Álgebra II
Segundo Cuatrimestre — 2006
Práctica 1

1. Sea $n \in \mathbb{N}$ y sea $G_n = \{z \in \mathbb{C} / z^n = 1\}$.

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

   b) Probar que G_n es cíclico, es decir, que existe $w \in G_n$ que satisface: $\forall\, z \in G_n\ \exists\, k \in \mathbb{Z}$ tal que $z = w^k$.

2. Sea $G = \mathbb{Z}_n = \{a \in \mathbb{Z}/0 \leq a < n\}$ con $a * b = r_n(a+b)$. Probar que $(\mathbb{Z}_n, *)$ es un grupo y determinar si es abeliano.

3. Sea $S^1 = \{z \in \mathbb{C}\ /\ |z| = 1\}$.

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

   b) Determinar si S^1 es cíclico.

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

   a) $G = \mathbb{N}_0 \qquad a * b = [a, b]$.

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

   c) $G = M_3(\mathbb{Z}) \qquad a * b = a \cdot b$.

   d) $G = M_n(\mathbb{R}) \qquad a * b = a + b$.

   e) $G = SL_n(\mathbb{R}) = \{a \in M_n(\mathbb{R})\ /\ det\ a = 1\} \qquad a * b = a \cdot b$.

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

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

   h) $G = S(X) = \{f : X \longrightarrow X\ /\ f$ es biyectiva$\}$, donde X es un conjunto no vacío y $f * g = f \circ g$.
   Notación: Cuando $X = \{1, \ldots, n\}$ $S(X)$ será notado S_n.

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

   j) $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \qquad (a, b) * (c, d) = (r_2(a+c), r_2(b+d))$.

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

5. Probar que

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

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

6. Probar que todos los grupos de 4 elementos son abelianos.
   (Sugerencia: hacer las posibles tablas de operaciones).

7. *a*) Sea $G = \{g_1, \ldots, g_n\}$ un grupo abeliano finito. Probar que

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

   b) Calcular $\sum\limits_{a \in \mathbb{Z}_n} a$.

   c) Calcular $\prod\limits_{w \in G_n} w$.

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

   $$(p-1)! \equiv -1(p)$$

8. Sea $(G, *)$ un grupo finito y sea $S \subset G$ un subconjunto no vacío. Probar que S es un subgrupo si y sólo si $x * y \in S, \forall x, y \in S$.

9. En cada uno de los siguientes casos, probar que H es un subgrupo de $(G, *)$:

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

   b) $G = D_4$ $\quad * = \circ \quad$ $H = \{1, \rho, \rho^2, \rho^3\}$.

   c) $G = GL_n(\mathbb{C})$ $\quad * = \cdot \quad$ $H = \mathcal{H}$ donde

   $$\mathcal{H} = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \right\}.$$

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

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

   f) $G = GL_n(\mathbb{R})$ $\quad * = \cdot \quad$ $H = SL_n(\mathbb{R})$.

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

10. Sea G un grupo y sean H_1 y H_2 dos subgrupos de G.

    a) Probar que $H_1 \cap H_2$ es un subgrupo.

    b) Probar que $H_1 \cup H_2$ es un subgrupo si y sólo si $H_1 \subset H_2$ o $H_2 \subset H_1$.

    c) ¿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 $H_i \subset H_j$?

11. Hallar todos los subgrupos cíclicos de: $\mathbb{Z}_2$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, G_3, G_4, S_3, $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ y $\mathbb{Z}_2 \oplus \mathbb{Z}_3$.

12. Sean G un grupo y $a \in G$. Probar que $Z_a = \{x \in G;\ x \cdot a = a \cdot x\}$ es un subgrupo de G.

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

14. Probar que si H es un subgrupo finito de $\mathbb{C}^*$ entonces existe $n \in \mathbb{N}_0$ tal que $H = G_n$.

15. Hallar $ord(x)$ en los casos:

    a) $G = S_8$ $\quad x = (1\,2)(5\,6\,7) \quad ; \quad x = (1\,2\,3\,5)(1\,3\,7\,8)$.

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

    c) $G = \mathcal{H}$ $\quad x = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

    d) $G = S^1$ $\quad x = \cos(\frac{2\pi}{n}) + i\ \sin(\frac{2\pi}{n})$.

    e) $G = D_4$ $\quad x = \rho^2\,\sigma \quad ; \quad x = \rho^3$.

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

16. Sea $x \in \mathbb{Z}_n$. Probar que $ord(x) = n$ si y sólo si $(x, n) = 1$.

17. *a*) Calcular el orden de todos los elementos de S_3.

    b) Sea $\sigma := (1\,3\,2)$,encontrar el subgrupo $C_\sigma = \{r \in S_3;\ r.\sigma = \sigma.r\}$.

    c) Hallar, si existe, un $\sigma \in S_3$ tal que el subgrupo C_σ tenga orden 1; tenga orden 2; tenga orden 3; tenga orden 6.

18. *a*) Hallar el orden de cada elemento de $\mathbb{Z}_{12}$ y determinar todos los $x \in \mathbb{Z}_{12}$ tales que el subgrupo cíclico generado por x coincide con $\mathbb{Z}_{12}$.

    b) Hallar el orden de cada elemento de $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ y en $\mathbb{Z}_4 \oplus \mathbb{Z}_6$.

    c) Inspirándose en *b*) probar que si G_1 y G_2 son grupos finitos, el orden de un elemento (g_1, g_2) en $G_1 \oplus G_2$ es el mínimo común múltiplo entre los órdenes de g_1 y g_2.

19. 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.

20. Sean $(G, \cdot)$ un grupo y $a, b \in G$

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

    1) $x \mapsto a \cdot x$ $\qquad$ 3) $x \mapsto a \cdot x \cdot a^{-1}$ $\qquad$ 5) $x \mapsto a \cdot x^{-1} \cdot a^{-1}$
    2) $x \mapsto a \cdot x \cdot b$ $\qquad$ 4) $x \mapsto x^{-1}$

    b) Determinar cuáles de estas aplicaciones son morfismos.

    c) Idem en el caso en que G sea abeliano.

21. Dados los grupos:

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

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

donde $\mathcal{K} = \{\pm 1, \pm i, \pm j, \pm k\}$ con $i^2 = j^2 = k^2 = -1$ y $i \cdot j = k = -j \cdot i$

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

22. Determinar si G y K son isomorfos en los casos:

   a) $G = \mathbb{Z}_4 \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_2$.
   b) $G = \mathbb{Z}_n \qquad K = G_n$.
   c) $G = \mathbb{Z}_{10} \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_5$.
   d) $G = \mathbb{Q} \qquad K = \mathbb{R}$.
   e) $G = \mathcal{U}_{16} \qquad K = \mathcal{H}$.
   f) $G = \mathcal{U}_{16} \qquad K = \mathbb{Z}_2 \oplus \mathbb{Z}_4$.
   g) $G = S_3 \qquad K = D_3$.
   h) $G = A_4 \qquad K = D_6$.

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

24. Sea $f : G \longrightarrow L$ un epimorfismo. Decidir para cuáles 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 6.
   (P_8) todo elemento tiene orden infinito.

25. Sea $f : G \longrightarrow L$ un monomorfismo. Decidir para cuáles P_i del ejercicio anterior vale: "L verifica $P_i \Rightarrow G$ verifica P_i".

26. *a*) Probar que $Aut(\mathbb{Z}) \simeq G_2$.
   b) Hallar $Hom(G_n\, , \mathbb{Z})$.
   c) Hallar $Hom(G\, , \mathbb{Z})$ para G un grupo de orden finito.

27. Sea $G = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} \; / \; a, b \in \mathbb{Z}_7, \text{ con } a \neq 0 \right\}$.

   a) Hallar el orden de G.
   b) Para cada primo p que divide al orden de G hallar todos los elementos de G que tengan orden p.

28. Sea p un número primo mayor que 2. Se considera el conjunto

$$G = \left\{ \left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) : \; a, b, c \in \mathbb{Z}_p \right\}$$

   Probar que G es un grupo no abeliano tal que todo elemento distinto de la identidad tiene orden p. ¿Qué pasa si $p = 2$?

29. *a*) Sean $a, b \in \mathbb{Z}$. Probar que $\{a, b\}$ es un sistema de generadores de $\mathbb{Z}$ si y sólo si $(a, b) = 1$.
   b) Probar que $\mathbb{Z}$ tiene sistemas de generadores minimales de n elementos $\forall n \in \mathbb{N}$.

30. Sea $G = M_2(\mathbb{Z}_2)$. Hallar $|G|$ y encontrar subgrupos de G de orden 2, 4 y 8.

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

    b) Probar que si $x^2 = 1$ para todo $x \in G$ entonces G es abeliano.

32. Probar que
    a) $Hom(\mathbb{Z}, \mathbb{Z}_n) \neq 0$.
    b) $Hom(\mathbb{Z}_5, \mathbb{Z}_7) = 0$.
    c) $Hom(\mathbb{Q}, \mathbb{Z}) = 0$.
    d) No existe un epimorfismo de $\mathbb{Z}$ en $\mathbb{Z} \oplus \mathbb{Z}$.

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

34. Sea $G = \left\{ \begin{pmatrix} 1 & b \\ 0 & a \end{pmatrix} \; / \; a, b \in \mathbb{Z}_4, \text{ con } (a,4) = 1 \right\}$. Probar que G es un grupo no abeliano de orden 8. ¿Es $G \simeq \mathcal{H}$? ¿Es $G \simeq D_4$?

35. Sea define la función de Euler $\varphi : \mathbb{N} \to \mathbb{N}$ de la siguiente forma:

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

a) Probar que si $(a,n) = 1$, entonces $a^{\varphi(n)} = 1(n)$.
Este resultado se conoce como *Teorema de Euler* y es una generalización del Pequeño Teorema de Fermat.

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

c) Probar que si $p \in \mathbb{N}$ es un primo y $r \in \mathbb{N}$, entonces

$$\varphi(p^r) = (p-1)p^{r-1}.$$

Concluir que si se conoce la factorización de n en primos, entonces se puede calcular $\varphi(n)$.

d) Probar que si $n, m \in \mathbb{N}$ son coprimos, entonces $\mathcal{U}_{nm} \simeq \mathcal{U}_n \times \mathcal{U}_m$.

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

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