APELLIDOS   NOMBRE

Observaciones:

-) Los cuatro ejercicios tienen el mismo valor. Cada ejercicio será puntuado sobre 10 para después calcular la nota global.

-) Para superar este examen habrá que alcanzar un mínimo de 3 puntos sobre 10 en cada uno de los ejercicios propuestos y sumar al menos 20 puntos entre los cuatro ejercicios.

Ejercicio 1. **a) (3 p.)** Sean X e Y unos conjuntos, $A \subset X$, $B \subset Y$ unos subconjuntos y $f : X \to Y$ una aplicación inyectiva. Probar que: $f^{-1}(f(A) \cap B) = A \cap f^{-1}(B)$.

b) (4 p.) Se considera la siguiente relación en $\mathbb{R}^2 \setminus \{(0,0)\}$:

$$\text{dados } (x,y),(x',y') \in \mathbb{R}^2 \setminus \{(0,0)\} : \qquad (x,y)\mathscr{R}(x',y') \overset{\text{def.}}{\iff} xy' = x'y.$$

Probar que $\mathscr{R}$ es una relación de equivalencia. ¿Cuál es la clase de equivalencia de $(1,0)$? ¿Y de $(1,1)$? Describir todas las clases de equivalencia de $\mathscr{R}$.

c) (3 p.) Sean X, Y, Z unos conjuntos y $f : Y \to Z$, $g : X \to Y, g' : X \to Y$ aplicaciones.
(c-1) Probar que si f es inyectiva y $f \circ g = f \circ g'$, entonces $g = g'$.
(c-2) Probar que si $f \circ g$ es sobreyectiva, entonces f es sobreyectiva.

Ejercicio 2. Se pide lo siguiente:

a) (3 p.) Enunciar el Teorema de Lagrange. Probar que si $f : G \to H$ es un homomorfismo sobreyectivo entre dos grupos finitos, entonces el orden de H divide al orden de G.

b) (2 p.) Contestar VERDADERO o FALSO a cada una de las afirmaciones siguientes[1]:

-) En $\mathbb{S}_4$ hay algún elemento de orden 6.	VERDADERO ☐	FALSO ☐
-) En $\mathbb{S}_7$ hay algún elemento de orden 12.	VERDADERO ☐	FALSO ☐
-) Hay algún epimorfismo $\mathbb{Z}/\mathbb{Z}20 \to \mathbb{Z}/\mathbb{Z}15$.	VERDADERO ☐	FALSO ☐
-) Hay algún monomorfismo $\mathbb{Z}/\mathbb{Z}7 \to \mathbb{Z}/\mathbb{Z}20$.	VERDADERO ☐	FALSO ☐

c) (2 p.) Encontrar dos subgrupos de $\mathbb{S}_5$ de orden 6, uno abeliano y otro no abeliano.

d) (3 p.) Sean G y H dos grupos (notados multiplicativamente), $f : G \to H$ un homomorfismo y G' un subgrupo de G. Probar que $f(G')$ es un subgrupo de H.

Ejercicio 3. **a) (2 p.)** Probar que $2^{341} \equiv 2 \pmod{341}$. (Se dice en este caso que el número 341 es **pseudo-primo en base** 2).

b) (2 p.) Probar que si p es primo y $m = k(p-1)+1$ entonces $a^m \equiv a \pmod{p}$.

c) (3 p.) Probar que si m es producto de primos distintos entonces $a \equiv b \pmod{m}$ si y sólo si $a \equiv b \pmod{p}$ para cada primo p dividendo a m.

d) (3 p.) Probar que $a^{561} \equiv a \pmod{561}$ para cualquier entero a. (El número 561, que no es primo, se dice que es un **número de Carmichael**).

Ejercicio 4. **a) (3 p.)** Probar que en $\mathbb{R}[x]$ los polinomios irreducibles tienen grado 1 o 2.

b) (3 p.) Sea el polinomio $f(x) = x^6 - 2x^5 + x^4 + 2x^3 - 8x^2 + 12x - 12$, Sabiendo que $\alpha = 1 + i$ es una raíz de $f(x)$, descomponerlo en factores irreducibles sobre $\mathbb{Z}$, $\mathbb{R}$ y $\mathbb{C}$.

c) (2 p.) Considerando ahora el polinomio anterior $f(x) \in \mathbb{F}_5[x]$, descomponerlo en factores irreducibles.

d) (2 p.) ¿Tiene $f(x)$ un inverso multiplicativo módulo $m(x) = x^4 + 3x^2 + 2$ en $\mathbb{F}_5[x]$? Calcularlo en caso afirmativo.

[1] No se pide probar nada. Cada respuesta correcta se contará como 0,5 puntos y cada respuesta incorrecta como -0,5 puntos. La puntuación de este apartado será siempre ≥ 0.