por qué?). Sea $\psi(k) = k\beta$. $\psi : \mathbb{Z}_q \longrightarrow \mathbb{Z}_q$ es isomorfismo. Tenemos $\varphi(1)(1) = \alpha \Rightarrow \varphi(1)(\beta) = \alpha\beta \Rightarrow \varphi(1)(\psi(1)) = \alpha'$, $(\psi \circ \varphi'(1))(1) = \alpha$.
$\Rightarrow \varphi(1) \circ \psi = \varphi'(1) \Rightarrow \forall x \in \mathbb{Z}_p : \varphi(x) \circ \psi = \varphi'(x) \Rightarrow \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p \cong \mathbb{Z}_q \rtimes_{\varphi'} \mathbb{Z}_p$.
$\psi \circ \varphi'(x) = \varphi(x)$