FACULTAD DE
CIENCIAS
UNIVERSIDAD DE CHILE

Apuntes de Ayudantía

ESTRUCTURAS ALGEBRAICAS

Claudio Bravo Castillo
December 28, 2016

Contents

AYUDANTÍAS ESTRUCTURAS ALGEBRAICAS

ESTRUCTURAS ALGEBRAICAS (PRIMAVERA 2016)

1. Grupos

Ayudantía I: En esta ayudantía comenzaremos a trabajar con la estructura algebráica de grupo. Estudiaremos el orden de algunos elementos de ciertos grupos.

1.- **Problema 1:**
Sea $G = \{z \in \mathbb{C} : z^n = 1 \text{ algún } n \in \mathbb{Z}\}$.

i.- Pruebe que G es un grupo con la multiplicación en $\mathbb{C}$.

ii.- Demuestre que G no es un grupo aditivo.

Desarrollo:

i.- Observe que G es un subconjunto del grupo $(\mathbb{C}^*, \cdot)$. Luego, para demostrar lo pedido, basta probar que G es subgrupo de $(\mathbb{C}^*, \cdot)$. En efecto, si $z, t \in G$ entonces $(zt)^n = z^n t^n = 1$ y $(z^{-1})^n = (z^n)^{-1} = 1$. Por lo tanto $zt, z^{-1} \in G$. Luego G es un grupo.

ii.- Observe que $i^4 = 1$ y $(-i)^4 = 1$. Si G fuera un subgrupo con la suma entonces $i + -i = 0 \in G$. Pero $0^n = 0 \neq 1$, para todo $n \in \mathbb{Z}$. Luego G no es un grupo con la suma de $\mathbb{C}$.

1.- **Ejercicio:** Pruebe que $G = \{z \in \mathbb{C} : z^n = 1 \text{ algún } n \in \mathbb{Z}\}$ es un grupo contenido estrictamente en $K = \{z \in \mathbb{C} : |z| = 1\}$.

2.- **Problema 2:**
Sea G grupo tal que $x^2 = 1$, para todo $x \in G$. Pruebe que G es abeliano.

Demostración: Considere $x, y \in G$. Entonces $(xy)^2 = 1 = x^2y^2$. Pero $(xy)^2 = xyxy$. Luego $xyxy = x^2y^2$. Multiplicando la igualdad anterior por x^{-1} a la izquierda y por y^{-1} a a derecha, deducimos que $yx = xy$. Luego G es un grupo abeliano.

3.- **Problema 3:**
Encuentre un elemento de orden 6 en $G = (\mathbb{Z}/7\mathbb{Z})^*$. Concluya que G es un grupo cíclico.

Demostración: Debemos encontrar un elemento $x \in \mathbb{Z}/7\mathbb{Z}$ tal que $x^6 \equiv 1(mod\ 7)$. Observe que como 7 es primo se tiene que $\mathbb{Z}/7\mathbb{Z}$ es cuerpo. Luego $(\mathbb{Z}/7\mathbb{Z})^* = (\mathbb{Z}/7\mathbb{Z}) - \{0\}$. Encontremos el orden de algunos elementos de G. En efecto $|1| = 1$ y $|-1| = 2$. Por otro lado $2^3 \equiv 1(mod\ 7)$. Por ello $|2| = 3$. Luego $(-2)^3 \equiv -1(mod\ 7)$. Por lo tanto $2^6 \equiv 1(mod\ 7)$ y sus potencias menores no son uno en el grupo. Por ello $x = 2$ cumple lo pedido. Observe además que $\langle x \rangle$ es un subgrupo de G, donde $|G| = |\,(\mathbb{Z}/7\mathbb{Z}) - 0\}| = 6$. Por ello $G = \langle x \rangle$. Luego G es un grupo cíclico.

3.- **Ejercicio:** Demuestre que $G = (\mathbb{Z}/13\mathbb{Z})^*$ es un grupo cíclico. Encuentre un generador de G.

4.- **Problema 4:**
Sea G grupo de orden par. Pruebe que G tiene un elemento de orden 2.

Demostración: Considere el conjunto $t(G) = \{g \in G : g^{-1} \neq g\}$. Observe que $x \in t(G)$ si y solamente si $x^{-1} \in t(G)$. Luego por cada elemento de G módulo inverso, tenemos dos elementos en G. Así $t(G)$ tiene un número par de elementos. Luego como $e \notin t(G)$, tenemos que existe $x \in G - t(G)$ con $x \neq e$. Es decir, tenemos un elemento no trivial tal que $x^{-1} = x$. Luego $|x| = 2$.

4.- **Ejercicio:** Asumiendo que $G = Gl_2(\mathbb{Z}/2\mathbb{Z})$ tiene 6 elementos, encuentre un elemento de orden 2 en G.

5.- **Problema 5:**
Sea $Gl_2(\mathbb{Z}/p\mathbb{Z}) = \{A \in \mathbb{M}_2(\mathbb{Z}/p\mathbb{Z}) : det(A) \neq 0\}$.

i.- Pruebe que G es grupo.

ii.- Determine el orden de $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ en $Gl_2(\mathbb{Z}/p\mathbb{Z})$.

Desarrollo:

i.- Por la asociatividad de las matrices tenemos que $A(BC) = (AB)C$, para cualquier $A, B, C \in G$. Por otro lado, si $det(A), det(B) \neq 0$ entonces $det(AB) = det(A)det(B) \neq 0$, por ello $AB \in G$. Además $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in G$ cumple con $AI = IA = A$, para todo $A \in G$. Por último si $det(A) \neq 0$ entonces existe A^{-1} tal que $AA^{-1} = A^{-1}A = I$ y $det(A^{-1}) = det(A)^{-1} \neq 0$. Por ello G es grupo.

ii.- Observe que $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ para todo $n \in \mathbb{N}$. Luego $A^n = I$ si y solamente si $n = ps$, algún $s \in \mathbb{N}$. Por lo tanto $n = p$ es la menor potencia tal que $A^n = I$. Por ello $|A| = p$.

5.- **Ejercicio:** Determine el orden de $A = \begin{pmatrix} 1 & 1 \\ 0 & p-1 \end{pmatrix}$ en $Gl_2(\mathbb{Z}/p\mathbb{Z})$.

Ayudantía II: En esta ayudantía estudiaremos los homomorfismos de grupos y trabajaremos con el primer teorema de isomorfía.

1.- **Problema 1:**
Sea $G = Gl_n(F)$ grupo de matrices invertibles con coeficientes sobre el cuerpo F.

i.- Pruebe que G es finito si y solamente si F es finito. Si G es finito calcule su orden en términos de la cantidad de elementos de F.

ii.- Demuestre que $det : G \to F^*$ es un homomorfismo de grupos. Pruebe que $Sl_n(F) = \{A \in Gl_n(F) : det(A) = 1\}$ es un subgrupo normal de G.

iii.- Concluya que $Gl_n(F)/Sl_n(F) \cong F^*$.

Desarrollo:

i.- Supongamos que F no es finito. Entonces en $Gl_n(F)$ existen infinitas matrices que en base canónica cumplen con $Ae_1 = fe_1$ y $Ae_i = e_i$, para $i \neq 1$ y $f \in F^*$ cualquiera. Recíprocamente, si F es finito, entonces $|\mathbb{M}_n(F)| = |F|^{n^2}$. Luego $|Gl_n(F)| \leq |F|^{n^2} < \infty$.

Supongamos ahora que F es finito y digamos que $|F| = q$. Entonces para la primera columna de una matriz cuaquiera en $Gl_n(F)$ tenemos $q^n - 1$ posibilidades. Esto se debe a que el la primera columna podemos poner cualquier vector de F^n salvo el nulo. Para la segunda columna podemos considerar cualquier vector salvo los múltiplos de la primera columna. Por ello tenemos $q^n - q$ posibilidades. Para la tercera columna podemos considerar cualquier vector salvo las combinaciones lineales de las primeras dos. En general en la columna $i + 1$podemos considerar cualquier vector salvo las combinaciones lineales de las i primeras. Luego para la columna $i + 1$ tenemos $q^n - q^i$ posibilidades. De esto se sigue que $|Gl_n(F)| = (q^n - 1) \cdots (q^n - q^i) \cdots (q^n - q^{n-1})$.

ii.- Considere $det : Gl_n(F) \to F^*$ función bien definida pues una matriz es invertible si y solamente si su determinante es no nulo. Por otro lado $det(AB) = det(A)det(B)$ y $det(A^{-1}) = det(A)^{-1}$. Por ello det es un homomorfismo de grupos. Observe que $\ker(det) = Sl_n(F)$. Por ello $Sl_n(F) \triangleleft Gl_n(F)$.

iii.- Si consideramos las matrices que en base canónica cumplen con $Ae_1 = fe_1$ y $Ae_i = e_i$, para $i \neq 1$ y $f \in F^*$ cualquiera, tenemos que $Im(det) = F^*$. Por el primer teorema de isomorfía concluimos que $Gl_n(F)/Sl_n(F) \cong F^*$.

2.- **Problema 2:**
Considere K un grupo cualquiera, se define $Aut(K) = \{\phi : K \to K : \phi \text{ isomorfismo }\}$. Calcule $G = Aut((\mathbb{Z}, +))$.

Desarrollo: Considere $\phi : \mathbb{Z} \to \mathbb{Z}$ un homomorfismo de grupos. Entonces $\phi(n) = n\phi(1)$. Por lo tanto $\phi(1)$ deterina el homomorfismo ϕ. Observe que $Im(\phi) = \phi(1)\mathbb{Z}$. Luego, como ϕ es sobreyectivo, tenemos que $Im(\phi) = \phi(1)\mathbb{Z} = \mathbb{Z}$. En particular $1 \in \phi(1)s$, para cierto $s \in \mathbb{Z}$. Por ello $\phi(1) = 1$ o $\phi(1) = -1$. De esto se sigue que $Aut(\mathbb{Z}) = \{id, -id\}$. Es decir $Aut(\mathbb{Z}) = C_2$.

2.- **Ejercicio:** Sea K un grupo. Pruebe que $Aut(K)$ es un grupo con la composición.

2.- **Ejercicio:** Sea $K = C_p$ un grupo cíclico con p elementos. Calcule $Aut(K)$.

3.- **Problema 3:**
Sea $\phi : G \to G$ función tal que $\phi(g) = g^2$. Pruebe que ϕ es homomorfismo si y solamente si G es abeliano.

Demostración: Supongamos que G es un grupo abeliano, entonces $\phi(ab) = (ab)^2 = abab = a^2b^2$. Luego $\phi(ab) = \phi(a)\phi(b)$. Por otro lado siempre $\phi(a^{-1}) = a^{-2} = \phi(a)^{-1}$. Esto prueba que ϕ es homomorfismo de grupos. Recíprocamente, si ϕ es homomorfismo de gurpos, entonces para cualquier $a, b \in G$ tenemos que $\phi(ab) = \phi(a)\phi(b)$. Es así como obtenemos que $abab = a^2b^2$. Luego $ba = ab$. Por ello G es un grupo abeliano.

4.- **Problema 4:**
Sea $\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$. Sea $\phi : \mathbb{R} \to \mathbb{S}^1$ la función definida por $\phi(r) = e^{2\pi ir}$.

i.- Pruebe que ϕ es homomorfismo de grupos y describa $\ker(\phi)$.

ii.- Pruebe que $\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$.

iii.- Calcule la fibra sobre $i \in \mathbb{S}^1$, es decir determine $\{x \in \mathbb{R} : \phi(x) = i\}$.

Desarrollo:

i.- Partamos por demostras que ϕ es un homomorfismo de grupos. En efecto, tenemos que $\phi(r+s) = e^{2\pi i(r+s)} = e^{2\pi ir}e^{2\pi is}$. Por lo tanto $\phi(r+s) = \phi(r)\phi(s)$. Además ϕ cumple con $\phi(-r) = e^{-2\pi ir} = \phi(r)^{-1}$. Por lo tanto ϕ es homomorfismo de grupos. Por otro lado $\ker(\phi) = \{r \in \mathbb{Z} : e^{2\pi ir} = 1\}$. Pero $e^{2\pi ir} = 1$ si y solamente si $r \in \mathbb{Z}$. Por lo tanto $\ker(\phi) = \mathbb{Z}$.

ii.- Observe que ϕ es una función sobreyectiva, debido a que todo $z \in \mathbb{C}$ tal que $|z| = 1$ cumple con $z = e^{2\pi ir}$, para cierto $r \in [0, 1[$. Luego, aplicando el primer teorema de isomorfía, tenemos que $\mathbb{S}^1 \cong \mathbb{R}/\mathbb{Z}$.

iii.- Supongamos que $e^{2\pi ir} = i = e^{\frac{\pi i}{2}}$. Entonces $r - \frac{1}{4} \in \ker(\phi) = \mathbb{Z}$. Por ende $\{x \in \mathbb{R} : \phi(x) = i\} = \{n + \frac{1}{4} : n \in \mathbb{Z}\}$.

5.- **Problema 5:**
Sea $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \in F^*, b \in F \right\}$. Sea $\phi : G \to F^* \times F^*$ la función definida por $\phi \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c)$.

i.- Pruebe que ϕ es homomorfismo de grupos y calcule $\ker(\phi)$.

ii.- Pruebe que $\ker(\phi) \cong (F, +)$.

Desarrollo:

i.- Demostremos que ϕ es homomorfismo de grupos. Sea $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ y $B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$. Entonces $A^{-1} = \begin{pmatrix} a^{-1} & -ba^{-1}c^{-1} \\ 0 & c^{-1} \end{pmatrix}$. Luego $\phi(A^{-1}) = (a^{-1}, c^{-1}) = \phi(A)^{-1}$. Además $AB = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}$. Por lo tanto $\phi(AB) = (ax, cz) = \phi(A)\phi(B)$. De esto se sigue que ϕ es un homomorfismo de grupos. Calculemos ahora el núcleo de dicho homomorfismo. En efecto $\ker(\phi) = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in F \right\}$.

ii.- Sea $H = \ker(\phi)$ y considere la función $\varphi : H \to F$ definida por $\varphi \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = b$. Observe el inverso de una matriz cualquiera $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$ es $A^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$. Por lo tanto $\varphi(A^{-1}) = -\varphi(A)$. Por otro lado el producto de dos matrices $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$, $C = \begin{pmatrix} 1 & d \\ 0 & 1 \end{pmatrix} \in H$ es $AC = \begin{pmatrix} 1 & b+d \\ 0 & 1 \end{pmatrix} \in H$. Por ello $\varphi(AC) = \varphi(A) + \varphi(C)$. Luego ϕ es un homomorfismo. Este homomorfismo tiene por núcleo al subgrupo $\ker(\varphi) = \{id\}$ y es claramente sobreyectivo. Por lo tanto φ es un isomorfismo de H con F. Esto concluye lo pedido.

Ayudantía III: En esta ayudantía estudiaremos ciertos subgrupos normales y calcularemos algunos cocientes de grupos.

1.- **Problema 1:**
Sea G grupo y considere $D = \{(g,g) \in G \times G\}$ subrgupo diagonal de $G \times G$.

i.- Pruebe que D no es un subgrupo normal de $G \times G$, si G no es un grupo abeliano.

ii.- Pruebe que $H = \{e\} \times G$ es un subrgupo normal de G

ii.- Demuestre que G es isomorfo a D y a H.

Desarrollo:

i.- Sea $g \in G$ elemento no conmutativo, es decir existe $h \in G$ tal que $g \neq hgh^{-1}$. Considere $(g,g) \in D$. Entonces $(e,h) \in G \times G$ cumple con $(e,h)(g,g)(e,h)^{-1} = (g, hgh^{-1}) \notin D$. Por ello D no es un subgrupo normal de $G \times G$.

ii.- Considere $(e,g) \in H$ y $(t,s) \in G \times G$ un elemento cuaquiera. Entonces $(t,s)(e,g)(t^{-1},s^{-1}) = (e, sgs^{-1}) \in H$. Por lo tanto H es un subgrupo normal de $G \times G$.

iii.- Considere $\pi : H \to G$ la función definida por $\pi(e,g) = g$. Claramente π es un homomorfismode grupos biyectivo. Por ende es isomorfismo. Por otro lado, si consideramos $\rho : D \to$ la función definida por $\rho(g,g) = g$, tenemos un homomorfismo de grupos biyectivo también. Por ende D es isomorfo a G. Esto prueba que un grupo puede ser isomorfo a varios subgrupos de otra cierta estructura, en donde los grupos imagen pueden no ser normales.

2.- **Problema 2:**
Sea $D_{2n} = \langle r, s : r^n = s^2 = 1, rs = sr^{-1} \rangle$ grupo dihedral.

i.- Pruebe que todo elemento de D_{2n} es de la forma $s^\epsilon r^i$, donde $\epsilon = 0, 1$ y $s = 0, \cdots, n-1$.

ii.- Pruebe que $\langle r \rangle \triangleleft D_{2n}$.

iii.- Pruebe que $D_{2n}/\langle r \rangle$ es un grupo cíclico con dos elementos

Desarrollo:

i.- Considere un elemento cualquiera $g \in D_{2n}$. Entonces por la relación $rs = sr^{-1}$ podemos dejar todas las potencias de s a la izquierda de la expresión de g y las potencias de r a la derecha. Luego $g = s^m r^i$. Pero, como $s^2 = 1$ y $r^n = 1$, tenemos que $g = s^\epsilon r^i$, con $s^\epsilon r^i$, donde $\epsilon = 0, 1$ y $s = 0, \cdots, n-1$.

ii.- Considere $r^i \in \langle r \rangle$ elemento cualquiera. Entonces $sr^j r^i (sr^j)^{-1} = sr^i s^{-1} = r^{-i} \in \langle r \rangle$. Por lo tanto $\langle r \rangle \triangleleft D_{2n}$.

iii.- Observe que $G = D_{2n}/\langle r \rangle$ es un grupo pues $\langle r \rangle$ es un subgrupo normal de D_{2n}. Además sabemos que $|G| = |D_{2n}|/|\langle r \rangle| = 2$. Por lo tanto G es un grupo cíclico.

3.- **Problema 3:**
Se define el *centro* de un grupo G como $Z(G) = \{g \in G : gx = xg, \ \forall x \in G\}$. Pruebe que $Z(G)$ es un subgrupo de G

Demostración: Observe que siempre $e \in Z(G)$. Además si $g, t \in Z(G)$ entonces $tgx = txg = xtg$, para todo $x \in G$. Por ello $tg \in Z(G)$. Por otro

lado $gx = xg$ implica que $xg^{-1} = g^{-1}x$. Por lo tanto $g \in Z(G)$ implica que $g^{-1} \in Z(G)$. De esto se sigue que $Z(G)$ es un subgrupo de G.

3.- **Ejercicio:** Definimos el *normalizador* de un subgrupo H de G por $N_G(H) = \{g \in G : gHg^{-1} = H\}$. Pruebe que $H \subset N_G(H)$ y que $N_G(H)$ es el máximo subgrupo de G, respecto a la inclusión, en donde H es un subgrupo normal.

3.- **Problema 3:**
Pruebe que $Z(G) \triangleleft G$. Demuestre además que $G/Z(G)$ es isomorfo a un subgrupo de $Aut(G)$.

Demostración: Considere la función $\theta : G \to Aut(G)$ definida por $\theta(g)(h) = ghg^{-1}$. Observe que θ está bien definida pues $\theta(g)$ es un automorfismo de G. $\theta(h)$ es un homomorfismo, ya que $\theta(g)(hk) = ghkg^{-1} = (ghg^{-1})(gkg^{-1})$ y $\theta(g)(h^{-1}) = gh^{-1}g^{-1} = \theta(g)(h)^{-1}$. Además es invertible pues $\theta(g)^{-1} = \theta(g^{-1})$. Además θ es un homomorfismo ya que $\theta(g) \circ \theta(g')(h) = \theta(g)(g'hg'^{-1}) = gg'h(gg')^{-1} = \theta(gg')(h)$, para todo $h \in G$. Es decir $\theta(g) \circ \theta(g') = \theta(gg')$. Por otro lado $\ker(\theta) = \{g \in G : ghg^{-1} = h\} = Z(G)$. Por lo tanto $Z(G) \triangleleft G$. Luego, por el primer teorema de isomorfía, tenemos que $G/Z(G)$ es isomorfo a un subgrupo de $Aut(G)$.

4.- **Problema 4:**
Calcule $Z(D_6)$, $Z(D_8)$ y $Z(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$.

Desarollo: Partamos analizando el centro de $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Observe que G es u grupo abeliano. Por lo tanto $Z(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ahora analicemos el centro de un grupo dihedral $G = D_{2n}$ para $n \geq 3$. Entonces un elemento $s^\epsilon r^i \in Z(D_{2n})$ si y solamente si conmuta con r y s. Observe que $rsr^ir^{-1} = sr^{i-2}$. Luego si $sr^i \in Z(D_{2n})$, tenemos que $sr^{i-2} = sr^i$. Por lo tanto $r^2 = 1$. Esto nos lleva a una contradicción. Por otro lado r^i conmuta con r, pero $sr^is^{-1} = r^{-i}$. Por lo tanto $r^i \in Z(G)$ si y solamente si $2i \equiv 0(mod\ n)$. Luego, si n es impar tenemos que $Z(G) = \{1\}$ y si $n = 2t$ es par, entonces $Z(G) = \{1, r^t\}$. Por lo tanto $Z(D_8) = \{1, r^4\}$ y $Z(D_6) = \{1\}$.

4.- **Ejercicio:** Calcule $Z(S_3)$ y $Z(S_4)$.

5.- **Problema 5:**
Sea G grupo de orden $|G| = p^n s$, donde $(p, s) = 1$. Suponga que en G existe un único subgrupo H de orden p^n. Pruebe que $H \triangleleft G$.

Demostración: Basta probar que para todo $g \in G$ se tiene que $gHg^{-1} = H$. En efecto, considere el subgrupo gHg^{-1} de G. Como la conjugación por un elemento del grupo es un automorfismo, tenemos que $|gHg^{-1}| = |H|$. Luego como G tiene un único grupo de orden p^n, tenemos que $gHg^{-1} = H$. Por lo tanto $H \triangleleft G$.

5.- **Ejercicio:** Demuestre que $A_3 = \{id, (123), (132)\}$ es un subrgupo normal de S_3.

Ayudantía IV: En esta ayudantía trabajaremos con el teorema de Lagrange. En todo lo que sigue usaremos el hecho de que en $\mathbb{Z}$ dos números son relativamente primos si y solamente si existe una combinación lineal entera de dichos números que da una unidad de $\mathbb{Z}$. Este hecho, por lo general, se demuestra en un curso de álgebra de primer año.

1.- **Problema 1:**
Sea G grupo tal que $|G| = p$ primo.

i.- Sea $x \in G - \{e\}$. Pruebe que $\langle x \rangle = G$.

ii.- Concluya que los únicos subgrupos de G son $\{e\}$ y G.

Desarrollo:

i.- Sea $x \in G$ un elemento no trivial. Entonces, por el teorema de Lagrange, $|x|$ divide a $|G|$. Como $|G| = p$ primo, tenemos que $|x| = 1$ o $|x| = p$. Si $|x| = 1$ entonces $x = e$ y esto no puede pasar pues x no es trivial. Luego $|x| = p$. Por lo tanto $\langle x \rangle \subset G$ tiene la misma cantidad de elementos que todo el grupo. Luego $\langle x \rangle = G$.

ii.- Supongamos que H es un sugrupo de G no trivial. Entonces existe $x \in H$ con $x \neq e$. Luego por [i] tenemos que $G = \langle x \rangle \subset H \subset G$. De esto concluimos que $H = G$.

1.- **Ejercicio:** Encuentre todos los generadores del grupo $G = \{x \in (\mathbb{Z}/7\mathbb{Z})^* : x^3 = 1\}$.

2.- **Problema 2:**
Sea $G = (\mathbb{Z}/n\mathbb{Z})^*$ y $\varphi(n) = |\{i : (i, n) = 1,\ i \leq n\}|$.

i.- Demuestre que $|G| = \varphi(n)$.

ii.- Pruebe que para todo $a \in \mathbb{Z}$ tal que $(a, n) = 1$ se tiene que $a^{\varphi(n)} \equiv 1(mod\ n)$.

iii.- Concluya que para todo $a \in \mathbb{Z}$ se tiene que $a^p \equiv a(mod\ p)$.

Desarrollo:

i.- Por definición G es el grupo de todos los elementos invertibles en $\mathbb{Z}/n\mathbb{Z}$. Supongamos que $\overline{i} \in \mathbb{Z}/n\mathbb{Z}$ es invertible. Entonces, sín pérdida de generalidad, podemos asumir que $i \leq n$. Luego, como existe $s \in \mathbb{Z}/n\mathbb{Z}$ tal que $is \equiv 1(mod\ n)$ tenemos que existe $t \in \mathbb{Z}$ tal que $is + tn = 1$. Por lo tanto $(i, n) = 1$. Por otro lado si tomamos la clase de un elemento $i \leq n$ tal que $(i, n) = 1$ tenemos que $\overline{is} + \overline{nt} = \overline{1}$. Por lo tanto $\overline{is} = 1$. Luego i es invertible en $\mathbb{Z}/n\mathbb{Z}$. DE esto concluimos que $|G| = \varphi(n)$.

ii.- Considere $a \in \mathbb{Z}$ elemento tal que $(a, n) = 1$ entonces por lo demostrado en [i] tenemos que $\overline{a} \in G$. Luego, por el teorema de Lagrange, tenemos que $\overline{a}^{|G|} = e$. Es decir $\overline{a}^{\varphi(n)} = 1$ en G. Si escribimos esto en términos de congruencias obtenemos que $a^{\varphi(n)} \equiv 1(mod\ n)$.

iii.- Supongamos que $n = p$ primo. Entonces todo número menor a p es relativamente primo con este. Luego $\varphi(p) = p - 1$. Esto nos dice que, para $a \in \mathbb{Z} - p\mathbb{Z}$ tenemos que $a^{p-1} \equiv 1(mod\ p)$. En particular $a^p \equiv a(mod\ p)$. Observe que esta última igualdad es válida para $\overline{a} \equiv 0(mod\ p)$, es decir es válidad para $a \in p\mathbb{Z}$. Por lo tanto, para todo $a \in \mathbb{Z}$ se tiene que $a^p \equiv a(mod\ p)$.

2.- **Ejercicio:** Demuestre que para todo $a \in \mathbb{Z}$ tal que p no lo divide, se tiene que $a^{p^2-p} \equiv 1(mod\ p^2)$.

3.- **Problema 3:**
Sean H, K subgrupos de G tales que $|H| = p$, $|K| = q$. para p, q primos distintos. Pruebe que $H \cap K = \{e\}$.

Demostración: Consideremos $x \in H \cap K$ entonces, por el teorema de Lagrange, tenemos que $|x|$ divide a p, q. Pero como p, q son primos distintos, existen $s, t \in \mathbb{Z}$ tales que $1 = sp + tq$. Luego si $|x|$ divide a p, q entonces $|x|$ divide a 1. Por ello $|x| = 1$. Luego $x = e$.

3.- **Ejercicio:** Pruebe que en S_5 se tiene que $\langle(12)\rangle \cap \langle(12345)\rangle = \{id\}$.

Ayudantía V: En esta ayudantía estudiaremos los productos directos de grupos y el tercer teorema de isomorfía. En esta ayudantía usaremos el hecho de que D_{2n} es un grupo con $2n$ elementos, de la forma $s^\epsilon r^i$, donde $\epsilon \in \{0,1\}$ e $i \in \{0, \cdots, n-1\}$.

1.- **Problema 1:**
Sean G_1, G_2 grupos. Pruebe que $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

Demostración: Considere $(g_1, g_2) \in Z(G_1 \times G_2)$. Entonces $(g_1, g_2)(h_1, h_2) = h_1, h_2)(g_1, g_2)$, para todo $(h_1, h_2) \in G_1 \times G_2$. Es decir $g_1 h_1 = h_1 g_1$ y $g_2 h_2 = h_2 g_2$. Luego cada componente de la tupla (g_1, g_2) esta en el centro del grupo al que pertenece. Por lo tanto $(g_1, g_2) \in Z(G_1) \times Z(g_2)$. Por lo tanto $Z(G_1 \times G_2) \subset Z(G_1) \times Z(G_2)$. Observe que todas las implicancias anterores son equivalencias. Por ello $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

1.- **Ejercicio:** Sean G, H grupos y considere $A \triangleleft G$ y $B \triangleleft H$. Pruebe que $(A \times B) \triangleleft (G \times H)$ y que $(G \times H)/(A \times B) \cong G/A \times H/B$.

2.- **Problema 2:**
Sean G_1, G_2 dos grupos.
i.- Pruebe que su $G_1 \cong G_2$ entonces $Z(G_1) \cong Z(G_2)$.
ii.- Concluya que $D_6 \times C_4$ no es isomorfo a D_{24}.

Desarrollo:
i.- Sea $\phi : G_1 \to G_2$ un isomorfismo. Entonces $g \in Z(G_1)$ si y solamente si $\phi(g) \in Z(G_2)$. Esto se debe a que si $gh = hg$, para todo $h \in G_1$, entonces $\phi(g)\phi(h) = \phi(h)\phi(g)$, para toma $\phi(H) \in Im(\phi) = G_2$. El recíproco se sigue tomando la función ϕ^{-1}. Luego $\phi(Z(G_1)) = Z(G_2)$. Luego la función inducida $\phi_Z : Z(G_1) \to Z(G_2)$ es un homomorfismo inyectivo y sobreyectivo, por la conclusión anterior. Por ende ϕ_Z es isomorfismo. De esto se sigue lo pedido.

ii.- Supongamos que $D_6 \times C_4$ es isomorfo a D_{24}. Entonces $Z(D_6 \times C_4) \cong Z(D_{24})$. Por lo mostrado en la ayudantía III, tenemos que $Z(D_{24}) \cong C_2$, mientras que $Z(D_6 \times C_4) \cong Z(D_{24}) = Z(D_6) \times Z(C_4) = \{e\} \times C_4$. Esto prubea que los centros tienen cardinalidad distinta, en particular son no isomorfos.

2.- **Ejercicio:** Pruebe que $C_4 \times D_{14}$ y D_{56} son grupos no isomorfos.

3.- **Problema 3:**
Sea $D_{12} = \langle s, t : s^2 = t^6 = 1, sts^{-1} = t^{-1} \rangle$ el grupo dihedral de 12 elementos y considere $H = \langle t^3 \rangle$.
i.- Pruebe que $H \triangleleft D_{12}$.
ii.- Pruebe que $D_{12}/H \cong D_6$.

Desarrollo:
i.- Observe que $st^{3i}s^{-1} = t^{-3i} \in H$ y $tt^{3i}t^{-1} = t^{3i} \in H$. Por lo tanto para todo $g \in D_{12}$ tenemos que $gHg^{-1} = H$. Luego $H \triangleleft D_{12}$.

ii.- Primero observe que $G = HN$, para $N = \langle s, t^2 \rangle$. Esto se debe a que $s \in HN$ Y $t = t^3 t^{-2} \in HN$. Por otro lado $H \cap N = \{1\}$. Esto se debe a que si $t^{2i} = t^{3j}$ entonces $t^{2i} = t^{3j} = t^{6k} = 1$ y a que si $st^{2i} = t^{3j}$ entonces $s = t^{3j-2i}$ lo que nos lleva a una contradicción. Por lo tanto, por el tercer

teorema de isomorfía tenemos que $G/H = HN/H \cong N/(N \cap H) \cong N$. Pero $N = \langle s, r : s^2 = r^3 = 1 \ , srs^{-1} = r^{-1} \rangle \cong D_6$. Por lo tanto $G/H \cong D_6$.

3.- **Ejercicio:** Sean $M, N \triangleleft G$. Pruebe que si $G = MN$ entonces $G/(M \cap N) \cong G/M \times G/N$.

4.- **Problema 4:**
Sea G grupo y N, H subgrupos de G con $N \triangleleft G$.

i.- Pruebe, usando el tercer teorema de isomorfía, que si G es grupo finito entonces $|NH| = |H||N|/|N \cap H|$.

ii.- Pruebe que si $N = \langle (123) \rangle$ y $H = \langle (12) \rangle$ entonces $S_3 = NH$.

iii.- Concluya que $S_3 \cong D_6$.

Desarrollo:

i.- El tercer teorema de isomorfía nos dice que, si N, H subgrupos de G con $N \triangleleft G$, entonces $NH/N \cong H/(H \cap N)$. Observe que si G es grupo finito entonces NH, H, N y $N \cap H$ son grupos finitos también. Luego igualando la cadinalidad a ambos lados del isomorfismo anterior obtenemos que $|NH|/|N| = [NH : N] = [H : N \cap H] = |H|/|H \cap N|$. Luego $|NH| = |H||N|/|N \cap H|$.

ii.- Considere $N = \langle (123) \rangle$ y $H = \langle (12) \rangle$ entonces $|N| = 3$ y $|H| = 2$. Luego si $x \in H \cap N$ se tiene que $x^3 = x^2 = id$. Por lo tanto $x = id$. Luego $N \cap H = \{id\}$. De esto se sigue que $|NH| = 6 = |S_3|$. Como $NH \subset S_3$ y tienen igual cardinal, concluimos que $NH = S_3$.

iii.- Por lo mostrado en [ii] tenemos que todo elemento en S_3 es producto de $s' = (12)$ y $t' = (123)$. Además estos elementos satisfacen que $s'^2 = 1$, $t'^3 = 1$ y $s't's'^{-1} = t'^{-1}$. Por lo tanto el homomorfismo $\phi : S_3 \to D_3$ definido por $\phi(12) = s$ y $\phi(123) = t$ es un homomorfismo invertile. Luego $S_3 \cong D_6$.

4.- **Ejercicio:** Pruebe que S_4 no es isomorfo a D_8.

Ayudantía VI: En esta ayudantía estudiaremos los grupos cíclicos. Es decir, estudiaremos los grupos generados por un solo elemento.

1.- **Problema 1:**
Sea $G = \langle x \rangle$ grupo cíclico de orden n.

i.- Sea H subgrupo de G. Pruebe que $H = \langle x^i \rangle$, algún $i \in \mathbb{Z}$.

ii.- Demuestre que $(i, n) = 1$ si y solamente si $H = G$.

iii.- Encuentre todos los subgrupos de $G = \{z \in \mathbb{C} : z^8 = 1\}$.

Desarrollo:

i.- Sea H subgrupo no trivial de G y considere $A = \{j : x^j \in H - \{e\},\ j \in \mathbb{N}\} \subset \mathbb{N}$ conjunto no vacio pues existe algún $y \in H - \{e\}$. Por principio del buen orden existe un primer elemento en A. Sea $x^i \in H$ con i minimal. Sea $x^k \in H$. Por algoritmo de la división se tiene que $k = is + t$ donde $t = 0$ o $t < i$. Observe que $x^t = x^k x^{-is} \in H$. Luego como i es minimal tenemos que $t = 0$. Por lo tanto $x^k = (x^i)^s$. Luego $H = \langle x^i \rangle$.

ii.- Si $H = G$ entonces $\langle x^i \rangle = G$. Luego $(x^i)^s = x$, para cierto $s \in \mathbb{Z}$. Por lo tanto $x^{-1}x^{is} = e$. Así $is - 1 = nt$, cierto $t \in \mathbb{Z}$. Luego si algún número primo p divide a i y n entonces p divide a 1. Por lo tanto no existe número primo que divida a i y n simultaneamente. Es decir $(i, n) = 1$. Recíprocamente si $(i, n) = 1$, por algoritmo de la división, se tiene que existen $s, t \in \mathbb{Z}$ tales que $is + tn = 1$. Luego $(x^i)^s = x \in H$. Por lo tanto $H = G$.

iii.- Observe que si $z^8 = 1$ se tiene que $|z| = 1$. Luego como los elementos son raices octavas de la unidad se tiene que $G = \langle z_0 \rangle$, donde $z_0 = e^{\frac{2\pi i}{8}}$. Por [i] los subgrupos no triviales de G son de la forma $H_2 = \langle z_0^2 \rangle$, $H_3 = \langle z_0^3 \rangle$, $H_4 = \langle z_0^4 \rangle$, $H_5 = \langle z_0^5 \rangle$, $H_6 = \langle z_0^6 \rangle$ y $H_7 = \langle z_0^7 \rangle$. Observe que, por [ii], tenemos que $G = H_3 = H_5 = H_7$. Por otro lado $H_2 = H_6$, esto se debe a que $z_0^6 = (z_0^2)^3 \in H_2$ y $(z_0)^2 = (z_0^6)^{-1} \in H_6$. Observe que $H_2 \subset H_4$, pero no son iguales ya que $z_0^2 \notin H_4$. Esto ya que si $z_0^2 \in H_4$ entonces $z_0^2 = z_0^{4t}$. Por lo tanto $2 = 4t + 8s$. Luego 4 divide a 2, lo que nos lleva a una contradicción. Por lo tanto los únicos subgrupos de G son $\{1\}$, H_2, H_4 y G.

1.- **Ejercicio:** Encuentre todos los subgrupos del grupo cíclico C_4.

1.- **Ejercicio:** Sea $G = C_n$ un grupo cíclico de orden n. Pruebe que G tiene subgrupos de orden d, para todo d divisor de n.

2.- **Problema 2:**
Encuentre todos los subgrupos de $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$.

Desarrollo: En la ayudantía II probamos que $H \cong (\mathbb{Z}, +)$. Por lo tanto los subgrupos de H están en correspondencia con los subgrupos de $\mathbb{Z}$. En clases se demostró que los subgrupos de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, para $n \in \mathbb{Z}$. Por lo tanto los subgrupos de H son de la forma $H_n = \left\{ \begin{pmatrix} 1 & nt \\ 0 & 1 \end{pmatrix} : t \in \mathbb{Z} \right\}$.

2.- **Ejercicio:** Sea $x \in G$. Pruebe que $N_G(\langle x \rangle) = \{g \in G : gxg^{-1} = x^a, \text{ para algún } a \in \mathbb{Z}\}$.

3.- **Problema 3:**
Sea G grupo.

i.- Pruebe que si $G/Z(G)$ es cíclico entonces G es abeliano.

ii.- Demuestre que si $Aut(G)$ es un grupo cíclico entonces G es abeliano.

iii.- Sea G grupo de orden pq y con centro no trivial. Pruebe que $Z(G) = G$.

Desarrollo:

i.- Sean $g, h \in G$ dos elementos cualquiera. Supongamos que $G/Z(G) = \langle \overline{r} \rangle$. Entonces $g = sr^i$, para cierto $s \in Z(G)$ y $h = tr^j$, para cierto $t \in Z(G)$. Luego $gh = sr^i tr^j = str^{i+j} = tsr^{j+i} = tr^j sr^i = hg$. Por ello G es un grupo abeliano.

ii.- Supongamos que $Aut(G)$ es un grupo cíclico. Por lo demostrado en la ayudantía III, tenemos que $G/Z(G)$ es isomorfo a un subgrupo de $Aut(G)$. Por el problema 1 todo subgrupo de un grupo cíclico es cíclico. Luego tenemos que $G/Z(G)$ es un grupo cíclico. De [i] se concluye que G es abeliano.

iii.- Supongamos que $|G| = pq$ y $|Z(G)| \neq 1$. Por lo tanto $|Z(G)| \in \{p, q, pq\}$. Supongamos que $|Z(G)| = p$, entonces $|G/Z/G)| = q$. Por lo demostrado en la ayudantía IV, tenemos que $G/Z(G)$ es un grupo cíclico de q elementos. Por el problema 2 concluimos que G abeliano. Por lo tanto $Z(G) = G$. Si $|Z(G)| = q$ el razonamiento es análogo. Finalmente si $|Z(G)| = pq$, se sigue de comparar los cardinales de G y $Z(G)$ que $G = Z(G)$.

3.- **Ejercicio:** Pruebe, mediante un ejemplo, que si $G/Z(G)$ es abeliano entonces G puede no ser abeliano.

4.- **Problema 4:**
Sea $G = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} : a, b \in \mathbb{C},\ a^3 = b^5 = 1 \right\}$. Pruebe que $G \cong \mathbb{Z}/15\mathbb{Z}$.

Demostración: Considere $K_3 = \{z \in \mathbb{C} : z^3 = 1\}$ y $K_5 = \{z \in \mathbb{C} : z^5 = 1\}$. Definimos $\phi : G \to K_3 \times K_5$ por $\phi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = (a, b)$. Entonces ϕ es un isomorfismo. Luego $G \cong K_3 \times K_5$. Pero $K_n \cong C_n$, donde C_n es el grupo cíclico con n elementos. Por lo tanto $G \cong C_3 \times C_5$. Además en clases se demostró que $C_n \times C_m = C_{mn}$, si $(m, n) = 1$. Por lo tanto $G \cong C_{15}$.

5.- **Problema 5:**
Pruebe que $(\mathbb{Q}, +)$ no es un grupo cíclico.

Demostración: Supongamos que $\mathbb{Q}$ es cíclico y esta generado por $\frac{n}{m}$, donde $(n, m) = 1$. Entonces $\frac{1}{2m} \in \left\langle \frac{n}{m} \right\rangle$. Luego existe $t \in \mathbb{Z}$ tal que $\frac{1}{2m} = \frac{tn}{m}$. Por lo tanto $m = 2mtn$. Luego $1 = 2tn$, lo que nos lleva a una contradicción. Por lo tanto $\mathbb{Q}$ no es un grupo cíclico.

5.- **Ejercicio:** Pruebe que $\mathbb{Q} \times \mathbb{Q}$ no es un grupo cíclico.

5.- **Ejercicio:** Pruebe que $\mathbb{Q}$ no es un grupo finitamente generado.

Ayudantía VII: En esta ayudantía trabajaremos ejemplos de acciones de grupos sobre si mismos, de forma tal de deducir nueva información de los grupos en cuestión.

1.- **Problema 1:**
Sea G un grupo de orden p^n, para cierto $n \in \mathbb{N}$ y p primo. Considere la acción de G sobre si mismo por conjugación.

i.- Demuestre que $\{x \in G : Orb(x) = \{x\}\} = Z(G)$.

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

iii.- Encuentre un grupo no abeliano de orden p^n, para cierto $n \in \mathbb{N}$ y p primo.

Desarrollo:

i.- Observe que $Orb(x) = \{gxg^{-1} \in G : g \in G\}$. Luego $Orb(x) = \{x\}$ si y solamente si $gxg^{-1} = x$, pata todo $g \in G$. Esto último es equivalente a que $x \in Z(G)$. Luego $\{x \in G : Orb(x) = \{x\}\} = Z(G)$.

ii.- Sabemos que toda acción de un grupo en un conjunto particiona dicho conjunto en orbitas. En nuestro caso, como G actúa en si mismo por conjugación tenemos que $|G| = |O_1| + \cdots + |O_k|$, donde $|O_i|$ son las diferentes orbitas que genera G. Observe que un elemento tiene orbita trivial si y solamente si es un elemento del centro, luego tenemos que $|G| = |Z(G)| + |O_{i_1}| + \cdots + |O_{i_k}|$, donde $|O_{i_l}| \neq 1$. Por otro lado sabemos que $|O_{i_l}| = |G|/|Stab_G(x_{i_l})|$, donde x_{i_l} es un elemento cualquiera de O_{i_l}. Luego $|O_{i_l}| = p^{s_{i_l}}$, para cierto $s_{i_l} \neq 0$. Por lo tanto p divide a $|G| - (|O_{i_1}| + \cdots + |O_{i_k}|)$. Concluimos que p divide a $|Z(G)|$. Luego $Z(G)$ no es trivial.

iii.- Considere $G = D_8 = \langle r, s : r^4 = s^2 = 1,\ srs^{-1} = r^{-1} \rangle$. Sabemos que $Z(G) = \{1, r^2\}$. Por lo tanto G es un grupo de orden 2^3 no abeliano.

1.- **Ejercicio:** Demuestre que para acción anterior $C_G(x) = Stab_G(x)$.

1.- **Ejercicio:** Demuestre que todo grupo de orden p^2 es abeliano

2.- **Problema 2:** 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. En efecto, 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.- **Ejercicio:** Calcule el numero de clases de conjugación en S_4.

3.- **Problema 3:** 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.

3.- **Ejercicio:** Demuestre que C_3 puede ser visto como un subgrupo normal de S_3.

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].

Ayudantía VIII: En esta ayudantía trabajaremos con ejemplos geometricos de acciones de grupos.

1.- **Problema 1:**
Sea G el grupo de movimientos rigidos (rotaciones) del dodecaedro y T el grupo simetrias del dodecaedro considerando las reflexiones.

i.- Calcule $|G|$.

ii.- Calcule $|T|$.

iii.- Asumiendo que $Z(A_5) = \{id\}$ y que $G \cong A_5$ pruebe que $T \cong A_5 \times C_2$.

Desarrollo:

i.- Considere la acción de G sobre las caras del dodecaedro regular. Esta acción es transitiva pues dejando una cara fija podemos llevar mediante rotaciones una cara vecina de esta a cuaquiera de sus otros 4 homologos. Luego una cara esta en una orbita si y solamente si esta su vecina. Esto implica que la acción sea transitiva. Por lo tanto si usamos la identidad:

$$|G/Stab_G(x)| = |Orb(x)|,$$

tenemos que $|G| = 12|Stab_G(x)|$. Por otro lado si dejamos una cara fija tenemos 5 rotaciones posibles del dodecaedro. Luego $|Stab_G(x)| = 5$. Por lo tanto $|G| = 60$.

ii.- Repetimos la misma acción que en [i]. Como $T \supset G$ tenemos que esta acción es también transitiva. Luego tenemos que $|T| = 12|Stab_T(x)|$. Pero si dejamos una cara fija entonces tenemos que el subgrupo de simetrias que del dodecaedro que cumplen con esto es isomorfo a D_{10}. Por lo tanto $|G| = 120$.

iii.- Considere $A = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$. Observe que la matriz A corresponde a la composición de las reflexiones respecto al eje x, y y z. Luego $A \in T$. Recordemos que todo elemento de T se puede ver como una única matriz en $\mathbb{M}_3(\mathbb{R})$, pues dichos elementos corresponden a rotaciones en el espacio. Observe que A conmuta con todos los elementos de T, por ser un multiplo de la identidad. Luego $\langle A\rangle \cap G = \{id\}$, pues $Z(G) \cong Z(A_5) = \{id\}$. Por otro lado $[T : G] = 2$, así $G \lhd T$. Observe que siempre $\langle A\rangle \lhd G$. Además $|\langle A\rangle||G| = |T|$. Concluimos que $T \cong G \times \langle A\rangle \cong A_5 \times C_2$.

1.- **Ejercicio:** Pruebe que $Z(A_5) = \{id\}$.

2.- **Problema 2:**
Sea G el grupo de movimientos rigidos del tetraedro. Calcule $|G|$.

Desarrollo: Considere la acción de G sobre las caras del tetraedro regular. Esta acción es transitiva. Luego si usamos que $|G/Stab_G(x)| = |Orb(x)|$ obtenemos que $|G| = 4|Stab_G(x)|$. Por otro lado si dejamos una cara fija tenemos 3 rotaciones posibles del dodecaedro. Luego $|Stab_G(x)| = 3$. Por lo tanto $|G| = 12$.

3.- **Problema 3:**
Determine de cuantas maneras esencialmente distintas se puede pintar con n colores un triangulo equilatero hecho de palitos de helado.

Desarrollo: Considere la acción de $G = D_3$ en el conjunto de todas las coloraciones posibles, con n colores, del triangulo equilatero. Sea X dicho conjunto. Entonces debemos calcular $|G \setminus X|$. Para ello usaremos la identidad $|G \setminus X| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$. Observe que en G está compuesto por 2 rotaciones de orden 3, la identidad y 3 reflexiones que cruzan un vertice y un lado. Observe que toda rotación de orden 3 cumple que un elemento de X es fijo por el si tiene los mismos colores en todas las aristas. Por otro lado toda reflexión que cruza un lado y un vértice cumple que un eleemnto de X es fijo por el si tiene los mismos colores en las aristas que permuta dicha reflexión. Por lo tanto tiene 2 aristas de igual color y la tercera de cualquier color. Por lo tanto:

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

2. Anillos

Ayudantía IX: En esta ayudantía comenzaremos a trabajar con la estructura de anillo. Veremos algunos ejemplos de anillos e ideales.

1.- **Problema 1:**
Sea $A = \mathbb{M}_2(\mathbb{Z})$ y considere $B = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} : x, y, z, w \in 2\mathbb{Z} \right\}$.

i.- Pruebe que B es un anillo.

ii.- Pruebe que B es un ideal de A.

Desarrollo:

i.- Demostremos que B es subanillo de A. Observe que B es no vacio dado que $O_{2\times 2} \in B$. Ahora bien, si consideramos dos matrices $X = (x_{ij})_{i,j=1}^2, Y = (y_{ij})_{i,j=1}^2 \in B$ entonces sus coeficientes cumplen con $x_{ij} \in 2\mathbb{Z}$ e $y_{ij} \in 2\mathbb{Z}$. Luego $(X \pm Y)_{ij} = x_i j \pm y_i j \in 2\mathbb{Z}$. Por lo tanto B es subgrupo de A. Por otro lado $(XY)_{ij} = \sum_{r=1}^2 x_{ir} y_{rj} \in 4\mathbb{Z} \subset 2\mathbb{Z}$. Por ello B es subanillo de A.

ii.- Observe que lo dicho en [i] prueba que si tomamos $Z \in A$ y $A \in B$ entonces $ZX \in B$, $XZ \in B$.

1.- **Ejercicio:** Sea $A = \mathbb{M}_2(\mathbb{Z})$ y considere:

$$B = \left\{ \begin{pmatrix} x & y \\ z & w \end{pmatrix} : y, z, w \in \mathbb{Z}\ , x \in 2\mathbb{Z} \right\}.$$

Pruebe que B no es un ideal de A.

2.- **Problema 2:**
Sea $A = \mathbb{Q}[x]$ en anillo de polinomios con coeficientes en $\mathbb{Q}$ y considere el ideal $J = (x^2 - 1, x^2 - 3x + 2)$.

i.- Pruebe que $J = (x - 1)$.

ii.- Concluya que $(x^2 - 1) \subsetneq J$.

Desarrollo:

i.- Observe que $x^2 - 1 = (x - 1)(x + 1)$ y que $x^2 - 3x + 2 = (x - 2)(x - 1)$. Por lo tanto todo elemento $v = p(x)(x^2 - 1) + q(x)(x^2 - 3x + 2)$ se reescribe como $v = s(x)(x - 1)$. Luego $J \subset (x - 1)$. Probemos que de hecho son el mismo conjunto. Observe que $1 = \frac{1}{3}(x + 1) - (x - 2)$, luego $(x - 1) = \frac{1}{3}[(x^2 - 1) - (x^2 - 3x + 2)]$. Por lo tanto $x - 1 \in J$. Luego $J = (x^2 - 1)$.

ii.- Observe primero que $x^2 - 1 = (x - 1)(x + 1) \in J$. Por lo tanto $(x^2 - 1) \subset J$. Supongamos que $J = (x^2 - 1)$ entonces existe un polinomio $t(x) \in \mathbb{Q}[x]$ tal que $x - 1 = q(x)(x^2 - 1)$ es decir $1 = q(x)(x + 1)$. Igualando en el grado a ambos lados de la ecuación anterior llegamos a una contradicción. Por lo tanto $(x^2 - 1) \subsetneq J$.

2.- **Ejercicio:** Pruebe que en $\mathbb{Q}[x]$ se tiene que los ideales $(p(x)), (q(x))$ son iguales si y solamente si $p(x) = aq(x)$, para cierto $a \in \mathbb{Q}^*$.

3.- **Problema 3:**
Sea $A = \mathcal{L}(\mathbb{R}^2, \mathbb{R}^2)$ el anillo de funciones lineales de $\mathbb{R}^2$ a $\mathbb{R}^2$. Considere $B = \{T \in A : T(e_1) = 0\}$, donde $e_1 = (1, 0) \in \mathbb{R}^2$.

i.- Demuestre que B es un anillo.

ii.- ¿Es B un ideal bilátero de A?

iii.- Pruebe que $B \cong \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

Desarrollo:

i.- Obsevre que $T = 0$, la transformación lineal nula, es un elemento de B. Además si $T, S \in B$ entonces $T(e_1) = S(e_1) = 0$. Luego $T \pm S(e_1) = 0$. Por lo tanto B es un subgrupo abeliano de A. Considere ahora $T, S \in B$ entonces $S \circ T(e_1) = S(0) = 0$. Por lo tanto B es un subanillo de A. Luego B es un anillo.

ii.- Considere S una tranformación lineal cualquiera. Entonces si $T \in B$ se tiene que $S \circ T(e_1) = S(0) = 0$. Luego B es un ideal izquierdo de A. Por otro lado si consideramos las tranformaciónes lineales $T(x, y) = (0, y)$ y $S(x, y) = (y, x)$ tenemos que $T \circ S(e_1) = T(e_2) = e_2 \neq 0$. Por lo tanto B no es ideal derecho de A. Luego B no es ideal bilátero de A.

iii.- Considere $\beta = \{e_1, e_2\}$ la base canónica de $\mathbb{R}^2$. Sabemos que fijando una base, existe una correspondencia biunívoca entre matrices y transformaciones lineales entre espacios vectoriales de dimensión finita. Además esta correspondecia respeta la suma y el producto de ambos anillos. Por lo tanto dicha función es un isomorfismo de anillos. Si a cada transformación $T \in B$ asociamos su matriz tenemos que $[T] = \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$, para ciertos $a, b \in \mathbb{R}$. Esto se debe a que $T(e_1) = 0.e_1 + 0.e_2$ y $T(e_2)a.e_1 + b.e_2$, para ciertos $a, b \in \mathbb{R}$. Luego $B \cong \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{R} \right\}$.

4.- **Problema 4:**
Sea $A = \mathbb{R}[x]$ el anillo de polinomios con coeficientes en $\mathbb{R}$. Considere $C = \{p(x) \in \mathbb{R}[x] : p(0) = p'(0) = 0\}$.

i.- Pruebe que C es un ideal de A.

ii.- Pruebe que $C = (x^2)$.

Desarrollo:

i.- Claramente el polinomio nulo es un elemento de C. Considere $p(x), q(x) \in C$ entonces $(p \pm q)(0) = 0$ y $(p + q)'(0) = 0$. Por lo tanto B es un subgrupo de A. Observe que A es un anillo conmutativo, por lo tanto si C es ideal por izquierda tenemos que este es ideal bilátero. En efecto, si consideramos $q(x) \in A$ tenemos que $pq(0) = 0$ y $(pq)'(0) = p'(0)q(0) + p(0)q'(0) = 0$. Por lo tanto $pq(x) \in C$. Luego C es un ideal de A.

ii.- Observe que si tenemos $p(x) = x^2 q(x)$ entonces $p(0) = 0$ y $p'(x) = x^2 q'(x) + 2xq(x)$, por lo tanto $p'(0) = 0$. Luego $(x^2) \subset C$. Por otro lado si tomamos un polinomio cualquiera $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in C$, entonces $0 = p(0) = a_0$ y $a_1 = p'(0) = 0$. Luego $p(x) = x^2(a_2 + a_3 x + \cdots + a_n x^{n-2})$. Luego $C \subset (x^2)$. Es así como $C = (x^2)$.

4.- **Ejercicio:** Pruebe que $C_k = \left\{p(x) \in \mathbb{R}[x] : p^{(i)}(0) = 0, \forall i \leq k\right\}$ es un ideal de $\mathbb{R}[x]$. Pruebe además que $C_k = (x^{k+1})$.

5.- **Problema 5:**
Sea $A = \mathbb{M}_2(\mathbb{R})$ el anillo de matrices con coeficientes reales y considere I ideal de A tal que $E_{11} \in I$, donde E_{ij} es la matriz elemental con un uno en

la entrada ij y ceros en las restantes. Pruebe que $I = A$.

Demostración: Observe que si tomamos $\lambda \in \mathbb{R}$ y $r \in I$ entonces $\lambda r = (\lambda \mathrm{id})r \in I$. Por lo tanto I es un subespacio vectorial de $\mathbb{M}_2(\mathbb{R})$. Luego para demostrar que $I = A$ basta probar que $E_{ij} \in I$, $\forall i, j \in \{1, 2\}$. En efecto $E_{12} = E_{11}E_{12} \in I$ y $E_{21} = E_{21}E_{11} \in I$. Por lo tanto $E_{11}, E_{12}, E_{21} \in I$. Finalmente, como $E_{22} = E_{21}E_{12} \in I$, concluimos que $A = I$.

5.- **Ejercicio:** Sea $A = \mathbb{M}_2(K)$, donde $K = \mathbb{R}$ o $K = \mathbb{C}$. Pruebe que si I es un ideal no nulo en A entonces $A = I$.

Ayudantía X: En esta ayudantía estudiaremos anillos cocientes y homomorfismos de anillos. En lo que sigue haremos uso del primer y tercer teorema de isomorfía.

1.- **Problema 1:**
Sea A anillo conmutativo con uno y $a \in A$ un elemento cualquiera. Con sidere el anillo $A[x]$ de polinomios con coeficientes en A. Pruebe que $A[x]/(x-a) \cong A$.

Demostración: Considere el homomorfismo $\phi : A[x] \to A$ definido por $\phi(p(x)) = p(a)$. Tomando la imagen de los polinomios constantes bajo la función ϕ obtenemos que $\phi(A[x]) = A$. Observe que todo polinomio $q(x) = (x-a)t(x)$ cumple con que $q(a) = 0$. Luego $(x-a) \subset \ker(\phi)$. Demostremos la contensión contraria. Sea $p(x)$ un polinomio en $A[x]$. Como $x-a$ es mónico, podemos aplicar división de polinomios para escribir $p(x) = (x-a)q(x) + b$, donde $b \in A$. Luego si $p(x) \in \ker(\phi)$ tenemos que $b = p(a) = 0$. Por lo tanto $p(x) \in (x-a)$. Es decir $\ker(\phi) = (x-a)$. Por primer teorema de isomorfía concluimos que $A[x]/(x-a) \cong A$.

1.- **Ejercicio:** Pruebe que, bajo las hipótesis anteriores, $A[x]$ es un anillo conmutativo con uno.

1.- **Ejercicio:** Demuestre que si A es un anillo tal que todo elemento no nulo es invertible, entonces $A[x]/(a) \cong \{0\}$, para $a \neq 0$.

2.- **Problema 2:**
Considere el anillo $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z},\ i^2 = -1\}$.
i.- Pruebe que $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$.
ii.- Demuestre que $\mathbb{Z}[i]/(1+i) \cong \mathbb{Z}/2\mathbb{Z}$.

Desarrollo:
i.- Considere el homomorfismo $\phi : \mathbb{Z}[x] \to \mathbb{Z}[i]$ definido por $\phi(p(x)) = p(i)$. Tomando la imagen de los polinomios lineales bajo la función ϕ obtenemos que $\phi(\mathbb{Z}[x]) = \mathbb{Z}[i]$. Observe que todo polinomio $q(x) = (x^2+1)t(x)$ cumple con que $q(i) = 0$. Luego $(x^2+1) \subset \ker(\phi)$. Por otro lado, sea $p(x)$ un polinomio en $A[x]$. Como x^2+1 es mónico, podemos aplicar división de polinomios para escribir $p(x) = (x^2+1)q(x) + (ax+b)$, donde $a, b \in \mathbb{Z}$. Luego si $p(x) \in \ker(\phi)$ tenemos que $ai + b = p(i) = 0$. Supongamos que $a \neq 0$, entonces $x = \frac{-b}{a} \in \mathbb{Q}$ cumple con $x^2 = -1$. Esto nos lleva a una contradicción. Por lo tanto $a = 0$ y luego $b = 0$. Así $(x^2+1) = \ker(\phi)$. Por el primer teorema de isomorfía concluimos que $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2+1)$.

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

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

Pero si usamos el tercer teorema de isomorfía:

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

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

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

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

2.- **Ejercicio:** Pruebe directamente que $\mathbb{Z}[i]$ es un subanillo de $\mathbb{C}$.

2.- **Ejercicio:** Demuestre que en $A = \mathbb{Z}[i]/(i+2)$ todo elemento no nulo es invertible.

3.- **Problema 3:**
Sea B un anillo conmutativo con uno, tal que si $xy = 0$ entonces $x = 0$ o $y = 0$. Este tipo de anillos se denomina **dominio de integridad**. Sea $\phi : \mathbb{Z} \to B$. Pruebe que B contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z}$, para p primo o bien B contiene un subgrupo isomorfo a $\mathbb{Z}$.

Demostración: Sabemos, por el primer teorema de isomorfiía, que $\mathbb{Z}/\ker(\phi)$ es isomorfo a un subanillo de B. Por otro lado $\ker(\phi)$ es un ideal de $\mathbb{Z}$. Luego $\ker(\phi) = n\mathbb{Z}$, para cierto $n \in \mathbb{Z}$ o $\ker(\phi) = \{0\}$. Si sucede lo segundo tenemos que B tiene un subgrupo isomorfo a $\mathbb{Z}$. Por otro lado, si $\ker(\phi) = n\mathbb{Z}$ y $n = st$, para $s, t \notin \{\pm 1\}$, entonces $\mathbb{Z}/n\mathbb{Z}$ es isomorfo a un subgrupo de B y $\overline{s}\overline{t} = \overline{0}$. Como B es dominio de integridad tenemos que $\overline{s} = \overline{0}$ o $\overline{t} = \overline{0}$. Sín perdida de generalidad $\overline{s} = \overline{0}$. Entonces $s = nu$. Luego en $\mathbb{Z}$ tenemos que $n = nus$, así $us = 1$. Luego $s \in \{\pm 1\}$. Esto nos lleva a una contracción. Por lo tanto n es un número primo. Es así como concluimos que B contiene un subgrupo isomorfo a $\mathbb{Z}/p\mathbb{Z}$, para cierto p primo.

4.- **Problema 4:** Sea B un dominio de integridad finito. Pruebe que todo elemento no nulo en B es invertible.

Desmostración: Sea $b \in B$ elemento no nulo. Considere la función $\phi : B \to B$ definida por $\phi(a) = ba$. Observe que $\phi(a+c) = b(a+c) = \phi(a)+\phi(c)$. Luego ϕ es un homomorfismo de grupos. Observe que $\ker(\phi) = \{a \in B : ba = 0\} = \{0\}$, pues B es dominio de integridad. Luego ϕ es un homomorfismo inyectivo. Como B es un conjunto finito, se tiene que ϕ es sobreyectivo. Es así como existe $a \in A$ tal que $ab = ba = 1$. Luego todo elemento no nulo en B es invertible.

5.- **Problema 5:**
Sea $A \subseteq B$ subanillo e $I \subseteq B$ un ideal.

i.- Pruebe que I es ideal de $A+I$ y que $I \cap A$ es un ideal de A.

ii.- Demuestre que $A + I/I \cong A/(A \cap I)$.

iii.- Concluya que si $n, m \in \mathbb{Z}$ son relativamente primos entonces $n\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$.

Desarrollo:

i.- Observe que I es un anillo contenido en $A+I$. Por ende I es subanillo de $A+I$. Por otro lado para todo $r \in A+I$ y $s \in I$ tenemos que $r \in B$. Luego $rs, sr \in I$. Por lo tanto I es ideal de $A+I$. Por otro lado $A \cap I$ es un anillo contenido en A. Luego $A \cap I$ es un subanillo de A. Considere $r \in A$ e $i \in A \cap I$, entonces $ri, ir \in A \cap I$, pues cada elemento está en A e I. Luego $A \cap I$ es un ideal de A.

ii.- Considere el homomorfismo $\phi : A+I \to A/(A\cap I)$ definido por $\phi(a+i) = \overline{a}$. Observe que ϕ está bien definido pues si $a+i = b+j$, con $a, b \in A$, $i, j \in I$ entonces $a - b = j - i \in A \cap I$. Luego $\phi(a+i) = \overline{a} = \overline{b} = \phi(b+j)$. Claramente ϕ es sobreyectivo. Por último, tenemos que $\ker(\phi) = \{a+i \in A+I : \overline{a} = 0\} = \{a+i \in A+I : a \in I\} = I$. Concluimos por primer teorema de isomorfía que $A + I/I \cong A/(A \cap I)$.

iii.- Considere $I = (m)$, $A = (n)$ como en la parte [i]. Entonces $(n)+(m) = (1)$, pues existe una combinación lineal entera de la forma $ns+mt = 1$. Además $n\mathbb{Z} \cap m\mathbb{Z} = nm\mathbb{Z}$, pues n y m no tienen factores comunes. Luego por [ii] tenemos que $\mathbb{Z}/m\mathbb{Z} = n\mathbb{Z} + m\mathbb{Z}/m\mathbb{Z} \cong n\mathbb{Z}/nm\mathbb{Z}$.

5.- **Ejercicio:** Pruebe que $n\mathbb{Z}/mcm(n,m)\mathbb{Z} \cong mcd(n,m)\mathbb{Z}/m\mathbb{Z}$. Concluya que $mdc(n,m)mcm(n,m) = nm$.

6.- **Problema 6:**
Sea I ideal de A.

i.- Pruebe que $I = A$ si y solamente si $A/I \cong \{0\}$.

ii.- Encuentre condiciones necesarias y suficientes sobre $a, b \in \mathbb{C}$ para que $(x-a)+(x-b) = \mathbb{C}[x]$.

Desarrollo:

i.- Sabemos que $A/I \cong \{0\}$ si y solamente si todo $a \in A$ cumple con $\overline{a} = \overline{0}$, es decir si y solamente si $a \in I$.

ii.- Por [i] debemos encontrar condiciones necesarias y suficientes para que $I = (x-a)+(x-b)$ cumpla con $\mathbb{C}[x]/I = \{0\}$. Observe que si $a = b$ entonces $I = (x-a)$. Por lo tanto $\mathbb{C}[x]/I \cong \mathbb{C} \neq \{0\}$. Luego $I \neq \mathbb{C}[x]$. Por otro lado si $a \neq b$ tenemos que $(a-b) \subset I$. Pero $1 = (a-b)^{-1}(a-b) \in I$. Es por ello que $\mathbb{C}[x] \subset I$. Luego $I = \mathbb{C}[x]$. Concluimos que $(x-a)+(x-b) = \mathbb{C}[x]$ si y solamente si $a \neq b$.

Ayudantía XI: En esta ayudantía estudiaremos productos de anillos y trabajaremos con el teorema chino de los restos. En lo que sigue usaremos la notación n para $\overline{n} \in \mathbb{Z}/m\mathbb{Z}$.

1.- **Problema 1:**
Sea $A = \mathbb{Z}/30\mathbb{Z}$.

i.- Encuentre los elementos idempotentes de A.

ii.- Descomponga $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Desarrollo:

i.- Observe que $(\mathbb{Z}/30\mathbb{Z})^2 = \{0, 1, 4, 16, 25, 6, 19, 12, 21, 10, 1, 24, 19, 16, 15\}$. Luego los elementos $\{6, 10, 15, 25, 21, 16\}$ son los súnico idempotentes no triviales del anillo A. Observe que A es conmutativo, por lo tanto los elementos anteriores son idempotentes centrales.

ii.- Observe que $6 + 15 + 10 = 1$ y además se tiene que $6.15 = 0$, $10.15 = 0$, $6.10 = 0$. Luego, por el teorema de descomposición de anillos por elementos idempotentes, tenemos que $A \cong 6\mathbb{Z}/30\mathbb{Z} \times 15\mathbb{Z}/30\mathbb{Z} \times 10\mathbb{Z}/15\mathbb{Z}$. Pero por lo mostrado en la ayudantía anterior tenemos que si n, m son relativamente primos entonces $n\mathbb{Z}/nm\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$. Luego $A \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Esto último pues $2\mathbb{Z}/3\mathbb{Z} = \mathbb{Z}/3\mathbb{Z}$. Observe que $6 \in \mathbb{Z}/30\mathbb{Z}$ corresponde en el producto de anillos a $(0, 1, 0)$. Esto pues el primer isomorfismo corresponde a la multiplicación por los elementos idempotentes centrales de cada clase en $\mathbb{Z}/30\mathbb{Z}$. Por lo mismo $10 \in \mathbb{Z}/30\mathbb{Z}$ corresponde en el producto de anillos a $(0, 0, 1)$ y $15 \in \mathbb{Z}/30\mathbb{Z}$ corresponde a $(1, 0, 0)$.

1.- **Ejercicio:** Sea $B = \mathbb{C}[x]/(x^2 + 5x + 4)$. Pruebe que $B \cong \mathbb{C} \times \mathbb{C}$. Usando esto encuentre un par de elementos idempotentes en B.

2.- **Problema 2:**
Sea $A = \mathbb{Z}/81\mathbb{Z}$. Pruebe que $T = \begin{pmatrix} 1 & 3 \\ 3 & 1 \end{pmatrix} \in \mathbb{M}_2(A)$ es un elemento invertible. Calcule su inverso.

Demostración: Observe que $T = \mathrm{id} + B$, donde $B = \begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$. Además $B^2 = 9\mathrm{id}$, luego $B^4 = 0$. Por lo tanto T es suma de un elemento invertible y otro nilpotente. Luego T es invertible. Además $(\mathrm{id} + B)(\mathrm{id} - B + B^2 - B^3) = (\mathrm{id} - B + B^2 - B^3)(\mathrm{id} + B) = \mathrm{id} - B^4 = \mathrm{id}$. De esto se sigue que $T^{-1} = (\mathrm{id} - B + B^2 - B^3) = \begin{pmatrix} 10 & -30 \\ -30 & 10 \end{pmatrix}$.

2.- **Ejercicio:** Sea $A = \mathbb{Z}/81\mathbb{Z}$. Pruebe que $T = \begin{pmatrix} 4 & 3 \\ 3 & 1 \end{pmatrix} \in \mathbb{M}_2(A)$ es un elemento invertible. Calcule su inverso.

3.- **Problema 3:**
Sea $p \in \mathbb{Z}$ primo. Pruebe que en $\mathbb{Z}/p^r\mathbb{Z}$ todo elemento es invertible o nilpotente.

Demostración: Considerede $n \in \mathbb{Z}$ un representante de la clase $\overline{n} \in \mathbb{Z}/p^r\mathbb{Z}$. Observe que si n y p^r son relativamente primos entonces existen $a, b \in \mathbb{Z}$ tales que $an + p^r b = 1$. Luego $\overline{an} = 1$. Es decir, si p no divide a n se tiene

que $\overline{n}$ es invertible. Por otro lado, si p divide a n entonces $n = ps$ cumple con $\overline{n}^r = \overline{p^r s^r} = \overline{0}$. Luego $\overline{n}$ es nilpotente. Esto demuestra lo pedido.

3.- **Ejercicio:** Sea A anillo conmutativo con uno. Pruebe $\mathfrak{N}(A) = \{a \in A : a^n = 0, \text{algún } n \in \mathbb{Z}\}$. Pruebe que $\mathfrak{N}(A)$ es un ideal de A. Calcule $\mathfrak{N}(\mathbb{Z}/p^r\mathbb{Z})$, para p primo. Concluya que $(\mathbb{Z}/p^r\mathbb{Z})/\mathfrak{N}(\mathbb{Z}/p^r\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$.

4.- **Problema 4:**
Sea $A = \mathbb{M}_2(\mathbb{Z}/6\mathbb{Z})$.

i.- Demuestre que $A \cong \mathbb{M}_2(\mathbb{Z}/3\mathbb{Z}) \times \mathbb{M}_2(\mathbb{Z}/2\mathbb{Z})$.

ii.- Sea K cuerpo. Pruebe que $\mathbb{M}_2(K)$ no es isomorfo a un producto de anillos.

iii.- Concluya que en A hay solamente dos idempotentes centrales.

Desarrollo:

i.- Observe que en $B = \mathbb{Z}/6\mathbb{Z}$ se tiene que $\{3, 4\}$ son un par de elementos idempotentes centrales. Luego dichos elementos descomponene B como $B \cong 3\mathbb{Z}/6\mathbb{Z} \times 4\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. Considere ahora las matrices $T = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ y $S = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$. Observe que dichas matrices son centrales. Además $S^2 = S$, $T^2 = T$ y $T = \text{id} - S$. Luego estas matrices descomponenen A como $A \cong A/TA \times A/SA$. Pero $TA = \mathbb{M}_2(3\mathbb{Z}/6\mathbb{Z}) \cong \mathbb{M}_2(\mathbb{Z}/2\mathbb{Z})$. Luego $A \cong \mathbb{M}_2(\mathbb{Z}/6\mathbb{Z})/\mathbb{M}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathbb{M}_2(\mathbb{Z}/6\mathbb{Z})/\mathbb{M}_2(\mathbb{Z}/3\mathbb{Z}) \cong \mathbb{M}_2(\mathbb{Z}/3\mathbb{Z}) \times \mathbb{M}_2(\mathbb{Z}/2\mathbb{Z})$.

ii.- Supongamos que $A \in \mathbb{M}_2(K)$ es idempotente no trivial. Luego dicho elemento, en cierta base apropiada, es $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$. Pero si consideramos $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ tenemos que $AB = B$ y $BA = 0$. Luego A no es central. Por ello $\mathbb{M}_2(K)$ no tiene elementos idempotentes centrales no triviales. Luego $\mathbb{M}_2(K)$ no es un producto de anillos.

iii.- Como $\mathbb{M}_2(\mathbb{Z}/3\mathbb{Z})$ y $\mathbb{M}_2(\mathbb{Z}/2\mathbb{Z})$ no son producto de anillos concluimos que estos no poseen elementos idempotentes no triviales. Luego tenemos que en A solamente existen dos elementos de este tipo.

5.- **Problema 5:**
Resuelva cada uno de los siguientes problemas.

i.- Encuentre las soluciones de $x^2 \equiv -1(55)$.

ii.- Resuelva el sistema: $2x + 3 \equiv 0(5)$, $2x + 5 \equiv 0(11)$.

Desarrollo:

i.- Observe que $(-10)^2 = 100 = -10$. Luego $-10 = 45$ es un elementos idempotente central de $A = \mathbb{Z}/55\mathbb{Z}$. Además 11 es otro elemento del mismo tipo. Por lo tanto $A \cong -10\mathbb{Z}/55\mathbb{Z} \times 11\mathbb{Z}/55\mathbb{Z} \cong \mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$. Observe que $(\mathbb{Z}/11\mathbb{Z})^2 = \{0, 1, 4, 9, 5, 3\}$. Luego $x^2 \equiv -1(11)$ no tiene solución a $x^2 \equiv -1(55)$. Esto pues si la hubiera, entonces cualquier x_0 solución de esta cumpliría con $(-10x_0)^2 = -1(11)$.

ii.- Resolvamos cada ecuación en cada cociente. En efecto $x \equiv 1(5)$ y $x \equiv -30 \equiv 3(11)$. Luego todo representante de una solución de la ecuación cumple con $x = 1 - 5n$, para algún $n \in \mathbb{Z}$. Por lo tanto $1 - 5n \equiv 3(11)$.

Así obetenemos que $5n \equiv -2(11)$. Luego $n \equiv 4(11)$. Es decir $n = 4 + 11k$, para cierto $k \in \mathbb{Z}$. Por lo tanto $x = 1 - 5n = 1 - 20 + 55k = -19 + 55k$. Es decir $x \equiv -19(55) \equiv 26(55)$.

5.- **Ejercicio:** Encuentre las soluciones del sistema: $2x^2 \equiv 3(11)$, $5x + 4 \equiv 0(3)$.

Ayudantía XII: En esta ayudantía estudiaremos ideales primos y maximales. Además se analizará el nilradical $\mathfrak{N}(A)$ y el radical de Jacobson $J(A)$ de ciertos anillos A.

1.- **Problema 1:**
El siguiente problema tiene por objetivo determinar el radical de Jacobson y el nilradical de $\mathbb{Z}/n\mathbb{Z}$. Sea A, A_1, A_2 anillos conmutativos con 1.

i.- Pruebe que $I \subset A_1 \times A_2$ es un ideal primo si y solamente si $I = A_1 \times P_2$ o $I = P_1 \times A_2$, para $P_1 \subset A_1$, $P_2 \subset A_2$ ideales primos.

ii.- Demuestre que $P \subset \mathbb{Z}/n\mathbb{Z}$ es un ideal primo si y solamente si P es maximal.

ii.- Concluya que $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) = J(\mathbb{Z}/n\mathbb{Z})$.

iv.- Pruebe que $\mathfrak{N}(A_1 \times A_2) = \mathfrak{N}(A_1) \times \mathfrak{N}(A_2)$.

v.- Calcule $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z})$.

Desarrollo:

i.- Observe que $A_1 \times A_2$ es un anillo conmutativo con uno. POr lo tanto $I = I_1 \times I_2$ ideal de $A_1 \times A_2$ es un ideal primo si y solamente si $A_1 \times A_2/(I_1 \times I_2)$ es un dominio de integridad. Pero $A_1 \times A_2/(I_1 \times I_2) \cong A_1/I_1 \times A_2/I_2$ es un dominio de integridad si uno de los factores es nulo y el otro es un dominio de integridad. Luego $I = A_1 \times P_2$ o $I = P_1 \times A_2$, para $P_1 \subset A_1$, $P_2 \subset A_2$ ideales primos.

ii.- Recoredemos que por teorema de correspondencia $P = m\mathbb{Z}/n\mathbb{Z}$. Luego $(\mathbb{Z}/n\mathbb{Z})/P \cong \mathbb{Z}/m\mathbb{Z}$ es un dominio de integridad si y solamente si m es primo. Es así como $(\mathbb{Z}/n\mathbb{Z})/P$ es cuerpo. Luego P es un ideal maximal. Por otro lado todo ideal maximal, en un anillo conmutativo con unidad, es un ideal primo.

iii.- Como sabemos $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) = \cap_{P \text{ primo}} P$ y $J(\mathbb{Z}/n\mathbb{Z}) = \cap_{M \text{ maximal}} M$. Luego como los ideales primo y maximales del anillo en cuestión son iguales, tenemos que $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) = J(\mathbb{Z}/n\mathbb{Z})$.

iv.- Como sabemos $\mathfrak{N}(A_1 \times A_2) = \cap\{P : P \subset A_1 \times A_2 \text{ primo}\}$. Pero los ideales primos de $A_1 \times A_2$ son de la forma $I = A_1 \times P_2$ o $I = P_1 \times A_2$, para $P_1 \subset A_1$, $P_2 \subset A_2$ ideales primos. Luego $\mathfrak{N}(A_1 \times A_2) = \cap\{P : P \subset A_1 \text{ primo}\} \times \cap\{P : P \subset A_2 \text{ primo}\} = \mathfrak{N}(A_1) \times \mathfrak{N}(A_2)$.

v.- Por el teorema chino de los restos tenemos que si $n = p_1^{a_1} \cdots p_n^{a_n}$ entonces $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_n^{a_n}\mathbb{Z}$. Aplicando [iv] tenemos que $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) \cong \mathfrak{N}(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times \mathfrak{N}(\mathbb{Z}/p_n^{a_n}\mathbb{Z})$. Pero por lo calculado en al ayundatía anterior sabemos que $\mathfrak{N}(\mathbb{Z}/p^r\mathbb{Z}) = p\mathbb{Z}/p^r\mathbb{Z}$, para todo p primo y $r > 0$. Luego $\mathfrak{N}(\mathbb{Z}/n\mathbb{Z}) \cong p_1\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times p_n\mathbb{Z}/p_n^{a_n}$.

1.- **Ejercicio:** Calcule el nilradical y el radical de Jacobson de $\mathbb{Z}$. Demuestre que ambos ideales coinciden.

2.- **Problema 2:**
Pruebe que $I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} : b \in \mathbb{Q} \right\}$ es un ideal del anillo no conmutativo $A = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{Q} \right\}$. Demuestre que I no es un ideal primo.

Demostración: Considere el homomorfismo $\phi : A \to \mathbb{Q} \times \mathbb{Q}$ definido

por $\phi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c)$. Observe que ϕ es un homorfismo sobreyectivo y $\ker(\phi) = I$. Luego I es un ideal bilátero de A tal que $A/I \cong \mathbb{Q} \times \mathbb{Q}$. Observe que A no es un anillo conmutativo por ello no podemos aplicar el criterio que nos dice que I ideal primo si y solamente si A/I es un dominio de integridad. Pero si podemos extraer las mismas ideas que estan en su demostración. Observe que A/I tiene divisores de O. Por elemplo $(1, 0)$ y $(0, 1)$ cumplen con esto. Tomando las preimagenes de estos elementos vía ϕ obetenmos que $x = \begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}, y = \begin{pmatrix} 0 & b' \\ 0 & 1 \end{pmatrix} \notin I$, para cualquiera $b, b' \in \mathbb{Q}$. Pero su producto $xy = \begin{pmatrix} 0 & b+b' \\ 0 & 0 \end{pmatrix} \in I$. Luego I no es un ideal primo.

3.- **Problema 3:**
Sea $I = (3) \subset \mathbb{Z}[i]$. Demuestre que I es un ideal primo de $\mathbb{Z}[i]$. Pruebe que I es también un ideal maximal.

Demostración: Para demostrar esto debemos clacular en cociente $\mathbb{Z}[i]/I$. Observe que $\mathbb{Z}[i]/(3) \cong \mathbb{Z}[x]/(3, x^2 + 1)$, ya que $\mathbb{Z}[i] \cong \mathbb{Z}[x]/(x^2 + 1)$ y $(3) \cong (3, x^2 + 1)/(x^2 + 1)$. Donde ambos isomorfismos se establecen vía la evaluación en i. Luego:

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

Pero si usamos el tercer teorema de isomorfía obetenemos que:

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

Si usamos nuevamente el tercer teorema de isomorfía obtenemos que:

$$\mathbb{Z}[i]/(3) \cong \mathbb{F}_3[x]/(1 + x^2).$$

Pero (x^2+1) es un ideal maximal en $\mathbb{F}_3$ pues si no fuese así $p(x) = x^2+1$ se escribiría como dos factores de grado 1 en $\mathbb{F}_3$. Luego $p(x)$ tendría raices en $\mathbb{F}_3$. Pero esto último no sucede pues $p(1) = p(-1) = 2$ y $p(0) = 1$. Luego $\mathbb{F}_3[x]/(1 + x^2)$ es cuerpo. Por lo tanto $I = (3)$ es un ideal maximal de $\mathbb{Z}[i]$, en particular es un ideal primo de dicho anillo.

3.- **Ejercicio:** Sea $I = (5) \subset \mathbb{Z}[i]$. Demuestre que I no es un ideal primo de $\mathbb{Z}[i]$. Calcule el cociente $\mathbb{Z}[i]/I$.

4.- **Problema 4:**
Sea $A = \mathbb{C}[x]/(x^2 - 3x + 2)$.
i.- Encuentre los ideales primos y maximales de A.
ii.- Calcule $\mathfrak{N}(A)$ y $J(A)$.

Desarrollo:
i.- Primero reescribamos el anillo A. Observe que $x^2 - 3x + 2 = (x - 1)(x - 2)$, donde $1 = (x-1)-(x-2)$. Por lo tanto $(x^2-3x+2) = (x-1)(x-2)$ donde $(x - 2) + (x - 1) = \mathbb{C}[x]$. Aplicando teorema chino de los restos obtenemos $A \cong \mathbb{C}[x]/(x - 1) \times \mathbb{C}[x]/(x - 2) \cong \mathbb{C} \times \mathbb{C}$. Luego debemos encontrar los ideales primos y maximales de $\mathbb{C} \times \mathbb{C}$. Aplicando lo dicho en el problema 1 tenemos que $\{\mathbb{C} \times \{0\}, \{0\} \times \mathbb{C}\}$ es el conjunto de ideales primos, el cual coincide con el conjunto de ideales maximales de A módulo isomorfismo.

De hecho, dicho conjunto de ideales corrsponde en A a $\{(x-1)/(x^2-3x+2), (x-2)/(x^2-3x+2)\}$.

ii.- Como sabemos $\mathfrak{N}(A) = \cap_{P \text{ primo}} P$ y $J(A) = \cap_{M \text{ maximal}} M$. Luego $J(A) = \mathfrak{N}(A) = \{0\}$.

5.- **Problema 5:**
Sea A anillo conmutativo con 1 tal que para todo $x \in A$ se tiene que $x^n = x$, para $n > 1$. Pruebe que todo ideal primo de A es maximal.

Demostración: Sea P un ideal primo de A. Entonces A/P es un dominio de integridad. Sea $x \in A$ tal que $x \notin P$, es decir $\overline{x} \in A/P$ es no nulo. Luego, como $x^n = x$ en A, tomando clases de los elementos en el cociente obtenemos que $\overline{x}^n = \overline{x}$. Es así como obtenemos que $\overline{x}(\overline{x}^{n-1} - \overline{1}) = \overline{0}$. Luego como A/P es dominio de integridad y $\overline{x} \neq \overline{0}$ tenemos que $\overline{x}\overline{x}^{n-2} = \overline{1}$. Por lo tanto en el anillo conmutativo A/P todo elemento no nulo es invertible. Luego A/P es cuerpo, equivalentemente P es un ideal maximal.

5.- **Ejercicio:** un anillo A se dice **Booleano** si $x^2 = x$, para todo $x \in A$. Muestre que todo ideal $P \subset A$ primo es maximal y que A/P es un cuerpo con dos elementos.

Ayudantía XIII: En esta ayudnatía estudiaremos los dominios euclideanos.

1.- **Problema 1:**
Muestre que $A = \mathbb{Z}[\sqrt{2}]$ 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 r es un resto. Esto demuestra que $\mathbb{Z}[\sqrt{2}]$ es dominio euclideano.

1.- **Ejercicio:** Pruebe que $\mathbb{Q}[w][x]$ es un dominio euclieano, donde $w = e^{\frac{2\pi i}{3}}$.

2.- **Problema 2:**
Escriba $I = (x + 3, x^5 + 7) \subseteq \mathbb{R}[x]$ como un ideal principal.

Desarrollo: Para encontrar un generador del grupo hay que aplicar el algoritmo de división entre $x+3$ y x^5+7 de forma de escribir $I = (x+3, c)$, donde $c \in \mathbb{R}$. En efecto $x^5 + 7 = (x + 3)(x^4 - 3x^3 + 9x^2 - 27x + 81) - 236$. Luego $I = (x + 3, -236) = \mathbb{R}[x]$, pues I contiene al elemento -236 que es invertible en $\mathbb{R}[x]$. Concluimos que $I = (1)$.

2.- **Ejercicio:** Escriba $(x^2 - nx + n, x^2 - mx + m) \subseteq \mathbb{R}[x]$ como un ideal principal, dependiendo de los valores de $n, m \in \mathbb{R}$.

3.- **Problema 3:**
Sea A un dominio de integridad, tal que $A[x]$ es un dominio de ideales principales. Es decir en $A[x]$ todo ideal es principal.

i.- Demuestre que A es cuerpo.

ii.- ¿Es $\mathbb{Z}[i][x]$ dominio de ideales principales?

3.- **Desarrollo:**

i.- 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.

ii.- 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 elementos invertibles en el anillo de enteros gaussianos es $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

4.- **Problema 4:**
Encuentre todos los ideales maximales $I \subseteq \mathbb{Z}[i]$ tales que $17 \in I$.

Desarrollo: Supongamos que I es un ideal maximal tal que $17 \in I$. Como $\mathbb{Z}[i]$ es un DIP tenemos que $I = (z)$, cierto $z \in \mathbb{Z}[i]$. Luego si $17 \in I$ tenemos que $z|17$. De hecho $z|17$ si y solamente si $17 \in (z)$. Pero $17 = (4+i)(4-i)$. Luego $4+i \in I$ o $4-i \in I$, pues I es maximal, en particular un ideal primo. Es decir $(4-i) \subseteq I$ o bien $(4+i) \subseteq I$. Por otro lado $(4 \pm i)$ cumple con $\mathbb{Z}[i]/(4 \pm i) \cong \mathbb{Z}[x]/(x^2+1, 4 \pm x) \cong \mathbb{Z}/(16+1) \cong \mathbb{F}_{17}$. Luego $(4 \pm i)$ es un ideal maximal de $\mathbb{Z}[i]$. Por lo tanto $I = (4+i)$ o bien $I = (4-i)$. En particular, esto nos dice que los únicos divisores no triviales de 17 en $\mathbb{Z}[i]$ son $4+i$ y $4-i$.

4.- **Ejercicio:** Encuentre todos los ideales maximales $I \subseteq \mathbb{Z}[w]$ tales que $2 \in I$, donde $w = e^{\frac{2\pi i}{3}}$.

Ayudantía XIV: En esta ayudantía seguiremos estudiando los dominios euclideanos. En particular analizaremos los ideales principales y el máximo común divisor.

1.- **Problema 1:**
Calcule el máximo común divisor entre $3+i$ y $5+i$ en $\mathbb{Z}[i]$. Use esto para determinar un generador del ideal $(3+i, 5+i)$ en $\mathbb{Z}[i]$.

Desarrollo: Observe que $2 = 5+i-(3+i)$. Luego si d divide a $5+i$ y $3+i$ entonces d divide a 2. Por otro lado 2 no divide a $5+i$ ni a $3+i$. Ahora bien $2 = -i(1+i)^2$, donde $(1+i)$ es maximal. Luego debemos buscar entre los divisores de este número el máximo común divisor de $5+i$ y $3+i$. Por otro lado $(1+i)(2-i) = 3+i$ y $(1+i)(3-2i) = 5+i$. Por lo tanto $(2) \subsetneq (3+i, 5+i) \subset (i+1)$. Pero $i+1 = 2(3+i)-(5+i)$. Luego $(3+i, 5+i) = (1+i)$. Esto prueba que el máximo común divosor entre $3+i$ y $5+i$ es $1+i$ y que $(3+i, 5+i) = (1+i)$.

1.- **Ejercicio:** Calcule el máximo común divisor entre $3+w$ y $5+w$ en $\mathbb{Z}[w]$, donde $w = e^{\frac{2\pi i}{3}}$.

2.- **Problema 2:**
Calcule el máximo común divisor entre 1527 y 321 en $\mathbb{Z}$. Use algoritmo de división. Escriba el máximo común divisor como una combinación lineal entera de 1527 y 321.

Desarrollo: Useamos el algoritmo de división. En efecto tenemos que $1527 = 4 \cdot 321 + 243$, $321 = 1 \cdot 243 + 78$, $243 = 3 \cdot 78 + 9$, $78 = 8 \cdot 9 + 6$, $9 = 1 \cdot 6 + 3$ y $6 = 2 \cdot 3 + 0$. Por lo tanto el máximo común divisor entre 1527 y 321 es 3. Observe que de las igualdades anteriores se desprende la igualdad $3 = 37 \cdot 1527 - 176 \cdot 321$.

2.- **Ejercicio:** Calcule el máximo común divisor entre 15268976 y 31 en $\mathbb{Z}$.

3.- **Problema 3:**
Sea $A = \mathbb{Z}[\sqrt{-5}] \subset \mathbb{C}$ y defina el ideal $I_2 = (2, 1+\sqrt{-5})$.

i.- Demuestre que I_2 es un ideal maximal de A.

ii.- Pruebe que I_2 no es un ideal principal.

iii.- Concluya que A no es un DE.

iv.- Pruebe que $I_2^2 = (2)$.

3.- **Desarrollo:**

i.- Observe que $A/I_2 \cong \mathbb{Z}[x]/(2, 1+x, x^2+5) \cong \mathbb{Z}/(2,6) = \mathbb{Z}/2\mathbb{Z}$. Por lo tanto A/I_2 es cuerpo. Esto último es equivalente a que I_2 sea un ideal maximal de A.

ii.- Supongamos que I_2 es un ideal principal, entonces $I_2 = (d)$, para cierto $d = a + b\sqrt{-5} \in A$. Entonces $2 = ad$ y $1+\sqrt{-5} = bd$, para ciertos $a, b \in A$. Tomando norma compleja en las igualdades anteriores, obtenemos que $N(a)N(d) = 4$ y $N(b)N(d) = 6$. Luego $N(d) \in \{1, 2\}$. Observe que si $N(d) = d\overline{d} = 1$ entonces $d \in A$ es invertible. Por lo tanto $I_2 = (d) = A$, lo que es contradictorio con lo dicho en [i]. Por lo tanto $N(d) = 2$. Luego $a^2 + 5d^2 = 2$ tiene solución con $a, d \in \mathbb{Z}$, lo que es falso. Por ello I_2 no es un ideal principal.

iii.- Sabemos que en un DE todo ideal es principal. Luego si A fuera un DE entonces I_2 sería un ideal principal, lo que contradice [ii].

iv.- Observe que $2 = (1+\sqrt{-5}-2)(1+\sqrt{-5}) - 2\cdot 2 \in I_2^2$. Por lo tanto $(2) \subseteq I_2^2$. Por otro lado, tenemos que el producto de dos elementos cualquiera de I_2 cumple con $(2z+(1+\sqrt{-5})w)(2a+(1+\sqrt{-5})b) = 4az + 2(aw(1+\sqrt{-5}) + zb(1+\sqrt{-5})) + 6wb + 2(1+\sqrt{5})wb \in (2)$. Esto prueba que $(2) \supseteq I_2^2$. Por lo tanto $I_2^2 = (2)$.

3.- **Ejercicio:** Pruebe que $I_3 = (3, 2+\sqrt{-5})$ y $I_3' = (3, 2-\sqrt{-5})$ son ideales maximales distintos y no principales en $\mathbb{Z}[\sqrt{-5}]$. Pruebe además que $I_3 I_3' = (3)$.

4.- **Problema 4:**
Demuestre las siguientes afirmaciones:
i.- Pruebe que $\big(\mathbb{C}[x]/(x^2+5)\big)[y]$ no es un DE.
ii.- Pruebe que $\big(\mathbb{Q}[x]/(x^2+5)\big)[y]$ es un DE.
Desarrollo:

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

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

4.- **Ejercicio:** Encuentre el máximo común divisor entre x^2+1 y $p(x) = x^3 + (i+5)x^2 + (7+5i)x + 7i$ en $\mathbb{C}[x]$. Evalue $p(x)$ en $\pm i$ y luego divida.

Ayudantía XV: En esta ayudantía seguiremos estudiando los dominios euclideanos. Haremos una miselanea de ejercicios.

1.- **Problema 1:**
Demuestre que $2+i$ y $2-i$ son relativamente primos en $\mathbb{Z}[i]$. Utilice esto para probar que el caballo recorre todo el tablero de ajedréz infinito.

Desarrollo: Observe que $2+i-(2-i)=2i$. Luego si $d=mcd(2+i,2-i)$ tenemos que d divide a $2i$. Por lo tanto $N(d)$ divide a 4. Por otro lado d divide a $2+i$, por lo tanto $N(d)$ divide a 5. Esto implica que $N(d)=1$. Luego $d\in\{\pm 1,\pm i\}$. Por lo tanto $2+i$ y $2-i$ son relativamente primos. Supongamos ahora que C es el conjunto que describe las posbibles coordenadas del caballo en el tablero. Identifiquemos la segunda coordenada con $i\in\mathbb{C}$. Luego el tablero infinito se identifica con el reticulado $\mathbb{Z}[i]$. Observe que, componiendo los movimientos del caballo, en C están todos los elementos de la forma $a(2+i)$, $b(2+i)$, $c(2i+1)$, $d(2i-1)$, donde $a,b,c,d\in\mathbb{Z}$. Por lo tanto $(2+i,2-i)\subset C$. Pero $(2+i,2-i)=\mathbb{Z}[i]$. Luego $C=\mathbb{Z}[i]$. Por lo anto el caballo recorre todo el tablero de ajedréz.

1.- **Ejercicio:** Suponga que el caballo de puede mover de a 4 casillas en linea recta y luego girar en noventa grados para moverse una casilla más. Describa los puntos en el tablero infito a los cuales puede llegar dicho caballo.

2.- **Problema 2:**
Encuentre la factorización en primos de $6\in\mathbb{Z}[w]$, para $w=e^{\frac{2\pi i}{3}}$.

Desarrollo: Observe que $6=2\cdot 3$ en $\mathbb{Z}[w]$. Luego por la unicidad de la factorización basta encontrar la descomposición en primos de 2 y 3 en $\mathbb{Z}[w]$. Para comenzar, observe que $\mathbb{Z}[w]/(2)\cong\mathbb{Z}[x]/(x^2+x+1,2)\cong\mathbb{F}_2[x]/(x^2+x+1)$. Ahora bien $p(x)=x^2+x+1$ genera un ideal maximal ya que $p(x)$ no se factoriza en $\mathbb{F}_2[x]$. Esto último se debe a que $p(X)$ no tiene raices en $\mathbb{F}_2$. Por lo tanto $\mathbb{Z}[w]/(2)$ es un cuerpo, luego 2 es un elemento primo en $\mathbb{Z}[w]$. Por otro lado, tenemos que $\mathbb{Z}[w]/(3)\cong\mathbb{Z}[x]/(x^2+x+1,3)\cong\mathbb{F}_3[x]/(x^2+x+1)=\mathbb{F}_3[x]/((x-1)^2)$. Por teorema de correspondencia los ideales maximales que contienen a (3) son los ideales de $\mathbb{Z}[w]/(3)$. Estos últimos ideales están en correspondencia con los elementos en $\mathbb{Z}[w]$ que dividen a 3. Observe que el único ideal no trivial de $\mathbb{F}_3[x]/((x-1)^2)$ es $(x-1)/((x-1)^2)$. Tomando preimagen vía los isomorfismos anteriores obtenemos que $3\in(w-1)$. De hecho $3=w(1-w)^2$, donde $\mathbb{Z}[w]/(w-1)\cong\mathbb{F}_3$. Por lo tanto $w-1$ es un elemento primo de $\mathbb{Z}[w]$. Esto prueba que la descomposición de $6\in\mathbb{Z}[w]$ es $6=w2(w-1)^2$, donde $w\in\mathbb{Z}[w]^*$.

2.- **Ejercicio:** Encuentre la factorización en primos de $210\in\mathbb{Z}[w]$, para $w=e^{\frac{2\pi i}{3}}$.

3.- **Problema 3:**
Muestre que todo ideal bilátero de $\mathbb{M}_2(\mathbb{Z})$ es principal.

Demostración: Sabemos que todo ideal bilátero I de $\mathbb{M}_2(\mathbb{Z})$ es de la

forma $I = \mathbb{M}_2(J)$, donde J es un ideal de $\mathbb{Z}$. Pero como $\mathbb{Z}$ es un dominio euclideano, tenemos que $J = N\mathbb{Z}$, para cierto $N \in \mathbb{Z}$. Luego $I = \mathbb{M}_2(N\mathbb{Z}) = (N\text{id})\mathbb{M}_2(\mathbb{Z})$. Por lo tanto el ideal I es principal.

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 $I_m = I_n$, $\forall n \geq m$.

Demostración: Observe que por lo visto en la ayudantía anterior $A = \mathbb{Z}[\sqrt{2}]$ es un dominio euclideano (DE), luego 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.

Ayudantía XVI: En esta ayudantía desarrollaremos problemas de todo lo visto en anillos.

1.- **Problema 1:**
Sean I, J ideales de A un anillo conmutativo con uno.

i.- Demuestre que si $I + J = A$ entonces $I \cap J = IJ$.

ii.- Demuestre que si $I + J = A$ entonces $I^2 + J^2 = A$.

Desarrollo:

i.- Observe que siempre $IJ \subset I \cap J$. Esto se debe a que cualquier elemento $\sum_{i=1}^{r} a_i b_i \in I, J$, para $a_i \in I$ y $b_j \in J$. Esto último se debe a que I, J son ideales biláteros. Por otro lado si $I + J = A$ entonces exiten $a \in I$, $b \in J$ tales que $a+b = 1$. Considere $c \in I \cap J$ entonces $c = ca+cb = ac+cb \in IJ$.

ii.- Para mostrar que $A = I^2 + J^2$ basta probar que $1 = x + y$, con $x \in I^2$ e $y \in J^2$. Pero sabemos que $1 = a + b$ para $a \in I$ y $b \in J$. Luego $1 = a^2 + b^2 + ab + ba \in I^2 + J$. Por lo tanto $I^2 + J = A$. Repitiendo el mismo argumento para subir el exponente de J, obtenemos que $I^2+J^2 = A$.

1.- **Ejercicio:** Encuentre ideales I, J de un anillo A tal que $IJ \subsetneq I \cap J$.

2.- **Problema 2:**
Considere $\mathbb{C}[x]$ el anillo de polinomios con coeficientes en $\mathbb{C}$.

i.- Sea $n \in \mathbb{Z}_{>0}$. Pruebe que $\mathbb{C}[x]/((x-1)^n)$ no es producto de anillos no triviales.

ii. Demuestre que $\mathbb{C}[x]/(x^2-1)$ es un producto de anillos. Encuentre su descomposición.

Desarrollo:

i.- Considere $p(x)$ polinomio en $\mathbb{C}[x]$. Entonces $(x-1)|p(x)$ o bien $p(x)$ y $(x-1)$ son relativamente primos. En el primer caso tenemos que $\overline{p(x)}^n = \overline{0}$ y en el segundo $\overline{p(x)}$ es invertible en $A = \mathbb{C}[x]/((x-1)^n)$. Mostremos que A no tiene elementos idempotentes no triviales. En efecto si $\overline{p(x)}$ es idempotente tenemos que $\overline{p(x)}^2 = \overline{p(x)}$. Supongamos que $\overline{p(x)}$ es nilpotente y no nulo. Considere $N = \min\{n \in \mathbb{Z}_{>0} : \overline{p(x)}^n = 0\}$ entonces $0 = \overline{p(x)}^N = \overline{p(x)}^{N-1}$, lo que nos lleva a una contradicción. Por lo tanto $\overline{p(x)} = \overline{0}$. Supongamos ahora que $\overline{p(x)}$ es invertible, entonces multiplicando por su inverso la relación de idempotencia, obtenemos que $\overline{p(x)} = \overline{1}$. Luego A no tiene elementos idempotentes no triviales. Por ello A no es producto de anillos no triviales.

ii.- Sabemos que $(x^2-1) = (x-1)(x+1)$, donde $(x-1)+(x+1) = \mathbb{C}[x]$. Por lo tanto por teorema chino de los restos, tenemos que $\mathbb{C}[x]/(x^2-1) \cong \mathbb{C}[x]/(x-1) \times \mathbb{C}[x]/(x+1) \cong \mathbb{C} \times \mathbb{C}$.

3.- **Problema 3:**
Sea A anillo conmutativo con uno y $\mathfrak{N}(A)$ su nilradical. Pruebe que son equivalentes los siguientes hechos:

i.- A tiene un solo ideal primo.

ii.- Todo elemento de A es unidad o nilpotente.

iii.- $A/\mathfrak{N}(A)$ es un cuerpo.

Demostración:

i-ii .- Supongamos que $x \in A$ no es un elemento invertible. Entonces $x \in P$ para P el único ideal maximal de A, que a su vez es un ideal primo. Observe que $P = \mathfrak{N}(A)$. Luego $x \in A$ es nilpotente.

ii-iii .- Observe que $A/\mathfrak{N}(A)$ es un anillo conmutativo con uno. Sea $\overline{x} \in A/\mathfrak{N}(A)$ elemento no nulo. Entonces $x \notin \mathfrak{N}(A)$. Luego $x \in A$ es invertible, es decir existe $y \in A$ tal que $xy = 1$ en A. Por ello $\overline{xy} = \overline{1}$. Esto implica que $A/\mathfrak{N}(A)$ es cuerpo.

iii-i .- Si $A/\mathfrak{N}(A)$ es un cuerpo entonces $\mathfrak{N}(A)$ es un ideal maximal, en particular primo. Supongamos que existe otro ideal primo $P \subset A$ entonces $\mathfrak{N}(A) \subset P \subsetneq A$. Por la maximalidad de $\mathfrak{N}(A)$ tenemos que $P = \mathfrak{N}(A)$. Por ello A tiene un solo ideal maximal.

3.- **Ejercicio:** Sea $n \in \mathbb{Z}_{>0}$. Pruebe que $\mathbb{C}[x]/((x-1)^n)$ tiene un solo ideal primo. Calculelo. Muestre que el nilradical de este anillo es un ideal maximal.

4.- **Problema 4:**
Sea $w = e^{\frac{2\pi i}{3}}$. Encuetre $a, b \in \mathbb{Z}[w]$ tales que $a(2+w) + b(3+2w) = 1$. No use algoritmo de división.

Desarrollo: Emplearemos la norma compleja restringida a $\mathbb{Z}[w]$, donde $w = \frac{-1+\sqrt{-3}}{2}$. Observe que $z = a+bw$ cumple con $N(z) = (a+bw)(a+b\overline{w}) = \left(\left(a - \frac{b}{2}\right) + \frac{b\sqrt{-3}}{2}\right)\left(\left(a - \frac{b}{2}\right) - \frac{b\sqrt{-3}}{2}\right) = a^2 - ab + b^2 \in \mathbb{Z}_{\geq 0}$. Luego $N(2+w) = 4$ y $N(3+2w) = 7$. Ahora bien, dichos números son coprimos en $\mathbb{Z}$. De hecho $1 = 7 - 2\cdot 3$. Por otro lado sabemos que $\overline{w} = w^2 = -1-w$, por lo tanto $1 = (3+2w^2)(3+2w) - 2(2+w^2)(2+w) = (1-2w)(3+2w) - 2(1-w)(2+w)$. Luego $a = -2 + 2w$ y $b = 1 - 2w$.

4.- **Ejercicio:** Replique lo mismo para la ecuación $a(2+i) + b(5+i) = 1$ en $\mathbb{Z}[i]$.

Ayudantía XVII: En esta ayudantía desarrollaremos problemas de todo lo visto en anillos.

1.- **Problema 1:**
Sean A anillo sin uno. Sea $R = A \times \mathbb{Z}$ con suma usual y producto $(a,n)(b,m) = (ab + na + mb, nm)$. Asumiendo que R es anillo pruebe lo siguiente:

i.- Demuestre que R sí tiene uno.

ii.- Demuestre que A es isomorfo a un subanillo de R.

Desarrollo:

i.- Observe que $(0,1) \in R$ cumple con $(0,1)(a,n) = (0+1\cdot a, n) = (a,n)(0,1)$. Por lo tanto R es un anillo con unidad.

ii.- Considere el homomorfismo $\phi : A \to R$ definido por $\phi(a) = (a,0)$. Dicha función es homomorfismo pues $\phi(a+b) = (a+b,0) = (a,0) + (b,0)$ y $\phi(a)\phi(b) = (a,0)(b,0) = (ab,0) = \phi(ab)$. Observe que $\ker(\phi) = \{0\}$. Por ello ϕ es inyectivo. Luego $A \cong Im(\phi)$ que es un subanillo de R.

i.- **Ejercicio:** Pruebe que el anillo R presentado anteriormente es un anillo.

2.- **Problema 2:**
Sea $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} \in \mathbb{N}$.

i.- Demuestre que $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^*$.

ii. Determine la estructura del grupo de unidades $(\mathbb{Z}/90\mathbb{Z})^*$.

Desarrollo:

i.- Sabemos que $(a,b) \in A \times B$ es invertible si y solamente si existe (c,d) tal que $(ac,bd) = (a,b)(c,d) = (1,1)$. Es decir $ac = 1$ y $db = 1$. Luego $(a,b) \in A \times B$ es invertible si y solamente si $a, b \in A$ son elementos invertibles. Es decir $(A \times B)^* = A^* \times B^*$. Por otro lado, si aplicamos el teorema chino de los restos tenemos que $(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})$. Luego si aplicamos el resultado anterior inductivamente, obtenemos que $(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^* \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^*$.

ii.- Usando el resultado anterior tenemos que $(\mathbb{Z}/90\mathbb{Z})^* \cong (\mathbb{Z}/4\mathbb{Z})^* \times (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^*$. Pero $(\mathbb{Z}/4\mathbb{Z})^* = \{1,3\} \cong C_2$, pues es el único grupo de orden 2. Lo mismo para $\mathbb{Z}/3\mathbb{Z})^* = \{1,2\} \cong C_2$. Por otro lado $(\mathbb{Z}/5\mathbb{Z})^* = \{1,2,3,4\}$ cumple con que $(2) = \{1,2,4,3\}$. Luego $(\mathbb{Z}/5\mathbb{Z})^* \cong C_4$. Por lo tanto $(\mathbb{Z}/90\mathbb{Z})^* \cong C_2 \times C_2 \times C_4$.

2.- **Ejercicio:** Calcule $G = (\mathbb{Z}/24\mathbb{Z})^*$. Demuestre que G no es un grupo cíclico.

3.- **Problema 3:**
Sea A anillo conmutativo con uno y $a_0, \cdots, a_n \in A$.

i.- Pruebe que si $a_0, \cdots, a_n$ son elementos nilpotentes entonces $p(x) = a_0 + \cdots + a_n x^n \in A[x]$ es un polinomio nilpotente.

ii.- Pruebe que si a_0, es invertible y $a_1, \cdots, a_n$ son elementos nilpotentes entonces $p(x) = a_0 + \cdots + a_n x^n \in A[x]$ es un polinomio invertible.

iii.- Concluya que $3x^2 + 6x + 1 \in \mathbb{Z}/27\mathbb{Z}[x]$ es un polinomio invertible.

Demostración:

i.- Observe que si $a_i^{n_i} = 0$ entonces $(a_i x)^{n_i} = 0$. Luego $p(x)$ es suma de elementos nilpotentes. Como el conjunto de elementos nilpotentes es un ideal obtenemos que $p(x)$ es nilpotente.

ii.- Observe que si a_0 es invertible y $a_1, \cdots, a_n$ son nilpotentes entonces $p(x) = a_0 + q(x)$, donde $q(x)$ es nilpotente. Esto último debido a lo mostrado en [i]. Luego, como toda suma de un elemento nilpotente con un elemento invertible es invertible en un anillo conmutativo, obtenemos que $p(x)$ es invertible.

iii.- Sabemos que $3, 6 \in \mathbb{Z}/27\mathbb{Z}$ son elementos nilpotentes. Luego como 1 es invertible tenemos por [ii] que $3x^2 + 6x + 1 \in \mathbb{Z}/27\mathbb{Z}[x]$ es un polinomio invertible.

3.- **Ejercicio:** Pruebe que si $p(x) = a_0 + \cdots + a_n x^n \in A[x]$ es nilpotente entonces $a_0, \cdots, a_n \in A$ son elementos nilpotentes.

4.- **Problema 4:**
Encuentre condiciones sobre $p(x) \in \mathbb{C}[x]$ necesarias y suficientes para que $\mathbb{C}[x]/(p(x))$ sea cuerpo.

Desarrollo: Sea $p(x) \in \mathbb{C}[x]$ un polinomio cualquiera de grado n. Entonces como $\mathbb{C}$ es algebraicamente cerrado, tenemos que $p(x)$ tiene todas sus raices en $\mathbb{C}$. Luego $p(x) = (x - z_1) \cdots (x - z_n)$, para ciertos $z_i \in \mathbb{C}$. Agrupemos los términos iguales en la factorización de $p(x)$. Así tenemos que $p(x) = (x - z_1)^{n_1} \cdots (x - z_k)^{n_k}$. Observe que si $z_i \neq z_j$ entonces $(x - z_i) + (z - x_j) = \mathbb{C}[x]$. Por lo tanto, por teorema chino de los restos tenemos que $\mathbb{C}[x]/(p(x)) \cong \mathbb{C}[x]/((x-z_1)^{n_1}) \times \cdots \times \mathbb{C}[x]/((x-z_k)^{n_k})$. Si dicho anillo es un cuerpo entonces $k = 1$. Además en ese caso, para que no existan elemento nilpotentes en el anillo se requiere que $n_1 = 1$. Por ello $p(x) = x - z_1$. En dicho caso $\mathbb{C}[x]/(p(x)) \cong \mathbb{C}$. Luego la condición necesaria y suficiente para que el cociente anterior sea cuerpo es que el grado del polinomio $p(x)$ sea 1.

4.- **Ejercicio:** Demuestre que el ideal $M = (x - 1, y + 2)$ es un ideal maximal de $\mathbb{C}[x][y]$.

3. Cuerpos

Ayudantía XVIII: En esta ayudantía comenzaremos a estudiar la estructura de cuerpos. Nos enfocaremos en las la adjunción de elementos en un cuerpo.

1.- **Problema 1:**
Sea L una extensión finita de K un cuerpo. Pruebe que para todo $\alpha \in L$ existe $p(x) \in K[x]$ no nulo tal que $p(\alpha) = 0$.

Demostración: Considere $\alpha \in L$ elemento cualquiera y supongamos que $[L : K] = dim_K L = n < \infty$. Observe que el conjunto $X = \{1, \alpha, \cdots \alpha^n\}$ tiene $n+1$ elementos. Por lo tanto X es un conjunto linealmente dependiente. Luego existen $a_0, \cdots, a_n$ no todos nulos tales que $p(\alpha) = \sum_{i=0}^{n} a_i \alpha^i = 0$, donde $p(x) = \sum_{i=0}^{n} a_i x^i \in K[x]$ es un polinomio no nulo.

i.- **Ejercicio:** Encuentre una extensión L de $\mathbb{Q}$ de grado infinito tal que para todo $\alpha \in L$ existe $p(x) \in \mathbb{Q}[x]$ no nulo que cumple con $p(\alpha) = 0$.

2.- **Problema 2:**
Considere $p(x) = x^2 + x + 1 \in \mathbb{F}_2[x]$.

i.- Pruebe que $L = \mathbb{F}_2[x]/(p(x))$ es un cuerpo. Determine su grado sobre $\mathbb{F}_2$.

ii.- Calcule el inverso de $\overline{x+1} \in L$.

iii.- Pruebe que si L es una extensión de $\mathbb{F}_2$ tal que $[L : \mathbb{F}_2] = 2$ y $L = \mathbb{F}_2(\theta)$ entonces $L \cong \mathbb{F}_2[x]/(p(x))$.

Desarrollo:

i.- Observe que $(p(x)) \subset \mathbb{F}_2[x]$ es un ideal maximal. Esto se debe a que $p(x)$ no tiene raices en $\mathbb{F}_2$ y fue analizado en el problema 3 de la ayudantía XII. Luego $L = \mathbb{F}_2[x]/(p(x))$ es un cuerpo. Por último tenemos que $[L : \mathbb{F}_2] = dim_{\mathbb{F}_2}\mathbb{F}_2[x]/(p(x)) = deg(p(x)) = 2$.

ii.- Tenemos que encontrar polinomios $s(x), t(x) \in \mathbb{F}_2[x]$ tales que $p(x)s(x) + (x+1)t(x) = 1$, pues en este caso $\overline{(x+1)}^{-1} = t(x)$. En efecto $p(x) - x(x+1) = 1$. Luego $\overline{(x+1)}^{-1} = \overline{x}$.

iii.- Considere $L = \mathbb{F}_2(\theta)$ una extensión de grado 2 de $\mathbb{F}_2$. Considere el homomorfismo de anillos $\phi : \mathbb{F}_2[x] \to L$ definida por $\phi(s(x)) = s(\alpha)$. Entonces $\ker(\phi) = (t(x))$, para cierto $t(x) \in \mathbb{F}_2[x]$. Luego $\mathbb{F}_2[x]/(t(x)) \hookrightarrow L$. Comparando el grado sobre $\mathbb{F}_2$ tenemos que $deg(t(x)) \leq 2$. Supongamos que $deg(t(x)) = 1$, entonces $t(x) = x - a_0$, con $a_0 \in \mathbb{F}_2$. Por lo tanto, como $t(\alpha) = 0$ tenemos que $\alpha = a_0 \in \mathbb{F}_2$. Luego $L = \mathbb{F}_2$, lo que contradice el hecho de que $[L : \mathbb{F}_2] = 2$. Por lo tanto $deg(t(x)) = 2$ y por igualdad en la dimensión tenemos que $L \cong \mathbb{F}_2[x]/(t(x))$, en donde ambos anillos son cuerpos. Por lo tanto $t(x)$ es un polinomio irreducible de grado 2 en $\mathbb{F}_2$. Los polinomios de grado dos en $\mathbb{F}_2[x]$ son $\{x^2, x^2+1, x^2+x, x^2+x+1\}$ en donde $p(x) = x^2 + x + 1$ es el único irreducible. Por lo tanto $t(x) = p(x)$. Esto concluye lo pedido.

2.- **Ejercicio:** Demuestre que $p(x) = x^3 - x + 1$ es un polinomio irreducible en $\mathbb{F}_3[x]$. Concluya que $L = \mathbb{F}_3[x]/(p(x))$ es cuerpo.

3.- **Problema 3:**
Considere $L = \mathbb{Q}(\sqrt[n]{2}) \subset \mathbb{C}$. Pruebe que $[L : \mathbb{Q}] = n$.

Demostración: Considere el homomorfismo $\phi : \mathbb{Q}[x] \to L$ definido por $\phi(x) = \sqrt[n]{2}$. Entonces como $p(x) = x^n - 2$ es un polinomio tal que $p(\sqrt[n]{2}) = 0$ tenemos que existe un homomorfismo $\overline{\phi} : \mathbb{Q}[x]/(p(x)) \to L$. Observe que por criterio de Einsenstein tenemos que $p(x)$ es irreducible sobre $\mathbb{Q}$. Por lo tanto $\mathbb{Q}[x]/(p(x)) \subset \mathbb{C}$ es un cuerpo que contiene a $\sqrt[n]{2}$. Por lo tanto $L \hookrightarrow \mathbb{Q}[x]/(p(x))$. Por otro lado como $\overline{\phi}$ es un homomorfismo no nulo, cuyo dominio es un cuerpo, tenemos que $\mathbb{Q}[x]/(p(x)) \hookrightarrow L$. Por lo tanto $L \cong \mathbb{Q}[x]/(p(x))$. Luego $[L : \mathbb{Q}] = deg(p(x)) = n$.

4.- **Problema 4:**
Sea $L = K(\alpha) \cong K[x]/(p(x))$, donde $p(x) \in K[x]$ es un polinomio irreducible.

i.- Muestre que existe $\sigma : L \to L$ automorfismo tal que $\sigma \mid_K = id$.

ii.- Pruebe que $\sigma = id$ si $\{a \in L : p(x) = 0\} = \{\alpha\}$.

ii.- Pruebe que existe $\sigma \neq id$ si $|\{a \in L : p(x) = 0\}| > 1$.

Desarrollo:

i.- Observe que todo elemento $\alpha' \in L$ tal que $irr_{\alpha'}(x) = p(x)$ cumple con que $\phi : K[x]/(p(x)) \to L$, $\phi(x) = \alpha'$ es un isomorfismo, pues inyectivo, ya que $p(x)$ es irreducible y sobreyectivo pues $[L : K] = deg(p(x)) = [K[x]/(p(x)) : K]$. Además $\phi|_K = id$. Por lo tanto existe $\sigma : L \to K[x]/(p(x)) \to L$ definida por $\sigma(\alpha) = \alpha'$ homomorfismo inyectivo entre espacios de igual dimensión. Por ello σ es un isomorfismo tal que $\sigma|_K = id$.

ii.- Observe que para todo $\sigma : L \to L$ automorfismo tal que $\sigma \mid_K = id$, se tiene que $p(\sigma(\alpha)) = \sigma(p(\alpha)) = \sigma(0) = 0$. Luego $\sigma(\alpha) \in L$ es una raiz de $p(x)$. Luego si $\{a \in L : p(x) = 0\} = \{\alpha\}$ tenemos que $\phi(\alpha) = \alpha$. Por ello $\phi = id$, esto ya que $K(\alpha) = K \oplus K\alpha \oplus \cdots \oplus K\alpha^t$, donde $deg(p(x)) = t + 1$, pues $K(\alpha) \cong K[x]/(p(x))$.

iii.- Por lo dicho en [i], si $|\{a \in L : p(x) = 0\}| > 1$, tenemos que $\sigma : L \to L$ definida por $\sigma(\alpha) = \alpha'$ define un isomorfismo de cuerpos, donde α' otra raiz de $p(x)$ en L. Esto prueba que existe σ no trivial.

4.- **Ejercicio:** Sea $d \in \mathbb{Z}$ elemento libre de cuadrado. Muestre que existen solamente dos automorfismos $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ tales que $\sigma|_{\mathbb{Q}} = id$.

Ayudantía XIX: En esta ayudantía estudiaremos la multiplicitivadad del grado en extensiones de cuerpos y calcularemos inversos multiplicativos en ciertos cuerpos.

1.- **Problema 1:**
Calcule el inverso multiplicativo de $1 + \sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$.

Desarrollo: Recordemos que por lo visto en la ayudantía XVII tenemos que $\phi : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{Q}(\sqrt[3]{2})$, $\phi(x) = \sqrt[3]{2}$ es un isomorfismo. Bajo este mismo tenemos que $\phi^{-1}(1 + \sqrt[3]{2} + \sqrt[3]{4}) = 1 + x + x^2$. Aplicando algoritmo de división obtenemos que $1 = (x - 1)(x^2 + x + 1) - (x^3 - 2)$. Por lo tanto, si aplicamos ϕ, obtenemos $1 = (\sqrt[3]{2} - 1)(\sqrt[3]{4} + \sqrt[3]{2} + 1)$. Luego $(\sqrt[3]{4} + \sqrt[3]{2} + 1)^{-1} = \sqrt[3]{2} - 1$.

i.- **Ejercicio:** Demuestre que el inverso de $a + b\sqrt{D} \in \mathbb{Q}(\sqrt{D})$ es $\frac{a - b\sqrt{D}}{a^2 - b^2 D}$.

2.- **Problema 2:**
Demuestre cada una de las siguientes aseveraciones:
i.- Sea $K = \mathbb{Q}(i, \sqrt{2})$. Pruebe que $[K : \mathbb{Q}] = 4$.
ii.- Sea $L = \mathbb{Q}(\sqrt{3}, \sqrt{2})$. Pruebe que $[L : \mathbb{Q}] = 4$.

Desarrollo:
i.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2$. Por otro lado $K = \mathbb{Q}(\sqrt{2})(i)$, donde $p(x) = x^2 + 1 \in \mathbb{Q}(\sqrt{2})[x]$ es un polinomio que se anula en i. Por lo tanto $[K : \mathbb{Q}(\sqrt{2})] = 1$ o 2. Si $[K : \mathbb{Q}(\sqrt{2})] = 1$ entonces $K = \mathbb{Q}(\sqrt{2})$. Luego $i \in \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$, lo que nos lleva a una constradicción. Por lo tanto $[K : \mathbb{Q}(\sqrt{2})] = 2$. Luego $[K : \mathbb{Q}] = 4$.
ii.- Sabemos que $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2$. Por otro lado $L = \mathbb{Q}(\sqrt{2})(\sqrt{3})$, donde $p(x) = x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ es un polinomio que se anula en i. Por lo tanto $[L : \mathbb{Q}(\sqrt{2})] = 1$ o 2. Si $[L : \mathbb{Q}(\sqrt{2})] = 1$ entonces $L = \mathbb{Q}(\sqrt{2})$. Luego $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Esto en particular nos dice que existe $z \in \mathbb{Q}(\sqrt{2})$ tal que $z^2 = 3$. Pero todo elemento $z \in \mathbb{Q}(\sqrt{2})$ es de la forma $a + b\sqrt{2}$, para $a, b \in \mathbb{Q}$, esto ya que $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2) = \mathbb{Q} \oplus \mathbb{Q}\overline{x}$. Por lo tanto tenemos que $a^2 + 2b^2 + 2ab\sqrt{2} = 3$, es decir $a = 0$ o $b = 0$ y $a^2 + 2b^2 = 3$, para $a, b \in \mathbb{Q}$. Por ello tenemos que $3 \in \mathbb{Q}^2$ o $\frac{3}{2} \in \mathbb{Q}^2$, esto nos lleva a una contradicción. Por lo tanto $[L : \mathbb{Q}(\sqrt{2})] = 2$. Luego $[L : \mathbb{Q}] = 4$.

2.- **Ejercicio:** Calcule el grado sobre $\mathbb{Q}$ de la extensión $L = \mathbb{Q}(w, \sqrt[3]{2})$, donde $w = e^{\frac{2\pi i}{3}}$.

3.- **Problema 3:**
Sea L una extensión de K finitamente generada.
i.- Pruebe que si todo elemento en L satisface un polinomio mónico sobre K, entonces $[L : K] < \infty$.
ii.- Concluya que $L = \mathbb{Q}(\sqrt[n]{2} : n \in \mathbb{N}) \subset \mathbb{C}$ no es una extensión finitamente generada de $\mathbb{Q}$. Puede asumir que en esta extensión todos los elementos satisfacen polinomios sobre $\mathbb{Q}$.

Desarrollo:
i.- Sabemos que $L = K(a_1, \cdots a_t)$, para ciertos $a_t \in L$. Por esto podemos generar la torre de cuerpos definida por $L_0 = K$ y $L_i = L_{i-1}(a_i)$. Entonces

como todo elemento en L satiface un polinomio sobre K tenemos que $[L_i : L_{i-1}] = \deg(irr_{a_i,L_{i-1}}(x)) < \infty$. Por lo multiplicatividad de grado en torres tenemos que $[L : K] = \sqcap \deg(irr_{a_i,L_{i-1}}(x)) < \infty$.

ii.- Observe que $L_n = \mathbb{Q}(\sqrt[n]{2})$ es una subextensión de L sobre $\mathbb{Q}$. Por lo probado en la ayudantía XVIII tenemos que $[L_n : \mathbb{Q}] = n$. Por lo tanto $[L : \mathbb{Q}] < n$, para todo $n \in \mathbb{N}$. Luego $[L : K] = \infty$. Por [i] concluimos que $L = \mathbb{Q}(\sqrt[n]{2} : n \in \mathbb{N})$ no es una extensión finitamente generada de $\mathbb{Q}$.

4.- **Problema 4:**
Considere $\eta = e^{\frac{2\pi i}{5}} \in \mathbb{C}$. Asumiendo que $\phi_5(x) = x^4 + x^3 + x^2 + x + 1$ es un polinomio irreducible sobre $\mathbb{Q}$, demuestre lo siguiente:

i.- Pruebe que $\mathbb{Q}(\eta)$ es una extensión de grado 4 de $\mathbb{Q}$.

ii.- Pruebe que $\mathbb{Q}(\eta + \eta^{-1})$ es una extensión de grado 2 de $\mathbb{Q}$

iii.- Escriba $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\sqrt{d})$, para cierto $d \in \mathbb{Z}$.

Desarrollo:

i.- Observe que η satisface la ecuación $x^5 - 1 = 0$. Pero como $\eta \neq 1$ tenemos que η satisface $\phi_5(x) = \frac{x^5-1}{x-1}$. Como este polinomio es irreducible, tenemos que $\phi_5(x) = irr_{\eta,\mathbb{Q}}(x)$. Luego $[\mathbb{Q}(\eta) : \mathbb{Q}] = deg(\phi_5(x)) = 4$.

ii.- Observe que $\mathbb{Q}(\eta) = \mathbb{Q}(\eta + \eta^{-1})(\eta)$, donde η satisface el polinomio $p(x) = x^2 - x(\eta+\eta^{-1}) + 1 \in \mathbb{Q}(\eta+\eta^{-1})[x]$. Por lo tanto $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta+\eta^{-1})] = 1$ o 2. Si $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta+\eta^{-1})] = 1$ entonces $\eta \in \mathbb{Q}(\eta+\eta^{-1})$, donde $\mathbb{Q}(\eta+\eta^{-1}) \subset \mathbb{R}$, puesto que $\eta + \eta^{-1} = \eta + \overline{\eta} \in \mathbb{R}$. Esto nos lleva a una contradicción. Por lo tanto $[\mathbb{Q}(\eta) : \mathbb{Q}(\eta + \eta^{-1})] = 2$. Luego $[\mathbb{Q}(\eta + \eta^{-1}) : \mathbb{Q}] = 2$.

iii.- Tenemos que $(\eta+\eta)^2 = \eta^2+2+\eta^3 = 1-\eta-\eta^{-1}$. Por lo tanto $\eta+\eta^{-1}$ satisface el polinomio $x^2 + x - 1$. Luego $\eta + \eta^{-1} = \frac{-1+\sqrt{5}}{2}$ o bien $\eta + \eta^{-1} = \frac{-1-\sqrt{5}}{2}$. En cualquier caso $\mathbb{Q}(\eta + \eta^{-1}) = \mathbb{Q}(\sqrt{5})$. Por ello $d = 5$.

4.- **Ejercicio:** Sea $\eta = e^{\frac{2\pi i}{5}}$. Encuentre el inverso de $1 + \eta$ en $\mathbb{Q}(\eta)$.

Ayudantía XX: En esta ayudantía estudiaremos algunos criterios de irreducibilidad de polinomios y trabajaremos con el lema de Gauss.

1.- **Problema 1:**
Sea $p(x) = a_0 + \cdots + a_{t-1}x^{t-1} + x^t \in \mathbb{Z}[x]$ un polinomio mónico. Pruebe que si $\overline{p(x)} = \overline{a_0} + \cdots + \overline{a_{t-1}}x^{t-1} + x^t \in \mathbb{Z}/p\mathbb{Z}[x]$ es irreducible para algún $p \in \mathbb{Z}$ primo, entonces $p(x)$ es irreducible.

Demostración: Supongamos que $p(x)$ se reduce en $\mathbb{Z}[x]$. Entonces $p(x) = s(x)t(x)$ donde $deg(s(x)), deg(t(x)) > 0$. Luego $\overline{p(x)} = \overline{s(x)t(x)} \in \mathbb{Z}/p\mathbb{Z}[x]$. Observe que los coeficientes a, b de mayor grado de $s(x)$ y $t(x)$ respectivamente, satisfacen que $ab = 1$. Luego $\overline{ab} = 1$. Por lo tanto $\overline{a}, \overline{b} \neq 0$. Esto implica que $deg(s(x)) = deg(\overline{s(x)}), deg(t(x)) = deg(\overline{t(x)})$. Es decir, probamos que $\overline{p(x)}$ se reduce en $\mathbb{Z}/p\mathbb{Z}[x]$, lo que nos lleva a una contradicción. Por lo tanto $p(x) \in \mathbb{Z}[x]$ es irreducible.

i.- **Ejercicio:** Muestre que $p(x) = x^3 + x + 1$ es irredcible sobre $\mathbb{Z}[x]$.

2.- **Problema 2:**
Sea $p(x) = x^4 + x + 1 \in \mathbb{Q}[x]$.
i.- Pruebe que $p(x)$ es irredicible sobre $\mathbb{Q}[x]$.
ii.- Sea η un raiz de $p(x)$. Calcule $[\mathbb{Q}(\eta) : \mathbb{Q}]$.

Desarrollo:
i.- Observe que por criterio de Gauss $p(x) \in \mathbb{Z}[x]$ irreducible sobre $\mathbb{Q}[x]$ si y solamnete si $p(x)$ es irreducible sobre $\mathbb{Z}[x]$. Esto último se debe a que $p(x)$ es un polinomio primitivo. Ahora bien, la reducción de $p(x)$ es $\mathbb{F}_2[x]$ cumple con que $\overline{p(1)} = 1$, $\overline{p(0)} = 1$. Por lo tanto $\overline{p(x)}$ no tiene factores lineales. Puesto que $deg(\overline{p(x)}) = 4$ tenemos que o bien $\overline{p(x)}$ es irreducible o bien $\overline{p}(x)$ es producto de polinomios irreducibles de grado 2. Observe que el único polinomio irreducible de grado 2 sobre $\mathbb{F}_2[x]$ es $x^2 + x + 1$. Luego si $\overline{p(x)}$ es reducible entonces $\overline{p(x)} = (x^2 + x + 1)^2 = x^4 + x^2 + 1$, lo que nos lleva a una contradicción. Luego $\overline{p}(x)$ es irreducible sobre $\mathbb{F}_2[x]$. Por el problema 1, tenemos que $p(x)$ es irreducible sobre $\mathbb{Z}[x]$ y esto último implica, por lema de Gauss, que $p(x)$ es irreducible sobre $\mathbb{Q}[x]$.
ii.- Observe que $irr_{\eta,\mathbb{Q}}(x) = p(x)$. Luego $[\mathbb{Q}(\eta) : \mathbb{Q}] = \deg(p(x)) = 4$.

2.- **Ejercicio:** Calcule $\frac{1}{1+\eta} \in \mathbb{Q}(\eta)$ en término de potencias de η y números racionales.

3.- **Problema 3:**
Sea $a = \sqrt{\frac{-4+\sqrt{8}}{2}} \in \mathbb{C}$.
i.- Encuentre el polonomio irreducible de a sobre $\mathbb{Q}[x]$.
ii.- Calcule $[\mathbb{Q}(a) : \mathbb{Q}]$.

Desarrollo:
i.- Observe que $q(x) = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$ se anula en $x = a$. Además $q(x)$ es irreducible sobre $\mathbb{Z}[x]$ por criterio de Einsenstein. Luego por lema de Gauss, como $q(x)$ es primitivo, tenemos que $q(x)$ es irreducible sobre $\mathbb{Q}[x]$. Por ello, podemos concluir que $q(x) = irr_{a,\mathbb{Q}}(x)$.
ii.- Observe que $[\mathbb{Q}(a) : \mathbb{Q}] = deg(irr_{a,\mathbb{Q}}(x)) = deg(q(x)) = 4$.

4.- **Problema 4:**
Sea $f : K[x] \to K[x]$ un automorfismo tal que $f|_K = id$.

i.- Pruebe que $p(x)$ es irreducible sobre $K[x]$ si y solamente si $f(p(x))$ irreducible.

ii.- Concluya que $p(x)$ es irreducible si y solamente si $p(x + a)$ es irreducible para algún $a \in K$.

Desarrollo:

i.- Supongamos que $f(p(x)) = s(x)t(x)$, donde $s(x), t(x)$ son polinomios no constantes. Entonces aplicando f^{-1} obtenemos que $p(x) = f^{-1}(s(x))f^{-1}(t(x))$. Observe que si $f^{-1}(s(x)) = c \in K$ entonces $s(x) = c \in K$. Por lo tanto $deg(f^{-1}(s(x))), deg(f^{-1}(t(x))) > 0$. Luego $f(p(x))$ reducible implica que $p(x)$ es reducible. Aplicando f^{-1} al polinomio $f(p(x))$ obtenemos la implicancia contraria. Por lo tanto $p(x)$ es irreducible sobre $K[x]$ si y solamente si $f(p(x))$ irreducible.

ii.- Observe que la función $f : K[x] \to K[x]$ definida por $f(p(x)) = p(x + a)$ es un homomorfismo cuya inversa es $g(p(x)) = p(x - a)$. Luego por [i] obtenemos que $p(x)$ es irreducible si y solamente si $p(x + a)$ es irreducible para algún $a \in K$.

4.- **Ejercicio:** Demuestre que todo automorfismo de $K[x]$ es dela forma $f(x) = x + a$, para cierto $a \in K$.

Ayudantía XXI: En esta ayudantía estudiaremos construcciones con regla y compás. Solo trabajaremos con números reales construictibles, pues para sus anaĺogos complejos basta tomar la proyección en cada coordenada para analizarlos.

1.- **Problema 1:**
Sea $D \in \mathbb{N}$. Muestre geometrica y algebraicamente que $\sqrt{D} \in \mathbb{R}$ es constructible con regla y compás.

Demostración: Primero demostremos esto geometricamente. En efecto lo probaremos por inducción sobre $D \in \mathbb{N}$. Observe que $\sqrt{2}$ es constructible ya que es la diagonal de un cuadrado cuyos lados tienen lago 1. Supongamos que construimos $\sqrt{D}$. Entonces trazando un segmento de largo 1, perpendicular al segmento de largo $\sqrt{D}$, obtenemos al trazar la diagonal un segmento de largo $\sqrt{D+1}$. Esto prueba que $\sqrt{D+1}$ es constructible con regla y compás.

Ahora probemos este hecho algebraicamente. Observe que $L = \mathbb{Q}(\sqrt{D})$ es una extensión de grado 1 o 2 de $\mathbb{Q}$, que se obtiene adjuntando una raiz cuadrática. Luego tenemos una torre de cuerpos de la forma:

$$\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = L\,,$$

donde $L_i = L_{i-1}(\sqrt{b_i})$, para cierto $b_i \in L_{i-1}$. Esto por lo visto en clase, implica que $\sqrt{D}$ es constructible con regla y compás. De hecho en nuestro caso $t = 0$ o $t = 1$.

2.- **Problema 2:**
Muestre que el cuerpo L de los números constructibles está estrictamente contenido en $\mathbb{R} \cap \overline{\mathbb{Q}}$.

Demostración: Primero observe que lo números constructibles son reales por definición. Supongamos que $\alpha \in \mathbb{R}$ es constructible. Entonces existe una torre de cuerpos: $\mathbb{Q} = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = K$, donde $L_i = L_{i-1}(\sqrt{b_i})$, para cierto $b_i \in L_{i-1}$ y $\alpha \in K$. Luego $[K : \mathbb{Q}] \leq 2^t < \infty$. Por ello α es algebraico sobre $\mathbb{Q}$. Luego $L \subset \mathbb{R} \cap \overline{\mathbb{Q}}$. Ahora bien, el número $\sqrt[3]{2} \in \mathbb{R} \cap \overline{\mathbb{Q}}$, pero no es constructible con regla y compás. Esto se debe a que si lo fuera entonces $3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2^s$, lo que nos lleva a una contradicción.

2.- **Ejercicio:** Muestre que el cuerpo de los números constructibles es numerable.

3.- **Problema 3:**
Demuestre que no es posible construir un cubo cuyo volumen sea el de la esfera unitaria.

Demostración: Supongamos que podemos construir dicho cubo. Entonces tenemos que existe un número constructible $r \in \mathbb{R}$ tal que $r^3 = \frac{4}{3}\pi$. Luego $r = \sqrt[3]{\frac{4}{3}\pi}$. Pero como todo número construictible es algebraico sobre $\mathbb{Q}$, esto implica que $\sqrt[3]{\frac{4}{3}\pi}$ es algebraico sobre $\mathbb{Q}$. Esto implica que $\frac{4}{3}\pi$ es algebraico sobre $\mathbb{Q}$, lo cual nos lleva a que π es algebraico sobre $\mathbb{Q}$. Esto nos da una contradicción.

4.- **Problema 4:**
Pruebe que $\cos\left(\frac{2\pi}{5}\right)$ es constructible con regla y compás. Concluya que el pentagono es construtible con regla y compás.

Demostración: Observe que $a = \cos\left(\frac{2\pi}{5}\right) \in \mathbb{Q}(b)$, donde $b = e^{\frac{2\pi i}{5}}$. De hecho $\mathbb{Q}(a) = \mathbb{Q}(b+b^{-1})$. Por otro lado $(b+b^{-1})^2 = 2+b^2+b^3 = 1-b-b^{-1}$, puesto que $b^4+b^3+b^2+b+1 = 0$. Luego tenemos que $b+b^{-1} = \frac{-1+\sqrt{5}}{2}$ o $b+b^{-1} = \frac{-1-\sqrt{5}}{2}$. En cualquier caso $\mathbb{Q}\left(\cos\left(\frac{2\pi}{5}\right)\right) = \mathbb{Q}(\sqrt{5})$. Dado que $\mathbb{Q}(\sqrt{5})$ es una extensión cuadrática de $\mathbb{Q}$ tenemos que $\cos\left(\frac{2\pi}{5}\right)$ es constructible con regla y compás. Ahora bien como podemos construir $\cos\left(\frac{2\pi}{5}\right)$ con regla y compás y $\sin\left(\frac{2\pi}{5}\right) = \sqrt{1-\cos\left(\frac{2\pi}{5}\right)^2}$ tenemos que $\sin\left(\frac{2\pi}{5}\right)$ es constructible. Luego podemos contruir uno de los lados del pentagono. Iterativamente construimos cada lado y de esta forma el pentagono.

4.- **Ejercicio:** Pruebe que $\cos\left(\frac{2\pi}{7}\right)$ no es constructible con regla y compás.

Ayudantía XXII: En esta ayudantía estudiaremos cuerpos finitos.

1.- **Problema 1:**
Sea $\mathbb{F}_p$ el cuerpo finito de p elementos.

i.- Pruebe que $\alpha^p = \alpha$, para todo $\alpha \in \mathbb{F}_p$.

ii.- Demuestre que no existen extensiones de grado p de $\mathbb{F}_p$ que se obtengan adjuntando raices p-ésimas.

iii.- Muestre que $p(x) = x^3 - x + 1$ es irreducible sobre $\mathbb{F}_3$.

iv.- Sea b una raiz de $p(x)$. Concluya que $L = \mathbb{F}_3(b)$ es una extensión de grado 3 de $\mathbb{F}_3$.

Desarrollo:

i.- Observe que para todo $\alpha \in \mathbb{F}_p^*$ se cumple, por teorema de lagrange, que $\alpha^{p-1} \equiv 1$. En particular tenemos que $\alpha^p \equiv \alpha$, para todo $\alpha \in \mathbb{F}_p^*$. Observe que esta última relación se cumple también para $\alpha = 0$. Esto prueba lo pedido.

ii.- Sea $L = \mathbb{F}_p(\theta)$ una extensión de grado p de $\mathbb{F}_p$, tal que $\theta^p = a \in \mathbb{F}_p$. Entonces $(\theta - a)^p = \theta^p - a^p = \theta^p - a = 0$. Luego como L es un dominio de integridad tenemos que $\theta = a \in \mathbb{F}_p$. Esto en particular implica que $L = \mathbb{F}_p$, lo cual nos lleva a una contradicción.

iii.- Para probar que $p(x)$ no tiene raices en $\mathbb{F}_3$ observe que $a^3 = a$, para todo $a \in \mathbb{F}_3$. Luego si $a \in \mathbb{F}_3$ es raiz de $p(x)$, tenemos que $0 = a^3 - a + 1 = 1$. Esto no lleva a una contradicción.

iv.- Tenemos que $p(x)$ es un polinomio de grado 3 sin raices en el cuerpo sobre el cual se define. Por lo tanto $p(x)$ es irreducible. Luego si b es un raiz de $p(x)$ tenemos que $L = \mathbb{F}_3(b) \cong \mathbb{F}_3[x]/(p(x))$ es una extensión de grado 3 de $\mathbb{F}_3$.

1.- **Ejercicio:** Muestre que $(p-1)! \equiv -1(p)$, para todo $p \in \mathbb{N}$ primo.

2.- **Problema 2:**
Sean L_1, L_2 extensiones finitas de $\mathbb{F}_p$ de igual grado.

i.- Pruebe que $L_1 = L_2$.

ii.- Concluya que para $\alpha \in \overline{\mathbb{F}_p}$ se tiene que $\{s \in \overline{\mathbb{F}_p} : irr_{\alpha,\mathbb{F}_p}(s) = 0\} \subset \mathbb{F}_p(\alpha)$.

Desarrollo:

i.- Sabemos que fijando una clausura algebraica de $\mathbb{F}_p$, tenemos que $L_1, L_2 \subset \overline{\mathbb{F}_p}$. Ahora bien para una extensión de grado n de $\mathbb{F}_p$, tenemos que L^* es un grupo de $p^n - 1$ elementos. Luego para todo $a \in L$ tenemos que $a^{p-1} = 1$. Luego $a^{p^n} = a$, para todo $a \in L$. Por otro lado las soluciones de la ecuación $x^{p^n} - x$ sobre $\overline{\mathbb{F}_p}$ son todas distintas. Esto se debe a que si $(x-z)^2$ divide a $x^{p^n} - x$ entonces $(x - z)$ divide a $x^{p^n} - x$ y a $(x^{p^n} - x)' = -1$. Esto nos da una contradicción. Luego por simple conteo, tenemos que $\{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\} = L$. En particular si tomamos de extensiones del mismo grado, obtenemos que son iguales.

ii.- Sea $\alpha \in \overline{\mathbb{F}_p}$ y sea $p(x) = irr_{\alpha,\mathbb{F}_p}(x)$. Digamos que el grado de $p(x)$ es n. Entonces $L = \mathbb{F}_p(\alpha)$ es una extensión de grado n de $\mathbb{F}_p$. Por otro lado, para cualquier otra raiz de $p(x)$, digamos b, tenemos que $\mathbb{F}_p(b)$ es también una extensión de $\mathbb{F}_p$ de grado n. Por lo mostrado en [i] tenemos que $\mathbb{F}_p(\alpha) = \mathbb{F}_p(b)$. Por lo tanto $b \in \mathbb{F}_p(\alpha)$. Esto prueba que $\{s \in \overline{\mathbb{F}_p} : irr_{\alpha,\mathbb{F}_p}(s) = 0\} \subset \mathbb{F}_p(\alpha)$.

3.- **Problema 3:**
Sea $\mathbb{F}_2[x]$ el anillo de polinomio sobre el cuerpo de dos elementos.

i.- Calcule el número de polinomios irreducibles de grado 4 que hay en $\mathbb{F}_2[x]$.

ii.- Determine dichos polinomios.

Desarrollo:

i.- Sea $p(x) \in \mathbb{F}_2[x]$ un polinomio irreducible cualquiera de grado 4. Entonces si b es raiz de $p(x)$ tenemos que $\mathbb{F}_2(b) = \{a \in \overline{\mathbb{F}_2} : a^{16} = a\}$. Por lo tanto b se anula en $p(x)$ y $x^{16} - x$. Luego, como $p(x) = irr_{b,\mathbb{F}_2}(x)$, tenemos que $p(x)|x^{16}-x$. Por lo tanto debemos buscar los factores de grado 4 de $x^{16}-x$. Observe que este polinomio tiene todas sus raices distintas, por lo mostrado en el problema 2, parte [i]. Luego tenemos que $x^{16} - x$ tiene dos factores de grado 1. Esto pues $1^{16} = 1$ y $0^{16} = 0$. Por otro lado, si tomamos un polinomio irreducible$q(x)$ que divide a $x^{16} - x$ entonces si c es raiz de $q(x)$, tenemos que $\mathbb{F}_2(c) \subset \mathbb{F}_2(b)$. Luego $deg(q(x)) = [\mathbb{F}_2(c) : \mathbb{F}_2]|[\mathbb{F}_2(b) : \mathbb{F}_2] = 4$. Por lo tanto $deg(q(x)) \in \{1, 2, 4\}$. Por lo tanto solo nos queda determinar lo polinomios de grado 2 que dividen a $x^{16} - x$. En efecto, el único polinomio de grado 2 irreducible sobre $\mathbb{F}_2$ es x^2+x+1. De hecho $\mathbb{F}_2[x]/(x^2+x+1) = \{a \in \overline{\mathbb{F}_2} : a^4 = a\} \subset \mathbb{F}_2(b)$, por ello x^2+x+1 divide a $x^{16}-x$. Por lo tanto el número de factores irreducibles de grado 4 de $x^{16} - x$ es $\frac{16-2-2}{4} = 3$. Luego en $\mathbb{F}_2[x]$ hay 3 polinomios irreducibles de grado 4.

ii.- Observe que, por lo dicho en [i], para encontrar dichos polinomios basta encontrar polinomio de grado 4 que no tengan raices en $\mathbb{F}_2$ y tales que sean distintos a $(x^2+x+1)^2 = x^4+x^2+1$. Así tenemos que x^4+x+1, x^4+x^3+1 y $x^4 + x^3 + x^2 + x + 1$ son los únicos polinomios irreducibles de grado 4 en $\mathbb{F}_2[x]$.

3.- **Ejericicio:** Calcule el grado y el número de polinomios irreducibles en $\mathbb{F}_3[x]$ que dividen a $q(x) = x^{27} - x$.

4.- **Problema 4:**
Pruebe que ningún cuerpo finito es algebraicamente cerrado.

Demostración: Sea L un cuerpo finito. Entonces existe p primo y $n \in \mathbb{N}$ tal que $L = \mathbb{F}_{p^n} = \{a \in \overline{\mathbb{F}_p} : a^{p^n} = a\}$. Luego tenemos que en polinomio $p(x) = x^{p^n} - x + 1 \in L[x]$ no tiene solucion en L. Por ello L no es algebraicamente cerrado.

4.- **Ejercicio:** Muestre que si $\phi : \mathbb{F} \to \mathbb{F}$ es un homomorfismo entre cuerpos finitos, entonces ϕ es un isomorfismo.

Ayudantía XXIII: En esta ayudantía seguiremos estudiando cuerpos finitos.

1.- **Problema 1:**
Sean $\mathbb{F}_{p^n}$ y $\mathbb{F}_{p^m}$ cuerpos finitos.

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

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

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

Desarrollo:

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

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

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

1.- **Ejercicio:** Muestre que $\mathbb{F}_8 \subseteq \mathbb{F}_{2^{3t}}$, para todo $t \in \mathbb{N}$.

2.- **Problema 2:**
Sea $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ a función definida por $\phi(\alpha) = \alpha^p$.

i.- Muestre que ϕ es un isomorfismo tal que $\phi|_{\mathbb{F}_p} = id$.

ii.- Calcule $|\phi|$.

Desarrollo:

i.- Primero mostremos que ϕ es un homomorfismo de anillos. Claramente se tiene que $\phi(ab) = (ab)^p = a^p b^p = \phi(a)\phi(b)$. Por otro lado tenemos que $\phi(a+b) = (a+b)^p = a^p + b^p = \phi(a) + \phi(b)$. Luego ϕ es un homomorfismo de grupos. Observe que $\phi(1) = 1$, por lo tanto $\phi \neq 0$. Luego $\ker(\phi)$ es un ideal estricto del cuerpo $\mathbb{F}_{p^n}$. Por lo tanto $\ker(\phi) = \{0\}$. Luego ϕ es inyectiva. Como $\phi : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ es una función inyectiva entre conjuntos finitos de igual cardianlidad, concluimos que ϕ es isomorfismo. Además para $a \in \mathbb{F}_p$ tenemos que $\phi(a) = a^p = a$.

ii.- Para calcular el orden del isomorfismo ϕ, basta encontrar el mínimo natural $m \in \mathbb{N}$ tal que $\phi^m = id$. Es decir, basta determinar $m \in \mathbb{N}$ tal que $a^{p^m} = a$, para todo $a \in \mathbb{F}_{p^n}$. Como la condición anterior de cumple para el natural n tenemos que $m \leq n$. Observe que si $m < n$, entonces $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$. Pero $|\mathbb{F}_{p^n}| = p^n > p^m = |\mathbb{F}_{p^m}|$, esto nos lleva a una contradicción. Por lo tanto $m = |\phi| = n$.

3.- **Problema 3:**
Sea $p(x) \in \mathbb{F}_p[x]$.

i.- Pruebe que $p(x^p) = p(x)^p$.

ii.- Concluya que $p(x) = x^{2p} + x^p + 1$ no es irreducible sobre $\mathbb{F}_p[x]$.

Desarrollo:

i.- Sea $p(x) = a_0 + a_1x + \cdots + a_nx^n$ entonces como $car(\mathbb{F}_p) = p$ se tiene que $p(x)^p = a_0^p + a_1^px^p + \cdots + a_n^px^{np}$. Pero, para $a \in \mathbb{F}_p$ sabemos que $a^p = a$. Luego tenemos que $p(x)^p = a_0 + a_1x^p + \cdots + a_nx^{np} = p(x^p)$.

ii.- Observe que $p(x) = x^{2p} + x^p + 1 = (x^2 + x + 1)^p$. Por lo tanto $p(x)$ no es irreducible sobre $\mathbb{F}_p[x]$.

4.- **Problema 4:**
Pruebe que $\mathbb{F}_9 = \mathbb{F}_3[x]/(x^2 + 1)$.

Demostración: Observe que $x^2 + 1$ es un polinomio irreducible sobre $\mathbb{F}_3$. Esto de debe a que no tiene raices en $\mathbb{F}_3$, puesto que $\mathbb{F}_3^2 = \{0, 1\}$. Por lo tanto $\mathbb{F}_3[x]/(x^2 + 1)$ es una extensión del cuerpo $\mathbb{F}_3$ de grado 2. Luego $\mathbb{F}_3[x]/(x^2 + 1)$ debe ser la única extensión de grado 2 de $\mathbb{F}_3$, es decir $\mathbb{F}_3[x]/(x^2 + 1) = \mathbb{F}_9$.

4.- **Ejercicio:** Sea $i \in \mathbb{F}_5$ un elemento tal que $i^2 = -1$. Pruebe que $\mathbb{F}_5(i) = \mathbb{F}_5$.

Ayudantía XXIV: En esta ayudantía haremos un repaso por lo ya estudiado en teoría de cuerpos.

1.- **Problema 1:**
Sea β una raiz de $x^3 - x + 1 \in \mathbb{F}_3[x]$.

i.- Encuentre $a, b, c \in \mathbb{F}_3$ tales que $a + b\beta + c\beta^2 = \frac{1}{2\beta+1}$.

ii.- Encuentre el polinomio minimal de $\beta + 1$.

Desarrollo:

i.- Sabemos que debemos aplicar el algoritmo de división sobre los polinomios $x^3 - x + 1$ y $2x + 1 = -x + 1$. En efecto, tenemos que $(x^3 - x + 1) - (-x + 1)(-x^2 - x) = 1$. Por lo tanto, al tomar el homomorfismo evaluación en β resulta $1 = (2\beta + 1)(\beta^2 + \beta)$. Por lo tanto, para obtener lo pedido, basta tomar $a = 0, b = c = 1$.

ii.- Observe que $\mathbb{F}_3(\beta) = \mathbb{F}_3(\beta + 1)$. Luego tenemos que $deg(irr_{\mathbb{F}_3,\beta+1}(x)) = [\mathbb{F}_3(\beta + 1) : \mathbb{F}_3] = [\mathbb{F}_3(\beta) : \mathbb{F}_3] = 3$. Esto último pues en la ayudantía 22 vimos que $[\mathbb{F}_3(\beta) : \mathbb{F}_3] = 3$. Además tenemos que $q(x) = (x-1)^3-(x-1)+1$ anula a $\beta + 1$. Como $q(x)$ tiene el grado correcto, dicho polinomio es el minimal de $\beta + 1$. Luego $irr_{\mathbb{F}_3,\beta+1}(x) = q(x) = x^3 - x + 1$. Observe que este polinomio es el mismo que el irreducible de β.

1.- **Ejercicio:** Bajo la misma hipótesis del problema anterior, encuentre el polinomio minimal de $\beta + 2$.

2.- **Problema 2:**
Sea $a = \sqrt{1 + \sqrt{2}} \in \mathbb{C}$.

i.- Calcule $[\mathbb{Q}(a) : \mathbb{Q}]$.

ii.- Determine el polinomio mónico irreducible de a sobre $\mathbb{Q}$.

Desarrollo:

i.- Observe que $a^2 - 1 = \sqrt{2}$. Por lo tanto $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(a)$. Además $x^2 - 1 - \sqrt{2}$ es un polinomio en $\mathbb{Q}(\sqrt{2})[x]$ que anula a $\sqrt{1 + \sqrt{2}}$. Por lo tanto $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})] = 1$ o 2. Si sucede lo primero, es decir si $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})] = 1$ entonces $1 + \sqrt{2}$ es un cuadrado en $\mathbb{Q}(\sqrt{2})$. Entonces existen $a, b \in \mathbb{Q}$ tales que $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2} = 1 + \sqrt{2}$. Por o tanto $1 = a^2 + 2b^2$ y $1 = 2ab$. Luego, despejando b de la segunda ecuación y sustituyendo esto en la primera, llegamos a que $2a^4 - 2a^2 + 1 = 0$. Pero $2x^4 - 2x^2 + 1$ no tiene soluciones en $\mathbb{Q}$. Por lo tanto $1 + \sqrt{2}$ no es un cuadrado en $\mathbb{Q}(\sqrt{2})$. Luego $[\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})] = 2$. Por lo tanto, se tiene que el grado de la extensión es $[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$.

ii.- Observe que si $x = \sqrt{1 + \sqrt{2}}$ entonces $x^2 - 1 = \sqrt{2}$. Luego tenemos que $(x^2 - 1)^2 - 2$ es un polinomio que se anula en a. Como el grado del polinomio irrecucible de a debe conincidir con $[\mathbb{Q}(a) : \mathbb{Q}] = 4$, tenemos que $irr_{\mathbb{Q},a}(x) = x^4 - 2x^2 - 1$.

3.- **Problema 3:**
Sea $p \in \mathbb{N}$ un número primo.

i.- Demuestre que si e polinomio de p lados es constructible entonces existe $n \in \mathbb{N}$ tal que $p = 1 + 2^n$.

ii.- Demuestre que el polinomio de 7 lados no es constructible con regla y compás.

Desarrollo:

i.- Sabemos que el polinomio de p lados es constructible con regla y comás si y solamente si $\eta = e^{\frac{2\pi i}{p}}$ es construtible como número complejo. Recordemos que $\mathbb{Q}(\eta)$ es una extensión de grado $p-1$ de $\mathbb{Q}$. Por lotro lado, si η es constructible con regla y compás, entonces existe un torre de cuerpos $\{L_i\}_{i=0}^{n}$ de indice dos tal que $\mathbb{Q} = L_0 \subset L_1 \subset \cdots L_n = \mathbb{Q}(\eta)$. Luego $[\mathbb{Q}(\eta) : \mathbb{Q}] = 2^n$, de lo que se sigue que $p = 1 + 2^n$, para cierto $n \in \mathbb{N}$.

ii.- Aplicaremos lo mostrado en [i]. En efecto, observe que $7 = 1 + 6$, donde 6 no es potencia de 2. Por lo tanto el poligono de 7 lados no es constructible.

4.- **Problema 4:**
En lo que sigue $\mathbb{F}_p$ es el cuerpo de p elementos.

i.- Sea $K = \mathbb{F}_5(a)$, donde $a^2 = 2$. Muestre que $[K : \mathbb{F}_5] = 2$.

ii.- Muestre que si α es raiz del polinomio irreducible $p(x) \in \mathbb{F}_p[x]$ de grado n entonces $T = \{\alpha, \alpha^p, \cdots, \alpha^{p^{m-1}}\}$ es un subconjunto del conjunto de raices de $p(x)$.

iii.- Pruebe que $|T| = n$. Concluya que $p(x)$ no tiene raices repetidas.

Desarrollo:

i.- Observe que $x^2 - 2$ es un polinomio irreducible en $\mathbb{F}_5[x]$ dado que no tiene raices en $\mathbb{F}_5$. Esto último ya que $\mathbb{F}_5^2 = \{0, 1, 4\}$. Por lo tanto $irr_{\mathbb{F}_5,a}(x) = x^2 - 2$. Luego $[K : \mathbb{F}_5] = deg(irr_{\mathbb{F}_5,a}(x)) = 2$.

ii.- Sea $p(x) = a_0 + a_1x + \cdots + a_nx^n$. Entonces tenemos que $p(x)^p = (a_0 + a_1x + \cdots + a_nx^n)^p = a_0^p x^p + \cdots + a_n^p x^{pn}$. Pero para todo $a_i \in \mathbb{F}_p$ se cumple que $a_i^p = a_i$. Por lo tanto $p(x)^p = p(x^p)$. Inductivamente se demuestra que $p(x)^{p^i} = p(x^{p^i})$. Luego si $p(\alpha) = 0$, tenemos que $p(\alpha^{p^i}) = p(\alpha)^{p^i} = 0$. Por ello T es un subconjunto del conjunto de ceros de $p(x)$.

iii.- Supongamos que $\alpha^{p^i} = \alpha^{p^j}$, con $i > j$. Entonces $\beta = \alpha^{p^j}$ cumple con $\beta^{p^{i-j}} = \beta$. Por lo tanto $\beta \in \mathbb{F}_{p^{i-j}}$, donde $i - j < n$. Pero, por lo visto en la ayudantía 22 en el problema 2, como $p(x)$ es un polinomio irreducible, se tiene que $\mathbb{F}_p(\alpha^{p^j}) = \mathbb{F}_p(\alpha) = \mathbb{F}_{p^n}$. Luego tenemos que $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^{i-j}}$. Lo cual nos lleva a una contradicción, pues $|\mathbb{F}_{p^{i-j}}| = p^{i-j} < p^n = |\mathbb{F}_{p^n}|$. Por lo tanto $|T| = n$. Luego como $p(x)$ tiene a lo más n raices distintas, tenemos que T es el conjunto de raices de $p(x)$ y por lo tanto $p(x)$ tiene todas sus raices distintas.

4.- **Ejercicio:** Estudie la noción de cuerpo perfecto. Pruebe que todo cuerpo finito es perfecto.