Ejercicio 1. Se pide lo siguiente:

1. (2 puntos) Dados unos conjuntos X, Y, unos subconjuntos $A \subset X$, $B \subset Y$ y una aplicación $f : X \to Y$, se pide:

a) La definición formal de la *imagen* de A por f, que denotamos por $f(A)$.

b) La definición formal de *anti-imagen* (o *imagen inversa*) de B por f, que denotamos por $f^{-1}(B)$.

c) Pruebe que si $B \subset f(X)$, entonces $f(f^{-1}(B)) = B$.

2. (2 puntos) Sean X,Y,Z conjuntos, $f : X \to Y$ una aplicación sobreyectiva y $h, h' : Y \to Z$ aplicaciones. Pruebe que si $h \circ f = h' \circ f$, entonces $h = h'$.

3. (3 puntos) Sean X,Y conjuntos, $f : X \to Y$ una aplicación y $\mathcal{S}$ una relación de equivalencia en Y. Definimos la siguiente relación $\mathcal{R}$ en X: dados $x, x' \in X$

$$x \mathcal{R} x' \overset{\text{def.}}{\Leftrightarrow} f(x) \mathcal{S} f(x').$$

a) Pruebe que $\mathcal{R}$ es una relación de equivalencia.

b) Pruebe que hay una aplicación inyectiva de $X/\mathcal{R}$ en $Y/\mathcal{S}$.

4. (3 puntos) Sean X e Y conjuntos. Para cada aplicación $f : X \to \mathcal{P}(Y)$ definimos la aplicación $\widehat{f} : Y \to \mathcal{P}(X)$ de la siguiente forma

$$\widehat{f}(y) := \{x \in X \mid y \in f(x)\} \quad \forall y \in Y.$$

Probar que la aplicación

$$f \in \mathcal{P}(Y)^X \longmapsto \widehat{f} \in \mathcal{P}(X)^Y$$

es biyectiva. (Indicación: tratar de definir una aplicación $\mathcal{P}(X)^Y \to \mathcal{P}(Y)^X$ que sea la inversa de la aplicación anterior.)

Solución.

1.

a): $f(A) = \{y \in Y \mid \exists x \in A \text{ tal que } y = f(x)\}$.

b): $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$.

c): Suponemos que $B \subset f(X)$, es decir, que todo elemento de B es imagen por f de algún elemento de X: $\forall b \in B \ \exists x \in X$ tal que $b = f(x)$.

Probemos $f(f^{-1}(B)) = B$ por doble inclusión. La inclusión $f(f^{-1}(B)) \subset B$ se verifica siempre sin ninguna hipótesis adicional (ver las notas de teoría). Probemos la otra inclusión $B \subset f(f^{-1}(B))$:

Si $b \in B$, por la hipótesis $B \subset f(X)$, existe un $x \in X$ tal que $f(x) = b$, de donde $x \in f^{-1}(B)$ y por tanto $f(x) \in f(f^{-1}(B))$, es decir, $b \in f(f^{-1}(B))$.

Esto prueba que $B \subset f(f^{-1}(B))$.

2. Para probar que $h = h'$ hemos de probar que para todo $y \in Y$, $h(y) = h'(y)$. Ahora bien, como f es sobre, para todo $y \in Y$ existe un $x \in X$ tal que $f(x) = y$, y por tanto

$$h(y) = h(f(x) = (h \circ f)(x) = (h' \circ f)(x) = h'(f(x) = h'(y).$$

3.

a): Es muy fácil y se deja al lector.

b): Hemos de definir una aplicación $X/\mathscr{R} \to Y/\mathscr{S}$ que sea inyectiva. El único dato de partida es la aplicación $f : X \to Y$. Los elementos del conjunto cociente $X/\mathscr{R}$ son las clases de equivalencia de $\mathscr{R}$ (en el conjunto X), que son de la forma $\mathscr{R}(x)$, con $x \in X$. Recordemos que

$$\mathscr{R}(x) = \{x' \in X \mid x\mathscr{R}x'\}.$$

De igual modo, los elementos del conjunto cociente $X/\mathscr{S}$ son las clases de equivalencia de $\mathscr{S}$ (en el conjunto Y) que serán de la forma $\mathscr{S}(y)$, con $y \in X$.

A cada $\mathscr{R}(x) \in X/\mathscr{R}$ lo único que se nos puede ocurrir asociarle en $Y/\mathscr{S}$ es $\mathscr{S}(f(x))$, pero tendremos que probar que dicha asociación está bien definida. Para ello, suponiendo que $\mathscr{R}(x) = \mathscr{R}(x')$ hay que comprobar que $\mathscr{S}(f(x)) = \mathscr{S}(f(x'))$, pero si $\mathscr{R}(x) = \mathscr{R}(x') \Rightarrow x\mathscr{R}x' \Rightarrow f(x)\mathscr{S}f(x') \Rightarrow \mathscr{S}(f(x)) = \mathscr{S}(f(x'))$. Así pues, la aplicación

$$\mathscr{R}(x) \in X/\mathscr{R} \longmapsto \mathscr{S}(f(x)) \in Y/\mathscr{S}$$

está bien definida. Para la inyectividad, dados $\mathscr{R}(x), \mathscr{R}(x') \in X/\mathscr{R}$, si sus imágenes son iguales, $\mathscr{S}(f(x)) = \mathscr{S}(f(x'))$, deducimos que $f(x)\mathscr{S}f(x')$ y, por definición de $\mathscr{R}$, que $x\mathscr{R}x'$, de donde $\mathscr{R}(x) = \mathscr{R}(x')$.

Lo anterior se puede expresar utilizando la propiedad universal del conjunto cociente. Para ello, notemos por $p : X \to X/\mathscr{R}$ y $q : Y \to Y/\mathscr{R}$ las proyecciones naturales y consideremos el siguiente diagrama (que es el único que podemos formar con los datos que nos dan):

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ X/\mathscr{R} & & Y/\mathscr{S}. \end{array}$$

Puesto que

$$x\mathscr{R}x' \Rightarrow f(x)\mathscr{S}f(x') \Rightarrow (q\circ f)(x) = q(f(x)) = \mathscr{S}(f(x)) = \mathscr{S}(f(x')) = q(f(x')) = (q\circ f)(x'),$$

la propiedad universal del conjunto cociente nos dice que existe una única aplicación $F : X/\mathscr{R} \to Y/\mathscr{S}$ que hace el diagrama anterior conmutativo, es decir, $F \circ p = q \circ f$.

Esta aplicación F coincide con la que hemos definido antes directamente, pero ahora, gracias a la propiedad universal, no hemos tenido que comprobar que está bien definida. La inyectividad de F se demuestra como antes.

4. Para mayor facilidad, pongámosle nombre a la aplicación que nos dan, por ejemplo, $H : \mathscr{P}(Y)^X \longrightarrow \mathscr{P}(X)^Y$, $H(f) = \widehat{f}$ para todo $f \in \mathscr{P}(Y)^X$.

Si nos proponen definir una aplicación en el otro sentido $\mathscr{P}(X)^Y \longrightarrow \mathscr{P}(Y)^X$, podemos intercambiar los papeles de X y de Y y definir $H' : \mathscr{P}(X)^Y \longrightarrow \mathscr{P}(Y)^X$ de forma análoga a H: $H'(g) = \widehat{g}$ para todo $g \in \mathscr{P}(X)^Y$, con

$$\widehat{g}(x) := \{y \in Y \mid x \in g(y)\} \quad \forall x \in X.$$

Veamos que $H' \circ H$ es la identidad, es decir, para todo $f \in \mathscr{P}(Y)^X$, $(H' \circ H)(f) = f$, o sea, $H'(H(f)) = f$. Notemos $g = H(f) = \widehat{f}$. Hemos de probar que $\widehat{g} = f$, es decir $\widehat{g}(x) = f(x)$ para todo $x \in X$. Pero hemos de tener en cuenta que $\widehat{g}(x)$ y $f(x)$ son

elementos de $\mathscr{P}(Y)$, es decir, subconjuntos de Y, y para probar que son iguales hemos de ver que tienen los mismos elementos, por ejemplo, por doble inclusión:

$\widehat{g}(x) \subset f(x)$: $\quad y \in \widehat{g}(x) \Rightarrow x \in g(y) \overset{g=\widehat{f}}{\Longrightarrow} x \in \widehat{f}(y) \Rightarrow y \in f(x)$.

$f(x) \subset \widehat{g}(x)$: $\quad y \in f(x) \Rightarrow x \in \widehat{f}(y) \overset{g=\widehat{f}}{\Longrightarrow} x \in g(y) \Rightarrow y \in \widehat{g}(x)$.

La prueba de que $H \circ H'$ es la identidad es completamente similar (cambiar los papeles de X y de Y). De hecho, habiendo demostrado que $H' \circ H$ es la identidad, puesto que lo hemos hecho para cualesquiera conjuntos X e Y, también hemos demostrado que $H \circ H'$ es la identidad.

Ejercicio 2.

1. (2 puntos). Define subgrupo normal, enuncia una condición equivalente y demuestra que lo es.

2. (3 puntos). Prueba que los siguientes grupos son isomorfos:

a) $(\mathbb{R}, +)$ y $((0, +\infty), \cdot)$.

b) $(\mathbb{Z}/\mathbb{Z}2, +)$ y $(\{\pm 1\}, \cdot)$.

c) El grupo cíclico $\mathscr{C}_n = \{1, x, ..., x^{n-1}\}$ de orden n y el subgrupo de S_n generado por el ciclo $(1\,2\,...\,n)$.

3. (5 puntos). En el conjunto $\{1, 2, 3, 4\}$ consideramos las siguientes particiones:

$$\begin{aligned} X_1 &= \{\{1,2\},\{3,4\}\} \\ X_2 &= \{\{1,3\},\{2,4\}\} \\ X_3 &= \{\{1,4\},\{2,3\}\} \end{aligned}$$

Sea $\sigma \in S_4$. Vamos a definir la acción de σ sobre cada X_i de una forma natural. Por ejemplo, si consideramos

$$X_3 = \{\{1,4\},\{2,3\}\},$$

$\sigma(X_3)$ será la partición que venga dada por

$$\{\{\sigma(1), \sigma(4)\}, \{\sigma(2), \sigma(3)\}\}.$$

a) Calcula $\sigma(X_i)$ y $\tau(X_i)$ para $i = 1, 2, 3$ y para

$$\sigma = (1\,2\,3\,4), \quad \tau = (1\,2)\ (3\,4).$$

b) Definimos la aplicación $\varphi : S_4 \longrightarrow S_3$, que envía cada permutación σ a la permutación que induce en el conjunto $\{X_1, X_2, X_3\}$. Asumimos (NO hay que probarlo) que φ es un homomorfismo de grupos. Hallar $\ker(\varphi)$.

c) Probar que φ es sobreyectiva.

SOLUCIÓN. **1.** Ver las notas de teoría.

2.

a): Consideramos la aplicación $f : \mathbb{R} \longrightarrow (0, +\infty)$ dada por la exponencial: $f(x) = e^x$ para todo $x \in \mathbb{R}$. Se trata de un homomorfismo de grupos por las propiedades de la exponencial: $e^{x+y} = e^x e^y$, $e^0 = 1$. Es además un isomorfismo porque es una aplicación biyectiva, siendo la aplicación inversa la aplicación dada por el logaritmo.

b): Consideremos la aplicación $f : \mathbb{Z}/\mathbb{Z}2 \longrightarrow \{1, -1\}$ dada por $f(\overline{0}) = 1$, $f(\overline{1}) = -1$. Es obviamente biyectiva y es un homomorfismo de grupos, pues $f(\overline{0}+\overline{0}) = f(\overline{0}) = 1 = f(\overline{0})f(\overline{0})$, $f(\overline{0}+\overline{1}) = f(\overline{1}) = -1 = f(\overline{0})f(\overline{-1})$, $f(\overline{1}+\overline{1}) = f(\overline{0}) = 1 = f(\overline{-1})f(\overline{-1})$.

Otra manera de responder a este apartado sería diciendo que ambos grupos son cíclicos del mismo orden y por tanto son isomorfos (lo sabemos por la teoría).

c): Ambos grupos son cíclicos del orden n y por tanto son isomorfos.

3.

a): Para $\sigma = (1\,2\,3\,4)$ tenemos

$$\sigma(X_1) = \{\{\sigma(1), \sigma(4)\}, \{\sigma(2), \sigma(3)\}\} = \{\{2, 1\}, \{3, 4\}\} = X_3,$$

$$\sigma(X_2) = \{\{\sigma(1), \sigma(3)\}, \{\sigma(2), \sigma(4)\}\} = \{\{2, 4\}, \{3, 1\}\} = X_2,$$

$$\sigma(X_3) = \cdots = X_1.$$

Para $\tau = (1\,2)\ (3\,4)$ tenemos

$$\tau(X_1) = \cdots = X_1, \quad \tau(X_2) = \cdots = X_2, \quad \tau(X_3) = \cdots = X_3.$$

b): Según hemos visto en a), la permutación τ induce la permutación identidad de $\{X_1, X_2, X_3\}$ y por tanto $\tau \in \ker(\varphi)$. Sin embargo la permutación σ induce la permutación $(1\,3)$ de $\{X_1, X_2, X_3\}$ y no pertenece pues al $\ker(\varphi)$.

Comprobamos como en a) que los productos de dos transposiciones disjuntas $(1\,3)\ (2\,4)$ y $(1\,4)\ (2\,3)$ también inducen la permutación identidad de $\{X_1, X_2, X_3\}$ y por tanto están en $\ker(\varphi)$. Así pues

$$\{(\,), (1\,2)\ (3\,4), (1\,3)\ (2\,4), (1\,4)\ (2\,3)\} \subset \ker(\varphi).$$

Si en $\ker(\varphi)$ hubiera algún elemento además de los anteriores, como se trata de un subgrupo normal, tendrían que estar también todos sus conjugados. Así pues basta que veamos si en $\ker(\varphi)$ hay algún ciclo de orden 3 (si está uno, estarán todos) o alguno de orden 4 (si está uno, estarán todos). Nótese que los elementos de S_4 sólo son de los siguientes tipos: la identidad, las transposiciones, los productos de dos transposiciones disjuntas, los ciclos de orden 3 y los ciclos de orden 4.

De orden 4 ya sabemos que hay uno que no está: σ, y por tanto en $\ker(\varphi)$ no hay ningún ciclo de orden 4.

Veamos qué pasa con los de orden 3. Consideremos $\varrho = (1\,2\,3)$:

$$\varrho(X_1) = \{\{\varrho(1), \varrho(4)\}, \{\varrho(2), \varrho(3)\}\} = \{\{2, 4\}, \{3, 1\}\} = X_2.$$

Sin tener que hacer más cálculos, ya sabemos que ϱ no induce la permutación identidad de de $\{X_1, X_2, X_3\}$ y por tanto no está en $\ker(\varphi)$.

Así concluimos que

$$\{(\,), (1\,2)\ (3\,4), (1\,3)\ (2\,4), (1\,4)\ (2\,3)\} = \ker(\varphi).$$

c): Por la factorización canónica, sabemos que

$$S_4/\ker(\varphi) \simeq \mathrm{Im}(\varphi)$$

y por tanto $\mathrm{Im}(\varphi)$ tendrá $\frac{4!}{4} = 6$ elementos, los mismos que S_3, por lo que $\mathrm{Im}(\varphi) = S_3$ y φ es sobreyectiva.

Los apartados b) y c) también se podrían haber resuelto calculando las permutaciones inducidas en $\{X_1, X_2, X_3\}$ por cada una de las 24 permutaciones de S_4, de la misma forma que en el apartado a).

Este procedimiento admite algunas variantes. Por ejemplo, para demostrar la sobreyectividad de φ bastaría calcular las permutaciones inducidas en $\{X_1, X_2, X_3\}$ por cada una de las 6 transposiciones de S_4. Así veríamos que obtenemos todas las transposiciones de $\{X_1, X_2, X_3\}$, y como las transposiciones generan a cada S_n, concluiríamos que φ es sobreyectiva.

Ejercicio 3.

1. (2,5 puntos)

a) Defina dominio de integridad.

b) Defina ideal de un anillo.

c) Sean I y J dos ideales no nulos de un dominio de integridad. Pruebe que $I \cap J \neq 0$.

2. (2,5 puntos) Sean m y n dos enteros positivos. En un juego, un jugador comienza con 0 puntos, y en cada jugada puede ganar n puntos, perder n puntos, ganar m puntos o perder m puntos. Conteste razonadamente: ¿Cuál es la mínima cantidad positiva de puntos que puede llegar a tener?

3. (2,5 puntos) ¿Cuántas soluciones tiene, en el anillo $\mathbb{Z}/\mathbb{Z}943$, la ecuación $851x \equiv 161$? Hallarlas todas.

4. (2,5 puntos) Sean $1 < a < n$ números enteros. Conteste razonadamente:

a) ¿Es posible que $a^{\varphi(n)} \equiv 0 \pmod{n}$?

b) ¿Es posible que $a^m \equiv 1 \pmod{n}$ con $0 < m < \varphi(n)$?

c) ¿Es posible que $a^n \equiv 1 \pmod{n}$?

d) ¿Es posible que $a^n \equiv 1 \pmod{n}$ si n es primo?

Solución.

1.

a) Un dominio de integridad es un anillo conmutativo y unitario sin divisores de cero, es decir, un anillo conmutativo y unitario A tal que para cualesquiera $x, y \in A$, si $x \neq 0$ e $y \neq 0$ se tiene $xy \neq 0$.

b) Un ideal I de un anillo $(A, +, \cdot)$ es un subconjunto no vacío $I \subset A$ tal que $(I, +)$ es un subgrupo de $(A, +)$, y además para todo $x \in A$ y todo $y \in I$ se tiene $xy \in I$.

c) Sean I y J dos ideales no nulos de un dominio de integridad A. Como son no nulos, existen elementos $x \in I$ e $y \in J$ tales que $x \neq 0$ e $y \neq 0$.

Como $x \in I$, $y \in A$ e I es un ideal, entonces $xy \in I$. Como $x \in A$, $y \in J$ y J es un ideal, entonces $xy \in J$. Por tanto, $xy \in I \cap J$.

Como $x \neq 0$, $y \neq 0$ y A es un dominio de integridad, $xy \neq 0$. Por tanto $I \cap J$ contiene un elemento distinto de cero, luego es un ideal no nulo.

2. Según las reglas del juego, las posibles puntuaciones del jugador son los números enteros de la forma $xm + yn$, con $x, y \in \mathbb{Z}$.

Sea $d = \mathrm{mcd}(m, n)$. Por la identidad de Bézout, existen números enteros α y β tales que $\alpha m + \beta n = d$. Por tanto, d es una posible puntuación del juego.

Por otra parte, d divide a m y a n, luego divide a cualquier puntuación de la forma $xm + yn$, con $x, y \in \mathbb{Z}$. Por tanto, d es la menor puntuación positiva posible.

3. Para ver si la ecuación tiene solución, calculamos el máximo común divisor de 943 y 851, mediante el algoritmo de Euclides.

$$943 = 1 \cdot 851 + 92$$

$$851 = 9 \cdot 92 + 23$$

$$92 = 4 \cdot 23 + 0$$

El último resto no nulo es 23, luego $\text{mcd}(943, 851) = 23$. Como $161 = 23 \cdot 7$, tenemos que $\text{mcd}(943, 851) = 23|161$, luego la ecuación

$$851x \equiv 161 \pmod{943}$$

tiene 23 soluciones.

Para hallarlas, dividimos los tres números que aparecen en la ecuación por 23, y obtenemos:

$$37x \equiv 7 \pmod{41}$$

Para despejar la x, hallamos el inverso de 37 módulo 41, usando la identidad de Bézout:

$$41 = 1 \cdot 37 + 4$$

$$37 = 9 \cdot 4 + 1$$

Por tanto: $1 = 37 - 9 \cdot 4 = 37 - 9(41 - 37) = 10 \cdot 37 - 9 \cdot 41$.

Observando esta igualdad módulo 41, vemos que el inverso de 37 módulo 41 es 10. Por tanto, despejando la x queda:

$$x \equiv 10 \cdot 7 \pmod{41}$$

$$x \equiv 70 \pmod{41}$$

$$x \equiv 29 \pmod{41}$$

Luego las 23 soluciones de la ecuación, en $\mathbb{Z}/\mathbb{Z}943$, son las del conjunto $\{29 + k41;\ k = 0, \ldots, 22\}$.

4. Sean $1 < a < n$ números enteros. Conteste razonadamente:

a) ¿Es posible que $a^{\varphi(n)} \equiv 0 \pmod{n}$? Sí, es posible. $2^2 \equiv 0 \pmod{4}$.

b) ¿Es posible que $a^m \equiv 1 \pmod{n}$ con $0 < m < \varphi(n)$? Sí, es posible. $2^3 \equiv 1 \pmod{7}$.

c) ¿Es posible que $a^n \equiv 1 \pmod{n}$? Sí, es posible. $3^4 \equiv 1 \pmod{4}$.

d) ¿Es posible que $a^n \equiv 1 \pmod{n}$ si n es primo?

No es posible. Como $1 < a < n$ y n es primo, a es primo con n. Entonces podemos aplicar el pequeño teorema de Fermat, y tenemos:

$$a^{n-1} \equiv 1 \pmod{n}.$$

Multiplicando la ecuación por a:

$$a^n \equiv a \pmod{n}.$$

Pero como $1 < a < n$, tenemos que $a \not\equiv 1 \pmod{n}$, luego

$$a^n \not\equiv 1 \pmod{n}.$$

Ejercicio 4.

1. (4 puntos) Probar el criterio de Eisenstein: "Sea un polinomio de grado $n > 0$

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \ , \ a_i \in \mathbb{Z}, i = 0, 1, \ldots, n.$$

Supongamos que existe un elemento irreducible $p \in \mathbb{Z}$ que divide a todos los coeficientes, salvo a a_n, y cuyo cuadrado p^2 no divide a a_0. Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$."
2. (3 puntos) Sea $f(x) = x^4 - 4x^3 + 6x^2 + x + 1 \in \mathbb{Z}[x]$. ¿Es $f(x)$ irreducible sobre $\mathbb{Q}$? (Indicación: Calcular $f(x+1)$).
3. (3 puntos) Sea $f(x) \in \mathbb{Z}[x]$ un polinomio. Notaremos por la misma letra $f(x)$ al correspondiente polinomio en $\mathbb{F}_p[x]$ con p primo. Razonar la veracidad o falsedad de las siguientes afirmaciones:

a) Si $f(x)$ es irreducible sobre $\mathbb{Q}$ también es irreducible sobre $\mathbb{F}_p$.
b) Si $f(x)$ es irreducible sobre $\mathbb{F}_p$ también es irreducible sobre $\mathbb{Q}$.

Solución.
1. Lo probaremos por reducción al absurdo. Supongamos que $f(x)$ es reducible en $\mathbb{Q}[x]$. En consecuencia se descompondrá en $\mathbb{Q}[x]$ en producto de dos polinomios de grado estrictamente inferior. Por el Lema de Gauss, se puede escribir

$$f(x) = (b_s x^s + b_{s-1}x^{s-1} + \ldots + b_1 x + b_0)(c_t x^t + c_{t-1}x^{t-1} + \ldots + c_1 x + c_0),$$

donde $b_i, c_j \in \mathbb{Z}$ para cualesquiera i, j y $s, t < n$.

Por la segunda hipótesis, p debe dividir a uno de entre b_0 y c_0, pero no a ambos. Supongamos pues sin pérdida de generalidad que $p|b_0$ y no divide a c_0. Como p no divide a a_n, no puede dividir a todos los b_i. Sea m el mínimo índice tal que p no divide a b_m, que sabemos que es menor que n. El coeficiente del término en x^m es

$$b_m c_0 + b_{m-1}c_1 + \ldots + b_0 c_m = a_m,$$

que no es divisible por p pues todos los sumandos lo son salvo el primero. Ahora bien, que a_m con $m < n$ no sea divisible por p es una contradicción, luego hemos terminado con la prueba.
2. Sea k un cuerpo y sea $f(x) \in k[x]$. Sabemos que si $f(x) = g(x) \cdot h(x)$ entonces $f(x+a) = g(x+a) \cdot h(x+a)$ para todo $a \in k$. Por tanto, $f(x)$ es reducible si y sólo si $f(x+a)$ es reducible.

Sea $f(x) = x^4 - 4x^3 + 6x^2 + x + 1 \in \mathbb{Z}[x]$, entonces $f(x+1) = x^4 + 5x + 5$. El polinomio $f(x+1)$ es irreducible por el criterio de Eisenstein (5 divide a todos los coeficientes menos al líder y 25 no divide al término independiente). Por tanto, $f(x)$ es irreducible.
3.

a) Es falso. El polinomio $f(x) = x^2 + 2$ es irreducible sobre $\mathbb{Q}$, pero $f(x) = x^2 \in \mathbb{F}_2[x]$ es reducible.

b) Es verdadero. Si un polinomio $f(x) \in \mathbb{Q}[x]$ es reducible, entonces $f(x) = g(x) \cdot h(x)$. Como al pasar a $\mathbb{F}_p$ se verifica que la clase del producto es el producto de las clases, se tiene que también $\bar{f}(x) = \bar{g}(x) \cdot \bar{h}(x)$ en $\mathbb{F}_p[x]$. Por tanto, si un polinomio es irreducible sobre $\mathbb{F}_p$ debe serlo también sore $\mathbb{Q}$