FACULTAD DE
CIENCIAS
UNIVERSIDAD DE CHILE

Apuntes de Ayudantía

GRUPOS Y ANILLOS

Claudio Bravo Castillo
August 20, 2016

Contents

AYUDANTÍAS

GRUPOS Y ANILLOS (OTOÑO 2016)

1. Grupos:

Ayudantía 1: En esta sección trabajaremos con un concepto de vital importancia en la teoría de grupos y en la matemática en general, estas son las acciones de grupos.

1.- **Problema 1:** Sea $G \cong C_n$ grupo cíclico de orden $n \in \mathbb{N}$ y sea $Aut(G)$ su grupo de automorfismos.

i.- Determine $|Aut(G)|$.

ii.- Demuestre que $Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Desarrollo:

i.- Recordemos que $Aut(G)$ actúa en G vía $\varphi.g := \varphi(g)$, para cualquiera $\varphi \in Aut(G)$, $g \in G$. Además todo homomorfismo φ de G está completamente determinado por su valor en σ, para $G = \langle \sigma \rangle$, ya que $\varphi(\sigma^i) = \varphi(\sigma)^i$. Además si $\varphi : G \longrightarrow G$, entonces $\varphi(\sigma) = \sigma^j$, para cierto $j \in \{1, \cdots, n\}$. Por otro lado si φ es ismomorfismo entonces $|\sigma| = |\varphi(\sigma)|$, reemplazando los valores respectivo obtenemos que $n = \frac{n}{(n,j)}$. Así $(n, j) = 1$, es decir ny j son relativamente primos, lo que equivale a que $j \in (\mathbb{Z}/n\mathbb{Z})^*$.

Reciprocamente para cualquiera $\varphi : G \to G$ tal que $\varphi(\sigma) = \sigma^j$, para $(j, n) = 1$ tenemos que φ es un automorfismo de G pues lleva el generador σ de G en otro generador del mismo grupo.

Luego $|Orb_{Aut(G)}(\sigma)| = |(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$, donde ϕ es la función de Euler.

Por último $Stab_{Aut(G)}(\sigma) = \{\varphi \in Aut(G) : \varphi(\sigma) = \sigma\} = id$. Por lo tanto $|Stab_{Aut(G)}(\sigma)| = 1$. Luego por la identidad

$$|Aut(G)| = |Orb_{Aut(G)}(\sigma)||Stab_{Aut(G)}(\sigma)|$$

tenemos que $|Aut(G)| = \phi(n)$, donde ϕ es la función de Euler.

ii.- Designemos por φ_j al automorfismo de G tal que $\varphi(\sigma) = \sigma^j$. Observe que la función:

$$\tau : Aut(G) \to (\mathbb{Z}/n\mathbb{Z})^* : \varphi_j \mapsto j,$$

es una función sobreyectiva, por lo visto en el ejercicio anterior. Como los conjuntos en cuestión son finitos y de igual cardinal, τ es una biyección. Además $\varphi_i(\varphi_j(\sigma)) = \sigma^{ij}$. Luego τ es homomorfismo, por ende isomorfismo.

2.- **Problema 2:** Sea $G \cong C_p \times C_p$, donde C_p es un grupo cíclico de p elementos, para p primo. Determine $|Aut(G)|$.

Desarrollo: Observe que $G \cong V$, donde $V = (\mathbb{F}_p)^2$ visto como $\mathbb{F}_p$-espacio

vectorial. Luego por lo visto en clases, $Aut(G) \cong Gl_2(\mathbb{F}_p)$ y dicho grupo tiene $(p^2-1)p(p-1)$ elementos.

3.- **Problema 3:** Sea G grupo simple y H subgrupo de G tal que $[G:H]=p$, para p primo. Demuestre que p es el primo más grande que divide a $|G|$ y que $p^i \nmid |G|$, $\forall i > 1$.

Demostración: Si $|G| = p$ el resultado se sigue facilmente. Si no es este el caso, considere la acción de G sobre el conjunto $X = \{gHg^{-1} : g \in G\}$ vía:

$$x.(gHg^{-1}) = (xg)H(xg)^{-1}.$$

Luego existe un homomorfismo $\varphi : G \to Biy(X)$ definido por $\varphi(g) = \sigma_g$, donde $\sigma_g(xHx^{-1}) = (gx)H(gx)^{-1}$. Observe que $\ker(\varphi) \triangleleft G$, luego $\ker(\varphi) = G$ o $\ker(\varphi) = \{0\}$.

Si $\ker(\varphi) = G$ entonces $\varphi = 0$. Pero $\sigma_g(H) = gHg^{-1}$, luego si $\varphi = 0$ entonces $\sigma_g(H) = H$. Por lo tanto $\forall g \in G$ tenemos que $gHg^{-1} = H$, es decir $H \triangleleft G$. Luego $H = G$, en cuyo caso $[G:H] = 1$ o bien $H = \{0\}$, en cuyo caso $|G| = [G:H] = p$. Ambas alternativas llevan a contradicciones.

Por otro lado si $\ker(\varphi) = \{0\}$ entonces $G \hookrightarrow Biy(X)$. Observe que $gHg^{-1} = hHh^{-1}$ sí y solamente sí $gh^{-1} \in N_G(H)$, es decir $|X| = [G : N_G(H)] \leq [G:H]$, pues $N_G(H) \supseteq H$.

Luego $|G|||Biy(X)| = r!$, donde $|X| = r \leq p$. Pero $p||G| = |H|[G:H]$. Luego si $q > p$ y $q||G|$ entonces $q|r!$ con $r \leq p$. Esto es contradictorio. Por otro lado si $p^i||G|$, para $i > 1$ entonces $p^i|r!$ luego $r = p$ y en este caso $p^{i-1}|(p-1)!$. Esto es contradictorio.

4.- **Problema 4:** Muestre que si un grupo G cumple con $|G| = n$ y p es el menor primo que divide a n.

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

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

iii.- Pruebe que $A_3 = \{id, (123), (132)\}$ es un subgrupo normal de S_3.

Desarrollo:

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

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

Esta acción induce un homomorfismo $\pi_H : G \to Biy(X)$, donde $\pi_H(g) = \sigma_g$, 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 $a \in G$, lo que equivale a que $(a^{-1}ga) \in H$, $\forall a \in G$. Así $K = \ker(\pi_H) = \cap_{a \in G} aHa^{-1}$.

Observe que $K \triangleleft G$ por ser núcleo de un homomorfismo. Además $K \subset H = eHe^{-1}$.

Sea $l = [H:K]$, así $[G:K] = [G:H][H:K] = pl$. Como X tiene p cosetos, tenemos que $G/K \hookrightarrow S_p$, donde S_p es el grupo de biyecciones de p elementos. Luego $pl = [G:K]|p!$, por lo tanto $l|(p-1)!$. Por otro lado, como p es el primo más pequeño que divide a $|G|$, tenemos que $l = 1$.

Finalmente $H = K \triangleleft G$.

ii.- Si $H \leq G$ tal que $[G : H] = 2$ como 2 es el primo más pequeo el resultado se sigue de la parte anterior.

iii.- Observe que $|A_3| = 3$ y $|S_3 = 6|$, luego $[S_3 : A_3] = 2$ y el resultado se sigue de lo expuesto en [ii].

5.- **Problema 5:** Sea G un grupo de orden n y S_n es el grupo de biyecciones de n elementos. Demuestre que existe un homomorfismo inyectivo $\varphi : G \to S_n$.

Demostración: Considere la acción de G sobre G vía $g.h = gh, \forall g, h \in G$. Esta acción de grupo induce un homomorfismo $\rho : G \to Biy(G)$ donde $\rho(g) = \sigma_g$, para $\sigma_g(h) = g.h = gh$. Observe que como $|G| = n$ tenemos que $Biy(G) \cong S_n$. Además $\ker(\rho) = \{g \in G : gh = 1, \forall h \in G\}$ tomando $h = 1$ tenemos que $\ker(\rho) = \{1\}$. Por lo tanto $\rho : G \to S_n$ es un homomorfismo inyectivo.

Ayudantía 2: En esta ayudantía trabajaremos los conceptos órbitas y estabilizadores de acciones de grupos.

1.- **Problema 1:** Considere la acción de $G = S_3$ sobre G por conjugación. Calcule el número de órbitas de dicha acción.

Desarrollo:

Partamos por considerar las órbitas más elementales. Observe que $\sigma(id)\sigma^{-1} = id$, $\forall \sigma \in G$. Luego $Orb_G(id) = \{id\}$.

Por otro lado el largo de cualquier permutación es la misma que la de su conjugado. Así $Orb_G((123)) \subseteq \{(123), (132)\}$. Pero $(12)(123)(12)^{-1} = (12)(123)(12) = (132)$. Luego $Orb_G((123)) = \{(123), (132)\}$.

Por último calculemos la órbita de la permutación (13). Recordemos que $(ab)^{-1} = (ab)$. Luego como $(12)(13)(12) = (23)$, $(12)(23)(12) = (13)$ y $(23)(13)(23) = (12)$ tenemos que $Orb_G((13)) = \{(12), (13), (23)\}$.

Finalmente concluimos que existen 3 clases de conjugación.

2.- **Problema 2:** Sea G grupo y $x \in Z(G)$. Considere la acción de G sobre sí mismo vía conjugación.

i.- Demuestre que $Orb_G(x) = \{x\}$.

ii.- Deduzca que $Z(S_3) = \{id\}$.

Desarrollo:

i.- Sabemos que por definición de centro de un grupo $xg = gx$, para todo $g \in G$. Luego $x = gxg^{-1}$, para todo $g \in G$. Es decir $Orb_G(x) = \{x\}$.

Observe que el recíproco de este hecho también es cierto. En efecto si $Orb_G(x) = \{x\}$ entonces $x = gxg^{-1}$, $\forall g \in G$. Luego $gx = xg$, $\forall g \in G$. Equivalentemente1 $x \in Z(G)$.

ii.- Basta analizar los elementos de S_3 con el fin de encontrar los elementos que tienen órbita trivial. Así concluimos que $Z(S_3) = \{id\}$.

3.- **Problema 3:** Sea $G = S_n$ grupo y considere el $\mathbb{F}_q$ espacio vectorial $V = \mathbb{F}_q^n$, donde $q = p^t$, para p primo. Definimos la acción de G sobre V de la manera siguiente. Sea $v = \sum_{i=1}^n \alpha_i e_i$ entonces:

$$\sigma.v = \sum_{i=1}^n \alpha_i e_{\sigma(i)}.$$

Calcule el número de órbitas de dicha acción.

Desarrollo:

Utilizaremos la siguiente igualdad vista en clases. Sea c el número de órbitas de una acción y $Fix(g) = \{v \in V : g.v = v\}$, entonces:

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

Sea $v = \sum_{i=1}^n \alpha_i e_i$ entonces $\sigma.v = v$ sí y solamente sí:

$$\sum_{i=1}^n \alpha_i e_i = \sum_{i=1}^n \alpha_i e_{\sigma(i)}.$$

Luego si $\sigma = (a_1 \cdots a_t)$ entonces $\alpha_{a_1} = \alpha_{a_2} = \cdots = \alpha_{a_t}$. Por lo tanto tenemos q^{n-t+1} posibles vectores con dicha propiedad. Por otro lado sabemos que existen $\binom{n}{t}$ permutaciones de largo t, para $t > 1$. Observe que si $t = 1$ entonces $\sigma = id$ y en dicho caso existen q^n elementos estables por la acción de σ. Por lo tanto:

$$c = \frac{1}{n!}\left[\sum_{t=2}^{n}\binom{n}{t}q^{n-t+1} + q^n\right].$$

Luego:

$$c = \frac{1}{n!}\left[q(q+1)^n - q^{n+1} - (n-1)q^n\right].$$

4.- **Problema 4:** Considere la acción de G sobre $Aut(G)$ vía:

$$(g.\varphi)(x) = \varphi(gxg^{-1}) = \varphi \circ \varphi_g(x),\ \forall g \in G\ \forall \varphi \in Aut(G),$$

donde $\varphi_g(x) = gxg^{-1}$ se denomina automorfismo interior.

i.- Calcule el número de órbitas de dicha acción. Concluya que $[G : Z(G)]||Aut(G)|$.

ii.- Calcule el número de órbitas para G grupo abeliano. Concluya que en este caso la acción es trivial.

iii.- Calcule el número de órbitas para $G = Q_8$

iv.- Demustre que $G/Z(G) \cong \{\varphi_g : \varphi_g\ aut.\ interior\}$. Concluya que $Z(G) \triangleleft G$ y deduzca nuevamente que $[G : Z(G)]||Aut(G)|$.

Desarrollo:

i.- Haremos uso de la identidad explicada en el problema anterior, que nos dice que el número de órbitas c de la acción es:

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

En efecto sea $g \in G$. Nos preguntamos cuantos automorfismos φ cumplen con $\varphi(gxg^{-1}) = \varphi(x), \forall x \in G$. Observe que como φ es inyectivo tenemos que $x = gxg^{-1}, \forall x \in G$. Luego $|Fix(g)| = |Aut(G)|$, si $g \in Z(G)$ o bien $|Fix(g)| = 0$, si $g \notin Z(G)$. De esto se sigue que:

$$c = \frac{|Z(G)||Aut(G)|}{|G|},$$

lo que es equivalente a:

$$c = \frac{|Aut(G)|}{[G : Z(G)]}.$$

Luego como $c \in \mathbb{N}$ concluimos que $[G : Z(G)]||Aut(G)|$.

ii.- Observe que si G es abeliano, entonces $[G : Z(G)] = 1$. Entonces $c = |Aut(G)|$. Luego existen tantas órbitas como elementos del conjunto sobre el que actúa G. Esto implica que $g.\varphi = \varphi$ para cualquier $g \in G$ y $\varphi \in Aut(G)$.

ii.- Sabemos que $Z(Q_8) = \{1, -1\}$. Por otro lado todo automorfismo φ de Q_8 en Q_8 cumple con $\varphi(1) = 1$, además como -1 es el único elemento de orden 2 tenemos que $\varphi(-1) = -1$. Por otro lado $\varphi(i) \in \{\pm i, \pm j, \pm k\}$ y $\varphi(j) \in \{\pm i, \pm j, \pm k\} - \{\varphi(i), \varphi(-i)\}$. Esto último pues una vez elegido el valor de $\varphi(i)$, el de $\varphi(-i) = -\varphi(i)$. Lo mismo para j y k. Además una vez

obtenido el valor de i y j el de $k = ij$ está únicamente determinado. Así tenemos que $|Aut(Q_8)| = 24$. Finalmente obtenemos que $c = \frac{48}{8} = 6$.

iv.- Observe que $\{\varphi_g : \varphi_g \; aut. \; interior\}$ es un grupo con la composición de funciones. A dicho grupo le llamaremos *grupo de automorfismos interiores de* G y lo denotaremos por $Inn(G)$. Observe que el homomorfismo $\rho : G \to Inn(G)$ definido por $\rho(g)(x) = gxg^{-1}$ es un morfismo sobreyectivo. Ahora bien $\ker(\rho) = \{g \in G : gxg^{-1} = x, \; \forall x \in G\} = Z(G)$. Luego $G/Z(G) \cong Inn(G)$.

Concluimos que $Z(G) \lhd G$. Además como $Inn(G) \leq Aut(G)$ tenemos que $[G : Z(G)] = |Inn(G)|$ cumple con $[G : Z(G)]||Aut(G)|$.

Ayudantía 3: En esta ayudantía trabajaremos los conceptos centro y centralizador en el grupo de biyecciones S_n.

1.- **Problema 1:** Sea $\sigma \in S_n$ y $x = (a_1 \cdots a_t)$ un ciclo de largo t. Demustre que $\sigma x \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_t))$.

Demostración: Sea $i \in \{1, \cdots, n\}$. Si $i = \sigma(a_j)$, algún $j \in \{1, \cdots t\}$, entonces $\sigma x \sigma^{-1}(i) = \sigma x(a_j) = \sigma(a_{j+1}) = (\sigma(a_1) \cdots \sigma(a_t))(i)$. Por otro lado si $i \neq \sigma(a_j)\ \forall j$, entonces $\sigma x \sigma^{-1}(i) = i = (\sigma(a_1) \cdots \sigma(a_t))(i)$. Luego por igualdad de funciones tenemos que $\sigma x \sigma^{-1} = (\sigma(a_1) \cdots \sigma(a_t))$.

1.- **Ejercicio 1:** Sea $\sigma \in S_n$ y $x = (a_{11} \cdots a_{1t_1}) \cdots (a_{r1} \cdots a_{rt_r}) \in S_n$ elemento cualquiera en S_n escrito como producto de ciclos disjuntos. Demustre que $\sigma x \sigma^{-1} = (\sigma(a_{11}) \cdots \sigma(a_{1t_1})) \cdots (\sigma(a_{r1}) \cdots \sigma(a_{rt_r}))$.

2.- **Problema 2:** Sea S_n grupo de biyecciones del conjunto de n elementos y considere la acción de S_n sobre sí mismo por conjugación.

i.- Demustre que si $x = (a_1 \cdots a_t)$ un ciclo de largo t, entonces $Orb_{S_n}(x) = Orb_{S_n}((1 \cdots t)) = \{(b_1 \cdots b_t) : b_i \in \{1, \cdots, n\}\}$.

ii.- Deduzca que $Z(S_n) = \{id\}$, para $n \geq 3$.

Desarrollo:

i.- Considere $\{b_1, \cdots, b_t\} \subseteq \{1, \cdots, n\}$. Entonces siempre existe una biyección σ tal que $\sigma(a_i) = b_i$. Luego $\sigma x \sigma^{-1} = (b_1 \cdots b_t)$. Por otro lado todo conjugado de x es un cíclo de largo t por lo probado en [1]. Esto implica que $Orb_{S_n}(x) = \{(b_1 \cdots b_t) : b_i \in \{1, \cdots, n\}\}$. Además como x es cualquier ciclo de largo t, podemos sín pérdida de generalidad asumir que es $(1 \cdots t)$. Luego $Orb_{S_n}(x) = Orb_{S_n}((1 \cdots t)) = \{(b_1 \cdots b_t) : b_i \in \{1, \cdots, n\}\}$.

ii.- Observe que el argumento dado en [1] se extiende a productos de ciclos disjuntos de largos distintos. Luego lo dicho en [i] prueba que la órbita de cualquier elemento no trivial tiene más de un elemento. Pero sabemos que $x \in Z(S_n)$ sí y solamente sí su órbita bajo la acción de conjugación consta sólo de x. Por lo tanto $Z(S_n) = \{id\}$.

3.- **Problema 3:** Sea $x = (12)(34)(56) \in S_6$. Calcule $|C_{S_6}(x)|$.

Desarrollo: Recordemos que G actúa en $\mathcal{P}(G)$ de la siguiente manera. Sea $S \subseteq G$, entonces $g.S := gSg^{-1}$. Así $G_S = \{g \in G : gSg^{-1} = S\}$. Luego $|\{gSg^{-1} : g \in G\}| = [G : G_S]$. Cuando $S = \{s\}$, decimos que $G_s = C_G(s)$ y entonces $|\{gsg^{-1} : g \in G\}| = [G : C_G(s)]$. Observe que si $x = (12)(34)(56)$ entonces para cualquier $\sigma \in S_n$ tenemos que $\sigma x \sigma^{-1} = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))(\sigma(5)\sigma(6))$. Luego los conjugados de x son 15, esto pues en la primera transposición el 1 puede ir a $2, 3, 4, 5, 6$ y luego, en la siguiente transposición, uno de los cuatro números retantes puede tomar 3 opciones. Con esto la última transpocición queda fija. Concluimos que $|C_{S_6}(x)| = \frac{6!}{15} = 48$.

4.- **Problema 4:** Sea $\sigma \in S_m$ un ciclo de largo m.

i.- Demuestre que $|C_{S_n}(\sigma)| = m(n-m)!$.

ii.- Pruebe que $C_{S_n}(\sigma) = \{\sigma^i \tau : 0 \leq i \leq m-1,\ \tau \in S_{n-m}\}$.

iii.- Calcule $|C_{S_7}((123))|$.

Desarrollo:

i.- Recordemos que si $\sigma = (a_1 \cdots a_m)$ entonces $g\sigma g^{-1} = (g(a_1) \cdots g(a_m))$. Luego $g(a_1) \in \{1, \cdots, n\}$, $g(a_2) \in \{1, \cdots, n\} - \{g(a_1)\}$ y así sucesivamente. Es decir fijados los valores de $g(a_1), \cdots, g(a_i)$ tenemos que $g(a_{i+1})$ puede tomar $n - i$ valores. Además de esto si permutamos los valores cíclicamente en una trasposición, obtenemos la misma transposición. Por lo tanto $|\{g\sigma g^{-1} : g \in G\}| = \frac{n(n-1)\cdots(n-m+1)}{m}$. Concluimos que $|C_{S_n}(\sigma)| = \frac{mn!}{n(n-1)\cdots(n-m+1)} = m(n-m)!$.

ii.- Observe que $\langle\sigma\rangle \subseteq C_{S_n}(\sigma)$. Por otro lado $g \in Biy(\{1, \cdots, n\} - \{a_1, \cdots, a_t\})$ cumple con $g\sigma g^{-1} = (g(a_1) \cdots g(a_m)) = \sigma$. Además $|C_{S_n}(\sigma)| = m(n-m)! = |\{\sigma^i\tau : 0 \leq i \leq m-1,\ \tau \in S_{n-m}\}|$, esto pues las biyecciones en S_{n-m} son disjuntas de las potencias de σ. Luego como existe una contensión y los conjuntos tienen igual cardinal, tenemos que $C_{S_n}(\sigma) = \{\sigma^i\tau : 0 \leq i \leq m-1,\ \tau \in S_{n-m}\}$.

iii.- Concluimos que $|C_{S_7}((123))| = 3(7-3)! = 72$.

4.- **Ejercicio:** Sea $\sigma \in S_n$ un producto de r transposiciones disjuntas. Pruebe que $|C_{S_n}(\sigma)| = 2^r r!(n-2r)!$.

Ayudantía 4: En esta ayudantía trabajaremos en torno a la ecuación de clase y sus aplicaciones.

1.- **Problema 1:** Pruebe que si un grupo G cumple con que $G/Z(G)$ cíclico, entonces G es un grupo abeliano. Concluya que $Inn(G) = \{id\}$.

Demostración:

Sea $G/Z(G) = \{g^i Z(G) : i \in \mathbb{Z}\}$ grupo cíclico. Consideremos $x, y \in G$, entonces $xZ(G) = g^i Z(G)$ e $yZ(G) = g^j Z(G)$, para ciertos $i, j \in \mathbb{Z}$. Es decir $x = ag^i$ e $y = bg^j$, para ciertos $a, b \in Z(G)$. Luego $xy = ag^i bg^j = abg^{i+j} = bag^{j+i} = yx$. Por lo tanto G es un grupo abeliano.

Recordando el isomorfismo visto en la ayudantía anterior, tenemos que $G/Z(G) \cong Inn(G)$. Luego como $G = Z(G)$, tenemos que $Inn(G) = \{id\}$.

2.- **Problema 2:** Sea G grupo de orden pq donde p y q son primos distintos.

i.- Pruebe que $|Z(G)| \neq q, p$.

ii.- Demuestre que todo grupo G de orden pq no abeliano tiene centro trivial. Calcule el $Z(S_3)$.

Desarrollo:

i.- Observe que si $|Z(G)| = p$ entonces $|G/Z(G)| = q$ primo. Luego $G/Z(G)$ es un grupo cíclico de orden q primo. Usando el problema 1 concluimos que G es un grupo abeliano. Luego $|Z(G)| = pq$ y esto nos lleva a una contradicción. El razonamiento con $|Z(G)| = q$ es análogo.

ii.- Sabemos que $|Z(G)||G|$ entonces $|Z(G)| \in \{pq, p, q, 1\}$. Luego si $|Z(G)| = pq$ tenemos que $G = Z(G)$, equivalentemente G es abeliano. Además $|Z(G)| \neq p, q$ por la parte [i]. Luego $|Z(G)| = 1$, es decir $Z(G) = \{e\}$.

Por último observe que, como S_3 es no abeliano y tiene orden $6 = 3 \cdot 2$, entonces $Z(S_3) = \{id\}$.

3.- **Problema 3:** Sea G un grupo de orden p^2, para p primo.

i.- Demuestre que G es abeliano.

ii.- Demuestre que $G \cong C_{p^2}$ o bien $G \cong C_p \times C_p$.

Desarrollo:

i.- Recordemos que como $|G| = p^2$ tenemos que $|Z(G)| \in \{p^2, p\}$. Si $|G| = |Z(G)| = p^2$ tenemos que G es abeliano. Por otro lado si $|Z(G)| = p$, entonces $|G/Z(G)| = p$, luego $G/Z(G)$ es cíclico. Por lo tanto, por el problema 1, G es abeliano.

ii.- Si G tiene un elemento de orden p^2, entonces $G \cong C_{p^2}$. Si esto no sucede, entonces todo elemento distinto de la identidad tiene orden p. Sea $x \in G - \{1\}$ e $y \in G - \langle x \rangle$. Entonces $|\langle x, y \rangle| > |x| = p$, puesto que $y \in \langle x, y \rangle - \langle x \rangle$. Así $|\langle x, y \rangle| = p^2$ y por lo tanto $G = \langle x, y \rangle$. Por otro lado $\psi : G \to \langle x \rangle \times \langle y \rangle$, definido por $\psi(x^i y^j) = (x^i, y^j)$ es un isomorfismo de grupos. Es decir $G \cong \langle x \rangle \times \langle y \rangle = C_p \times C_p$.

4.- **Problema 4:** Demuestre que no existen grupos simples de orden p^m, para $m > 1$ y p primo.

Demostración: Utilizaremos el teorema de cauchy para grupos abelianos. Este dice que si p primo cumple con $p||G|$, entonces G tiene un subgrupo de orden p.

Recordemos que todo grupo de orden p^m tiene centro no trivial. Así $|Z(G)| = p^t$, para cierto $t \in \{1, \cdots, m\}$. Por lo tanto $p||Z(G)|$. Luego $Z(G)$ tiene un subgrupo de orden p, debido a que este grupo es ciertamente abeliano. A posteriori G tiene un subgrupo de orden p, digamos $H = \langle h \rangle$, para cierto $h \in H$.

Por otro lado si tomamos cualquier $g \in G$ tenemos que $ghg^{-1} = h$, puesto que $h \in Z(G)$. Esto implica que $gHg^{-1} = H$, $\forall g \in G$. En otras palabras $H \triangleleft G$. Por ende G tiene un subgrupo normal de orden p y esto implica que no es simple.

5.- **Problema 5:** Sea G es un grupo de orden p^3, para cierto p primo, con G no abeliano.

i.- Pruebe que $|Z(G)| = p$.

ii.- Calcule el centro de D_8 y Q_8.

iii.- Calcule $Inn(G)$ y concluya que $Inn(D_8) = Inn(Q_8) = C_2 \times C_2$.

Desarrollo:

i.- Recordemos que como corolario de la ecuación de clase tenemos que todo p-grupo tiene centro no trivial. Luego $|Z(G)| \in \{p^3, p^2, p\}$.

Es evidente que si $|Z(G)| = p^3$ entonces $G = Z(G)$. Lo que es equivalente a que G sea abeliano.

Por otro lado si $|Z(G)| = p^2$ entonces $|G/Z(G)| = p$ primo. Luego $G/Z(G)$ es cíclico y por ende G es abeliano. Finalmente $|Z(G)| = p$.

ii.- Para calcular el centro de Q_8 y D_8 observemos que $|Q_8| = |D_8| = 8$ y estos son grupos no abelianos. Luego $|Z(D_8)| = |Z(Q_8)| = 2$. En el caso del grupo cuaternionico Q_8 tenemos que $\{\pm 1\} \subset Z(G)$. Luego $Z(G) = \{\pm 1\}$. Por otro lado en el caso del grupo diedral $D_8 = \langle r, s : r^4 = s^2 = 1,\ sr = r^{-1}s \rangle$ tenemos que $1 \in Z(G)$, por ende nos falta un elemento en el centro del grupo. Observe que $sr^2 = r^3sr = r^6s = r^2s$ y $r^2r = rr^2$. Por lo tanto $Z(D_8) = \{1, r^2\}$.

iii.- Para calcular los grupos de automorfismos interiores basta calcular el cociente $G/Z(G)$. Observe que $|G/Z(G)| = p^2$. Luego por el problema 3 tenemos que $G/Z(G)$ es isomorfo a C_{p^2} o $C_p \times C_p$. Si $G/Z(G) \cong C_{p^2}$ entonces G es abeliano. Luego $Inn(G) \cong G/Z(G) \cong C_p \times C_p$. En particular $Inn(D_8) = Inn(Q_8) = C_2 \times C_2$.

6.- **Problema 6:** Sea $G = Gl_n(\mathbb{F}_p)$ grupo de matrices invertibles sobre $\mathbb{F}_p$.

i.- Calcule el orden del subgrupo $H = \{(a_ij) : a_ii = 1\, a_{ij} = 0\ sii > j$.

ii.- Concluya que $Z(H)$ es no trivial.

iii.- Calcule el orden de cualquier elemento σ conjugado a $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en $Gl_2(\mathbb{F}_p)$. Pruebe que $\langle \sigma \rangle \cong C_p$.

Desarrollo:

i.- Para encontrar dicho valor, analicemos el conjunto en cuestión. Sea $A = (a_ij) \in H$. Observe que a_{12} puede tomar cualquier valor en $\mathbb{F}_p$. Lo mismo va a suceder en a_{13} y a_{23}, esto pues en cualquier caso $det(A) = 1 \in \mathbb{F}_p^*$. Así (a_ij) puede tomar cualquier valor en $\mathbb{F}_p$. Por lo tanto tenemos p^α elemnetos

diferentes, donde $\alpha = \sum_{i=1}^{n-1} i = \frac{n(n-1)}{2}$. En síntesis $|H| = p^{\frac{n(n-1)}{2}}$. Observe que este grupo tiene por orden la mayor potencia de p que divide a $|G|$.

ii.- Como H es un grupo de orden p tenemos, como consecuencia de la ecuación de clase, que $Z(H)$ es no trivial.

iii.- Sea $w = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Entonces $|\sigma| = |w|$. Pero por inducción se puede demostrar que $w^i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$. Luego $|w| = p$ y por lo tanto $|\sigma| = p$. Concluimos que como $|\langle\sigma\rangle| = |\sigma| = p$, entonces $\langle\sigma\rangle \cong C_p$.

Ayudantía 5: En esta ayudantía tiene por objetivo demostrar el teorema general de Cauchy y trabajar con sus aplicaciones.

1.- **Problema 1:** Sea G un grupo de orden n. 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 $C_p = \langle a \rangle$.

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 $O = Orb((g_1, \cdots, g_p))$, $S = Stab((g_1, \cdots, g_p))$ la órbita y el establizador de $(g_1, \cdots, g_p) \in G^p$ respectivamente. Recordemos que $|O| = \frac{|H|}{|S|}$. Luego debemos encontrar el número de elemntos del estabilizador. 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 $gg_i = g_i$, así $g = 1$.

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 $g^p g_i = g^p g_{i+pk} = g_i$. Por lo tanto $g^p = 1$. Pero por hipótesis esto implica que $g = 1$. Esto tiene por consecuencia que $g_1 = g_{1+k} = \cdots = g_{1+pk}$, es decir todas las coordenadas son iguales, puesto que $\langle k \rangle \cong C_p$.

Por lo tanto $S = \{1\} \times C_p$, si $g_1 = \cdots = g_p$ o bien $S = \{1\} \times \{1\}$. Concluimos 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 actua en órbitas disjuntas. Observe que la órbita de tamao 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 tamao 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 $p \neq n$. 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.

i.- Pruebe que G tiene un subgrupo normal H de orden p.

ii.- Demuestre que G tiene un subgrupo normal H_s de orden p^s, para cualquier $s \leq n$.

Desarrollo:

i.- Observe que por lo dicho en la ayudantía previa, tenemos que $|Z(G)| = p^m$, cierto $1 < m \leq n$. Por lo tanto tenemos, por el teorema de Cauchy, un subgrupo H de orden p en G. Ahora bien como $H \leq Z(G)$ tenemos que $H \triangleleft G$.

ii.- Razonaremos por inducción. Si $n = 1$ es trivial. Para $n = 2$ sabemos por [i] que existe $H \triangleleft G$, con $|H| = p$. Además $G, \{1\} \triangleleft G$ de orden p^2 y 1 respectivamente.

Supongamos que la afirmación es cierta para $n \in \mathbb{N}$. Sea G grupo de orden p^{n+1}. Entonces por [i] 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 $|K_s| = p^{s+1}$. Definimos $H_s = K_{s-1}$. Entonces 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:** Sea G un grupo de orden pq, para $p < q$ primos.

i.- Demuestre que G tiene un subgrupo normal de orden q.

ii.- De un contraejemplo para la normalidad de un grupo de orden p.

Desarrollo:

i.- Sabemos que $q||G|$, luego por el teorema de Cauchy tenemos que existe un subgrupo H de G de orden q. Luego como $[G : H] = p$ menor primo que divide al orden de G, tenemos que, por lo visto en la ayudantía 2, $H \triangleleft G$.

ii.- Considere $G = S_3$, donde $|G| = 3 \cdot 2$. Dicho grupo tiene un sólo subgrupo normal. Este es el grupo alternante A_3 de orden 3. Así no existen subgrupos normales de orden 2.

3.- **Ejercicio:** Pruebe que si G es un grupo abeliano de orden pq, entonces G es cíclico.

4.- **Problema 4:** Encuentre todos los grupos abelianos simples.

Desarrollo: Observe que si G es un grupo abeliano simple entonces sus unicos subgrupos son los triviales. Esto último debido a que todo subgrupo de un grupo abeliano es normal. Ahora bien $p||G|$, para cierto p primo. Por el teorema de Cauchy tenemos que existe H subgrupo de G con $|H| = p$. Luego $G = H \cong C_p$.

Ayudantía 6: Esta ayudantía tiene por objetivo comenzar a trabajar con los teoremas de Sylow.

1.- **Problema 1:** Sean $H, K \triangleleft G$ tales que $H \cap K = \{1\}$ y $|G| = |H||K|$. Pruebe que $G \cong H \times K$.

Demostración: Sea $\phi : H \times K \to G$, $\phi(h,k) = hk$ función entre grupos. Observe que $\phi(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. Por otro lado $\phi(h_1,k_1)\phi(h_2k_2) = h_1k_1h_2k_2$. Pero por la normalidad de H y K tenemos que existen $h_3 \in H$, $k_3 \in K$ tales que $h_1k_1h_2k_2 = h_1h_2k_3k_2 = h_1h_3k_1k_2$. Luego $h_2k_3 = h_3k_1$, es decir $h_2(k_3k_1^{-1})h_2^{-1} = h_3h_2^{-1} \in H \cap K$. Luego $h_3 = h_2$ y $k_3 = k_1$. Por lo tanto $\phi(h_1,k_1)\phi(h_2,k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 = \phi(h_1h_2, k_1k_2)$. Es decir ϕ es homomorfismo de grupos.

Observe que $\ker(\phi) = \{(h,k) : hk = 1\}$. Pero si $hk = 1$, entonces $h = k^{-1} \in H \cap K$. Por ello $h = k = 1$. Luego $\ker(\phi) = \{(1,1)\}$, es decir ϕ es inyectivo. Además como los conjuntos finitos de partida y llegada tienen igual número de elementos, tenemos que ϕ es biyectiva.

1.- **Ejercicio:** Sea G grupo de orden 50 que tiene un grupo normal de orden 2. Pruebe que $G \cong C_{50}$ o bien $G \cong C_5 \times C_{10}$.

2.- **Problema 2:** Sea G grupo.

i.- Encuentre todos los grupos G de orden 21 salvo isomorfía.

ii.- Encuentre todos los grupos G de orden 15.

iii.- Generalice estas ideas.

Desarrollo:

i.- Sea G grupo tal que $|G| = 21 = 7 \cdot 3$. Entonces existe $S \leq G$ un 7-Sylow y $T \leq G$ un 3-Sylow. Observe que $n_7 \equiv 1(7)$ y que $n_7|3$. Por lo tanto $n_7 = 1$, es decir $S \triangleleft G$. Además $n_3 \equiv 1(3)$ y $n_3|7$. Así $n_3 = 1, 7$. Dividamos el análisis en casos.

Si $n_3 = 1$, entonces $T \triangleleft G$. Luego $H, T \triangleleft G$, con $H \cap T = \{1\}$ y $|G| = |H||T|$. Por lo tanto $G \cong H \times K \cong C_3 \times C_7 \cong C_{21}$, por teorema chino.

Si $n_3 = 7$, tenemos que existen 7 subgrupos de orden 3 en G. Sea $T = \{1, a, a^2\}$ grupo de orden 3. Como $S \triangleleft G$ tenemos que $aSa^{-1} = S$. Luego si $S = \{1, b, \cdots, b^6\}$ entonces $aba^{-1} = b^i$, cierto $i \in \{1, \cdots, 6\}$. Observe que, por inducción, $ab^ka = b^{ik}$ y $a^nba^{-n} = b^{i^n}$. Luego requerimos que $b = a^3ba^{-3} = b^{i^3}$, es decir $i^3 \equiv 1(7)$. Por lo tanto $i \in \{1, 2, 4\}$. Observe que si $i = 1$ entonces G abeliano y por lo tanto $n_3 = 1$. Concluimos que:

$$G \cong \langle a, b : b^7 = a^3 = 1,\ aba^{-1} = b^2 \rangle,$$

o bien:

$$G \cong \langle a, b : b^7 = a^3 = 1,\ aba^{-1} = b^4 \rangle.$$

ii.- Sea G grupo de orden $15 = 3 \cdot 5$. Entonces existe $S \leq G$ un 5-Sylow y $T \leq G$ un 3-Sylow. Observe que $n_5|3$ y $n_5 \equiv 1(5)$. Luego $n_5 = 1$, es decir $S \triangleleft G$. Análogamente $n_3|5$ y $n_3 \equiv 1(3)$. Entonces $n_3 = 1$, es decir $T \triangleleft G$. Luego $G \cong H \times T \cong C_3 \times C_5 \cong C_{15}$.

iii.- En general si $|G| = pq$, con $p > q$ y $p \neq 1(q)$ entonces $G \cong C_p \times C_q \cong C_{pq}$. En otro caso hay que aplicar el prodecimiento visto en [i], que es completamente general.

3.- **Problema 3:** Sea G grupo de orden 312. Pruebe que G tiene un p-subgrupo de Sylow normal, para cierto p primo. Determine dicho número primo.

Desarrollo: Evidentemente usaremos los teoremas de Sylow. Observe que $|G| = 312 = 2^3 \cdot 3 \cdot 13$. Observe que $n_{13}|24$ y $n_{13} \equiv 1(13)$. Luego $n_{13} \in \{1, 2, 4, 8, 3, 6, 12, 24\}$. Pero todos los valores menos el 24 son menores y $24 \equiv 11(13)$. Por ello $n_{13} = 1$. Luego existe un 13-Sylow normal en G. Esto nos dice que G no es simple.

4.- **Problema 4:** Sea G grupo.

i.- Pruebe que no existen grupos de orden 35 simples.

ii.- Encuentre todos los grupos de orden $3^2 \cdot 5$.

Desarrollo:

i.- Si G es un grupo de orden $35 = 7 \cdot 5$. Entonces $n_7|5$ y $n_7 \equiv 1(7)$. Luego $n_7 = 1$, es decir existe $H \triangleleft G$ un 7-Sylow. Por otro lado $n_5|7$ y $n_5 \equiv 1(5)$. Luego $n_5 = 1$, es decir existe $S \triangleleft G$ un 5-Sylow. Luego como $S \cap H = \{1\}$ tenemos que $G \cong H \times S \cong C_7 \times C_5 \cong C_{35}$. En particular G no es simple.

ii.- Sea G grupo de orden $3^2 \cdot 5$. Entonces $n_3|5$ y $n_3 \equiv 1(3)$. Luego $n_3 = 1$, es decir existe $H \triangleleft G$ un 3-Sylow. Por otro lado $n_5|3^2$ y $n_5 \equiv 1(5)$. Luego $n_5 = 1$, es decir existe $S \triangleleft G$ un 5-Sylow. Luego como $S \cap H = \{1\}$ tenemos que $G \cong H \times S \cong C_9 \times C_5 \cong C_{45}$ o bien $G \cong C_3 \times C_3 \times C_5$.

5.- **Problema 5:** Pruebe que todo grupo de orden $56 = 7 \cdot 2^3$ no es simple.

Demostración: Observe que por el teorema de Sylow existen $T, H \leq G$ que son 2-Sylow y 7-Sylow respectivamente. Además $n_7|2^3$ y $n_7 \equiv 1(7)$. Luego $n_7 \in \{1, 8\}$. Por otro lado $n_2|7$ y $n_2 \equiv 1(2)$, esto implica que $n_2 \in \{1, 7\}$. Observe que si $n_2 = 1$ o $n_7 = 1$ entonces G tiene un 2-Sylow o un 7-Sylow normal, respectivamente. Luego G no es simple. Por lo tanto solo debemos descartar el caso $n_2 = 7, n_7 = 8$.

En efecto, si T es un 2-Sylow y H es un 7-Sylow entonces $H \cap T = \{1\}$. Esto pues si $x \in H \cap T$ entonces $|x||7, 2^3$. Luego $|x| = 1$, es decir $x = 1$. Además los 2-Sylow se intersectan a lo más en 4 elementos, pues si lo hacen en 8 de estos, resultan ser el mismo subgrupo. También todos los 7-Sylow son cílicos, luego si dos de estos se intersectan en un elemento no trivial, los subgrupos resultan ser los mismos. Esto último se debe a que si $H_1 \cap H_2 \subseteq \{1, x\}$ entonces $\langle x \rangle \cong C_7$, luego $|H_1 \cap H_2| = 7$, es decir $H_1 = H_2 = H_1 \cap H_2$. Por lo tanto en G tenemos por lo mínimo $1 + 6 \cdot 8 + 7 \cdot 4 = 77$ elementos. Esto es contradictorio.

Ayudantía 7: Esta ayudantía tiene por objetivo seguir trabajando con los teoremas de Sylow.

1.- **Problema 1:** Sea G grupo de orden $p^t m$, con $(m,p)=1$. Por lo teoremas de Sylow, existe un p-subgrupo de Sylow $S \subset G$. Además los demás p-subgrupos de Sylow son conjugados de S.

i.- Pruebe que el número n_p de p-subgrupos de Sylow diferentes es $[G : N_G(S)]$.

ii.- Deduzca que $n_p | m$.

iii.- Pruebe que si $n_p = 1$ entonces $S \triangleleft G$.

Demostración:

i.- Observe que $gSg^{-1} = tSt^{-1}$ sí y solamente sí $gt^{-1} \in N_G(S)$. Luego por cada clase en $G/N_G(S)$ tenemos un conjugado de S distinto. Por ello $n_p = |G/N_G(S)| = [G : N_G(S)]$.

ii.- Observe que $m = [G : S] = [G : N_G(S)][N_G(S) : G]$. Luego $n_p | m$.

iii.- Observe que si $n_p = 1$ entonces para cualquier $g \in G$ tenemos que $gSg^{-1} = S$. Luego $S \triangleleft G$.

2.- **Problema 2:** Sea G grupo de orden 39.

i.- Encuentre todos los grupos de dicho orden, salvo isomorfía.

ii.- Encuentre todos los elementos de orden 3 en dichos grupos.

iii.- Suponga que G es abeliano. Calcule su grupo de automorfismos.

Desarrollo:

i.- Usaremos los teoremas de Sylow. Observe que $n_{13} | 3$ y $n_{13} \equiv 1(13)$. Luego $n_{13} = 1$. Es decir existe $T \leq G$ un 13-Sylow normal. Por otro lado $n_3 | 13$ y $n_3 \equiv 1(3)$. Luego $n_3 = 1$ o $n_3 = 13$. Dividamos el análisis en casos:

a.- Si $n_3 = 1$. Entonces existe $S \leq G$ un 13-Sylow normal. 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.- 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 $aTa^{-1} = T$. Luego 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 $a^n b a^{-n} = b^{i^n}$. Luego requerimos que $b = a^3 b a^{-3} = b^{i^3}$, 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 un una homomorfismo que envia generadores en generadores, luego es un isomorfismo. Observe que está bien definida pues $\phi(ab) = a^2 b = ab^9 a = b^{81} a^2 = b^3 a^2 = \phi(b^3 a)$. Luego $G_1 \cong G_2$.

ii.- Recordemos que todos los elementos de orden 3 generan subgrupos de G de orden 3. Dichos subgrupos, en el caso abeliano $G \cong C_{39} = \langle \sigma \rangle$ solo uno y es $H = \langle \sigma^{13} \rangle$. Por otro lado si G no es abeliano, entonces son los conjugados de $S = \langle a \rangle$, es decir los subgrupos $S' = b^i S b^{-i} = \langle b^i a b^{-i} \rangle$, para $i \in \{0, \cdots, 12\}$. Luego los elementos de orden 3 en G son los elementos $b^i a b^{-i}, b^i a^2 b^{-i}$ donde $i \in \{0, \cdots, 12\}$.

iii.- Observe que si G es un grupo abeliano, entonces $G \cong C_{39}$. Luego por lo visto en la ayudantía 1 tenemos que $Aut(G) \cong (\mathbb{Z}/39\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/13\mathbb{Z})^* \cong C_2 \times C_{12}$.

3.- **Problema 3:** Sea $G \cong S_5$ grupo de permutaciones.

i.- Encuentre un 5-Sylow de G. Demuestre que no es normal.

ii.- Demuestre que existen 6 subgrupos de orden 5 en G.

Desarrollo:

i.- Observe primero que $|G| = 2^3 \cdot 5 \cdot 3$. Luego H es un 5-Sylow sí y solamente sí tiene orden 5. Considere el subgrupo $H = \langle(12345)\rangle$, es decir $H = \{id, (12345), (24135), (31425), (43215)\}$ de orden 5. Recordemos que $\sigma(12345)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))$. Luego $H \lhd G$ si contiene a todas las permutaciones de largo 5. Pero $(42315) \notin H$. Luego H no es normal en G.

ii.- Observe que $n_5 \in \{1, 3, 6, 12, 24, 2, 4, 8\}$. Pero $n_5 \cong 1(5)$. Luego $n_5 \in \{1, 6\}$. Luego si $n_5 = 1$ entonces $H \lhd G$, lo que claramente es falso. Luego $n_5 = 6$. Por ello existen 6 subgrupos de orden 5 en G.

4.- **Problema 4:** Sea $G = Q_8$. Encuentre una cadena de subgrupos de G tales que :

$$N_0 = \{e\} \lhd N_1 \lhd \cdots N_t = G,$$

y $N_i/N_{i-1} \cong C_2$, para todo $i \in \{1, \cdots, t\}$.

Desarrollo: Recordemos que $N_3 = Q_8 = \langle i, j : j^4 = i^4\, ij = j^3 i\rangle$, en donde identificamos $i^2 = j^2 = -1$. Sea $N_3 = \langle i\rangle = \{-1, -i, i, 1\}$. Observe que $jij^{-1} = -jij = j^2 i = -i$. Luego $N_2 \lhd G$ con cociente $|G/N_2| = 2$, luego $G/N_2 \cong C_2$. Considere entonces $N_1 = \langle -1\rangle = \{1, -1\}$. Como $N_1 = Z(G)$ tenemos que $N_1 \lhd N_2$ con $|N_2/N_1| = 2$. Luego $N_2/N_2 \cong C_2$. Por último $N_0 = \{1\}$. Observe que salvo isomorfía la cadena que damos es:

$$\{1\} \lhd C_2 \lhd C_4 \lhd Q_8.$$

Observe tambien que como N_2 debe tener 4 elementos tenemos que $\pm i, \pm j$ o $\pm k = \pm ij$ es un elemento de N_2. Luego $N_2 = \langle i\rangle, \langle j\rangle$ o $\langle k\rangle$ y el único subgrupo normal de indice 2 de N_2 es $N_1 = \langle -1\rangle$, pues dicho grupo debe tener 2 elementos. En síntesis, salvo isomorfismo, la cadena anterior es única.

1.- **Ejercicio:** Replique esto para $G = D_{16}$.

Ayudantía 8: En esta ayudantía presentaremos técnicas más abanzadas para estudiar grupos finitos, haciendo uno de los teoremas de Sylow.

1.- **Problema 1:** Demuestra que todo grupo de orden 24 no es simple.

Demostración: En este caso $n_3|8$ y $n_2|3$. Además para todo primo $n_p \equiv 1(p)$. Por lo tanto $n_3 \in \{1,4\}$ y $n_2 \in \{1,3\}$.

Sabemos que si $n_3 = 1$ o $n_4 = 1$ entonces G tiene un p-Sylow normal, para $p = 3$ o $p = 2$ respectivamente. Supongamos entonces que $n_3 = 4$ y $n_2 = 3$. Sabemos que G actúa por conjugación transitivamente sobre los 3-Sylow. Luego tenemos un homomorfismo $\psi : G \to Biy(\{3 - Sylow\}) \cong S_4$, donde $\psi(g)(H) = gHg^{-1}$. En este caso se tiene que $\ker(\psi) = \{g \in G : gHg^{-1} = H, \forall H\, 3 - Sylow\}$. Observe que no existen 3-Sylow normales, pues todos los 3-Sylow son conjugados y si hubiera alguno normal, entonces habria sólo uno. Por lo tanto $\ker(\psi) \neq G$. Luego si G es simple se tiene que $\ker(G) = \{e\}$. Luego $G \cong S_4$, pues tienen igual orden y existe un morfismo inyectivo. Pero S_4 no es simple ya que $A_4 \lhd S_4$. Esto concluye lo pedido.

2.- **Problema 2:** Pruebe que todo grupo G de orden 380 tiene un subgrupo normal de orden 95

Desarrollo: Observe que $|G| = 4 \cdot 5 \cdot 19$. En este caso utilizando las relaciones de congruencia se tiene que $n_5 \in \{1, 76\}$ y $n_{19} \in \{1, 20\}$. Si $n_5 = 76$ y $n_{19} = 20$ se tiene que en G existen $20 \cdot 18$ elementos de orden 19, $4 \cdot 76$ elementos de orden 4 y un elemento de orden 1. Esto se debe a que los 5-Sylow y los 19-Sylow distintos se intersectan trivialmente. Luego $|G| \geq 665 > |G|$, lo que nos lleva a una contradicción. Por lo tanto $n_5 = 1$ o $n_{19} = 1$, esto quiere decir que existe un 5-Sylow $P \lhd G$ o bien un 19-Sylow $Q \lhd G$.

Si $P \lhd G$, entonces G/P es un grupo de orden $4 \cdot 19$. En este grupo $n_1 9|4$ y $n_{19} \equiv 1(19)$. Por lo tanto $n_{19} = 1$, luego existe un 19-Sylow $S \lhd G/P$. Por lo tanto $\pi_P^{-1}(S) \lhd G$ con $|\pi_P^{-1}(S)| = 95$.

Por otro lado si $Q \lhd G$, entonces G/Q es un grupo de orden $4 \cdot 5$. En este grupo $n_5|4$ y $n_5 \equiv 1(5)$. Por lo tanto $n_5 = 1$, luego existe un 5-Sylow $S \lhd G/Q$. Por lo tanto $\pi_Q^{-1}(S) \lhd G$ con $|\pi_Q^{-1}(S)| = 95$. En cualquier caso se concluye lo pedido.

3.- **Problema 3:** Sea G grupo finito de orden 231. Demuestre que G tiene un únido 11-Sylow y que este está contenido en el centro de G.

Desarrollo: Observe que $|G| = 5 \cdot 7 \cdot 11$. Luego $n_7|5 \cdot 11$ y $n_7 \equiv 1(7)$. Por lo tanto $n_7 = 1$. Luego existe un 7-Sylow $H \lhd G$.

Observe que el homomorfismo $\phi : G \to Aut(H)$ definido por $\phi(g)(h) = ghg^{-1}$ tiene por núcleo $\ker(\phi) = \{g \in G : gh = hg, \forall h \in H\}$. Este morfismo está bien definido pues $H \lhd G$. Recordemos que si $|H| = 7$ entoncces $H \cong C_7$ y luego $Aut(H) \cong C_6$. Por lo tanto $|G/\ker(\phi)|6$. Luego si $|G/\ker(\phi)| \in \{2, 3, 6\}$ entonces $2, 3||G|$, lo cual es contradictorio. Por lo tanto $|G/\ker(\phi)| = 1$. Luego $G = \ker(\phi)$, es decir para todo $g \in G, h \in H$ se tiene que $hg = hg$. Esto prueba que $H \subset Z(G)$.

Ayudantía 9: En esta ayudantía estudiaremos las consecuencias teóricas que tienen los teoremas de Sylow.

1.- **Problema 1:** Sea $p \neq 2$ primo. Si G es un grupo de orden $2p$ pruebe que $G \cong C_{2p}$ o bien $G \cong D_{2p}$.

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

Si $n_2 = 1$, entonces $T \triangleleft G$. Además $T \cap S = \{1\}$, pues si $x \in T \cap S$ entonces $|x||2, p$, luego $|x| = 1$. Por lo tanto $G \cong T \times S \cong C_p \times C_2 \cong C_{2p}$.

Si $n_2 = p$, entonces existen p 2-subgrupos de Sylow de G. Entonces usamos el procedimiento visto en la ayudant"ia anterior. En efecto, 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 $bab^{-1} = a^{-1}$, por lo tanto:

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

1.- **Ejercicio:** Si $p \equiv 1(4)$ encuentre los grupos G de orden $4p$.

2.- **Problema 2:** *Argumento de Fratini.* Sea G grupo y $H \leq G$. Si P es un p-subgrupo de Sylow de H entonces $G = N_G(P)H$.

Demostración: Sabemos que siempre $G \supseteq N_G(P)H$. Por lo tanto debemos demostrar la contensión contraria. Observe que si P es un p-Sylow de H, entonces $\{hPh^{-1} : h \in H\} = Syl(H)$. Sea $g \in G$, como $H \triangleleft G$ tenemos que $gPg^{-1} \subseteq H$. Luego como $|gPg^{-1}| = |P|$ tenemos que $gPg^{-1} \in Syl(H)$. Luego $gPg^{-1} = hPh^{-1}$, para cierto $h \in H$. Es decir $gh^{-1} \in N_G(P)$. Luego $g \in N_G(P)H$. Concluimos que $G = N_G(P)H$.

3.- **Problema 3:** Sea $P \in Syl_p(H)$ y $H \leq K$.

i.- Si $P \triangleleft H$ y $H \triangleleft K$ entonces $P \triangleleft K$.

ii.- Deduzca que si $P \in Syl_p(G)$ entonces $H = N_G(P)$ cumple con $N_G(H) = H$.

Desarrollo:

i.- Sabemos que $P \triangleleft H$ sí y solamente sí P es el único p-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-Sylow de H. Luego $gPg^{-1} = P$. Es decir $P \triangleleft K$.

ii.- Si $P \in Syl_p(G)$, entonces $P \triangleleft N_G(P) = H$ por definición de $N_G(P)$. Luego como $H \triangleleft N_G(H) = K$ 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 $N_G(N_G(P)) = N_G(P)$.

4.- **Problema 4:** Sea G un p-grupo. Demuestre que si $H \subsetneq G$ es un subgrupo propio de G, entonces $H \subsetneq N_G(H)$.

Demostración: Pendiente.

Ayudantía 10: En esta ayudantía estudiaremos un tipo especial de grupos, llamados grupos solubles.

1.- **Problema 1:** Sea G grupo abeliano. Es un hecho que $G \cong C_{n_1} \times \cdots \times C_{n_t}$. Demustre que G es un grupo soluble.

Demostración: Considere $H_i = C_{n_1} \times \cdots \times C_{n_i}$ subgrupo de G. Como G es abeliano $H_i \triangleleft G$, en particular $H_i \triangleleft H_{i+1}$. Además $H_{i+1}/H_i \cong C_{n_{i+1}}$ grupo cíclico. Esto demuestra que G es soluble. Así todo grupo abeliano es soluble.

2.- **Problema 2:** Sea $p \neq 2$ primo. Sea $G = D_{2p}$ grupo dihedral. Demuestre que G es soluble.

Demostración: Sabemos que $G = \langle a, b : a^p = b^2 = 1, ba = a^{-1}b\rangle$. Considere $H = \langle a\rangle$. Entonces $[G : H] = 2$. Luego, por lo demostrado en las primeras ayudantías, $H \triangleleft G$. Además $|G/H| = 2$, por lo tanto $G/H \cong C_2$. Por otro lado $H/\{1\} \cong H \cong C_p$. Si utilizamos la cadena de subgrupos:

$$\{1\} \triangleleft H \triangleleft G,$$

con cocientes $G/H \cong C_2$, $H \cong C_p$, entonces concluimos que G es soluble.

2.- **Ejercicio:** Demuestre que D_{2n} es soluble para cualquier $n \in \mathbb{N}$.

3.- **Problema 3:** Sea G grupo.
i.- Si $|G| = 15$, pruebe que G es soluble.
ii.- Demuestre que S_4 es soluble.

Desarrollo:
i.- Sabemos que si $|G| = 15$ entonces, por lo demostrado en las ayudantías previas vía teoremas de Sylow, tenemos que $G \cong C_{15}$. Luego $\{e\} \triangleleft G$ es una cadena que hace a G soluble.

ii.- Sabemos que siempre $A_4 \triangleleft S_4$. Ahora escribamos A_4 por extensión. En efecto, $A_4 = \{id, (123), (132), (124), (142), (124), (243), (12)(34), (14)(32)\}$. Entonces $K_4 = \{id, (12)(34), (13)(24), (14)(32)\} \cong C_2 \times C_2$ es un subgrupo normal de S_4, pues para cualquier $\sigma \in S_4$ tenemos que $\sigma(ij)(kl)\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l)) \in K_4$, para cualquiera i, j, k, l. Por último consideremos $\{id, (12)(34)\} \cong C_2$ subgrupo normal de K_4, pues K_4 es abeliano. Así tenemos:

$$\{id\} \triangleleft C_2 \triangleleft K_4 \triangleleft A_4 \triangleleft S_4,$$

donde $K_4/C_2 \cong C_2$, $A_4/K_4 \cong C_3$ y $S_4/A_4 \cong C_2$. Por lo tanto S_4 es un grupo soluble.

3.- **Ejercicio:** Pruebe que S_3 es soluble.

4.- **Problema 4:** Pruebe que si H, K son grupos solubles entonces $G = H \times K$ es soluble.

Demostración: Escribamos las hipótesis. Sabemos que existe una cadena de subgrupos de H:

$$\{e\} = H_0 \triangleleft H_1 \triangleleft \cdots \triangleleft H_n = H,$$

donde H_i/H_{i-1} es cíclico para todos i y además existe una cadena de subgrupos de K:

$$\{e\} = K_0 \triangleleft K_1 \triangleleft \cdots \triangleleft K_t = K,$$

tal que K_i/K_{i-1} es cíclico para cualquiera i. Recordemos que $I \times J \triangleleft A \times B$ sí y solamente si $(a,b)(i,j)(a^{-1},b^{-1}) = (aia^{-1}, ajb^{-1}) \in I \times J$, para cualquier $a \in A$, $b \in B$, $i \in I$, $j \in J$. Luego lo anteior sucede sí y solamente sí $I \triangleleft A$ y $J \triangleleft B$. Aplicando esto a nuestro caso, obtenemos una cadena de subgrupos de G:

$$H_0 \times K_0 \triangleleft H_1 \times K_0 \triangleleft \cdots \triangleleft H_n \times K_0 \triangleleft H_n \times K_1 \triangleleft \cdots H_n \times K_t,$$

donde $(H_0 \times K_i)/(H_0 \times H_{i-1}) \cong H_i/H_{i-1}$ cíclico y $(H_n \times K_i)/(H_n \times K_{i-1}) \cong K_i/K_{i-1}$ cíclico. Por lo tanto $H \times K$ es soluble.

5.- **Problema 5:** Sea $\phi : G \to G'$ homomorfismo de grupos.

i.- Demuestre que si G es soluble, entonces $\phi(G)$ es soluble.

ii.- Pruebe que si $G = H \times K$ es soluble, entonces H y K son grupos solubles.

Desarollo:

i.- Sabemos que existe una cadena de subgrupos de G:

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_t = G,$$

donde G_i/G_{i-1} es un grupo cíclico. Considere entonces la cadena de subgrupos de la imagen de G:

$$\{e\} = \phi(G_0) \subseteq \phi(G_1) \subseteq \cdots \subseteq \phi(G).$$

Observe que si $x = \phi(g_i) \in \phi(G_i)$ e $y = \phi(g_{i+1}) \in \phi(G_{i+1})$, entonces $yxy^{-1} = \phi(g_{i+1}g_ig_{i+1}^{-1}) \in \phi(G_i)$. Luego $\phi(G_i) \triangleleft \phi(G_{i+1})$.

Considere el homomorfismo $\psi : G_i \to \phi(G_i)/\phi(G_{i-1})$, definido por $\psi(g) = \overline{\phi(g)}$. Entonces claramente ψ es sobreyectiva, con núcleo $\ker(\psi) = \{g \in G_i : \phi(g) \in \phi(G_{i-1})\} = G_{i-1}(\ker(\phi) \cap G_{i-1})$. Por lo tanto $\phi(G_i)/\phi(G_{i-1}) \cong G_i/G_{i-1}(\ker(\phi) \cap G_{i-1}) \hookrightarrow G_i/G_{i-1}$ cíclico. Por lo tanto $\phi(G_i)/\phi(G_{i-1}$ es cíclico. Esto demuestra que $\phi(G)$ es soluble.

ii.- Considere $\pi_H : G \to H$ proyección en la primera coordenada. Esta función es un homomorfismo sobreyectivo. Por lo tanto, por [i], H es soluble. Análogamente, tomando la imagen por π_K de G, obtenemos que K es soluble.

Ayudantía 11: En esta ayudantía estudiaremos un tipo especial de producto, este es el producto semidirecto de grupos.

1.- **Problema 1:** Para $n > 2$ considere $\phi : C_2 \to Aut\,(\mathbb{Z}/n\mathbb{Z})$ homomorfismo definido por $\phi(a)(x) = (-1)^a x$. Demuestre que $D_{2n} \cong \mathbb{Z}/n\mathbb{Z} \ltimes_\phi C_2$.

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 $bab^{-1} = a^{-1} \in N$. Observe que $N \cong C_n$. Considere $H = \langle b\rangle \cong C_2$. Observe que $b \notin N$. Luego $|N \cap H| = 1$, 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 $D_{2n} = HN$.

Lemma 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 $g = hn$. Además $G \cong H \rtimes_\phi N$, para $\phi(n)(h) = hnh^{-1}$.*

Proof. Por lo dicho en el lo previo al problema (es completamente general) tenemos que $G = HN$. Luego para cualquier $g \in G$ existen $h \in Hn \in N$ tales que $g = hn$. Si existe otro par (h_1, n_1) tal que $g = hn = h_1n_1$ entonces $h^{-1}h_1 = n_1n^{-1} \in H \cap N = \{1\}$. Luego $h = h_1$ y $n = n_1$.

Considere la función $f : G \to H \rtimes_\phi N$ definida por $f(g) = (h, n)$. Está función esta bien definida por lo dicho anteriormente. Además es claramente sobreyectiva. Demostremos que es homomorfismo de grupos. Observe que $f(g_1)f(g_2) = (h_1, n_1)(h_2, n_2) = (h_1\phi(n_1)(h_2), n_1n_2)$. Así $f(g_1)f(g_2) = (h_1n_1h_2n_1^{-1}, n_1n_2)$. Por otro lado se cumple que $g_1g_2 = h_1n_1h_2n_2 = h_1(n_1h_2n_1^{-1})(n_1n_2)$. Luego $f(g_1g_2) = (h_1n_1h_2n_1^{-1}, n_1n_2) = f(g_1)f(g_2)$. Por ellos f es homomorfismo de grupos y como $f(g) = (1, 1)$ implica que $g = 1$ tenemos que f es isomorfismo de grupos. Luego $G \cong H \rtimes_\phi N$, para $\phi(n)(h) = hnh^{-1}$. □

En nuestro caso tenemos que $D_{2n} \cong C_2 \rtimes_\phi C_n$, para $\phi(a)(b) = bab^{-1} = a^{-1}$.

2.- **Problema 2:** Sean G_1, G_2 grupos y $\phi : G_1 \to Aut(G_2)$ homomorfismo de grupos.

i.- Pruebe que $G_2 \times \{e\} \triangleleft G_2 \rtimes_\phi G_1$.

ii.- Demuestre que $\{e\} \times G_1 \triangleleft G_2 \rtimes_\phi G_1$ sí y solamente sí $\phi(a) = id$, para todo $a \in G_1$.

Desarrollo:

i.- Sea $(g_2, e) \in G_2 \times \{e\}$. Considere $(h_2, h_1) \in G_2 \rtimes_\phi G_1$ elemento cualquiera. Entonces $(h_2, h_1)(g_2, e)(h_2, h_1)^{-1} = (h_2, h_1)(g_2, e)(\phi(h_1^{-1})(h_2^{-1}), h_1^{-1})$. Lo que es igual a $(h_1\phi(h_1)(g_2), h_1)(\phi(h_1^{-1})(h_2^{-1}), h_1^{-1}) = (*, e) \in G_2 \times \{e\}$.

ii.- Supongamos que $\phi(a_1) = id_{G_2}$ para cualquier $a_1 \in G_1$. Entonces

$$(a_2, a_1)(e, g_1)(a_2, a_1)^{-1} = (a_2, a_1)(e, g_1)(\phi(a_1^{-1})(a_2^{-1}), a_1^{-1}).$$

Multiplicando los primeros términos obtenemos que lo anterior es igual a

$$(a_1\phi(a_1)(e_2), a_1g_1)(\phi(a_1^{-1})(a_2^{-1}), a_1^{-1}) = (a_2e, a_1g_1)(a_2^{-1}, a_1^{-1}).$$

Luego $(a_2, a_1)(e, g_1)(a_2, a_1)^{-1} = (e, a_1g_1a_1^{-1})$. Por ello $\{e\} \times G_1 \triangleleft G_2 \rtimes_\phi G_1$.

Inversamente si $\{e\} \times G_1 \triangleleft G_2 \rtimes_\phi G_1$ entonces $(h_2, h_1)(g_2, e) = (e, t_1)(h_2, h_1)$, para cierto $t_1 \in G_1$. Es decir $(a_2\phi(g_1)(e), a_1g_1) = (e\phi(a_1)(a_2), t_1a_1)$. Por lo

tanto, si igualamos la segunda componente obtenemos que $a_2 = \phi(a_1)(a_2)$. Luego $\phi(a_1) = id$, para cualquier $a_1 \in G_1$.

3.- **Problema 3:** Encuentre todos los grupos de orden 21 salvo isomorfía, escritos como producto directo y semidirecto de grupos cíclicos.

Desarrollo: Por lo demostrado en las ayudantías previas, sabemos que existen dos grupos de orden 21 salvo isomorfía. Estos son $G = C_{21}$ y $G = \langle a, b : a^3 = b^7 = 1, aba^{-1} = b^2 \rangle$. Si $G \cong C_{21}$, entonces el problema queda solucionado. Si $G = \langle a, b : a^3 = b^7 = 1, aba^{-1} = b^2 \rangle$, entonces por lo destrado en las ayudantiás previas, existe un 7-Sylow $S \triangleleft G$. Además existe un 3-Sylow T, tal que $G = |T||S|$ y $T \cap S = \{1\}$. Luego por lo visto en el lema 1, tenemos que $G \cong T \rtimes_\phi S$, para $\phi(s)(t) = tst^{-1}$, para cualquier $t \in T$, $s \in S$. Luego $G \cong C_3 \rtimes_\phi C_7$, para $\phi(b)(a) = aba^{-1} = b^2$, donde $C_3 \cong \langle a \rangle$ y $C_7 = \langle b \rangle$.

3.- **Ejercicio:** Pruebe que $C_3 \ltimes_\phi C_2$ es soluble, para cierto ϕ homomorfismo.

4.- **Problema 4:** Demuestre que para cualquier homomorfismo $\phi : C_{13} \to Aut(C_3)$, se tiene que $C_{13} \ltimes_\phi C_3$ es soluble.

Demostración: Una forma de atacar este problema es notar que problema es notando que $|C_{13} \ltimes_\phi C_3| = |C_{13}||C_3| = 39$. Luego por lo visto en las ayudantías previas tenemos dos casos.

Primero si $G \cong C_{39}$, entonces G es abeliano. Por lo tanto soluble.

Por otro lado, si $G = \langle a, b : a^3 = b^{13} = 1, aba^{-1} = b^2 \rangle$, entonces por lo destrado en las ayudantiás previas, existe un 13-Sylow $S \triangleleft G$. Entonces $|G/S| = 3$ y $S \cong C_{13}$. Luego $G/S \cong C_3$. Por lo tanto la cadena $\{1\} \triangleleft S \triangleleft G$ convierte a G en un grupo soluble.

Ayudantía 12: En esta ayudantía estudiaremos un tipo especial de grupos, llamados grupos nilpotentes.

1.- **Problema 1:** Pruebe que $G^i/G^{i+1} \subseteq Z(G/G^{i+1})$, para cualquier $i \in \mathbb{N}$.

Demostración: Recordemos que $G^{i+1} = [G^i, G] \subset G^i$, con $G^0 = G$. Entonces $G^i/G^{i+1} \subset G/G^{i+1}$. Observe que $G^{i+1} \triangleleft G$ pues $x(g_i g g_i^{-1} g^{-1})x^{-1} = (xg_i x^{-1})(xgx^{-1})(xg_1 x^{-1})^{-1}(xgx^{-1})^{-1}$, para $g_i \in G^{i+1}$ y $g \in G$. Concluimos por inducción. Tomamos $\overline{x} \in G^i/G^{i+1}$ y $\overline{z} \in G/G^{i+1}$. Debemos probar que $\overline{xzx^{-1}z^{-1}} = \overline{1}$, es decir $xzx^{-1}z^{-1} \in G^{i+1}$. Esto se cumple por la definición de G^{i+1}. Esto además prueba que $G^i/G^{i+1} = Z(G/G^{i+1})$.

2.- **Problema 2:** Demuestre que $G = S_3$ no es nilpotente. Concluya que existen grupos solubles no nilpotentes.

Demostración: Observe que $G^0 = S_3$ y $G^1 = [S_3, G_3] \triangleleft G_3$, pero siempre se cumple que $(12)(13)(12)(13) = (213) \in G^1$. Por lo tanto $G^1 = A_3$ o $G^1 = S_3$. Observe que si $x \in A_3$ entonces $(yxy^{-1})x^{-1} \in A_3$, por la normalidad de A_3 en S_3. Por otro lado si $x, y \in S_3 - A_3$ entonces $yxy^{-1}x^{-1} \in A_3$, esto se puede probar en todos lo casos. Luego $G^1 = A_3$. Ahora bien $[S_3, A_3] \subseteq A_3$ pero $(123)(12)(132)(12) = (321) \in [G_3, A_3]$. Por lo tanto $A_3 = [S_3, A_3]$. Luego $G^n = G^1 = A_3$, para todo $n \geq 1$. Luego S_3 no es soluble. Esto demuestra que hay grupos solubles no nilpotentes.

3.- **Problema 3:** Sea G grupo y H subgrupo cualquiera de G.
i.- Si G es nilpotente, pruebe que H es nilpotente.
ii.- Pruebe que S_n no es nilpotente para $n \geq 3$.

Desarrollo:
i.- Demostremos por inducción que $H^i \subseteq G^i$, para cualquier $i \in \mathbb{N}$. Observe que para $i = 0$ es cierto pues $H \subseteq G$. Supongamos que $H^i \subseteq G^i$ para cierto $i \in \mathbb{N}$. Entonces $H^{i+1} = [H, H^i] \subseteq [G, G^i] = G^{i+1}$. Esto concluye lo deseado. Luego si $G^n = \{1\}$, para cierto $n \in \mathbb{N}$, entonces $H^n = \{1\}$. Por ello H es nilpotente.

ii.- Si S_n fuera nilpotente para $n \geq 3$, entonces $S_3 \subseteq S_n$ es nilpotente. Esto es contradictorio. Por lo tanto S_n no es nilpotente para $n \geq 3$.

4.- **Problema 4:** Encuentre los valores de $n \in \mathbb{N}$ tales que $G = D_{2n}$ es nilpotente.

Demostración: Recordemos que $G_{2n} = \langle x, y : x^n = y^2 = 1, yxy^{-1} = x^{-1} \rangle$. Analicemos G^1. Observe que $[x^i, y] = x^i(yx^{-i}y^{-1}) = x^i(x^{-1})^i = x^{2i}$ y $[y, x^i] = (yx^i y^{-1})x^{-i} = x^{-2i}$. Por lo tanto $G^1 = (x^2)$. Probemos por inducción que $G^i = (x^{2^i})$. Para $n = 1$ ya fue probado. Supongamoslo cierto para $n \in \mathbb{N}$. Entonces $[G^n, G]$ está generado por $[x^{2^n i}, x] = 1$, $[x^{2^n i}, y] = x^{2^{n+1} i}$ y $[y, x^{2^n i}] = x^{2^{n+1} i}$. Esto se debe a los cálculos ya hechos. Luego $G^i = (x^{2^i})$ para cualquier $i \in \mathbb{N}$. Si $G^i = \{1\}$, para cierto $i \in \mathbb{N}$, entonces $n | 2^i$. Por lo tanto $n = 2^j$, para cierto $j \in \mathbb{N}$.

4.- **Ejercicio:** Demuestre que D_8, D_{16} son grupos nilpotentes usando serie de conmutadores y serie central.

5.- **Ejercicio:** Pruebe, usando serie central, que todo grupo de orden p^3 es nilpotente.

Ayudantía 13: En esta ayudantía estudiaremos grupos definidos por generadores y relaciones.

1.- **Problema 1:** Considere $G = \langle x, y : x^p = y^p = 1, xy = yx\rangle$. Demuestre que $G \cong C_p \times C_p$.

Demostración: Considere la función $\phi : C_p \times C_p \to G$ tal que $\phi(\sigma, 1) = x, \phi(1, \tau) = y$, para σ, τ generadores fijos de C_p. La extendemos multiplicativamente. Observe que esta función está bien definida pues $(\sigma, 1)^p = (1, \tau)^p = (1, 1)$ y $(\sigma, 1)(1, \tau) = (\sigma, \tau) = (1, \tau)(\sigma, 1)$. Claramente la función es sobreyectiva. Por otro lado, como $C_p \times C_p$ es abeliano, $\ker(\phi) = \{(\sigma^i, \tau^j) : x^i y^j = 1\}$, es decir $\ker(\phi) = \{(\sigma^i, \tau^j) : x^i = y^{-j}\} = \{(1, 1)\}$, puesto que si no, el grupo G estará dado en un generador. Luego $G \cong C_p \times C_p$.

2.- **Problema 2:** Se define el grupo dihedral infinito por $D_\infty = \langle a, b : a^2 = 1, aba^{-1} = b^{-1}\rangle$.

i.- Demuestre que $G = \langle d, c : d^2 = c^2 = 1\rangle$ es isomorfo D_∞.

ii.- Pruebe que todo grupo dihedral finito D_{2n} es un cociente de D_∞.

Demostración:

1.- Considere el homomorfismo $\phi : D_\infty \to G$ definido en los generadores por $\phi(a) = c$, $\phi(ab) = d$. Es decir $\phi(b) = c^{-1}d$. Este morfismo está bien definido pues $c^2 = 1$ y $c(c^{-1}d)c^{-1} = dc^{-1} = d^{-1}c = (c^{-1}d)^{-1}$. El morfismo en cuestión es la extensión multiplicativa de la función dada sobre los generadores. Claramente la función es sobreyectiva.

Por otro lado considere la relación inversa de ϕ, definida sobre los generadores de G por $\chi(c) = a$, $\chi(d) = ab$, es decir $\chi(c^{-1}d) = b$. Observe que esta función está bien definida pues $a^2 = 1$ y $(ab)^2 = abab = b^{-1}b = 1$. Claramente esta función es también sobreyectiva. Luego ϕ es un homomorfismo biyectivo.

ii.- Considere el morfismo $\phi : D_\infty \to D_{2n}$ definido por $\phi(a) = a'$, $\phi(b) = b'$, para $D_{2n} = \langle a', b' : a'^2 = 1, b'^n = 1, a'b'a'^{-1} = b'^{-1}\rangle$. Esta función está bien definida pues $a^2 = 1$ y $a'^2 = 1$, además $aba^{-1} = b^{-1}$ y $a'b'a'^{-1} = b'^{-1}$. Observe que claramente la función ϕ es sobreyectiva. Luego $D_\infty / \ker(\phi) \cong D_{2n}$.

3.- **Problema 3:** Sea $G = \langle a, b, c : a^2 = b^2 = c^2 = 1, aba = bab, bcb = cbc, ac = ca\rangle$. Pruebe que G tiene a lo menos 24 elementos.

Demostración: Considere $a = (12)$, $b = (23)$, $c = (34) \in S_4$. Estos elementos satisfacen las relaciones que cumplen los generadores de G. Luego S_4 es un cociente de G. Por lo tanto G tiene a lo menos 24 elementos. De hecho, si G es finito entonces $|G|$ es un múltiplo de 24.

4.- **Problema 4:** Sea $G = \langle a, b, c : a^3b^5c^7 = e\rangle$. Pruebe que G tiene infinitos elementos.

Demostración: Observe que $G = \langle a, b, c : a^3b^5c^7 = e\rangle$ se incrusta en el grupo abeliano libre con los mismos generadores y relaciones. Luego si vemos el grupo $G_{ab} = \langle a, b, c : a^3b^5c^7 = e, ab = ba, bc = bc, ac = ca\rangle$ aditivamente, entonces $G_{ab} = \langle a, b, c : 3a + 5b + 7c = 0\rangle \cong \mathbb{Z}^3/((3, 5, 7))$. Luego contar elementos en G_{ab} es lo mismo que contar tuplas de enteros que

tengan por diferencia un múltiplo de $(3, 5, 7)$. Podemos poner por ejemplos las tuplas $(n, 0, 0)$ que son infinitas y distintas en el cociente. Por lo tanto hay infinitos elementos en G_{ab}. Luego hay infinitos elementos en G.

2. Anillos:

Ayudantía 14: En esta ayudantía estudiaremos el anillo de matrices y la descomposición de anillos vía idempotentes centrales.

1.- **Problema 1:** Sea $A = \mathbb{C}[x]/(x^2+1)$.

i.- Demustre que $A \cong \mathbb{C} \times \mathbb{C}$.

ii.- Encuentre idempotentes centrales en A que induzcan la descomposición mencionada en [i].

Desarrollo:

i.- Recordemos que en $\mathbb{C}$ se tiene que $x^2+1 = (x+i)(x-i)$, donde $1 = \frac{(x+i)-(x-i)}{2i}$. Por lo tanto $(x+i), (x-i)$ son relativamente primos en $\mathbb{C}[x]$. Luego como $A = \mathbb{C}[x]/(x^2+1) \cong \mathbb{C}[x]/(x+i)(x-i)$, por teorema chino de los restos $A \cong \mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i)$.

Pero para cualquier anillo B se tiene que $\phi : B[x] \to B$ definida por $B(p(x)) = p(b)$ es un homomorfismo sobreyctivo cuyo nucleo es $\ker(\phi) = \{p(x) : p(b) = 0\}$. Observe que si $p(b) = 0$, por algoritmo de la división (se puede hacer pues $x-b$ tiene primer coeficiente invertible) se tiene que $p(x) = (x-b)q(x) + r$, pero como $p(b) = r = 0$ tenemos que $p(x) = (x-b)q(x)$. Luego $\ker(\phi) = (x-b)$. Por lo tanto $B[x]/(x-b) \cong B$.

Concluimos que $A \cong \mathbb{C} \times \mathbb{C}$.

ii.- Sabemos que $A \cong \mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i) \cong \mathbb{C} \times \mathbb{C}$. Debemos encontrar una preimagen de $(1,0)$ en A. Pero su preimagen en $\mathbb{C}[x]/(x-i) \times \mathbb{C}[x]/(x+i)$ es $(\overline{1}, 0)$. Luego necesitamos un polinomio $p(x) \in \mathbb{C}[x]$ tal que $p(x) \equiv 1(x-i)$ y $p(x) \equiv 0(x+i)$. Como queremos ver su imagen en A podemos suponer que $p(x) = ax + b$ (aplicamos algoritmo de la división y nos quedamos con su resto). Por lo tanto necesitamos que $ai + b = 1$, $-ai + b = 0$. Por ello $p(x) = \frac{x+i}{2i}$ cumple con lo pedido.

Conclumos que $\overline{\frac{1}{2i}(x+i)}$ y $\overline{\frac{1}{2i}(i-x)}$ son idempotentes centrales en A.

2.- **Problema 2:** Sea $f : A \to A$ homomorfismo de anillos tal que $f^2 = f$.

i.- Pruebe que $A = Im(f) \oplus \ker(f)$.

ii.- Demuestre que $\mathbb{Z}/6\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Demostración:

i.- Partamos considerando un elemento cualquiera $a \in A$. Entonces $f(a) \in Im(f)$. Observe que $a - f(a)$ cumple con $f(a - f(a)) = f(a) - f^2(a) = 0$. Por lo tanto $a \in \ker(f)$. Luego $A = Im(f) + \ker(f)$.

Por otro lado si consideramos $a \in Im(f) \cap \ker(f)$ entonces $a = f(b)$, cierto $b \in A$ y además $0 = f(a) = f^2(b) = f(b)$. Por lo tanto $a = f(b) = 0$. Concluimos que $A = Im(f) \oplus \ker(f)$.

ii.- Sea $A = \mathbb{Z}/6\mathbb{Z}$. Considere el siguiente homomorfismo. $f : A \to A$ tal que $f(\overline{x}) = \overline{3x}$. Entonces $f^2(\overline{x}) = \overline{9x} = \overline{3x}$. Por lo tanto $f^2 = f$. Luego por [i] se tiene que $A = Im(f) \times \ker(f)$. Pero $Im(f) = \{\overline{3}, \overline{0}\} \cong \mathbb{Z}/2\mathbb{Z}$. Además $\ker(f) = \{\overline{2}, \overline{0}, \overline{4}\} \cong \mathbb{Z}/3\mathbb{Z}$. Por lo tanto $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

2.- **Ejercicio:** Pruebe que $A = Im(f) \oplus \ker(f)$ es equivalente a que $f : A \to A$ cumpla con $f^2 = f$. Pruebe además que en este caso f inyectiva sí y solamente sí f sobreyectiva.

2.- **Observación:** Observe que los endomorfismos idempotentes, es decir los homomorfimos $f : A \to A$ inducen una descomposición de A y por ello tienen asociados pares de elementos idempotentes centrales $(e, 1-e)$. Por otro lado todo elemento $e \in A$ idempotente central induce una homomorfismo $f : A \to A$ definido por $f(a) = ea$. A posteriori hablar de endomorfismo idempotentes, descomposicón de anillos en producto y elementos idempotentes centrales es "lo mismo".

3.- **Problema 3:** Sea $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} : a, b \in \mathbb{R} \right\}$ subconjunto de $A = \mathbb{M}_2(\mathbb{R})$.

i.- Pruebe que I es un ideal izquierdo de A, pero no bilátero.

ii.- Encuentre los ideales izquierdos J de A tales que $\{0\} \subset J \subset I$.

Desarrollo:

i.- Claramente I es un subgrupo aditivo de A. Observe que $\begin{pmatrix} x & z \\ y & w \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} ax + zb & 0 \\ ay + bw & 0 \end{pmatrix} \in I$. Por ello I es ideal izquierdo de A.

Por otro lado $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \begin{pmatrix} x & z \\ y & w \end{pmatrix} = \begin{pmatrix} ax & az \\ bx & bz \end{pmatrix}$. Por lo tanto para $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \in I$ tenemos que $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \notin I$. Por ello I no es ideal bilátero de A.

ii.- Considere $J \neq \{0\}$ ideal izquierdo de A contenido en I. Entonces existe $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in J$, con a o $b \neq 0$. Sín perdida de generalidad $a \neq 0$. Entonces $\begin{pmatrix} a^{-1} & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$ y $\begin{pmatrix} 0 & 0 \\ a^{-1} & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}$. Así $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \in I$. Luego $I = J$. Por lo tanto los unicos ideales izquierdos que complen lo pedido son $\{0\}$ e I.

4.- **Problema 4:** Sea $A = \mathbb{M}_2(K)$.

i.- Pruebe que si $K = \mathbb{R}$ entonces en A existen infinitas soluciones a la ecuación $x^2 + 1 = 0$.

ii.- Encuentre las soluciones de la ecuación $x^2 = x$ en A, para $K = \mathbb{F}_2$.

iii.- ¿Es posible expresar $A = \mathbb{M}_2(\mathbb{F}_2)$ como producto de anillos no triviales?

Desarrollo:

i.- Reecordemos que la martriz $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ cumple con $A^2 = -id$. Luego dicha matriz satisface lo pedido. Ahora bien cualquier matriz conjugada a ella satisface la misma ecuación, por lo tanto para encontrar infinitas soluciones basta con conjugarla por matrices en $Gl_2(\mathbb{R})$. Por ejemplo $A_n = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{n} \end{pmatrix} = \begin{pmatrix} 0 & -\frac{1}{n} \\ n & 0 \end{pmatrix}$ es una suseción de matrices que son solución de $x^2 + 1 = 0$.

ii.- Recordemos que si una matriz cumple con $x^2 - x = 0$, entonces es $0, id$ o bien en alguna base es de la forma $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Luego todos las posibles

matrices son los conjugados de A por elementos de $Gl_2(\mathbb{F}_2) \cong S_3$. De hecho

$$Gl_2(\mathbb{F}_2) = \left\{ id, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\}.$$

Por lo tanto los elementos idempotentes no triviales estan en:

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

i.- Observe que ninguno de los elementos de N está en el centro de A. Puede hacer lo calculos para ver que $Z(A) = \{0, id\}$. Por lo tanto no existen idempotentes centrales en A no triviales. Luego A no puede ser expresado como producto de anillos no triviales.

Ayudantía 15: En esta ayudantía estudiaremos los anillos euclideanos, cuerpos de cocientes y anillos de enteros.

1.- **Problema 1:** Demustre que $\mathbb{Z}[\sqrt{2}]$ es un dominio euclideano.

Demostración: Considere $a+b\sqrt{2}, c+d\sqrt{2} \neq 0 \in \mathbb{Z}[\sqrt{2}]$. Considere $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{ac-2bd+(ad+bc)\sqrt{2}}{c^2-2d^2}$.
Renombrando los elementos , podemos decir que $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = s+t\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Tomemos $x, y \in \mathbb{Z}$ numeros más proximos a s, t respectivamente, entonces $|x-s| \leq \frac{1}{2}, |y-t| \leq \frac{1}{2}$. Considere $x+y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.
Entonces obtenemos el candidado a resto:

$$r = a+b\sqrt{2} - (c+d\sqrt{2})(x+y\sqrt{2}) \in \mathbb{Z}[\sqrt{2}],$$

Observe que dicho candidato cumple con:

$$N(r) = N(c+d\sqrt{2})N((s+t\sqrt{2}) - (x+y\sqrt{2})),$$

de esto se sigue que

$$N(r) = N(c+d\sqrt{2})[(s-x)^2 - 2(t-y)^2] \leq \frac{3}{4}N(c+d\sqrt{2}),$$

Por lo tanto:

$$N(r) < N(c+d\sqrt{2}).$$

Luego nuestro r es un resto. Esto demuestra que $\mathbb{Z}[\sqrt{2}]$ es dominio euclideano.

1.- **Observación :** Observe que la demostración del hecho anterior es esencialmente la misma que para verificar que $\mathbb{Z}[i]$ es un dominio euclideano. La unica diferencia se puede apreciar en que el anillo $\mathbb{Z}[i]$ se inyecta en $\mathbb{C}$, mientras que $\mathbb{Z}[\sqrt{2}]$ se inyecta en $\mathbb{R}$.

2.- **Problema 2:** Demuestre todo dominio euclideano A es normal, es decir : Si $a \in Q(A)$ es raíz de un polinomio mónico con coeficientes en A entonces $a \in A$. Use el hecho de que en un dominio euclideano todo elemento es producto de primos. (Elementos generadores de ideales primos).

Demostración: Considere $\alpha = \frac{a}{b} \in Q(A)$ elemento que es raiz de :

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in A[x]$$

Luego:

$$p(\alpha) = \left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 = 0$$

Multiplicando por b^n:

$$a^n + ba_{n-1}a^{n-1} + \cdots + b^n a_0 = 0.$$

Pero si $\pi | b$, donde $\pi \in A$ es primo, entonces

$$\pi | a^n = -b(a_{n-1}a^{n-1} + \cdots + b^{n-1}a_0).$$

Luego $a^n \in (\pi)$, como π primo , $a \in (\pi)$. O sea $\pi | a$.
Repitiendo el proceso , en cada primo que divide a b tenemos que este divide a a. Por lo tanto $\alpha \in A$.

3.- **Problema 3:** Demuestre que el cuerpo de cocientes de $A = \mathbb{Z}[\sqrt{D}]$, para $D \in \mathbb{Z}$ libre de cuadrados, es $\mathbb{Q}[\sqrt{D}]$.

Demostración: Considere $\frac{a+b\sqrt{D}}{c+d\sqrt{D}} \in Q(A)$, con $c + d\sqrt{D} \neq 0$. Entonces :

$$\frac{a + b\sqrt{D}}{c + d\sqrt{D}} = \frac{ac - bdD - (ad + bc)\sqrt{D}}{c^2 - Dd^2}.$$

Esto pues si multiplicamos de forma cruzada obtenemos la igualdad [Lea la definición de igualdad en el cuerpo de cocientes]. Por ello $Q(A) \subseteq \mathbb{Q}[\sqrt{D}]$. La inclusión contraria se tiene pues $\frac{a}{b} + \frac{c}{d}\sqrt{D} = \frac{ad+bc\sqrt{D}}{bd}$.

4.- **Problema 4:** Sea $A = \mathbb{Z}[i]$ anillo de enteros gaussianos.

i.- Demuestre que $(2 + i)$ es un ideal maximal de A.

ii.- Encuentre un m.c.d entre $(2 + i)$ y $5i$.

iii.- Demuestre que $\mathbb{Z}[i]/(3i + 1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Desarrollo:

i.- Observe que:

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

ya que $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$ y $(2 + i) \cong (2 + x, x^2 + 1)/(x^2 + 1)$. Donde ambos isomorfismos se establecen vía la evaluación en i. Luego:

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

Pero si usamos el tercer teorema de isomorfía:

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

Pero $(2 + x, x^2 + 1) = (5, x + 1)$, pues $5 = x^2 + 1 - (x - 2)(x + 2)$. Por lo tanto:

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

Este último isomorfismo se obtiene evaluando en $u = x + 2$.

Luego $\mathbb{Z}[i]/(1+i)$ es un cuerpo y por ello $I = (1+i)$ es un ideal maximal.

ii.- Recordemos que $d = mcd(2 + i, 5i)$ es un elemento generador de $(2 + i) + (5i) = (d)$. Por otro lado $5i = (2 + i)(2 - i)i$. Por lo tanto $(2 + i) + (5i) = (2 + i)$. Luego un mcd de $2 + i$ y $5i$ es $d = 2 + i$.

iii.- Observe que $A = \mathbb{Z}[i]$ es un dominio de integridad. Luego podemos ocupar el teorema chino de los restos sobre este anillo A.

En efecto, $(3i+1) = ((i+1)(i+2)) = (i+1)(i+2)$, donde $(i+2)-(i+1) = 1$. Por ello los ideales $(i + 1)$ e $(i + 2)$ son relativamente primos. Así:

$$\mathbb{Z}[i]/(3i + 1) \cong \mathbb{Z}[i]/(i + 1) \times \mathbb{Z}[i]/(i + 2)$$

Sabemos que, por lo visto en [i] que:

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

De forma análoga se demuestra que [ejercicio] :

$$\mathbb{Z}[i]/(i + 1) \cong \mathbb{Z}/3\mathbb{Z}.$$

Finalmente:

$$\mathbb{Z}[i]/(3i+1) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \cong \mathbb{Z}/10\mathbb{Z}.$$

Ayudantía 16: En esta ayudantía estudiaremos los anillos de factoriazión única y los dominios de ideales principales.

1.- **Problema 1:** Sea A un dominio de integridad, tal que $A[x]$ es un dominio de ideales principales, demuestre que A es cuerpo. Muestre con un contraejemplo que este hecho no se extiende para $A[x]$ dominio de factorización única. ¿Es $\mathbb{Z}[i][x]$ dominio de ideales principales?

1.- **Desarrollo:** Considere $I = (x)$ ideal de $A[x]$. La estrategia para atacar este problema es demostrar que I es un ideal primo de $A[x]$, luego como $A[x]$ es DIP, se tiene que este ideal es maximal. En efecto, por lo visto en una de las primeras ayudantias de anillos:

$$A[x]/I \cong A$$

Con A dominio de integridad. Luego como el anillo de partida es conmutativo con 1 y $A[x]/I$ es dominio de integridad ,tenemos que I es ideal primo. Como $A[x]$ es DIP se concluye que I es maximal. Luego el cociente $A[x]/I \cong A$ es cuerpo.

Observe además que este resultado no se extiende a DFU, pues $\mathbb{Z}[x]$ es un DFU [se verá la proxima clase, por ahora créalo], con $\mathbb{Z}$ dominio de integridad, pero no cuerpo.

Por último si $\mathbb{Z}[i][x]$ fuese DIP entonces por lo anterior $\mathbb{Z}[i]$ es un cuerpo, pero esto es falso de hecho el grupo de invertibles de los enteros gaussianos $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

1 **Observación :** Sabemos que el recíproco es cierto. Es decir sabemos que $A[x]$ es DIP, cuando A es cuerpo.

2.- **Problema 2:** Muestre que $A = \mathbb{Z}[\sqrt{-5}]$ no es un dominio de factorización única.

2.- **Desarrollo:** Observe que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Demostremos que estas dos escrituras con elementos irreducibles es esencialmente distinta. Partamos por demostrar que estos elementos son irreducibles. Considere $N(a + b\sqrt{-5}) = a^2 + 5b^2$ norma compleja de $a + b\sqrt{-5}$.

Observe que si $3 = ab$ entonces $9 = N(3) = N(a)N(b)$. Luego como la ecuación $x^2 + 5b^2 = 3$ no tiene soluciones enteras, tenemos que $N(a) = 9$ y $N(b) = 1$ o viceversa. Por ello $1 = N(a) = a\overline{a}$, es decir a es unidad. El mismo argumento es válido para demostrar que $2 \in A$ es irreducible. Ahora bien si $1 + \sqrt{-5} = ab$ entonces $6 = N(a)N(b)$. Entonces como no hay elementos de norma 2 y 3 se tiene que a es unidad o b es unidad. Lo mismo para $1 - \sqrt{-5} \in A$. Por lo tanto $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5} \in A$ son elementos irreducibles. Observe que si estos elementos fueran asociados, como la norma de las unidades de A es 1, tendriamos que $4 = N(2) = N(1 + \sqrt{-5}) = 6$ o bien $9 = N(3) = N(1 + \sqrt{-5}) = 6$. Por ello las dos factorizaciones de $6 \in A$ son esencialemente distintas.

3.- **Problema 3:** Muestre que $A = \left(\mathbb{Q}[x]/(x^2 + x + 1)\right)[y]$ es un dominio de factorización única.

3.- **Desarrollo:** Mostremos que A es un DFU. Partamos analizando la estructura del anillo $A' = \mathbb{Q}[x]/(x^2 + x + 1)$.

En efecto, observe que $\phi_3(x) = x^2 + x + 1$ es irreducible. Esto pues ϕ es un polinomio cuadrático sin raíces en $\mathbb{Q}$. Luego como $\mathbb{Q}[x]$ es DIP, pues es el anillo de polinomios sobre un cuerpo, tenemos que $I = (x^2 + x + 1)$ es un ideal maximal. Por lo tanto el cociente $A' = \mathbb{Q}[x]/(x^2 + x + 1)$ es cuerpo.

Luego como todo anillo de polinomios sobre un cuerpo es un DE, tenemos que A es DE. Luego es DIP y más especificamente A es DFU.

4.- **Problema 4:** Demuestre que en el anillo $A = \mathbb{Z}[\sqrt{2}]$ se cumple que toda cadena ascendente de ideales tiene un elemento maximal. Es decir, toda familia de ideales $\{I_n\}_{n\in\mathbb{N}} \subset \mathcal{P}(A)$, que cumple con:

$$I_1 \subseteq I_2 \subseteq \cdots I_n \subseteq \cdots$$

tiene un elemento maximal I_m tal que $I_m = I_n$, $\forall n \geq m$.

4.- **Demostración:** Observe que por lo visto en la ayudantía anterior $A = \mathbb{Z}[\sqrt{2}]$ es un dominio euclideano (DE), luego por lo visto en clases, este es un dominio de ideales principales. Considere el ideal $I = \cup_{i\in\mathbb{N}} I_i$. Como A es DIP, tenemos que existe $a \in A$ tal que $I = (a)$. Luego $a \in I_m$, para algún $m \in \mathbb{N}$. Por lo tanto $I_m \subseteq I \subseteq I_m$. Esto es equivalente a que $I = I_m$. En otras palabras $I_m = I_i$, para cualquier $i \geq m$.

4.- **Ejercicio:** Pruebe que la condición de que toda cadena ascendente de ideales de A tenga un elemento maximal es equivalente a que todo ideal de A sea finitamente generado.

4.- **Observación:** El ejercicio anterior da una solución sencilla al problema 4.

Ayudantía 17: En esta ayudantía estudiaremos algunas tecnicas claves en la teoriá de anillos y analizaremos la irreducibilidad de algunos polinomios sobre DFU.

1.- **Problema 1:** Encuentre condiciones sobre $n, m \in \mathbb{Z}$ para que $(x-n)$ y $(x+m)$ sean comaximales en $\mathbb{Z}[x]$.

1.- **Desarrollo:** Queremos que $(x-n)+(x-m) = \mathbb{Z}[x]$. Para encontrar condiciones para que esto ocurra cocientemos por el ideal $(x-m)+(x-n) = (x-m, x-n)$. En efecto $\mathbb{Z}[x]/(x-n, x-m) \cong \mathbb{Z}/(n-m)$. Esto último debido a que el morfismo $\rho : \mathbb{Z}[x] \to \mathbb{Z}/(n-m)$ definido por $\rho(p(x)) = p(n)$ cumple con ser sobreyectivo y además su número es $p(x) \in \mathbb{Z}[x]$ tales que $p(n) = a(n-m)$ es decir $q(x) = p(x) - a(x-m)$ cumple con $q(n) = 0$. Por lo visto en una de las ayudantás anteriores, esto último implica que $q(x) = s(x)(x-n)$. Luego $p(x) = s(x)(x-n) + a(x-m)$. Por lo tanto $\ker(\rho) = (x-n, x-m)$. Luego por primer teorema de isomorfiá $\mathbb{Z}[x]/(x-n, x-m) \cong \mathbb{Z}/(n-m)$.

De esto concluimos que para que $(x-n), (x-m)$ sean comaximales se requiere que $(n-m) = \mathbb{Z}$. Es decir que $n - m = \pm 1$. Dicha condición es suficiente pues si $n - m = \pm 1$ entonces $(x-m) - (x-n) = \pm 1$ y esto implica que $\pm 1 \in (x-n, x-m)$. Lo que nos diche que dichos ideales son comaximales.

2.- **Problema 2:** Sea η_5 una raiz quinta primitiva de la unidad. Demuestre que en $\mathbb{Z}[\eta_5]$ el ideal $(\eta_5 - 1)$ es maximal y que $u = \eta_5 + 1$ es unidad.

2.- **Demostración:** Afirmamos que $\mathbb{Z}[\eta_5] \cong \mathbb{Z}/(p(x))$, donde $p(x) = x^4 + x^3 + x^2 + x + 1$. En efecto el morfismo $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\eta_5]$ definido por $\phi(q(x)) = q(\eta_5)$ es sobreyctivo y tiene por núcleo a $\ker(\phi) = \{q(x) : q(\eta_5) = 0\}$. Recordemos que podemos hacer el algoritmo de la división si el polinomio por el cual dividimos es mónico. Luego si $q(x) \in \ker(\phi)$ entonces $q(x) = p(x)s(x) + t(x)$, donde $deg(t) < deg(p)$ o $t = 0$. Si evaluamos en $x = \eta_5$ entonces $t(\eta_5) = 0$. Luego η_5 satisface un polinomio de grado menor a $p(x)$. Esto sucede si $t = 0$. Por lo tanto $q(x) \in (p(x))$. Luego $\mathbb{Z}[\eta_5] \cong \mathbb{Z}/(p(x))$.

Ahora bien, el isomorfismo anterior induce un isomorfismo $(\eta_5 + 1) \cong (x-1, p(x))/(p(x))$. Por lo tanto

$$\mathbb{Z}[\eta_5]/(\eta_5 - 1) \cong \mathbb{Z}[x]/(p(x))/(x-1, p(x))/(p(x)),$$

Luego por uno de los teoremas de isomorfía tenemos que $\mathbb{Z}[\eta_5]/(\eta_5 - 1) \cong \mathbb{Z}[x]/(x-1, p(x))$. Haciendo uso del morfismo evaluación en 1 resulta:

$$\mathbb{Z}[\eta_5]/(\eta_5 - 1) \cong \mathbb{Z}/(5),$$

que sabemos que es cuerpo. Por lo tanto $(\eta_5 - 1)$ es un ideal maximal.

Por otro lado el ideal $(\eta_5 + 1)$ cumple con $\mathbb{Z}[\eta_5]/(\eta_5 + 1) \cong \mathbb{Z}[x]/(x + 1, p(x))$. Haciendo uso del isomorfismo evaluación en -1 se tiene que $\mathbb{Z}[\eta_5]/(\eta_5 + 1) \cong \mathbb{Z}/(1) = \{0\}$. Luego $u = \eta_5 + 1$ es invertible.

Otra forma de argumentar que u es unidad, es la siguiente. Observe que $(x-1)p(x) = x^5 - 1$. Luego $(\eta_5 - 1)p(\eta_5) = -1$. Por lo tanto el inverso de u es $v = -p(\eta_5)$.

3.- **Problema 3:** Demuestre que $x^n + yx + y$ es irreducible en $\mathbb{Z}[x, y]$.

3.- **Demostración:** Considere $p(x, y) = x^n + x + y \in A[x] = \mathbb{Z}[x, y]$, donde $A = \mathbb{Z}[y]$. Sabemos que $A = \mathbb{Z}[y]$ es un DFU, debido a que $\mathbb{Z}$ es DFU y además sabemos que el elemento $\pi = y$ es primo, pues $A/(y) \cong \mathbb{Z}$ dominio. Observe que y divide a todos los coeficientes del polinomio a excepción del de grado mayor y además y^2 no divide al termino constante. Luego por criterio de Eisenstein $p(x, y)$ es irreducible en $K[y]$, donde $K = Quot(A) = \mathbb{Q}(y)$. Observe que $p(x, y)$ es un polinomio mónico en $A[x]$ y por lo tanto primitivo. Luego por lema de Gauss $p(x, y)$ es irreducible en $A[x]$. Luego $p(x, y)$ es irreducible en $\mathbb{Z}[x, y]$.

4.- **Problema 4:** Sea $\phi(x) = x^3 + 5x + (2 + i) \in \mathbb{Z}[i][x]$. Demustre que (ϕ) es maximal en $\mathbb{Q}[i][x]$.

4.- **Demostración:** Considere el polinomio $\phi(x) = x^3 + 5x + (2 + i) \in \mathbb{Z}[i][x]$. Observe $\mathbb{Z}[i]$ es un DIP y por lo tanto es un DFU. Además el elemento primo $\pi = 2 + i$ (es primo, por lo visto en las ayudantías anteriores) divide a todos los coeficientes del polinomio, excepto el de mayor grado, pues $5 = (2+i)(2-i)$. Por último π^2 no divide al término libre de $\phi(x)$. Por criterio de Eisentein $\phi(x)$ es irreducible en $Quot(\mathbb{Z}[i])[x]$. Pero $Quot(\mathbb{Z}[i]) = \mathbb{Q}[i]$. Esto concluye lo pedido.

Ayudantía 18: En esta ayudantía trabajaremos la localización de anillos.

1.- **Problema 1:** Determine la estructura de los siguientes anillos:
i.- $A = \mathbb{Z}[w]/(3w-1)$.

ii.- $A = \mathbb{Z}[i]/(5i+2)$.

1.- **Desarrollo:** Partamos con un lema importante.

Lemma 2. *$\mathbb{Z}[x]/(sx-1) \cong S^{-1}\mathbb{Z} = \mathbb{Z}_{(s)}$, donde $S = \{1, s, s^2, \cdots\}$.*

Proof. Considere el homomorfismo de anillos $\phi : \mathbb{Z}[x] \to S^{-1}\mathbb{Z}$ definido por $\phi(p(x)) = p(\frac{1}{s})$. Claramente ϕ es sobreyectivo pues $\phi(ax^n) = a/s^n$. Observe que si $p(x) \in \mathbb{Z}[x]$ cumple con $p(\frac{1}{s}) = 0$ entonces en $\mathbb{Q}[x]$ se tiene que $p(x) = (x - \frac{1}{s})r(x)$, con $r(x) \in \mathbb{Q}[x]$. Por lema de Gauss, tenemos que $p(x) = (sx-1)l(x)$, donde $l(x) \in \mathbb{Z}[x]$. □

i.- Recordemos que $\mathbb{Z}[w]/(3w-1) \cong \mathbb{Z}[x]/(3x-1, x^2+x+1)$. La justificación a de esto se hizo en las ayudantías anteriores. Observe que por el tercer teorema de ismorfá:

$$\mathbb{Z}[w]/(3w-1) \cong \mathbb{Z}[x]/(3x-1)/(3x-1, x^2+x+1)/(3x-1).$$

Por lo mencionado en el lema previo $\mathbb{Z}[x]/(3x-1) \cong \mathbb{Z}_{(3)}$. Por el mismo isomorfismo obtenemos que $(3x-1, x^2+x+1)/(3x-1) \cong (\frac{13}{9}) = (13)$, puesto que $9 \in \mathbb{Z}_{(3)}$ es invertible. Por lo tanto:

$$\mathbb{Z}[w]/(3w-1) \cong \mathbb{Z}_{(3)}/(13).$$

Si tomamos el ismorfismo inverso al cosiderado en la demostración del lema previo, tenemos que $\mathbb{Z}[w]/(3w-1) \cong \mathbb{Z}[x]/(13, 3x-1) \cong \mathbb{F}_{13}/(3x-1)$. Como $3 \cdot 4 = -1$ en $\mathbb{F}_{13}$ tenemos que:

$$\mathbb{Z}[w]/(3w-1) \cong \mathbb{F}_{13}/(x+4) \cong \mathbb{Z}/13\mathbb{Z}.$$

Por lo tanto A es cuerpo. Equivalentemente $(3w-1)$ es un ideal maximal en $\mathbb{Z}[w]$.

ii.- Recordemos que $\mathbb{Z}[i]/(5i+2) \cong \mathbb{Z}[x]/(5x+2, x^2+1)$. Luego por el tercer teorema de ismorfá:

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

Por lo mencionado en el lema previo $\mathbb{Z}[x]/(5x+2) \cong \mathbb{Z}[\frac{-2}{5}] \subset \mathbb{Z}_{(5)}$, donde $\mathbb{Z}[\frac{-2}{5}]$ es el anillo de polinomios evaluados en $\frac{-2}{5}$. Por el mismo isomorfismo obtenemos que $(5x+2, x^2+1)/(5x+2) \cong (\frac{29}{25}) = (29)$, puesto que $25 \in \mathbb{Z}[\frac{-2}{5}]$ es invertible. Por lo tanto:

$$\mathbb{Z}[i]/(5i+2) \cong \mathbb{Z}\left[\frac{-2}{5}\right]/(29).$$

Si tomamos el ismorfismo inverso al anteriormente, tenemos que $\mathbb{Z}[i]/(5i+2) \cong \mathbb{Z}[x]/(29, 5x+2) \cong \mathbb{F}_{29}/(5x+2)$. Como $5 \cdot 6 = 1$ en $\mathbb{F}_{29}$ tenemos que:

$$\mathbb{Z}[i]/(5i+2) \cong \mathbb{F}_{29}/(x+12) \cong \mathbb{Z}/29\mathbb{Z}.$$

Por lo tanto A es cuerpo. Equivalentemente $(5i+2)$ es un ideal maximal en $\mathbb{Z}[i]$.

2.- **Problema 2:** Describa los primos $p \in \mathbb{Z}$ que son primos en el anillo $\mathbb{Z}[\frac{1}{3i}]$, en términos del cuerpo finito $\mathbb{F}_p$.

2.- **Desarrollo:** Sea p primo en $\mathbb{Z}$. Estudiemos el cociente $\mathbb{Z}[\frac{1}{3i}]/(p)$. Observe que $\mathbb{Z}[\frac{1}{3i}] \cong \mathbb{Z}/(9x^2+1)$. Este isomorfismo se obtiene vía el homomorfismo $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\frac{1}{3i}]$ definido por $\phi(p(x)) = p(\frac{1}{3i})$.

2.- **Ejercicio**: Pruebe que este homomorfismo induce un isomorfismo entre $\mathbb{Z}[\frac{1}{3i}]$ y $\mathbb{Z}[x]/(9x^2+1)$.

Luego $\mathbb{Z}[\frac{1}{3i}]/(p) \cong \mathbb{Z}[x]/(9x^2+1, p) \cong \mathbb{F}_p[x]/(9x^2+1) \cong \mathbb{F}_p[\frac{-i}{3}]$. Supongamos que $p \neq 3$, en este caso 3 es invertible en $\mathbb{F}_p$. Por lo tanto $\mathbb{Z}[\frac{1}{3i}] \cong \mathbb{F}_p[i]$. Si no existen elementos en $\mathbb{F}_p$ tales que $x^2 = -1$ entonces el polinomio $g(x) = x^2+1$ es irreducible en $\mathbb{F}_p$, por lo tanto $\mathbb{F}_p[i]$ es cuerpo y luego p es maximal en $\mathbb{Z}[\frac{1}{3i}]$, en particular p es primo.

Por otro lado si $p = 3$ entonces $\mathbb{Z}[\frac{1}{3i}]/(3) \cong \mathbb{F}_3[x]/(9x^2+1) \cong \mathbb{F}_3[x]/(1) \cong \{0\}$. Por lo tanto $(3) = \mathbb{Z}[\frac{1}{3i}]$. Luego $p = 3$ no es primo en $\mathbb{Z}[\frac{1}{3i}]$.

2.- **Observación:** Se puede demostrar que $\mathbb{F}_p[i]$ es cuerpo sí y solamente sí $p \equiv 3 (mod\, 4)$.

3.- **Problema 3:** Sea $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ que tiene una raiz en $\mathbb{Q}$. Probar que su reducción módulo p tiene una raiz en $\mathbb{Z}/p\mathbb{Z}$ para todo primo $p \nmid a_n$.

3.- **Demostración:** Sea $\frac{r}{s} \in \mathbb{Q}$, con $(r,s) = 1$ raiz de $f(x)$. Entonces por el criterio de la raiz racional, tenemos que $r|a_0$ y $s|a_n$. Sea p primo tal que $p \nmid a_n$ entonces $p \nmid s$. Por lo tanto existe $s^{-1} \in \mathbb{Z}/p\mathbb{Z}$. Observe que $\frac{r}{s} \in S^{-1}\mathbb{Z}$, para $S = \{1, s, s^2, \cdots\}$. Considere el morfismo $\phi : S^{-1}\mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ definido por $\phi(p(x)) = p(x) (mod\, p)$, bien definido por $s^{-1} \in \mathbb{Z}/p\mathbb{Z}$. Luego evaluando en r/s la imagen de $f(x)$ por ϕ tenemos que $f(rs^{-1}) = 0 (mod\, p)$.

4.- **Problema 4:** Sea $A = \mathbb{Z}[x, x^{-1}]$ anillo de polinomios en las variables x, x^{-1} y sea $B = A/(x+1+x^{-1})$. Pruebe que B es un DFU.

4.- **Demostración:** Observe que $B \cong \mathbb{Z}[x, x^{-1}]/(\frac{x^2+x+2}{x})$. Como $x \in \mathbb{Z}[x]$ es invertible tenemos que $B = \mathbb{Z}[x, x^{-1}]/(x^2+x+1)$. Ahora bien, observe que todo polinomio en $p(x, x^{-1}) = \frac{q(x)}{x^n}$. Por lo tanto $A = S^{-1}\mathbb{Z}[x]$, donde $S = \{1, x, x^2, \cdots\}$. Por lo tanto:

$$B = S^{-1}\mathbb{Z}[x]/S^{-1}(x^2+x+1) \cong S^{-1}\left(\mathbb{Z}[x]/(x^2+x+1)\right).$$

Luego vía el morfismo evaluación en $w = e^{\frac{2i\pi}{3}}$, tenemos que $\mathbb{Z}[x]/(x^2+x+1) \cong \mathbb{Z}[w]$. Como la imagen de x vía el isomorfismo en w elemento invertible en $\mathbb{Z}[w]$ tenemos que:

$$B \cong S^{-1}\left(\mathbb{Z}[x]/(x^2+x+1)\right) \cong \mathbb{Z}[w],$$

que ya sabemos que es un DIP, en particular un DFU.

3. Módulos:

Ayudantía 19: En esta ayudantía trabajaremos con los conceptos básicos de la teoría de módulos.

1.- **Problema 1:** Demuestre que la acción de $\mathbb{Z}$ sobre $(G,+)$ grupo abeliano :

$$n.g := g + \cdots + g$$

convierte a G en un $\mathbb{Z}$- módulo. Responda:

i ¿Cuál es la torsión de G?

ii ¿Existen grupos de torsión que no sean finitos?

i.- **Desarrollo:** Demostremos primero que la acción anterior le da a G estructura de $\mathbb{Z}$-módulo. Basta demostrar cada axioma, en efecto:

i $1.g = g$, $\forall g \in G$.

ii $(nm).g = n(g + \cdots + g) = n.(m.g)$, $\forall g \in G\,, \forall n, m \in \mathbb{Z}$.

iii $(n+m).g = g + \cdots + g = n.g + m.g$, $\forall g \in G\,, \forall n, m \in \mathbb{Z}$.

iv $n(g_1 + g_2) = (g_1 + g_2) + \cdots + (g_1 + g_2) = g_1 + \cdots + g_1 + g_2 + \cdots + g_2 = n.g_1 + n.g_2$, $\forall g_1, g_2 \in G$, $\forall n \in \mathbb{Z}$.

Luego G es un $\mathbb{Z}$- módulo. Observe que la conmutatividad de G es crucial en la identidad [iv].

Ahora encontremos la torsión de dicho grupo , es decir, determinemos el submódulo :

$$Tor(G) = \{g \in G : \exists n \in \mathbb{Z} : n.g = 0\},$$

Observe que $g \in Tor(G)$ si y sólamente si existe $n \in \mathbb{Z}$ con $g + \cdots + g = 0$, luego el orden de $g \in G$ es finito y si $g \in G$ tiene orden finito se tiene que $g \in Tor(G)$, pues basta tomar $n = |g|$. Así:

$$Tor(G) = \{g \in G : |g| = n < \infty\}.$$

Observe que si G es finito, todo $g \in G$ tiene orden finito, por lo tanto $Tor(G) = G$.

ii.- Para respoder a esto basta encontrar un grupo infinito tal que todos sus elementos sean de orden finito. Considere por ejemplo $G = \oplus_{i \in \mathbb{N}} C_2$. Este es un grupo infinito, pero todos sus elementos tienen orden 2.

2.- **Problema 2:** Sea $F : M \to N$ homomorfismo de R-módulos. Este se dice cancelable a la izquierda si $F \circ g = F \circ h$ implica que $g = h : L \to M$. Demuestre que F cancelable a la izquiera si y sólamente si F inyectivo.

2.- **Demostración:** Primero supongamos $F : M \to N$ homomorfismo inyectivo. Sea L cualquier R-módulo y $g, h : L \to M$ homomorfismos tales que $F \circ g = F \circ h$. Considere $x \in L$ cualquiera, entonces si $F \circ g(x) = F \circ h(x)$ se tiene que $F((g-h)(x)) = 0$, como F inyectiva, su nucleo es trivial , así $g(x) = h(x), \forall x \in L$. Luego $g = h$.

Inversamente considere el R-módulo $L = ker(F)$ y considere $g = i : L \to M : x \mapsto x$ homomorfismo inclusión. Entonces $F \circ g(x) = 0 = F \circ 0(x)$, $\forall x \in L$, donde $0(x)$ denota la función nula evaluada en $x \in L$. Como F es cancelable por izquiera $g = i = 0$, luego el único elemento de $L = ker(F)$ es el cero, es decir F es inyectiva.

2.- **Ejercicio:** Enuncie y demuestre un criterio análogo para cancelable a la derecha.

3.- **Problema 3:** Sea R anillo conmutativo con unidad.
i.- Muestre que si M es un R-módulo entonces $M \cong Hom_R(R, M)$.
ii.- Deduzca que $R \cong Hom_R(R, R)$.

3.- **Desarrollo:** Demostremos cada parte del ejercicio. En efecto:
i.- Sea $h : R \to M$ un R-homomorfismo. Entonces $h(r) = h(r.1) = r.h(1)$, donde $h(1) \in M$. Motivados por lo anterior , considere la función evaluación $\phi : Hom_R(R, M) \to M : h \mapsto h(1)$, esta es claramente un homomorfismo de R-módulos.

3.- **Ejercicio:** Demuestre que $Hom_R(R, M)$ es un R-módulo con la suma y ponderación usual de funciones.

Ahora bien, si $h(1) = 0$ entonces $h(r) = r.h(1) = 0, \forall r \in R$. Luego $Ker(\phi) = 0$ por lo tanto ϕ es una función inyectiva. Para ver que es sobreyectiva, considere $m \in M$, entonces definimos $h_m : R \to M : r \mapsto r.m$. Observe que $h_m(n + tk) = (n + tk).m = n.m + t.(k.m) = h_m(n) + t.h_m(k)$. Por lo tanto $h_m \in Hom_R(R, M)$. Luego $\phi(h_m) = m$. Esto concluye que ϕ es un isomorfismo, por lo tanto $M \cong Hom_R(R, M)$.
ii.- Considere R como R-módulo. Entonces $R \cong Hom(R, R)$

4.- **Problema 4:** Sean N_j, P R-módulos , donde $j \in \{1, \cdots, n\}$. Considere $M = \oplus_{j=1}^{n} N_j$. Demuestre que si tomamos $F_j : N_j \to P$ homomorfismos, entonces existe un único homomorfismo $F : M \to P$ tal que $F|_{N_j} = F_j$.

4.- **Desarrollo:** Primero la existencia. En efecto, considere $m = m_1 + \cdots + m_n \in M$ elemento cualquiera. Entonces definimos:

$$F : M \to P : m \mapsto F_1(m_1) + \cdots + F_n(m_n),$$

función bien definida pues m tiene una única escritura de este tipo. Observe que esta función es un homomorfismo ya que si $n = n_1 + \cdots + n_n$ y $m = m_1 + \cdots + m_n$ entonces $m + \lambda n = (m_1 + \lambda n_1) + \cdots + (m_n + \lambda n_n)$, luego $F(m + \lambda n) = \sum F_i(m_i + \lambda n_i) = \sum F_i(m_i) + \lambda F_i(n_i)$, por ello $F(m + \lambda n) = F(m) + \lambda F(n)$. Es decir F es homomorfismo y cumple con $F|_{N_j} = F_j$.

Ahora la unicidad. Si hubiese otra función $G : N \to P$ homomorfismo tal que $G|_{N_j} = F_j$ entonces, para $m = m_1 + \cdots + m_n$ se tiene que:

$$G(m) = \sum G(m_i) = \sum F_i(m_i) = F(m), \forall m \in M$$

Luego $G = F$. Por lo tanto existe un único homorfismo F.

4.- **Observación:** Usando este hecho es probible probar que si R es conmutativo, entonces: $Hom_R(\oplus_{j=1}^{n} N_j, P) \cong \oplus_{j=1}^{n} Hom_R(N_j, P)$. Su demostración queda de **ejercicio.**

Ayudantía 20: En esta ayudantía trabajaremos módulos libres y finitamente generados.

1.- **Problema 1:** *Lema de Nakayama:* Sea M un R-módulo finitamente generado. Se define el conjunto radical de M por:

$$rad(M) := \cap\{T : T\, submodulo\, maximal\, de\, M\}.$$

i.- Demuestre que $rad(M)$ es un submódulo de M.

ii.- Demuestre si N es un submódulo de M tal que $N + rad(M) = M$ entonces $N = M$.

1R.- **Desarrollo:**

i.- En general la intersección arbitaria de submódulos de M es submóludo del mismo. Esto se debe a que si tomamos x, y en la intersección de todos los submódulos en cuestión, entonces $x, y \in T$, $\forall T$ luego $x + \lambda y \in T$, $\forall T$ por ser T submódulo. Por lo tanto $x + \lambda y$ está en la intersección de todos los submódulos considerados. Observe que la intersección es no trivial pues $0 \in T$, $\forall T$.

ii.- Supongamos $N \neq M$ entonces, por un argumento vía lema de zorn, como M es finitamente generado, se tiene que existe un ideal maximal T de M tal que $N \subseteq T$. Además $rad(M) \subseteq T$, pues T es uno de los tantos conjuntos que se intersecta para definir $rad(M)$. Luego $M = N + rad(M) \subseteq T$ por lo tanto $M = T$, pero por definición de un ideal maximal $T \neq M$. Por ello $N = M$.

2.- **Problema 2:** Considere M un R-módulo cualquiera y defina su módulo dual por:

$$M^* = Hom_R(M, R) = \{f : M \to R :\ f\, homomorfismo\}.$$

i.- Pruebe que si M es un módulo libre de rango finito entonces M^* es libre.

ii.- Pruebe que con M como en [i], el rango de M es igual al rango de M^*.

iii.- Pruebe que $Hom_{\mathbb{Z}}(\mathbb{Z}[\eta_p], \mathbb{Z})$ es un módulo libre de rango $p - 1$.

1.- **Desarrollo:** Demostremos cada punto.

i.- Demostremos el punto [i] e [ii].

Considere $\beta = \{f_i\}_{i=1}^n$ subconjunto de $Hom_R(M, R)$ dado por los funcionales:

$$f_i : M \to R : m = r_1 m_1 + \cdots + r_n m_n \mapsto r_i$$

Que corresponden a la proyección en la i-ésima coordenada, donde $\{m_i\}_{i=1}^n$ es base de M como R-módulo.

Observe que si $f \in Hom_R(M, R)$ entonces $f(m) = f(r_1 m_1 + \cdots + r_n m_n) = r_1 f(m_1) + \cdots r_n f(m_n) = \sum_{i=1}^n f_i(m) f(m_i)$, $\forall m \in M$. Luego todo homomorfismo se escribe como:

$$f = \sum_{i=1}^{n} f(m_i) f_i$$

Por lo tanto β genera el R-módulo $Hom_R(M, R)$.

Además si $f = \sum_{i=1}^n a_i f_i$, para ciertos $a_i \in A$, entonces evaluando f en $m = m_i$ concluimos que $a_i = f(m_i)$. Por ello la combinación lineal anterior es única. Por lo tanto β es base de M^*.

Concluimos que M^* es un R-módulo libre de rango igual al de M.

iii.- Por lo anterior basta demostrar que $M = (\mathbb{Z}[\eta_p])$ es un $\mathbb{Z}$-módulo libre de rango $p-1$. Observe que todo elemento en M se escribe de la forma:

$$m = n_0 + n_1\eta_p + \cdots + n_{p-2}\eta_p^{p-2},\ n_i \in \mathbb{Z}$$

Esto ya que $\mathbb{Z}[\eta_p] \cong \mathbb{Z}[x]/(\phi_p(x))$, donde $\phi_p(x) = x^{p-1}+(p-1)x^{p-2}+\cdots+1$. Esto pues, todo polinomio de grado menor a $p-2$ no cae en la clase del 0, pero cuando tenemos un polinomio de grado mayor a $p-1$ hay que reducir módulo $\phi_p(x)$.

Ahora bien esta escritura es única ya que si $m = n_0 + n_1\eta_p + \cdots + n_{p-2}\eta_p^{p-2} = m = t_0 + t_1\eta_p + \cdots + t_{p-2}\eta_p^{p-2}$ donde $t_i, n_i \in \mathbb{Z}$, entonces:

$$0 = (n_0 - t_0) + (n_1 - t_1)\eta_p + \cdots + (n_{p-2} - t_{p-2})\eta_p^{p-2}$$

Luego el polinomio $p(x) = (n_0-t_0)+(n_1-t_1)x+\cdots+(n_{p-2}-t_{p-2})x^{p-2}$ es divisible por $\phi_p(x)$ que tiene grado mayor. Lo que es contradictorio, salvo si $p(x) = 0$. Luego $M = \mathbb{Z} \oplus \mathbb{Z}\eta_p \oplus \cdots \mathbb{Z}\eta_p^{p-2}$. Esto concluye que M es un $\mathbb{Z}$-módulo libre de rango $p-1$ y por ello M^* también.

1 **Observación:** Una generalización del hecho anterior es que si N es libre de rango n y M también lo es, con rango m entonces $Hom_R(M,N) \cong \mathbb{M}_{n\times m}(R)$ es un módulo libre de rango mn.

3.- **Problema 3:** Muestre que $\mathbb{Z}[i] \oplus \mathbb{Z}[w]$, donde $w = e^{\frac{2i\pi}{3}}$ es un $\mathbb{Z}$-módulo libre de rango 4.

3.- **Demostración:** Probemos un hecho más general, demostremos que si M, N son R-módulos libres de rango m y n respectivamente, entonces $M \oplus N$ es un R-módulo libre de rango $m+n$, pues entonces como :

$$\mathbb{Z}[i] = \mathbb{Z} \oplus i\mathbb{Z}$$

$$\mathbb{Z}[w] = \mathbb{Z} \oplus w\mathbb{Z}$$

Se tiene que ambos son módulos libres de rango dos, luego su suma directa es libre de rango 4.

Demostremos lo pedido. En efecto, sea $\{n_1, \cdots n_n\}$ base de N y $\{m_1, \cdots, m_m\}$ base de M. Entonces considere $\beta = \{n_1, \cdots, n_n, m_1, \cdots, m_m\}$ subconjunto de $M \oplus N$. Entonces si tomamos $m+n \in M \oplus N$ se tiene que:

$$m + n = r_1m_1 + \cdots r_mm_m + t_1n_1 + \cdots t_nn_n$$

Luego β genera $M \oplus N$. Es linealmente independiente pues si:

$$(r_1m_1 + \cdots r_mm_m) + (t_1n_1 + \cdots t_nn_n) = 0$$

Entonces, como $r_1m_1 + \cdots r_mm_m \in M$, $t_1n_1 + \cdots t_nn_n \in N$, se tiene que $t_1n_1 + \cdots t_nn_n = 0$ y $r_1m_1 + \cdots r_mm_m = 0$ luego $t_i, r_i = 0$. Así el conjunto β es base de $M \oplus N$. Por lo tanto $M \oplus N$ es un R-módulo libre de rango $m+n$.

4.- **Problema 4:** Demustre que todo $R = \mathbb{R}[x]/(x^2+x+1)$-módulo M es libre.

4.- **Demostración:** Basta probar que $R = \mathbb{R}[x]/(x^2+x+1)$ es un cuerpo, pues en este caso M es un A-espacio vectorial y en este contexto sabemos que existen bases.

Observe que $p(x) = x^2 + x + 1$ no tiene raices reales. Por lo tanto si $p(x) = s(x)t(x)$ entonces $deg(s) = 0, deg(t) = 2$ o bien $deg(s) = deg(t) = 1$. Si $deg(s) = deg(t) = 1$, entonces $p(x)$ tiene una raiz en $\mathbb{R}$. Por lo tanto $s(x)$ o $t(x)$ es constante y por lo tanto invertible. Esto nos dice que $p(x)$ es irreducible. Como $A = \mathbb{R}[x]$ es un DIP, se tiene que $(p(x))$ es maximal en $\mathbb{R}[x]$. Por lo tanto $\mathbb{R}[x]/(x^2 + x + 1)$ es cuerpo.

Ayudantía 211: En esta ayudantía, seguiremos estudiando los módulos finitamente generados y los módulos libres.

1.- **Problema 1:** Sea R anillo con $1_R \neq 0_R$ y considere el R-módulo $M = \{f : X \to R : f \text{función}\}$ con la suma y poderación usual de funciones. Pruebe que si $|X| = n$ entonces $M \cong R^n$.

1.- **Demostración:** Supongamos que $|X| = n$. Sea $x_i \in X$ un elemento cualquiera y considere la función $\delta_i : X \to R$ definida por $\delta_i(y) = 1$, si $x_i = y$ y $\delta_i(y) = 0$ en otro caso. Entonces $\beta = \{\delta_i\}_{i=1}^n$ es un subconjunto de M. Demostraremos que este conjunto es una base para M como R-módulo. En efecto, si tomamos una función cualquiera $f : X \to R$ se tiene que $f = \Sigma_{i=1}^n f(x_i)\delta_i$. Por lo tanto β genera M. Supongamos ahora que $\Sigma_{i=1}^n \alpha_i \delta_i = 0$ entonces evaluando en cada punto $x_i \in X$ concluimos que $\alpha_i = 0$. Por lo tanto β es base de M, luego $M \cong R^n$.

2.- **Problema 2:** Considere $M = \mathbb{Q}/\mathbb{Z}$ un $\mathbb{Z}$-módulo con las operaciones usuales en $\mathbb{Q}$ extendidas al cociente.

i.- Pruebe que M no es un $\mathbb{Z}$-módulo finitamente generado.

ii.- Pruebe que M no es un $\mathbb{Z}$-módulo libre.

2.- **Desarrollo:**

i.- Supongamos que existe un conjunto finito $\left\{\overline{\frac{n_i}{m_i}}\right\}_{i=1}^s$ que genera M como $\mathbb{Z}$-módulo. Sea p primo tal que p no divide a ningún $m_i \in \mathbb{N}$. Dicho elemento existe pues $\mathbb{Z}$ es un dominio de factorización única. Considere $x = \overline{\frac{1}{p}} \in M$. Entonces si $x = \Sigma_{i=1}^s \alpha_i \overline{\frac{n_i}{m_i}}$, con $\alpha_i \in \mathbb{Z}$, se tiene que $\Sigma_{i=1}^s \alpha_i \frac{n_i}{m_i} = \frac{1}{p} + r$, con $r \in \mathbb{Z}$ .Luego al multiplicar por $\Pi_{i=1}^s m_i$ obtenemos que $\frac{\Pi_{i=1}^s m_i}{p} \in \mathbb{Z}$. Por lo tanto $p|m_i$, algún i. Esto nos lleva a una contradicción. Luego M no es finitamente generado.

ii.- Supongamos que M es libre, entonces exste una base $\beta = \{x_i\}_{i\in I}$ tal que $M \cong \oplus_{i\in I}\mathbb{Z}x_i$. Supongamos que tenemos un elemento $x = \Sigma_{i\text{fin.}}\alpha_i x_i \in M$ de torsión entonces si $rx = 0$, para $r \neq 0$, tenemos que $\Sigma_{i\text{fin.}} r\alpha_i x_i = 0$. Como los x_i son linealmente independientes se tiene que $r\alpha_i = 0$. Luego como $r \neq 0$ se tiene que $\alpha_i = 0$, para todo i en la suma anterior. Luego $Tor(M) = \{0\}$. Pero claramente si tomamos $y = \overline{\frac{n}{m}} \in M$ se tiene que $my = 0$. Luego $Tor(M) = M$. Esto nos lleva a una contradicción, por lo tanto M no es libre como $\mathbb{Z}$-módulo.

3.- **Problema 3:** Sea M un R-módulo, con R un dominio de integridad.

i.- Pruebe que si M es un módulo de torsión entonces $Hom_R(M, R) = \{0\}$.

ii.- Demuestre que si G es un grupo abeliano finito entonces $Hom_{\mathbb{Z}}(G, \mathbb{Z}) = \{0\}$.

iii.- Concluya que si $M \cong Tor(M) \oplus R^k$ entonces $Hom_R(M) \cong R^k$.

3.- **Demostración:**

i.- Sea $f : M \to R$ es homomorfismo de R-módulos. Como M es de torsión se tiene que para cualquier $m \in M$ existe $r \in R/\{0\}$ tal que $rm = 0$. Luego $0 = f(rm) = rf(m)$. Luego como $r \neq 0$ y R es un dominio de integridad, se tiene que $f(m) = 0$. Luego $f = 0$. Esto concluye lo pedido.

ii.- Basta observar que si G es un grupo abeliano finito de orden n, entonces $n.G = 0$. Luego G es un $\mathbb{Z}$-módulo de torsión. Usando la parte [i] se concluye lo pedido.

iii.- Para demostrar esto usaremos un el siguiente hecho. Si $M \cong M_1 \oplus M_2$ entonces $Hom_R(M,N) \cong Hom_R(M_1,N) \oplus Hom_R(M_2,N)$, su demostración queda de ejercicio. Entonces si $M \cong Tor(M) \oplus R^k$ se tiene que $Hom_R(M) \cong Hom_R(Tor(M),R) \oplus \oplus_{i=1}^{k} Hom_R(R,R)$. Por la parte [i] del ejercicio se tiene que $Hom_R(Tor(M),R) = \{0\}$. Además por el ejercicio 3 de la ayudantía 19 tenemos que $Hom_R(R,R) \cong R$. De estos dos hechos concluimos que $Hom_R(M) \cong R^k$.

3.- **Ejercicio:** Sean M, M_1, M_2 y N módulos sobre R. Si $M \cong M_1 \oplus M_2$ entonces $Hom_R(M,N) \cong Hom_R(M_1,N) \oplus Hom_R(M_2,N)$. [Para su demostración basese en lo demostrado en el problema 4 de la ayudantía 19]

4.- **Problema 4:** Sea $M = \{A \in \mathbb{M}_n(\mathbb{Z}) : A^t = -A\}$ un $\mathbb{Z}$-submódulo de $\mathbb{M}_2(\mathbb{Z})$ y considere $N = \{A \in \mathbb{M}_n(\mathbb{Z}) : A^t = A\}$ otro $\mathbb{Z}$-submódulo. Pruebe que $M \ncong N$.

4.- **Demostración:** Partamos con un par de observaciones. Sea $e_{ij} = (\delta_{ij})$ una matriz elemental cualquiera. Entonces si $A = (a_{ij})_{i,j=1}^{n}$ cumple con $A^t = -A$ se tiene que $a_{ij} = -a_{ji}$, para cualquier i, j. Por ello $a_{ii} = 0$, para cualquier i y además $A = \Sigma_{i<j} a_{ij}(e_{ij} - e_{ji})$. Observe que $\{e_{ij} - e_{ji}\}$ cumple con que $\Sigma_{i<j}\beta_{ij}(e_{ij} - e_{ji}) = 0$ implica que $\beta_{ij} = 0$. Por lo tanto $M = \oplus_{i<j}\mathbb{Z}(e_{ij} - e_{ji})$. Luego $M \cong \mathbb{Z}^r$, donde $r = \frac{n(n-1)}{2}$.

Por otro lado si $A = (a_{ij})_{i,j=1}^{n}$ cumple con $A^t = A$ se tiene que $a_{ij} = a_{ji}$, para cualquier i, j. Por ello $A = \Sigma_{i<j} a_{ij}(e_{ij} + e_{ji}) + \Sigma_{i=1}^{n} a_{ii}e_{ii}$. Observe que $\{e_{ij} + e_{ji}\} \cup \{e_{ii}\}$ cumple con que $\Sigma_{i<j}\beta_{ij}(e_{ij} + e_{ji}) + \Sigma_{i=1}^{n}\beta_{ii}e_{ii} = 0$ implica que $\beta_{ij} = 0$ para todo $i \leq j$. Por lo tanto $M = \oplus_{i<j}\mathbb{Z}(e_{ij} - e_{ji}) \oplus \oplus_{i=1}^{n}\mathbb{Z}e_{ii}$. Luego $M \cong \mathbb{Z}^s$, donde $s = \frac{n(n+1)}{2}$.

Finalmente, comose vió en cátedra, si $M \cong N$ se tiene que $r = s$ y esto para solamente si $n = 0$. Este caso es trivial y por ello no lo consideramos. Luego $M \ncong N$.

Ayudantía 22: En esta ayudantía trabajaremos con el teorema de estructura de módulos finitamente generados sobre DIP.

1.- **Problema 1:**

i.- Encuentre todos los grupos abelianos, salvo isomorfismo, de orden pqr, donde p, q, r son numeros primos distintos.

ii.- Repita lo anterior para grupos abelianos de orden p^2qr.

1.- **Desarrollo:** Partamos hablando de la teoría general. Sabemos que un grupo abeliano finitamente generado siempre es isomorfo a:

$$G \cong \mathbb{Z}^k \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_t\mathbb{Z},$$

donde $k \geq 0$ y $n_{i+1}|n_i$. Dichos valores n_i son los factores invariantes de G y si G es un grupo finito se tiene que $k = 0$ y $n_1 \cdots n_t = |G|$, entonces si $p||G|$ necesariamente $p|n_1$.

i.- Si $|G| = pqr$ entonces $n_1 \cdots n_t = pqr$ y además $n_{i+1}|n_i$. Luego $pqr = n_1$. Por lo tanto:

$$G \cong \mathbb{Z}/pqr\mathbb{Z}.$$

Además $n_1 = pqr$ es el único factor invariante de G.

ii.- Ahora bien si $|G| = p^2qr$ se tiene que $n_1 = pqr$ o bien $n_1 = p^2qr$. En el primer caso $n_2 = p$. Luego:

$$G \cong \mathbb{Z}/p^2qr\mathbb{Z},$$

Con un único factor invariante $n_1 = p^2qr$. Por otro lado, si $n_1 = p^2qr$ entonces:

$$G \cong \mathbb{Z}/pqr\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}.$$

Con dos factores invariantes $n_1 = pqr$ y $n_2 = p$.

2.- **Problema 2:** Encuentre todos los grupos abelianos de orden 72 salvo isomorfismo.

2.- **Desarrollo:** Basta encontrar los factores invariantes de G grupo abeliano de orden $|G| = 72 = 2^3 3^2$.

Por lo visto en el problema 1, tenemos que $2 \cdot 3|n_1$, así tenemos que:

1.- Si $n_1 = 2 \cdot 3$ entonces $n_2 = 2 \cdot 3$ y $n_3 = 2$. Por lo tanto:

$$G \cong \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

2.- Si $n_1 = 2^2 \cdot 3$ entonces $n_2 = 2 \cdot 3$. Por lo tanto:

$$G \cong \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

3.- Si $n_1 = 2^3 \cdot 3$ entonces $n_2 = 3$. Por lo tanto:

$$G \cong \mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}.$$

4.- Si $n_1 = 2 \cdot 3^2$ entonces $n_2 = 2$ y $n_3 = 2$. Por lo tanto:

$$G \cong \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

5.- Si $n_1 = 2^2 \cdot 3^2$ entonces $n_2 = 2$. Por lo tanto:

$$G \cong \mathbb{Z}/36\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

6.- Si $n_1 = 2^3 \cdot 3^2$. Luego:

$$G \cong \mathbb{Z}/72\mathbb{Z}.$$

3.- **Problema 3:** Encuentre todos los $\mathbb{Z}[i]$-módulos M finitamente generados tales que $Ann(M) = ((2+i)^2)$.

3.- **Desarrollo:** Primero observe que si M es un módulo finitamente generado cuya parte libre es no trivial, entonces $Ann(M) = (0)$. Esto se debe a que si $M \cong R^n \oplus Tor(M)$, con $n > 0$, entonces si $a.M = 0$ se tiene que $a.R^n = 0$ y $a.Tor(M) = 0$, pero si $a.(r_1, \cdots r_n) = 0$, con $a \neq 0$ entonces $ar_i = 0, \forall i$. Como A es un DIP, en particular un DI, se tiene que $r_i = 0, \forall i$ y por ende $a.R^n \neq 0$. En particular, en nuestro caso, como M tiene anulador no trivial, se tiene que su parte libre es trivial.

Ahora bien, si $M \cong \oplus_{k=1}^{n} \oplus_{j=1}^{a_k} \mathbb{Z}[i]/(p_k^{e_{kj}})$, donde p es primo en $\mathbb{Z}[i]$ y $e_{k1} \leq \cdots e_{ka_k}$, entonces $(2+i)^2.M = 0$ sí y solamente sí $p_1 = 2+i$, $n = 1$ y $e_{1a_1} = 2$. Esto se debe a que el primo $2+i$ cumple con $p \neq 2+i$ entonces $2+i$ es invertible en $\mathbb{Z}[i]/(p^e)$ y por ello no anula al submódulo $\mathbb{Z}[i]/(p^e)$ y además $Ann(\mathbb{Z}[i]/(2+i)^e) = (2+i)^e$. Por lo tanto:

$$M \cong \oplus_{k=1}^{t} \mathbb{Z}[i]/(2+i) \oplus \oplus_{j=1}^{s} \mathbb{Z}[i]/((2+i)^2),$$

con $s > 0$.

4.- **Problema 4:** Sea $\Lambda \subseteq \mathbb{Q}^n$ un $\mathbb{Z}$-submódulo finitamente generado tal que exite una base $\{f_1, \cdots, f_n\}$ de $\mathbb{Q}^n$ que cumple con $\Lambda \subset \oplus_{i=1}^{n} \mathbb{Z} f_i$. Este tipo de estructura recibe el nombre de $\mathbb{Z}$-**Reticulado**. Pruebe que existe $\{e_1, \cdots, e_m\} \subseteq \Lambda$ tal que $\Lambda = \oplus_{i=1}^{m} \mathbb{Z} e_i$.

4.- **Demostración:** Observe que lo que se desea probar es que el $\mathbb{Z}$-módulo Λ es libre. Para probar esto solo usaremos la hipótesis de que $\Lambda \subset \mathbb{Q}^n$.

En efecto, observe que Λ es un módulo finitamente generado sobre un DIP. Luego Λ es libre sí y sólamente sí es libre de torsión. Mostremos entonces que Λ es libre de torsión. Supongamos que $(a_1, \cdots, a_n) \in \Lambda$ es de torsión, es decir existe $a \in \mathbb{Z} - \{0\}$ tal que $a.(a_1, \cdots, a_n) = 0$. Entonces $(a.a_1, \cdots, a.a_n) = 0$, por lo tanto $a.a_i = aa_i = 0$ en $\mathbb{Q}$. Como $a \neq 0$ se tiene que $a_i = 0, \forall i$, pues en $\mathbb{Q}$ la acción es por multiplicación y $\mathbb{Q}$ es un DI. Luego $(a_1, \cdots, a_n) = 0$ y por lo tanto Λ es libre de torsión. Esto termina la demostración.

Ayudantía 23: En esta ayudantía, haciendo uso de la teoría de módulos finitamente generados sobre DIP, demostraremos el teorema de estructura de Jordan para matrices.

En todo lo que sigue, para K cuerpo, $V = K^n$ y $L : V \to V$ transformación lineal, V es un $K[x]$-módulo vía $x.v = L(v)$.

1.- **Problema 1:** Pruebe que V es un $K[x]$-módulo de torsión finitamente generado.

1.- **Demostración:** Primero mostremos que V es un $K[x]$-módulo de torsión. Considere $v \in V$ un elemento cualquiera y contruyamos el conjunto $\{v, L(v), \cdots, L^n(v)\}$. Observe que este conjunto contiene $n+1$ elementos de un espacio vectorial de dimensión n. Por lo tanto dichos elementos son linealmente dependientes, es decir existen constantes $a_0, a_1, \cdots, a_n$ no todas nulas tales que $a_0 v + a_1 L(v) + \cdots + a_n L^n(v) = 0$, es decir $p(x).v = 0$, para $p(x) = a_0 + a_1 x + \cdots + a_n x^n \neq 0$. Por ende V es un $K[x]$-módulo de torsión.

Ahora probemos que V es finitamente generado. En efecto, sabemos que V tiene base canónica $\{e_i\}_{i=1}^n$ tal que todo elemento $v \in V$ es de la forma $v = a_1 v_1 + \cdots + a_n v_n$. Luego si consideramos los coeficientes $a_i \in K$ como polinomios constantes, se tiene que $v = a_1.v_1 + \cdots + a_n.v_n$. Por ello $\{e_i\}_{i=1}^n$ es un conjunto de generadores de V como $K[x]$-módulo.

2.- **Problema 2:** Supongamos que $K = \mathbb{C}$.

i.- Encuentre todos los elementos primos en $\mathbb{C}[x]$.

ii.- Concluya que $V \cong \oplus_{i=1}^m \oplus_{j=1}^{a_i} \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$, donde $e_{i1} \leq \cdots \leq e_{ia_i}$.

2.- **Desarrollo:**

i.- Sea $p(x)$ un elemento primo en $C[x]$ 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 $x - z = p(x)$ es primo ya que $\mathbb{C}[x]/(x-z) \cong \mathbb{C}$. Dicho isomorfismo se establece vía el homomorfismo evaluación en z.

ii.- Por el teorema de estructura de módulos sobre DIP, tenemos que $V \cong \mathbb{C}[x]^s \oplus_{i=1}^m \oplus_{j=1}^{a_i} \mathbb{C}[x]/(p_i(x))^{e_{ij}})$, donde $e_{i1} \leq \cdots \leq e_{ia_i}$ y $p_i(x)$ es primo en $\mathbb{C}[x]$. Pero como V es un $C[x]$-módulo de torsión, se tiene que $s = 0$. Además por [i] tenemos que $p_i(x) = x - \lambda_i$, para ciertos $\lambda_i \in \mathbb{C}$.

3.- **Problema 3:** Demuestre el teorema de Jordan que da forma canónica a L. Establezca la relación entre la torsión de V y los valores propios de L y el polinomio minimal de L.

3.- **Demostración:** Partamos demostrando el teorema de Jordan. Sabemos que existe $\phi : V \to \oplus_{i=1}^m \oplus_{j=1}^{a_i} \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$ isomorfismo, donde $e_{i1} \leq \cdots \leq e_{ia_i}$. Considere $W_{ij} = \phi^{-1}(\mathbb{C}[x]/((x-\lambda_i)^{e_{ij}}))$. Observe que W_{ij} es un subespacio vectorial de V, pues es un $\mathbb{C}[x]$-submódulo, en particular un $\mathbb{C}$-submódulo. Observe que el isomorfismo ϕ al restringirlo a W_{ij} hace que $W_{ij} \cong \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$. Por lo tanto $Ann(W_{ij}) = Ann(\mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})) = (x-\lambda_i)^{e_{ij}}$. Por lo tanto existe $w = w_{ij} \in W_{ij}$

tal que $(L-\lambda_i I)^{e_{ij}}(w) = (x-\lambda_i)^{e_{ij}}.w = 0$, pero $(L-\lambda_i I)^{e_{ij}-1}(w) = (x-\lambda_i)^{e_{ij}-1}.w \neq 0$.

Observe que el isomorfismo $W_{ij} \cong \mathbb{C}[x]/((x-\lambda_i)^{e_{ij}})$ es como $C[x]$-módulos, en particular como $\mathbb{C}$-módulo. En particular:

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

Considere el conjunto $\beta = \{w, N(w), \cdots, N^{e_{ij}-1}(w)\cdots\} \subset W_{ij}$, donde $N = L - \lambda_i I$. 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 $a_0 = 0$, si luego aplicamos $N^{e_{ij}-2}$ a la suma resultante se obtiene que $a_1 = 0$ y así inductivamente deducimos que $a_i = 0$, $\forall i$. Luego β es un conjunto linealmente independiente de W_{ij}. Como tiene la cantidad correcta de elementos, de tiene 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 $L = N + \lambda_i I$ se ve como una matriz:

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

Si tomamos por base de V a la unión de las bases de los subespacios W_{ij}, en esta base L tiene forma de Jordan. Observe que los polinomios primos lineales determinan los valores propios de L. Además se tiene que $min_L(x) = \sqcap_{i=1}^{n}(x-\lambda_i)^{e_{ia_i}}$, pues la potencia e_{ia_i} es la minima tal que cada bloque, asociado al autovalor λ_i, se anula.

3.- **Ejercicio:** Pruebe que $dim_K K[x]/(q(x)) = deg(q(x))$, para cualquier $q(x) \in K[x]$, con K cuerpo.

3.- **Ejercicio:** Escriba $[L] = [N] + [D]$, con $[N]$ nilpotente (es decir $[N]^t = 0$, para cierto $t \in \mathbb{N}$) y $[D]$ diagonal. Demuestre que $[N][D] = [D][N]$.

4.- **Problema 4:** Sea $A \in \mathbb{M}_n(K)$ matriz idempotente, es decir $A^2 = A$. Pruebe que existe una matriz U invertible tal que $UAU^{-1} = D$, donde D es una matriz diagonal con 0 y 1 es su diagonal.

4.- **Demostración:** Recordemos que $M = K^n$ es un $K[x]$-módulo con $x.v = A(v)$. Observe que $A^2(v) - A(v) = 0$, es decir $x(x-1) = x^2 - x \in Ann_{K[x]}(M) = (s(x))$. Observe que si $A = I$ o $A = 0$ entonces tomamos $U = id$ y tenemos lo pedido. Por otro si A es un idempotente no trivial como $x(x-1) = x^2 - x = s(x)t(x)$. Por la factorización única en $K[x]$ se tiene que $s(x) = x$, $s(x) = x-1$ o $s(x) = x^2 - x$. Como $A \neq 0, I$ tenemos que $Ann_{K[x]}(M) = (x^2 - x)$. Luego por el teorema de estructura de módulos sobre DIP, se tiene que $M \cong \oplus_{i=1}^{n} K[x]/((x-1)^{e_i}) \oplus$

$\oplus_{j=1}^{m} K[x]/((x-1)^{f_j})$. Sabemos que $(x(x-1)) = Ann_{K[x]}(M)$, pero como $Ann(M) = Ann\left(\oplus_{i=1}^{n} K[x]/((x-1)^{e_i}) \oplus \oplus_{j=1}^{m} K[x]/((x-1)^{f_j})\right)$, se tiene que $Ann(M) = \cap_{i=1}^{n}(x-1)^{e_i} \cap \cap_{j=1}^{m}(x)^{f_j}$, así obtenemos que $e_i = f_j = 1$.

Usando lo expuesto en el problema 3 se tiene que cada bloque nipotente, asociado al autovalor 1 o 0 tiene dimensión 1. Por lo tanto en alguna base $[A] = D$, con D diagonal con ceros y unos en su diagonal. Tomando la matriz cambio de base se concluye.

Ayudantía 24: En esta ayudantía, hablaremos acerca de modulos finitamente generados sobre DIP. Utilizaremos tecnicas, como la reducción matricial vía operaciones filas y comunas, para entender de mejor manera dichos módulos.

1.- **Problema 1:** Considere la matriz $A \in \mathbb{M}_n(\mathbb{Z})$ definida por:

$$A = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & & & \\ n-2 & 0 & \cdots & 1 & 0 & 0 \\ n-1 & 0 & \cdots & 0 & p & 0 \end{bmatrix},$$

donde $p \in \mathbb{Z}$ es un entero primo. Muestre que el $\mathbb{Z}$-módulo $M = \mathbb{Z}^n/Im(A)$ es un irreducible, es decir sus únicos submódulos son $\{0\}$ y M.

1.- **Demostración:** En clases se demostró que si aplicamos operaciones filas enteras y operaciones columnas enteras a A ontendremos una matriz tal que al cocientar $\mathbb{Z}^n$ por el submódulo imagen es igual a $\mathbb{Z}^n/Im(A)$. Apliquemos dichas operaciones a la matriz A. Si intercambiamos la ultima columna por la primera obtenemos que:

$$A \equiv \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 2 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & n-2 & 0 & \cdots & 1 & 0 \\ 0 & n-1 & 0 & \cdots & 0 & p \end{bmatrix},$$

Restando la i veces la segunda fila a la i-ésima fila obtenemos que:

$$A \equiv \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & & & & & \\ 0 & 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & p \end{bmatrix}.$$

Luego $\mathbb{Z}^n/Im(A) \cong \mathbb{Z}^n/(\mathbb{Z}^{n-1} \times p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$. Observe que todo $\mathbb{Z}$-submódulo de M es un ideal de $\mathbb{Z}/p\mathbb{Z}$. Por lo tanto los únicos submódulos de M son $\{0\}$ y M. Es por esto que M es irreducible.

2.- **Problema 2:** Considere $N = \{(a, b, c) : a + 2b \in 5\mathbb{Z},\ 2a + b \in 3\mathbb{Z}\}$ un $\mathbb{Z}$-submódulo de $\mathbb{Z}^3$.

i.- Pruebe que N es un $\mathbb{Z}$-módulo libre de rango 3.

ii.- Calcule el cociente $\mathbb{Z}^3/N$.

2.- **Desarrollo:**

i.- Utilicemos el algoritmo que se desprende de la demostración de que todo submódulo de un módulo libre sobre un DIP es libre (Por eso mismo N es un módulo libre). En efecto hay que encontrar un elemento en N tal que su

última coordenada genere el ideal imagen por la proyección, luego intersectar el submódulo por el nucleo de la proyección y seguir el prodecimiento inductivamente con la proyección a la i-ésima coordenada. Apliquemos esto. Considere $(0,0,1) \in N$ entonces $\pi_3(0,0,1) = 1$, por lo tanto el ideal que genera es todo el anillo. Luego $(0,0,1)$ es un elemento de la base. Luego $N_2 = N \cap \ker(\pi_3) = \{(a,b,0) : a+2b \in 5\mathbb{Z},\ 2a+b \in 3\mathbb{Z}\}$. Observe que $(13,1,0) \in N_2$. Luego $\pi_2(13,1,0) = 1$ genera todo el anillo $\mathbb{Z}$ al tomar ponderaciones del vector. Por lo tanto es otro elemento de la imagen. Por último $N_3 = N \cap \ker(\pi_2) = \{(a,0,0) : a \in 5\mathbb{Z},\ 2a \in 3\mathbb{Z}\}$. Luego si $(a,0,0) \in N_3$ se tiene que $5|a$ y $3|a$, por lo tanto $15|a$. Luego $a = 15$ es el elemento menor que cumple con esto. Así $(15,0,0)$ es el tercer elemento de la base. Esto muestra que el módulo $N = \mathbb{Z}(15,0,0) \oplus \mathbb{Z}(13,1,0) \oplus \mathbb{Z}(0,0,1)$. Luego N es un módulo libre de rango 3.

ii.- Para calcular el cociente observe que la última coordenada de $\mathbb{Z}^3$ se anula al cocientar por N , pues $(0,0,1) \in N$. Luego basta reducir la matriz $T = \begin{bmatrix} 13 & 15 \\ 1 & 0 \end{bmatrix}$. Observe que si restamos 13-veces la segunda fila a la primera obtenemos que $T \equiv \begin{bmatrix} 0 & 15 \\ 1 & 0 \end{bmatrix}$. Luego $\mathbb{Z}^3/N \cong \mathbb{Z}/15\mathbb{Z}$.

3.- **Problema 3:** Considere el $\mathbb{Z}[i]$-módulo:

$$N = \{(a,b) : a+2b \in (2+i),\ a+b \in (3+i)\}.$$

i.- Pruebe que $N \cong \mathbb{Z}[i]^2$.
ii.- Calcule el cociente $\mathbb{Z}[i]^2/N$.

3.- **Demostración:**
i.- Apliquemos lo mismo que se dijo en el problema 3. En efecto $(4+i,-1) \in N$ cumple con $\pi_2(4+i.-1) = -1$ generador de todo el anillo. Por lo tanto $(4+i,-1)$ es un elemento de la base. Luego $N_2 = N \cap \ker(\pi_2) = \{(a,0) : a \in (2+i),\ a \in (3+i)\}$. Observe que $1 = 3+i-(2+i)$, por lo tanto $\mathbb{Z}[i] = (2+i)+(3+i)$ como ideales. Luego $(3+i)(2+i) = (7+5i)$ como ideales. Por lo tanto $(a,0) \in N_2$ si y solamente si $a \in (7+5i)$. Luego $(0,7+5i)$ es otro elemento de la base de N. Por lo tanto $N = \mathbb{Z}[i](4+i,-1) \oplus \mathbb{Z}[i](0,7+5i)$. Luego $N \cong \mathbb{Z}[i]$.

ii.- Para calcular dicho cociente basta aplicar operaciones filas y columnas enteras a la matriz $T = \begin{bmatrix} 7+5i & 4+i \\ 0 & -1 \end{bmatrix}$. Observe que si sumamos $4+i$-veces la segunda fila a la primera obtenemos que $T \equiv \begin{bmatrix} 7+5i & 0 \\ 0 & -1 \end{bmatrix}$. Por lo tanto $\mathbb{Z}[i]^2/N \cong \mathbb{Z}[i]/(7+5i)$. Por teorema chino de los restos, como $(3+i)(2+i) = (7+5i)$ y $\mathbb{Z}[i] = (2+i)+(3+i)$ se tiene que $\mathbb{Z}[i]/(7+5i) \cong \mathbb{Z}[i]/(2+i) \times \mathbb{Z}[i]/(3+i) \cong \mathbb{Z}/(5) \times \mathbb{Z}/(10)$. Esto pues $\mathbb{Z}[i]/(3+i) \cong \mathbb{Z}[x]/(x^2+1, x+3) \cong \mathbb{Z}/(10)$ y $\mathbb{Z}[i]/(2+i) \cong \mathbb{Z}[x]/(x^2+1, x+2) \cong \mathbb{Z}/(5)$. Por lo tanto $\mathbb{Z}[i]^2/N \cong \mathbb{Z}/(5) \times \mathbb{Z}/(10)$.

4.- **Problema 4:** Demuestre que el grupo abeliano $A = \langle a,b : a+b = 0,\ 5a+2b = 0,\ 10a+b = 0\rangle$ es un grupo cíclico.

4.- **Demostración:** Basta observar que $a = -b$. Luego el grupo está generado solamente por a y las ecuaciones que lo definen se reescriben como:

$$A = \langle a : 3a = 0,\ 9a = 0\rangle = \langle a : 3a = 0\rangle.$$

Por lo tanto $A \cong \mathbb{Z}/3\mathbb{Z}$.