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.

Solución. **a)** Siempre se tiene que $f^{-1}(f(A) \cap B) = f^{-1}(f(A)) \cap f^{-1}(B) \supset A \cap f^{-1}(B)$. Para probar la otra inclusión basta probar, usando que f es inyectiva, que $f^{-1}(f(A)) \subset A$. Para ello, si $x \in f^{-1}(f(A))$, entonces $f(x) \in f(A)$, de donde existe un $x' \in A$ tal que $f(x) = f(x')$; como f es inyectiva, se tiene $x = x'$ y por tanto $x \in A$.

También se podría haber probado directamente sin utilizar ningún resultado previo por doble inclusión y aplicando sólo las definiciones:

$$x \in A \cap f^{-1}(B) \Rightarrow \cdots \Rightarrow x \in f^{-1}(f(A) \cap B); \; x \in f^{-1}(f(A) \cap B) \Rightarrow \cdots \Rightarrow x \in A \cap f^{-1}(B).$$

La primera cadena de implicaciones se prueba sin ninguna hipótesis sobre f, y para la segunda cadena hay que utilizar que f es inyectiva.

b) Las propiedades reflexiva y simétrica son muy fáciles y no las escribiremos. Veamos la transitiva. Sean $(x,y),(x',y'),(x'',y'') \in \mathbb{R}^2 \setminus \{(0,0)\}$ tales que $(x,y)\mathscr{R}(x',y')$ y $(x',y')\mathscr{R}(x'',y'')$, es decir: (i) $xy' = x'y$, (ii) $x'y'' = x''y'$. Deducimos:

$$xy' = x'y \overset{\cdot y''}{\Longrightarrow} xy'y'' = x'yy'' \overset{\text{(ii)}}{\Longrightarrow} xy'y'' = yx''y'.$$

Si y' fuera distinto de 0, podríamos cancelar y' y concluir que $xy'' = yx''$, de donde $(x,y)\mathscr{R}(x'',y'')$. Ahora bien, lo que sabemos es que $(x',y') \neq (0,0)$, y por tanto $y' \neq 0$ o $x' \neq 0$. Si y' fuera igual a cero, entonces x' sería distinto de 0 y procederíamos del siguiente modo:

$$x'y'' = x''y' \overset{\cdot x}{\Longrightarrow} xx'y'' = xx''y' \overset{\text{(i)}}{\Longrightarrow} xx'y'' = x'yx'' \overset{x' \neq 0}{\Longrightarrow} xy'' = yx'' \iff (x,y)\mathscr{R}(x'',y'').$$

Las clases de equivalencia de $(1,0)$ y $(1,1)$ son

$$\overline{(1,0)} = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid y = 0\}, \quad \overline{(1,1)} = \{(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\} \mid x = y\},$$

que correponden al eje OX privado del origen y a la diagonal del primer cuadrante privada del origen.

En general, la clase de equivalencia de (x,y) está formada por todos los vectores no nulos proporcionales a (x,y), y por tanto las clases de equivalencia de $\mathscr{R}$ serán las distintas rectas de $\mathbb{R}^2$ que pasan por el origen, privadas del origen.

(c-1) Supongamos que f es inyectiva. Si $f \circ g = f \circ g'$, entonces $(f \circ g)(x) = (f \circ g')(x)$ para todo $x \in X$, es decir $f(g(x)) = f(g'(x))$ para todo $x \in X$, y como f es inyectiva, $g(x) = g'(x)$ para todo $x \in X$, de donde $g = g'$.

(c-2) Supongamos que $f \circ g$ es sobreyectiva. Entonces, para cada $z \in Z$ existirá un $x \in X$ tal que $f(g(x)) = (f \circ g)(x) = z$, y por tanto, si tomamos $y = g(x) \in Y$ tendremos $f(y) = z$. Así pues, 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.

Solución. a)

Teorema de Lagrange: Si G es un grupo finito y H es un subrgrupo de G, entonces $|H|$ divide a $|G|$.

Llamemos K al núcleo de f. Por la factorización canónica de f deducimos que los grupos G/K y H son isomorfos y por tanto tienen el mismo número de elementos, es decir $\frac{|G|}{|K|} = |H|$, o lo que es lo mismo $|G| = |K| \cdot |H|$, y por tanto $|H|$ divide a $|G|$.

b)

-) 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) El subgrupo cíclico $G = \langle (12)(345) \rangle \subset \mathbb{S}_5$ es abeliano (todos los grupos cíclicos lo son) y tiene 6 elementos pues el orden de $(12)(345)$ es 6.

El grupo $\mathbb{S}_3$ tiene 6 elementos y sabemos que no es abeliano. Ahora bien, al grupo $\mathbb{S}_3$ lo podemos considerar como un subgrupo de $\mathbb{S}_5$. Concretamente se trataría del subgrupo de $\mathbb{S}_5$ formado por aquellas permutaciones de $\{1, 2, 3, 4, 5\}$ que dejan fijos a 4 y a 5.

d) Para probar que $f(G')$ es un subgrupo de H tenemos que probar:

(i) $e_H \in f(G')$: en efecto, $e_G \in G'$ por ser G' un subrgrupo de G y por tanto $e_H = f(e_G) \in f(G')$,

(ii) si $h, h' \in f(G')$, entonces $hh' \in f(G')$: en efecto, existen $g, g' \in G'$ tales que $f(g) = h$, $f(g') = h'$, y como G' es subgrupo de G, $gg' \in G'$ y por tanto $hh' = f(g)f(g') = f(gg') \in f(G')$,

(ii) si $h \in f(G')$, entonces $h^{-1} \in f(G')$: en efecto, existe $g \in G'$ tal que $h = f(g)$, y como G' es subgrupo de G, $g^{-1} \in G'$, de donde $h^{-1} = f(g)^{-1} = f(g^{-1}) \in f(G')$.

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**).

Solución. a) Dado que 341 y 2 son primos entre sí, podemos intentar aplicar el Teorema de Euler. Como $341 = 11 \cdot 31$, $\varphi(341) = 10 \cdot 30 = 300$, luego tenemos que $2^{300} \equiv 1 \pmod{341}$. De aquí deducimos que $2^{341} = 2^{300} \cdot 2^{41} \equiv 2^{41} \pmod{341}$. Y por aquí ya no podemos seguir avanzando.

Parece que debemos calcular las potencias de 2 módulo 341. Veamos, la primera que supera el valor de 341 es $2^9 = 512$. Tenemos

$$2^9 = 512 \equiv 171 \pmod{341}.$$

[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.

Multiplicando por 2 se tiene

$$2^{10} = 2^9 \cdot 2 \equiv 171 \cdot 2 = 342 \equiv 1 \pmod{341}.$$

Luego $2^{10} \equiv 1 \pmod{341}$. De este hecho se deduce fácilmente que $2^{340} \equiv 1 \pmod{341}$ y de aquí que

$$2^{341} \equiv 2 \pmod{341}.$$

b) Si $p \mid a$ entonces $a \equiv 0 \pmod{p}$ y $a^m \equiv 0 \pmod{p}$, luego $a^m \equiv a \pmod{p}$.

Si $p \nmid a$, por el teorema de Fermat se tiene que $a^{p-1} \equiv 1 \pmod{p}$. De aquí, dado que $m = k(p-1)+1$, obtenemos

$$a^m = a^{k(p-1)+1} = (a^{p-1})^k \cdot a \equiv a \pmod{p}.$$

c) Para la primera implicación no es necesaria la hipótesis de que "m sea producto de primos distintos". En efecto, sea p un factor (primo) de m, si $a \equiv b \pmod{m}$ entonces $m \mid a-b$, como $p \mid m$, tenemos que $p \mid a-b$. Es decir, $a \equiv b \pmod{p}$.

Recíprocamente, supongamos que "$m = p_1 \cdots p_r$ es producto de primos distintos" y que $a \equiv b \pmod{p_i}$ para todo $i = 1, \dots r$. Por tanto $p_i \mid a-b$ para todo $i = 1, \dots r$.

Sabemos que si a, b son dos enteros primos entre sí que dividen a un entero c entonces $ab \mid c$ (ver ejercicio 19 de la relación del tema 3).

Podemos extender este resultado por recurrencia (inducción) a los r factores primos distintos de m, pues $p_1 \cdots p_j$ y p_{j+1} son primos entre sí. Si ambos dividen a m entonces $p_1 \cdots p_j p_{j+1}$ también divide a m. Comenzando con $j = 1$ en $r-1$ pasos se tiene que

$$m = p_1 \cdots p_r \mid a-b.$$

De donde $a \equiv b \pmod{m}$.

d) Para probar que $a^{561} \equiv a \pmod{561}$ usaremos los apartados **b)** y **c)**.

Como $561 = 3 \cdot 11 \cdot 17$ es producto de primos distintos, por **c)** es suficiente probar que $a^{561} \equiv a \pmod{p}$ para cada valor de $p = 3, 11, 17$.

Ahora usamos el apartado **b)**:

-) $561 = 230 \cdot 2 + 1 \Rightarrow a^{561} \equiv a \pmod{3}$.
-) $561 = 56 \cdot 10 + 1 \Rightarrow a^{561} \equiv a \pmod{11}$.
-) $561 = 35 \cdot 16 + 1 \Rightarrow a^{561} \equiv a \pmod{17}$.

Luego $a^{561} \equiv a \pmod{561}$.

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.

Solución. **a)** Veamos primero que las raíces complejas no reales de un polinomio real vienen "por parejas". Sea $f(x) \in \mathbb{R}[x]$ un polinomio que tiene una raíz $\alpha = a + ib \in \mathbb{C} \setminus \mathbb{R}$, entonces $f(\alpha) = 0$. Conjugando se tiene

$$\overline{f(\alpha)} = f(\overline{\alpha}) = \overline{0} = 0.$$

Luego α y $\overline{\alpha}$ son raíces de $f(x)$.

Además $\alpha + \overline{\alpha} = 2a \in \mathbb{R}$ y $\alpha\overline{\alpha} = a^2 + b^2 \in \mathbb{R}$, de donde

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha} \in \mathbb{R}[x]$$

es un factor real e irreducible de $f(x)$.

Por tanto, si $f(x) \in \mathbb{R}[x]$ es un polinomio de grado mayor o igual que 3, pueden ocurrir dos cosas: que todas sus raíces sean reales o que tenga alguna raíz α compleja no real.

En el primer caso el polinomio es reducible pues se descompone en factores de grado 1. En el segundo caso el polinomio tiene como factor $(x-\alpha)(x-\overline{\alpha}) \in \mathbb{R}[x]$.

Luego todo polinomio real de grado mayor o igual que 3 es reducible.

b) Como $f(x)$ es un polinomio entero (real) y $\alpha = 1+i$ una raíz de $f(x)$ entonces $\overline{\alpha} = 1-i$ también es raíz. Luego el polinomio

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2x + 2 \in \mathbb{Z}[x]$$

es un factor de $f(x)$.

Dividiendo tenemos

$$\begin{array}{rl} x^6-2x^5\ +x^4+2x^3-8x^2+12x-12 = \left(x^2-2x+2\right)\left(x^4-x^2-6\right) \\ \underline{-x^6+2x^5-2x^4} \\ \quad -x^4+2x^3-8x^2 \\ \quad \underline{x^4-2x^3+2x^2} \\ \quad\quad -6x^2+12x-12 \\ \quad\quad \underline{6x^2-12x+12} \\ \quad\quad\quad 0 \end{array}$$

Sobre $\mathbb{Q}$ el factor x^2-2x+2 es irreducible, pues sus raíces α y $\overline{\alpha}$ no están en $\mathbb{Q}$.

Veamos qué ocurre con el otro factor x^4-x^2-6. Normalmente miraríamos ahora si alguna de las posibles raíces racionales (±1, ±2, ±3 y ±6) es raíz de este polinomio. Pero al ser un polinomio "bicuadrado" podemos despejar x^2 de la ecuación $x^4-x^2-6=0$ como en una ecuación de segundo grado:

$$x^2 = \frac{1\pm\sqrt{1+24}}{2} = \begin{cases} 3 \\ -2 \end{cases}.$$

Luego $x^4-x^2-6=(x^2-3)(x^2+2)$. Las raíces de x^2-3 son $\pm\sqrt{3}\in\mathbb{R}\setminus\mathbb{Q}$ y las de x^2+2 son $\pm\sqrt{2}i\in\mathbb{C}\setminus\mathbb{R}$. Sobre $\mathbb{Q}$ ambos polinomios son irreducibles.

Con esta información ya tenemos las factorizaciones

-) sobre $\mathbb{Z}$: $f(x)=(x^2-2x+2)(x^2-3)(x^2+2)$,
-) sobre $\mathbb{R}$: $f(x)=(x^2-2x+2)(x-\sqrt{3})(x+\sqrt{3})(x^2+2)$
-) y sobre $\mathbb{C}$: $f(x)=(x-\alpha)(x-\overline{\alpha})(x-\sqrt{3})(x+\sqrt{3})(x-\sqrt{2}i)(x+\sqrt{2}i)$

c) De la descomposición anterior sobre $\mathbb{Z}$, $f(x)=(x^2-2x+2)(x^2-3)(x^2+2)$ obtenemos una descomposición sobre $\mathbb{F}_5$:

$$f(x)=(x^2+3x+2)(x^2+2)(x^2+2)=(x^2+3x+2)(x^2+2)^2$$

cuyos factores pueden **no** ser irreducibles.

El factor $x^2+3x+2=(x+1)(x+2)$, sin embargo el factor x^2+2 es irreducible porque ninguno de los elementos de $\mathbb{F}_5$ es raíz. Luego la factorización es

$$f(x)=(x+1)(x+2)(x^2+2)^2.$$

d) El polinomio $f(x)$ tiene inverso multiplicativo módulo $m(x)$ si y sólo si $\mathrm{mcd}(f(x),m(x))=1$. Calculemos el máximo común divisor de ambos polinomios. Siguiendo el algoritmo de Euclides dividimos $f(x)$ entre $m(x)$:

$$f(x)=(x^2+3x+3)\cdot m(x)+r(x),$$

siendo $r(x)=3x^3+x^2+x+2$. Ahora, dividiendo $m(x)$ entre $r(x)$ se obtiene:

$$m(x)=(2x+1)\cdot r(x)+0.$$

Luego $\mathrm{mcd}(f(x),m(x))=r(x)=3x^3+x^2+x+2\neq 1$ y *$f(x)$ no tiene inverso multiplicativo módulo $m(x)$ en $\mathbb{F}_5[x]$*.