ALGEBRA II - Práctica N°1 - Primer cuatrimestre de 2003

Grupos, subgrupos y morfismos.

Ejercicio 1. Dado $n \in \mathbb{N}$, sea $G_n = \{z \in \mathbb{C} \,/\, z^n = 1\}$.

i) Probar que $(G_n\,, \cdot)$ es un grupo abeliano y hallar z^{-1} para cada $z \in G_n$.

ii) Probar que G_n es cíclico, es decir, que existe $w \in G_n$ que satisface

$$\forall\, z \in G_n\, \exists\, k \in \mathbb{Z} \text{ tal que } z = w^k.$$

iii) Probar que

a) $G_n \subseteq G_m$ si y sólo si $n|m$.

b) $G_n \cap G_m = G_{(n:m)}$.

c) $\{w.z \,/\, w \in G_n \text{ y } z \in G_m\} = G_{[n:m]}$.

Ejercicio 2. Sea $S^1 = \{z \in \mathbb{C} \,/\, |z| = 1\}$. Probar que $(S^1, \cdot)$ es un grupo abeliano y hallar z^{-1} para cada $z \in S^1$. ¿Es S^1 cíclico?

Ejercicio 3. Sea $G = \mathbb{Z}_n = \{a \in \mathbb{Z} \;/\; 0 \leq a < n\}$ $\qquad a +_n b = r_n(a + b)$.
Probar que Z_n es un grupo abeliano. ¿Es $\mathbb{Z}_n$ cíclico?

Ejercicio 4. En cada uno de los siguientes casos determinar si $(G, *)$ es un grupo y, en caso afirmativo, determinar si es abeliano:

i) $G = \mathbb{N}_0 \qquad a * b = [a : b]$ si $a \neq 0$ ó $b \neq 0$ y $0 * 0 = 0$

ii) $G = \mathbb{Q}_{>0} \qquad a * b = a.b$

iii) $G = \mathbb{Z}^{3\times 3} \qquad a * b = a.b$

iv) $G = \mathbb{R}^{n\times n} \qquad a * b = a + b$

v) $G = SL(n, \mathbb{R}) = \{a \in \mathbb{R}^{n\times n} \,/\, \det\ a = 1\} \qquad a * b = a.b$

vi) $G = End_K(V)$, con V un K-espacio vectorial $\qquad f * g = f \circ g$

vii) $G = \{f \in End_{\mathbb{R}}(\mathbb{R}^n) \,/\, d(f(x), f(y)) = d(x, y)\ \forall\, x, y \in \mathbb{R}^n\} \qquad f * g = f \circ g$

viii) $G = S(X) = \{f : X \longrightarrow X \,/\, f \text{ es biyectiva}\}$, donde X es un conjunto no vacío $f * g = f \circ g$

Notación: Cuando $X = \{1, \ldots, n\}$, $S(X)$ será notado S_n.

ix) $G = S(\mathbb{Z}) \qquad f * g = f \circ g^{-1}$

x) $G = \mathcal{U}_n = \{a \in \mathbb{Z}_n \,/\, (a : n) = 1\} \qquad a * b = r_n(a.b)$

xi) $G = \mathbb{Z} \times \mathbb{Z}^- = \{\, (a,b) \,/\, a,b \in \mathbb{Z} \,\}$ $\qquad (a,b) * (c,d) = (a + (-1)^b c\,,\, b+d)$

xii) $G = G_\infty = \displaystyle\bigcup_{n \in \mathbb{N}} G_n \qquad * = \cdot$

xiii) $G = H_1 \times H_2 \qquad (x,y) * (z,w) = (x \circ z, y \triangle w)$ donde $\{H_1, \circ\}$ y $\{H_2, \triangle\}$ son grupos.

Ejercicio 5. Probar que todos los grupos de 4 elementos son abelianos. (Sugerencia: considerar las posibles tablas de multiplicación).

Ejercicio 6. Sea G un grupo tal que todo elemento $x \in G$ cumple $x^2 = 1$. Probar que G es abeliano.

Ejercicio 7.

i) Sea $G = \{g_1, g_2, \ldots, g_n\}$ un grupo abeliano finito. Probar que

$$\sum_{i=1}^{n} g_i = \sum_{g \in G \ / \ 2g = 0} g.$$

ii) Calcular $\displaystyle\sum_{a \in \mathbb{Z}_n} a$.

iii) Calcular $\displaystyle\prod_{w \in G_n} w$.

iv) Sea $p \in \mathbb{N}$ un número primo. Probar el Teorema de Wilson:

$$(p-1)! \equiv -1 \pmod{p}$$

(Sugerencia: considerar el grupo $G = \mathcal{U}_p$ definido en el ejercicio 4, ítem x).)

Ejercicio 8. Sea $(G, \cdot)$ un grupo y sea S un subconjunto no vacío de G. Probar que

i) S es un subgrupo de G si y sólo si $x.y^{-1} \in S \ \forall\, x, y \in S$.

ii) Si G es finito entonces S es un subgrupo de G si y sólo si $x.y \in S \ \forall\, x, y \in S$.

Ejercicio 9. Sea G un grupo y sean H_1, H_2 y H_3 subgrupos de G.

i) Probar que $H_1 \cap H_2$ es un subgrupo de G.

ii) Probar que $H_1 \cup H_2$ es un subgrupo de G si y sólo si $H_1 \subset H_2$ ó $H_2 \subset H_1$.

iii) ¿Es cierto que si $H_1 \cup H_2 \cup H_3$ es un subgrupo de G, entonces $\exists\, i, j$ con $i \neq j$ tal que $H_i \subset H_j$?

Ejercicio 10. Probar que H es un subgrupo de $(G, *)$ en cada uno de los siguientes casos:

i) $G = \mathbb{C}^*$ $\quad * = \cdot$ $\quad H = S^1$

ii) $G = D_4$ $\quad H = \{1, \rho, \rho^2, \rho^3\}$

iii) $G = GL(2, \mathbb{C})$ $\quad * = \cdot$ $\quad H = \mathcal{H}$
donde $\mathcal{H} = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$

iv) $G = S^1$ $\quad * = \cdot$ $\quad H = G_n$

v) $G = \mathbb{Z}_{2n}$ $\quad a * b = r_{2n}(a + b)$ $\quad H = \{a \in G \,/\, a \text{ es par}\}$

vi) $G = GL(n, \mathbb{R})$ $\quad * = \cdot$ $\quad H = SL(n, \mathbb{R})$

vii) $g = S_7$ $\quad * = \circ$ $\quad H = \{\, id, (1\ 2\ 3\ 4), (1\ 3)(2\ 4), (1\ 4\ 3\ 2) \,\}$

viii) $G = D_6$ $\quad H = \{\, 1, \sigma, \rho^3, \sigma * \rho^3 \,\}$

ix) $G = \mathbb{Q}$ $\quad * = +$ $\quad H = \{\, \frac{m}{n} \in \mathbb{Q} \,/\, (m, n) = 1 \text{ y } n = 2^i.5^j \text{ con } i, j \in \mathbb{N}_0 \,\}$

x) $G = \mathbb{Q}$ $\quad * = +$ $\quad H = \{\, \frac{m}{n} \in \mathbb{Q} \,/\, (m, n) = 1 \text{ y } n \text{ es libre de cuadrados} \,\}$

xi) $G = \mathbb{Z} \times \mathbb{Z}^-$ $\quad *$ como en 4. xi) $\quad H = \{\, (a, b) \in \mathbb{Z} \times \mathbb{Z}^- \,/\, a \equiv b \pmod 2 \,\}$

Ejercicio 11. Sea $G = \mathbb{Z}_2^{2\times 2}$. Calcular $|G|$ y hallar subgrupos de G de orden 2, 4 y 8.

Ejercicio 12. Calcular todos los subgrupos de $\mathcal{H}$, de D_4 y de $\mathcal{U}_{12}$.

Ejercicio 13.

i) Probar que si H es un subgrupo de $\mathbb{Z}$ entonces existe $n \in \mathbb{N}_0$ tal que $H = n.\mathbb{Z}$.

ii) Probar que si H es un subgrupo finito de $\mathbb{C}^*$ entonces existe $n \in \mathbb{N}$ tal que $H = G_n$.

iii) Probar que H es un subgrupo de G_n si y sólo si $H = G_d$ para algún d tal que $d \mid n$.

Ejercicio 14. Hallar $\mathcal{C}(G)$ (el **centro** de G) en cada uno de los siguientes casos:

i) $G = D_n$

ii) $G = S_4$

iii) $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \,/\, a, b, c \in \mathbb{Z}_3 \right\}$

iv) $G = \mathcal{H}$

v) $GL(n, \mathbb{R})$

vi) $SL(n, \mathbb{R})$

vii) $\mathbb{Z} \times \mathbb{Z}^-$

Ejercicio 15.

i) Encontrar sistemas de generadores de los siguientes grupos:

a) $\mathbb{C}^*$ b)$\mathbb{Z}$ c) D_n

d) $\mathbb{Z}_n$ e) $\mathcal{U}_{12}$ f) $\mathbb{Q}^*$

g) $\mathbb{Q}_{>0}$ h) $\mathbb{Z} \oplus \mathbb{Z}$ j) $\mathbb{Z} \times \mathbb{Z}^-$

¿Cuáles son finitamente generados? ¿Cuáles son cíclicos?

ii) Sean $a, b \in \mathbb{Z}$. Probar que $\{a, b\}$ es un sistema de generadores de $\mathbb{Z}$ si y sólo si $(a : b) = 1$.

iii) Probar que $\mathbb{Z}$ tiene sistemas de generadores minimales de n elementos $\forall n \in \mathbb{N}$.

iv) Probar que

a) $\left\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\right\}$ es un sistema de generadores de $GL(2, \mathbb{Z})$.

b) $\left\{\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)\right\}$ es un sistema de generadores de $SL(2, \mathbb{Z})$.

v) Probar que todo subgrupo finitamente generado de $\mathbb{Q}$ es cíclico.

vi) Probar que, si $n \geq 3$, los triciclos generan A_n.

Ejercicio 16. Sea G un grupo y S un subgrupo propio. Probar que $< G - S >= G$.

Ejercicio 17.

i) Hallar $[G, G]$ en cada uno de los siguientes casos:

a) $G = D_n$ b) $G = \mathcal{H}$

c) $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} / \, a, b, c \in \mathbb{Z}_2 \right\}$ d) $\mathbb{Z} \times \mathbb{Z}^-$

ii) Probar que $[S_n, S_n] = A_n$.

iii) Sea G un grupo libre en las letras X e Y. Probar que un elemento $w \in [G, G]$ si y sólo si las sumas de los respectivos exponentes de X y de Y en w dan cero.

Ejercicio 18. Hallar $ord(x)$ en los siguientes casos:

i) $G = S_8$ $x = (1\ 2)(5\ 6\ 7)$; $x = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8)$; $x = (1\ 2\ 3\ 5)(1\ 3\ 7\ 8)$

ii) $G = \mathbb{Z}_{12}$ $\quad x = 2$; $x = 3$; $x = 4$

iii) $G = \mathcal{H}$ $\quad x = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$

iv) $G = S^1$ $\quad x = cos\,\frac{2\pi}{n} + i\ sen\,\frac{2\pi}{n}$; $x = cos\,\frac{6\pi}{n} + i\ sen\,\frac{6\pi}{n}$; $x = cos\,\frac{5\pi}{n} + i\ sen\,\frac{5\pi}{n}$

v) $G = D_4$ $\quad x = \rho^2 * \sigma$; $x = \rho^3$

vi) G un grupo cualquiera y $x = a^d$, donde $a \in G$ es un elemento de orden n y d es un número natural.

vii) $G = \mathbb{Z}_n$ $\quad x \in \mathbb{Z}_n$ un elemento cualquiera.
Deducir que $x \in \mathbb{Z}_n$ es un generador de $\mathbb{Z}_n$ si y sólo si $(x : n) = 1$.

Ejercicio 19. Sea $G = \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & a \end{smallmatrix}\right) / \, a, b \in \mathbb{Z}_7, \text{ con } a \neq 0 \right\}$.

i) Hallar el orden de G.

ii) Para cada primo p que divide al orden de G hallar todos los elementos de G que tengan orden p.

Ejercicio 20.

i) Probar que si G_1 y G_2 son grupos tales que $g_1 \in G_1$ y $g_2 \in G_2$ tienen órdenes finitos, el orden de $(g_1, g_2) \in G_1 \times G_2$ es el mínimo común múltiplo entre los órdenes de g_1 y g_2.

ii) Sean $a, b \in G$ dos elementos que conmutan tales que $a^n = 1$ y $b^m = 1$. Probar que $(a.b)^{[n:m]} = 1$. Deducir que si dos elementos conmutan y tienen orden finito, entonces el producto tiene orden finito. ¿Es necesariamente el orden del producto el mínimo común múltiplo de los órdenes?

iii) Sean
$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$
en $GL(2, \mathbb{Q})$. Probar que A y B tienen orden finito pero $A.B$ tiene orden infinito.

Ejercicio 21. Sea p un número primo, $m \in \mathbb{N}$ y sea G un grupo de orden p^m. Probar que existe un elemento de orden p en G.

Ejercicio 22. Sea p un número primo mayor que 2. Se considera el conjunto de matrices
$$G = \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} \ / \ a, b, c \in \mathbb{Z}_p \right\}.$$

Probar que $(G, \cdot)$ es un grupo no abeliano tal que todo elemento distinto de I_3 tiene orden p. ¿Qué pasa cuando $p = 2$?

Ejercicio 23. Sea $(G, \cdot)$ un grupo y sean $a, b \in G$.

i) Probar que las siguientes aplicaciones de G en G son biyectivas y encontrar sus inversas:

a) $x \longrightarrow a.x$ b) $x \longrightarrow a.x.b$

c) $x \longrightarrow a.x.a^{-1}$ d) $x \longrightarrow x^{-1}$

e) $x \longrightarrow a.x^{-1}.a^{-1}$

ii) Determinar cuáles de las aplicaciones definidas en i) son morfismos.

iii) Idem ii) en el caso en que G sea abeliano.

Ejercicio 24. En cada uno de los siguientes casos, verificar que f es un morfismo de grupos, calcular $\mathrm{Nu}(f)$ e $\mathrm{Im}(f)$ y, si f es isomorfismo, calcular f^{-1}:

i) $f : \mathbb{R} \to S^1$, $f(x) = e^{ix}$.

ii) $f : \mathbb{Q} \to S^1$, $f(x) = e^{ix\pi}$.

iii) $f : \mathbb{R}^{n\times n} \to \mathbb{R}^{n\times n}$, $f(a) = a^t$.

iv) $f : GL(n, \mathbb{R}) \to GL(n, R)$, $f(a) = (a^{-1})^t$.

v) $f : \mathbb{R}^* \to \mathbb{R}^*$, $f(x) = x^2$.

vi) $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(x) = x^n$.

vii) $f : \mathbb{C}^* \to \mathbb{C}^*$, $f(x) = \left(\frac{x}{|x|}\right)^4$.

viii) $f : D_n \to D_n$, $f(\rho^i\sigma^j) = \rho^{j-i}\sigma^j$ $(0 \le i < n\ ; 0 \le j < 2)$.

Ejercicio 25. Dados los grupos:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \qquad \mathbb{Z}_2 \oplus \mathbb{Z}_4 \qquad \mathbb{Z}_2 \oplus G_4 \qquad \mathbb{Z}_8$$

$$D_4 \qquad G_8 \qquad \mathcal{H}$$

Decidir cuáles son abelianos, cuáles son cíclicos y cuáles son isomorfos entre sí.

Ejercicio 26. Determinar si G y K son isomorfos en cada uno de los siguientes casos:

i) $G = \mathbb{Z}_4 \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_2$

ii) $G = \mathbb{Z}_n \qquad K = G_n$

iii) $G = \mathbb{Z}_{10} \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_5$

iv) $G = \mathbb{Q} \qquad K = \mathbb{R}$

v) $G = \mathcal{U}_{16} \qquad K = \mathcal{H}$

vi) $G = \mathcal{U}_{16} \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_4$

vii) $G = S_3 \qquad K = D_3$

viii) $G = A_4 \qquad K = D_6$

ix) Si $(m, n) = 1$, $G = \mathbb{Z}_{n.m} \qquad K = \mathbb{Z}_n \oplus \mathbb{Z}_m$

Ejercicio 27. Sea $f : G \longrightarrow G'$ un morfismo de grupos. Probar que si $ord(x)$ es finito, $ord(f(x))$ divide a $ord(x)$.

Ejercicio 28. Sea $G = \left\{ \left(\begin{smallmatrix} 1 & b \\ 0 & a \end{smallmatrix} \right) / \, a, b \in \mathbb{Z}_4, \text{ con } (a, 4) = 1 \right\}$

Probar que G es un grupo no abeliano de orden 8. ¿Es $G \simeq \mathcal{H}$? ¿Es $G \simeq D_4$?

Ejercicio 29. Sea p un primo.

i) Calcular el orden de $GL(2, \mathbb{Z}_p)$.

ii) Probar que $SL(2, \mathbb{Z}_p)$ es un grupo no abeliano de orden $p(p^2 - 1)$

iii) Caracterizar $SL(2, \mathbb{Z}_p)$ en el caso $p = 2$.

Ejercicio 30.

i) Probar que son equivalentes:
   a) G es un grupo abeliano.
   b) La aplicación $f : G \longrightarrow G$ definida por $f(x) = x^{-1}$ es un morfismo de grupos.
   c) La aplicación $f : G \longrightarrow G$ definida por $f(x) = x^2$ es un morfismo de grupos.

ii) Sea G un grupo. Probar que si existe $n \in \mathbb{Z}$ tal que $f(x) = x^n$, $g(x) = x^{n+1}$ y $h(x) = x^{n+2}$ son morfismos, entonces G es abeliano.

Ejercicio 31.

i) Sea $f : G \longrightarrow L$ un epimorfismo de grupos. Decidir para cuáles de las siguientes propiedades P_i vale "G verifica $P_i \Rightarrow L$ verifica P_i":

(P_1) tener n elementos.
(P_2) ser finito.
(P_3) ser conmutativo.
(P_4) ser no conmutativo.
(P_5) ser cíclico.
(P_6) todo elemento tiene orden finito.
(P_7) todo elemento tiene orden infinito.
(P_8) ser finitamente generado.

ii) Idem i) con f monomorfismo.

Ejercicio 32. Probar que:

i) $Aut(\mathbb{Z}) \simeq G_2$

ii) $Hom(\mathbb{Z}\,,\,\mathbb{Z}_n) \neq 0 \qquad (n > 1)$

iii) $Hom(\mathbb{Z}_n\,,\,\mathbb{Z}_m) \simeq \mathbb{Z}_{(n:m)}$

iv) $Hom(\mathbb{Q}\,,\,\mathbb{Z}) = 0$

v) No existe un epimorfismo de $\mathbb{Z}$ en $\mathbb{Z} \oplus \mathbb{Z}$

Ejercicio 33. Caracterizar los siguientes grupos:

i) $Hom(G\,,\,\mathbb{Z})$ para G un grupo de orden finito.

ii) $Hom(\mathbb{R}^*, \mathbb{Q}^*)$

iii) $Hom(D_3, D_3)$

iv) $Aut(D_3)$

Ejercicio 34. Hallar dos grupos G y K no isomorfos tales que $Aut(G) \simeq Aut(K)$

Ejercicio 35. Sea p un primo y sea G un grupo abeliano tal que todo elemento de $G - \{0\}$ tiene orden p. Se define la acción $\cdot : \mathbb{Z}_p \times G \to G$ en la forma usual.

i) Probar que $(G, +, \cdot)$ es un $\mathbb{Z}_p$-espacio vectorial.

ii) Deducir que si G es un grupo abeliano finito tal que todo elemento de $G - \{0\}$ tiene orden p, entonces $G \simeq \mathbb{Z}_p^n$ para algún $n \in \mathbb{N}_0$.

Ejercicio 36. Se define la función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ de la siguiente forma:

$$\varphi(n) = \#\{h \in \mathbb{N} \ / \ 1 \leq h \leq n \text{ y } (h : n) = 1\} = |\mathcal{U}_n|.$$

i) Deducir que si $(a : n) = 1$, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$ (generalización del pequeño teorema de Fermat).

ii) Probar que si $n, m \in \mathbb{N}$, $(n : m) = 1$ entonces $\varphi(n.m) = \varphi(n).\varphi(m)$. (Sugerencia: probar que la función $f : \mathcal{U}_{n.m} \to \mathcal{U}_n \times \mathcal{U}_m$ dada por $f(x) = (r_n(x), r_m(x))$ está bien definida y es biyectiva.)

iii) Probar que si $p \in \mathbb{N}$ es un primo y $r \in \mathbb{N}$ entonces $\varphi(p^r) = (p-1).p^{r-1}$ (y por lo tanto, se puede calcular $\varphi(n)$ para cualquier n si se conoce su factorización en primos).

iv) Probar que si $n, m \in \mathbb{N}$, $(n : m) = 1$ entonces $\mathcal{U}_{n.m} \simeq \mathcal{U}_n \times \mathcal{U}_m$

v) Hallar todos los $n \in \mathbb{N}$ tales que $\mathcal{U}_n \simeq \mathbb{Z}_4$.

vi) Hallar todos los $n \in \mathbb{N}$ tales que $\mathcal{U}_n \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$.