Grupos y Anillos. Examen Final. 28 de mayo de 2020. Soluciones

Problemas de Grupos comunes
Problema 1

(1) **Calcular las clases de conjugación y el centro de D_{12}.**

(2) **Calcular las clases de conjugación y el centro de D_5.**

(3) **Calcular las clases de conjugación y el centro de D_{16}.**

(4) **Calcular las clases de conjugación y el centro de A_4.**

Voy a poner en general cómo calcular el centro y las clases de conjugación del grupo diédrico $D_n = \langle a, b | a^n = b^2 = 1, ba = a^{-1}b\rangle$. En primer lugar si $g \in \langle a\rangle$ entonces $\langle a\rangle \subseteq C_G(g)$ lo que implica que $|g^G| = [D_n : C_{D_n}(g)] \in \{1, 2\}$. Además $|g^{D_n}| = 1$ si y solo si $g^{D_n} = \{g\}$ si y solo si $g \in Z(D_n)$. Como además $g^b = g^{-1}$ y $g = g^{-1}$ si y solo si $|g| \in \{1, 2\}$ y $|a^i| = \frac{n}{\gcd(i,n)}$, deducimos que si $0 \leq i < n$ entonces $a^i \in Z(D_n)$ si y solo si $|a^{iD_n}| = 1$ si y solo si $\gcd i, n \in \{n, \frac{n}{2}$ si y solo si $i \in \{0, \frac{n}{2}\}$. Por otro a^ib no conmuta nunca con a (salvo que $n = 1, 2$). Por tanto si n es impar entonces $Z(D_n) = \{1\}$ y si n es par entonces $Z(D_n) = \{1, a^{\frac{n}{2}}\}$.

Además, si n es impar, los elementos de la forma a^i se dividen en $1 + \frac{n-1}{2} = \frac{n+1}{2}$ clase de conjugación formadas por $1^{D_n} = \{1\}$ y $a^{iD_n} = \{a^i, a^{-i} = a^{n-i}\}$ con $1 \leq i \leq \frac{n-1}{2}$. Sin embargo si n es par estos elementos se dividen en $2 + \frac{n-2}{2} = \frac{n+2}{2}$ clases de conjugación formadas por $1^{D_n} = \{1\}$, $a^{\frac{n}{2}D_n} = \{a^{\frac{n}{2}}\}$ y $a^{iD_n} = \{a^i, a^{-i} = a^{n-i}\}$ con $1 \leq i \leq \frac{n}{2} - 1$.

Falta clasificar los elementos de la forma $g = a^ib$ en clases de conjugación. Para ello observamos que todo elemento de la forma a^i está en $C_G(g)$ si y solo si está en el centro y si y solo si conmuta con a^ig. Por tanto $C_G(g) = Z(G) \cup Z(G)g$ con lo que $|C_{D_n}(g)| = 2|Z(G)|$ y por tanto $|g^{D_n}| = [D_n : C_G(g)] = \frac{n}{|Z(G)|}$. Luego si n es impar g^G contiene n elementos, con lo que contiene todos los elementos de la forma a^ig y si n es par dichos elementos se dividen en dos clases con $\frac{n}{2}$ elementos cada una. Para ver exactamente cuales son esos elementos observamos que

$$a^iba^{-i} = a^{2i}b \quad \text{y} \quad a^i(ab)a^{-i} = a^{1+2i}b.$$

Por tanto, las dos clases de conjugación con elementos de la forma a^ib son $b^{D_n} = \{a^{2i}b : i = 0, 1 \ldots, \frac{n}{2} - 1\}$ y $(ab)^{D_n} = \{a^{1+2i}b : i = 0, 1 \ldots, \frac{n}{2} - 1\}$.

Para calcular el centro y las clases de conjugación de los elementos de A_4 observamos que dos elementos de A_4 que sean conjugados en A_4 también serán conjugados en S_4 y por tanto tienen el mismo tipo, pero el recíproco no tiene por qué verificarse. Como A_4 tiene elementos de tres tipos $[1], [2, 2]$ y $[3]$ cada clase de conjugación de A_4 está contenida dentro de una de las siguientes clases de conjugación de S_4:

$$\begin{aligned} 1^{S_4} &= \{1\}, \\ ((1\ 2)(3\ 4))^{S_4} &= \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\ (1\ 2\ 3)^{S_4} &= \{(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}. \end{aligned}$$

Claramente $1^{A_4} = \{1\}$, con lo que la primera es una clase de conjugación de A_4. También la segunda lo va ser pues es fácil ver que los tres elementos son conjugados en A_4:

$$(1\ 2)(3\ 4)^{(1\ 2\ 3)} = (1\ 3)(2\ 4), \quad (1\ 2)(3\ 4)^{(1\ 2\ 4)} = (1\ 4)(2\ 3).$$

Sin embargo el último conjunto no puede ser una clase de conjugación de A_4 pues su cardinal 8 no divide 6 que es al orden de A_4. En realidad, el centralizador de cualquier 3-ciclo g en A_4 es el grupo generado por g, que tiene 3 elementos con lo que $g^{A_4} = [A_4 : C_{A_4}(g)] = \frac{12}{3} = 4$. Por tanto, los ocho elementos de $(1\ 2\ 3)^{S_4}$ se tienen que dividir en dos clases de conjugación de A_4. En concreto

$$(1\ 2\ 3)^{A_4} = \{(1\ 2\ 3), (1\ 2\ 3)^{(1\ 2)(3\ 4)} = (1\ 4\ 2), (1\ 2\ 3)^{(1\ 3)(2\ 4)} = (1\ 3\ 4), (1\ 2\ 3)^{(1\ 4)(2\ 3)} = (2\ 4\ 3)\}$$

y

$$(1\ 3\ 2) = (1\ 2\ 3)^{S_4} \setminus (1\ 2\ 3)^{A_4} = \{(1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 3), (2\ 3\ 4)\}.$$

Problema 2

(1) **Sea G un grupo finito. Demostrar que si G no es un p-grupo entonces tiene dos subgrupos H y K tales que $H \not\subseteq K$ y $K \not\subseteq H$.**

Por el Teorema de Cauchy, G tiene un elemento h de orden p y otro k de orden q. Aplicando el Teorema de Lagrange se deduce que $H = \langle h \rangle$ y $K = \langle k \rangle$ cumplen lo que se pide.

(2) **Sean σ y τ dos elementos de A_n que tienen el mismo tipo. Demostrar que si $|M(\sigma)| \leq n-2$ entonces σ y τ son conjugados en A_n.**

Como σ y τ tienen el mismo tipo son conjugados en S_n. Por tanto existe $\alpha \in S_n$ tal que $\sigma^\alpha = \tau$. Si $\alpha \in A_n$ entonces σ y τ son conjugados en A_n. Supongamos que $\alpha \notin A_n$. Como $|M(\sigma)| \leq n-2$ se tiene que S_n contiene un 2-ciclo ρ disjunto con σ. Eso implica que σ y ρ conmutan y $\beta = \rho\alpha \in A_n$. Luego $\tau = \sigma^\alpha = \sigma^{\rho\alpha} = \sigma^\beta$ y por tanto σ y τ son conjugados en A_n.

(3) **Demostrar que el centro de S_n tiene más de un elemento si y solo si $n = 2$.**

Si $n \leq 2$ entonces S_n es conmutativo y por tanto $|Z(S_n)| = |S_n| = n$. Supongamos que $n > 2$ y sea $\sigma \in S_n \setminus \{1\}$. Sean $i \in M(\sigma)$ y $j = \sigma(i)$. Sea k un elemento de $\{1, \ldots, n\}$ distinto de i y j. Entonces $\sigma(i\ k)\sigma^{-1} = (j\ \sigma(k)) \neq (i\ k)$ y por tanto $\sigma \notin Z(S_n)$. Por tanto $|Z(S_n)| = 1$.

(4) **Demostrar que si H es un subgrupo cíclico y normal de un grupo G entonces todo subgrupo de H es normal en G.**

Sea h un generador de H y sea K un subgrupo de H. Entonces $K = \langle h^n \rangle$ para algún entero n. Sea $g \in G$. Entonces $h^g = h^r$ para algún entero r. Si $k \in K$ entonces $k = h^m$. Usando que la conjugación por g es un automorfismo deducimos que $h^g = (h^m)^g = (h^g)^m = (h^r)^m = h^{rm} \in K$. Por tanto K es normal en G.

Problema 3

(1) **Sea A un grupo abeliano finito no cíclico. Demostrar que existe un número primo p tal que A contiene al menos 3 subgrupos distintos de orden p.**

Sean $(d_1, \ldots, d_n)$ la lista de los divisores elementales. Como A no es cíclico $n \geq 2$ y A contiene un subgrupo isomorfo a $C_{d_1} \times C_{d_2}$. Sea p un divisor de d_2. Como d_2 divide a d_1 también tenemos que p divide a d_2. Por tanto cada uno de los factores C_{d_i} con $i = 1, 2$ contiene un elemento de orden p con lo que A contiene un subgrupo $\langle a_1 \rangle \times \langle a_2 \rangle$ con $|a_1| = |a_2| = p$. Entonces $\langle a_1 \rangle, \langle a_2 \rangle$ y $\langle a_1 a_2 \rangle$ son tres subgrupos de orden p.

(2) **Sean A un grupo abeliano finito y p un número primo. Sea n el número de subgrupos de A de orden p. Demostrar que $n \neq 2$.**

Si A es cíclico, entonces $n = 1$. En caso contrario el argumento del problema anterior muestra que $n \geq 3$.

(3) **Sea p un primo, n un entero mayor que 1 y A un grupo isomorfo a $C_{p^n} \times C_p$. Demostrar que A tiene un grupo B de orden p tal que $f(B) = B$ para todo automorfismo f de A.**

(4) **Sea p un primo, n un número natural y A un grupo isomorfo a $C_{p^n} \times C_p$. Supongamos que para todo elemento a de orden p de A existe un automorfismo f de A tal que $f(a) \notin \langle a \rangle$. Demostrar que $n = 1$.**

Claramente los dos últimos problemas piden demostrar dos propiedades una de las cuales es la contra-reciproca de la otra. Por tanto realizamos el (3) y la misma solución sirve para el (4).

Tenemos $A = \langle a \rangle_{p^n} \times \langle b \rangle_p$ y sea $B = A^{p^{n-1}} = \{g^{p^{n-1}} : g \in A\}$. Si f es un automorfismo de A y $b \in B$ entonces $b = g^{p^{n-1}}$ para algún $g \in A$ con lo que $f(b) = f(g)^{p^{n-1}} \in B$. Esto demuestra que $f(B) \subseteq B$ y como B y $f(B)$ son conjuntos finitos del mismo cardinal por ser f un automorfismo, con lo que $f(B) = B$. Claramente B es un subgrupo de A (por ser A abeliano) y solo falta demostrar que tiene orden p. Pero cada elemento de A es de la forma $g = a^i b^j$ y como $n \geq 2$ se cumple que $g^{p^{n-1}} = a^{ip^{n-1}}$. Eso demuestra que $B = \langle a^{p^{n-1}} \rangle$ y por tanto $|B| = \frac{|a|}{\text{mcd}(|a|, p^{n-1})} = p$.

Problemas de Anillos.

Problema 4

(1) **Sea p un número primo. Demostrar que un polinomio de $\mathbb{Z}_{p^2}[X]$ es divisor de 0 si y solo si pertenece al ideal generado por la clase de p módulo p^2.**

Sea $f = \sum_{i \geq 0} f_i X^i$ con $f_i \in \mathbb{Z}_{p^2}$. Abusando de la notación denotamos por p a $p + (p^2)$. Si $f \in (p)$, entonces $pf = 0$ con lo que f es un divisor de 0. Recíprocamente, supongamos que $f \notin (p)$. Eso implica que $f_i \notin (p)$ para algún $i \geq 0$ y denotamos por i el menor entero no negativo que cumple esta condición. Supongamos que $fg = 0$ para un polinomio $g = \sum_{i \geq 0} g_i X^i$ con cada $g_i \in \mathbb{Z}_{p^2}$. Sea $\phi : \mathbb{Z}_{p^2} \to \mathbb{Z}_p$ el homomorfismo que asocia $x + (p^2)$ con $x + (p)$. Por la Propiedad Universal del Anillo de Polinomios ϕ se extiende de forma

única a un homomorfismo que asocia X consigo mismoa y que también denotamos ϕ. Claramente (p) es el núcleo de ϕ con lo que $\phi(f) \neq 0$ mientras que $\phi(f)\phi(g) = \phi(fg) = 0$. Como $\mathbb{Z}_p$ es un cuerpo $\mathbb{Z}_p[X]$ es un dominio, con lo que $\phi(g) = 0$, o sea $p \mid g_i$ para todo i. Si $g \neq 0$ entonces existe un j (que elegimos mínimo) con $p^2 \nmid g_j$. Entonces el coeficiente de $i+j$ en fg es $0 = \sum_{n=0}^{i+j} f_n g_{i+j-n}$. Pero $p \mid f_n$ para todo $n < i$ y si $i < n \leq i + ji$ entonces $0 \leq i + j - n < j$ con lo que $p \mid g_{i+j-n}$. Por tanto $p \mid f_i g_j$. Como $p \nmid f_i$, f_i es invertible en $\mathbb{Z}_{p^2}$, con lo que $g_j = 0$, en contra de la construcción. Esto demuestra que f no es divisor de 0.

(2) **Sea p un número primo (positivo) y sea A el subanillo de $\mathbb{Q}$ formado por las fracciones cuyo denominador no es múltiplo de p. Demostrar que todo ideal no nulo de A está generado por p^n para algún $n \geq 0$. Describir los elementos invertibles y los irreducibles de A.**

En primer lugar está claro que una fracción $\frac{a}{b}$ en la que ni a ni b son múltiplos de p es invertible en A. Recíprocamente si x es un elemento invertible de A entonces $x = \frac{a}{b}$ con a y b enteros de forma que $p \nmid b$ y $x^{-1} = \frac{c}{d}$ para enteros c y d con $p \nmid d$. Eso implica que $p \nmid bd = ac$ y por tanto $p \nmid a$. Luego A^* está formado por las fracciones con numerador y denominador entero no múltiplo de p.

Sea I un ideal no nulo de A. Vamos a ver que $p^n \in I$ para algún entero positivo. En efecto, como $I \neq 0$ existen enteros $a \neq 0$ y $p \nmid b$ tales que $x = \frac{a}{b} \in I$. Si ponemos $a = p^n c$ con $p \nmid c$ entonces, $\frac{b}{c} \in A$ y por tanto $\frac{b}{c}x = p^n \in I$. Sea n el menor entero no negativo tal que $p^n \in I$. Entonces $(p^n) \subseteq I$. Sea $x \in I \setminus \{0\}$ y escribamos x como fracción de números enteros $x = \frac{a}{b}$ con $p \nmid b$. Pongamos $a = p^m c$ con $p \nmid c$. de nuevo $\frac{c}{b} \in A^*$ con lo que $p^m = \frac{b}{c}x \in I$. Por la elección de n tenemos que $m \geq n$ con lo que $p^m \in (p^n)$ y por tanto $x = p^m \frac{c}{b} \in (p^n)$. Concluimos que $I = (p^n)$.

El párrafo anterior muestra que A es un DIP en ql eque el único ideal maximal es (p). Como en un DIP los irreducibles son los elementos que general un ideal maximal los irreducibles serán los asociados de p es decir los elementos de la forma $\frac{pa}{b}$ con a y b enteros coprimos con p.

(3) **Sea K un cuerpo y sea $K(X)$ el cuerpo de cocientes de $K[X]$. Sea A el subanillo de $K(X)$ formado por las fracciones de la forma P/X^n con $P \in K[X]$ y $n \in \mathbb{N}$. Demostrar que para todo $a \in A \setminus \{0\}$ existen enteros únicos $n \leq m$ tales que $a = \sum_{i=n}^{m} a_i X^i$ con $a_i \in K$ para todo i y $a_n a_m \neq 0$ y que $\delta(a) = m - n$ define una función euclídea en A. Describir los elementos invertibles de A.**

Sea $a = \frac{P}{X^k}$ con $P \in K[X]$. Supongamos que P tiene grado u y que v es el menor de los grados de los monomios no nulos que forman P. O sea $P = \sum_{i=v}^{u} p_i X^i$ con $0 \leq v \leq u$ y $p_v p_u \neq 0$. Si $m = u - k$ y $n = v - k$ entonces $a = \sum_{i=u}^{v} p_i X^{i-k} = \sum_{i=m}^{n} p_{i+k} X^i$, con lo que $a_i = p_{i+k}$ satisface la propiedad requerida. Recíprocamente si $a = \sum_{i=n_1}^{m_1} b_i X^i$ con $n_1 \leq m_1$ y $b_n b_m \neq 0$, entonces $\sum_{i=n_1}^{m_1} b_i X^{i+k} = X^k a = P$ lo que implica que $n_1 = n$, $m_1 = m$ y $b_i = p_{i+k} = a_i$ para todo i.

Usando que K es un cuerpo es fácil ver que $\delta(ab) = \delta(a) + \delta(b)$ lo que implica que si $a \mid b$ entonces $\delta(a) \leq \delta(b)$. Esto demuestra que δ verifica el primer axioma de función

euclídea.

Para demostrar que δ verifica el segundo axioma de función euclídea tomemos $a = \sum_{i=n}^{m} a_i X^i$ y $b = \sum_{i=u}^{v} b_i X^i$ con $a_n a_m b_u b_v \neq 0$. Sean $k = \max(0, -n)$ y $l = \max(0, -u)$. Entonces $A = X^k a$ y $B = X^l b$ pertenecen a $K[X]$ y se cumple que $\mathrm{gr}(A) = \delta(a)$ y $\mathrm{gr}(B) = \delta(b)$. Como sabemos que el grado es una función euclídea en $K[X]$ existen polinomios Q y R tales que $A = BQ + R$ y o bien $R = 0$ ó $\mathrm{gr}(Q) < \mathrm{gr}(B)$. Sean $q = \frac{B}{X^{k-l}}$ y $r = \frac{R}{X^k}$. Entonces $a = \frac{A}{X^k} = \frac{BQ+R}{X^k} = \frac{Q}{X^{k-l}} \frac{B}{X^l} + \frac{R}{X^k} = qb + r$ y, o bien $r = 0$ ó $\delta(r) = \delta(R) \leq \mathrm{gr}(R) < \mathrm{gr}(B) = \delta(b)$.

Como consecuencia de que δ es una función euclídea y que $\delta(1) = 0$ deducimos que $A^* = \{a \in A : \delta(a) = 0\} = \{\alpha X^n : \alpha \in K \setminus \{0\}, n \in \mathbb{Z}\}$.

(4) **Sean K un cuerpo, $a \in K$ y $K(X)$ el cuerpo de cocientes de $K[X]$. Sea A el subanillo de $K(X)$ formado por las fracciones $\frac{P}{Q}$ con $P, Q \in K[X]$ y $Q(a) \neq 0$. Demostrar que todo ideal no nulo de A está generado por $(X-a)^n$ para algún $n \geq 0$. Describir los elementos invertibles y los irreducibles de A.**

Por el Teorema de Ruffini $Q(a) = 0$ si y solo si $X - a \mid Q$. El ejercicio se hace igual que el ejercicio (2) con $X - a$ tomando el papel de p. Así los invertibles son las fracciones $\frac{P}{Q}$ con $P(a)Q(a) \neq 0$ y los irreducibles las fracciones de la forma $(X-a)\frac{P}{Q}$ con $P(a)Q(a) \neq 0$.

Problema 5

(1) Factorizar los dos polinomios de la forma $X^5 + aX^4 + aX^3 - aX^2 + 1$ en $\mathbb{Z}_2[X]$ y decidir para qué números enteros a los polinomios de esa forma son irreducibles en $\mathbb{Q}[X]$.

(2) Factorizar los dos polinomios de la forma $X^5 + aX^3 + 1$ en $\mathbb{Z}_2[X]$ y decidir para qué números enteros a los polinomios de esa forma son irreducibles en $\mathbb{Q}[X]$.

(3) Factorizar los dos polinomios de la forma $X^5 + aX^4 + aX^2 - aX + 1$ en $\mathbb{Z}_2[X]$ y decidir para qué números enteros a los polinomios de esa forma son irreducibles en $\mathbb{Q}[X]$.

(4) Factorizar los dos polinomios de la forma $X^5 + aX^2 + 1$ en $\mathbb{Z}_2[X]$ y decidir para qué números enteros a los polinomios de esa forma son irreducibles en $\mathbb{Q}[X]$.

Llamamos al polinomio f cuando lo consideramos en $\mathbb{Q}[X]$. Tenemos que factorizar f_2 y decidir sobre la irreducibilidad de $\mathbb{Q}[X]$.

Las únicas raíces posibles de f en $\mathbb{Q}$ son 1 y -1. Si 1 es raíz entonces $a = -2$ y si -1 es raíz entonces $a = 0$. Por tanto, si $a = 0$ ó -2 entonces f es reducible en ambos casos.

Si a es par entonces $f_2 = (X+1)g$ con $g = X^4 + X^3 + X^2 + X + 1$. Además g es irreducible pues no tiene ninguna raíz en $\mathbb{Z}_2$ y no es $(X^2 + X + 1)^2 = X^4 + X^2 + 1$. Esto nos da la factorización de f_2. Por tanto f no es divisible por un polinomio de grado 2. Con lo que si $a \neq 0, 2$ entonces f es irreducible en $\mathbb{Z}[X]$ y como f es primitivo, también es irreducible en $\mathbb{Q}[X]$.

Supongamos que a es impar. Entonces $f_2 \in \{X^5 + X^4 + X^3 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^2 + 1, X^5 + X^3 + X^2 + X + 1\}$. En los cuatro casos f_2 no tiene raíces en $\mathbb{Z}_2$. Si no fuera

irreducible sería el producto de dos polinomio irreducibles de grados 2 y 3 respectivamente. Solo hay un irreducible de grado 2 (X^2+X+1) y dos de grado 3 (X^3+X+1 y X^3+X^2+1). Multiplicando obtenemos

$$(X^2+X+1)(X^3+X+1) = X^5+X^4+1 \quad (X^2+X+1)(X^3+X^2+1) = X^5+X+1$$

que no es ninguno de los cuatro casos. Por tanto f_2 es irreducible en $\mathbb{Z}_2[X]$. Por el Criterio de Reducción f es irreducible en $\mathbb{Z}[X]$ y como f es primitivo también es irreducible en $\mathbb{Q}[X]$.

Problemas de Grupos no comunes
Problema 4

(1) **Demostrar que el número de clases de conjugación de D_n es $\frac{n+3}{2}$ si n es impar y $\frac{n+6}{2}$ si n es par.**

Ver la solución del problema 1.

(2) **Sean a y b dos elementos de un grupo G, $n=|a|$ y $m=|b|$ y supongamos que $bab^{-1}=a^r$. Demostrar que $\mathrm{mcd}(r,n)=1$ y $r^m \equiv 1 \bmod n$.**

Como la conjugación es un automorfismo del grupo se tiene que $|a^r| = |bab^{-1}| = |a| = n$ y por tanto $n = |a^r| = \frac{n}{\mathrm{mcd}(r,n)}$ con o que $\mathrm{mcd}(r,n)=1$. Por otro lado por inducción sobre i es fácil demostrar que $b^i a b^{-i} = a^{r^i}$. En particular, como $b=1$ tenemos que $a = b^m a b^{-m} = a^{r^m}$ y por tanto $a^{r^m-1}=1$ con lo que n divide a r^m-1 o lo que es lo mismo $r^m \equiv 1 \bmod n$.

(3) **Sean p un número primo y sean n y m dos números naturales con $p \nmid n$. Demostrar (1) $n^{(p-1)p^{m-1}} \equiv 1 \bmod p^m$ y (2) $n^{p^{m-1}} \equiv 1 \bmod p^m$ si y solo si $n \equiv 1 \bmod p$.**

El cardinal del grupo $\mathbb{Z}_{p^m}^*$ de unidades $\mathbb{Z}_{p^m}$ es $\varphi(p^m) = (p-1)p^{m-1}$. Por el Teorema de Lagrange $g^{(p-1)p^{m-1}} = 1$ para todo $g \in \mathbb{Z}_{p^m}^*$. Como n representa un elemento $n+(p^m)$ de $\mathbb{Z}_{p^m}^*$ se deduce que $n^{(p-1)p^{m-1}} \equiv 1 \bmod p^m$.

Consideremos ahora el homomorfismo $f : \mathbb{Z}_{p^m} \to \mathbb{Z}_p$ dado por $f(a+(p^m)) = a+(p)$. Este homomorfismo se restringe a un homomorfismo $\phi : \mathbb{Z}_{p^m}^* \to \mathbb{Z}_p^*$. Este homomorfismo es suprayectivo pues cada elemento $x = a+(p) \in \mathbb{Z}_p$ es la imagen de $a+(p^n)$. Además $x \in \mathbb{Z}_p^*$ si y solo si $p \nmid a$ en cuyo caso $a+(p^n) \in \mathbb{Z}_{p^m}^*$. Aplicando el Primer Teorema de Isomorfía tenemos que $|\ker\phi| = \frac{|\mathbb{Z}_{p^m}^*|}{|\mathbb{Z}_p^*|} = \frac{(p-1)p^{m-1}}{p-1} = p^{m-1}$. Si $n \equiv 1 \bmod p$ entonces $n+(p^m) \in \ker\phi$ y por tanto, aplicando de nuevo el Teorema de Lagrange y lo que acabamos demostrar sobre el cardinal de $\ker\phi$ deducimos que $n^{p^{m-1}} \equiv 1 \bmod p^m$.

Recíprocamente, supongamos que $n^{p^{m-1}} \equiv 1 \bmod p^m$. Eso implica que $n+(p^m)$ tiene orden potencia de p y por tanto también $n+(p) = \phi(n+(p^m))$ tiene orden potencia de p. Pero ese orden es divisor de $p-1$, por el Teorema de Lagrange (o el Teorema de Fermat). Por tanto, el orden de $n+(p)$ es 1, es decir $n \equiv 1 \bmod p$.

(4) **Sea G un grupo de orden $2p$ con p primo impar. Demostrar que G es isomorfo a C_{2p} o a D_p.**

Por el Teorema de Cauchy G tiene un elemento a de orden p y un elemento b de orden 2. Entonces $\langle a\rangle$ es un subgrupo de índice 2 de G y por tanto se trata de un subgrupo normal de G. Luego $a^b = a^r$ para algún entero r. Por otro lado $a = a^{b^2} = (a^r)^b = (a^b)^r = a^{r^2}$. Esto implica que $r^2 \equiv 1 \bmod p$. Como $\mathbb{Z}_p$ es un cuerpo esto implica que $r \equiv 1 \bmod p$ o $r \equiv -1 \bmod p$. En el primer caso a y b conmutan y por tanto G es un grupo abeliano de orden $2p$. En tal caso, del Teorema de Estructura de Grupos Abelianos se deduce que G es cíclico. Supongamos que $r \equiv -1 \bmod p$. Entonces $a^b = a^{-1}$ o lo que es lo mismo $ba = a^{-1}b$ y ahora está claro que G es isomorfo al grupo diédrico D_p.

Problema 5

(1) **Demostrar que si G es un grupo no abeliano de orden p^3 con p un número primo entonces $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.**

Por el Teorema de Lagrange, $|Z(G)|$ es $1, p, p^2$ ó p^3. El último caso no se da porque G no es abeliano y el primero porque G es un p-grupo y por tanto su centro no es trivial. Además, $G/Z(G)$ no es cíclico porque en caso contrario G es abeliano. Por tanto, $|G/Z(G)|$ no puede tener orden primo, lo que excluye también la opción $|Z(G)| = p^2$. Por tanto $G/Z(G)$ es un grupo de orden p^2 que no es cíclico. Lo primero implica que $G/Z(G)$ es abeliano y, usando el Teorema de Estructura de Grupos Abelianos deducimos que $G/Z(G) \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

(2) **Sea H un subgrupo de índice dos en un grupo G. Supongamos que H tiene dos elementos x e y que son conjugados en G pero no lo son en H. Demostrar que $C_G(x) \subseteq H$.**

Sea $g \in C_G(x)$ y sea $h \in G$ tal que $y = x^h$. Entonces $x^{gh} = (x^g)^h = x^h = y$. Como x e y no son conjugados en H se tiene que $h, gh \notin H$, pero como H tiene índice 2 en G se tiene que $g \in H$, como queríamos demostrar.

(3) **Sea H un subgrupo de S_n con $n \neq 4$. Demostrar que si $H \not\subseteq A_n$ y $|H| \geq 3$, entonces H no es simple.**

(4) **Sea H un subgrupo simple de S_n, con $n \geq 4$ que contiene más de dos elementos. Demostrar que $H \subseteq A_n$.**

Los dos problemas son equivalentes con lo que vamos a solucionar solo el segundo. Por el Tercer Teorema de Isomorfía $H \cap A_n$ es un subgrupo normal de H. Por tanto si H es simple entonces $H \cap A_n = 1$ ó $H \cap A_n = A_n$. Lo segundo implica que $H \subseteq A_n$ que es lo que queremos demostrar. Por tanto, basta demostrar que $H \cap A_n \neq 1$. Pero en tal caso, por el Tercer Teorema de Isomorfía $|H| = |H/H \cap A_n| = |HA_n/A_n| \leq |S_n/A_n| = 2$.

Como H tiene al menos tres elementos existen H tiene dos elementos distintos g y h tal que $1 \neq x = gh^{-1} \in H \cap A_n$, lo que demuestra que efectivamente $H \cap A_n \neq 1$. Obsérvese que las hipótesis $n \neq 4$ o $n \geq 4$ en realidad no hacían falta.