FACULTAD DE
CIENCIAS
UNIVERSIDAD DE CHILE

Apuntes de Ayudantía

Álgebra de postgrado

Claudio Bravo Castillo
5 de septiembre de 2018

Ad solis ortv vsqve ad occasvm et plvs vltra.

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 las paginas web:

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

y

`https://www.u-cursos.cl/ciencias/2018/2/POST1121/1/material_docente/`.

Cabe mencionar que en las notas se dejan algunos ejercicios al lector.

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 $\mathrm{Sly}_p(G)$ 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 $P \in \mathrm{Syl}_p(H)$ entonces $G = N_G(P)H$.

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

iii.- Deduzca que si $P \in \mathrm{Syl}_p(G)$ 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 $\mathrm{Syl}_p(H) = \{hPh^{-1} : h \in H\}$. 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 $gPg^{-1} \in \mathrm{Syl}_p(H)$. 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 $P \in \mathrm{Syl}_p(G)$, 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 $w = e^{\frac{2\pi i}{3}}$ y considere el anillo $\mathbb{Z}[w] = \{a + bw : a, b \in \mathbb{Z}\}$.

i.- Pruebe que (7) no es un ideal maximal de $\mathbb{Z}[w]$.

ii.- Encuentre los ideales maximales que contienen a (7).

Desarrollo:

i.- Estudiemos el cociente $\mathbb{Z}[w]/(7)$. En efecto, tenemos que $\mathbb{Z}[w] \cong \mathbb{Z}[x]/(x^2 + x + 1)$ vía el homomorfismo ϕ definido por $\phi(\overline{p(x)}) = p(w)$. Luego, factorizando dicho homomorfismo, tenemos que:

$$\mathbb{Z}[w]/(7) \cong (\mathbb{Z}[x]/(x^2 + x + 1))/((7, x^2 + x + 1)/(x^2 + x + 1)).$$

Por uno de los teoremas de isomorfía, concluimos que:

$$\mathbb{Z}[w]/(7) \cong \mathbb{Z}[x]/(7, x^2 + x + 1).$$

Empleando nuevamente uno de los teoremas de isomorfía, deducimos que $\mathbb{Z}[w]/(7) \cong (\mathbb{Z}[x]/(7))/((7, x^2 + x + 1)/(7)) \cong \mathbb{F}_7[x]/(x^2 + x + 1)$. Observe que $(x^2+x+1) = (x-2)(x+3)$ y $\mathbb{F}_7[x] = (x+3)+(x-2)$. Luego, por teorema chino de los restos, deducimos que $\mathbb{Z}[w]/(7) \cong \mathbb{F}_7[x]/(x-2) \times \mathbb{F}_7[x]/(x+3) \cong \mathbb{F}_7 \times \mathbb{F}_7$. Por lo tanto $\mathbb{Z}[w]/(7)$ no es cuerpo, lo que implica que (7) no es maximal.

ii.- Observe que los ideales maximales de $\mathbb{F}_7 \times \mathbb{F}_7$ son $\mathbb{F}_7 \times \{0\}$ y $\{0\} \times \mathbb{F}_7$. Luego, los ideales maximales que contienen a (7) son las preimagenes vía la proyección canónica de los ideales maximales de $\mathbb{Z}[w]/(7) \cong \mathbb{F}_7 \times \mathbb{F}_7$. Por un cálculo vía los homomorfismos mostrados en [i] deducimos que $(w-2) \cong \{0\} \times \mathbb{F}_7$ y $(w+3) \cong \mathbb{F}_7 \times \{0\}$. Además, como $7 = (w+3)(2-w)$, tenemos que $(7, w-2) = (w-2)$ y $(7, w+3) = (w+3)$. Por lo tanto, los únicos ideales maximales que contienen a (7) son $(w-2)$ y $(w+3)$.

3.- **Problema 3:*** 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 $a = a_1 b_1$, 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 $a_1 = a_2 b_2$ 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].

4.- **Problema 4*:** 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.

5.- **Problema 5*:** 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 $a = a_1 d$, $b = b_1 d$. 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 $a_1 u + b_1 v = 1$. Por lo tanto $d = au + bv \in (a, b)$. Esto demuestra la igualdad entre los ideales citados previamente. Concluimos que A es un DIP

6.- **Problema 6:** 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.

Ayudantía 10: En esta ayudantía se exponen algunos problemas referidos a localización de anillos.

1.- **Problema 1:** Sea A anillo conmutativo con uno y S un conjunto multiplicativo.

i.- Supongamos que A es un DIP y $K = \text{Quot}(A)$. Considere $y \in K$. Pruebe son equivalentes las siguientes afirmaciones:

a.- $y \in A$.

b.- $y \in A_p$, para todo $p \subset A$ ideal primo.

c.- $y \in A_m$, para todo $m \subset A$ ideal maximal.

ii.- Demuestre, usando localización, que $\mathfrak{N}(A) = \bigcap\{p : p \subset A \text{ ideal primo}\}$.

iii.- Pruebe que si A es un DIP entonces $S^{-1}A$ es un DIP.

Desarrollo:

i.- Observe que si A es un dominio, entonces $A \hookrightarrow A_p$, para todo $p \subset A$ primo. Esto se debe a que $\ker(f_p) = \{a \in A : sa = 0, \text{algún} s \in S\} = \{0\}$, donde f_p es la función definida en el problema 3 de la ayudantía II. Luego, [a] implica [b] y [b] implica [c] claramente. Supongamos que $y \notin A$. Entonces $y = \frac{a}{b}$, donde $a \in A$ y $b \in A - A^*$. Observe que podemos suponer que $(a, b) = A$, puesto que si no es así, entonces $(a, b) = (c)$, para cierto $c \in A$. Luego $y = \frac{a}{b} = \frac{ca'}{cb'} = \frac{a'}{b}$ para ciertos $a', b' \in A$ tales que $(a', b') = A$. Por otro lado, como $b \in A - A^*$ tenemos que existe un ideal maximal m de A tal que $(b) \subset m$. Luego, si $y \in A_m$, tenemos que $\frac{a}{b} = \frac{c}{d}$, para cierto $c \in A$, $d \in m^c$. Esto último, es equivalente a que $ad = cb$, donde $bc \in m$. Por lo tanto $ad \in m$. Ahora bien, como m es un ideal primo, tenemos que $a \in m$. Por lo tanto $(a, b) \subset m$. Esto nos lleva a una contradicción.

ii.- Siempre se cumple que $\mathfrak{N}(A) \subset \bigcap\{p : p \subset A \text{ ideal primo}\}$. Esto se debe a que si $x^n = 0$, entonces como $0 \in p$ tenemos que $x^n \in p$. Luego, como p es un ideal primo, tenemos que $x \in p$. Supongamos ahora que $x \notin \mathfrak{N}(A)$. Entonces $0 \notin \{x^n\}_{n\in\mathbb{N}}$. Luego $A_x \neq 0$, donde $A_x = S^{-1}A$, para $S = \{x^n\}_{n\in\mathbb{N}}$. En particular, existe un ideal maximal M en A_x. Sea $\pi : A \to A_x$ el homomorfismo definido por $\pi(a) = \frac{a}{1}$. Entonces $p = \pi^{-1}(M)$ es un ideal primo de A. Luego, por lo visto en la guia 2, tenemos que $p \cap S = \emptyset$. En particular $x \notin p$.

iii.- Sabemos que todo ideal de $S^{-1}A$ es de la forma $S^{-1}I$, con I ideal de A. Sea $S^{-1}I$ un ideal de $S^{-1}A$. Como A es un DIP, tenemos que $I = (y)$, para cierto $y \in A$. Luego $S^{-1}I = (y)_{S^{-1}A}$. Esto concluye lo pedido.

2.- **Problema 2:** Sea A anillo conmutativo con uno y $p \subset A$ un ideal primo. Definimos el anillo A_p como la localización de A en el conjunto $S = A - p$. Definimos el homomorfismo $f_p : A \to A_p$ por $f_p(a) = \frac{a}{1}$.

i.- Sea $x \in A$. Pruebe que $f_p(x) = 0$, para todo p primo de A, si y solamente si $x = 0$.

ii.- Demuestre que A_p tiene un único ideal maximal.

iii.- Sea $A = \mathbb{Z}$ y (p) un ideal primo de $\mathbb{Z}$. Muestre que el único ideal maximal de $\mathbb{Z}_{(p)}$ es $p\mathbb{Z}_{(p)}$ y que dicho ideal cumple con $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)} \cong \mathbb{Z}/p\mathbb{Z}$.

Desarrollo:

i.- Supongamos que $x \in \ker(f_p)$, para todo p primo. Observe que $\text{Ann}(x)$ es un ideal de A. Supongamos que $\text{Ann}(x) \neq A$. Entonces existe m ideal maximal tal que $\text{Ann}(x) \subseteq m$. Luego, si consideramos $p = m$, tenemos que $x \notin \ker(f_p)$.

Esto último ya que, si $x \in \ker(f_p)$ entonces existe $s \in A - p$ tal que $sx = 0$. Luego $s \in \text{Ann}(x) \subseteq m$. Por lo tanto $\text{Ann}(x) = A$, en particular $1 \in \text{Ann}(x)$, luego $x = 0$.

ii.- Considere $m = pA_p = \left\{p\frac{t}{s} : s \in A - p,\ t \in A\right\}$. Entonces todo elemento $u = \frac{a}{s} \notin pA_p$ cumple con $\frac{s}{a} \in A$, es decir $u \in A_p^*$. Esto implica que m es un ideal maximal. Por otro lado si $n \subset A$ es otro ideal maximal, tenemos que existe $x \in n - m$. Luego $x \in n$ es invertible, lo cual nos lleva a una contradicción.

iii.- Por lo mostrado en [i] tenemos que $p\mathbb{Z}_{(p)}$ es el único ideal maximal de $\mathbb{Z}_{(p)}$. Considere el homomorfismo $g_p : \mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ definido por $g_p(a) = \overline{\left(\frac{a}{1}\right)}$. Observe que $\ker(g_p) = \{a \in \mathbb{Z} : \exists s \in \mathbb{Z} - (p), t \in \mathbb{Z} : s(a - pt) = 0\}$. Pero, como $\mathbb{Z}$ no tiene divisores de 0, tenemos que $\ker(g_p) = p\mathbb{Z}$. Luego, existe un homomorfismo inyectivo $h_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ definido por $h_p(\overline{a}) = \overline{\left(\frac{a}{1}\right)}$. Esta última función es sobreyectiva, pues si $s \notin (p)$ entonces $\overline{s} \in \mathbb{Z}/p\mathbb{Z}$ es invertible y así $h_p(\overline{as^{-1}}) = \overline{\left(\frac{a}{s}\right)}$.

3.- **Problema 3:** Sea A anillo conmutativo con uno, $S \subset A$ un conjunto multiplicativo, I un ideal de A tal que y $\pi : A \to A/I$ la proyección canónica.

i.- Sea $T = \pi(S)$. Pruebe que $S^{-1}A/S^{-1}I \cong T^{-1}(A/I)$.

ii.- Considere el anillo $B = \mathbb{Q}[x, x^{-1}]$. Encuentre un conjunto multiplicativo $S \subset \mathbb{Q}[x]$ tal que $B = S^{-1}\mathbb{Q}[x]$.

iii.- Sea $n \in \mathbb{N}$. Pruebe que $I = (x^{n-1} + px^{-1})$ es un ideal maximal de B.

Desarrollo:

i.- Considere el homomorfismo $\phi : S^{-1}A \to T^{-1}(A/I)$ definido por $\phi\left(\frac{a}{s}\right) = \frac{\overline{a}}{\overline{s}}$. Obserbe que ϕ está bien definido, pues si $t(as' - a's) = 0$, para cierto $t \in S$ entonces tomando clases módulo I tenemos que $\overline{t}(\overline{as}' - \overline{a's}) = \overline{0}$, para $\overline{t} \in T$. Claramente ϕ es sobreyectivo y $\ker(\phi) = \left\{\frac{a}{s} : \exists t \in S : t(a) \in I\right\}$. Luego, como $\frac{ta}{ts} = \frac{a}{s}$, tenemos que $\ker(\phi) = S^{-1}I$. Por primer teorema de isomorfía concluimos que $S^{-1}A/S^{-1}I \cong T^{-1}(A/I)$.

ii.- Observe que los elementos de $B = \mathbb{Q}[x, x^{-1}]$ son polinomios en las variables x y x^{-1}. Luego si $a \in B$ se tiene que $a = x^{-N}q(x)$, para cierto $N \in \mathbb{N}$ y $p(x)$ polinomio. Por lo tanto $B = S^{-1}\mathbb{Q}[x]$, donde $S = \{x^m\}_{m\in\mathbb{N}}$.

iii.- Siempre podemos escribir $I = (x^n + p)$, esto pues $x \in B$ es invertible. Luego, por la parte [i], tenemos que si $T = \{\overline{x}^m\}_{m\in\mathbb{N}} \subset \mathbb{Q}[x]/(x^n + p)$, entonces $B/I \cong T^{-1}(\mathbb{Q}[x]/(x^n + p))$. Por otro lado, tenemos que $p(x) = x^n + p$ es un polinomio irredcible en $\mathbb{Z}[x]$. Esto se debe al lema de Einsenstein mostrado en la ayudantía anterior. Observe que si $p(x) = s(x)h(x)$, donde $s(x), h(x) \in \mathbb{Q}[x]$ y $\deg(s(x)), \deg(h(x)) > 0$, entonces por lema de Gauss, tenemos que existen $S(x), H(x) \in \mathbb{Z}[x]$ tales que $\deg(s(x)) = \deg(S(x))$ y $\deg(h(x)) = \deg(H(x))$ y $p(x) = S(x)H(x)$. Esto último contradice la irreducibilidad de $p(x)$ es $\mathbb{Z}[x]$. Luego $p(x)$ es irreducible en $\mathbb{Q}[x]$. Por último, como todo elementos irreducible es primo en un DIP y todo ideal generado por un primo es maximal en un anillo de la misma naturaleza, tenemos que $(x^n + p)$ es maximal en $\mathbb{Q}[x]$. Por ende $\mathbb{Q}[x]/(x^n + p)$ es cuerpo. Concluimos que $B/I \cong T(\mathbb{Q}[x]/(x^n + p)) = \mathbb{Q}[x]/(x^n + p)$.

2.1. Interludio: Anillos p-ádicos: En esta ayudantía estudiaremos un caso especial de anillo. Definimos $\mathbb{Z}_p$ por $\lim \mathbb{Z}/p^r\mathbb{Z} = \{(a_i)_{i\in\mathbb{N}} : a_i \in \mathbb{Z}/p^i\mathbb{Z}\,, \pi_{ij}(a_j) = a_i\,, \forall j \geq i\}$, donde $\pi_{ij} : \mathbb{Z}/p^j\mathbb{Z} \to \mathbb{Z}/p^i\mathbb{Z}$ es el homomorfismo de reducción módulo p^i.

1.- **Problema 1:** Sea $S = \{\sum_{i=0}^{\infty} a_i p^i : a_i \in \{0, \cdots, p-1\}\}$.

i.- Pruebe que $S \cong \mathbb{Z}_p$.

ii.- Muestre que $\mathbb{Z}_p$ es un anillo local.

Desarrollo:

i.- Sea $\phi : S \to \mathbb{Z}_p$ la función definida por $\phi\left(\sum_{i=0}^{\infty} a_i p^i\right) = \left(\sum_{i=1}^{n-1} a_i p^i\right)_{n\in\mathbb{N}}$. Observe que ϕ está bien definida pues si $b_n = \sum_{i=1}^{n-1} a_i p^i$ entonces $\pi_{nm}(b_m) = b_n$, para todo $m \geq n$. Claramente ϕ es un homomorfismo de grupos y $\phi(1) = (1)_{n\in\mathbb{N}}$. Además, comparando cada coeficiente para el producto se series, podemos concluir que $\phi(xy) = \phi(x)\phi(y)$. Por lo tanto ϕ es un homomorfismo de anillos. Demostremos ahora que ϕ es una función biyectiva. En efecto, si $\left(\sum_{i=1}^{n-1} a_i p^i\right)_{n\in\mathbb{N}} = \left(\sum_{i=1}^{n-1} b_i p^i\right)_{n\in\mathbb{N}}$, para todo $n \in \mathbb{N}$, comparando el primer elemento en las tuplas obtenemos que $a_0 = b_0 \,(\text{mod } p)$. Luego, como $a_0, b_0 \leq p-1$, tenemos que $a_0 = b_0$. Comparando el segundo término en las tuplas obtenemos que $a_1 p = b_1 p \,(\text{mod } p^2)$, equivalentemente obtenemos que $a_1 = b_1 \,(\text{mod } p)$. Esto último implica que $a_1 = b_1$. Por inducción se obtiene que $a_i = b_i$. Luego ϕ es inyectiva. Consideremos $(b_n)_{n\in\mathbb{N}} \in \mathbb{Z}_p$. Tomamos a_1 como un representante de $b_1 \in \mathbb{Z}/p\mathbb{Z}$ tal que $a_1 \in \{0, \cdots, p-1\}$. Para encontrar un elemento a_1 tal que $\phi\left(\sum_{i=0}^{\infty} a_i p^i\right) = (b_n)_{n\in\mathbb{N}}$ hacemos lo siguiente. Imponemos la condición $a_0 + a_1 p = b_1 \,(\text{mod } p^2)$. Esto último es equivalente a que $b_0 + a_1 p = b_1 \,(\text{mod } p^2)$. Pero, como $b_0 = b_1 \,(\text{mod } p)$, tenemos que $b_0 - b_1 = pk$, para cierto $k \in \mathbb{Z}$. Consideramos entonces a_1 como un representante de k en $\{0, \cdots, p-1\}$, pues este elemento satiface la identidad $b_0 + a_1 p = b_1 \,(\text{mod } p^2)$. Por inducción determinamos cada a_i. Esto demuestra que ϕ es sobreyectiva.

ii.- Considere el ideal $pS = \{\sum_{i=1}^{\infty} a_i p^i : a_i \in \{0, \cdots, p-1\}\}$. Observe que todo un elemento $b = \sum_{i=0}^{\infty} b_i p^i \in S - pS$ es invertible. Esto último ya que $b_0 \neq 0$ y por lo tanto existe $a_0 \in \{0, \cdots, p-1\}$ tal que $a_0 b_0 = 1 + pc_1$. Luego podemos resolver la ecuación $a_0 b_1 + b_0 a_1 = 0 \,(\text{mod } p)$ y encontrar b_1. Por inducción encontramos los demás coeficientes de $b^{-1} = \sum_{i=0}^{\infty} a_i p^i$.

2.- **Problema 2:** En lo que sigue identificaremos $\mathbb{Z}_p$ con S. Sea $a \in \mathbb{Z}_p$ un elemento no nulo y supongamos que $a = \sum_{i=n}^{\infty} a_i p^i$, con $a_n \neq 0$. Definimos la valuación a por $v(a) = i$ y definimos $v(0) = \infty$. Se entiende por valor absoluto p-ádico de a a la función definida por $|a|_p = p^{-i} = p^{-v_p(a)}$ y $|0| = 0$.

i.- Demuestre que $|x+y|_p \leq \text{máx}\{|x|_p, |y|_p\}$ y $|xy|_p = |x|_p |y|_p$, para todo $x, y \in \mathbb{Z}_p$.

ii.- Pruebe que el único ideal maximal de $\mathbb{Z}_p$ es $m = \{a : |a|_p < 1\}$.

Desarrollo:

i.- Observe que ambas identidades se siguen facil si $x = 0$ o $y = 0$. Supongamos que $x, y \neq 0$. Entonces podemos escribir $x = \sum_{i=n}^{\infty} a_i p^i$ e $y = \sum_{i=m}^{\infty} b_i p^i$,

donde $a_n, b_m \neq 0$. Supongamos, sín pérdida de generalidad, que $n \geq m$. Por lo tanto $x + y = \sum_{i=m}^{\infty}(a_i + b_i)p^i$. Luego $|x + y|_p = p^s$, donde $s \geq m$. Es así como concluimos que $|x + y|_p \leq p^m = \text{máx}\{|x|_p, |y|_p\}$. Por otro lado, si el término de menor exponente de p en x es a_n y su análogo para y es b_m tenemos que el término de menor exponente para xy es $a_n b_m$. Por lo tanto $|xy|_p = p^{-n-m} = |x|_p|y|_p$.

ii.- Sabemos que el único ideal maximal de $\mathbb{Z}_p$ es $m = \{\sum_{i=1}^{\infty} a_i p^i : a_i \in \{0, \cdots, p-1\}\}$. Luego, por la defínción del valor absoluto p-ádico, tenemos que $x = \sum_{i=0}^{\infty} a_i p^i \in m$ si y solamente si $|x|_p \leq p^{-1}$. Por lo tanto, como el conjunto de valores que toma $|\cdot|_p$ es el conjunto de potencias negativas y enteras de p, concluimos que $m = \{a : |a|_p < 1\}$.

3.- **Problema 3:** Sabemos que $\mathbb{Z}$ es isomorfo a un subanillo de $\mathbb{Z}_p$.

i.- Pruebe que para todo $n \in \mathbb{Z} - \{0\}$ se tiene que $|n|_p = p^{-i}$, donde $n = p^i m$, para $(m, p) = 1$.

ii.- Muestre para todo $n \in \mathbb{Z} - \{0\}$ se cumple que $|n|_p = 1$, para casi todo p primo.

iii.- Pruebe que para todo $n \in \mathbb{Z} - \{0\}$ se cumple que $\prod_p |n|_p = \frac{1}{|n|}$, donde $|\cdot|$ es el valor absoluto usual en $\mathbb{Z}$.

Desarrollo:

i.- Observe que $|-1| = 1$. Luego podemos suponer que $n \in \mathbb{N}$. Supongamos que $n = p^i m$, donde $(m, p) = 1$. Entonces $n = 0 \pmod{p^i}$ y $n \neq 0 \pmod{p^{i+1}}$. Luego si $n = \sum_{j=0}^{\infty} a_j p^j$ tenemos que $\sum_{j=0}^{n-1} a_j p^j = 0 \pmod{p^j}$. Por comparación de términos en la igualdad anterior, concluimos que $a_j = 0$, para todo $j \leq n-1$. Por otro lado, si $a_i = 0$, tenemos que $n = 0 \pmod{p^{i+1}}$ y esto nos lleva a una contradicción. Por lo tanto $n = \sum_{j=i} a_j p^j$, donde $a_i \neq 0$. Esto implica que $|n|_p = p^{-i}$.

ii.- Sabemos que, por la factorización única de los enteros, existen finitos primos que dividan a n. Luego, todos los primos, salvo finitos de ellos, cumplen con que $(n, p) = 1$. De esto último se sigue que $|n|_p = 1$, para casi todo p primo.

iii.- Observe que el producto $\prod_p |n|_p$ está bien definido por lo mencionado en [ii]. Además, por [i], podemos restringirnos a trabajar con $n \in \mathbb{N}$. Por la factorización única en $\mathbb{Z}$ tenemos que $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Luego se cumple que $|n|_{p_i} = p_i^{-\alpha_i}$ y $|n|_q = 1$, para todo $q \neq p_i$. De esto se sigue que $\prod_p |n|_p = p_1^{-\alpha_1} \cdots p_r^{-\alpha_r} = \frac{1}{|n|}$.

3. Módulos:

Ayudantía 11: En esta ayudantía comenzaremos a estudiar módulos. Analizaremos ciertos ejemplos interesantes.

1.- **Problema 1:** Sea K una extensión finita de $\mathbb{Q}$. Decimos que $a \in K$ es un elemento entero sobre $\mathbb{Z}$ si existe $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ tal que $p(a) = 0$. Definimos el anillo de enteros de K por:

$$\mathcal{O}_K = \{a \in K : a \text{ es entero sobre } \mathbb{Z}\}.$$

i.- Pruebe que $a \in \mathcal{O}_K$ si y solamente si $\mathbb{Z}[a]$ está contenido subanillo de K el cual es un $\mathbb{Z}$-m0́dulo finitamente generado.

ii.- Muestre que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo. Demuestre que $\mathcal{O}_K$ es también un anillo.

iii.- Pruebe que $\mathcal{O}_K$ es libre de torsión.

Desarrollo:

i.- Supongamos primero que a es entero, entonces $a^n = -a_{n-1}a^{n-1} - \cdots - a_0$, para ciertos $a_i \in \mathbb{Z}$. Por lo tanto, tenemos que $a^n \in \mathbb{Z} + a\mathbb{Z} + \cdots a^{n-1}\mathbb{Z}$. De la misma forma tenemos que $a^{n+1} = -a_{n-1}a^n - \cdots - a_0 a \in \mathbb{Z} + a\mathbb{Z} + \cdots a^{n-1}\mathbb{Z}$. Por inducción $a^k \in \mathbb{Z} + a\mathbb{Z} + \cdots a^{n-1}\mathbb{Z}$, para todo $k \in \mathbb{N}$. Luego tenemos que el anillo $\mathbb{Z}[a] = \mathbb{Z} + a\mathbb{Z} + \cdots a^{n-1}\mathbb{Z}$ es un $\mathbb{Z}$-módulo finitamente generado. Inversamente, supongamos que $\mathbb{Z}[a] \subset M$, donde M es un anillo tal que, como $\mathbb{Z}$-módulo es finitamente generado. Considere $\phi : M \to M$ el $\mathbb{Z}$-homomorfismo definido por $\phi(m) = am$. Sea $\{x_1, \cdots, x_n\}$ un conjunto de generadores de M. Entonces $\phi(x_i) = \sum_{j=1}^n a_{ij}x_j$, donde $a_{ij} \in \mathbb{Z}$. Luego, tenemos que $\sum_{j=1}^n (\delta_{ij}\phi - a_{ij})(x_j) = 0$. Multiplicando por la adjunta de $(\delta_{ij}\phi - a_{ij})$ tenemos que $\det(\delta_{ij}\phi - a_{ij})(x_k) = 0$, $\forall k \in \{1, \cdots, n\}$. Es decir, la aplicación anterior es nula. Expandiendo el determinante, tenemos que existen $p(x) \in \mathbb{Z}[x]$ mónico tal que $p(\phi) = 0$. Como ϕ es el morfismo multiplicación por a, evaluando en $m = 1$, tenemos que $p(a) = 0$.

ii.- Basta probar que $\mathcal{O}_K$ es un anillo. Claramente se tiene que si $a \in \mathcal{O}_K$ entonces $-a \in \mathcal{O}_K$. Probemos que si $a, b \in \mathcal{O}_K$ entonces $ab, a + b \in \mathcal{O}_K$. Por [i], basta ver que si $\mathbb{Z}[a]$ y $\mathbb{Z}[b]$ son finitamente generados entonces $\mathbb{Z}[ab], \mathbb{Z}[a + b]$ están contiendos en anillos, los cuales como $\mathbb{Z}$-módulos son finitamente generados. Observe que por lo mostrado en [i], se tiene que existen $n, m \in \mathbb{N}$ tal que $a^t \in \mathbb{Z} + a\mathbb{Z} + \cdots a^{n-1}$ y $b^t \in \mathbb{Z} + a\mathbb{Z} + \cdots a^{m-1}$, para todo $t \in \mathbb{N}$. Luego, se tiene que $(ab)^t, (a + b)^t \in \sum_{i,j=1}^{n-1,m-1} a^i b^j \mathbb{Z}$, para todo $t \in \mathbb{N}$. Esto prueba que $\mathbb{Z}[a + b], \mathbb{Z}[ab]$ están contenidos en anillo $M = \sum_{i,j=1}^{n-1,m-1} a^i b^j \mathbb{Z}$, el cual es finitamente generado como $\mathbb{Z}$-módulo. Por [i], se concluye que $ab, a + b \in \mathcal{O}_K$.

iii.- Supongamos que existen $n \in \mathbb{N}$ y $a \in K$ tales que $na = 0$. Entonces como $na \in K$, se tiene que $n = 0$ o $a = 0$. Esto prueba que $\mathcal{O}_K$ es libre de torsión.

2.- **Problema 2:** Sea A un anillo conmutativo con uno e I un ideal de A. Considere M un A-módulo. Es un hecho, que si M, N con $A-$módulos se tiene que $\mathrm{Hom}_A(M, N)$ es un A-módulo con las operaciones definidas punto a punto.

i.- Determine $\mathrm{Hom}_A(A^n, M)$. Concluya que $\mathrm{Hom}_A(A^n, A/I) \cong (A/I)^n$.

ii.- Determine $\mathrm{Hom}_A(M, A^n)$.

iii.- Calcule $\mathrm{Hom}_A(A/I, A^n)$.
Desarrollo:

i.- Considere $\phi : A^n \to M$ un homomorfismo cualquiera. Observe que ϕ está unívocamente determinado por $\phi(e_i)$, donde $e_i = (0, \cdots, 1, \cdots, 0)$. Esto pues si $a = \sum_{i=1}^n a_i e_i$ entonces $\phi(a) = \sum_{i=1}^n a_i \phi(e_i)$. Como $\phi(e_i) \in M$ tenemos que ϕ está completamente determinada por su valor en una tupla de M^n. Observe además que toda tupla en $(m_i)_{i=1}^n \in M^n$ define un homomorfismo, por $\phi(a) = \sum_{i=1}^n a_i \phi(e_i)$, donde $a = \sum_{i=1}^n a_i e_i$. Este homomorfismo está bien definido, pues todo elemento $a \in A^n$ se escribe de forma única como $a = \sum_{i=1}^n a_i e_i$, con $a_i \in A$. Luego, tenemos una función biyectiva $\psi : \mathrm{Hom}_A(A^n, M) \to M^n$. Esta función es un homomorfismo de A-módulos dado que $\psi(a\phi_1 + \phi_2) = (a\phi_1(e_i) + \phi_2(e_i))_{i=1}^n = a\psi(\phi_1) + \psi(\phi_2)$. Luego $\mathrm{Hom}_A(A^n, M) \cong M^n$, en particular tenemos que $\mathrm{Hom}_A(A^n, A/I) \cong (A/I)^n$.

ii.- Observe que todo homomorfismo $\phi : M \to A^n$ está univocamente determinado por los homomorfismos $\phi_i : M \to A$, donde $\phi_i = \pi_i \circ \phi$. Además, si consideramos n homomorfismos $f_i : M \to A$, tenemos que la función $\phi : M \to A^n$ definida por $\phi = (f_i)_{i=1}^n$ es un homomorfismo de A-módulos. Por último como $\pi_i(f + ag) = \pi_i(f) + a\pi_i(g)$, para todo $f, g \in \mathrm{Hom}_A(M, A^n)$, tenemos que $\mathrm{Hom}_A(M, A^n) \cong \mathrm{Hom}_A(M, A)^n$.

iii.- Por otro lado, si $M = A/I$ tenemos que todo homomorfismo $h : A/I \to A$ está determinado por la imagen de $h(\overline{1})$. Esto se debe a que $h(\overline{a}) = ah(\overline{1})$, para todo $a \in A$. El elemento $h(\overline{1})$ cumple con $0 = h(\overline{0}) = h(\overline{i}) = ih(\overline{1})$, para todo $i \in I$. Además cualquier $b \in A$ tal que $ib = 0$, $\forall i \in I$ define un homomorfismo por $h(\overline{a}) = ab$. Por lo tanto $\mathrm{Hom}_A(A/I, A) \cong \{a \in A : ai = 0, \forall i \in I\}$. De esto se sigue que $\mathrm{Hom}_A(A/I, A^n) \cong \{(a_k)_{k=1}^n \in A^n : a_k i = 0, \forall i \in I, \forall k \in \{1, \cdots, n\}\}$.

3.- **Problema 3*:** Sea A un anillo y M un A-módulo noetheriano, es decir un A-módulo donde toda cadena creciente de submódulos:

$$M_0 \subseteq M_1 \subseteq M_2 \cdots \subseteq M_n \subseteq \cdots,$$

cumple con $M_n = M_N$, para todo $n \geq N$ fijo. Suponga que $f : M \to M$ es un A-homomorfismo epiyectivo. Demuestre que f es inyectivo.
Demostración: Basta probar que $\ker(f) = \{0\}$. En efecto considere la cadena de A-submódulos de M definida por:

$$\ker(f) \subseteq \ker(f^2) \subseteq \cdots \subseteq \ker(f^2) \subseteq \cdots$$

Por la condición de noetherianidad tenemos que existe $N \in \mathbb{N}$ tal que $\ker(f^n) = \ker(f^N)$, para todo $n \geq N$. Considere $v_1 \in \ker(f)$. Por la sobreyectividad de f existe $v_2 \in M$ tal que $v_1 = f(v_2)$. Haciendo uso nuevamente de la sobreyectividad de f deducimos que existe $v_3 \in M$ tal que $v_2 = f(v_3)$. En general podemos encontrar $v_k \in M$ tal que $f(v_k) = v_{k-1}$. Por lo tanto:

$$0 = f(v_1) = f^2(v_2) = \cdots = f^{N+1}(v_{N+1}).$$

Esto implica que $v_{N+1} \in \ker(f^{N+1})$. Luego, como $\ker(f^N) = \ker(f^{N+1})$, se tiene que $v_{N+1} \in \ker(f^N)$. Es decir $0 = f^N(v_{N+1})$. Concluimos que:

$$0 = f^N(v_{N+1}) = f^{N-1}(v_N) = \cdots = f^1(v_2) = v_1,$$

lo cual demuestra lo pedido.

Ayudantía 12: En esta ayudantía estudiaremos el teorema de estructura de módulos finitamente generados sobre DIP.

1.- **Problema 1:** Sea V un $\mathbb{C}$-espacio vectorial de dimensión finita y $T : V \to V$ una transformación lineal. Definimos en V la estructura de $\mathbb{C}[x]$-módulo por $p(x).v = p(T)(v)$.

i.- Demuestre que V es $\mathbb{C}[x]$-módulo de torsión.

ii.- Encuentre todos los elementos primos en $\mathbb{C}[x]$. Concluya que existe un isomorfismo de $\mathbb{C}[x]$-módulo:

$$V \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}}),$$

donde $e_{i1} \leq \cdots \leq e_{ia_i}$.

iii.- Demuestre el teorema de Jordan que da forma canónica a T. Establezca la relación entre la torsión de V, los valores propios de T y el polinomio minimal de T.

Desarrollo:

i.- Supongamos que $\dim_{\mathbb{C}}(V) = n < \infty$. Para cualquier $v \in V$ se tiene que $\{T^i(v)\}_{i=0}^{n}$ es un conjunto l.d. Luego existen constantes $a_0, \cdots, a_n \in K$, no todas nulas, tales que $\sum_{i=0}^{n} a_i T^i(v) = 0$. Es decir, para $p(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{C}[x] - \{0\}$ se tiene que $p(x).v = 0$. Por lo tanto V es un $\mathbb{C}[x]$-módulo de torsión.

ii.- Sea $p(x)$ un elemento primo en $\mathbb{C}[x]$ cualquiera. Observe que, por el teorema fundamental del álgebra, se tiene que existe $z \in \mathbb{C}$ tal que $(x-z)|p(x)$, es decir $p(x) = (x-z)q(x)$. Pero como $p(x)$ es primo, en un DIP, se tiene que $p(x)$ es irreducible. Luego $q(x) = c \in \mathbb{C}$ constante. Por ello $p(x) = (x-z)$, algún $z \in \mathbb{C}$ o algún asociado a $(x-z)$. Por otro lado $p(x) = x-z$ es primo ya que $\mathbb{C}[x]/(x-z) \cong \mathbb{C}$. Dicho isomorfismo se establece vía el homomorfismo evaluación en z. Por el teorema de estructura de módulos sobre DIP, tenemos que $V \cong \mathbb{C}[x]^s \oplus \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} \mathbb{C}[x]/(p_i(x))^{e_{ij}})$, donde $e_{i1} \leq \cdots \leq e_{ia_i}$ y $p_i(x)$ es primo en $\mathbb{C}[x]$. Pero como V es un $\mathbb{C}[x]$-módulo de torsión, se tiene que $s = 0$. Además, por lo anterior, tenemos que $p_i(x) = x - \lambda_i$, para ciertos $\lambda_i \in \mathbb{C}$.

iii.- Partamos demostrando el teorema de Jordan. Sabemos que existe $\phi : V \to \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$ isomorfismo, donde $e_{i1} \leq \cdots \leq e_{ia_i}$. Considere $W_{ij} = \phi^{-1}\left(\mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})\right)$. Observe que W_{ij} es un subespacio vectorial de V, pues W_{ij} es un $\mathbb{C}[x]$-submódulo, en particular un $\mathbb{C}$-submódulo. Observe que el isomorfismo ϕ, al restringirlo a W_{ij}, establece un isomorfismo $W_{ij} \cong \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$. Por lo tanto $\mathrm{Ann}(W_{ij}) = \mathrm{Ann}\left(\mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})\right) = (x-\lambda_i)^{e_{ij}}$. Luego existe $w = w_{ij} \in W_{ij}$ tal que $(T-\lambda_i I)^{e_{ij}}(w) = (x-\lambda_i)^{e_{ij}}.w = 0$, pero $(T-\lambda_i I)^{e_{ij}-1}(w) = (x-\lambda_i)^{e_{ij}-1}.w \neq 0$. Observe que el isomorfismo $W_{ij} \cong \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$ es en particular un isomorfismo de $\mathbb{C}$-módulos. Por lo tanto:

$$\dim_{\mathbb{C}} W_{ij} = \dim_{\mathbb{C}} \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}}) = e_{ij}.$$

Considere el conjunto $\beta = \{w, N(w), \cdots, N^{e_{ij}-1}(w)\} \subset W_{ij}$, donde $N = T - \lambda_i I$. Observe que si $\sum_{k=0}^{e_{ij}-1} a_k N^k(w) = 0$ para ciertos $a_k \in \mathbb{C}$, entonces aplicando $N^{e_{ij}-1}$ a la suma anterior, obtenemos que $a_0 = 0$. Luego, si

aplicamos $N^{e_{ij}-2}$ a la suma resultante, se obtiene que $a_1 = 0$ y así inductivamente deducimos que $a_i = 0$, $\forall i$. Por lo tanto β es un conjunto linealmente independiente de W_{ij}. De esta forma onbtenemos que β es base de W_{ij}. En esta base N se ve como una matriz de la forma:

$$[N] = \begin{bmatrix} 0 & \cdots & 0 & 0 \\ 1 & \cdots & 0 & 0 \\ \vdots & & & \\ 0 & \cdots & 1 & 0 \end{bmatrix},$$

es decir como un bloque nilpotente. En la misma base $T = N + \lambda_i I$ tiene asociada la matriz:

$$[T|_{W_ij}] = \begin{bmatrix} \lambda_i & \cdots & 0 & 0 \\ 1 & \cdots & 0 & 0 \\ \vdots & & & \\ 0 & \cdots & \lambda_i & 0 \\ 0 & \cdots & 1 & \lambda_i \end{bmatrix} \in \mathbb{M}_{e_{ij}}(\mathbb{C}).$$

Si tomamos por base de V a la unión de las bases de los subespacios W_{ij}, obtenemos al forma de Jordan para T. Observe que los polinomios primos lineales que participan de la descomposición de V como $\mathbb{C}[x]$-módulo, determinan los valores propios de T. Además se tiene que $\min_T(x) = \prod_{i=1}^{n}(x - \lambda_i)^{e_{ia_i}}$, pues la potencia e_{ia_i} es la minima tal que cada bloque asociado al autovalor λ_i se anula.

Observación 1. *Notar que en la descomposición anterior el cuerpo de escalares $\mathbb{C}$ puede ser reemplazado por cualquier otro cuerpo que contenga a todos los valores propios de T y la forma de Jordan anterior se obtienen análogamente. Por otro lado, si el cuerpo de escalares no contiene todos los valores propios de T entonces solo podemos descomponer V como suma de cocientes de $F[x]$ por potencias de polinomios primos.*

2.- **Problema 2*:** Sea V un $\mathbb{Q}$-espacio vectorial tal que $\dim_{\mathbb{Q}}(V) = n < \infty$ y sea $T : V \to V$ una transformación lineal tal que:

$$v = T(T(T(v))) + T(T(v)), \quad v \in V, \tag{5}$$

Demuestre que n es divisible por 3.

Demostración: Considere la acción de $\mathbb{Q}[x]$ sobre V por $x.v = T(v)$. Observe que la condición (5) implica que $(x^3 + x^2 + 1) \subset \text{Ann}(V)$. Notar que $x^3 + x^2 + 1$ es un polinomio irreducible sobre $\mathbb{Q}[x]$, pues no tiene raices racionales. Por otro lado, como $\mathbb{Q}[x]$ es un DIP, tenemos que existe $p(x) \in \mathbb{Q}[x]$ tal que $\text{Ann}(V) = (p(x))$. Esto implica que $(x^3 + x^2 + 1) \subset (p(x))$ y por la irreducibilidad de $x^3 + x^2 + 1$ tenemos que $p(x) = (x^3 + x^2 + 1)^t$, donde $t = 0, 1$. Note que si $p(x) = 1$ entonces $1 \in \text{Ann}(V)$, luego $0 = 1.v = v$, para todo $v \in V$. Esto implica que $n = 0$, y este número cumple con ser divisible por 3. Por otro lado, si $n \neq 0$, por el teorema de estructura de módulos sobre DIP, tenemos que existen polinomios $p_1, \cdots, p_m$ irreducibles sobre $\mathbb{Q}[x]$ y

distintos tales que existe un $\mathbb{Q}[x]$-isomorfismo:

$$V \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} \mathbb{Q}[x]/(p_i(x)^{e_{ij}}),$$

donde $e_{i1} \leq \cdots \leq e_{ia_i}$. Dada esta descomposición tenemos que $p(x) = \prod_{i=1}^{m} p_i(x)^{e_{ia_i}}$. Luego $m = 1$, $e_{1j} = 1$ y $p_1(x) = (x^2 + x^2 + 1)$. Por lo tanto tenemos que:

$$V \cong \bigoplus_{j=1}^{a_1} \mathbb{Q}[x]/(x^3 + x^2 + 1).$$

Como el isomorfismo anterior es en particular un $\mathbb{Q}$-isomorfismo, tenemos que $n = 3\sum_{j=1}^{a_1} 1 = 3a_1$, luego n es divisible por 3.

3.- **Problema 3*:** Sea F un cuerpo, sea V un F-espacio vectorial de dimensión finita, y sea $T : V \to V$ una transformación lineal. Un vector $v \in V$ se dice cíclico para T si $\{v, T(v), T^2(v), \cdots\}$ genera V. Suponga que todo $v \in V - \{0\}$ es un vector cíclico para T. Demuestre que el polinomio característico de T es irreducible sobre F.
Demostración: Sea $V \cong \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} F[x]/(p_i(x)^{e_{ij}})$ la descomposición de Jordan de V sobre el cuerpo F, donde $p_i(x) \in F[x]$ es irreducible. Notar que $n = \sum^{m} \sum^{a_i} \deg(p_i)e_{ij}$. Luego, como el polinomio minimal de T es:

$$m(x) = \prod_{i=1}^{m} p_1(x)^{e_{ij}}, \text{ donde } r = \deg(m),$$

tenemos que el conjunto $\langle\{v, \cdots, T^r(x)\}\rangle = \langle\{v, T(v), \cdots\}\rangle = V$. Esto prueba que $n \leq r$, lo cual es imposible, salvo si cada $a_i = 1$. Por lo tanto:

$$V \cong \bigoplus_{i=1}^{m} F[x]/(p_i(x)^{e_{i1}}).$$

Considere $w \in V$ como el vector correspondiente a la preimagen del elemento $(\overline{1}, \overline{0}, \cdots, \overline{0})$ vía el isomorfismo anterior. Entonces $p_1(x)^{e_{i1}}.w = 0$. Reescribiendo el conjunto generador asociado a las pontencias $T^i(w)$ concluimos que w no es cíclico, salvo si $n = \sum_{i}^{m} \deg(p_i)e_{i1} = \deg(p_1)e_{11}$. De esto se sigue que $m = 1$. Es por esto que:

$$V \cong F[x]/(p_1(x)^{e_{11}}).$$

Finalmente considerando $v \in V$ como la preimagen de $p_1(x)^{e_{11}-1}$ vía el isomorfismo anterior, tenemos que $p_1(x).v = 0$. Por ende v no es un vector cíclico, salvo si $e_{11} = 1$. De esto se sigue que $V \cong F[x]/(p_1(x))$. Por lo tanto el polinomio irreducible de T es $p_1(x)$, polinomio que sabemos es irreducible por hipótesis.

4.- **Problema 4*:** Sea $E_{1,1}, \cdots, E_{n,n}$ la base canónica de $\mathbb{M}_n(\mathbb{C})$. Sea $T : \mathbb{M}_n(\mathbb{C}) \to \mathbb{M}_n(\mathbb{C})$ definida por $T(E_{i,j}) = E_{i-1,j+1}$ donde los subíndices se entienden módulo n. Encuentre la forma de Jordan de T y demuestre su respuesta.
Demostración: Note que $T^n(E_{i,j}) = E_{i-n,j+n} = E_{i,j}$, para todo $i, j \in \{1, \cdots, n\}$. Por lo tanto $T^n = \text{id}$. Esto implica que el polinomio minimal de T divide a $p(x) = x^n - 1$. Notar que $p(x)$ es un polinomio cuyas raices son

$\{\zeta_n^i\}_{i=0}^n$ las raices n-ésimas de la unidad. Luego, por lo visto en el Problema 1, tenemos que:

$$\mathbb{M}_n(\mathbb{C}) \cong \prod_{\text{algunos j}} \prod_{k=1}^{a_j} \mathbb{C}[x]/(x-\zeta_n^j).$$

En lo que sigue determinaremos cuales raices de la unidad son autovalores de T y determinaremos la dimensión a_j de los espacios propios. Sea $w_j = E_{1,1}+\zeta_n^j T(E_{1,1})+\cdots+\zeta_n^{j(n-1)}T^{n-1}(E_{1,1}) \in \mathbb{M}_n(\mathbb{C})$, entonces por definición de w_j, tenemos que $T(w_j) = \zeta_n^j w_j$. Luego todas las raices de la unidad son autovalores de T. Note que si $w = \sum_{i,j} \alpha_{i,j}E_{i,j}$ es un autovector de T asociado al autovalor $\eta = \zeta_n^j$, entonces igualando los escalares en la identidad:

$$T(w) = \eta w,$$

obtenemos que $\alpha_{i,j} = \eta\alpha_{i-1,i+1} = \eta^2\alpha_{i-2,j+2} = \cdots = \eta^{n-1}\alpha_{i-n+1,j+n-1}$. Por ende hay n vectores linealmente independientes en el espacio propio asociado al autovalor η. Concluimos que la forma de Jordan de T está constituida por n-bloques diagonales asociados a los autovalores $\{\zeta_n^i\}_{i=0}^n$, todos de simensión n.

5.- **Problema 5:** Sea K una extensión finita de $\mathbb{Q}$ y considere el anillo $\mathcal{O}_K = \{x \in K : x \text{ es entero sobre } \mathbb{Z}\}$.

i.- Usando el hecho de que $\mathcal{O}_K$ es finitamente generado, muestre que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre.

ii.- Pruebe que $K/\mathcal{O}_K$ es un $\mathbb{Z}$-módulo de torsión.

iii.- Usando el hecho, de que K es un $\mathbb{Z}$-módulo de rango[2] $n = [K : \mathbb{Q}]$, concluya que $\mathcal{O}_K$ tiene rango n.

Desarrollo:

i.- Sabemos que $\mathcal{O}_K$ es un módulo libre de torsión y finitamente generado. Como $\mathbb{Z}$ es un DIP, podemos concluir que $\mathcal{O}_K \cong \mathbb{Z}^t$, para cierto $t \in \mathbb{N}$.

ii.- Sea $x \in K$ un elemento cualquiera. Sea $n = [K : \mathbb{Q}]$. Observe que el conjunto $\{1, x, \cdots, x^n\}$ es linealmente dependiente. Por lo tanto existen constantes $a_0, \cdots, a_n \in \mathbb{Q}$, no todas nulas, tales que $\sum_{i=0}^n a_i x^i = 0$. Multiplicando por el máximo común divisor de los divisores de $a_i \in \mathbb{Q}$, obtenemos $b_i \in \mathbb{Z}$, no todos nulos, tales que $\sum_{i=0}^n a_i x^i = 0$. Sín perdida de generalidad podemos admitir que $a_n \neq 0$. Multiplicando la última igualdad por a_n^{n-1} obtenemos $(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$. Luego $a_n x \in \mathcal{O}_K$. Esto implica que $K/\mathcal{O}_K$ es un $\mathbb{Z}$-módulo de torsión.

iii.- Lo probado en [ii], junto con el teorema de estructura, prueba que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de rango $n = [K : \mathbb{Q}]$.

[2]Esto será demostrado cuando estudiemos tensores

Ayudantía 13: En esta ayudantía estudiaremos el módulo $\mathrm{Hom}_A(M,N)$ y daremos algunos ejemplos importantes al respecto.

1.- **Problema 1:** Sea A un anillo con uno y suponga que existen anillos con unidad A_1, A_2 tales que $A = A_1 \times A_2$. Sea M un A-módulo.

i.- Pruebe que $M \cong M_1 \times M_2$, donde M_1 es un A_1-módulo y M_2 es un A_2-módulo.

ii.- Demuestre que todo $\mathbb{Q}[x]/(x^2-2x-3)$-módulo es libre sobre $\mathbb{Q}$.

Desarrollo:

i.- Sean $(1,0),(0,1) \in A$ y consideremos $M_1 = (1,0)M$, $M_2 = (0,1)M$. Observe que M_1, M_2 son A-módulos pues $(a,b)(1,0)M = (1,0)(a,b)M \subset (1,0)M$ y lo mismo se cumple para M_2. Además, si $n \in M_1 \cap M_2$ entonces $n = (1,0)m = (0,1)m'$. Luego, multiplicando la ecuación anterior por $(1,0)$ obtenemos que $(1,0)n = (1,0)m = 0$, es decir $n = 0$. Además todo $m \in M$ se escribe como $m = (1,0)m + (0,1)m$. Esto nos dice que $M \cong M_1 \oplus M_2$. Además tenemos que $(a,b)(1,0)m = (a,0)m$, para todo $(a,b) \in A$. Por lo tanto A_1 actúa en M_1 de la misma forma que actúa A. Esto implica que M_1 es un A_1-módulo. Por la misma razón M_2 es un A_2-módulo.

ii.- Sea M un $\mathbb{Q}[x]/(x^2-2x-3)$-módulo. Observe que, por teorema chino de los restos, tenemos que $\mathbb{Q}[x]/(x^2-2x-3) \cong \mathbb{Q} \times \mathbb{Q}$. Luego $M \cong M_1 \times M_2$, donde M_1, M_2 son $\mathbb{Q}$-módulos, es decir M_1, M_2 son $\mathbb{Q}$-espacios vectoriales. Como en todo espacio vectorial existe una base, se tiene que M es suma directa de módulos libre y en particular es un módulo libre.

2.- **Problema 2:** Sea A un anillo conmutativo con uno y sea $\{M_i\}_{i\in I}$ una colección, posiblemente infinita, de A-módulos.

i.- Demuestre que $\mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) \cong \prod_{i\in I} \mathrm{Hom}_A(M_i,N)$.

ii.- Muestre que si M es un A-módulo libre entonces $\mathrm{Hom}_A(M,N) \cong \prod_{i\in I} N$.

Desarrollo:

i.- Sea $f \in \mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right)$ y considere $f_i : M_i \to N$ definido por $f_i(m_i) = f((\delta_{ij}m_i)_{i\in I})$, donde δ_{ij} es la función delta de Kronecker. Observe que f_i es un homomorfismo pues f lo es. De esta forma obtenemos un homomorfismo $\phi : \mathrm{Hom}_A\left(\bigoplus_{i\in I} M_i, N\right) \to \prod_{i\in I} \mathrm{Hom}_A(M_i,N)$ definido por $\phi(f) = (f_i)_{i\in I}$. Observe que $\phi(f) = 0$ implica que $f_i = 0$, para todo $i \in I$. Luego tenemos que $f((m_i)_{i\in I}) = \sum_{\text{sop. fin.}} f(m_i) = \sum_{\text{sop. fin.}} f_i(m_i) = 0$. Por lo tanto ϕ es inyectiva. Sea $(f_i)_{i\in I} \in \prod_{i\in I} \mathrm{Hom}_A(M_i,N)$ y definimos $f \in \left(\bigoplus_{i\in I} M_i, N\right)$ por $f(m) = \sum_{\text{sop. fin.}} f_i(m_i)$, donde $m = \sum_{\text{sop. fin.}} m_i$. Observe que si $m = \sum_{\text{sop. fin.}} m_i$ y $n = \sum_{\text{sop. fin.}} n_i$, entonces para $a \in A$ tenemos que $m + an = \sum_{\text{sop. fin.}} m_i + an_i$, tomando un conjunto suficientemente grande por soporte. De esta manera tenemos que $f(m+an) = f(m) + af(n)$. Por ello f es un homomorfismo de módulos. Concluimos que ϕ es un isomomorfismo.

ii.- Basta observar que si M es libre, entonces $M \cong \bigoplus_{i\in I} A$. De esto se sigue que $\mathrm{Hom}_A(M,N) \cong \prod_{i\in I} \mathrm{Hom}_A(A,N) \cong \prod_{i\in I} N$, pues $\mathrm{Hom}_A(A,N) \cong N$.

3.- **Problema 3:** Pruebe que $0 \to Y' \xrightarrow{f} Y \xrightarrow{g} Y''$ es una sucesión exacta si y solamente si $0 \to \mathrm{Hom}_A(X,Y') \xrightarrow{f^*} \mathrm{Hom}_A(X,Y) \xrightarrow{g^*} \mathrm{Hom}_A(X,Y'')$ es exacta, para todo A-módulo X.

Demostración: Supongamos que $0 \to Y' \xrightarrow{f} Y \xrightarrow{g} Y''$ es una sucesión

exacta. Recordemos que en general $t^*(h) = t \circ h$. Es facil demostrar, a partir de la definición anterior, que $g^* \circ f^* = (g \circ f)^*$. Luego, en nuestro caso tenemos que $g^* \circ f^* = 0$. En particular, se cumple que $\text{Im}(f^*) \subset \ker(g^*)$. Sea $h \in \ker(g^*)$, es decir $g \circ h(x) = 0$, para todo $x \in X$, es decir $h(x) \in \ker(g)$, para todo $x \in X$. Por la exactitud de $Y' \xrightarrow{f} Y \xrightarrow{g} Y''$, tenemos que existe $y_x \in Y'$ tal que $h(x) = f(y_x)$. Observe que, por la inyectividad de f, para cada $x \in X$ existe un único elemento $y_x \in Y'$ tal que $h(x) = f(y_x)$. De esta forma tenemos que existe $\tau : X \to Y'$ función definida por $\tau(x) = y_x$ tal que $h = f \circ \tau$. Se sigue, del hecho de que h, f son homomorfismos de módulos, que τ es homomorfismo. Esto prueba que $\text{Im}(f^*) \supset \ker(g^*)$. Solo nos resta probar que f^* es inyectivo. Supongamos que $h \in \ker(f^*)$, entonces $f \circ h(x) = 0$, para todo $x \in X$. Se sigue, de la inyectividad de f, que $h(x) = 0$, para todo $x \in X$. Supongamos ahora que $0 \to \text{Hom}_A(X, Y') \xrightarrow{f^*} \text{Hom}_A(X, Y) \xrightarrow{g^*} \text{Hom}_A(X, Y'')$ es exacta, para todo A-módulo X. Considere $X = A$, entonces, por lo visto en el Problema 2, tenemos que $\text{Hom}_A(X, Y) \cong Y$. Se sigue de $f \circ h(1) = f(h(1))$, que el homomorfismo $Y' \to Y$ inducido por f^*, vía los isomorfismos anteriores, es f. Lo mismo vale para g. De esto concluimos que $0 \to Y' \xrightarrow{f} Y \xrightarrow{g} Y''$ es una sucesión exacta.

4.- **Problema 4:** Sea I un A-módulo. Decimos que I es un módulo inyectivo si dados homomorfismos $g : M' \to I$ y $f : M' \to M$ inyectivo, existe un homomorfismo $h : M \to I$ tal que $g = h \circ f$.

i.- Muestre que I inyectivo si y solamente si $\text{Hom}_A(\cdot, I)$ es exacto.

ii.- Muestre que si I inyectivo entonces $0 \to I \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ escinde.

iii.- Concluya que si I es inyectivo y I es un submódulo de M entonces existe un submódulo Q de M tal que $I \oplus Q = M$.

Desarrollo:

i.- Probemos que I inyectiva implica que $\text{Hom}_A(\cdot, I)$ es exacto. Es un ejercicio, de la misma complejidad que el Problema 3, demostrar que si $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ es una sucesión exacta entonces $0 \to \text{Hom}_A(M'', I) \xrightarrow{g_*} \text{Hom}_A(M, I) \xrightarrow{f_*} \text{Hom}_A(M', I)$ es exacta, independiente de la hipótesis de inyectividad en I. Por ello, solo debemos probar la sobreyectivdad de f_*. Sea $\tau \in \text{Hom}_A(M', I)$, entonces como f es inyectiva e I es inyectivo tenemos que existe $h \in \text{Hom}_A(M, I)$ tal que $\tau = h \circ f = f_*(h)$. Ahora supongamos que $\text{Hom}_A(\cdot, I)$ es exacto. Sea $\tau : M' \to I$ y $f : M' \to M$ inyectiva. Considere la sucesión exacta $0 \to M' \xrightarrow{f} M \xrightarrow{\pi} M/\text{Im(f)} \to 0$, entonces existe la sucesión exacta larga $0 \to \text{Hom}_A(M/\text{Im}(f), I) \xrightarrow{\pi_*} \text{Hom}_A(M, I) \xrightarrow{f_*} \text{Hom}_A(M', I) \to 0$. En particular f_* es sobreyectiva. Luego para $\tau : M' \to I$ existe $h : M \to I$ tal que $\tau = f_*(h) = h \circ f$.

ii.- Supongamos que I es inyectivo y sea $0 \to I \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta. Entonces considerando $g = id : I \to I$ tenemos que existe $h : M \to I$ tal que $id = h \circ f$. Por lo tanto $0 \to I \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ una sucesión exacta escindida.

iii.- Considere la sucesión exacta $0 \to I \xrightarrow{i} M \xrightarrow{\pi} M/I \to 0$. Entonces como I es inyectivo, tenemos que la sucesión exacta anterior escinde, es decir existe

$h : M \to I$ tal que $h \circ i = id$. Luego, como la escisión de sucesiones exactas de módulos es equivalente a la escritura como producto, tenemos que $M = \mathrm{Im}(i) \oplus \ker(h) = I \oplus \ker(h)$. Se concluye lo pedido tomando $Q = \ker(h)$.

Ayudantía 14: En esta ayudantía estudiaremos tensores de módulos y en particular trabajaremos con algunos ejemplos de módulos sobre DIP.

1.- **Problema 1:** Sean $(M_i)_{i\in I}$ un conjunto de A-módulos, $M = \oplus_{i\in I} M_i$ y N un A-módulo cualquiera. Demuestre que:

$$M \otimes_A N \cong \bigoplus_{i\in I} M_i \otimes N.$$

Demostración: Por claridad, en lo que sigue denotaremos a los elementos de la suma directa M como sumas finitas de elementos en M_i, $i \in I$. Considere el A-homomorfismo bilineal $f : M \times N \to \bigoplus_{i\in I} M_i \otimes N$ definido por $f(\sum m_i, n) = \sum m_i \otimes n$. Luego, por la propiedad universal del producto tensorial, tenemos que existe una única función A-lineal $\psi : M \otimes N \to \bigoplus_{i\in I} M_i \otimes N$ tal que $\psi(\sum m_i \otimes n) = \sum m_i \otimes n$. Por otro lado, exite el A-morfismo bilineal $g : M_i \times N \to M \otimes N$ definido por $g(m_i, n) = m_i \otimes n$, en donde en el miembro de la izquierda entendemos que $m_i \in M$. Nuevamente por la propiedad universal del producto tensorial, tenemos que existe $g' : M_i \otimes N \to M \otimes N$ definido por $g(m_i \otimes n) = m_i \otimes n$. Por ende podemos construir el A-homomorfismo:

$$\phi : \bigoplus_{i\in I} M_i \otimes N \to M \otimes N,$$

definido por $\phi(\sum m_i \otimes n_i) = \sum m_i \otimes n_i$, donde cada $n_i \in N$. Finalmente, es sencillo probar que $\psi \circ \phi = \mathrm{id}_{M\otimes_A N}$ y que $\phi \circ \psi = \mathrm{id}_{\bigoplus_{i\in I} M_i\otimes N}$. Esto concluye lo pedido.

2.- **Problema 2:** Sea M un A-módulo y $S \subset A$ un conjunto multiplicatico con uno. Se define el módulo localizado $S^{-1}M$ por:

$$S^{-1}M = \left\{ \frac{m}{s} : m \in M,\ s \in S \right\},$$

con la identificación $\frac{m}{s} = \frac{m'}{s'} \Leftrightarrow \exists t \in S :\ t(s'm - sm') = 0$. Tomando $M = A$ y empleando la misma construcción podemos definir el anillo localizado $S^{-1}A$, el cual resulta ser un anillo con la multiplicación evidente.

i.- Pruebe que $S^{-1}M$ es un $S^{-1}A$-módulo.

ii.- Muestre que $M \otimes_A S^{-1}A \cong S^{-1}M$.

iii.- Concluya que si A es un DI y $K = \mathrm{Quot}(A)$ entonces $M \otimes_A K$ es un K-módulo libre.

Desarrollo:

i.- Definimos la acción de $S^{-1}A$ sobre $S^{-1}M$ por $\frac{a}{s}.\frac{m}{t} = \frac{am}{st}$, donde $a \in A$, $s, t \in S$ y $m \in M$. Observe que si $\frac{a}{s} = \frac{a'}{s'}$ y $\frac{m}{t} = \frac{m'}{t'}$ entonces existen $s'', t'' \in S$ tales que $s''(as' - a's) = 0$ y $t''(t'm - tm') = 0$. Luego tenemos que $s''t''(s't'am - sta'm') = 0$. Por lo tanto la acción está bien definida. Es relativamente sencillo demostrar que se cumplen los axiomas de módulo en este caso.

ii.- Considere el A-morfismo bilineal $\phi : M \times S^{-1}A \to S^{-1}M$ definido por $\phi\left(m, \frac{a}{s}\right) = \frac{am}{s}$. Se sigue, de un argumento análogo al dado en [i], que ϕ está bien definido. Por la propiedad universal del producto tensorial tenemos que existe un único homomorfismo de A-módulos $\psi : M \otimes_A S^{-1}A \to S^{-1}M$

tal que $\psi\left(m \otimes \frac{a}{s}\right) = \phi\left(m, \frac{a}{s}\right) = \frac{am}{s}$. Por otro lado, considere la función $\varphi : S^{-1}M \to M \otimes_A S^{-1}A$ definida por $\varphi\left(\frac{m}{s}\right) = m \otimes \frac{1}{s}$. Observe que φ está bien definida, pues si $\frac{m'}{s'} = \frac{m}{s}$ entonces existe $t \in S$ tal que $ts'm = tsm'$, luego tenemos que $m \otimes \frac{1}{s} = ts'm \otimes \frac{1}{ts's} = tsm' \otimes \frac{1}{ts's} = m' \otimes \frac{1}{s'}$. Observe que $\varphi \circ \psi = id_{M \otimes S^{-1}A}$ y $\psi \circ \varphi = id_{S^{-1}M}$. Luego tenemos que ψ es un homomorfismo biyectivo. Concluimos que ψ es un isomorfismo.

iii.- Se deduce, de lo mostrado en [i] e [ii] que $M \otimes_A K$ es un K-módulo. Luego tenemos que $M \otimes_A K$ es un K-espacio vectorial. Por lo tanto $M \otimes_A K$ es libre sobre K.

3.- **Problema 3:** Sea K una extensión finita de $\mathbb{Q}$ y considere:

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ es entero sobre } \mathbb{Z}\}.$$

i.- Pruebe que en general, si $M = A^n \oplus \text{Tor}(M)$ y $K = \text{Quot}(A)$ entonces $M \otimes_A K \cong K^n$.

ii.- Usando el hecho de que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo finitamente generado, pruebe que $\mathcal{O}_K \cong \mathbb{Z}^n$, donde $n = [K : \mathbb{Q}]$.

Desarrollo:

i.- En lo que sigue usaremos que $M \otimes_A \bigoplus_{i \in I} M_i \cong \bigoplus_{i \in I}(M \otimes_A M_i)$. En efecto tenemos que $M \otimes_A K \cong \bigoplus_{i=1}^n (A \otimes_A K) \bigoplus (\text{Tor}(M) \otimes_A K)$. Es un ejercicio probar, vía la propiedad universal del producto tensorial, que $A \otimes_A K \cong K$. Por otro lado, como $\text{Tor}(M)$ es un módulo de torsión, para todo $m \in \text{Tor}(M)$ existe $s \in S$ tal que $sm = 0$. Luego todo elemento $m \otimes t \in \text{Tor}(M) \otimes_A K$ es igual a $sm \otimes ts^{-1} = 0$. Concluimos que $\text{Tor}(M) \otimes_A K = \{0\}$ y por lo tanto $M \otimes_A K \cong K^n$.

ii.- Sabemos que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo libre de torsión. Usando el hecho de que $\mathcal{O}_K$ es un $\mathbb{Z}$-módulo finitamente generado concluimos, por teorema de estructura, que $\mathcal{O}_K \cong \mathbb{Z}^t$, para cierto $t \in \mathbb{N}$. Sea $x \in K$ un elemento cualquiera. Sea $n = [K : \mathbb{Q}]$. Observe que el conjunto $\{1, x, \cdots, x^n\}$ es linealmente dependiente. Por lo tanto existen constantes $a_0, \cdots, a_n \in \mathbb{Q}$, no todas nulas, tales que $\sum_{i=0}^n a_i x^i = 0$. Multiplicando por el máximo común divisor de los divisores de $a_i \in \mathbb{Q}$, obtenemos $b_i \in \mathbb{Z}$, no todos nulos, tales que $\sum_{i=0}^n a_i x^i = 0$. Sín perdida de generalidad podemos admitir que $a_n \neq 0$. Multiplicando la última igualdad por a_n^{n-1} obtenemos $(a_n x)^n + a_{n-1}(a_n x)^{n-1} + \cdots + a_0 a_n^{n-1} = 0$. Luego $a_n x \in \mathcal{O}_K$. Esto prueba que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K \cong S^{-1}\mathcal{O}_K \cong K$, donde $S = \mathbb{Z} - \{0\}$. Por otro lado, tenemos, por [i], que $\mathbb{Q} \otimes_{\mathbb{Z}} \mathcal{O}_K \cong \mathbb{Q}^t$. Igualando las dimensiones sobre $\mathbb{Q}$ de $\mathbb{Q}^t$ y K, concluimos que $t = n$. Esto prueba lo pedido. Esto da una segunda demostración al hecho citado en la ayudantía 12.

4.- **Problema 4:** Sea A un dominio de integridad. Pruebe que si $f : A^n \to A^m$ es un homomorfismo sobreyectivo de A-módulo entonces $m \leq n$.

2.- **Demostración:** Sea $K = \text{Quot}(A)$. Considere el K-homomorfismo $g : K^n \to K^m$ definido por $g\left(\sum_{i=1}^n a_i e_i\right) = a_i f(e_i)$, donde $e_i = (\delta_{ij})_{j=1}^n$. Note que $g : K^n \to K^n$ es el morfismo inducido por f sobre $K^n \cong A^n \otimes_A K$, vía:

$$G : A^n \otimes_A K \to A^n \otimes_A K, \quad G(v \otimes r) = G(v) \otimes r.$$

Sea $e_j \in K^m$, como f es sobreyectiva, existe $v_j \in A^n \subset K^n$ tal que $f(v_j) = e_j$. Luego g es sobreyectiva, pues para todo $v \in K^m$ escrito de la

forma $v = \sum_{j=1}^{m} b_j e_j$ existe $w = \sum_{j=1}^{m} b_j v_j \in K^n$ tal que $g(w) = v$. Observe que g es una transformación K-lineal sobreyectiva, luego $m \leq n$.

5.- **Problema 5:** Este problema tiene por objetivo probar que si M es un A-módulo finitamente generado, con A un DIP, entonces $M \otimes_A M = \{0\}$ entonces $M = \{0\}$.

i.- Pruebe que si I, J son ideales de A entonces $A/I \otimes_A A/J \cong A/(I+J)$.

ii.- Pruebe que si $M \otimes_A M = \{0\}$ entonces $M = \{0\}$.

Desarrollo:

i.- Considere $\phi : A/I \times A/J \to A/(I+J)$ la función A-bilineal definida por $\phi(a,b) = ab$, donde $a \in A/I$ y $b \in A/J$. Note que dicha función bilineal está bien definida, pues si $a_1 = a_2 + i$, $b_1 = b_2 + j$, donde $a_i, b_j \in A$ e $i \in I$, $j \in J$, se tiene que:

$$a_1 b_1 = (a_2 + i)(b_2 + j) = a_2 b_2 + b_2 i + a_2 j i j$$

Por ende $a_1 b_1 = a_2 b_2 \in A/(I+J)$. Luego, por la propiedad universal del producto tensorial, existe un único morfismo $\psi : A/I \otimes_A A/J \to A/(I+J)$ definido por $\psi(a \otimes b) = ab$. Considere $g : A/(I+J) \to A/I \otimes_A A/J$ la función definida por $g(a) = a \otimes 1$. Observe que g está bien definida, pues si $x = y + (i+j)$, donde $i \in I$ y $j \in J$ entonces $x \otimes 1 = y \otimes 1 + i \otimes 1 + j \otimes 1 = y \otimes 1 + 1 \otimes j = y \otimes 1$. Además se tiene que $\psi \circ g = id$, $g \circ \psi = id$. Concluimos que ψ es un isomorfismo.

ii.- Por el teorema de estructura de módulos sobre DIP tenemos que existe $k \in \mathbb{Z}$ y $\{p_1, \cdots, p_m\}$ ideales primos en A tales que:

$$M \cong A^k \oplus \bigoplus_{i=1}^{m} \bigoplus_{j=1}^{a_i} A/(p_i^{e_{ij}}),$$

donde $e_{i1} \leq \cdots \leq e_{ia_i}$. Recordemos que el tensor distribuye sobre las sumas directas, luego si $M \otimes_A M = \{0\}$, tenemos que en particular que:

$$A^{k^2} \cong A^k \otimes A^k = \{0\},$$

y además:

$$A/(p_i^{e_{ij}}) \otimes_A A/(p_i^{e_{ij}}) = \{0\}.$$

De esto se sigue que $k = 0$ y que $A/(p_i^{e_{ij}}) \cong A/(p_i^{e_{ij}}) \otimes_A A/(p_i^{e_{ij}}) = \{0\}$. Por lo tanto cada factor invariante es nulo. Concluimos que $M = \{0\}$.

3.1. Interludio: Módulos planos: En esta ayudantía estudiaremos la categoría de módulos planos.

1.- **Problema 1:** Se dice que un A-módulo M es plano si para todo homomorfismo inyectivo $\phi : K \to L$, el homomorfismo inducido $\phi* : M \otimes_A K \to M \otimes_A L$ es inyectivo, donde $\phi * (m \otimes k) = m \otimes \phi(k)$.

i.- Pruebe que M es un módulo plano si y solamente si $M \otimes_A -$ es un functor exacto.

ii.- Muestre que si M es plano e I es un ideal de A, entonces existe un homomorfismo inyectivo $I \otimes_A M \hookrightarrow M$.

1.- **Desarrollo:**

i.- Supongamos que $M \otimes_A -$ es un functor exacto y sea $\phi : K \to L$ un homomorfismo inyectivo. Entonces tenemos la sucesión exacta:

$$0 \to K \xrightarrow{\phi} L \xrightarrow{\pi} L/\mathrm{Im}(f) \to 0.$$

Aplicando la exactitud del functor $M \otimes_A -$ obtenemos la sucesión exacta:

$$0 \to M \otimes_A K \xrightarrow{\phi*} M \otimes_A L \xrightarrow{\pi*} M \otimes_A L/\mathrm{Im}(f) \to 0.$$

En particular, se tiene que el homomorfismo inducido ψ es inyectivo.

Recíprocamente, sea $0 \to K \xrightarrow{\phi} L \xrightarrow{g} P \to 0$ una sucesión exacta. Sabemos que siempre se tiene la siguiente sucesión exacta:

$$K \xrightarrow{\phi*} L \xrightarrow{g*} P \to 0.$$

Ahora bien, como $\phi*$ es inyectiva por hipótesis, tenemos que podemos extender la sucesión anterior y agregar un módulo nulo a la izquierda.

ii.- Considere el homomorfismo inclusión $i : I \to A$. Como M es plano, tenemos que existe un homomorfismo inyectivo $i* : I \otimes_A \to A \otimes_A M$. Por otro lado, tenemos que $A \otimes_A M \cong M$. Componiendo $i*$ con el isomorfismo anterior, obtenemos un homomorfismo inyectivo $I \otimes_R M \hookrightarrow M$.

2.- **Problema 2:** Muestre que los siguientes módulos tienen o no la propiedad de planitud.

i.- Si $S \subset A$ es un conjunto multiplicativo, muestre que $S^{-1}A$ es un A-módulo plano.

ii.- Mustre que todo módulo libre es plano.

iii.- Pruebe que $\mathbb{Z}/n\mathbb{Z}$ no es un $\mathbb{Z}$-módulo plano.

2.- **Desarrollo:**

i.- Sea $M = S^{-1}A$ y sea $\phi : K \to L$ un homomorfismo inyectivo. Entonces tenemos que el homomorfismo $f* : M \otimes K \to M \otimes L$ se factoriza al homomorfismo $*f : S^{-1}K \to S^{-1}L$ definido por $*f\left(\frac{k}{s}\right) = \frac{f(k)}{s}$. Esto se debe a que $M \otimes K \cong S^{-1}K$ vía $\left(\frac{a}{s}\right) \otimes k \to \frac{ak}{s}$ y lo mismo se tiene para $M \otimes L \cong S^{-1}L$. Supongamos que $*f\left(\frac{k}{s}\right) = 0$, entonces existe $t \in S$ tal que $tf(k) = 0$. Luego tenemos que $f(tk) = 0$. Como f es inyectivo, tenemos que $tk = 0$, es decir $\frac{k}{s} = 0$. Esto prueba que $*f$ es inyectiva. Por ende $f*$ es inyectiva. Concluimos que M es plano.

ii.- Sea $M = \bigoplus_{i\in I} A$ y sea $\phi : K \to L$ un homomorfismo inyectivo. Entonces tenemos que el homomorfismo $f* : M \otimes K \to M \otimes L$ se factoriza al homomorfismo $*f : \bigoplus_{i\in I} K \to \bigoplus_{i\in I} L$ definido por $*f((k_i)_{i\in I}) = (f(k_i))_{i\in I}$. Esto se debe a que $M \otimes K \cong \bigoplus_{i\in I} K$ vía $(a_i)_{i\in I} \otimes k \to (a_i k)_{i\in I}$ y lo mismo para $M \otimes L \cong \bigoplus_{i\in I} L$. Observe que, como f es inyectivo, se tiene que $*f$ es inyectivo. Concluimos que $f*$ es inyectivo y por ende M es plano.

iii.- Supongamos que $\mathbb{Z}/n\mathbb{Z}$ es un $\mathbb{Z}$-módulo plano. Considere el homomorfismo inyectivo $f : \mathbb{Z} \to \mathbb{Z}$ definido por $f(x) = nx$. Para dicho f, existe el homomorfismo inyectivo $f* : \mathbb{Z}/\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z} \to \mathbb{Z}/\mathbb{Z}\otimes_{\mathbb{Z}}\mathbb{Z}$. Recordemos que $M\otimes_A A \cong M$ vía $m \otimes a \mapsto am$. Componiendo $f*$ con el isomorfismo previo obtenemos un homomorfismo inyectivo $g* : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ definido por $g * (\overline{x}) = \overline{nx} = \overline{0}$. Esto nos lleva a una contradicción.

4. Cuerpos:

Ayudantía 15: En esta ayudantía comenzaremos a estudiar cuerpos. En particular, analizaremos problemas asociados al grado de extensiones e incrustaciones de cuerpos.

1.- **Problema 1:** Sea F un cuerpo y α un elemento algebraico sobre F.

i.- Pruebe que si $[F(\alpha):F]$ es impar, entonces $F(\alpha)=F(\alpha^2)$.

ii.- Suponga que $F=\mathbb{Q}$ y $\alpha\in\mathbb{C}$ es algebraico sobre $\mathbb{Q}$. Sea $p(x)=\text{irr}_{\alpha,\mathbb{Q}}(x)$. Muestre que α es un cuadrado en $\mathbb{Q}(\alpha)$ si y solamente si $p(x^2)$ es reducible.

Desarrollo:

i.- Considere la extensión de cuerpos $F\subset F(\alpha^2)\subset F(\alpha)$. Note que α satisface el polinomio cuadrático $p(x)=x^2-\alpha^2\in F(\alpha^2)[x]$. Luego, como $[F(\alpha):F(\alpha^2)]=\deg(\text{irr}_{\alpha,F(\alpha^2)}(x))$ y $\text{irr}_{\alpha,F(\alpha^2)}|p(x)$ se tiene que $[F(\alpha):F(\alpha^2)]\in\{1,2\}$. Si $[F(\alpha):F(\alpha^2)]=2$, tenemos que $[F(\alpha):F]=2[F(\alpha^2):F]$, lo que contradice la imparidad de $[F(\alpha):F]$. Esto no perdite concluir que $[F(\alpha^2):F(\alpha)]=1$ y por lo tanto $F(\alpha)=F(\alpha^2)$.

ii.- Primero supongamos que $\alpha=\beta^2$, para cierto $\beta\in\mathbb{Q}(\alpha)$. Note que β satisface el polinomio mónico $p(x^2)$. Por lo tanto $\text{irr}_{\beta,\mathbb{Q}}(x)|p(x^2)$. Por otro lado, como $\mathbb{Q}(\beta)=\mathbb{Q}(\alpha)$, se tiene que $\deg(\text{irr}_{\beta,\mathbb{Q}}(x))=\deg(p(x))$. Esto implica que $p(x^2)=\text{irr}_{\beta,\mathbb{Q}}(x)s(x)$, donde $\deg(s(x))=\deg(p(x))>0$. Concluimos que $p(x^2)$ es reducible sobre $\mathbb{Q}[x]$. Supongamos ahora que $\alpha\notin\mathbb{Q}(\alpha)^2$ y sea $\beta\in\overline{\mathbb{Q}}$ un elemento tal que $\beta^2=\alpha$. Es facil probar que $[\mathbb{Q}(\beta):\mathbb{Q}(\alpha)]=2$. De la multiplicatividad de los grados en torres, tenemos que $[\mathbb{Q}(\beta):\mathbb{Q}]=2\deg(p(x))$. Por otro lado, como $p(x^2)$ es un polinomio mónico que se anula en β, tenemos que $\text{irr}_{\beta,\mathbb{Q}}=p(x^2)$. Esto prueba que $p(x^2)$ es irreducible.

2.- **Problema 2:** Sea $w=e^{\frac{2\pi i}{3}}$ y considere el cuerpo $L=\mathbb{Q}(\sqrt[3]{2},w)$.

i.- Pruebe que $[L:\mathbb{Q}]=6$.

ii.- Muestre que $\sqrt[3]{2}\notin L$, para todo $L=\mathbb{Q}(\theta_1,\cdots,\theta_n)$, donde $\theta_i^2\in\mathbb{Q}$.

Desarrollo:

i.- Sabemos que $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=\deg(x^3-2)=3$. Por la multiplicatividad del grado, para probar lo pedido, basta demostrar que $[L:\mathbb{Q}(\sqrt[3]{2})]=2$. En efecto, sabemos que $q(x)=x^2+x+1$ es un polinomio que se anula en w. Por otro lado, sabemos que $L\cong\mathbb{Q}(\sqrt[3]{2})[x]/(p(x))$, donde $p(x)$ es un polinomio irreducible. Luego $p(x)$ divide a x^2+x+1. Por lo tanto $[L:\mathbb{Q}(\sqrt[3]{2})]\leq 2$. Si $[L:\mathbb{Q}(\sqrt[3]{2})]=1$, entonces el cuerpo $\mathbb{Q}(\sqrt[3]{2})\subset\mathbb{R}$ conincide con L, el cual contiene el elemento no real, a saber $w\in L$. Esto implica que $[L:\mathbb{Q}(\sqrt[3]{2})]=2$ y se concluye lo pedido.

ii.- Definimos $L_i=\mathbb{Q}(\theta_1,\cdots,\theta_i)$, para $i\in\{1,\cdots n\}$. Note que $L_{i+1}=L_i(\theta_{i+1})$, donde $\theta_{i+1}^2\in L_i$. Por lo tanto $[L_{i+1}:L_i]\in\{1,2\}$. Esto implica que $[L:\mathbb{Q}]=2^t$, para cierto $t\leq n$. Luego, si $\sqrt[3]{2}\in L$, se tiene que $\mathbb{Q}(\sqrt[3]{2})\subset L$, por lo que 3 divide a 2^t. Esto nos lleva a una contradicción.

3.- **Problema 3:** Sea $p \neq 2$ un número primo y sean $\zeta_p = e^{\frac{2\pi i}{p}}$, $K = \mathbb{Q}(\zeta_p)$. Se define el simbolo de Legendre de n módulo p por:

$$\binom{n}{p} = \begin{cases} 0 & \text{si} \quad p|n \\ 1 & \text{si} \quad p \nmid n \text{ y } \overline{n} \in \mathbb{F}_p^2 \\ -1 & \text{si} \quad p \nmid n \text{ y } \overline{n} \notin \mathbb{F}_p^2 \end{cases} .$$

i.- Pruebe que $\sum_{n=1}^{p-1} \binom{n}{p} = 0$ y que $\binom{n}{p}\binom{m}{p} = \binom{nm}{p}$.

ii.- Se define la suma de Gauss por $S := \sum_{n=1}^{p-1} \binom{n}{p}\zeta_p^n$. Pruebe que $S^2 = \binom{-1}{p}p$.

iii.- Pruebe que $\binom{-1}{p} = 1$, si $p \equiv 1(4)$ y que $\binom{-1}{p} = -1$, si $p \equiv 3(4)$.

iv.- Concluya que $\mathbb{Q}(\sqrt{p}) \subset K$, si $p \equiv 1(4)$ y que $\mathbb{Q}(\sqrt{-p}) \subset K$, si $p \equiv 3(4)$.

Desarrollo:

i.- Sea $G = \mathbb{F}_p^*$ el grupo de elementos invertibles en $\mathbb{F}_p$. Definimos el homomorfismo $\mu : G \to G$ por $\mu(a) = a^2$. Note que $\ker(\mu) = \{1, -1\}$. Por lo tanto $|\text{Im}(\mu)| = \frac{p-1}{2}$. Esto implica que en $\mathbb{F}_p^*$ existen tantos elementos cuadrados como no cuadrados. De esto se sigue que $\sum_{n=1}^{p-1} \binom{n}{p} = 0$. Note además que la demostración anterior nos dice que $\mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong C_2$. Por lo tanto el producto de dos elemntos no cuadrados en $\mathbb{F}_p$ es un cuadrado. Esto prueba que $\binom{n}{p}\binom{m}{p} = \binom{nm}{p}$.

ii.- Por definición, se tiene que $S^2 = \sum_{n,m} \binom{n}{p}\binom{m}{p}\zeta_p^{n+m}$. Luego por lo mostrado en [i], tenemos que $S^2 = \sum_{n,m} \binom{nm}{p}\zeta_p^{n+m}$. Sea $r = n + m$, entonces $S^2 = \sum_{r,m} \binom{(r-m)m}{p}\zeta_p^r = \sum_{r,m}^{m\neq 0} \binom{rm^{-1}-1}{p}\zeta_p^r = \sum_r \zeta_p^r \sum_{m\neq 0} \binom{rm^{-1}-1}{p}$. Note que si $r \neq 0$ entonces $rm^{-1} - 1 = rs^{-1} - 1$ si y solamente si $s = m$. Por lo tanto $\{rm^{-1} - 1 : m \in \mathbb{F}_p^*\} = \mathbb{F}_p^* - \{-1\}$. Por lo tanto $S^2 = -\sum_{r\neq 0} \binom{-1}{p} + (p-1)\binom{-1}{p} = p\binom{-1}{p}$, dado que $\sum_{r=0}^{p-1} \zeta_p = 0$.

iii.- Sabemos que $\mathbb{F}_p^*$ es un grupo cíclico con $p - 1$ elementos. Sea $z \in \mathbb{F}_p^*$ un generador de dicho grupo. Note que $\binom{-1}{p} = 1$ si y solamente si existe $a \in \mathbb{F}_p^*$ tal que $|a| = 4$. Luego, si $\binom{-1}{p} = 1$, tenemos que por teorema de Lagrande $4|p-1$. Esto nos dice que $p \equiv 1(4)$. Por otro lado, si $p \equiv 1(4)$, se tiene que $a = z^{\frac{p-1}{4}}$ satisface $a^2 = -1$ y por ende $\binom{-1}{p} = 1$.

iv.- Esto se sigue directo, del hecho de que $S^2 \in K$ y de los items [ii], [iii].

4.- **Problema 4:** Sea K/F una extensión finita de grado n y sea $\phi : K \to \overline{F}$ un homomorfismo tal que $\phi|_F = \text{id}$.

i.- Sea $\alpha \in K$. Mustre que $\phi(\alpha)$ es una raiz de $p(x) = \text{irr}_{\alpha,F}(x)$.

ii.- Asuma que $K = F(\alpha)$ y sea $G = \left\{\phi : K \to \overline{F} : \phi|_F = \text{id}\right\}$. Muestre que $|G| \leq n$ y que $|G| = n$ si y solamente si $p(x) = \text{irr}_{\alpha,F}(x)$ tiene toda sus raices distintas.

iii.- Sea $\zeta_n = e^{\frac{2\pi i}{n}}$, como en [2]. Asuma que $F = \mathbb{Q}$ y $K = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$. Pruebe que $\phi(K) \subset \mathbb{R}$, para todo $\phi \in G$.

Desarrollo:

i.- Basta probar que $\beta = \phi(\alpha)$ cumple con $p(\beta) = 0$. En efecto, se tiene que si $p(x) = a_0 + a_1x + \cdots + a_nx^n$ entonces $p(\beta) = a_0 + a_1\phi(\alpha) + a_n\phi(\alpha^n) = \phi(p(\alpha)) = 0$, debido a que $\phi(a_i) = a_i$.

ii.- Note que si dos homomorfismos $\phi_1, \phi_2 : K \to \overline{F}$ cumplen con $\phi_1(\alpha) = \phi_1(\alpha)$, entonces $\phi_1 = \phi_2$. Por otro lado, dada una raiz β de $p(x)$, existe un isomorfismo $\Psi_1 : F[x]/(p(x)) \to F(\beta)$ definido por $\Psi_1(\overline{x}) = \beta$. Por la misma razón existe un isomorfismo $\Psi_2 : F[x]/(p(x)) \to F(\alpha)$ definido por $\Psi_2(\overline{x}) = \alpha$. Por lo tanto, existe un isomorfismo $\phi : F(\alpha) \to F(\beta) \subset \overline{F}$ definido por $\phi = \Psi_2^{-1} \circ \Psi_1$. Note que $\phi(\alpha) = \beta$. Esto nos permite concluir que G está en biyección con el número de raices de $p(x)$. De esto se sigue lo pedido.

iii.- Sea $\phi \in G$ un elemento cualquiera. Extendiendo ϕ al cuerpo $\mathbb{Q}(\zeta_n)$ (Ver Teorema 2.8 Segre Lang, Algebra), por lo mostrado en [i], tenemos que $\phi(\zeta_n) = \zeta_n^a$, para cierto $a \in \mathbb{Z}$. Por lo tanto $\phi(\zeta_n + \zeta_n^{-1}) = \zeta_n^a + \zeta_n^{-a}$. Sea $\overline{(\cdot)}$ la función conjugación. Note que $\overline{\zeta_n^a} = \zeta_n^{-a}$, pues ζ_n^a es una raiz de la unidad. De esto se sigue que $\overline{\phi(\zeta_n + \zeta_n^{-1})} = \phi(\zeta_n + \zeta_n^{-1})$ y por ende $\phi(\zeta_n + \zeta_n^{-1}) \in \mathbb{R}$. Concluimos que $\phi(K) \subset \mathbb{R}$.

Ayudantía 16: En esta ayudantía estudiaremos cuerpos finitos.

1.- **Problema 1:** Sea $n \in \mathbb{N}$ y $\mathbb{F}_p$ el cuerpo de p elementos con p primo, y sea $L \subset \overline{\mathbb{F}_p}$ el cuerpo de descomposición de $G(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

i.- Demuestre que el conjunto de raices de $G(x)$ es un subcuerpo de L.

ii.- Demuestre que L es igual al conjunto de raices de $G(x)$ y que $|L| = p^n$.

iii.- Muestre que todo cuerpo $\mathbb{F}_p \subset K \subset \overline{\mathbb{F}_p}$ de grado n es igual a L. En lo que sigue denotamos a L por $\mathbb{F}_{p^n}$.

Desarrollo:

i.- Sean α, β dos raices de $G(x)$. Entonces $(\alpha+\beta)^p = \alpha^p + \beta^p = \alpha + \beta$. Luego $\alpha+\beta$ es una raíz de $G(x)$. Por el mismo argumento $\alpha-\beta$ es raíz. El argumento para el producto y el inverso es inmediato. Luego se tiene lo pedido.

ii.- Note que el conjunto de raices de $G(x)$ es un cuerpo el cual contiene a $\mathbb{F}_p$. Por ende L es igual al conjunto de raices de $G(x)$. Esto demuestra lo pedido. En lo que sigue mostraremos que $|L| = p^n$. En efecto, si G tiene una raíz repetida, entonces $G(x) = (x-a)^2 s(x)$. Por lo tanto $x-a$ divide a $G(x)$ y $G'(x)$, pero esto es falso ya que $G'(x) = -1$. Concluimos que $G(x)$ tiene p^n raices y de esto se sigue lo pedido.

iii.- Supongamos que K es una extensión de grado n de $\mathbb{F}_p$. Entonces K^* es un grupo de $p^n - 1$ elementos y por ende todo $\alpha \in K$ satisface que $\alpha^{p^n} = \alpha$. Esto equivale a que α sea una raiz de $G(x)$. Luego $K \subset L$, y concluimos la igualdad de conjuntos de la igualdad de sus cardinalidades.

2.- **Problema 2:** Sean $\mathbb{F}_{p^n}, \mathbb{F}_{p^m} \subset \overline{\mathbb{F}_p}$ cuerpos finitos.

i.- Muestre que $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$ si y solamente si $n|m$.

ii.- Concluya que $x^{p^n} - x$ divide a $x^{p^m} - x$ si y solamente si $n|m$.

iii.- Muestre que $\mathbb{F}_8 \nsubseteq \mathbb{F}_{32}$.

Desarrollo:

i.- Supongamos primero que $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$. Entonces tenemos que $[\mathbb{F}_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^n} : \mathbb{F}_p]$. Por lo tanto $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ divide a $m = [\mathbb{F}_{p^m} : \mathbb{F}_p]$. Supongamos ahora que $n|m$. Sabemos que todo elemento $a \in \mathbb{F}_{p^n}$ cumple con $a^{p^n} = a$. Luego $a^{p^m} = a^{p^n \cdots p^n} = a$. Por lo tanto $a \in \mathbb{F}_{p^m} = \{a \in \overline{\mathbb{F}_p} : a^{p^m} = a\}$. Esto implica que $\mathbb{F}_{p^n} \subseteq \mathbb{F}_{p^m}$.

ii.- Primero supongamos que $x^{p^n} - x$ divide a $x^{p^m} - x$. Entonces tenemos que $\mathbb{F}_{p^n} = \{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\} \subset \{a \in \overline{\mathbb{F}_p} : a^{p^m} = a\} = \mathbb{F}_{p^m}$. Luego, por [i], concluimos que $n|m$. Por otro lado, si $n|m$ entonces podemos escribir:

$$x^{p^m} - x = x^{p^n \cdots p^n} - x = x^{p^n \cdots p^n} - \cdots + x^{p^n p^n} - x^{p^n} + x^{p^n} - x,$$

Luego:

$$x^{p^m} - x = (x^{p^n} - x)^{p^n \cdots p^n} + \cdots + (x^{p^n} - x)^{p^n} + (x^{p^n} - x),$$

Por ende $x^{p^m} - x = (x^{p^n} - x)s(x)$. Concluimos que $x^{p^n} - x$ divide a $x^{p^m} - x$.

iii.- Observe que $\mathbb{F}_8 = \mathbb{F}_{2^3}$ y $\mathbb{F}_{32} = \mathbb{F}_{2^5}$. Luego si $\mathbb{F}_8 \subset \mathbb{F}_{32}$ tendriamos que 3 divide a 5, lo cual nos lleva a una contradicción.

3.- **Problema 3*:** Determine el número de polinomios distintos de cada grado que tiene la factorización en irreducibles en $\mathbb{F}_2[x]$ de $P(x) = x^{256} + x$.

Desarrollo: En todo lo que sigue fijamos una clausura algebraica $\overline{\mathbb{F}_2}$ de $\mathbb{F}_2$. Note que si $p(x)$ es un polinomio irreducible que divide a $P(x)$ entonces toda

raiz $\alpha \in K$ de $p(x)$ satisface $\alpha^{2^8} = \alpha^{256} = \alpha$. Por lo tanto $\alpha \in \mathbb{F}_{2^8}$, donde $\mathbb{F}_{2^8}$ es la única extensión de grado 8 de $\mathbb{F}_2$ contenida en $\overline{\mathbb{F}_2}$. Por otro lado, si $\alpha \in \mathbb{F}_{2^8}$, entonces $p(x) = \text{irr}_{\alpha,\mathbb{F}_2}(x)$ divide a $P(x)$, puesto que $P(\alpha) = 0$. Note que, por lo demostrado en el Problema 1, se tiene que $P(x)$ no tiene raices repetidas en $\mathbb{F}_{2^8}$. En particular, cada uno de los factores irreducibles de $P(x)$ tienen potencia uno en su factorización y todos son separables. Concluimos que $P(x)$ es el producto de los polinomios minimales de elementos en $\mathbb{F}_{2^8}$. En particular, solo existen polinomios de grado $1, 2, 4$ y 8 que dividen a $P(x)$. Es sencillo ver (Ejericicio), a partir del Problema 2, que:

$$\mathbb{F}_{2^{2^i}} \supset \mathbb{F}_{2^{2^{i-1}}} \supset \cdots \supset \mathbb{F}_2,$$

y que, como para todo $k \in \mathbb{N}$ se tiene que $[\mathbb{F}_{2^{2^k}} : \mathbb{F}_{2^{2^{k-1}}}] = 2$, no existen cuerpos L_k distintos de $\mathbb{F}_{2^{2^k}}, \mathbb{F}_{2^{2^{k-1}}}$ tales que $\mathbb{F}_{2^{2^k}} \supset L_k \supset \mathbb{F}_{2^{2^{k-1}}}$. Por lo tanto, todo elemento $\alpha \in \mathbb{F}_{2^{2^i}} - \mathbb{F}_{2^{2^{i-1}}}$ es un elemento primitivo de la extensión $\mathbb{F}_{2^{2^i}}/\mathbb{F}_2$. Por ende $\text{irr}_{\alpha,\mathbb{F}_2}(x)$ tiene grado 2^i. Vía esta caracterización determinamos la factorización de $P(x)$ como sigue.

i.- Note que los polinomios de grado 1 que dividen a $P(x)$ son tantos como elementos en $\mathbb{F}_2$. En efecto, estos son $x, x-1$.

ii.- Por otro lado el número de polinomios irrecibles de grado 2 que divide a $P(x)$ es $\frac{1}{2}(|\mathbb{F}_{2^2}| - |\mathbb{F}_2|) = 1$. En efecto, dicho polonimio es $x^2 + x + 1$.

iii.- El número de polinomios irreducible de grado 4 que divide a $P(x)$ es $\frac{1}{4}(|\mathbb{F}_{2^4}| - |\mathbb{F}_{2^2}|) = 3$.

iv.- Por último, el número de polinomios irreducible de grado 8 que divide a $P(x)$ es $\frac{1}{8}(|\mathbb{F}_{2^8}| - |\mathbb{F}_{2^4}|) = 30$.

4.- **Problema 4*:** Demuestre que para todo entero positivo n existe un polinomio irreducible $f_n \in \mathbb{F}_p[x]$ y de grado n.
Demostración: Sea $z \in \mathbb{F}_{p^n}$ un generador del grupo cíclico $\mathbb{F}^*_{p^n}$. Entonces el orden de z satisface que $|z| = p^n - 1$. Supongamos que z es un elemento en algún subcuerpo propio de $\mathbb{F}_{p^n}$, es decir $z \in \mathbb{F}_{p^m}$, para $m|n$. Entonces $z^{p^m-1} = 1$ y por ende tiene orden menor a $p^n - 1$. Concluimos que $z \in \mathbb{F}_{p^n}$ no están en ningún subcuerpo propio de $\mathbb{F}_{p^n}$.Note que esto implica que $\mathbb{F}_p(z) = \mathbb{F}_{p^n}$. Por ende $p_n(x) = \text{irr}_{z,\mathbb{F}_p}$ es un polinomio irreducible de grado n.

5.- **Problema 5*:** Sean p y q números primos diferentes. Demuestre que el polinomio:

$$\phi(x) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

tiene una raíz en $\mathbb{F}_{q^2}$ si y solo si $q^2 \equiv 1(\text{ mod } p)$.
Demostración: Observe que las raices de $\phi(x)$ son las raices de $G(x) = x^p - 1$ distintas de 1. Por lo tanto si $\phi(x)$ tiene un raíz $\alpha \in \mathbb{F}_{q^2}$ se tiene que $\alpha^p = 1$ y $\alpha \neq 1$. Por ende $\alpha \in \mathbb{F}^*_{q^2}$ tiene orden p. Por teorema de Lagrange obtenemos que $q^2 \equiv 1(\text{ mod } p)$. Ahora bien, supongamos que $q^2 \equiv 1(\text{ mod } p)$. Entonces, como $\mathbb{F}^*_{q^2}$ es un grupo cíclico, tenemos que existe $\alpha \in \mathbb{F}_{q^2}$ tal que $\alpha^p = 1$ y $\alpha \neq 1$. De esto se sigue lo pedido.

6.- **Problema 6:** Sea $L = \mathbb{F}_5(\sqrt{2}) \subset \overline{\mathbb{F}_5}$ el mínimo cuerpo que contiene a $\mathbb{F}_5$ y una raiz de $2 \in \mathbb{F}_5$.

i.- Muestre que $L = \mathbb{F}_{25}$.

ii.- Pruebe que x^2+2 se descompone en $L[x]$.
Desarrollo:

i.- Sabemos que $L \cong \mathbb{F}_5[x]/(p(x))$, para cierto polinomio irreducible $p(x) \in \mathbb{F}_2[x]$ tal que $p(\sqrt{2}) = 0$. Por definición, x^2-2 se anula en $\sqrt{2}$. Por lo tanto, si demostramos que x^2-2 es irreducible en $\mathbb{F}_5[x]$, tenemos que $[L:\mathbb{F}_5] = \deg(x^2-2) = 2$. Observe que $\mathbb{F}_5^2 = \{0,1,-1\}$. Por lo tanto x^2-2 no tiene raices en $\mathbb{F}_5$. Esto implica que x^2-2 es irreducible sobre $\mathbb{F}_5[x]$.

ii.- Note que $(2\sqrt{2})^2 = 8 = -2$ en L. Por lo tanto $x^2+2 = (x-2\sqrt{2})(x+2\sqrt{2})$ en $L[x]$.

Ayudantía 17: En esta ayudantía trabajaremos con cuerpos de descomposición de polinomios.

1.- **Problema 1:** El siguiente problema tiene por objetivo calcular cuerpos de descomposición.

i.- Sea F un cuerpo, $\overline{F}$ su clausura algebraica y $p(x) \in F[x]$ un polinomio cualquiera. Muestre que el cuerpo de descomposición $K \subset \overline{F}$ de $p(x)$ sobre F es $K = F(\alpha_1, \cdots, \alpha_n)$, donde $\{\alpha_i\}_{i=1}^n \subset \overline{F}$ es el conjunto de raices de $p(x)$.

ii.- Demuestre que el cuerpo de descomposición de $p(x) = x^4 + ax^2 + b^2$ sobre $\mathbb{Q}$ es $\mathbb{Q}(z)$, donde $z = \sqrt{\frac{-a+\sqrt{a^2-4b^2}}{2}}$.

iii.- Demuestre que el cuerpo de descomposicón de $x^6 - 3$ sobre $\mathbb{F}_5$ tiene grado dos.

Desarrollo:

i.- Es sencillo ver que $p(x) = \prod_{i=1}^n (x - \alpha_i)$ en $F(\alpha_1, \cdots, \alpha_n)[x]$. Supongamos que $F \subset M \subset \overline{F}$ es otro cuerpo en el que $p(x)$ se factoriza linealmente. Como los factores lineales de $p(x)$ son de la forma $x - \alpha_i$ se tiene que $\alpha_i \in M$, para todo $i \in \{1, \cdots, n\}$. Por lo tanto $F(\alpha_1, \cdots, \alpha_n) \subset M$ y en particular la inclusión $F(\alpha_1, \cdots, \alpha_n) \to M$ es un homomorfismo no trivial que extiende la inclusión $F \to M$. Para efecto de todos los cálculos que siguen entendemos los cuerpos de descomposición como subconjuntos de la clausura algebraica respectiva.

ii.- Note que las raices de $p(x)$ son de la forma $\pm\sqrt{\frac{-a\pm\sqrt{a^2-4b^2}}{2}}$. Luego el cuerpo de descomposición de $p(x)$ sobre $\mathbb{Q}$ es $\mathbb{Q}(z, z')$, donde $z' = \sqrt{\frac{-a-\sqrt{a^2-4b^2}}{2}}$ y z es como antes. Por otro lado tenemos que $zz' = b$. Por lo tanto $z' = \frac{b}{z}$ y se tiene que $\mathbb{Q}(z)$ es el cuerpo de descomposición de $p(x)$.

iii.- Observe que $3 = 2^3$ en $\mathbb{F}_5$, por ende $x^6 - 3 = (x^2-2)(x^4+2x^2+4)$. Escribiendo $x^4 + 2x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$ se obtiene que $a = -c = 2$ y $b = d = -2$. Por lo tanto $x^6 - 3 = (x^2 - 2)(x^2 + 2x - 2)(x^2 - 2x - 2)$. Sea $\theta \in \overline{\mathbb{F}_5}$ un elemento tal que $\theta^2 = 2$. Escribimos $z = a\theta + b$. Luego si $z^2 \pm 2z - 2 = 0$, se tiene que $z = 2\theta \mp 1$ o $z = -2\theta \mp 1$. Esto implica que el cuerpo de descomposión de $p(x)$ es $L = \mathbb{F}_5(\theta)$, el cual sabemos tiene grado 2 sobre $\mathbb{F}_5$.

2.- **Problema 2:** Sea $a = \sqrt{2} + \sqrt{3} \in \mathbb{C}$ y $L = \mathbb{Q}(a)$. Considere el cuerpo de descomposición $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ del polinomio $p(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$.

i.- Pruebe que $\sqrt{6} \in L$.

ii.- Pruebe que $[K : \mathbb{Q}] = 4$.

iii.- Demuestre que $L \neq \mathbb{Q}(\sqrt{6})$.

iv.- Concluir que $L = K$.

v.- Encontrar un polinomio irreducible sobre $\mathbb{Q}[x]$ que se anule en a.

Desarrollo:

i.- Note que $a^2 = 5 + 2\sqrt{6}$. Luego, tenemos que $\sqrt{6} = \frac{a^2-5}{2} \in L$.

ii.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Luego, para probar que $[K : \mathbb{Q}] = 4$, basta demostrar que $[K : \mathbb{Q}(\sqrt{2})] = 2$. Note que $K = \mathbb{Q}(\sqrt{2})(\sqrt{3}) \cong \mathbb{Q}(\sqrt{2})[x]/(p(x))$, donde $p(x)$ divide a $x^2 - 3$, puesto que $x^2 - 3$ se anula en $\sqrt{3}$. Luego $[K :$

$\mathbb{Q}(\sqrt{2})] \in \{1, 2\}$. Observe que si $[K : \mathbb{Q}(\sqrt{2})] = 1$, entonces $\sqrt{3} = a + b\sqrt{2}$, para ciertos $a, b \in \mathbb{Q}$. Luego, tenemos que $3 = a^2 + 2b^2 + 2ab\sqrt{2}$. Por lo tanto $b = 0$, lo que implica que $\sqrt{3} \in \mathbb{Q}$. Esto es contradictorio. Concluimos que $[K : \mathbb{Q}(\sqrt{2})] = 2$.

iii.- Supogamos que $L = \mathbb{Q}(\sqrt{6})$. Entonces $[L : \mathbb{Q}] = 2$ y entonces existe $a, b \in \mathbb{Q}$ tales que $(\sqrt{2} + \sqrt{3})^2 + a(\sqrt{2} + \sqrt{3}) + b = 0$. Por lo tanto, se tiene que $2\sqrt{6} + a\sqrt{2} + a\sqrt{3} + 5 + b = 0$. Por otro lado, lo demostrado en [ii] implica que $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ es un conjunto linealmente independiente (ver teorema 1.2.3 del apunte). Este hecho, nos lleva a una contradicción. Por lo tanto $L \neq \mathbb{Q}(\sqrt{6})$.

iv.- Claramente se tiene que $L \subset K$. Por [i] e [iii] tenemos que $\mathbb{Q}(\sqrt{6}) \subsetneq L$. Por lo tanto $[L : \mathbb{Q}] = 4$. Esto nos permite concluir que $[K : L] = 1$. Luego $L = K$.

v.- En efecto $a^2 = 5 + 2\sqrt{6}$, luego tenemos que $(a^2 - 5)^2 = 24$. Por lo tanto, se tiene que $q(x)(x) = x^4 - 10x^2 + 1$ es un polinomio que se anula en a. Lo mostrado en [iv] implica que $L = \mathbb{Q}[x]/(p(x))$, donde $p(x)$ es irreducible de grado 4. Por otro lado, tenemos que $p(x)$ divide a $q(x)$. Por igualdad en el grado, tenemos que $p(x) = uq(x)$, donde $u \in \mathbb{Q}$. Esto implica que $q(x)$ es irreducible.

3.- **Problema 3*:** Sea $\mathbb{F}_q$ el cuerpo finito de q elementos y sea:

$$g(y) = y^4 + y^3 + y^2 + y + 1.$$

i.- Demuestre que si $g(y)$ tiene una raiz en $\mathbb{F}_q$, entonces $g(y)$ se factoriza linealmente sobre $\mathbb{F}_q$. Demuestre que esto pasa si y solamente si $q \equiv 0, 1 (\text{mod } 5)$.

ii.- Suponga que en $\mathbb{F}_q$ el polinomio $g(y)$ tiene un factor $h(y)$ irreducible, mónico y de grado 2. Muestre que $h(0) = 1$.

Desarrollo:

i.- Observe que $g(y) = \frac{y^5 - 1}{y - 1}$. Por ende estudiamos la raices de $y^5 - 1$. Sea $X = \{x \in \mathbb{F}_q\} : x^5 = 1\} \subset \mathbb{F}_q^*$. Como $\mathbb{F}_q^*$ es un grupo cíclico, tenemos que $X \neq 1\}$ si y solamente si $5|q - 1$, es decir $q \equiv 1 (\text{mod } 5)$. Por otro lado, el polinomio $y^5 - 1$ tiene raices repetidas si y solamente si $\text{car}(\mathbb{F}_q) = 5$. En dicho caso $g(y) = (y - 1)^4$ y $q \equiv 0 (\text{mod } 5)$. En cualquier otro caso $q(y)$ no tiene raices en $\mathbb{F}_q$. Note que en cualquier caso X es un subgrupo cíclico de $\mathbb{F}_q^*$ y por ende cualquier raíz de $q(y)$ genera X. Esto demuestra lo pedido.

ii.- Por la parte [i], si $g(y)$ tiene un factor irreducible de grado dos, entonces este se factoriza como producto de dos polinomios irreducibles de dicho grado. Sea $\mathbb{L} \subset \overline{\mathbb{F}_q}$ el cuerpo de descomposición de $g(y)$ sobre $\mathbb{F}_q$. Entonces $\mathbb{L} = \mathbb{F}_{q^2}$. Luego, por [i], tenemos que $q^2 \equiv 1 (\text{mod } 5)$, y por ende $q \equiv -1 (\text{mod } 5)$. Sea $y_0 \in \mathbb{L}$ un generador del grupo X. Entonces $h(y) = (y - y_0^i)(y - y_0^j) = y^2 - (y_0^i + y_0^j)y + y_0^{i+j} \in \mathbb{F}_q[y]$. Luego, si $i + j \neq 5$ tenemos que $y_0^{i+j} \in \mathbb{F}_q$ genera X y por ende $X \subset \mathbb{F}_q$, lo cual es contradictorio. Conclimos que $h(0) = y_0^{i+j} = 1$.

4.- **Problema 4:** Sean $p, q \in \mathbb{Z}$ primos distintos sí.

i.- Encuentre el cuerpo de descomposición K del polinomio $p(x) = x^p - q$ sobre $\mathbb{Q}$ y determine $[K : \mathbb{Q}]$.

ii.- Para $p = 3$, exhiba una base de K como $\mathbb{Q}$-espacio vectorial.

iii.- Para $p = 3$, encuentre un elemento primitivo de $K/\mathbb{Q}$.

Desarrollo:

i.- En todo lo que sigue consideramos el cuerpo algebraicamente cerrado $\mathbb{C}$ que contiene a $\mathbb{Q}$ y en este cuerpo estudiamos K. Sea $\zeta_p = e^{\frac{2\pi i}{p}} \in \mathbb{C}$. Claramente el conjunto de raices de $p(x)$ es $X = \{\zeta_p^a \sqrt[p]{q} : a \in \{1, \cdots, p\}\}$. Luego como todos los elementos de X estan generados por ζ_p y $\sqrt[q]{p}$ se tiene que $K = \mathbb{Q}(\zeta_p, \sqrt[p]{q})$. Sea $L_1 = \mathbb{Q}(\sqrt[p]{q})$ y $L_2 = \mathbb{Q}(\zeta_p)$. Note que, por criterio de Eisenstein y Gauss, tenemos que $[L_1 : \mathbb{Q}] = p$ y que $[L_2 : \mathbb{Q}] = p-1$. Por otro lado, como $K = L_2(\sqrt[p]{q})$ y $\sqrt[p]{q}$ se anula en $p(x)$, tenemos que $[K : L_2] \leq p$. Esto último implica que $[K : \mathbb{Q}] \leq p(p-1)$. Ahora bien, por la multiplicatividad del grado, tenemos que $[L_1 : \mathbb{Q}], [L_2 : \mathbb{Q}]$ dividen a $[K : \mathbb{Q}]$. Por lo tanto $p, p-1$ dividen a $[K : \mathbb{Q}]$. Como $p, p-1$ son relativamente primos, lo anterior implica que $p(p-1)$ divide a $[K : \mathbb{Q}]$. Concluimos que $[K : \mathbb{Q}] = p(p-1)$.

ii.- Note que una base de L_1 sobre $\mathbb{Q}$ es $\{1, \sqrt[3]{q}, \sqrt[3]{q^2}\}$. Por otro lado, como $[K : L_2] = 2$, tenemos que el conjunto generador $\{1, \zeta_3\}$ es una base de K como L_2 espacio vectorial. Luego una base de K sobre $\mathbb{Q}$ consiste en tomar todos los productos posibles de los elementos de las dos bases anteriores, es decir $\beta = \{1, \zeta_3, \sqrt[3]{q}, \zeta_3\sqrt[3]{q}, \sqrt[3]{q^2}, \zeta_3\sqrt[3]{q^2}\}$ es una base de $K/\mathbb{Q}$.

iii.- Demostraremos que el elemento $z = \sqrt[3]{q} + \zeta_3$ es un elemento primitivo para la extensión. De la identidad $\zeta_p^2 = -\zeta_p - 1$, se sigue que $z^2 = \sqrt[3]{q^2} - 1 - \zeta_3 - 2\zeta_3\sqrt[3]{q}$ y que $z^3 = (1+q) - 3\sqrt[3]{q} - 3\zeta_3\sqrt[3]{q} + 3\zeta_3\sqrt[3]{q^2}$. Por lo tanto, los vectores $1, z, z^2, z^3$ se pueden reescribir en la base β como:

$$1 = (1,0,0,0,0,0),$$
$$z = (0,1,1,0,0,0),$$
$$z^2 = (-1,-1,0,2,1,0),$$
$$z^3 = (1+q,0,-3,-3,0,3).$$

Note que estos cuatro elementos son linealmente idenpendientes. Por ende la extensión $F = \mathbb{Q}(z)$ es una extensión de grado a lo menos 4, contenida en K. Por la multiplicavidad del grado tenemos que $[F : \mathbb{Q}] \in \{1, 2, 3, 6\}$. Concluimos que $[F : \mathbb{Q}] = 6$ y por ende $F = K$.

5.- **Problema 5:** Sea K una extensión finita de F. Pruebe que K es el cuerpo de descomposición de un polinomio en $F[x]$ si y solamente si todo polinomio irreducible en $F[x]$ que tiene una raiz en K se factoriza completamente en $K[x]$.

Demostración: Supongamos que todo polinomio irreducible que tiene una raiz en K se factoriza completamente. Escribimos $K = F(\theta_1, \cdots, \theta_r)$ y sea $p_i(x) = \text{irr}_{\theta_i, F}(x)$. Note que $p_i(x)$ es irreducible y tienen una raiz en K. Por lo tanto $p_i(x)$ se descompone completamente en K. Esto implica que K es el cuerpo de descomposición de $p(x) = \prod_{i=1}^r p_i(x)$. Supongamos ahora que K es el cuerpo de descomposición de un polinomio $q(x) \in F[x]$ y sea $\overline{F}$ una clausura algebraica de F que contiene a K. Para concluir lo pedido basta probar que si $\alpha, \beta \in \overline{F}$ son raices de un polinomio irreducible $p(x) \in F[x]$ y $\alpha \in K$, entonces $\beta \in K$. Por la proposición 1.2.11 vista en clase, se tiene que existe un isomorfismo $i : F(\alpha) \to F(\beta)$ tal que $i|_F = \text{id}$. Note que, por el ejericicio 1i, K es un cuerpo de descomposición de $q(x) \in F(\alpha)[x]$. Por el mismo argumento $K(\beta)$ es un cuerpo de descomposición de $q(x) \in F(\beta)[x]$. Luego, por el Teorema 1.2.9 existe un isomorfismo $\psi : K(\alpha) \to K(\beta)$ tal que $\psi|_{F(\alpha)} = \text{id}$. Por lo tanto, si $\alpha \in K$, tenemos que $1 = [K(\alpha) : K] =$

$\frac{[K(\alpha):F(\alpha)][F(\alpha):F]}{[K:F]} = \frac{[K(\beta):F(\beta)][F(\beta):F]}{[K:F]} = [K(\beta):K]$. Concluimos que $\beta \in K$.

6.- **Problema 6:** Sea K una extensión algebraica de F contenida en $\overline{F}$. Decimos que K/F satisface (N) si toda F-incrustación de K en $\overline{F}$ induce un automorfismo de K.

i.- Muestre que si K es el cuerpo de descomposición de una familia de polinomios en $F[x]$, entonces K/F satisface (N).

ii.- Muestre que si todo polinomio irreducible en $F[x]$ que tienen una raiz en K se descompone completamente, entonces K/F satisface (N).

Desarrollo:

i.- Sea $\{f_i(x)\}_{i\in I}$ un conjunto de polinomios tal que sus raices generan K y $\sigma : K \to \overline{F}$ una F-incrustación. Considere $\alpha \in K$ una raiz de $f_i(x)$. Entonces, por lo mostrado en el problema 4i de la ayudantía 15, tenemos que $\sigma(\alpha)$ es otra raiz de $f_i(x)$. Por lo tanto $\sigma(\alpha) \in K$. Luego, como K está generado por las raices de $\{f_i(x)\}_{i\in I}$, tenemos que $\sigma(K) \subset K$. El Lema 2.1 de §2 Algebra Segre Lang, implica que σ es un automorfismo. En el caso en que $[K : F] < \infty$ dicho resultado se sigue de un cálculo sencillo con dimensión.

ii.- Una forma directa de probar este resultado en invocando la equivalencia mostrada en el ejercicio previo. Otra forma de demostrarla es la que sigue. Sea $\sigma : K \to \overline{F}$ una F-incrustación, $\alpha \in K$ y $p(x) = \mathrm{irr}_{\alpha,F}(x)$. Entonces nuevamente por el problema 4i de la ayudantía 15, tenemos que $\sigma(\alpha)$ es una raiz de $p(x)$. Luego, por hipótesis, tenemos que $\sigma(\alpha) \in K$. Esto prueba que $\sigma(K) \subset K$. Concluimos que σ es un automorfismo.

Ayudantía 18: En esta ayudantía trabajaremos con extensiones separables.

1.- **Problema 1*:** Sea $\mathbb{F}_p$ el cuerpo finito de p elementos. Sea $L = \mathbb{F}_p(u, v)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u, v]$ y sea $K = \mathbb{F}_p(u^p, v^p)$ el cuerpo de cocientes del anillo de polinomios $\mathbb{F}_p[u^p, v^p]$.

i.- Demuestre que L/K es una extensión de grado p^2.

ii.- Demuestre que todo elemento de L es inseparable sobre K o bien pertenece a K.

iii.- Pruebe que L/K no es simple.

Demostración:

i.- Considere $F = \mathbb{F}_p(u, v^p) = \text{Quot}(\mathbb{F}_p[u, v^p])$. Note que $F = K(u)$ y que $L = F(v)$. El elemento $u \in F$ se anula en el polinomio $p(x) = x^p - u^p \in K[x]$, donde u^p es un elemento primo en el anillo $\mathbb{F}_p(v^p)[u^p]$. Por lema de Einsenstein tenemos que $p(x)$ es irreducible en $\mathbb{F}_p(v^p)[u^p]$. Luego, por lema de Gauss, tenemos que $p(x)$ es irreducible en $K[x]$. Esto implica que $[F : K] = p$. Por otro lado $v \in L$ se anula en el polinomio $q(x) = x^p - v^p \in F[x]$, donde v^p es un elemento primo en el anillo $\mathbb{F}_p(u)[v^p]$. Por lema de Einsenstein tenemos que $p(x)$ es irreducible en $\mathbb{F}_p(u)[v^p]$. Luego, por lema de Gauss, tenemos que $p(x)$ es irreducible en $F[x]$. Esto nos lleva a que $[L : F] = p$. Concluimos que $[L : K] = p^2$.

ii.- Considere ahora un elemento $y \in L$ cualquiera. Por definición de cuerpo de cocientes $y = \frac{r(u,v)}{s(u,v)}$, donde $s(u, v) \neq 0$. Note que todo polinomio $r(u, v) = p_0(u) + p_1(u)v + \cdots + p_n(u)v^n \in \mathbb{F}_p[u, v]$ satisface que $r(u, v)^p = p_0(u)^p + p_1(u)^p v^p + \cdots + p_n(u)^p v^{np}$. Ahora bien, todo polinomio $q(u) = a_0 + a_1 u + \cdots + a_n u^n \in \mathbb{F}_p[u]$ cumple con $q(u)^p = a_0 + a_1 u^p + \cdots + a_n u^{np}$, puesto que $a_i^p = a_i$, para todo $a_i \in \mathbb{F}_p$. De esto se sigue que $r(u, v)^p = r(u^p, v^p)$. Por lo tanto $y^p = \frac{r(u^p,v^p)}{s(u^p,v^p)} \in K$. Esto implica que el elemento $y \in L$ satisface el polinomio $p(x) = x^p - \alpha$, con $\alpha \in K$. Por lo tanto $\text{irr}_{y,K}(x)$ divide a $x^p - \alpha$. Note que $p(x) = (x - y)^p$ en F. Por ende $\text{irr}_{y,K}(x)$ es inseparable o bien tiene grado 1. Esto nos permite concluir que $y \in L$ es inseparable sobre K o bien $y \in K$.

iii.- Note que lo probado en el item [ii] demuestra que para todo $\alpha \in L$ se cumple que $\text{irr}_{K,\alpha}(x)$ tiene grado menor o igual a p. En particular ninguno de estos elementos genera la extensión L de grado p^2 sobre K.

2.- **Problema 2*:** Sea $K = \mathbb{F}_p(x)$ el cuerpo de funciones en una variable sobre $\mathbb{F}_p$, y sea L el cuerpo de descomposición del polinomio $y^p - x \in K[y]$. Demuestre que el grupo de los automorfismos del cuerpo F que fijan K es trivial.

Demostración: Sea $\alpha \in \overline{K}$ una raíz de $y^p - x \in K[y]$. Entonces $y^p - x = y^p - \alpha^p = (y - \alpha)^p$. Por lo tanto $L = K(\alpha)$. Ahora bien, cualquier automorfismo que L que fija K envía α a una raíz de $y^p - x$. Como dichas raices son todas iguales a α, obtenemos que el único automorfismo posible es el trivial.

3.- **Problema 3*:** Sea F un cuerpo y $g(x) \in F[x]$ un polinomio irreducible y mónico. Suponga que en alguna extensión de F el polinomio $g(x)$ tiene una raiz α y otra raiz $\alpha + 1$. Demuestre que F tiene característica finita.

Demostración: Dado que g es un polinomio mónico irreducible que anula a α, tenemos que $g(x) = \text{irr}_{\alpha,F}(x)$. Ahora bien, como el mismo hecho se cumple para $\alpha+1$, se tiene que $\text{irr}_{\alpha+1,F}(x) = g(x)$. Utilizando el automorfismo σ de $F[x]$ definido por $x \mapsto x-1$, se tiene que $\text{irr}_{\alpha,F}(x) = g(x-1)$. Por lo tanto $g(x) = g(x-1)$. Es decir $g(x)$ es invariante por la acción de automorfismo σ. Luego $g(x) = \sigma^i(g(x)) = g(x-i)$, para todo $i \in \mathbb{Z}$. En particular $\alpha + i$ es una raiz de $g(x)$, para todo $i \in \mathbb{Z}$. Como $g(x)$ tiene un número finito de raices, tenemos que $\alpha + i = \alpha$, para cierto $i \in \mathbb{Z} - \{0\}$. Esto implica que $i = 0$, para cierto $i \in \mathbb{Z} - \{0\}$. Por lo tanto F tiene característica finita.

4.- **Problema 4:** Sea K un cuerpo de característica p y $\alpha \in \overline{K}$ un elemento separable. Pruebe que $K(\alpha) = K(\alpha^{p^i})$, para todo $i \in \mathbb{N}$.

Demostración: Es facil probar que $K(\alpha^{p^i}) \subset K(\alpha)$, por ende solo debemos demostrar que $K(\alpha^{p^i}) \supset K(\alpha)$. Note que α satisface el polinomio $r(x) \in K(\alpha^{p^i})$ definido por $r(x) = x^{p^i} - \alpha^{p^i}$. Por otro lado tenemos que $\text{irr}_{\alpha,K(\alpha^{p^i})}(x)$ divide a $\text{irr}_{\alpha,K}(x)$, puesto que $\text{irr}_{\alpha,K}(x) \in K(\alpha^{p^i})[x]$ es un polinomio que se anula en α. Por el mismo argumento $\text{irr}_{\alpha,K(\alpha^{p^i})}(x)$ divide a $r(x)$. Por hipótesis sabemos que $\text{irr}_{\alpha,K}$ es separable. Luego, el hecho de que $\text{irr}_{\alpha,K(\alpha^{p^i})}(x)$ divide a $\text{irr}_{\alpha,K}(x)$, implica que $\text{irr}_{\alpha,K(\alpha^{p^i})}(x)$ es separable. Ahora bien, en $K(\alpha)$ se tiene que $r(x) = (x-\alpha)^{p^i}$. Por ende la condición de que $\text{irr}_{\alpha,K(\alpha^{p^i})}(x)$ divida a $r(x)$, implica que $\text{irr}_{\alpha,K(\alpha^{p^i})}(x) = x - \alpha$. Esto nos permite concluir que $\alpha \in K(\alpha^{p^i})$.

Ayudantía 19: En esta ayudantía estudiaremos extensiones galoisianas y grupos de automorfismo de cuerpos. Denotamos por $\mathrm{Aut}(L/K)$ al grupo de automorfismos de L que fijan K y por $\mathrm{Gal}(L/K)$ a los automorfismos de L que fijan K, para L/K una extensión galoisiana.

1.- **Problema 1:**

i.- Calcule $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p))$.

i.- Calcule $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p-x))$. Demuestre que $\mathbb{F}_p(x)$ es una extensión galoisiana de $\mathbb{F}_p(x^p-x)$.

ii.- ¿Es $\mathbb{F}_2(\sqrt[3]{t})$ una extensión galoisiana de $\mathbb{F}_2(t)$?

Desarrollo:

i.- Este ejercicio de desarrolló en la ayudantía anterior y se cumple que $\mathrm{Aut}(\mathbb{F}_p(x)/\mathbb{F}_p(x^p)) = \{\mathrm{id}\}$.

ii.- Al igual que en [i], es sencillo notar que la extensión $K = \mathbb{F}_p(x)$ de $F = \mathbb{F}_p(x^p - x)$ se cumple que $K = F(x)$, donde $x \in K$ es anulado por el polinomio $p(y) = y^p - y - x^p + x \in F[y]$. Note que $p(y)$ tiene por raices a los elementos $\{x + i : i \in \mathbb{F}_p\}$. Por lo tanto $p(y)$ es un polinomio separable y en particular $\mathrm{irr}_{x,F}(y)$ lo es. Como $p(y)$ tiene todas sus raices en K, tenemos que $\mathrm{irr}_{x,F}(y)$ tiene todas sus raices en K. Esto prueba que K/F es una extensión galoisiana. Note que existen p incrustaciones $\phi : K \to \overline{F}$ que son la identidad sobre F. Se sigue directamente de la definición de las funciones $\{\phi_i : x \mapsto x+i : i \in \mathbb{F}_p\}$, que estas son homomorfismos no triviales entre espacios de igual dimensión y por ende F-automorfismos. Luego, como la extensión es galoisiana, tenemos que $\mathrm{Gal}(K/F)$ tiene p elementos. Es inmediato, de la defínción de ϕ_1, que este automorfismo tiene orden p. Por lo tanto $\mathrm{Gal}(K/F) \cong C_p$. En particular, como $p = |\mathrm{Gal}(K/F)| = [K : F]$, tenemos que $\mathrm{irr}_{x,F}(y) = p(y)$.

iii.- Note la extensión $K = \mathbb{F}_2(\sqrt[3]{t})$ de $F = \mathbb{F}_2(t)$ cumple con $K = F(\sqrt[3]{t})$, donde $\mathrm{irr}_{\sqrt[3]{t},F}(y) = y^3 - t$. Esto último pues $\sqrt[3]{t}$ se anula en $p(y) = y^3 - t$ y dicho polonomio es irreducible por criterio de Einsenstein. Note que las distintas raices de $p(y)$ son $\{\sqrt[3]{t}w^i : i = 0, 1, 2\}$, donde w es una raiz primitiva de la unidad. No obstante, si $\left(\frac{r(\sqrt[3]{t})}{s(\sqrt[3]{t})}\right)^3 = 1$ en K, se tiene que la factorización en irreducibles de $r(\sqrt[3]{t})$ y de $s(\sqrt[3]{t})$ es la misma. Por ende $\frac{r(\sqrt[3]{t})}{s(\sqrt[3]{t})} \in \mathbb{F}_2$ y en dicho cuerpo la única raiz de la unidad es 1. Concluimos que K/F no es una extensión normal y por ende no es galoisiana.

2.- **Problema 2:** Sea K el cuerpo de descomposición de $p(x) = x^6 - 3$ sobre $\mathbb{Q}(\sqrt{-3})$.

i.- Pruebe que K es una extensión galoisiana de $\mathbb{Q}(\sqrt{-3})$.

ii.- Calcule $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{-3}))$.

Desarrollo:

i.- Note que por ser K un cuerpo de descoposición sobre $\mathbb{Q}(\sqrt{-3})$, este cuerpo es una extensión normal de $\mathbb{Q}(\sqrt{-3})$. Por otro lado, como $\mathrm{car}(\mathbb{Q}(\sqrt{-3})) = 0$, tenemos que $K/\mathbb{Q}(\sqrt{-3})$ es una extensión separable. Concluimos que dicha extensión es galoisiana.

ii.- Es inmediato de la expresión de $w = e^{\frac{2\pi i}{3}}$ como número complejo que $\mathbb{Q}(w) = \mathbb{Q}(\sqrt{-3})$. Por otro lado, las distintas raices complejas de $p(x) =$

$(x^3-\sqrt{3})(x^3+\sqrt{3})$ son $\{\pm\sqrt[6]{3}w^i : i=0,1,2\}$. Por lo tanto $K=\mathbb{Q}(\sqrt[6]{3},w)=\mathbb{Q}(\sqrt{-3})(\sqrt[6]{3})$. Note que $[K:\mathbb{Q}(\sqrt{-3})]\leq 6$, puesto que el elemento primitivo $\sqrt[6]{3}$ de $K/\mathbb{Q}(\sqrt{-3})$ se anula en $p(x)$. Por otro lado $[K:\mathbb{Q}(\sqrt[6]{3})]=2$, puesto que $K\neq\mathbb{Q}(\sqrt[6]{3})$ y w se anula en $s(x)=x^2+x+1$. Esto implica que $[K:\mathbb{Q}]]=12$ y por lo tanto $[K:\mathbb{Q}(\sqrt{-3})]=6$. En particular $p(x)=\text{irr}_{\sqrt[6]{3},\mathbb{Q}(\sqrt{-3})}(x)$. Por otro lado, como las $\mathbb{Q}(\sqrt{-3})$-incrustaciones de K llevan $\sqrt[6]{3}$ a sus raices conjugadas, tenemos que dichos homomorfismos están definidos por:

$$\phi:\sqrt[6]{3}\mapsto\pm\sqrt[6]{3}w^i,\quad w\mapsto w.$$

Observe el isomorfismo $\sigma:\sqrt[6]{3}\mapsto-\sqrt[6]{3}w$ tiene orden 6. Por lo tanto, como $|\text{Gal}(L/\mathbb{Q}(\sqrt{-3})|=6$, concluimos que $\text{Gal}(K/\mathbb{Q}(\sqrt{-3}))\cong C_6$.

3.- **Problema 3:** Sea $\zeta_p=e^{\frac{2\pi i}{p}}$, para p primo distinto de 2 y considere $F=\mathbb{Q}(\zeta_p)$.

i.- Pruebe que existe una única extensión $L\subset F$ tal que $[L:\mathbb{Q}]=2$.

ii.- Para $p=7$, encuentre todos los cuerpos L tales que $\mathbb{Q}\subset L\subset F$.

Desarrollo:

i.- Observe que F es el cuerpo de descomposición de x^p-1 sobre $\mathbb{Q}$. Por lo tanto F es una extensión normal y separable de $\mathbb{Q}$, luego dicha extensión es galoisiana. Por la correspondencia entre subcuerpos F y subgrupos de $\text{Gal}(F/\mathbb{Q})$, tenemos que basta probar que $\text{Gal}(F/\mathbb{Q})$ tiene un único subgrupo de indice 2. En efecto, calculemos el grupo de Galois de $K/\mathbb{Q}$. Sabemos que una $\mathbb{Q}$-incrustación lleva ζ_p a ζ_p^i, donde $(i,p)=1$, puesto que esta últimas son las raices de $\text{irr}_{\mathbb{Q},\zeta_p}(x)=\frac{x^p-1}{x-1}$. Por lo tanto los automorfismos de K, que fijan a $\mathbb{Q}$ obligadamente, son $\{\phi_i : i=1,\cdots,p-1\}$, donde:

$$\phi_i(\zeta_p)=\zeta_p^i.$$

Es sencillo notar, calculando la imagen sobre el elemento primitivo ζ_p, que $\phi_i\circ\phi_j=\phi_{ij}$, para todo $i,j\in\{1,\cdots,p-1\}$. Esto determina un homomorfismo $\psi:\text{Gal}(K/\mathbb{Q})\to c_{p-1}$ definido por $\psi(\phi_i)=\bar{i}$. Note que ψ es claramente sobreyectivo y que si $\psi(\phi_i)=\overline{1}$, entonces $\bar{i}=\overline{1}$ y por ende $\phi_i(\zeta_p)=\zeta_p$. Esto último equivale a que $\psi(\phi)=\text{id}$. Concluimos que $\text{Gal}(K\mathbb{Q})\cong C_{p-1}$. Se sigue del hecho de que $\text{Gal}(K\mathbb{Q})$ es un grupo cíclico de orden divisible por 2, que existe un único subgrupo de íncice 2. Otra obsevación, es que dicho cuerpo L fue determinado en el problema 2 de la ayudantía 19 y corresponde a $\mathbb{Q}(\sqrt{p})\subset K$, si $p\equiv 1(4)$ o bien $\mathbb{Q}(\sqrt{-p})\subset K$, si $p\equiv 3(4)$.

ii.- Por el teorema de correspondencia entre subgrupos y subcuerpos de una extensión galoisiana, tenemos que los los cuerpos L tales que $\mathbb{Q}\subset L\subset F$ están en correspondecia con los subgrupos de $\text{Gal}(L/\mathbb{Q})\cong C_6$. En efecto dichos subgrupos son $\{C_6,C_3,C_2,\{\text{id}\}\}$. Note que $[C_6:C_3]=2$ y por lo tanto $F^{C_3}=\mathbb{Q}(\sqrt{-7})$. Por otro lado $[C_6:C_2]=3$ y por ende F_2 es el único subcuerpo de F tal que $[F:F^{C_2}]=2$. Note que $L_1=\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ cumple con $L_1\neq F$, puesto L_1 es un subcuerpo de $\mathbb{R}$ y ζ_7 satisface $q(x)=x^2-x(\zeta_7+\zeta_7^{-1})+1\in L_1[x]$. De esto se sigue que $[F:L_1]=2$. Por ende $F^{C_2}=L_1=\mathbb{Q}(\zeta_7+\zeta_7^{-1})$. Concluimos que os cuerpos L tales que $\mathbb{Q}\subset L\subset F$ son $\{F,\mathbb{Q}(\zeta_7+\zeta_7^{-1}),\mathbb{Q}(\sqrt{-7}),\mathbb{Q}\}$.

4.- **Problema 4*:** Sean $\{p_1, \cdots, p_n\}$ un conjunto de primos distintos entre si y sea $K = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$.

i.- Pruebe que $[K : \mathbb{Q}] = 2^n$.

ii.- Demuestre que K es una extensión galoisiana de $\mathbb{Q}$ y determine $G = \mathrm{Gal}(K/\mathbb{Q})$.

ii.- Demuestre que $\alpha = \sum_{i=1}^{n} \sqrt{p_i}$ es un elemento primitivo para la extensión $K/\mathbb{Q}$.

Desarrollo:

i.- Probemos, por induccción sobre n, que dado un conjuto de primos distintos:

$$\{p_1, \cdots, p_n, q_1, \cdots, q_m\},$$

se tiene que $\sqrt{q_1 \cdots q_m} \notin \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_n})$. Para $n = 1$ se sigue del hecho que seala que si $d_1, d_1, d_1 d_2 \notin \mathbb{Q}^2$ entonces $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ es una extensión cuártica de $\mathbb{Q}$. Supongamos que la afirmación es cierta para todo natural menor a n. Sea $F = \mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_{n-1}})$ y $L = F(\sqrt{p_n})$. Note que $\mathrm{irr}_{\sqrt{p_n},F}(x)$ divide a $x^2 - p_n$ y por lo tanto $[L : F] \leq 2$. Si $L = F$ entonces $\sqrt{p_n} \in F$, lo que contradice la hipótesis de inducción al tomar $m = 1$ y $q_1 = p_n$. Esto implica que $[L : F] = 2$ y que $\{1, \sqrt{p_n}\}$ es una base de L/F. Supongamos que $\sqrt{q_1 \cdots q_m} = a + b\sqrt{p_n}$, donde $a, b \in F$. Si $a = 0$ entonces $\sqrt{q_1 \cdots q_m p_n} = bp_n \in F$, lo que contradice la hipótesis de inducción. De la misma forma, si $b = 0$ tenemos que $\sqrt{q_1, \cdots q_m} = a \in F$, lo que nos lleva a una contradicción. Por último, si $a, b \neq 0$ tenemos que $\sqrt{p_n} = \frac{q_1 \cdots q_m - a^2 - b^2 p_n}{2ab} \in F$, lo que nos lleva a una contradicción. De la demostración anterior anterior se desprende que $[K : \mathbb{Q}] = 2^n$.

ii.- Observe que K es el cuerpo de descomposición sobre $\mathbb{Q}$ del polinomio $p(x) = \prod_{i=1}^{n}(x^2 - p_i)$. Por lo tanto K es una extensión normal de $\mathbb{Q}$. Esto implica que K es una extensión galoisiana de $\mathbb{Q}$. En particular tenemos que $|G| = [K : \mathbb{Q}] = 2^n$. Sea $\phi : K \to K$ un automorfismo cualquiera. Como $\phi(\sqrt{p_i})$ es otra raiz de $x^2 - p_i$, se tiene que $\phi(\sqrt{p_i}) \in \{\pm\sqrt{p_i}\}$. Por lo tanto el conjunto de funciones $\phi : K \to K$ definidas por $\phi(\sqrt{p_i}) = \pm\sqrt{p_i}$ constituye el conjunto de todos los posibles automorfismos de K. Dado que $|G| = 2^n$, tenemos que las funciones anteriores son los automorfismos de K. Note que todo $\phi \in G$ cumple con $\phi^2 = \mathrm{id}$, por ende G es abeliano. Por el teorema fundamental de módulos sobre DIP concluimos que $G = \prod_{i=1}^{n} C_2$. Es más, sean $\sigma_i : K \to K$ los automorfismos definidos por $\sigma(\sqrt{p_i}) = -\sqrt{p_i}$ y $\sigma(\sqrt{p_j}) = \sqrt{p_j}$, para todo $j \neq i$, entonces $G = \langle \sigma_i : \sigma_i^2 = \mathrm{id}, \sigma_i\sigma_j = \sigma_j\sigma_i \rangle \cong \prod_{i=1}^{n} C_2$.

iii.- Sea $E = \mathbb{Q}(\alpha) \subset K$. Note que si $\phi \in \mathrm{Gal}(K/E)$ entonces $\phi(\alpha) = \alpha$. Pero $\phi(\alpha) = \sum_{i \in A} \sqrt{p_i} - \sum_{i \in B} \sqrt{p_i}$, donde $A \cap B = \emptyset$, $A \cup B = \{1, \cdots, n\}$ y donde A es el conjunto de indices i tales que ϕ deja fijo a $\sqrt{p_i}$. Por $\mathbb{Q}$-independencia lineal de $\{\sqrt{p_1} \cdots, \sqrt{p_n}\}$ se tiene que $\phi(\alpha) = \alpha$ si y solamente si $\phi = \mathrm{id}$. Por el teorema de correspondencia de Galois concluimos que $E = K$.

5.- **Problema 5*:** Sea $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ y σ el $\mathbb{Q}$-automorfismo de F tal que $\sigma(\sqrt{2}) = \sqrt{2}$ y $\sigma(\sqrt{3}) = -\sqrt{3}$. Sea $a = (2 + \sqrt{2})(3 + \sqrt{3})$. Prube que:

i.- Si $b \in K$ es tal que $b^2 = a$, entonces $b\sigma(b) \in \mathbb{Q}(\sqrt{2})$.

ii.- Demuestre que a no es un cuadrado en K.

Desarrollo:

i.- Es sencillo probar que $K^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{2})$ (ejercicio). Por ende, para demostrar que $b\sigma(b) \in \mathbb{Q}(\sqrt{2})$, basta probar que dicho elemento es fijo por el

automorfismo σ. En efecto $\sigma(b\sigma(b)) = \sigma(b)\sigma^2(b)$. Pero $\sigma^2 = \mathrm{id}$, por lo que $\sigma(b\sigma(b)) = b\sigma(b)$. Esto demuestra que $b\sigma(b) \in \mathbb{Q}(\sqrt{2})$.

ii.- Supongamos que a es un cuadrado en K, entonces existe $b \in K$ tal que $b^2 = a$. Por lo mostrado en [i] tenemos que $b\sigma(b) \in \mathbb{Q}(\sqrt{2})$. Por lo tanto $a\sigma(a) = b^2\sigma(b)^2$ es un cuadrado en $\mathbb{Q}(\sqrt{2})$. Pero $a\sigma(a) = 6(2+\sqrt{2})^2$, es un elemento de norma $\mathrm{N}(a\sigma(a)) = 72 \notin \mathbb{Q}^2$. Esto implica que $a\sigma(a)$ no es un cuadrado en $\mathbb{Q}(\sqrt{2})$. Concluimos que a no es un cuadrado en K.

6.- **Problema 6*:** Sea $f = x^2 + x^{-2} \in \mathbb{C}(x)$, donde $\mathbb{C}(x)$ es el cuerpo de funciones racionales sobre $\mathbb{C}$. Sea $k = \mathbb{C}(f) \subset \mathbb{C}(x)$. Determine si la extensión $\mathbb{C}(x)/k$ es galoisiana.
Desarrollo: Observe que $\mathbb{C}(x) = k(x)$, donde x satisface el polinomio $s(y) = y^4 + 1 - y^2 f$. De hecho, el conjunto de raices de $s(y)$ es $\{\pm x, \pm x^{-1}\} \subset \mathbb{C}(x)$. Esto implica que $\mathbb{C}(x)$ es el cuerpo de descomposición del polinomio $s(y)$ sobre k. Como $\mathrm{car}(k) = 0$, concluimos que $\mathbb{C}(x)/k$ es galoisiana.

7.- **Problema 7:** Sea $K = \mathbb{Q}(\sqrt[3]{2}, w)$, donde $w = e^{\frac{2\pi i}{3}}$.

i.- Demuestre que K es una extensión galoisiana de $\mathbb{Q}$ y determine $G = \mathrm{Gal}(K/\mathbb{Q})$.

ii.- Determine los cuerpos fijos por cada uno de los subgrupos de G.
Desarrollo:

i.- Observe que K es el cuerpo de descomposición, contenido en $\mathbb{C}$, del polinomio separable $p(x) = x^3 - 2$. Esto implica que $K/\mathbb{Q}$ es una extensión galoisiana. En particular tenemos que $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 6$. Por otro lado, como los automorfismos de K llevan los generadores w, $\sqrt[3]{2}$ a sus conjugados tenemos que las únicas funciones candidatas a $\mathbb{Q}$-automorfimos de K son:

$$\phi_{ij} : \sqrt[3]{2} \to \sqrt[3]{2}w^i, \quad w \to w^j,$$

donde $i = 0, 1, 2$ y $j = 1, 2$. Dado que ya sabemos que existen 6 automorfismos de K, tenemos que $\mathrm{Gal}(K/\mathbb{Q}) = \{\phi_{ij}\}$. Considere:

$$\sigma : \sqrt[3]{2} \to \sqrt[3]{2}w, \quad w \to w,$$

$$\tau : \sqrt[3]{2} \to \sqrt[3]{2}, \quad w \to w^2.$$

Note que $\tau^2 = \mathrm{id}$ y $\sigma^3 = \mathrm{id}$. Ahora bien, como $\sigma^i(\sqrt[3]{2}) = \sqrt[3]{2}w^i$, tenemos que $\{\phi_{ij}\} = \{\sigma^i\tau^j : i = 0, 1, 2, \text{ y } j = 1, 2\}$. Esto prueba que $G = \langle \sigma, \tau \rangle$. Por último note que $\sigma^2\tau = \tau\sigma$. Esto nos permite concluir que:

$$G = \langle \sigma, \tau : \sigma^3 = \mathrm{id}, \tau^2 = \mathrm{id}, \sigma^2\tau = \tau\sigma \rangle \cong D_6.$$

ii.- Los subgrupos no triviales de G son $\langle\sigma\rangle$, $\langle\tau\rangle$, $\langle\tau\sigma\rangle$ y $\langle\tau\sigma^2\rangle$. Por otro lado, se sigue del problema 2 de la prueba 1, tenemos que:

$$\beta = \{1, \sqrt[3]{2}, \sqrt[2]{4}, w, w\sqrt[3]{2}, w\sqrt[3]{4}\},$$

es una $\mathbb{Q}$-base de K. Por lo tanto, $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w + a_5 w\sqrt[3]{2} + a_6 w\sqrt[3]{4} \in K^{\langle\tau\rangle}$ si y solamente si $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w^{-1} + a_5 w^{-1}\sqrt[3]{2} + a_6 w^{-1}\sqrt[3]{4}$. Pero $w^{-1} = -1 - w$ y por ende $z = a_1 - a_4 + (a_2 - a_5)\sqrt[3]{2} + (a_3 - a_6)\sqrt[3]{4} - a_4 w - a_5 w\sqrt[3]{2} - a_6 w\sqrt[3]{4}$. Por la independencia lineal de β tenemos que $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4}$. Esto implica que $K^{\langle\tau\rangle} = \mathbb{Q}(\sqrt[3]{2})$. Por un argumento análogo se tiene que $K^{\langle\tau\sigma\rangle} = \mathbb{Q}(w\sqrt[3]{2})$ y $K^{\langle\tau\sigma^2\rangle} = \mathbb{Q}(w^2\sqrt[3]{2})$ (ejercicio). Por otro lado $z = a_1 + a_2\sqrt[3]{2} + a_3\sqrt[3]{4} + a_4 w + a_5 w\sqrt[3]{2} + a_6 w\sqrt[3]{4} \in K^{\langle\sigma\rangle}$ si y solamente si $z = a_1 + a_2 w\sqrt[3]{2} + a_3 w^2\sqrt[3]{4} + a_4 w + a_5 w^2\sqrt[3]{2} + a_6\sqrt[3]{4} =$

$a_1+a_2w\sqrt[3]{2}+a_3(-w-1)\sqrt[3]{4}+a_4w+a_5(-w-1)\sqrt[3]{2}+a_6\sqrt[3]{4}$. Nuevamente por la independencia lineal de β tenemos que $a_2 = a_3 = a_5 = a_6$. Esto nos lleva a que $K^{\langle\sigma\rangle} = \mathbb{Q}(w)$. Es sencillo ver que $K^{\{\mathrm{id}\}} = K$ y que $K^G = \mathbb{Q}(w)^G = \mathbb{Q}$. Concluimos que $\{\mathbb{Q}, \mathbb{Q}(w), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}w), \mathbb{Q}(\sqrt[3]{2}w^2)\}$ son los cuerpos fijos por los subgrupos de G.

Ayudantía 20: En esta ayudantía seguiremos estudiando extensiones galoisianas.

1.- **Problema 1:** Sea K/F una extensión galoisiana cuyo grupo de Galois es G. Sean L, L' dos cuerpos intermedios y $H = \mathrm{Gal}(K/L)$, $H' = \mathrm{Gal}(K/L')$.

i.- Pruebe que $\mathrm{Gal}(K/LL') = H \cap H'$. Concluya que $K^{H\cap H'} = LL'$.

ii.- Pruebe que $K^{\langle HH'\rangle} = L \cap L'$. Concluya que $\mathrm{Gal}(K/L \cap L') = \langle HH'\rangle$.

Desarrollo:

i.- Como $K^{H\cap H'} \supset K^H, K^{H'}$, se tiene que $K^{H\cap H'} \supset L, L'$. Por lo tanto tenemos que $K^{H\cap H'} \supset LL'$. Si consideramos los grupos de Gaolois relativos y usamos la correspondencia de Galois, tenemos que la contensión anterior implica que $H \cap H' \subset \mathrm{Gal}(K/LL')$. Sea $\sigma \in \mathrm{Gal}(K/LL')$, entonces $\sigma(a) = a$, para todo $a \in L$ y para todo $a \in L'$. Esto implica que $\sigma \in H \cap H'$. Concluimos que $\mathrm{Gal}(K/LL') = H \cap H'$. Ahora bien, por el teorema de correspondencia de Galois, definido por $\mathrm{Gal}(K/K^{H''}) = H''$, tenemos que $K^{H\cap H'} = LL'$.

ii.- Es sencillo probar, a partir del hecho de que $K^{\langle HH'\rangle} \subset K^H, K^{H'}$, que $K^{\langle HH'\rangle} \subset L \cap L'$. Sean $\sigma = \prod_{i=1}^s \sigma_{i,H}\sigma_{i,H'} \in \langle HH'\rangle$ y $a \in L \cap L'$, donde $\sigma_{i,H} \in H$ y $\sigma_{i,H'} \in H'$. Entonces $\sigma(a) = \prod_{i=1}^s \sigma_H \circ \sigma_{H'}(a) = a$, para todo $a \in H \cap H'$. Por lo tanto $L \cap L' = K^{\langle HH'\rangle}$. Se sigue directamente la correspondecia de Galois definida por $\mathrm{Gal}(K/K^{H''}) = H''$ que se tiene la identidad de grupos $\mathrm{Gal}(K/L \cap L') = \langle HH'\rangle$.

2.- **Problema 2:** Sea $\overline{\mathbb{F}_p}$ una clausura algebraica de $\mathbb{F}_p$ y $K = \mathbb{F}_{p^n}$ la extensión de grado n de $\mathbb{F}_p$ contenida en $\overline{\mathbb{F}_p}$.

i.- Determine el grupo $G = \mathrm{Gal}(K/\mathbb{Q})$.

ii.- Determine los cuerpos fijos por cada uno de los subgrupos de G.

Desarrollo:

i.- Sabemos que $|G| = [K : \mathbb{F}_p] = n$. Ahora bíen, el automorfismo $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ fija el cuerpo $\mathbb{F}_p$ y cumple con $\phi^n = \mathrm{id}$. Por otro lado, si $\phi^d = \mathrm{id}$, para $d < n$, se tiene que $\mathbb{F}_{p^n} \subset \{\alpha \in \overline{\mathbb{F}_p} : \alpha^{p^d} = \alpha\} = \mathbb{F}_{p^d}$. Esto último es un absurdo. Concluimos que ϕ es un generador de G y por ende $G \cong C_n$.

ii.- Por la ciclicidad de G tenemos que todos sus subgrupos son también cíclicos. Es más, todos los subgrupos de G son de la forma $H = \langle\phi^d\rangle$, donde $d|n$. Note que $K^H = \{a \in K : a^{p^d} = a\} = \mathbb{F}_{p^d}$. Esto nos dice que $\{\mathbb{F}_{p^d} : d|n\}$ es el conjunto de los cuerpos fijos por los subgrupos de G.

3.- **Problema 3*:** Sea $f(x) \in \mathbb{Q}[x]$ un polinomio de grado $n \geq 3$ sin raices múltiples en $\mathbb{C}$. Sea $E \subset \mathbb{C}$ el cuerpo de descomposición de $f(x)$ sobre $\mathbb{Q}$, y suponga que $\mathrm{Gal}(E/\mathbb{Q}) \cong S_n$, el grupo de permutaciones de n objetos.

i.- Demuestre que $f(x)$ es irreducible en $\mathbb{Q}[x]$.

ii.- Sea $\alpha \in \mathbb{C}$ una raiz de $f(x)$. Demuestre que la identidad es el único automorfismo del cuerpo $\mathbb{Q}(\alpha)$.

Desarrollo:

i.- Supongamos que $f(x)$ es reducible y sea α_1 una raiz de $f(x)$. Entonces $q_1(x) = \mathrm{irr}_{\alpha_1,F}(x)$ divide a $f(x)$ y $\deg(q_1(x)) < n$. Por lo tanto la extensión $F_1 = \mathbb{Q}(\alpha_1)$ cumple con $[F_1 : \mathbb{Q}] < n$. Por otro lado, dado que adjuntamos la raiz α_1 de $f(x)$ en F_1, se tiene que E es el cuerpo de descomposición de $f_2(x) = \frac{f(x)}{x-\alpha_1}$. En este caso, tenemos que $f_2(x)$ puede ser reducible o no

en $F_1[x]$. Por lo tanto, si α_2 es una raiz de $q_1(x)$ y $F_2 = F_1(\alpha_2)$ tenemos que $[F_2 : F_1] \leq n-1$. Repitiendo el mismo argumento inductivamente, obtenemos extensiones $F_i = \mathbb{Q}(\alpha_1, \cdots, \alpha_i)$ de $\mathbb{Q}$, donde $\{\alpha_1, \cdots, \alpha_i\}$ es un conjunto de raices de $f(x)$ y tales que $[F_{i+1} : F_i] \leq n-i$. Definimos F_0 como $\mathbb{Q}$. Note que $E = F_n$ y que $[E : \mathbb{Q}] = |\mathrm{Gal}(E/\mathbb{Q})| = n!$, pues $E/\mathbb{Q}$ es una extensión galosiana. Por construcción de los cuerpos F_i, tenemos que $[E : \mathbb{Q}] = \prod_{i=0}^{n-1} [F_i : F_{i+1}] < n!$, lo que nos lleva a una contradicción.

ii.- Sea $\{\alpha_1, \cdots, \alpha_n\}$ el conjunto de raices de $f(x)$. El argumento dado en [i] prueba que los cuerpos $F_i = \mathbb{Q}(\alpha_1, \cdots, \alpha_i)$ cumplen con $[F_{i+1} : F_i] = n-i$. En particular, para una raiz α fija, se tiene no existe otra raiz de $f(x)$ en $\mathbb{Q}(\alpha)$. Sea $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ un automorfismo cualquiera. Entonces, como $\phi(\alpha)$ es una raiz de $f(x)$ en $\mathbb{Q}(\alpha)$, tenemos que $\phi(\alpha) = \alpha$. Esto nos permite concluir que $\phi = \mathrm{id}$.

4.- **Problema 4*:** Sea $f(x) \in \mathbb{Q}[x]$ un polinomio irreducible y sean $\alpha, \beta \in \mathbb{C}$ raíces de f. Suponga que $K/\mathbb{Q}$ es una extensión galoisiana finita con $K \subset \mathbb{C}$. Demuestre que el cuerpo $K \cap \mathbb{Q}(\alpha)$ es isomorfo a $K \cap \mathbb{Q}(\beta)$.

Demostración: Como α y β son raíces del mimo polinomio irreducible, existe un isomorfismo $\phi : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$. En particular, la restricción ψ de ϕ a $K \cap \mathbb{Q}(\alpha)$ satisface:

$$\psi : K \cap \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta).$$

Sea $z \in K \cap \mathbb{Q}(\alpha)$, entonces $\mathbb{Q}(z)$ es una extensión finita de K. Por lo tanto, el homomorfismo $\psi_2 : \mathbb{Q}(z) \to \mathbb{C}$ definido por $\psi_2(z) = \psi(z)$ se puede extender a un homomorfismo $\tau : K \to \mathbb{C}$. Luego, como K es normal, tenemos que $\tau(K) = K$, y por ende $\psi(z) \in K$. Concluimos que $\psi : K \cap \mathbb{Q}(\alpha) \to K \cap \mathbb{Q}(\beta)$. Usando el mismo argumento que antes, para ψ^{-1} se prueba que existe un homomorfismo:

$$\psi' : K \cap \mathbb{Q}(\beta) \to K \cap \mathbb{Q}(\alpha),$$

tal que $\psi' = \phi^{-1}|_{K \cap \mathbb{Q}(\beta)}$. Luego tenemos que $\psi \circ \psi' = \mathrm{id}$ y $\psi' \circ \psi = \mathrm{id}$. Concluimos que el cuerpo $K \cap \mathbb{Q}(\alpha)$ es isomorfo a $K \cap \mathbb{Q}(\beta)$.

5.- **Problema 5*:** Sea $f(x) \in \mathbb{Z}[x]$ un polinomio mónico, irreducible sobre $\mathbb{Q}[x]$, de grado $n \geq 2$ y tal que:

$$x^n f(x^{-1}) = f(x).$$

Sea $\alpha \in \mathbb{C}$ una raíz de f y sea $K = \mathbb{Q}(\alpha + \alpha^{-1})$.

i.- Demuestre que $[\mathbb{Q}(\alpha) : K] \leq 2$.

ii.- Demuestre que $[\mathbb{Q}(\alpha) : K] = 2$.

Desarrollo:

i.- Observe que $\mathbb{Q}(\alpha) = K(\alpha)$ y α satisface el polinomio $x^2 - x(\alpha + \alpha^{-1}) + 1 \in K[x]$. Por lo tanto $[\mathbb{Q}(\alpha) : K] \leq 2$.

ii.- Note que $z = 0, 1, -1$ no son raíces de f, pues en dicho caso $f(x) = \mathrm{irr}_{z,\mathbb{Q}}(x)$ es un polinomio de grado 1. Observe además que α^{-1} es una raíz de f, pues $\alpha^n f(\alpha^{-1}) = f(\alpha) = 0$. Como 1 y -1 no son raices de f se tiene que $\alpha \neq \alpha^{-1}$. Por lo tanto existe un isomorfismo no trivial $c : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ definido por $c(\alpha) = \alpha^{-1}$. Ahora bien $c : K \to K$ es el morfismo identidad, ya que $c(\alpha + \alpha^{-1}) = \alpha + \alpha^{-1}$. Esto prueba que $K \neq \mathbb{Q}(\alpha)$. Por lo tanto $[\mathbb{Q}(\alpha) : K] = 2$.