ESTRUCTURAS ALGEBRAICAS (5-10-2015)	Grado en Matemáticas Curso 2015-2016	Hoja A2

1. (Clases laterales) Calcula las clases a la derecha y a la izquierda del subgrupo H de G en los siguientes casos:

a) $G = \mathbb{Z}$ y $H = 4\mathbb{Z}$.

b) $G = S_3$ y $H = \langle (123) \rangle$.

c) $G = S_4$ y H el subgrupo de S_4 cuyos elementos fijan a 4.

d) $G = \mathbb{Z}_{30}^{\times}$ y $H = \langle \overline{11} \rangle$.

2. (Clases laterales) Sea $\mathbb{C}^*$ el grupo de los complejos no nulos con el producto, y sea $H = S^1$. Da una descripción geométrica de las clases de equivalencia a izquierda de H en $\mathbb{C}^*$.

3. (Cíclicos) Sea G un grupo cíclico de orden 18. Encuentra el número de elementos que generan el grupo.

4. (Lagrange) Un grupo G tiene dos subgrupos distintos H y K de orden 31. Demuestra que $H \cap K = \{1\}$.

5. (Clases laterales) Supongamos que $|G| = 33$. Demuestra que G contiene un elemento de orden 3.

6. (Lagrange) Supongamos que $|G| = 8$. Demuestra que G contiene un elemento de orden 2.

7. (Lagrange) Sea G un grupo de orden 8. Probar que G es cíclico o $a^4 = 1$ para cualquier $a \in G$.

8. (Abelianos) Supongamos que G es un grupo abeliano de orden impar. Demuestra que el producto de todos los elementos de G da como resultado la identidad.

9. (Cíclicos) **Subgrupos de $\mathbb{Z}$.**

a) Demuestra que todo subgrupo de $\mathbb{Z}$ es cíclico, de la forma $k\mathbb{Z}$ para algún entero k.

b) Demuestra que hay tantos subgrupos en $\mathbb{Z}$ como enteros no negativos.

c) Dados dos enteros positivos r, s, demuestra que $r\mathbb{Z} \subset s\mathbb{Z}$ si y sólo si r es un múltiplo de s.

d) Halla todos los subgrupos de $\mathbb{Z}$ que contienen a $6\mathbb{Z}$.

10. (Normales) Sea Q_8 el grupo de cuaterniones. Demuestra que todo subgrupo H de Q_8 es normal. Estudia los distintos grupos Q_8/H.

11. (Normales) Sea G un grupo y sean $H < G$ y $K \lhd G$. Demuestra que $HK = KH$ y que $HK < G$.

12. (Normales) Encuentra todos los subgrupos normales de S_3 y de D_4.

13. (Cíclicos) **Subgrupos de C_n.**

a) Halla todos los subgrupos de C_6.

b) Demuestra que todo subgrupo de C_n es cíclico.

c) Indica cuántos subgrupos tiene C_{100}.

14. (Teorema de Isomorfía) Si G es finito de orden 17, el único homomorfismo de G en el grupo de permutaciones S_6 es el trivial, y el único homomorfismo de S_6 en G es el trivial.

15. (Normales) Sea $G = \mathrm{GL}(2, \mathbb{Q})$ y $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| n \in \mathbb{Z} \right\}$. Demostrar que $H < G$, pero $H \ntriangleleft G$.

16. (Lagrange) Sea G un grupo de orden par. Demostrar que existe $g \in G$ de orden 2. *Sugerencia: empareja cada elemento distinto del neutro con su inverso.*

17. (Lagrange) Sea $n \in \mathbb{N}$ y $n = n_1 + \ldots + n_r$, $n_j \in \mathbb{N}$. Demostrar que $n!$ es divisible por $\prod_{i=1}^{r} n_i!$.

18. (Normales) Sea G un grupo y $H \lhd G$ de índice n (es decir $|G/H| = n$). Demostrar que si $g \in G$, entonces $g^n \in H$. Dar un ejemplo en el que esto sea falso si $H \ntrianglelefteq G$.

19. (p-grupos) Sea G un grupo. Se define el exponente de G como el menor $n \in \mathbb{N}$, $n \neq 0$, tal que $g^n = e$ para todo $g \in G$. Demostrar:

a) Todo grupo de exponente 2 es conmutativo.

b) Para todo primo impar p, se define el grupo de Heisenberg H_p como

$$H_p = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a, b, c \in \mathbb{Z}_p \right\}.$$

Demostrar que H_p tiene exponente p, pero no es conmutativo.

20. (p-grupos) Usa el problema anterior para demostrar que los órdenes de los elementos de H_p coinciden con los órdenes de los elementos de $\mathbb{Z}_p^3$ pero que aún así dichos grupos no son isomorfos.

21. (Clases laterales) Sea G un grupo y $H, H' \leq G$. Se dice que H y H' son conmensurables si

$$[H : H \cap H'] < \infty \qquad \text{y} \qquad [H' : H \cap H'] < \infty.$$

Demostrar que la conmensurabilidad es una relación de equivalencia en el conjunto de subgrupos de G.

22. (Clases de conjugación) Comprueba que las siguientes matrices son elementos conjugados en $\mathrm{GL}(3, \mathbb{C})$:

$$A = \begin{pmatrix} -20 & -178 & -103 \\ -3 & -29 & -17 \\ 9 & 84 & 49 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2\pi i}{3}} & 0 \\ 0 & 0 & e^{\frac{4\pi i}{3}} \end{pmatrix}$$

Usa ese hecho para calcular el orden de A. *Sugerencia: para ver que son conjugados puedes comprobar que tienen los mismos autovalores.*

23. (Clases de conjugación) Diagonaliza la matriz de $\mathrm{GL}(2, \mathbb{Z}_{17})$

$$A = \begin{pmatrix} \overline{9} & \overline{2} \\ \overline{6} & \overline{11} \end{pmatrix},$$

es decir, encuentra una matriz diagonal que sea conjugada a A en $\mathrm{GL}(2, \mathbb{Z}_{17})$. ¿Cuál es el orden de A?

24. (Lagrange) Sea $G = \mathrm{GL}(2, \mathbb{Z}_p)$.

a) Demuestra que el subconjunto de matrices triangulares superiores es un subgrupo de G.

b) ¿Podemos deducir del apartado anterior que $p(p-1)^2$ divide a $|G|$?

25. (Normales) Sea $G = \mathrm{GL}(2, \mathbb{Z}_p)$.

a) Una aplicación lineal es biyectiva si y sólo si los vectores columna de su matriz son linealmente independientes (ya que son las imágenes de los vectores de la base estándar). Usa dicho hecho para demostrar que $|G| = (p^2 - 1)(p^2 - p)$.

b) Calcula el tamaño de $G/\mathrm{SL}(2, \mathbb{Z}_p)$ y úsalo, junto con el apartado anterior, para determinar el tamaño de $\mathrm{SL}(2, \mathbb{Z}_p)$.

c) Demuestra que $\mathrm{SL}(2, \mathbb{Z}_p)$ es normal en G. ¿A qué grupo conocido es isomorfo $G/\mathrm{SL}(2, \mathbb{Z}_p)$?

26. (Normales) Encuentra los subgrupos normales no triviales del subgrupo de S_4 generado por (12) y $(13)(24)$, y calcula las tablas de los grupos cocientes correspondientes. ¿A qué grupos que conocemos son isomorfos dichos cocientes?

27. (Normales) Calcula todos los posibles homomorfismos de D_4 en $\mathbb{Z}_{17}^{\times}$, y para cada uno anota el subgrupo normal de D_4 correspondiente al núcleo. ¿Existe algún encaje de $\mathbb{Z}_8^{\times}$ en $\mathbb{Z}_{17}^{\times}$?

28. (Resolubles) Sea p primo y $d \geq 1$. Considera el subgrupo T de $\mathrm{GL}(3, \mathbb{Z}_p)$ de matrices triangulares superiores y el subgrupo de $N \leq T$ de matrices con $\overline{1}$s en la diagonal.

a) Demuestra que N es normal en T y que T/N es isomorfo al subgrupo $D \leq \mathrm{GL}(3, \mathbb{Z}_p)$ de matrices diagonales.

b) Encuentra un subgrupo normal de N buscando un homomorfismo $f : N \to \mathbb{Z}_p^2$ y usando el teorema de isomorfía. *Sugerencia: para encontrar f, multiplica dos elementos generales de N y observa que componentes se parecen a la suma en $\mathbb{Z}_p^2$.*

c) Usa la información de los apartados anteriores para demostrar que N y T son grupos resolubles.

d) Prueba que podemos conseguir la parametrización

$$N = \{a^i b^j c^k : i, j, k \leq p, a^p = b^p = c^p = 1, ba = abc^{-1}, ca = ac, cb = bc\}$$

para ciertos $a, b, c \in N$. Usa esas reglas de multiplicación para calcular i, j, k en $(a^2b^3c^4)(a^3bc^2) = a^i b^j c^k$.

29. (Lagrange) Demuestra el Teorema de Euler para residuos módulo n: todo elemento $a \in \mathbb{Z}_n^{\times}$ satisface la ecuación $a^{\phi(n)} = \overline{1}$, con $\phi(n) = |\mathbb{Z}_n^{\times}|$. ¿Cuál es el resto de $2^{50}7^{20}$ módulo 15?

30. (Normales) Sea G un grupo de tamaño 28 con un subgrupo normal N de tamaño 7. Demuestra que en G existe algún elemento de orden 14.

31. (Resolubles) Sea $G = \langle (2354), (12345) \rangle \leq S_5$.

a) Demuestra que $N = \langle (12345) \rangle$ es normal en G y que $|G/N| = 4$. Deduce el tamaño de G.

b) Usa el apartado anterior para mostrar que $G = \{a^i b^j : i \leq 4, j \leq 5\}$ con $a = (2354)$ y $b = (12345)$, con $a^{-1}ba = b^3$. Usa dicha identidad para calcular i, j en $a^2b^3a^3b^4 = a^i b^j$.

32. (Clases de conjugación) Sea S el subgrupo de $\mathrm{SL}(2, \mathbb{Z}_5)$ de matrices triangulares superiores.

a) Demuestra que $|S| = 20$. Por teoría sabemos que el número de conjugados de un elemento del grupo tiene que dividir al orden del grupo. ¿Qué posibilidades hay a priori para los cardinales de las clases de conjugación de S?

b) Calcula el centralizador de cada elemento g de S. Usa dichos centralizadores para calcular los tamaños de clases de conjugación de S, y observa que

$$20 = 5 + 5 + 2 + 2 + 2 + 2 + 1 + 1$$

es la ecuación de clases de este grupo. Calcula de forma explícita los elementos de cada clase.

33. (Teorema de Isomorfía) Podemos extender la definición de $\mathrm{GL}(d, \mathbb{Z}_p)$, p primo al caso en que el módulo sea cualquier número natural n mediante la definición

$$\mathrm{GL}(d, \mathbb{Z}_n) = \{A \in M_d(\mathbb{Z}_n) : \det A \in \mathbb{Z}_n^{\times}\},$$

sólo que ahora sus elementos no podemos verlos como aplicaciones lineales de un espacio vectorial.

a) Comprueba que es un grupo.
Sugerencia: ten en cuenta que la formula $A^{-1} = (\det A)^{-1}(Adj A)^t$ sabemos que se satisface si la matriz A tiene coeficientes en $\mathbb{Z} \subset \mathbb{R}$, y que $Adj A$ también tendría coeficientes en $\mathbb{Z}$.

b) Consideramos la aplicación $f : \mathrm{GL}(2, \mathbb{Z}_{p^\alpha}) \to \mathrm{GL}(2, \mathbb{Z}_p)$ definida por $A \mapsto \tilde{A}$, con $\tilde{A}$ la matriz que se obtiene al reducir los coeficientes de A módulo p. Demuestra que está bien definida y que es un homomorfismo sobreyectivo.

c) Deduce que $|\mathrm{GL}(2,\mathbb{Z}_{p^\alpha})| = (p^{\alpha-1})^4|\mathrm{GL}(2,\mathbb{Z}_p)|$, luego por un problema anterior $|\mathrm{GL}(2,\mathbb{Z}_{p^\alpha})| = p^{4\alpha-4}(p^2-1)(p^2-p)$.

d) Podemos igualmente definir $\mathrm{SL}(d,\mathbb{Z}_n) \le \mathrm{GL}(d,\mathbb{Z}_n)$ como $\mathrm{SL}(d,\mathbb{Z}_n) = \{A \in M_d(\mathbb{Z}_n) : \det A = \overline{1}\}$. Demuestra que $|\mathrm{SL}(2,\mathbb{Z}_{p^\alpha})| = p^{3\alpha-3}(p+1)(p^2-p)$.

34. (Resolubles) Consideramos $V_4 \subset S_4$ el subconjunto formado por la identidad y los dos por dos ciclos.

a) Demuestra que V_4 es un subgrupo de S_4 de tamaño 4.

b) Demuestra que si $f \in S_4$ y $(a,b)(c,d) \in V_4$, se cumple la fórmula $f(a,b)(c,d)f^{-1} = (f(a),f(b))(f(c),f(d))$.

c) Usa el apartado anterior para demostrar que V_4 es normal en S_4.

d) Demuestra que $V_4 \cong D_2$ y que $S_4/V_4 \cong D_3$.

e) Concluye que S_4 es resoluble, y deduce la parametrización $S_4 = \{a^i b^j u^k v^l : i \le 2, j \le 3, k, l \le 2\}$ para ciertos $a,b,u,v \in S_4$.

35. (Simples) Considera el grupo $G = \mathrm{SL}(2,K)$ con K igual a $\mathbb{C},\mathbb{R}$ o $\mathbb{Z}_p$, con $p \ge 5$ primo. Se cumple que en G dos matrices distintas de $\pm I$ son conjugadas si y sólo si sus trazas son iguales, y por tanto las clases de conjugación son $\{I\}$, $\{-I\}$ y $C(t)$ $t \in K$, con $C(t)$ el conjunto de matrices de traza t distintas de $\pm I$ (en el caso $K = \mathbb{C}$ esto se puede ver trivialmente usando la forma de Jordan; en los otros casos se puede demostrar directamente).
Asumiendo dicho resultado, vamos a usar que un subgrupo normal es unión de clases de conjugación para demostrar que el único subgrupo no trivial de G es $\{I,-I\}$.

a) Muestra que si $H \le G$ y $H \supset C(t)$ para algún t, entonces $H \supset C(2+2^{-1})$ usando la identidad

$$\begin{pmatrix} t & 2 \\ -2^{-1} & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & t \end{pmatrix} = \begin{pmatrix} 2 & t \\ 0 & 2^{-1} \end{pmatrix} \ne \pm I.$$

b) Muestra que si $H \le G$ y $H \supset C(2+2^{-1})$ entonces $H \supset C(2)$ usando la identidad

$$\begin{pmatrix} 2^{-1} & 1 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 0 & 2^{-1} \end{pmatrix} = u(1) \qquad \text{con} \quad u(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.$$

c) Muestra que si $g \in G$ no es una matriz triangular inferior entonces podemos encontrar $x, y \in K$ tales que $u(x)^t g u(y)^t$ es igual a $u(z)$ para algún z.

d) Usa el apartado anterior para mostrar que $\langle C(2) \rangle = G$. *Sugerencia: si $g \in G$ es triangular inferior $gu(1)$ no lo es.*

e) Concluye que el único subgrupo normal no trivial de G es $\langle -I \rangle$, y que por tanto $\mathrm{PSL}(2,K) := \mathrm{SL}(2,K)/\langle -I \rangle$ es un grupo simple.

36. (Lagrange) Sea G un grupo de orden n. Demuestra que G puede generarse con $\Omega(n)$ generadores, con $\Omega(n)$ el número de divisores primos de n contados con multiplicidad.

37. (Abelianos) Sea G un grupo abeliano finito tal que la ecuación $x^n = e$ tiene como mucho n soluciones en G para cada n. Demuestra que G es cíclico. *Sugerencia: Si G no fuera cíclico, entonces tendría un subgrupo $H = \langle x,y \rangle$ no cíclico, y $h^{|H|} = 1$ para todo $h \in H$.*

38. (Abelianos) Sea G un grupo tal que $x^2 = e$ para todo x. Demuestra que G es abeliano.

39. (Abelianos) Un grupo G es abeliano si y sólo si la función $f : G \longrightarrow G$ dada por $f(x) = x^{-1}$ es un homomorfismo.

40. (Simples) Sean G, G' grupos tal que G es simple. Demuestra que si existe un homomorfismo $f : G \longrightarrow G'$ no trivial, entonces f es inyectivo.