APELLIDOS NOMBRE

Instrucciones. Escribir la respuesta a cada cuestión en hojas separadas. Entregar al final las hojas ordenadas por cuestiones. Durante la realización del examen exclusivamente se podrá disponer de material de escritura. Ningún otro objeto está permitido. El examen se puntuará sobre 30 puntos y cada uno de los ejercicios sobre 10 puntos.

Ejercicio 1. (10 puntos) De los 3 apartados siguientes, **contestar al primero y elegir uno de entre los otros dos**:

1. (6 puntos) Sea $f : G \to G'$ un homomorfismo de grupos y H' un subgrupo normal de G'. Probar que $f^{-1}(H')$ es un subgrupo normal de G. Probar que hay un homomorfismo natural inyectivo $G/f^{-1}(H') \hookrightarrow G'/H'$.

Solución. Probemos primero que $f^{-1}(H')$ es un subgrupo de G. Como $f(e_G) = e_{G'} \in H'$ (puesto que H' es un subgrupo de G'), se tiene que $e_G \in f^{-1}(H')$.

Si $x, y \in f^{-1}(H')$, se tiene que $f(x), f(y) \in H'$, y como H' es un subgrupo de G', $f(x)f(y)^{-1} \in H'$. Ahora bien, por ser f homomorfismo: $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} \in H'$, de donde $xy^{-1} \in f^{-1}(H')$.

Veamos ahora que $f^{-1}(H')$ es un subgrupo normal de G, i.e. que para todo $z \in G$ y para todo $x \in f^{-1}(H')$, ha de tenerse que $zxz^{-1} \in f^{-1}(H')$. Ahora bien, por ser f homomorfismo: $f(zxz^{-1}) = f(z)f(x)f(z^{-1}) = f(z)f(x)f(z)^{-1}$, que debe pertenecer a H' puesto que $f(x) \in H'$, $f(z) \in G'$ y H' es un subgrupo normal de G'

Para la última parte, consideremos el homomorfismo $g : G \longrightarrow G'/H'$ que se obtiene al componer la proyección natural $G' \longrightarrow G'/H'$ con $f : G \longrightarrow G'$. Primero comprobamos que el núcleo de g coincide con $f^{-1}(H')$. El homomorfismo natural inyectivo que nos piden es la composición de la inclusión de $\mathrm{Im}(g)$ en G'/H' con el isomorfismo $\overline{g} : G/\ker(g) = G/f^{-1}(H') \xrightarrow{\sim} \mathrm{Im}(g)$ que aparece en la factorización canónica de g.

2. (4 puntos, **a elegir**) Sea A un anillo e $I \subset A$ un ideal. Probar que I es un ideal primo si y sólo si A/I es un dominio de integridad.

Solución. Ver las notas del Tema 3.

3. (4 puntos, **a elegir**) Enunciar y probar el Lema de Gauss.

Solución. Ver las notas del Tema 4.

Ejercicio 2. (10 puntos) Se pide lo siguiente:

1. (5 puntos) Sea $N > 1$ un número natural fijo. Discutir, dependiendo de N, si el siguiente sistema de congruencias tiene soluciones o no, y cuando las tenga, calcularlas:

$$\begin{array}{rcl} x & \equiv & 6 \pmod{N} \\ x & \equiv & 7 \pmod{N+1}. \end{array}$$

Solución. Como N y $N+1$ son primos entre sí (de hecho se tiene la siguiente igualdad de Bézout: $(-1)N + (N+1) = 1$), el sistema tiene solución única módulo $N(N+1)$. Calculemos dicha solución. Por la primera ecuación, $x = 6 + Nk$, $k \in \mathbb{Z}$ y sustituyendo en la segunda ecuación:

$$6 + Nk \equiv 7 \pmod{N+1} \iff Nk \equiv 1 \pmod{N+1}.$$

Utilizando la identidad de Bézout $(-1)N + (N+1) = 1$ deducimos que el inverso de la clase de N en $\mathbb{Z}/\mathbb{Z}(N+1)$ es la clase de -1 (o de N) y por tanto:

$$k \equiv -1 \pmod{N+1} \iff k \equiv N \pmod{N+1} \iff k = N + \ell(N+1),\ \ell \in \mathbb{Z}.$$

Sustituyendo en la expresión de x obtenemos:

$$x = 6 + Nk = 6 + N(N + \ell(N+1)) = 6 + N^2 + \ell(N(N+1)),$$

y por tanto la solución del sistema es: $x \equiv 6 + N^2 \pmod{N(N+1)}$.

1. (5 puntos) Calcular el resto de la división euclídea de $8^{23^{61}}$ al dividirlo por 27.

Solución. Se trata de calcular el entero x con $0 \leq x < 27$ tal que

$$8^{23^{61}} \equiv x \pmod{27}.$$

Por el Teorema de Euler, puesto que $\mathrm{mcd}(8, 27) = 1$, sabemos que:

$$8^{\phi(27)} \equiv 1 \pmod{27},$$

con $\phi(27) = \phi(3^3) = (3-1)3^2 = 18$. Nos interesará pues calcular el resto de la división de 23^{61} por 18, que llamaremos y:

$$23^{61} \equiv y \pmod{18}, \quad 0 \leq y < 18,$$

y como 23 es congruente con 5 módulo 18, tendremos

$$23^{61} \equiv 5^{61} \equiv y \pmod{18}, \quad 0 \leq y < 18.$$

Se trata de nuevo de una aplicación del Teorema de Euler. Puesto que $\mathrm{mcd}(5, 18) = 1$, sabemos que:

$$5^{\phi(18)} \equiv 1 \pmod{18},$$

con $\phi(18) = \phi(2 \cdot 3^2) = \phi(2)\phi(3^2) = 1 \cdot (3-1) \cdot 3 = 6$. Por tanto $5^{61} = 5^{10 \cdot 6 + 1} = (5^6)^{10} \cdot 5$

$$5^{61} \equiv 5 \equiv y \pmod{18} \implies y = 5.$$

Así pues, $23^{61} = q \cdot 18 + 5$, de donde

$$8^{23^{61}} \equiv (8^{18})^q \cdot 8^5 \equiv 8^5 \equiv x \pmod{27},$$

y el resto x buscado será el resto de la división de 8^5 por 27. Ahora bien

$$8^5 \equiv 8^2 \cdot 8^2 \cdot 8 \equiv 64 \cdot 64 \cdot 8 \equiv 10 \cdot 10 \cdot 8 \equiv 17 \pmod{27}$$

y por tanto: $\boxed{x = 17}$.

Ejercicio 3. (10 puntos) Se pide lo siguiente:

1. (3 puntos) Consideremos el polinomio $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}[x]$ y el anillo cociente $A = \mathbb{Q}[x]/\langle f(x) \rangle$. ¿Por qué la clase de x en A es una unidad? Calcular su inverso (en A). Dar un divisor de 0 concreto y no nulo de A.

Solución. La clase de x en A es una unidad si y sólo si $\mathrm{mcd}(x, f(x)) = 1$, lo que es cierto pues: $f(x) - (x^2 + x + 1)x = 1$ (esta sería una identidad de Bézout) para x y $f(x)$).

El inverso de la clase de x en A será por tanto la clase de $-(x^2 + x + 1)$ en A.

Como $f(-1) = 0$, se tiene que $X + 1$ es un divisor de $f(x)$. De hecho $f(x) = (x+1)(x^2+1)$. Las clases de $x + 1$ y de $x^2 + 1$ en A son distintas de 0, y sin embargo su producto es 0, por tanto ambas clases son divisores de 0 no nulos de A.

2. (3 puntos) Sea $p > 0$ un primo fijo. Para cada entero $d \geq 2$ dar un ejemplo de un polinomio de grado d mónico $g(x) \in \mathbb{Z}[x]$ que sea irreducible en $\mathbb{Q}[x]$ y para el que su reducción módulo p no sea irreducible en $\mathbb{F}_p[x]$.

Solución. El polinomio $f_d(x) := x^d + px^{d-1} + \cdots + px + p \in \mathbb{Z}[x]$ está en las condiciones que establece el criterio de Eisenstein y por lo tanto es irreducible en $\mathbb{Q}[x]$ (y en $\mathbb{Z}[x]$). Ahora bien, su reducción módulo p es el polinomio $x^d \in \mathbb{F}_p[x]$, que obviamente no es irreducible ($d \geq 2$).

3. (2 puntos) Sea $p > 0$ un primo y $h(x) \in \mathbb{F}_p[x]$ un polinomio irreducible de grado $d \geq 2$. ¿Es $K = \mathbb{F}_p[x]/\langle h(x) \rangle$ un cuerpo? ¿Cuántos elementos tiene K? ¿Cúal es el orden del grupo de las unidades de K?

UNIVERSIDAD DE SEVILLA

Solución. Sabemos por las notas de Teoría que si k es un cuerpo e $I = \langle f(x) \rangle \subset k[x]$ es un ideal no nulo y distinto del total, i.e. $f(x) \neq 0$ y $f(x)$ no es constante, el cociente $k[x]/I$ es un cuerpo si y sólo si $f(x)$ es un polinomio irreducible. Así pues K es un cuerpo.

El número de elementos de K es el número de restos distintos módulo $f(x)$, es decir, la cantidad de polinomios de $k[x]$ de grado $\leq d-1$. Por tanto K tiene p^d elementos.

Como K es un cuerpo, el grupo de sus unidades consistirá en todos sus elementos no nulos y por tanto su orden será $p^d - 1$.

4. (2 puntos) Siguiendo con las condiciones del apartado 3., si $q(x) \in \mathbb{F}_p[x]$ es un polinomio no divisible por $h(x)$, ¿se tiene que $h(x)$ divide a $q(x)^{p^d-1} - 1$?

Solución. Si $q(x) \in \mathbb{F}_p[x]$ es un polinomio no divisible por $h(x)$, entonces su clase $\overline{q(x)}$ en K será una unidad, por lo que, de forma análoga a la prueba del Pequeño Teorema de Fermat (que usa un corolario del Teorema de Lagrange), deducimos que:

$$\overline{q(x)}^{p^d-1} = \overline{1} \iff \overline{(q(x)^{p^d-1} - 1)} = \overline{0},$$

es decir $q(x)^{p^d-1} - 1$ es múltiplo de $h(x)$.

UNIVERSIDAD DE SEVILLA