Grupos y Anillos. Examen Final. Parte no común. 10 de julio de 2020.

Problemas de grupos comunes

(1) (2 puntos)

Sea H un subgrupo de un grupo G y sea $N_G(H) = \{g \in G : gH = Hg\}$. Demostrar

- **(a)** **$N_G(H)$ es un subgrupo de G que contiene a H como subgrupo normal.**
- **(b)** **Si K es un subgrupo de G que contiene a H como subgrupo normal entonces K está contenido en $N_G(H)$. O sea $N_G(H)$ es el mayor subgrupo de G que contiene a H como subgrupo normal.**
- **(c)** **El cardinal del conjunto $\{H^g : g \in G\}$ de conjugados de H en G es igual a $[G : N_G(H)]$.**

Consideramos G actuando por la derecha en el conjunto de subgrupos por conjugación, o sea $K \cdot g = K^g$. Entonces $N_G(H) = \text{Estab}_G(H)$. En particular, $N_G(H)$ es un subgrupo de G y la órbita de H tiene cardinal $[G : N_G(H)]$. Como dicha órbita es $\{H^g : g \in G\}$ el apartado (c) ya estará y del apartado (a) solo falta ver que H está contenido en $N_G(H)$:Si $h \in H$ entonces $hH = H = Hh$, con lo que $H \subseteq N_G(H)$ y en particular $N_G(H) \neq \emptyset$. Sean $a, b \in N_G(H)$ y sea $h \in H$. Finalmente, si $k \in K$ entonces $kH = Hk$ porque H es un subgrupo normal de K. Luego $k \in N_G(H)$. Esto demuestra (b).

Sea n un número natural y sea G un grupo cíclico de orden n. Demostrar las siguientes afirmaciones:

- **(a)** **Si r es un entero coprimo con n entonces la aplicación $\sigma_r : G \to G$ dada por $\sigma_r(g) = g^r$ es un automorfismo de G.**
- **(b)** **La aplicación $r + n\mathbb{Z} \to \sigma_r$ está bien definida y define un isomorfismo del grupo $\mathbb{Z}_n^*$ de unidades del anillo $\mathbb{Z}_n$ al grupo de automorfismos de G.**

(a) Como G es abeliano, si $g, h \in G$ entonces $\sigma_r(gh) = (gh)^r = g^r h^r = \sigma_r(g)\sigma_r(h)$. Esto demuestra que σ_r es un homomorfismo. Como r y n son coprimos, existen enteros a, b tales que $ar + bn = 1$. Eso implica que a es coprimo con n y $\sigma_a\sigma_r(g) = g^{ar} = g^{ar+bn} = g$ para todo $g \in G$, pues $g^n = 1$. Luego $\sigma_a \circ \sigma_r$ es la identidad de G y análogamente $\sigma_r \circ \sigma_a$ es la identidad de G. Por tanto σ_r es un automorfismo.

(b) Si r y s son enteros tales que $r \equiv s \mod n$ entonces $s = r + mn$ para otro entero m y por tanto $\sigma_s(g) = g^s = g^{r+mn} = g^r = \sigma_r(g)$, pues $g^n = 1$. Eso demuestra que la aplicación $r + n\mathbb{Z} \mapsto \sigma_r$ está bien definida. Además, para todo r y s se tiene que $\sigma_r\sigma_s(g) = g^{rs} = \sigma_{rs}(g)$, lo que demuestra que la aplicación es un homomorfismo. Una vez que sabemos que es homomorfismo para ver que es inyectiva vemos que el núcleo es trivial. En efecto, si $r + n\mathbb{Z}$ está en el núcleo, $\sigma_r = 1$ lo que implica que $g^r = g$ para todo $g \in G$, o lo que es lo mismo $g^{r-1} = 1$. Pero G tiene un elemento de orden n con lo que n divide a $r - 1$, o sea $r + n\mathbb{Z} = 1 + n\mathbb{Z}$. Luego efectivamente el núcleo es trivial y la aplicación es inyectiva. Para ver que es suprayectiva tomamos un automorfismo cualquiera f de G y fijemos un generador g de G. Entonces $f(g) = g^r$ para algún entero r. Además $f(g^s) = g$ para otro entero s, por ser f suprayectiva. Eso implica que $g^{rs} = f(g^s) = g$, con lo que $g^{rs-1} = 1$ y por tanto $rs - 1$ divide a $n = |g|$. Por tanto $rs \equiv 1 \mod n$ lo que implica que $r + n\mathbb{Z}$ es invertible en $\mathbb{Z}_n^*$. Además $f(g) = \sigma_r(g)$ y como g genera G se tiene que $f = \sigma_r$.

Sea G un grupo y sea H un subgrupo de G. El core de H en G es $\text{Core}_G(H) = \cap_{g\in G} H^g$. Demostrar:

(a) **$\text{Core}_G(H)$ es un subgrupo normal de G contenido en H.**

(b) **Si K es un subgrupo normal de G contenido en H entonces $K \subseteq \text{Core}_G(H)$. O sea $\text{Core}_G(H)$ es el mayor subgrupo normal de G contenido en H.**

(c) **Si $[G : H]$ es finito entonces $[G : \text{Core}_G(H)]$ es finito.**

(a) Como la conjugación es un automorfismo, cada H^g es un subgrupo de G y por tanto $\text{Core}_G(H)$ es subgrupo de G por ser intersección de subgrupos. Como H es uno de esos subgrupos, $\text{Core}_G(H) \subseteq H$. Si $a, b \in G$ y $x \in \text{Core}_G(H)$ entonces $x \in H^{ba^{-1}}$, o sea $x = h^{ba^{-1}}$ para algún $h \in H$. Luego $x^a = h^b \in H^b$. Esto demuestra que $x^a \in \cap_{b\in G} H^b = \text{Core}_G(H)$ para todo $x \in \text{Core}_G(H)$ y todo $a \in G$. Luego $\text{Core}_G(H)$ es normal en G.

(b) Si K es un subgrupo normal de G contenido en H entonces $K = K^g \subseteq H^g$ para todo $g \in G$ y por tanto $K \subseteq \cap_{g\in G} H^g = \text{Core}_G(H)$.

(c) Como conjugar por un elemento g de G es un automorfismo de G que envía H a H^g se tiene que $[G : H] = [G : H^g]$ para todo $g \in G$. Por tanto, si $[G : H]$ es finito también lo es $[G : H^g]$ para todo $g \in G$. Sea $x_1, \dots, x_n$ un conjunto de representantes de las clases laterales por la derecha de H en G. Eso implica que todo elemento de G es de la forma hx_i para algún $h \in H$ y algún i. Entonces $H^{hx_i} = H^{x_i}$ con lo que $\text{Core}_G(H) = \cap_{h\in H} \cap_{i=1}^n H^{x_i} = \cap_{i=1}^n H^{x_i}$. Ahora razonamos por inducción en k para ver que $[G : \cap_{i=1}^k H^{x_i}]$ es finito. Si $k = 1$ basta aplicar lo que hemos dicho arriba. Para el paso de inducción vamos a usar las siguiente fórmula para dos subgrupos A y B de G: $|A \cdot B| \cdot |A \cap B| = |A| \cdot |B|$ que se vio en el Problema 4.2.7 y la obvia fórmula $[G : A] = [G : B][B : A]$ para el caso en que A esté contenido en B. Si $k > 1$, ponemos $K = \cap_{i=1}^{k-1} H^{x_i}$. Por hipótesis de inducción $[G : K]$ es finito. Como además $[G : H^{x_k}]$ también es finito tenemos que $[H^{x_k} : H^{x_k} \cap K] = \frac{|H^{x_k}|}{H^{x_k} \cap K} = \frac{|H^{x_k} K|}{|K|} \le [G : K] < \infty$. Por tanto $[G : \cap_{i=1}^k H_i] = [G : H^{x_k} \cap K] = [G : H^{x_k}][H^{x_k} : H_k \cap K]$ es finito. Esto concluye el argumento de inducción. Aplicándolo para $k = n$ tenemos que $[G : \text{Core}_G(H)] = [G : \cap_{i=1}^n H^{x_i}]$ es finito.

Sea G un grupo y sea H un subgrupo de G. Se llama clausura normal de H en G a $CN_G(H) = \cap_{H\subseteq N \trianglelefteq G} N$. Demostrar:

(a) **$CN_G(H)$ es un subgrupo normal de G que contiene a H.**

(b) **Todo subgrupo normal de G que contiene a H también contiene a $CN_G(H)$. O sea $CN_G(H)$ es el menor subgrupo normal de G que contiene a H.**

(c) **$CN_G(H) = \{h_1^{g_1} \cdots h_k^{g_k} : k \ge 0, h_1, \dots, h_k \in H, g_1, \dots, g_k \in G\}$.**

(a) Como $CN_G(H)$ es intersección de subgrupos normales de G, él es normal en G, y como todos esos subgrupos contienen a H la intersección también contiene a H.

(b) Si K es un subgrupo de G que contiene a H, entonces K es uno de los subgrupos que se usan en la construcción de $CN_G(H)$ como intersección de subgrupos y por tanto $CN_G(H)$ está contenido en K.

(c) Sea K el conjunto de la derecha. Como $H \subseteq CN_G(H)$ y $CN_G(H)$ es un subgrupo normal de G todos los elementos que forma K están en $CN_G(H)$, o sea $K \subseteq CN_G(H)$.

Si $x, y \in K$ entonces $x = h_1^{g_1} \cdots h_k^{g_k}$ e $y = h_{k+1}^{g_{k+1}} \cdots h_n^{g_n}$ con $g_1, \dots, g_n \in G$ y $h_1, \dots, h_n \in H$. Por tanto $xy = h_1^{g_1} \cdots h_n^{g_n} \in K$ y $x^{-1} = (h_1^{g_1} \cdots h_k^{g_k})^{-1} = h_k^{-1 g_k} \cdots h_1^{-1 g_1} \in K$. Esto demuestra que K es un subgrupo de G que obviamente contiene a H. Además, si $g \in G$ entonces $x^g = h_1^{g_1 g} \cdots h_k^{g_k g} \in K$, con lo que K es normal en G. Como claramente K contiene a H, tenemos que K es un subgrupo normal de G que contiene a H y por el apartado (b) se tiene que $CN_G(H) \subseteq K$.

(2) (1.5 puntos)

Demostrar que si g y h son elementos de un grupo entonces gh y hg tienen el mismo orden.

La conjugación con un elemento de G es un autormorfismo de G y por tanto asocia elementos del mismo orden. Como $(gh)^g = g^{-1}ghg = hg$, se tiene que gh y hg son conjugados y por tanto tienen el mismo orden.

Demostrar que si H y K son subgrupos normales de G con $H \cap K = 1$ entonces $hk = kh$ para todo $h \in H$ y $k \in K$.

Sean $h \in H$ y $k \in K$. Como H y K son subgrupos normales de G se tiene que $h^{-1}, h^k \in H$ y $(k^{-1})^h \in K$. Por tanto $h^{-1}k^{-1}hk = h^{-1}k^k \in H$ y $h^{-1}k^{-1}hk = (k^{-1})^h k \in K$. Deducimos pues que $h^{-1}k^{-1}hk$ con lo que $h^{-1}k^{-1}hk = 1$ o lo que es lo mismo $hk = kh$.

Demostrar que si N es un subgrupo normal de un grupo G entonces el centro $Z(N)$ de N y el centralizador $C_G(N)$ de N en G son ambos subgrupos normales de G.

Sean $g \in G$, $h \in C_G(N)$ y $n \in N$. Entonces $gng^{-1} \in N$, por ser N normal en G, con lo que $(gng^{-1})h = hgng^{-1}$. Luego $h^g n = g^{-1}hgn = g^{-1}h(gng^{-1})g = g^{-1}(gng^{-1})hg = nh^g$. Esto demuestra que $h^g \in C_G(N)$. Por tanto $C_G(N)$ es normal en G. Como $Z(N) = N \cap C_G(N)$ y la intersección de dos subgrupos normales de G es normal en G, deducimos que $Z(N)$ es normal en G.

Sea H un subgrupo normal de S_n. Demostrar que si H contiene una transposición entonces $H = S_n$.

Todas las transposiciones de S_n son conjugadas en S_n con lo que si H contiene una transposición entonces las contiene todas, por ser H normal en S_n. Como S_n está generado por las transposiciones deducimos que $H = S_n$.

Problemas Examen final.
Anillos

(3) (2 puntos)

Sea K un cuerpo. Demostrar que para cada dos enteros n y m se verifica que el polinomio $Y^n + XY^m + X^2Y^m + X^3Y$ es irreducible en $K[X,Y]$.

Sea K un cuerpo. Demostrar que para cada dos números naturales n y m se verifica que el polinomio $Y^3 + X^nY^2 + X^mY + X$ es irreducible en $K[X,Y]$.

En el primer casos basta considerar el polinomio como un polinomio en la variable Y con coeficientes en $K[X]$ y aplicar el Criterio de Eisenstein con el irreducible X del DFU $K[X]$ y en el segundo igual intercambiando los papeles de X e Y.

Sea D un DFU y sean p y q irreducibles no asociados de D y n un número natural. Demostrar que el polinomio $pX^n + q^2$ es irreducible en $D[X]$.

Sea D un DFU y sean p y q irreducibles no asociados de D y n un número entero mayor que 1. Demostrar que el polinomio $pX^n + pqX + q^2$ es irreducible en $D[X]$.

En ambos, basta aplicar la versión del Criterio de Eisenstein "al revés" que aparece en el Problema 3.4.1. con el irreducible p.

(4) (1.5 puntos)

Demostrar que si D es un DFU entonces la intersección de cada dos ideales principales de D es otro ideal principal.

Sea $a, b \in D$. Si $a = 0$ o $b = 0$ entonces $(a) \cap (b) = (0)$. Supongamos que $a \neq 0$ y $b \neq 0$ y sean $a = up_1^{\alpha_1} \dots p_k^{\alpha_k}$ y $b = vp_1^{\beta_1} \dots p_k^{\beta_k}$ factorizaciones de a y b con $p_1, \dots, p_k$ irreducibles no asociados. Para cada $i = 1, \dots, k$ sea $\gamma_i = \max(\alpha_i, \beta_i)$ y sea $m = p_1^{\gamma_1} \dots p_k^{\gamma_k}$. Claramente $a \mid m$ y $b \mid m$ con lo que $(m) \cap (a) \cap (b)$. Por otro lado si x es un elemento de $(a) \cap (b)$ distinto de 0 entonces m divide a $p_i^{\gamma_i}$ para todo i pues divide a a o a b y ambos dividen a x. Por tanto $m \mid x$, con lo que $x \in (m)$. Esto demuestra que $(a) \cap (b) = (m)$.

Sea D un dominio de factorización en el que el ideal generado por cada dos elementos es principal. Demostrar que D es un DFU.

Como D es DF, basta demostrar que todo irreducible p de D es primo. Sean $a, b \in D$ tales que $p \mid ab$ y $p \nmid a$. Por hipótesis $(a, p) = (c)$ para algún $c \in D$. Entonces $p \in (c)$ o sea $c \mid p$ pero a y c no son asociados porque $a \in (c) \setminus (p)$. Por tanto c es unidad. Es decir $(a, p) = D$ con lo que $1 = ax + py$ con $x, y \in D$. Entonces $b = abx + pby$ es múltiplo de p.

Sea D un DFU en el que el ideal generado por cada dos elementos es principal. Demostrar que D es un DIP.

Para cada $a \in D \setminus 0$ sea $\varphi(a)$ el número de irreducibles es una factorización de a. Sea I un ideal no nulo de D y sea a un elemento de I con $\varphi(a)$ mínimo. Vamos a ver que $I = (a)$. Claramente $(a) \subseteq I$. Sea $x \in I$. Por hipótesis $(a, x) = (b)$ con $b \in I$. Por tanto $a \mid b$, lo que implica que $\varphi(b) \leq \varphi(a)$. Por la minimalidad de $\varphi(a)$ tenemos que $\varphi(b) = \varphi(a)$ lo que implica que a y b son asociados. Luego $x \in (b) = (a)$, es decir $x \in (a)$. Luego $I = (a)$, como queríamos.

Grupos

(3) (2 puntos)

Calcular todos los grupos abelianos de orden p^2q^3 salvo isomorfismos con p y q dos primos distintos.

Calcular todos los grupos abelianos de orden p^4qr salvo isomorfismos con p, q y r tres primos distintos.

Por el Teorema de Estructura de Grupos Abelianos Finitos todo grupo abeliano de orden p^2 es la suma directa de uno de orden p^2 y unos de orden q^3. Los divisores elementales del primero serán $[p^2]$ o $[p,p]$ y los del segundo serán $[q^3]$, $[q^2,q]$ ó $[q,q,q]$. Combinando las dos primeras opciones con las tres segunda obtenemos que todo grupo abeliano de orden p^2q^3 es isomorfo a exactamente uno de los siguientes grupos:

$$\begin{aligned}
C_{p^2} \times C_{q^3} &\cong C_{p^2q^3} \\
C_{p^2} \times C_{q^2} \times C_q &\cong C_{p^2q^2} \times C_q \\
C_{p^2} \times C_q \times C_q \times C_q &\cong C_{p^2q} \times C_q \times C_q \\
C_p \times C_p \times C_{q^3} &\cong C_{pq^3} \times C_p \\
C_p \times C_p \times C_{q^2} \times C_q &\cong C_{pq^2} \times C_{pq} \\
C_p \times C_p \times C_q \times C_q \times C_q &\cong C_{pq} \times C_{pq} \times C_q.
\end{aligned}$$

De forma similar todo grupo de orden p^4 es isomorfo a C_{p^4}, $C_{p^3} \times C_p$, $C_{p^2} \times C_{p^2}$, $C_{p^2} \times C_p \times C_p$ ó $C_{p^2} \times C_p \times C_p$. Como todo grupo de orden q es isomorfo a C_q tenemos que cada grupo de orden p^4qr es isomorfo a exactamente uno de los siguientes:

$$\begin{aligned}
C_{p^4} \times C_q \times C_r &\cong C_{p^4qr} \\
C_{p^3} \times C_p \times C_q \times C_r &\cong C_{p^3qr} \times C_p \\
C_{p^2} \times C_{p^2} \times C_q \times C_r &\cong C_{p^2qr} \times C_{p^2} \\
C_{p^2} \times C_p \times C_p \times C_q \times C_r &\cong C_{p^2qr} \times C_p \times C_p \\
C_p \times C_p \times C_p \times C_p \times C_q \times C_r &\cong C_{pqr} \times C_p \times C_p \times C_p
\end{aligned}$$

Encontrar dos subgrupos H y K del grupo diédrico D_4 tales que $HK = \{hk : h \in H, k \in K\}$ no sea un subgrupo de D_4.

Tenemos $D_4 = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$ con $a^4 = b^2 = 1$, $ba = a^{-1}b$. Entonces $H = \langle b \rangle = \{1, b\}$ y $K = \langle ab \rangle = \{1, ab\}$ y $HK = \{1, b, ab, bab = a^{-1}\}$ no es un subgrupo porque contiene a a^{-1} pero no contiene a a.

Sean p un número primo, k y n números naturales y A un p-grupo abeliano de orden p^{n+1}. Sea $B = \{a^p : a \in A\}$. Demostrar que B es cíclico de orden p^k si y solo si $A \cong C_{p^{k+1}} \times C_p^{n-k}$.

Sea $A = \langle a_1 \rangle_{p^{\alpha_1}} \oplus \cdots \oplus \langle a_r \rangle_{p^{\alpha_r}}$ una descomposición primaria de A. Entonces $B = \langle a_1^p \rangle_{p^{\alpha_1 - 1}} \oplus \cdots \oplus \langle a_r^p \rangle_{p^{\alpha_r - 1}}$. Luego B es cíclico de orden k si y solo si $\alpha_1 = k+1$ y $\alpha_2 = \cdots = \alpha_r = 1$ (lo que implicará que $n+1 = k+1+r-1$, o sea $r = n-k+1$) lo que es equivalente a que A es isomorfo a $C_{p^{k+1}} \times C_p^{n-k}$.

(4) (1.5 puntos)

Sea G un grupo y sea H la diagonal de $G \times G$, o sea $H = \{(g,g) : g \in G\}$. Demostrar que H es un subgrupo de $G \times G$ y que H es normal en $G \times G$ si y solo si G es abeliano.

Claramente $(1,1) \in H$, y si $x, y \in H$ entonces $x = (g,g)$ e $y = (h,h)$ para ciertos $g, h \in G$. Entonces $xy^{-1} = (g,g)(h,h)^{-1} = (gh^{-1}, gh^{-1}) \in H$. Esto demuestra que H es subgrupo de $G \times G$. Si G es abeliano, entonces $G \times G$ también lo es y por tanto H es normal en $G \times G$. En caso contrario existen $g, h \in G$ tales que $gh \neq hg$, o lo que es lo mismo $g^{-1}hg \neq h$. En tal caso $(h,h) \in H$ pero $(g,1)^{-1}(h,h)(g,1) = (g^{-1}hg, h) \notin H$, con lo que H no es normal en $G \times G$.

Sea A un grupo abeliano finito y sea a un elemento de A de orden máximo. Demostrar que $\langle a \rangle$ es un sumando directo de A.

Sea $(d_1, \dots, d_k)$ la lista de factores invariantes de A. Entonces $|a| = d_1$ y $A = A_1 \oplus A_2 \oplus \cdots \oplus A_k$ con A_i cíclico de orden d_i. Si $a = a_1 + \cdots + a_k$ entonces $|d_1| = \text{mcm}(|a_1|, \dots, |a_k|)$ y cada $|a_i|$ divide a d_i que a su vez divide a d_1. Eso implica que $|d_1| = |a_i|$ para algún i. Eso implica que $|d_1| = |d_i|$ y podemos suponer sin pérdida de generalidad que $i = 1$. Sea $B = A_2 \oplus \cdots \oplus A_k$.

Si $x \in \langle a \rangle \cap B$ entonces $x = na = b_2 + \cdots + b_k$ con $b_i \in A_i$ para todo $i = 2, \dots, k$ y $n \in \mathbb{Z}$. Entonces $na_1 = (b_2 - na_2) + \cdots + (b_k - na_k) \in \langle a_1 \rangle \cap B = \{0\}$. Por tanto $na_1 = 0$, lo que implica que $d_1 = |a_1| = |a| \mid n$ y por tanto $x = na = 0$. Esto demuestra que $\langle a \rangle \cap B = \{0\}$ y por tanto $|\langle a \rangle + B| = |\langle a \rangle| \cdot |B| = |A|$, lo que implica que $B = \langle a \rangle \oplus B$. Luego $\langle a \rangle$ es un sumando directo de A.

Dar un ejemplo de un grupo G y de un número natural n para el que $G^n = \{g^n : g \in G\}$ no sea subgrupo de G. Demostrar que si G^n es subgrupo de G entonces es normal en G.

$S_3^3 = \{1, (1\ 2), (1\ 3), (2\ 3)\}$ que no es un subgrupo de S_3. Si $x \in G^n$ y $g \in G$ entonces $x = h^n$ para algún $h \in G$ y $x^g = (h^g)^n \in G^n$. Por tanto, si G es subgrupo entonces es normal en G.

Demostrar que si K es un subgrupo normal de G de índice primo p y H es un subgrupo de G no contenido en K entonces $HK = G$ y $[H : H \cap K] = p$.

Como H no está contenido en K, HK contiene propiamente a K y como K es normal en G, por el Tercer Teorema de Isomorfía HK es un subgrupo de G y $1 \neq HK/K \cong$

$H/H \cap K$. Entonces $|HK/K$ es un divisor de $|G/K| = p$, distinto de 1, con lo que $HK = G$ y $[H : H \cap K] = [G : K] = p$.