FACULTAD DE
CIENCIAS
UNIVERSIDAD DE CHILE

Apuntes de Ayudantía

Álgebra de postgrado

Claudio Bravo Castillo
19 de mayo de 2018

Este documento se desarrolló como una ayuda para estudiantes de postgrado de la Universidad de Chile y P. Universidad Católica de Chile, en el marco de un curso de Álgebra I y II llevado a cabo por el Dr. Antonio Behn. En el se ilustran varios problemas de examenes de calificación de la U. de Chile, los cuales de destacan con un (*), y algunos de los problemas presentes en este documento hacen referencia a ciertos ejercicios disponibles en la pagina web:

`https://www.u-cursos.cl/ciencias/2018/1/POST0090/1/material_docente/`

Cabe destacar que en las actuales notas se dejan ciertos ejercicios propuestos.

Índice

1. Grupos:

Ayudantía 1: En esta ayudantía estudiaremos acciones de grupos y recordaremos ciertas nociones básicas de la teoría de grupos.

1.- **Problema 1*:** Sea G un grupo finito[1] y $H \subsetneq G$ un subgrupo propio. Demuestre que $\bigcup_{g\in G} gHg^{-1} \neq G$.
Demostración: Primero observe que si $\{g_i\}_{i\in I}$ es un conjunto de representantes de las clases en $G/N_G(H)$, entonces:

$$\bigcup_{g\in G} gHg^{-1} = \bigcup_{i\in I} g_iHg_i^{-1},$$

esto pues todo $g \in G$ se escribe como $g = g_it$, donde $t \in N_G(H)$ y se cumple que $gHg^{-1} = g_itHt^{-1}g_i^{-1} = g_iHg_i^{-1}$, por definición del conjunto normalizador.

Por otro lado, sabemos que $|H| = |gHg^{-1}|$, para cualquier $g \in G$. De esto se sigue que:

$$\left|\bigcup_{g\in G} gHg^{-1}\right| \leq [G : N_G(H)]|H|. \tag{1}$$

Note que si $\bigcup_{g\in G} gHg^{-1} = G$, entonces $[G : H]|H| = |G| \leq [G : N_G(H)]|H|$. Por lo tanto $[G : H] \leq [G : N_G(H)]$, de lo que se sigue que $|H| \geq |N_G(H)|$. Por lo tanto $H = N_G(H)$ y entonces la ecuación (1) es una igualdad. Dicha igualdad se cumple si y solo si los conjuntos $g_iHg_i^{-1}$ son disjuntos. Esto último es falso pues $e \in g_iHg_i^{-1}$, para todo $i \in I$.

2.- **Problema 2:** Sea G un grupo de orden p^n, donde p es un número primo y $n > 0$.

i.- Demuestre que si $n = 1$ entonces G es cíclico.

ii.- Demuestre que $Z(G) \neq \{e\}$.

iii.- Pruebe que si $n = 2$ entonces G es abeliano.

iv.- Encuentre un ejemplo para $n > 2$ en el que G no sea un grupo abeliano.

Desarrollo:

i.- Sea $g \in G$ un elemento no trivial y considere el subgrupo $H = \langle g\rangle$, cuyo cardinal es mayor o igual a 2. Por el teorema de Lagrande tenemos que $|H|$ divide a $|G| = p$. Por ende $|H| = p$, lo que nos permite concluir que $H = G$.

ii.- Considere la acción de G sobre si mismo por conjugación. Dicha acción, al igual que cualquier otra, divide a G en órbitas disjuntas y por ende:

$$|G| = \sum |\mathrm{Orb}_G(g_i)|\,.$$

Una de dichas órbitas $\mathrm{Orb}(g_i)$ es trivial si y solamente si para todo $g \in G$ se tiene que $gg_ig^{-1} = g_i$, es decir si $g_i \in Z(G)$. Concluimos que el número de órbitas triviales es $|Z(G)| > 1$, pues $e \in Z(G)$. Por otro lado, la relación órbita-estabilizador nos dice que $|\mathrm{Orb}(g_i)| = [G : \mathrm{Stab}_G(g_i)]$. Luego si

[1]Para ver un contraejemplo a este enunciado en cardinal infinito, desarrolle el problema 7 de su guia de ejercicios.

$\mathrm{Orb}(g_i)$ no es trivial, tenemos que p divide a $|\mathrm{Orb}(g_i)|$. Luego, como:

$$p^n = |G| = |Z(G)| + \sum_{\text{no triv.}} |\mathrm{Orb}_G(g_i)|\,,$$

se tiene que p divide a $|Z(G)|$ y concluimos lo pedido.

iii.- Basta probar que si $G/Z(G)$ es un grupo cíclico entonces G es un grupo abeliano (Ejercicio). Entonces, como $|G/Z(G)| \leq p$, por la parte [i] concluimos lo pedido.

iv.- Considere el grupo $D_8 = \langle r, s : r^4 = s^2 = e, srs = r^{-1}\rangle$ correspondiente a las simetrias del octágono regular. Dicho grupo tiene 8 elementos, pero no es abeliano.

3.- **Problema 3:** Sea S_n el grupo de permutaciones de n elementos, $\mathbb{F}$ un cuerpo cualquiera y $\{e_i\}_{i=1}^n$ la base canónica de $\mathbb{F}^n$. Para $\sigma \in S_n$ definimos la matriz I_σ como la matriz que tiene por columnas a los vectores $e_{\sigma(i)}$, donde $i \in \{1, \cdots, n\}$. Considere la función $\phi : S_n \to \mathrm{Gl}_n(\mathbb{F})$ dada por $\phi(\sigma) = I_\sigma$. Definimos el signo $\mathrm{sgn}(\sigma)$ de σ por $\mathrm{sgn}(\sigma) = \det(I_\sigma) \in \{\pm 1\}$.

i.- Pruebe que ϕ es un homomorfismo inyectivo.

ii.- Muestre que $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau\sigma\tau^{-1})$, para todo $\sigma, \tau \in S_n$.

iii.- Muestre que si $\sigma = \tau_1 \cdots \tau_r$ es un producto de r transposiciones entonces $\mathrm{sgn}(\sigma) = (-1)^r$.

iv.- Pruebe que $A_n = \{\sigma \in S_n : \mathrm{sgn}(\sigma) = 1\}$ es un grupo normal de S_n y determine el cociente S_n/A_n.

Desarrollo:

i.- Observe que I_σ es la matriz que representa a la única transformación lineal que lleva e_i en $e_{\sigma(i)}$. Por lo tanto $I_{\tau\sigma}$ es matriz asociada a la composición de $I_\tau \circ I_\sigma$. De esto se sigue que $I_{\tau\sigma} = I_\tau I_\sigma$, para cualquier $\sigma, \tau \in S_n$. Además, claramente se tiene que $I_{\mathrm{id}} = I$, donde $I \in \mathrm{Gl}_n(\mathbb{F})$ es la matriz identidad. Concluimos que ϕ es un homomorfismo de grupos. Por otro lado $\sigma \in \ker(\phi)$ si y solamente si $e_i = e_{\sigma(i)}$, para todo $i \in \{1, \cdots, n\}$. Esto último es equivalente a qu $\sigma(i) = i$, para todo $i \in \{1, \cdots, n\}$. Se concluye que $\ker(\phi) = \{\mathrm{id}\}$ y por ende ϕ es inyectivo.

ii.- Note que $\mathrm{sgn}(\tau\sigma\tau^{-1}) = \mathrm{sgn}(\tau)\mathrm{sgn}(\sigma)\mathrm{sgn}(\tau)^{-1}$. Ahora bien, como sgn es un homomorfismo de S_n a un grupo abeliano, tenemos que $\mathrm{sgn}(\tau\sigma\tau^{-1}) = \mathrm{sgn}(\tau)\mathrm{sgn}(\tau)^{-1}\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma)$.

iii.- Por [i] basta probar que el signo $\mathrm{sgn}((a, b))$ de la transposición $\tau = (a, b)$ es -1. Note que, en este caso, tenemos que I_τ es la transformación lineal que intercambia la fila a con la fila b de la matriz identidad $I \in \mathrm{Gl}_n(\mathbb{F})$. Por lo tanto $\det(I_\tau) = -1$.

iv.- Se sigue de la definición del homomorfismo sgn que $A_n = \ker(\mathrm{sgn})$. Por lo tanto A_n es un subgrupo normal de S_n. Ahora bien, sabemos que $\mathrm{sgn}((a, b)) = -1$. Por lo que sgn es un homomorfismo sobreyectivo. Concluimos, vía el primer teorema de isomorfía, que $S_n/A_n \cong C_2$, donde C_2 es el grupo cíclico de dos elementos.

4.- **Problema 4:** Sea G un grupo de orden n y sea p el menor primo que divide a n.

i.- Demuestre que todo subgrupo de índice p es normal en G.

ii.- Concluya que si existe $H \leq G$ tal que $[G : H] = 2$ entonces $H \triangleleft G$.

Desarrollo:

i.- Sea $H \leq G$ con $[G:H] = p$ primo. Considere la acción de G sobre el conjunto de clases laterales $X = G/H$, vía:

$$g.(aH) = (ga)H.$$

Esta acción induce un homomorfismo $\pi_H : G \to Biy(X)$ definido por $\pi_H(g) = \sigma_g$, donde $\sigma_g(aH) = g.(aH) = (ga)H$. Observe que:

$$\ker(\pi_H) = \{g \in G : gaH = aH, \forall a \in G\}.$$

Es decir $g \in \ker(\pi_H)$ sí y solamente sí $(a^{-1}ga)H = H$ para cualquier $a \in G$. Esto último equivale a que $(a^{-1}ga) \in H$, $\forall a \in G$. Así tenemos que:

$$K = \ker(\pi_H) = \bigcap_{a \in G} aHa^{-1}$$

Observe que $K \lhd G$, por ser núcleo de un homomorfismo. Además $K \subset eHe^{-1} = H$. Sea $l = [H:K]$, así tenemos que $[G:K] = [G:H][H:K] = pl$. Como X tiene p elementos, tenemos que $G/K \hookrightarrow S_p$, donde S_p es el grupo de biyecciones de p elementos. Luego tenemos que $l|(p-1)!$ y en particular los divisores primos de l son menores a p. Por otro lado, como p es el primo más pequeño que divide a $|G|$ y $l||G|$, tenemos que $l = 1$. Podemos concluir de esto último que $H = K$.

ii.- Si existe $H \leq G$ tal que $[G:H] = 2$, como 2 es el primo más pequeño existente, el resultado se sigue de la parte [i].

5.- **Problema 5:** Sea G un grupo de orden n y S_n el grupo de biyecciones de n elementos. Demuestre que existe un homomorfismo inyectivo $\varphi : G \to S_n$.
Demostración: Considere la acción de G sí mismo, definida por $g.h = gh$, $\forall g, h \in G$. Esta acción de grupo induce un homomorfismo $\rho : G \to \mathrm{Biy}(G)$ donde $\rho(g) = \sigma_g$, para $\sigma_g(h) = g.h = gh$. Observe que como $|G| = n$ tenemos que $\mathrm{Biy}(G) \cong S_n$. Además $\ker(\rho) = \{g \in G : gh = h, \forall h \in G\}$, tomando $h = 1$ tenemos que $\ker(\rho) = \{1\}$. Por lo tanto $\rho : G \to S_n$ es un homomorfismo inyectivo.

6.- **Problema 6*:** Sea G grupo finito, $N \lhd G$ y p un primo tal que $p \nmid |G|$. Considere el conjunto:

$$X = \{(g_1, \cdots, g_p) \in G^p : g_1 g_2 \cdots g_p \in N \text{y } g_p g_{p-1} \cdots g_1 \in N\}.$$

Muestre que p divide a $|X| - |N|$.
Demostración: Observe que, como N es un grupo normal de G, se tiene que $g_1^{-1} g_1 g_2 \cdots g_p g_1 \in N$, es decir $g_2 \cdots g_p g_1 \in N$. Aplicando inductivamente este argumento tenemos que $g_{i+1} g_{i+2} \cdots g_p g_1 \cdots g_i \in N$, para todo $i \in \{0, \cdots, p-1\}$. Aplicando el mismo principio a la otra identidad que define X se tiene que $g_i g_{i-1} \cdots g_1 g_p \cdots g_{i+2} g_{i+1} \in N$, para todo $i \in \{0, \cdots, p-1\}$. Luego tenemos que el grupo cíclico $C_p = \mathbb{Z}/p\mathbb{Z}$ actúa sobre X vía:

$$\overline{i}.(g_1, \cdots, g_p) = (g_{i+1}, g_{i+2}, \cdots, g_p, g_1, \cdots, g_i).$$

Ahora bien, dado que la acción de C_p sobre un X particiona a X en órbitas disjuntas, nosotros podemos calcular el número de X contando el número de elementos en cada órbita. En efecto, tenemos que:

$$|X| = |X^{'}| + \sum_{i=1}^{r} |\mathrm{Orb}(x_i)|,$$

donde X' es el conjunto de puntos fijos por C_p y cada x_i tiene su órbita no trivial, es decir $|\mathrm{Orb}(x_i)| \neq 1$. Por la relación órbita-estabilizador tenemos que $|\mathrm{Orb}(x_i)| = [C_p : \mathrm{Stab}(x_i)] = p$. Por lo tanto p divide a $|X| - |X'|$. En lo que sigue analizaremos X'. Observe que si $(g_1, \cdots, g_p) = (g_{i+1}, \cdots, g_p, g_1, \cdots, g_i)$, para todo i entonces se tiene que $(g_1, \cdots, g_p) = (g, \cdots, g)$, para cierto $g \in G$ tal que $g^p \in N$. Por otro lado en G/N se tiene que $\overline{g}^{|G|} = \overline{e}$. Luego, como $p \nmid |G|$, tenemos que existen $a, b \in \mathbb{Z}$ tales que $1 = ap + b|G|$. Por lo tanto tenemos que $\overline{g} = (\overline{g}^p)^a(\overline{g}^{|G|})^b = \overline{e}$, es decir $g \in N$. De esto se sigue que $|X'| = |N|$ y por lo tanto p divide a $|X| - |N|$.

Ayudantía 2: En esta ayudantía seguiremos estudiando acciones de grupo y comenzaremos nuestro análisis de los teoremas de Sylow. Como ejemplo del trabajo en acciones demostraremos el teorema de Cauchy.

1.- **Problema 1: (Teorema de Cauchy)** Sea G un grupo de orden n y considere la acción de $H = G \times C_p$ sobre G^p vía:

$$(g, a^k)(g_1, \cdots, g_p) = (gg_{1+k}, \cdots, gg_{p+k}),\ \forall g, g_i \in G,$$

donde a es un generador de el grupo cíclico C_p de orden p.

i.- Suponga que G no tiene elementos de orden p. Calcule el número de elementos de cada órbita en G^p.

ii.- Pruebe que bajo la misma hipótesis de [i] tenemos que $p \nmid n$.

iii.- Concluya que si $p|n$ entonces existe un subgrupo H de G con $|H| = p$.

iv.- Concluya que si $n \neq 0$ en $\mathbb{F}_p$ entonces $n^{p-1} = 1$.

Desarrollo:

i.- Sean $O = \text{Orb}((g_1, \cdots, g_p))$ y $S = \text{Stab}((g_1, \cdots, g_p))$ la órbita y el estabilizador de $(g_1, \cdots, g_p) \in G^p$ respectivamente. Recordemos que $|O| = \frac{|H|}{|S|}$. Luego, para calcular el el orden de O, debemos encontrar el número de elementos del estabilizador S. Observe que:

$$(g_1, \cdots, g_p) = (g, a^k)(g_1, \cdots, g_p) = (gg_{1+k}, \cdots, gg_{p+k}),$$

sí y solamente sí $gg_{i+k} = g_i$, $\forall i$. Luego, si $k = 0$, entonces $gg_i = g_i$ y así tenemos que $g = 1$. Por otro lado si $k \neq 0$, entonces $gg_{i+2k} = g_{i+k}$. Luego $g^2 g_{i+2k} = g_i$. Por inducción $g^t g_{i+tk} = g_i$. Luego tenemos que $g^p g_i = g^p g_{i+pk} = g_i$ y por lo tanto $g^p = 1$. Pero, por hipótesis, esto implica que $g = 1$. Esto tiene por consecuencia que $g_1 = g_{1+k} = \cdots = g_{1+pk}$ y por lo tanto la tupla $(g_1, \cdots, g_p)$ tiene todas sus coordenadas iguales. Concluimos que $S = \{e\} \times C_p$, si $g_1 = \cdots = g_p$ o bien $S = \{e\} \times \{e\}$. En particular, tenemos que $|O| = n$, si $g_1 = \cdots = g_p$ y $|O| = np$, en otro caso.

ii.- Recordemos que toda acción de grupo, divide el conjunto sobre el que actúa en órbitas disjuntas. Observe que la órbita de tamaño n es única, pues $O = O((g, \cdots, g)) = O((1, \cdots, 1))$. Luego $n^p = |G^p| = n + npN$, donde N es el número de órbitas de cardinalidad np. Dividiendo por n, obtenemos que $n^{p-1} = 1 + pN$, es decir $p|(n^{p-1} - 1)$. Luego si $p|n$ tenemos que $p|1$, lo que es contradictorio. Por lo tanto $p \nmid n$.

iii.- Por contrapositivo, si $p|n$ entonces existe solución no trivial de $x^p = 1$ en G. Digamos $g \in G$. Tomando $H = \langle g \rangle \leq G$ tenemos lo pedido.

iv.- Observe que $n \neq 0$ en $\mathbb{F}_p$ implica que $p \nmid n$. Tomando el grupo $G = C_n$, donde no existe solución no trivial de la ecuación $x^p = 1$, tenemos que $p|(n^{p-1} - 1)$. Es decir $n^{p-1} = 1$ en $\mathbb{F}_p$.

2.- **Problema 2:** Sea G grupo de orden p^n, donde $n \geq 1$ y p es primo. Demuestre que G tiene un subgrupo normal H_s de orden p^s, para cualquier $s \leq n$.

Demostración: Razonamos por inducción. Si $n = 1$ es trivial. Para $n = 2$, por lo mostrado en el item [iii] del problema anterior aplicado a $Z(G)$, tenemos que existe $H \triangleleft G$, con $|H| = p$. Por otro lado los grupos $G, \{1\} \triangleleft G$ tienen orden p^2 y 1 respectivamente y completan el conjunto de subgrupos que debemos encontrar. Supongamos que la afirmación es cierta para $n \in \mathbb{N}$. Sea G grupo de orden p^{n+1}. Entonces, por item [iii] del problema anterior

aplicado a $Z(G)$, tenemos que existe $H \triangleleft G$ con $|H| = p$. Equivalentemente G/H es un grupo de orden $|G/H| = p^n$. Por hipótesis de inducción, existe $K_s/H \triangleleft G/H$, con $|K_s/H| = p^s$. Luego $|K_s| = p^{s+1}$ y por ende definimos $H_s = K_{s-1}$. Si tomamos $g \in G, x \in K_s$ tenemos que $gxg^{-1} \in H_sH \subset H_s$. Por lo tanto $H_s \triangleleft G$. Luego tenemos grupos normales de todos los ordenes posibles. Observe que $H_0 = \{1\}$ y $H_1 = H$.

3.- **Problema 3:** Demuestre lo siguiente:

i.- Sea G un grupo de orden 66. Pruebe que existe $K \triangleleft G$ con $|K| = 33$.

ii.- Sea G un grupo de orden pqr, con $p < q < r$ primos y $pq = 2 + 5r$. Pruebe que existe $K \triangleleft G$ con $|K| = qr$.

Desarrollo:

i.- Observe que $n_{11} \in \{1, 2, 3, 6\}$ y $n_{11} \equiv 1 (\text{mod } 11)$. Por lo tanto, tenemos que $n_{11} = 1$, es decir existe un único 11-Sylow H en G. Como los p-subgrupos de Sylow se obtienen conjugando un p-subgrupo de Sylow fijo, tenemos que $H \triangleleft G$. Sea T un 3-subgrupo de Sylow cualquiera. Como $H \triangleleft G$ tenemos que $HT = \{ht : h \in H, t \in T\}$ es un subrgupo de G. Además se cumple que $|HT| = |H||T|/(|H \cap T|)$. Pero si $x \in H \cap T$ entonces $|x|$ es divisible por 3 y 11. Como $(3, 11) = 1$, tenemos que $|x| = 1$, es decir $H \cap T = \{e\}$, por lo cual $|HT| = |H||T| = 33$. Ahora bien como $[G : HT] = 2$, concluimos que $K = HT$ es un subgrupo normal de G de orden 33.

ii.- Sea n_r el número de r-subgrupos de Sylow en G. Por los teoremas de Sylow, tenemos que $n_r \in \{1, p, q, pq\}$. Por los mismo teoremas sabemos que $n_r \equiv 1 (\text{mod } r)$. Por lo tanto si $n_r = p$ tenemos que $r|p - 1$, donde $r > p - 1 \geq 0$. Esto nos lleva a una contradicción. Por el mismo argumento tenemos que $n_r \neq q$. Ahora bien, como $pq \equiv 2 (\text{mod } r)$, tenemos que $n_r \neq pq$. Esto prueba que $n_r = 1$, es decir existe un r-subgrupo de Sylow $H \triangleleft G$. Sea T un q-subgrupo de Sylow. Por el mismo argumento que el dado en [i], tenemos que HT es un subgrupo de G. Ahora bien, como $[G : HT] = p$ es el mínimo primo que divide a $|G|$, tenemos que $K = HT$ es un subgrupo normal de G de orden qr.

4.- **Problema 4*:** Sea G un grupo de orden p^2q, donde p y q son primos distintos. Pruebe que G tiene un subgrupo normal distinto de G y $\{e\}$.

Demostración: Primero supongamos que $p > q$. Entonces $n_p \in \{1, q\}$. Si $n_p = q$, entonces tenemos que $p|q - 1$. En particular, tenemos que $p \leq q - 1$. Esto nos lleva a una contradicción. Luego $n_p = 1$ y por lo tanto existe $H \triangleleft G$ con $|H| = p^2$. Supongamos ahora que $p < q$. Entonces tenemos que $n_q \in \{1, p, p^2\}$. Observe que, por el mismo argumento que el dado para $p > q$, tenemos que $n_q \neq p$. Supongamos que $n_q = p^2$. Entonces se cumple que q divide a $p^2 - 1 = (p - 1)(p + 1)$. Como $q \nmid p - 1$, tenemos que $q|p + 1$. En particular, tenemos que $q \leq p + 1$ y por ende $p = q + 1$. Como p, q son primos, concluimos que $q = 3$ y $p = 2$, es decir $|G| = 12$. Supongamos que $n_2 = 3$ y $n_3 = 4$. En este caso, tenemos por conteo de elementos, que en los 2-subgrupos de Sylow hay a los menos $2 \cdot 1 + 3$ elementos distintos de la identidad y en los 3-subgrupos de Sylow hay a lo menos $2 \cdot 4$ de estos elementos. Por lo tanto $|G| \geq 14$, lo que claramente es contradictorio. Concluimos que $n_q = 1$ y por lo tanto existe $H \triangleleft G$ con $|H| = q$. Esto prueba lo pedido.

5.- **Problema 5:** Determine de cuantas maneras esencialmente distintas se puede pintar con n colores un triangulo equilatero hecho de palitos de helado.
Desarrollo: Considere la acción de $G = D_3$ sobre el conjunto X de todas las coloraciones del triangulo realizdas con n colores. Nuestro problema radica en calcular $|G \setminus X|$. Para ello usaremos la identidad:

$$|G \setminus X| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|.$$

Observe que en G está compuesto por 2 rotaciones de orden 3, la identidad y 3 reflexiones que cruzan un vertice y un lado. Note que toda rotación de orden 3 cumple que un elemento de X es fijo por esta, si tiene los mismos colores en todas las aristas. Por lo tanto existen n triangulos coloreados que son fijos por una reflexión de orden 3. Por otro lado, un elemento de X es fijo por la acción de una reflexión si tiene los mismos colores en las aristas que permuta dicha reflexión. Es decir, si dicho elemento tiene 2 aristas de igual color y la tercera de cualquier color. Luego tenemos $2n$ triangulos coloreados que son fijas por una reflexión. Finalmente, como $|\mathrm{Fix}(id)| = 3n$, concluimos que:

$$|G \setminus X| = \frac{1}{6}(n^3 + 2n + 3n^2).$$

Ayudantía 3: En esta ayudantía seguiremos estudiando el teorema se Sylow. En particular, clasificaremos grupos de ciertos órdenes. En lo que sigue $\text{Sly}_p(G)$ corresponde al conjunto de p-subgrupos de Sylow del grupo G.

1.- **Problema 1:** Sea G grupo y $H \leq K \leq G$.

i.- **(Argumento de Frattini)** Suponga que $H \triangleleft G$. Pruebe que si $P \in \text{Syl}_p(H)$ entonces $G = N_G(P)H$.

ii.- **(P-grupos son característicos)** Demuestre que si $P \in \text{Syl}_p(H)$, $P \triangleleft H$ y $H \triangleleft K$ entonces $P \triangleleft K$.

iii.- Deduzca que si $P \in \text{Syl}_p(G)$ entonces $H = N_G(P)$ cumple con $N_G(H) = H$.

Desarrollo:

i.- Sabemos que $G \supseteq N_G(P)H$. Por lo tanto debemos demostrar la contención inversa. Observe que si P es un p-subgrupo de Sylow de H, entonces $\text{Syl}_p(H) = \{hPh^{-1} : h \in H\}$. Sea $g \in G$, como $H \triangleleft G$, tenemos que $gPg^{-1} \subseteq H$. Luego, como $|gPg^{-1}| = |P|$ tiene exponente p maximal en $|G|$ y por lo tanto en $|H|$, tenemos que $gPg^{-1} \in \text{Syl}_p(H)$. Por lo tanto se cumple que $gPg^{-1} = hPh^{-1}$, para cierto $h \in H$. Es decir $gh^{-1} \in N_G(P)$. Luego $g \in N_G(P)H$. Concluimos que $G = N_G(P)H$.

i.- Sabemos que $P \triangleleft H$ sí y solamente sí P es el único p-subgrupo de Sylow de H. Sea $g \in K$ entonces, como $H \triangleleft K$, tenemos que $gPg^{-1} \subset H$. Como $|gPg^{-1}| = |P|$ tenemos que gPg^{-1} es un p-subgrupo de Sylow de H. Luego, como P es el único p-subgrupo de Sylow de H, tenemos que $gPg^{-1} = P$.

ii.- Si $P \in \text{Syl}_p(G)$, entonces $P \triangleleft H$, por definición de H. Como $H \triangleleft N_G(H)$ tenemos que $P \triangleleft N_G(H)$. Es decir $N_G(H) \subseteq H = N_G(P)$, pues $N_G(P)$ es el maximo subgrupo de G tal que P es normal. Además siempre se cumple que $H \subseteq N_G(H)$. Por lo tanto $H = N_G(H)$, es decir $N_G(N_G(P)) = N_G(P)$.

2.- **Problema 2*:** Sea G un grupo finito con la propiedad de que para todo H, K subgrupos de G se cumple que $HK \subseteq KH$. Demuestre que para todo p primo, el grupo G tiene un único p-subgrupo de Sylow, el cual es normal.
Demostración: Considere P, Q dos p-subgrupos de Sylow cualquiera de G. Entonces por la propiedad de G se cumple que $PQ \subseteq QP$. Probemos que, bajo estas hipótesis, PQ es un subgrupo de G. En efecto, claramente $e \in PQ$ y además si $x_1, x_2 \in P$ y $y_1, y_2 \in Q$ se tiene que:

$$x_1y_1x_2y_2 = x_1\overline{xy}y_2,$$

para ciertos $\overline{x} \in P, \overline{y} \in Q$ tales que $y_1x_2 = \overline{xy}$. Por lo tanto $PQ \leq G$. Ahora bien, si $|G| = p^n m$, donde $(p, m) = 1$, tenemos que $|P| = |Q| = p^n$. Por lo tanto el cardinal del compósito PQ es:

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^{2n-t},$$

donde $t \in \{0, \cdots, n\}$ cumple con $|P \cap Q| = p^t$. Por otro lado, por el teorema de Lagrange, tenemos que $|PQ|$ divide a $|G|$. Concluimos que $t = n$ y por lo tanto $P = P \cap Q = Q$. De esto se sigue que G tiene un único p-subgrupo de Sylow. Por último, como los p-subgrupos de Sylow de un grupo dado son conjugados entre si, se deduce que dicho p-grupo es normal en este caso.

3.- **Problema 3:** Encuentre todos los grupos de orden 39 salvo isomorfismo.
Desarrollo: Sea G un grupo de orden 39. Observe que $n_{13}|3$ y $n_{13} \equiv 1(13)$.

Por lo tanto $n_{13} = 1$. Es decir existe un único 13- subgrupo de Sylow $T \triangleleft G$. Por otro lado $n_3|13$ y $n_3 \equiv 1(3)$. Luego tenemos que $n_3 = 1$ o $n_3 = 13$. Dividamos el análisis en casos:

a.- Supongamos que $n_3 = 1$. Entonces existe un 3- subgrupo de Sylow $S \leq G$ normal en G. Luego, como $|G| = |S||T|$ y $S \cap T \subset \{x \in G : |x||3, 5\} = \{e\}$, tenemos que $G \cong C_3 \times C_{13} \cong C_{39}$.

b.- Por otro lado, si $n_3 = 13$, entonces tenemos que existen 13 subgrupos de orden 3 en G. Sea $S = \{1, a, a^2\}$ grupo de orden 3. Como $T \triangleleft G$ tenemos que $aTa^{-1} = T$. Si $T = \{1, b, \cdots, b^{12}\}$ entonces $aba^{-1} = b^i$, cierto $i \in \{1, \cdots, 12\}$. Observe que, por inducción, $ab^k a^{-1} = b^{ik}$ y $a^n ba^{-n} = b^{i^n}$. Luego se tiene que $b = a^3 ba^{-3} = b^{i^3}$, es decir $i^3 \equiv 1(13)$. Por lo tanto $i \in \{1, 3, 9\}$. Observe que si $i = 1$ entonces G abeliano y por lo tanto $n_3 = 1$. Concluimos que:

$$G \cong G_1 = \langle a, b : b^{13} = a^3 = 1,\ aba^{-1} = b^3 \rangle,$$

o bien:

$$G \cong G_2 = \langle a, b : b^{13} = a^3 = 1,\ aba^{-1} = b^9 \rangle.$$

Observe que $G_2 \cong G_2$, pues $\phi : G_1 \to G_2$ definido por $\phi(a) = a^2, \phi(b) = b$ es isomorfismo. Observe ϕ que está bien definida pues $\phi(ab) = a^2 b = ab^9 a = b^{81} a^2 = b^3 a^2 = \phi(b^3 a)$. Por lo tanto existen solo dos grupos de orden 39 módulo isomorfismo.

4.- **Problema 4:** Sean p, q primos tales que $p > q$.

i.- Suponga que $p \equiv 1(\text{mod } q)$. Muestre que existe un grupo no abeliano de orden pq.

ii.- Suponga que $q \nmid p - 1$. Pruebe que todo grupo de orden pq es cíclico.

Desarrollo: Sea G un grupo de orden pq. Es facil ver que $n_p \in \{1, q\}$ cumple con $n_p = 1$, dado que $p > q$. Por lo tanto, en G existe un único p-subgrupo de Sylow $P \triangleleft G$. En lo que sigue haremos uso de esta observación.

i.- Supongamos que $P = \langle t \rangle$. Considere $H = \text{Aut}(P)$. Es un resultado conocido que $H \cong C_{p-1}$, dado que todos los automorfismos θ de P cumplen con $\theta(t) = t^i$, donde $(i, p) = 1$. Luego, como $q|p - 1$, por teorema de Cauchy tenemos que existe $\theta \in H$ tal que $|\theta| = q$. Sea $S = \langle s \rangle$ un q-subgrupo de Sylow de G. Observe que $SP = G$. Luego el grupo G, de existir, debe estar generado por los elementos s y t, los cuales deben cumplir la relación $sts^{-1} = t^i$, para cierto $i \in \mathbb{N}$. Por lo analizado en el problema 2, tenemos que $t^{i^q} = t$. Ahora bien, siempre existe un $i \in \mathbb{N}$ tal que $i \neq 1(\text{mod } p)$ e $i^q \equiv 1(\text{mod } p)$, puesto que, por lo dicho anteriormente, siempre existe un automorfismo de orden q. Note que, para concluir el hecho anterior pudo haberse usado el teorema de Euler. Concluimos que siempre existe el grupo no abeliano:

$$G = \langle t, s : t^p = 1, s^q = 1, sts^{-1} = t^i \rangle,$$

el cual tiene orden pq.

ii.- En este caso, tenemos que $n_q = 1$, dado que $n_q \in \{1, p\}$. Por lo tanto en G existe un único q-subgrupo de Sylow $Q \triangleleft G$. Claramente $P \cap Q = \{e\}$ y $|P||Q| = |G|$. Concluimos que $G \cong P \times Q \cong C_p \times C_q \cong C_{pq}$.

5.- **Problema 5*:** Sea $p \neq 2$ un número primo y G es un grupo de orden $2p$. Pruebe que $G \cong C_{2p}$ o bien $G \cong D_{2p}$.

Demostración: Por los teoremas se Sylow existen $T \leq G$ un 2-subgrupo de Sylow de G y $S \leq G$ un p-subgrupo de Sylow de G. Observe que $n_p|2$ y $n_p \equiv 1(p)$. Luego tenemos que $n_p = 1$, lo que equivale a que exista un único p-subgrupo de Sylow $S \triangleleft G$. Por otro lado, tenemos que $n_2 \in \{1, p\}$. Dividamos nuestro análisis dependiendo del valor de n_2.

a.- Supongamos que $n_2 = 1$. Entonces $T \triangleleft G$. Además $T \cap S = \{1\}$, pues si $x \in T \cap S$ entonces $|x||2, p$, por ende $|x| = 1$. Por lo tanto $G \cong T \times S \cong C_p \times C_2 \cong C_{2p}$.

b.- Supongamos que $n_2 = p$. Si $T = \langle b \rangle$ y $S = \langle a \rangle$ entonces $bab^{-1} = a^i$, donde $i^2 \equiv 1(p)$. Por lo tanto $i \equiv 1(p)$ o bien $i \equiv -1(p)$. Si $i \equiv 1(p)$, entonces $ab = ab$ y por ende G es abeliano, lo que nos lleva a una contradicción pues $n_2 \neq 1$. Por lo tanto $bab^{-1} = a^{-1}$. Concluimos que en este caso se cumple que:

$$G \cong \langle a, b : a^p = b^2 = 1,\, bab^{-1} = a^{-1} \rangle \cong D_{2p}.$$

Observe que este problema pudo haberse hecho con las mismas herramientas expuestas en el problema 4 al consideras las soluciones de la ecuación $i^2 \equiv 1(\mod p)$ al estudiar los homomorfismos de $T \to \mathrm{Aut}(S)$.

Ayudantía 4: En esta ayudantía trabajaremos con productos semidirectos.

1.- **Problema 1:** Si $G = HN$ con $H \cap N = \{1\}$ y $N \triangleleft G$, entonces para cualquier $g \in G$ existen únicos $h \in H, n \in N$ tales que $g = nh$. Además $G \cong N \rtimes_\phi H$, para $\phi(h)(n) = hnh^{-1}$.
Demostración: De la definición de composito se sigue que para cualquier $g \in G$ existen elementos $h \in H, n \in N$ tales que $g = nh$. Demostremos la unicidad de esta última expresión. En efecto, si $g = n_1h_1 = n_2h_2$, tenemos que $n_2^{-1}n_1 = h_2h_1^{-1} \in H \cap N$. Por lo tanto $n_1 = n_2$ y $h_1 = h_2$. Con esto mencionado, considere la función sobreyectiva $\rho : G \to N \rtimes_\phi H$ definida por $\rho(nh) = (n, h)$. Por la unicidad anterior, tenemos que $\rho(e) = (e, e)$ y que:

$$\rho(n_1h_1n_2h_2) = \rho(n_1h_1n_2h_1^{-1}h_1h_2) = (n_1h_1n_2h_1^{-1}, h_1h_2) = \rho(n_1h_1)\rho(n_2h_2).$$

Concluimos que ρ es un homomorfismo sobreyectivo, y como $\ker(\rho) = \{e\}$, obtenemos que ρ es un isomorfismo.

2.- **Problema 2:** Para $n > 2$ considere $\phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}\,(\mathbb{Z}/n\mathbb{Z})$ el homomorfismo definido por $\phi(a)(x) = (-1)^a x$. Demuestre que $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$.
Demostración: Sabemos que $D_{2n} = \langle a, b : a^n = b^2 = 1, bab^{-1} = a^{-1}\rangle$. Además $N = \langle a\rangle \triangleleft D_{2n}$, pues $bab^{-1} = a^{-1} \in N$, donde N es un grupo cíclico de orden n. Considere $H = \langle b\rangle$ un 2-Sylow de D_{2n} de orden 2. Observe que $b \notin N$. Luego $|N \cap H| = 1$, y por ello $H \cap N = \{1\}$. Ahora bien, como $N \triangleleft D_{2n}$, HN tiene estructura de grupo, y como $|HK| = \frac{|H||N|}{|H\cap N|} = |H||N| = |D_{2n}|$, tenemos que $D_{2n} = HN$. Del problema 1 se sigue que $D_{2n} \cong N \rtimes_\psi H$, donde $\psi(b)(a) = a^{-1}$. Identificando los grupos N y H con cocientes de $\mathbb{Z}$ y escribiendo ψ aditivamente, concluimos que $G \cong \mathbb{Z}/n\mathbb{Z} \rtimes_\phi \mathbb{Z}/2\mathbb{Z}$.

3.- **Problema 3:** Sean H, H' y N grupos y suponga que $f : H \to H'$, $d : H \to \mathrm{Aut}(N)$ y $d' : H' \to \mathrm{Aut}(N)$ son homomorfismos de grupos tales que $d = d' \circ f$.

i.- Encuentre un homomorfismo $g : N \rtimes_d H \to N \rtimes_{d'} H'$ que extienda f.

ii.- Demuestre que f es un isomorfismo si y solamente si g también lo es.
Desarrollo:

i.- Considere el homomorfismo $g : N \rtimes_d H \to N \rtimes_{d'} H'$ definido por $g(n, h) = (n, f(h))$. Observe que g está bien definido, pues:

$$g(n_1, h_1)g(n_2, h_2) = (n_1, f(h_1))(n_2, f(h_2)) = (n_1d'(f(h_1))(n_2), f(h_1h_2)).$$

Luego, como $d = d' \circ f$, tenemos que $g(n_1, h_1)g(n_2, h_2) = g((n_1, h_1)(n_2, h_2))$. Note además que la función g restringida a $\{0\} \times H$ es $g|_{\{0\}\times H} = f$.

ii.- Observe que $\ker(g) = \{0\} \times \ker(f)$ y que $\mathrm{Im}(g) = H \times \mathrm{Im}(f)$, como conjuntos. De esto se sigue que f es biyectiva si y solamente si g también lo es.

4.- **Problema 4:** Clasifique todos los grupos de orden 20 salvo isomorfía.
Desarrollo: Sea G un grupo de orden 20. Usando la notación de la teoría de Sylow, tenemos que $n_5 = 1$. Luego existe un único 5-sugbrupo de Sylow en G, el cual es normal. Sea N dicho subgrupo. Además $n_2 \in \{1, 5\}$.

i.- Supongamos que $n_2 = 1$. Entonces existe un único 2-sugbrupo de Sylow en G, el cual es normal. Sea H dicho subgrupo. Es directo de $(|N|, |H|) = 1$ que $N \cap H = \{e\}$. Luego, como $N, H \triangleleft G$ y $G = NH$ tenemos que $G \cong N \times H$. Por último, como $|H| = 4$, tenemos que $H \cong C_2 \times C_2$ o bien $H \cong C_4$. Esto

implica que $G \cong C_{20}$ o bien $G \cong C_{10} \times C_2$. Note que estos grupos son no isomorfos, pues el primero tiene un elemento de orden 20 mientras que el segundo no.

ii.- Considere $n_2 = 5$ y sea H un 2-Sylow de G. Mediante el mismo argumento que se dió en [i], se prueba que $G = NH$, donde $N = \langle n \rangle \lhd G$. Luego, por la proposición 1, tenemos que $G \cong N \rtimes_\phi H$, para cierto $\phi : H \to \mathrm{Aut}(N)$. Note que $\mathrm{Aut}(N) \cong C_4$ y observe que si ϕ es trivial, entonces $G \cong H \times N$, el cual es un grupo abeliano. Por ende volvemos a la clasificación hecha en [i].

Si suponemos que $H \cong C_2 \times C_2 \cong \langle a, b : a^2 = b^2 = 1, ab = ba \rangle$ entonces tenemos que los únicos homomorfismos no triviales $\phi_1, \phi_2, \phi_3 : C_2 \times C_2 \to \mathrm{Aut}(N)$ son los definidos por:

$$\phi_1((a,b)) = (\mathrm{id}, -\mathrm{id}),$$
$$\phi_2((a,b)) = (-\mathrm{id}, \mathrm{id}),$$
$$\phi_3((a,b)) = (-\mathrm{id}, -\mathrm{id}).$$

Considere los automorfismos $f_1, f_2 : H \to H$ definidos por $f_1(a,b) = (b,a)$ y $f_1(a,b) = (ab, b)$. Es directo de la defínción sobre los generadores que $\phi_1 \circ f_1 = \phi_2$ y que $\phi_1 \circ f_2 = \phi_3$. Del problema 2, concluimos que los tres automorfismos dan origen a grupos isomorfos. Luego en este caso solo tenemos un grupo módulo isomorfía, el cual es no abeliano. Del problema 1, se sigue que dico grupo es:

$$G_0 = \langle a, b, n : a^2 = b^2 = n^5 = e, ana^{-1} = n^{-1}, bnb^{-1} = n^{-1} \rangle.$$

Por otro lado, si $H \cong C_4 = \langle a \rangle$, tenemos que existen tres homomorfismos $\psi_1, \psi_2, \psi_3 : C_4 \to (C_7)^*$ no triviales, los cuales estan en correspondencia con las soluciones no triviales de $x^4 \equiv 1 (\mod 7)$, y son:

$$\psi_1(a) = 2\mathrm{id},$$
$$\psi_2(a) = 3\mathrm{id},$$
$$\psi_3(a) = -\mathrm{id},$$

donde $N\mathrm{id}$ es el automorfismo $x \to x^N$. Note que si escribimos los grupos inducidos por ψ_1 y ψ_2 son:

$$G_1' = \langle a, n : a^4 = n^5 = e, ana^{-1} = n^2 \rangle$$

$$G_2' = \langle a, n : a^4 = n^5 = e, ana^{-1} = n^3 \rangle$$

Ahora bien, es sencillo porbar que los elementos $a^3, n \in G_1'$ cumplen con las mismas relaciones que $a, n \in G_2'$. De esto se sigue que ambos grupos son isomorfos. Luego, en este caso, tenemos dos grupos de orden 20, posiblemente no isomorfos. A saber:

$$G_1 = \langle a, n : a^4 = n^5 = e, ana^{-1} = n^2 \rangle.$$

$$G_3 = \langle a, n : a^4 = n^5 = e, ana^{-1} = n^4 \rangle.$$

Del problema 1 se sigue que, para cualquier homomorfismo $\phi : H \to \mathrm{Aut}(N)$, se tiene que $\ker(\phi) = \{h \in H : hnh^{-1} = n, \forall n \in N\} = C_H(N)$ es un invariante del grupo (por ser el centralizador de un p-Sylow en un q-Sylow).

Luego, como $\ker(\phi_1) = \{e, a^2\}$ y $\ker(\phi_3) = \{e\}$, se tiene que G_1 no es isomorfo a G_2. Por otro lado, como G_1 y G_2 tienen por 2-Sylow al grupo C_4 y G_0 tiene por 2-Sylow al grupo de Klein, tenemos que G_1 y G_2 no son isomorfos a G_0. Concluimos que existen 5 grupo de orden 20. A saber, los grupos no abelianos G_0, G_1, G_3 y los grupos abelianos C_{20} y $C_{10} \times C_2$.

5.- **Problema 5*:** Determine cuantos grupos no isomorfos existen de orden 88 y que contienen al menos un elemento de orden 8.
Desarrollo: Sea G un grupo de orden 88. Por los teorema de Sylow, tenemos que $n_{11} = 1$ y por ende existe un único 11-Sylow N en G, el cual es normal. Note que G tiene un subgrupo cíclico H de orden 8 el cual es cíclico. Luego como dicho subgrupo es un 2-Sylow, tenemos que los 2-subgrupos de Sylow de G son todos cíclicos. Supongamos que existe solamente un 2-Sylow en G. Usando las mismas herramientas del problema 4 podemos concluir, que en este caso, se tiene que $G \cong H \times N \cong C_8 \times C_{11} \cong C_{88}$. Supongamos ahora que $n_2 = 11$ y digamos que $H = \langle a \rangle$ y que $N = \langle b \rangle$. En dicho caso, por el problema 1, tenemos que G es un producto semidirecto de N y H dado por un homomorfismo $C_8 \cong H \to \mathrm{Aut}(N)$. Como la única condición sobre la imagen de a en $\mathrm{Aut}(N)$ es que tenga orden 8, tenemos que dicha imagen está descrita por un homomorfismo que envia $b \to b^x$, donde $x^8 \equiv 1(\mod 11)$. Ahora bien, si $x^8 \equiv 1(\mod 11)$, se tiene que x^4 es una raiz de 1 en $\mathbb{Z}/11\mathbb{Z}$. Por ende $x^4 \equiv 1(\mod 11)$ o bien $x^4 \equiv -1(\mod 11)$. Pero en $\mathbb{Z}/11\mathbb{Z}$ no existen raices de -1. Por lo tanto $x^4 \equiv 1(\mod 11)$. Empleando el mismo argumento deducimos que $x^2 \equiv 1(\mod 11)$ y por lo tanto $x \equiv 1$ o $-1(\mod 11)$. De esto se sigue que el único homomorfismo no trivial de $H \to \mathrm{Aut}(N)$ es ψ definido por $\psi(a)(b) = b^{-1}$. Por ende el único grupo no abeliano que cumple nuestras hipótesis es:

$$G_0 = \langle a, b : a^8 = b^{11} = e, aba = b^{-1} \rangle.$$

Concluimos que existen dos grupos no isomorfos de orden 88 que contienen al menos un elemento de orden 8.

6.- **Problema 6:** Sea F un cuerpo y $G \subset \mathbb{M}_2(F)$ el grupo de matrices triagulares superiores. Pruebe que $G \cong F \rtimes (F^* \times F^*)$.
Desarrollo: Considere el subgrupo D de matrices diagonales y U el subgrupo definido por:

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in F \right\}.$$

Note que toda matriz $g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in G$ puede escribirse como:

$$g = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} 1 & a^{-1}b \\ 0 & 1 \end{pmatrix}.$$

Por lo tanto $G = DU$. Claramente $D \cap U = \{\mathrm{id}\}$. Además $U \triangleleft G$, puesto que:

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & y^{-1} \end{pmatrix} = \begin{pmatrix} 1 & y^{-1}xa \\ 0 & 1 \end{pmatrix}. \tag{2}$$

Por el problema 1, deducimos que $G \cong U \rtimes_\phi D$, para ϕ el homomorfismo definido por 2. Por último, como $U \cong F$ y $D \cong F^* \times F^*$, se tiene lo pedido.

Ayudantía 5: En esta ayudantía repasaremos lo visto en las anteriores, con el objetivo de preparar la primera prueba.

1.- **Problema 1*:** Sea p primo tal que $\text{car}(\mathbb{F}) = p$. Determine todas las clases de conjugación de los elementos de orden p en $G = \text{Gl}_2(\mathbb{F})$.
Desarrollo: Sea $A \in G$ una matriz de orden p, es decir $A^p = \text{id}$ y $A \neq \text{id}$. Como el cuerpo $\mathbb{F}$ tiene característica p, se cumple que $(A-\text{id})^p = A^p - \text{id} = 0$. Luego, la matriz $B = A-\text{id}$ es nilpotente. Es un hecho conocido de álgebra lineal, que cualquier matriz nilpotente en $\mathbb{M}_2(\mathbb{F})$ es conjugada a:

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

Luego existe una matriz invertible $g \in G$ tal que $A-\text{id} = gNg^{-1}$. Concluimos que $A = g(N+\text{id})g^{-1}$ y que por lo tanto existe solo una clase de conjugación para elementos de orden p en G.

2.- **Problema 2:** Sea G un grupo de orden 105. Pruebe que si G tiene un 3-Sylow normal, entonces G es abeliano.
Desarrollo: Observe que $|G| = 3 \cdot 5 \cdot 7$. Por ende $n_5 \in \{1, 3, 7, 21\}$ y $n_5 \equiv 1(\ 5\ )$. Por lo tanto $n_5 = 1$ o bien $n_5 = 21$. De igual manera, $n_7 \in \{1, 3, 5, 15\}$ y $n_7 \equiv 1(\ 7\ )$. Por lo que $n_7 = 1$ o 15. En el caso en que $n_7 = 15$ y $n_5 = 21$, como cualquier elementos en la intersección entre 5 o 7-Sylow genera todo el grupo, tenemos que en G existen a lo menos $15 \cdot 6 + 21 \cdot 4 = 174$ elementos. Esto nos lleva a una contradicción. Por lo tanto alguno de los Sylow anteriores es normal. Dividimos nuestro estudio de acuerdo al caso.

Si $n_5 = 1$, entonces tenemos un 3-subgrupo de Sylow $N \triangleleft G$ y un 5-subgrupo de Sylow $K \triangleleft G$. Considere $H = NK$, el cual es un subgrupo normal de G, y sea S un 7-subgrupo de Sylow de G. Por las mismas cuentas que hemos hecho en las ayudantías anteriores, tenemos que $HS = G$ y $H \cap S = \{e\}$. Por lo tanto G es isomorfo a algún producto semidirecto de H con S, determinado por un homomorfismo $\phi : S \to \text{Aut}(H)$. Note que $H \cong C_{15}$, pues nuevamente por lo teoremas de Sylow, se puede deducir que el único grupo de orden 15 es el cíclico. Luego Aut(H) $\cong (\mathbb{Z}/15\mathbb{Z})^*$, el cual tiene tantos elementos como número relativamente primos a 15 existen y sean menores que este. Concluimos que $|\text{Aut}(H)| = 8$. Luego el único homomorfismo $\phi : S \to \text{Aut}(H)$ es el trivial (por cuestión de el orden de los grupos). Concluimos entonces que $G \cong S \times H \cong \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/105\mathbb{Z}$.

Si $n_7 = 1$, entonces tenemos un 3-subgrupo de Sylow $N \triangleleft G$ y un 7-subgrupo de Sylow $K \triangleleft G$. Considere $H = NK$, el cual es un subgrupo normal de G, y sea S un 5-subgrupo de Sylow de G. Por un razonamiento anaálogo al antrior, tenemos que $HS = G$ y $H \cap S = \{e\}$. Luego G es isomorfo a algún producto semidirecto de H con S, determinado por un homomorfismo $\phi : S \to \text{Aut}(H)$. Note que $H \cong C_{21}$, por los teoremas de Sylow (Ejercicio). Luego Aut(H) $\cong (\mathbb{Z}/21\mathbb{Z})^*$, el cual tiene tantos elementos como número relativamente primos a 21 existen y sean menores que este. Deducimos que $|\text{Aut}(H)| = 12$. Luego el único homomorfismo $\phi : S \to \text{Aut}(H)$ es el trivial. Concluimos entonces que $G \cong S \times H \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z} \cong \mathbb{Z}/105\mathbb{Z}$.

3.- **Problema 3:** Demuestre que los 3-subgrupos de Sylow de S_6 son isomorfos a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Demostración: Note que el subgrupo $N = \langle (123), (456) \rangle \subset S_6$ tiene orden 9 y es isomorfo a $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Esto se debe a que las tuplas (123) y (456) son disjuntas. Por otro lado, el orden de S_6 es $6! = 5 \cdot 3^2 \cdot 2^4$. Luego todo 3-subgrupo de Sylow de S_6 tiene orden 9 y, por los teoremas de Sylow, podemos concluir que es conjugado a N. En particular dichos 3-subgrupos son isomorfos a N, de lo que se sigue lo pedido.

Ayudantía 6: En esta sesión estudiaremos dos tipos especiales de grupos denominados solubles y nilpotentes.

1.- **Problema 1:** Sean G, H, K tres grupos tales que $1 \to^f H \to G \to^g N \to 1$ es una sucesión exacta.

i.- Mustre que si H y N son grupos solubles entonces G también lo es.

ii.- Deduzca que si $H \triangleleft G$ es soluble y su cociente G/N es soluble, entonces G es soluble.

iii.- Demuestre que S_3 es un grupo soluble.

Desarrollo:

i.- Para hacer más simple esta demostración identificaremos H con su subgrupo imagen en G. Dado que N es un grupo soluble considere la series de composición:

$$\{e_N\} = N_0 \triangleleft N_1 \triangleleft \cdots \triangleleft H_n = H,$$

donde N_{i+1}/N_i es un grupo abeliano para todo $i \in \{1, \cdots, n-1\}$. Al tomar preimagenes por g en la serie anterior obtenemos:

$$\ker(g) = g^{-1}(N_0) \subset g^{-1}(N_1) \subset \cdots \subset g^{-1}(H_n) = G. \tag{3}$$

Note que el homomorfismo g induce homomorfismos $g_i : g^{-1}(N_{i+1}) \to N_{i+1}/N_i$ tales que $\ker(g_i) = g^{-1}(N_i)$. Esto implica que $g^{-1}(N_i) \triangleleft g^{-1}(N_{i+1})$ y que su cociente es abeliano. Ahora bien, como $H = \ker(g)$, tenemos que podemos considerar la serie de composición de cociente abeliano:

$$\{e_G\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_m = H. \tag{4}$$

Yuxtaponiendo a la serie (3), la serie (4), obtenemos una serie de composición para G, la cual cumple con las propiedades deseadas.

ii.- Considere la sucesión exacta $1 \to H \to G \to G/H \to 1$ y aplique el item [i].

iii.- Considere el subgrupo normal $A_3 \triangleleft S_3$, el cual es abeliano, pues tiene 3 elementos y cuyo cociente es $G/A_3 \cong \mathbb{Z}/2\mathbb{Z}$. Aplicando el item [ii] a este caso particular podemos deducir que S_3 es un grupo soluble.

2.- **Problema 2:** Considere el grupo $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in F^*, b \in F \right\}$.

i.- Encuentre una serie de composición de cociente abeliano para G.

ii.- Calcule el subgrupo de conmutadores de G y con ello de una nueva demostración de la solubilidad de G.

Desarrollo:

i.- Considere el homomorfismo $\phi : G \to F^* \times F^*$ definido por:

$$\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, c).$$

Dicho homomorfismo el claramente sobreyectivo y su núcleo es el subgrupo $N = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\}$. Esto muestra que N es un subgrupo normal de G, cuyo cociente es isomorfo al grupo abeliano $F^* \times F^*$. Luego como $N \cong F$ tenemos la serie de composición de cociente abeliano:

$$\{\mathrm{id}\} \triangleleft N \triangleleft G.$$

Esto prueba que G es un grupo soluble.

ii.- Calculemos el conmutador de dos matrices cualquiera $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in G$. En efecto dicho conmutador es:

$$g = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix}\begin{pmatrix} x^{-1} & -yx^{-1}z^{-1} \\ 0 & z^{-1} \end{pmatrix},$$

Multiplicando dichas matrices se obtiene que:

$$g = \begin{pmatrix} 1 & -zy^{-1} - bc^{-1}y^{-1}x + azc^{-1}y^{-1} + bc^{-1} \\ 0 & 1 \end{pmatrix}.$$

Luego el subgrupo de conmutadores $G^{(1)}$ de G está contenido en el grupo N definido en el item anterior. Como dicho grupo es abeliano concluimos que $G^{(2)} = \{\mathrm{id}\}$. Esto da una demostración alternativa a la mostrada en [i] del hecho de que G es abeliano.

3.- **Problema 3*:** Sea G grupo finito soluble y considere $N \triangleleft G$ minimal.

i.- Pruebe que N es abeliano.

ii.- Demuestre que existe p primo tal que $x^p = e$, para todo $x \in N$.

Desarrollo:

i.- Sabemos que existe una cadena normal $\{e\} \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_s = G$, donde H_{i+1}/H_i es un grupo abeliano $\forall i \in \{1, \cdots, s\}$. En particular, tenemos que:

$$\{e\} \triangleleft H_1 \cap N \triangleleft H_2 \cap N \triangleleft \cdots H_{s-1} \cap N \triangleleft N,$$

es una cadena normal, donde $H_{i+1} \cap N/H_i \cap N \hookrightarrow H_{i+1}/H_i$ es un grupo abeliano $\forall i$. Por la minimalidad de N tenemos que $H_{s-1} \cap N = \{e\}$ o bien $H_{s-1} \cap N = N$. En el primer caso, tenemos que N es un grupo abeliano. En el segundo caso tenemos que nuestra cadena normal se reduce a $\{e\} \triangleleft H_1 \cap N \triangleleft H_2 \cap N \triangleleft \cdots \triangleleft H_{s-2} \cap N \triangleleft N$ y aplicamos el mismo argumento. Note que si $N \subset H_1$, entonces N es abeliano, puesto que H_1 es un grupo abeliano. Esto concluye lo pedido.

ii.- Considere una cadena normal para G como la mostrada en [i]. Sabemos que H_{i+1}/H_i es un grupo abeliano $\forall i \in \{1, \cdots, s\}$. Luego, por el teorema de módulos finitamente generados sobre DIP, tenemos que $H_{i+1}/H_i \cong \prod_{k=1}^{n} \prod_{j=1}^{a_k} \mathbb{Z}/p_k^{e_{kj}}$. En particular, tenemos que H_{i+1}/H_i tiene un subgrupo de indice p_1. Luego, si tomamos la preimagen de este subgrupo bajo la proyección, encontramos $H_i \triangleleft K \triangleleft H_{i+1}$, donde $[K : H_{i+1}] = p_1$. Aplicando este algoritmo a K/H_i obtenemos K' tal que $H_i \triangleleft K' \triangleleft K \triangleleft H_{i+1}$ y $[H_{i+1} : K] = p_1$ y $[K : K'] = p_2$ primo. Aplicando inductivamente este razonamiento sobre cada cociente H_{i+1}/H_i, encontramos una cadena normal $\{e\} \triangleleft K_1 \triangleleft K_2 \triangleleft \cdots \triangleleft K_s = G$, donde $K_{i+1}/K_i \cong C_{q_i}$, para cierto q_i primo. Luego $N \cong C_{q_s}$ o bien $N \cap K_{s-1} = N$, por el mismo argumento que se dió en [i]. Aplicamos entonces el mismo razonamiento que en [i]. Esto implica que $N \cong C_{q_i}$, para algún i. En particular existe p primo tal que $x^p = e$, para todo $x \in N$.

4.- **Problema 4:** Sea $G = D_{2n} = \langle a, b : a^2 = b^n = e, aba^{-1} = b^{-1} \rangle$ el grupo dihedral de $2n$ elementos.

i.- Calcule $[G, G]$.

ii.- Pruebe que G es soluble.

iii.- Pruebe que G es nilpotente si y solamente si n es potecia de 2.

Desarrollo:

i.- Es claro que $[a^i, a^j] = [b^i, b^j] = e$. Por ende solo debemos calcular los conmutadores $[ab^i, b^j], [ab^i, ab^j]$. En efecto $[ab^i, b^j] = ab^j b^i b^{-j} a^{-1} b^{-i} = b^{-2i}$ y $[ab^i, ab^j] = b^{2(j-i)}$. Por lo tanto $[G, G] = (b^2)$.

ii.- Note que $G^{(1)}$ es un grupo abeliano. Por lo tanto $G^{(2)} = [G^{(1)}, G^{(1)}] = \{e\}$. Esto prueba que D_{2n} es un grupo soluble.

iii.- El cálculo hecho en [i] implica que $G^2 = [G^1, G] = (b^4)$. Por inducción tenemos que $G^t = (b^{2^t})$. Luego G es nilpotente si y solamente si $n|2^t$, para cierto $t \in \mathbb{N}$. Esto es equivalente a que n sea una potencia de 2.

5.- **Problema 5:** Usando que todos subgrupo propio de un grupo nilpotente es un subgrupo propio de su normalizador, pruebe que un grupo finito G es nilpotente si y solamente si todo subgrupo maximal de G es normal.
Demostración: Supongamos que G es nilpotente y consideremos M un grupo maximal de G. Sabemos que $M \subsetneq G$, luego, por la nilpotencia de G, tenemos que $M \subsetneq N_G(M)$. Esto implica que $N_G(M) = G$. Es decir $M \lhd G$. Recíprocamente, supongamos que todo subgrupo maximal de G es normal. Sea P un p-subgrupo de Sylow de G. Si demostramos que $P \lhd G$ entonces se obtiene lo pedido. Supongamos que P no es un subrgupo normal de G y sea M un subgrupo maximal que contiene a $N_G(P)$. Por hipótesis $M \lhd G$. Luego por el argumento de Frattini (Ver problema 1 de la ayudantía 3), tenemos que $G = MN_G(P)$. Pero por construcción $MN_G(P) = M$. Esto nos lleva a una contradicción.

6.- **Problema 6:** Si H, N son grupos nilpotentes y $1 \to^f H \to G \to^g N \to 1$ es una sucesión exacta, ¿Es cierto que G es nilpotente?
Desarrollo: Esta propiedad es falsa en general. Por ejemplo considere $G = S_3$, $H = A_3$ y $N = S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$. En este caso los grupos H y N son abelianos, y por ende nilpotentes. No obstante G no es nilpotente, ya que no es el producto directo de sus subgrupos de Sylow. Note que el mismo ejemplo dice que la nilpotencia no es una propiedad que se mantenga al considerar el producto semidirecto de grupos nilpotentes. Por ende, aunque nos restringieramos al caso de sucesiones exactas escindidas, la premisa anterior es falsa.

2. Anillos:

Ayudantía 7: En esta ayudantía estudiaremos la parte básica de la teoría de anillos, en particular trabajaremos con ideales y polinomios.

1.- **Problema 1:** Sea $\mathbb{H} = \mathbb{H}_{\mathbb{R}}$ el anillo de cuaterniones de Hamilton.

i.- Pruebe que en $\mathbb{H}$ existen infinitas soluciones de la ecuación $x^2 + 1 = 0$.

ii.- Muestre que en $\mathbb{H}$ hay infinitos subanillos isomorfos a $\mathbb{C}$.

Desarrollo:

i.- Sea $q \in \mathbb{H}$ un cuaternión cualquiera. Escribiendo $q = a_0 + a_1 i + a_2 j + a_3 ij$, tenemos que si $-1 = q^2 = a_0^2 + 2a_0(a_1 i + a_2 j + a_3 ij) + (a_1 i + a_2 j + a_3 ij)^2$, entonces $a_0 = 0$ o bien $a_1 = a_2 = a_3 = 0$. En el segundo caso tenemos que $a_0^2 = -1$ y esta ecuación no tiene solución real. En el otro caso tenemos que $q^2 = -a_1^2 - a_2^2 - a_3^2 = -1$. Es decir, las componentes de los cuaterniones que en este caso satisfacen la solución se encuentran en la esfera real. Luego hay infinitas de estas soluciones.

ii.- Sea $q = a_1 i + a_2 j + a_3 ij \in \mathbb{H}$ tal que $a_1^2 + a_2^2 + a_3^2 = 1$. Considere la transformación $\mathbb{R}$-lineal $\phi_q : \mathbb{C} \to \mathbb{H}$ definida por $\phi_q(i) = q$. Observe que ϕ es un homomorfimo de anillos cuyo kernell es trivial. Por lo tanto, por primer teorema de isomorfía tenemos que $\mathbb{C} \cong \mathrm{Im}(\phi_q)$. Observe también que si $\mathrm{Im}(\phi_q) = \mathrm{Im}(\phi_{q'})$ entonces $q = a_0 + bq'$. Luego $-1 = q^2 = a_0^2 + 2ba_0 q' + b^2 q'^2 = a_0^2 + 2ba_0 q' - b^2$. Igualando las componentes en el anillo $\mathbb{H}$ tenemos que $a_0 = 0$ y $b = \pm 1$. Por lo tanto tenemos tantos subanillos $H_q = \mathrm{Im}(\phi_q)$ isomorfos a $\mathbb{H}$ como elementos en la semi-esfera real. Luego hay infinitos.

2.- **Problema 2:** Sea X espacio Hausdorff compacto. Considere $C(X) = \{f : X \to \mathbb{R} : f \text{ continua}\}$. Sea $x \in X$ y considere $m_x = \{f \in C(X) : f(x) = 0\}$.

i.- Muestre que m_x es un ideal maximal de $C(X)$ respecto a la inclusión.

ii.- Sea $\mathrm{Max}(C(X))$ es el conjunto de ideales maximales de $C(X)$ y considere la función $u : X \to \mathrm{Max}(C(X))$ definida por $u(x) = m_x$. Pruebe que u es una función biyectiva.

iii.- Describa todos los homomorfismos $\mathbb{R}$-lineales de $C(X)$ a $\mathbb{R}$.

Desarrollo:

i.- Considere el homomorfimo $ev_x : C(X) \to \mathbb{R}$ definido por $ev_x(f) = f(x)$. Observe que $\ker(ev_x) = m_x$. Además para todo $r \in \mathbb{R}$, existe $f = \mathbf{1}r \in C(x)$ tal que $ev_x(f) = r$, donde $\mathbf{1}$ es la función constante igual a 1. Por el primer teorema de isomorfía tenemos que $C(X)/m_x \cong \mathbb{R}$, en donde este último anillo es un cuerpo. Por lo tanto m_x es un ideal maximal.

ii.- Sea m un ideal maximal de $C(X)$ y $V = \{x \in X : f(x) = 0, \forall f \in m\}$. Supongamos que $V = \emptyset$ entonces para todo $x \in X$ existe $f_x \in m$ tal que $f_x(x) \neq 0$. Como f_x es continua existe una vecindad U_x de x tal que f_x no se anula en ningún punto de U_x. Por la compacidad de X tenemos que existen finitos U_{x_i} tales que $\cup_{i=1}^n U_{x_i} = X$. Considere entonces $f = f_1^2 + \cdots + f_n^2 \in m$. Esta última función no tiene ceros en ningún punto de X y por lo tanto es invertible, con inversa contínua. Luego $m = C(X)$. Por lo tanto $V \neq \emptyset$. Sea $x \in V$, entonces por defineión $m \subseteq m_x$. Por maximalidad concluimos que $m = m_x$. Esto prueba la sobreyectividad de u. Para la inyectividad, supongamos $x \neq y$. Como X es Hausdorff y compacto, por lema de Uryson

existe una función contínua f tal que $f(x) = 0$, pero $f(y) \neq 0$. Luego $m_x \neq m_y$.

iii.- Sea $\phi : C(X) \to \mathbb{R}$ un homomorfismo $\mathbb{R}$-lineal. Como $\phi(r\mathbf{1}) = r$, para todo $r \in \mathbb{R}$, tenemos que ϕ es sobreyectiva. Luego $C(x)/\ker(\phi) \cong \mathbb{R}$. Por ende $\ker(\phi)$ es un ideal maximal de $C(X)$. Por [ii] tenemos que $\ker(\phi) = m_x$, para cierto $x \in X$. Por otro lado, para todo $f \in C(X)$ se tiene que $\phi(f - \phi(f)\mathbf{1}) = 0$. Es decir $f - \phi(f)\mathbf{1} \in m_x$. Por definición de m_x concluimos que $f(x) - \phi(f) = 0$. Es decir $f(x) = \phi(f)$. Por ende $\phi = ev_x$.

3.- **Problema 3:** Sea A un anillo conmutativo. Se define el radical $r(I)$ de un ideal I por $r(I) = \{b \in A : b^n \in I, \text{ algún } n \in \mathbb{N}\}$.

i.- Muestre que $r(I)$ es un ideal que contiene a I.

ii.- Puebe que $r(r(I)) = r(I)$.

iii.- Muestre que $r(I) = A$ si y solamente si $I = A$.

iv.- Muestre que $r(I + J) = r(r(I) + r(J))$.

v.- Pruebe que si $r(I) + r(J) = A$ entonces $I + J = A$.

Desarrollo:

i.- Sea $a, b \in r(I)$. Entonces existen $n, m \in \mathbb{N}$ tales que $a^n \in I$ y $b^m \in I$. Por lo tanto $(a+b)^{n+m} \in I$. Luego $a+b \in r(I)$. Por otro lado, para $r \in A$ cualquiera tenemos que $(ra)^n = r^n a^n \in I$. Luego $ra \in I$. Esto prueba que $r(I)$ es un ideal. Además, para todo $i \in I$ tenemos que $i^1 \in I$. Luego $I \subseteq r(I)$.

ii.- Basta probar que $r(r(I)) \subseteq r(I)$. Sea $x \in A$ tal que $x^n \in r(I)$ entonces existe $m \in \mathbb{N}$ tal que $x^{nm} = (x^n)^m \in I$. Luego $x \in r(I)$.

iii.- Claramente $r(A) = A$. Por otro lado si $r(I) = A$ entonces $1 \in r(I)$. Por lo tanto existe $n \in \mathbb{N}$ tal que $1 = 1^n \in I$. Esto prueba que $I = A$.

iv.- Claramente $r(I + J) \subseteq r(r(I) + r(J))$. Por otro lado si $x \in r(r(I) + r(J))$ tenemos que $x^n \in r(I) + r(J)$, para cierto $n \in \mathbb{N}$. Es decir $x^n = a + b$, donde $a^s \in I$ y $b^t \in J$, para ciertos $s, t \in \mathbb{N}$. Luego $x^{n(s+t)} = (a + b)^{s+t} \in I + J$ y así $x \in r(I + J)$.

v.- Supongamos que $r(I) + r(J) = A$. Entonces $r(I + J) = r(r(I) + r(J)) = A$. Por [iv] concluimos que $I + J = A$.

4.- **Problema 4:** Sea A anillo conmutativo con uno y sea $f = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$.

i.- Pruebe que $f \in A[x]^*$ si y solamente si $a_0 \in A^*$ y a_i es nilpotente, para todo $i \in \{1, \cdots, n\}$.

ii.- Se define el radical de Jacobson de A por:

$$J(A) = \{a \in A : 1 + ay \in A^*, \forall y \in A\}.$$

Pruebe que $J(A) = \bigcap\{m : m \text{ es ideal maximal}\}$.

iii.- Concluya que el nilradical $\mathfrak{N}(A[x])$ de $A[x]$ coindice con el radical de Jacobson $J(A[x])$.

Desarrollo:

i.- Para comenzar, supongamos que $a_0 \in A^*$ y a_i es nilpotente, para todo $i \in \{1, \cdots, n\}$. Entonces $f(x) = a_0 + x(a_1 + \cdots + a_n x^{n-1})$, donde $x(a_1 + \cdots + a_n x^{n-1})$ es nilpotente. Luego el resultado sigue del hecho de que la suma de un elemento invertible y un nilpotente es invertible. Supongamos que $f \in A[x]^*$, es decir existe $g = b_0 + b_1 x + \cdots + b_m x^m \in A[x]$ tal que $fg(x) = gf(x) = 1$. Considerando el producto de los términos de grado 0, deducimos que $a_0 \in A^*$. Por otro lado tenemos que $a_n b_m = 0$, $a_{n-1} b_m + b_{m-1} a_n = 0$ y

más relaciones que se obtienen comparando los términos de grado mayor a 0 en $fg(x) = 1$. En particular, si multiplicamos por las potencias crecientes de a_n, obtenemos que $a_n^{k+1} b_{m-k} = 0$. Luego, tenemos que $a_n^{m+1} b_0 = 0$. Por otro lado, como b_0 es invertible, tenemos que $a_n^{m+1} = 0$, es decir a_n es nilpotente. Además, como $f - a_n$ es invertible, tenemos por inducción que a_i es nilpotente, para todo $i \in \{1, \cdots, n\}$.

ii.- Supongamos que $1 + ay$ no es unidad, para cierto $y \in A$. Entonces existe m ideal maximal tal que $1 + ay \in m$. Luego si $a \in \bigcap\{m : m \text{ es ideal maximal}\}$, tenemos en particular que $a \in m$. Por lo tanto tenemos que $ay \in m$ y luego $1 \in m$, lo cual nos lleva a una contradicción. Supongamos ahora que $a \notin m$, para cierto m ideal maximal de A. Entonces $m + (a) = A$. Luego $1 = ya + s$, para ciertos $a \in A$ y $s \in m$. Por lo tanto $v = 1 + (-y)a \in m$, en particular v no es invertible.

iii.- Claramente $\mathfrak{N}(A[x]) \subset J(A[x])$. Por otro lado, si $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ cumple con que $1 + fg(x) \in A[x]^*$, para todo $g(x) \in A[x]$, entonces considerando $g(x) = x$ obtenemos que $1 + a_0 x + \cdots + a_n x^{n+1} \in A[x]^*$. Por [i] esto implica que a_i es nilpotente, $\forall i$. Luego $f(x)$ es nilpotente.

5.- **Problema 5:** Sea A anillo conmutativo con uno y $p_1, \cdots, p_n$ ideales del anillo A.

i.- Demuestre que $I \subset \bigcup_{i=1}^n p_i$ si y solamente si $I \subset p_i$, para cierto $i \in \{1, \cdots, n\}$.

ii.- Suponga que I es un ideal primo. Pruebe que $I \supset \bigcap_{i=1}^n p_i$ si y solamente si $I \supset p_i$, para cierto $i \in \{1, \cdots, n\}$.

Desarrollo:

i.- Este ejercicio forma parte de la Guia 5.

ii.- Claramente si $I \supset p_i$ entonces $I \supset \bigcap_{i=1}^n p_i$. Demostremos el recíproco por contradicción. Si para todo $i \in \{1, \cdots, n\}$ existe $x_i \in p_i - I$ entonces $x = x_1 \cdots x_i \in \bigcap_{i=1}^n p_i$, por la defínción de ideal. Luego si $I \supset \bigcap_{i=1}^n p_i$ entonces $x \in I$. Como I es un ideal primo tenemos que álgun $x_i \in I$, lo cual nos lleva a una contradicción.

Ayudantía 8: En esta ayudantía trabajaremos con anillos noetherianos, dominios de factorización única y estudiaremos algunos criterios de irreducibilidad de polinomios.

1.- **Problema 1:** Sea $A = \mathbb{Z}[i] \subset \mathbb{C}$, el anillo de enteros gaussianos.

i.- Muestre que A es un DIP.

ii.- Pruebe que todo DIP es un anillo noetheriano. Concluya que A es un anillo noetheriano.

iii.- Muestre que $5 \in \mathbb{Z}[i]$ no es un elemento primo. Determine su descomposición en irreducibles.

Desarrollo:

i.- Sea I ideal no nulo de A y considere $a \in I$ elemento de norma compleja minimal y no nula. Existen elementos de norma no nula porque $N(z) = 0$ si y solamente si $z = 0$. Más aún, existe un elemto de norma minimal por principio del buen orden. Entonces tenemos que $(a) \subset I$. Por otro lado, si $b \in I$, entonces por algoritmo de división existen $s, t \in A$ tales que $b = sa+t$, donde $t = 0$ o $N(t) < N(a)$. Luego, como $t = b - sa \in I$ y $N(a)$ es minimal en I, tenemos que $t = 0$. Esto implica que $b \in (a)$. Por lo tanto $I = (a)$.

ii.- Un DIP cumple con que todo ideal contenido en el es finitamente generado, puesto que está generado por un solo elemento. Sabemos que esto último es equivalente a que el anillo sea noetheriano. Por [i] concluimos que A es un anillo noetheriano.

iii.- Para demostrar o refutar la primalidad de $5 \in \mathbb{Z}[i]$ debemos examinar el cociente $B = \mathbb{Z}[i]/(5)$. En efecto $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$ vía el isomorfismo inducido por la evaluación en $x = i$. Note que la preimagen de (5) por la evaluación en $x = i$ es $(x^2 + 1, 5)$. Por lo tanto:

$$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[x]/(x^2 + 1)/(5, x^2 + 1)/(x^2 + 1),$$

Luego por uno de los teoremas de isomorfía, tenemos que:

$$\mathbb{Z}[i]/(5) \cong \mathbb{Z}[x]/(5, x^2 + 1)/ \cong \mathbb{F}_5[x]/(x^2 + 1).$$

Ahora bien, el polinomio $x^2 + 1$ se factoriza en $\mathbb{F}_5$ el cuerpo de 5 elementos como $x^2 + 1 = (x - 2)(x + 2)$. Por lo tanto B tiene divisores de cero, lo que prueba que dicho anillo no es un dominio de integridad. Del argumento anterior se desprende que la factorización de 5 en elementos irreducibles debe ser $5 = (2 + i)(2 - i)$, dado que via los isomorfismos empleados x va a dar al elemento $i \in A$. En efecto, no es dificil, vía los mismo argumentos anteriores, percatarse que $2 + i$ y $2 - i$ son elementos irreduucibles en $\mathbb{Z}[i]$ (Ejercicio). Esto concluye lo pedido.

2.- **Problema 2:*** Sea A anillo conmutativo con uno.

i.- Muestre que si A es un anillo noetheriano entonces A/I es noetheriano, para todo ideal $I \subset A$.

ii.- Pruebe que en un dominio noetheriano existe factorización en elementos irreducibles, para todo elemento no invertible.

iii.- Es un hecho probado, que si A es un anillo noetheriano entonces $A[x]$ también lo es. Sea $p \in \mathbb{Z}$ primo. Muestre que todo $a \in \mathbb{Z}[\sqrt{p}]$ no invertible tiene una factorización en irreducibles.

Desarrollo:

i.- Considere $\{\overline{0}\} \subset J_1 \subset \cdots \subset J_n \subset \cdots$, una cadena de ideales en A/I. Por el teorema de correspondencia, tenemos que para todo $k \in \mathbb{N}$ existe I_k ideal de A que contiene a I tal que $J_k = I_k/I$. He decho $I_0 = I$. De esto se obtiene la cadena ascendente $\{0\} \subset I \subset I_1 \subset \cdots\cdots I_n \subset \cdots$. Por la notherianidad de A, concluimos que existe $N \in \mathbb{N}$ tal que $I_N = I_n$, para todo $n \geq N$. En particular, $J_N = J_n$, para todo $n \geq N$. Esto prueba que A/I es noetheriano.

ii.- En lo que sigue probaremos que en todo dominio noetheriano A hay factorización en irreducibles de todo elemento no invertible. En efecto, si $a \in A$ no es irreducible se tiene que $a = a_1b_1$, donde a_1 o b_1 no es invertible. Supongamos, sín perdida de generalidad, que a_1 no es invertible. Entonces, si a_1 no es irreducible, existen $a_2, b_2 \in A$ tales que $a_1 = a_2b_2$ y a_2 o b_2 no es invertible. Por otro lado si a_1 es irreducible, tenemos su factorización y aplicamos el mismo argumento a b_1. Por inducción obtenemos una cadena de ideales:

$$(a) \subset (a_1) \subset (a_2) \subset \cdots (a_n) \subset \cdots$$

Luego como A es noetheriano, esta cadena es estacionaria. Entonces en algún paso de la inducción obteniamos un elemento irreducible. Esto implica la factorización de $a \in A$.

iii.- Observe que $\mathbb{Z}[\sqrt{p}] \cong \mathbb{Z}[x]/(x^2 - p)$. Además, dado que $\mathbb{Z}$ es un anillo noetheriano puesto que es un DIP, tenemos que $\mathbb{Z}[x]$ es un anillo noetheriano. Luego por [i], se tiene que $\mathbb{Z}[\sqrt{p}] \cong \mathbb{Z}[x]/(x^2 - p)$ es un anillo noetheriano. Luego este resultado se sigue de [ii].

3.- **Problema 3*:** Sea A un anillo conmutativo y sea $m \subset A$ un ideal maximal y principal de A. Demuestre que no existe un ideal I de A tal que $m^2 \subsetneq I \subsetneq m$.
Demostración: Consideremos $m = (\pi)$, donde $\pi \in A$. Sea I un ideal tal que $m^2 \subsetneq I \subsetneq m$. Entonces como $m^2 = (\pi^2)$, tenemos que $(\pi^2) \subsetneq I \subsetneq (\pi)$. Note que todo elemento $a \in I$ se escribe como $a = \pi b$, con $b \in A$. Por lo tanto $(\pi) \subset \pi^{-1}I \subset A$, donde $\pi^{-1}I = \{b \in A : \exists a \in I \text{ tal que } a = \pi b\}$. Observe que $\pi^{-1}I$ es un ideal de A. Además si $\pi^{-1}I = A$, entonces $\pi \cdot 1 = \pi \in I$, lo que es falso. Por otro lado, si $(\pi) = \pi^{-1}I$ entonces todo $b \in I$ se escribiría como $b = c_b\pi$. Por ende todo $a \in I$ se escribiría como $a = \pi^2 c_b$. Esto demuestra que $m^2 = I$, lo que es contradictorio. Concluimos, de la maximalidad de m, que dicho ideal I no puede existir.

4.- **Problema 4*:** Sea A un DFU noetheriano en el que se cumple que para todo $a, b \in A$, no ambos nulos y sin dividores primos comunes, existen $u, v \in A$ tales que $au + bv = 1$. Demuestre que A es un DIP.
Demostración: Debemos probar que todo ideal $I \subset A$ está generado por un elemento. Observe que, por ser A noetheriano, tenemos que todo ideal de A es finitamente generado. Luego que si logramos probar que un ideal de la forma $I = (a, b)$ está generado por un elemento $d \in A$, entonces por inducción sobre el número de generadores, obtenemos lo pedido. Considere $d \in A$ un máximo común divisor entre a y b. Como d divide a a y b tenemos que $a = a_1d$, $b = b_1d$. Luego $(d) \supset (a, b)$. Probemos por lo tanto que $(d) = (a, b)$. En efecto, $a_1, b_1 \in A$ son elementos sin divisores primos comunes. Esto de debe a que si $p|a_1, b_1$ entonces dp es un divisor comun de a, b tal que $(dp) \subsetneq (d)$, lo que contradice la elección de $d \in A$. Por la hipótesis respecto de A tenemos que existen $u, v \in A$ tales que $a_1u + b_1v = 1$. Por lo tanto $d = au + bv \in (a, b)$.

Esto demuestra la igualdad entre los ideales citados previamente. Concluimos que A es un DIP

5.- **Problema 5:** Sea A un dominio de factorización única (DFU).

i.- **Lema de Einsenstein**. Sea $p \in A$ un elemento irreducible y $f(x) = \sum_{i=0}^{n} a_i x^i \in A[x]$. Pruebe que si $p|a_i$, $\forall i \in \{0, \cdots, n-1\}$, $p \nmid a_n$ y $p^2 \nmid a_0$ entonces $f(x)$ es irreducible.

ii.- Sea $p(x, y) = x^n + y \in \mathbb{Z}[x, y]$. Muestre que $p(x, y)$ es un polinomio irreducible.

iii.- Muestre que $p(x, y) = x^4 + y^2 \in \mathbb{C}[x, y]$ no es irreducible.

Desarrollo:

i.- Considere $g(x) = \sum_{i=0}^{s} b_i x^i$ y $h(x) = \sum_{i=0}^{t} c_i x^i$ dos polinomios tales que $f(x) = g(x)h(x)$. Entonces como $a_0 = b_0 c_0$ y $p|a_0$, pero $p^2 \nmid a_0$ tenemos que $p|b_0$ o $p|c_0$, sin que sea posible que ambos hechos ocurran. Sín pérdida de generalidad, supongamos que $b_0 \equiv 0 (\text{mod } p)$. Entonces, como $c_0 b_1 + c_1 b_0 \equiv 0 \,(\text{mod } p)$, tenemos que $c_0 b_1 \equiv 0 (\text{mod } p)$. Luego, como $A/(p)$ es un dominio de integridad, tenemos que $b_1 \equiv 0 \,(\text{mod } p)$. Por inducción obtenemos que $b_s \equiv 0 \,(\text{mod } p)$. Por lo tanto $p|a_n$. Esto nos lleva a una contradicción.

ii.- Sea $y \in \mathbb{Z}[y]$ entonces $\mathbb{Z}[y]/(y) \cong \mathbb{Z}$, en particular obtenemos que $y \in \mathbb{Z}[y]$ es un elemento primo. Luego y es un elemento irreducible, puesto que $\mathbb{Z}[y]$ es un DFU y en un DFU todo elemento primo es irreducible. Ocupando el criterio mostrado en [i], para $p = y$ concluimos lo pedido.

iii.- Observe que $p(x, y) = (x^2 + iy)(x^2 - iy)$, en donde $x^2 + iy$ y $x^2 - iy$ cumplen con $\mathbb{Z}[x, y]/(x \pm iy) \cong \mathbb{Z}[y]$. Por lo tanto $x^2 + iy$ y $x^2 - iy$ son elementos irreducibles y por ende no invertibles. Esto prueba que $p(x, y)$ es reducible. Esto muestra que el criterio mostrado en [i] depende fuertemente de la condición $p^2 \nmid a_0$.

Ayudantía 9: En esta ayudantía haremos un repaso general por la teoría de anillos e incluiremos algunos ejercicios asociados con polinomios y Lema de Gauss.

1.- **Problema 1*:** Sea A un anillo conmutativo con 1. Diremos que un elemento $s \in A$ no nulo y no invertible es especial si para todo $a \in A$ existen $q, r \in A$ tales que:

$$a = qs + r, \text{ donde } r = 0 \text{ o bien } r \text{ es invertible.}$$

i.- Demuestre que todo polinomio de grado 1 en $\mathbb{Q}[x]$ es especial.
ii.- Si $s \in A$ es especial, demuestre que (s) es un ideal maximal de A.
iii.- Demuestre que no hay elementos especiales en $\mathbb{Z}[x]$.
Desarrollo:
i.- Sea f un polinomio de grado 1 y $a \in \mathbb{Q}[x]$ otro polinomio cualquiera. Por algoritmo de división existen $q, r \in \mathbb{Q}[x]$ tales que $a = qs + r$, donde $r = 0$ o bien $\deg(r) < 1$. Note que $\det(r) = 0$ implica que $r \in \mathbb{Q}$ y por ende es invertible o nulo. Esto prueba lo pedido.
ii.- Sea $s \in A$ un elemento especial y supongamos que $(s) \subset I \subset A$. Sea $a \in I$, entonces existen $q_a, r_a \in A$ tales que $a = q_a s + r_a$ tales que $r_a = 0$ o bien r_a investible. Note que si $r_a = 0$ para todo $a \in I$ entonces $(s) = I$. Por otro lado, si $r_a \neq 0$ para algún $a \in I$ entonces $r_a = a - sq_a \in I$ es invertible. Luego $I = A$. Esto demuestra la maximalidad de (s).
iii.- Recordemos que los elementos invertibles de $\mathbb{Z}[x]$ son $\{1, -1\}$. Sea $s \in \mathbb{Z}[x]$ un elemento especial. Entonces para todo $a \in \mathbb{Z}[x]$ se cumple que existe q, r tales que $a = qs + r$, donde $r \in \{0, 1, -1\}$. En particular tenemos que para $a = s + 2$ se cumple que $s + 2 = qs + r$. Igualando el grado en ambas expresiones y analizando su término de grado mayor deducimos que $q = 1$. Por lo tanto $s + 2 = s + r$. Luego $r = 2$, lo cual es imposible.

2.- **Problema 2:** Sea $A = \mathbb{Z}[\sqrt{-n}]$, donde $n \in \mathbb{Z}_{>3}$ es libre de cuadrados.
i.- Determine A^*
ii.- Pruebe que $2, \sqrt{-n}$ y $1 + \sqrt{-n}$ son elementos irreducibles de A
iii.- Pruebe que A no es un DFU.
Desarrollo:
i.- Observe que si $ab = 1$, con $a, b \in A$ entonces, aplicando la norma compleja en la ecuación anterior, tenemos que $N(a)N(b) = 1$, donde $N(a), N(b) \in \mathbb{Z}$. Por lo tanto $N(a), N(b) \in \{\pm 1\}$. Por otro lado, la norma de un elemento $z = x + y\sqrt{-n} \in A$ es $N(z) = x^2 + ny^2$. Es así como $N(a) = 1$ implica que $a \in \{\pm 1\}$. Concluimos que $A^* = \{\pm 1\}$.
ii.- Supongamos que $2 = ab$, donde $a, b \in A$. Entonces $4 = N(a)N(b)$. Luego $N(a), N(b) \in \{1, 2, 4\}$. Escribiendo la norma de $a = x + y\sqrt{-n}$ como $N(a) = x^2 + ny^2$, observamos que, como $n > 3$, se tiene que $N(a) \neq 2$ y que $N(a) = 4$ si y solamente si $x \in \{\pm 2\}$. Luego b es invertible. Concluimos entonces que 2 es irreducible. De la misma manera, como $N(\sqrt{-n}) = n$ y como $x^2 + y^2 n = n$ implica que $y \in \{\pm 1\}$ y $x = 0$, tenemos que $\sqrt{-n}$ es irreducible. Por último veamos que $1 + \sqrt{-n}$ es irreducible. Sea $1 + \sqrt{-n} = ab$. Entonces $1 + n = N(a)N(b)$. Luego si $N(a) = x^2 + ny^2$ es un divisor de $1 + n$, tenemos que o bien $x, y \in \{\pm 1\}$ y en este caso $N(b) = 1$ o bien $n + 1$ es un cuadrado en $\mathbb{Z}$, en cuyo caso $1 + \sqrt{-n} = ab$, con $a \in \mathbb{Z}$. Pero como el maximo común

dividor entre las componentes de $a+\sqrt{-n}$ es 1, concluimos que $a=1$. Por lo tanto $1+\sqrt{-n}$ es irreducible.

iii.- Supongamos que n es impar, entonces $(1+\sqrt{-n})^2 = 1+n+2\sqrt{-n} = 2c$, para cierto $c \in A$. Observe que $2, 1+\sqrt{-n}$ son elementos irreducibles que no difieren en un elemento invertible, pues si así fuera, entonces $4 = 1+n$, luego $n=3$, lo que es contradictorio. Por otro lado, si n es par, entonces $(\sqrt{-n})^2 = n = 2c$, para cierto $c \in A$. Observe que $2, \sqrt{-n}$ son elementos irreducibles que no difieren en un elemento invertible, pues si así fuera, entonces $4 = n$, lo que es contradictorio pues n es libre de cuadrados. Concluimos que A no es DFU.

3.- **Problema 3:** Sea A anillo conmutativo con uno.

i.- Pruebe que si A es un DIP entonces todo ideal primo de A no nulo es maximal.

ii.- Sea A un dominio que no es cuerpo. Pruebe que $A[x]$ no es DIP.

iii.- Encuentre un anillo A tal que A no es DIP, pero para el cual A/I es DIP, para cierto ideal $I \subset A$.

Desarrollo:

i.- Sea p un ideal primo en A y sea J un ideal de A tal que $p \subset J \subsetneq A$. Entonces como A es un DIP, tenemos que $p=(a)$ y $J=(b)$. Por lo tanto $a=bt$, para cierto $t \in A$. Luego $bt = a \in p$ y como p es un ideal primo, concluimos que $b \in p$ o bien $t \in p$. En el primer caso tenemos que $p=J$. En el segundo caso concluimos que $t=as$, para cierto $s \in A$. Luego $a(1-bs)=0$ y como $a \neq 0$, tenemos que $bs=1$, es decir $b \in A^*$. Por lo tanto $J=A$, lo que nos lleva a una contradicción.

ii.- Supongamos que $A[x]$ es DIP. Entonces $p=(x)$ es un ideal primo, puesto que $A[x]/(x) \cong A$ es un dominio de integridad. Luego, por [i], tenemos que p es un ideal maximal. Esto implica que A es un cuerpo, lo que nos lleva a una contradicción.

iii.- Observe que [ii] muestra que $\mathbb{Z}[x]$ no es un DIP, pero su cociente por $I = (x^2+1)$ es $\mathbb{Z}[x]/(x^2+1) \cong \mathbb{Z}[i]$. Sabemos que este último anillo es un DIP.

4.- **Problema 4*:** Considere el anillo $A=\mathbb{Z}[x]$ y su ideal $I=(15, x^2+2)$. Demuestre que I está contenido en un número finito de ideales maximales de A y determine cuántos son.

Demostración: Observe primero que si $m \supset I$ es un ideal maximal, entonces m/I es un ideal maximal de A/I e inversamente todo ideal maximal de A/I es de esta forma. Por ende basta evaluar el cociente A/I y encontrar todos los ideales maximales de este. En efecto:

$$A/I \cong \mathbb{F}_{15}[x]/(x^2+2).$$

Por teorema chino de los restos tenemos que $\mathbb{F}_{15} \cong \mathbb{F}_3 \times \mathbb{F}_5$. No es dificil probar que de hecho esto implica que $\mathbb{F}_{15}[x] \cong \mathbb{F}_3[x] \times \mathbb{F}_5[x]$ (Ejercicio) y por ende:

$$A/I \cong \mathbb{F}_3/(x^2+2) \times \mathbb{F}_5[x]/(x^2+2).$$

Ahora bien en $\mathbb{F}_3$ tenemos que $x^2+2 = x^2-1 = (x-1)(x+1)$, donde $1 = \frac{1}{2}(x+1-(x-1))$. Nuevamente, por teorema chino de los restos, tenemos que $\mathbb{F}_3/(x^2+2) \cong \mathbb{F}_3[x]/(x-1) \times \mathbb{F}_3[x]/(x+1)$. Empleando las funciones

evaluación en 1 y -1 concluimos que:

$$\mathbb{F}_3/(x^2+2) \cong \mathbb{F}_3 \times \mathbb{F}_3.$$

Por otro lado, el polinomio x^2+2 es irreducible en $\mathbb{F}_5[x]$, dado que no tiene factores de grado 1. Lo anterior es una consecuencia de la no existencia de raices de x^2+2 en $\mathbb{F}_5$. Como $\mathbb{F}_5[x]$ es un DIP, tenemos que $\widehat{m} = (x^2+2)$ es un ideal maximal de $\mathbb{F}_5[x]$ y por lo tanto $\mathbb{F}_5[x]/\widehat{m}$ es un cuerpo. Concluimos que:

$$A/I \cong (\mathbb{F}_3)_1 \times (\mathbb{F}_3)_2 \times \mathbb{F}_5[x]/(x^2+2),$$

es un producto de 3 cuerpos, donde los subíndices distingen las coordenadas. De esto se sigue que los ideales maximales de A/I son $(\mathbb{F}_3)_1 \times (\mathbb{F}_3)_2$, $(\mathbb{F}_3)_1 \times \mathbb{F}_5[x]$ y $(\mathbb{F}_3)_2 \times \mathbb{F}_5[x]$. Concluimos que I está contenido en 3 ideales maximales. Notese que estos ideales maximales pueden ser calculados usando los isomorfismos expĺicitos que provienen del teorema chino de los restos.

5.- **Problema 5:** Demuestre las siguientes afirmaciones:

i.- Pruebe que $\left(\mathbb{C}[x]/(x^2+5)\right)[y]$ no es un DE.

ii.- Pruebe que $\left(\mathbb{Q}[x]/(x^2+5)\right)[y]$ es un DE.

iii.- Demuestre que $\left(\mathbb{Z}[x]/(x^2+2)\right)[y]$ es un DFU.

Desarrollo:

i.- Observe que $\mathbb{C}[x]/(x^2+5) = \mathbb{C}[x]/(x-\sqrt{-5})(x+\sqrt{-5})$, donde $(x-\sqrt{-5})+(x+\sqrt{-5}) = (1)$. Por teorema chino de los restos tenemos que $\mathbb{C}[x]/(x^2+5) \cong \mathbb{C}[x]/(x-\sqrt{-5}) \times \mathbb{C}[x]/(x+\sqrt{-5}) \cong \mathbb{C}\times\mathbb{C}$. Luego $\mathbb{C}[x]/(x^2+5)$ no es dominio de integridad. Por lo tanto $\left(\mathbb{C}[x]/(x^2+5)\right)[y]$ no es dominio de integridad. En particular no es un dominio euclideano.

ii.- Sabemos, por el problema 3, que $A = \left(\mathbb{Q}[x]/(x^2+5)\right)[y]$ es un dominio euclideano si y solamente si $B = \mathbb{Q}[x]/(x^2+5)$ es un cuerpo. Es decir A es un DE si y solamente si (x^2+5) es un ideal maximal de $\mathbb{Q}[x]$. Supongamos que (x^2+5) no es maximal, es decir supongamos que existe un ideal J tal que $(x^2+5) \subsetneq J \subsetneq \mathbb{Q}[x]$. Pero como $\mathbb{Q}[x]$ es un DE tenemos que $J = r(x)$. Luego $r(x)s(x) = x^2+5$. Pero $\deg(r(x)) > 1$, pues $J \neq \mathbb{Q}[x]$. Por lo tanto $\deg(r(x)) = \deg(s(x)) = 1$. Esto implica que existe un racional $u \in \mathbb{Q}$ tal que $u^2 = -5$, lo que nos lleva a una contradicción. Por lo tanto (x^2+5) es maximal en $\mathbb{Q}[x]$. Por lo tanto A es un DE.

iii.- En clases se demostró que $A[y]$ es un DFU cuando A lo es. Por ende una estrategia posible para atacar este problema es demostrar que $\mathbb{Z}[x]/(x^2+2)$ es un DFU. En efecto probemos que $\mathbb{Z}[x]/(x^2+2) \cong \mathbb{Z}[\sqrt{-2}]$ el cual es sabido que es un DE y en particular un DFU. En general este tipo de isomorfismos se ha admitido, en esta y la ayudantía anterior, como un hecho. No obstante en este item lo demostraremos con rigurosidad. En efecto, siempre es posible establecer el homomorfismo sobreyectivo $f : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{-2}] \subset \mathbb{C}$ definido por $f(p(x)) = p(\sqrt{-2})$. Es inmediato que $(x^2+2) \subset \ker(f)$. Por ende basta probar la contención inversa. En efecto si $p(\sqrt{-2}) = 0$ entonces, por un argumento análogo al dado en [ii], tenemos que x^2+2 es el único polinomio irreducible que se anula en $\sqrt{-2}$ y por ende genera el ideal maximal:

$$I = \{s(x) \in \mathbb{Q}[x] : s(\sqrt{-2}) = 0\}.$$

Luego, como en $\mathbb{Q}[x]$ se tiene $p(x) \in (x^2+2)$, se tiene que $p(x) = (x^2+2)Q(x)$, donde $Q(x) \in \mathbb{Q}[x]$. Ahora bien, por Lema de Gauss tenemos que existe $q(x) \in \mathbb{Z}[x]$ tal que $p(x) = (x^2+2)q(x)$. Esto prueba la igualdad requerida.